TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GTVT
KHOA CÔNG NGHỆ THÔNG TIN

Lê Đàm Tuấn Đạt
Trần Thị Lan Anh
Hoàng Ngọc Khánh

ĐỒ ÁN PHÂN TÍCH VÀ THIẾT KẾ MẠNG MÁY TÍNH

ĐỒ ÁN

Ngành: Mạng máy tính và truyền thông dữ liệu

HÀ NỘI - 2023

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GTVT
KHOA CÔNG NGHỆ THÔNG TIN

Lê Đàm Tuấn Đạt
Trần Thị Lan Anh
Hoàng Ngọc Khánh

ĐỒ ÁN PHÂN TÍCH VÀ THIẾT KẾ MẠNG MÁY TÍNH

ĐỒ ÁN
Ngành: Mạng máy tính và truyền thông dữ liệu

Giảng viên hướng dẫn: Th.s Lương Hoàng Anh

HÀ NỘI - 2023

MỤC LỤC

MỤC LỤC ẢNH

CHƯƠNG I : CƠ SỞ LÝ THUYẾT

1.1. Định nghĩa về mạng máy tính

Mạng máy tính là tập hợp các máy tính đơn lẻ được kết nối với nhau bằng các phương tiện truyền vật lý (Transmission Medium) và theo một kiến trúc mạng xác định (Network Architecture).

Mạng viễn thông cũng là mạng máy tính. Các node chuyển mạch là hệ thống máy tính được kết nối với nhau bằng các đường truyền dẫn và hoạt động truyền thông tuân theo các chuẩn mô hình tham chiếu OSI.

1.2. Phân loại mạng máy tính

1.2.1. Phân loại mạng theo khoảng cách địa lý

Hiện nay, mạng máy tính được phát triển khắp nơi với những ứng dụng ngày càng đa dạng nên việc phân loại mạng máy tính là một việc rất phức tạp. Người ta có thể chia các mạng máy tính theo khoảng cách địa lý ra làm các loại mạng sau :

Mạng cục bộ LAN (Local Area Networks):

Mạng cục bộ LAN: kết nối các máy tính đơn lẻ thành mạng nội bộ, tạo khả năng trao đổi thông tin và chia sẻ tài nguyên trong cơ quan, xí nghiệp... Có hai loại mạng LAN khác nhau: LAN nối dây (sử dụng các loại cáp) và LAN không dây (sử dụng sóng cao tần hay tia hồng ngoại). Đặc điểm của mạng LAN :

- Có băng thông lớn
- Phạm vi kết nối có giới hạn tương đối nhỏ.
- Chi phí thấp

Mạng diện rộng WAN (Wide Area Network):

Mạng diện rộng WAN (Wide Area Network): phạm vi của mạng có thể vượt qua biên giới quốc gia và thậm chí cả lục địa. Cáp truyền qua đại dương hoặc vệ tinh được dùng cho việc truyền dữ liệu trong mạng WAN. Đặc điểm cảu mạng WAN :

- Hoạt động trên phạm vi một quốc gia hoặc trên toàn cầu.
- Tốc độ truyền dữ liệu thấp so với mạng cục bộ.
- Lỗi truyền cao.

Mạng toàn cầu GAN (Global Area Network) :

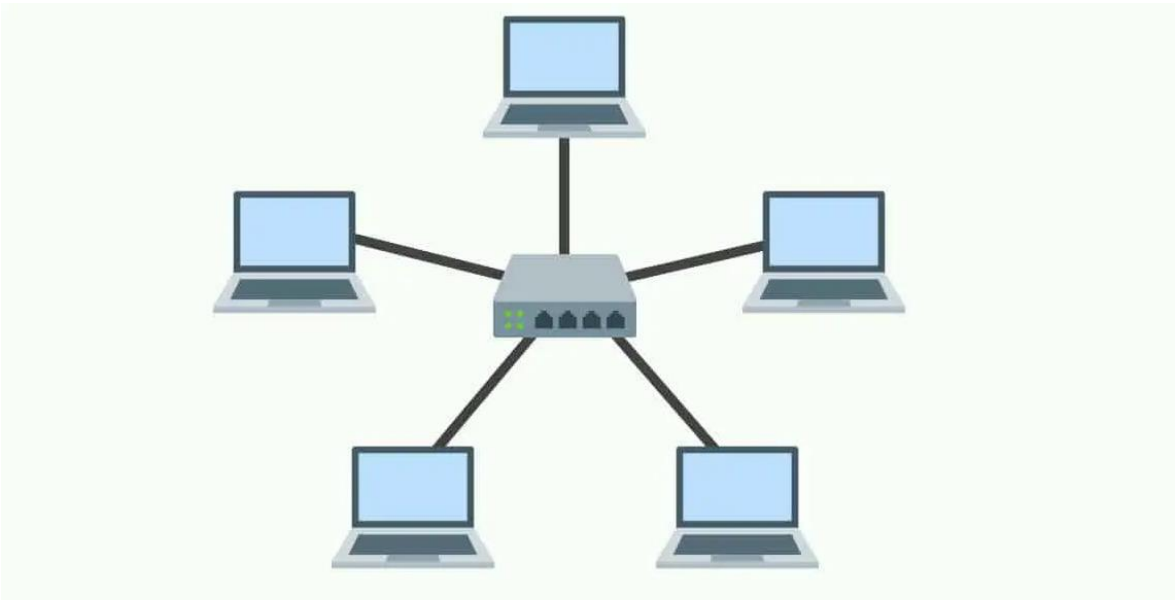
Mạng GAN (Global Area Network) đề cập đến một mạng bao gồm nhiều mạng được kết nối với nhau bao phủ một khu vực địa lý không giới hạn. Thuật ngữ này đồng nghĩa với Internet và được coi là mạng toàn cầu.

Không giống như mạng cục bộ (LAN) và mạng diện rộng (WAN), GAN bao phủ một khu vực địa lý rộng lớn. Bởi vì GAN được sử dụng để hỗ trợ giao tiếp di động trên một số mạng LAN không dây. Thách thức chính đối với bất kỳ GAN nào là chuyển giao tiếp của người dùng từ vùng phủ sóng cục bộ này sang vùng phủ tiếp theo.

1.2.2. Phân loại mạng theo Topology

Theo topology, mạng được chia làm các loại như mạng hình sao (Star topology), mạng tuyến tính (Bus topology), mạng vòng (Ring topology) và mạng kết hợp.

Mạng hình sao (Star topology)



Hình 1.1: Mạng hình sao

Mạng hình sao có tất cả các trạm được kết nối với một thiết bị trung tâm có nhiệm vụ nhận tín hiệu từ các trạm và chuyển đến trạm đích. Tùy theo yêu cầu truyền thông trên mạng mà thiết bị trung tâm có thể là hub, switch, router hay máy chủ trung tâm. Vai trò của thiết bị trung tâm là thiết lập các liên kết Point-to-Point.

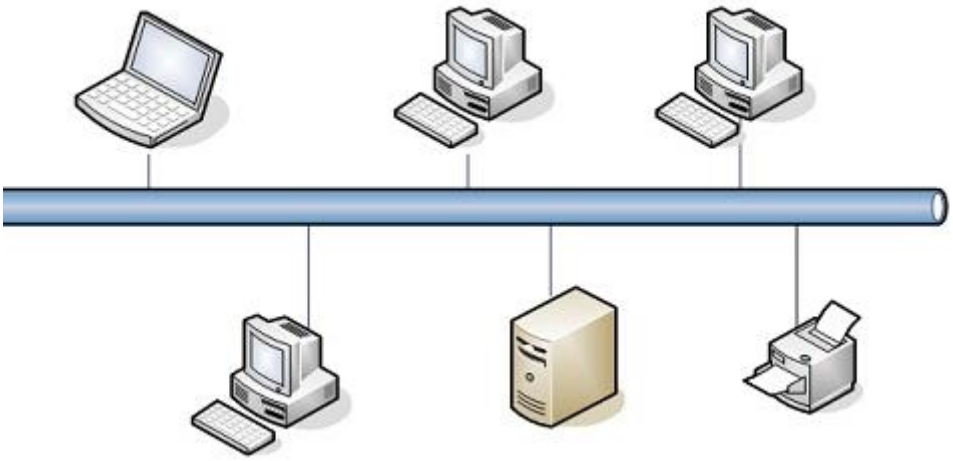
- Ưu điểm: Thiết lập mạng đơn giản, dễ dàng cấu hình lại mạng (thêm, bớt các trạm), dễ dàng kiểm soát và khắc phục sự cố, tận dụng được tối đa tốc độ truyền của đường truyền vật lý.

- Khuyết điểm: Độ dài đường truyền nối một trạm với thiết bị trung tâm bị hạn chế (bán kính khoảng 100m với công nghệ hiện nay).

Mạng tuyến tính (Bus topology)

Tất cả các node truy nhập chung trên một đường truyền vật lý được giới hạn hai đầu bằng hai đầu nối đặc biệt gọi là terminator. Mỗi trạm được nối với trục chính (BUS) qua một đầu nối chữ T (T-connector) hoặc một thiết bị thu phát (transceiver)

- Ưu điểm: Dễ thiết kế và chi phí thấp, nếu một nút mạng hỏng thì không ảnh hưởng đến hoạt động của toàn mạng.
- Khuyết điểm: Tính ổn định kém, dễ xảy ra xung đột thông tin trên đường truyền.

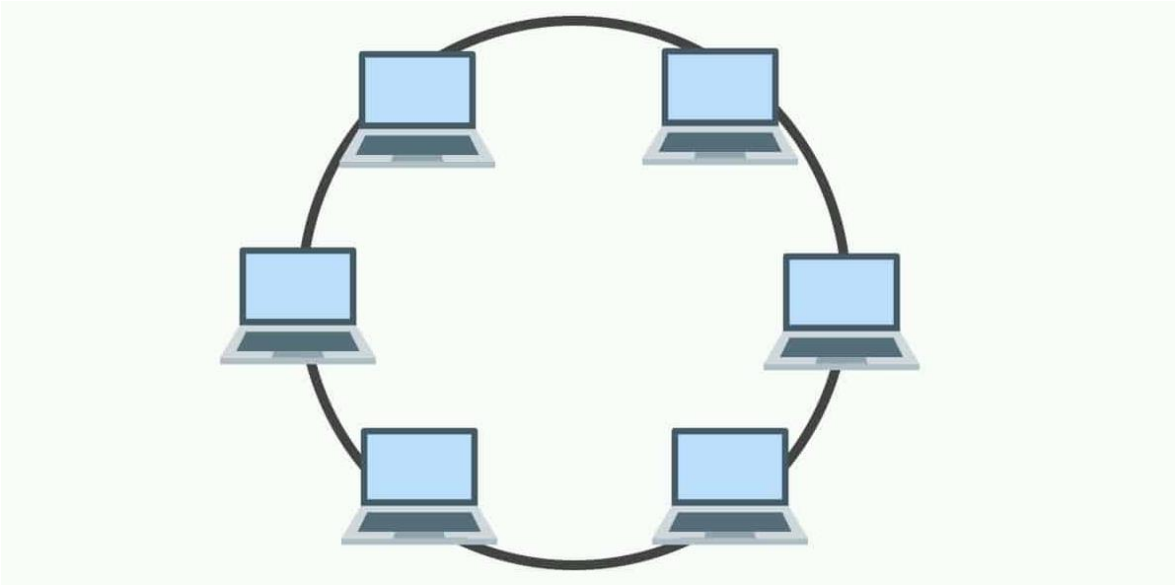


Hình 1.2: Mạng tuyến tính

Mạng vòng (Ring topology)

Với mạng vòng (Ring topology) tất cả các node cùng truy nhập chung trên một đường truyền vật lý. Tín hiệu được lưu chuyển trên vòng theo một chiều duy nhất, theo liên kết điểm - điểm. Dữ liệu được chuyển một cách tuần tự từng bit quanh vòng, qua các bộ chuyển tiếp. Bộ chuyển tiếp có ba chức năng: chèn, nhận và hủy bỏ thông tin. Các bộ chuyển tiếp sẽ kiểm tra địa chỉ đích trong các gói dữ liệu khi đi qua nó.

- Ưu điểm: Với dạng kết nối này có ưu điểm là không tốn nhiều dây cáp, tốc độ truyền dữ liệu cao, không gây ách tắc.
- Nhược điểm: Các giao thức để truyền dữ liệu phức tạp và nếu có trục trặc trên một trạm thì cũng ảnh hưởng đến toàn mạng



Hình 1.3: Mạng vòng

1.2.3. Phân loại mạng theo chức năng

Mạng ngang hàng Peer-to-Peer

Trong mô hình ngang hàng tất cả các máy đều là máy chủ đồng thời cũng là máy khách. Các máy trên mạng chia sẻ tài nguyên không phụ thuộc vào nhau. 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 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, vì vậy có thể phải biết mật khẩu để có thể truy nhập được tới các tài nguyên được chia sẻ.

Mạng Client-Server

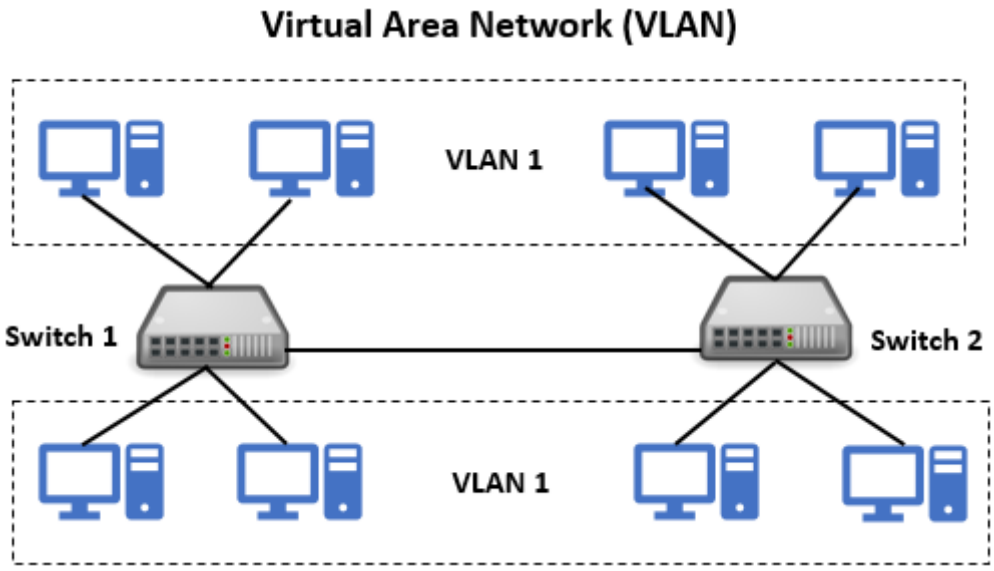
Mô hình Client/Server mô tả các dịch vụ mạng và các ứng dụng được sử dụng để truy nhập các dịch vụ. Là mô hình phân chia các thao tác thành hai phần: phía Client cung cấp cho người sử dụng một giao diện để yêu cầu dịch vụ từ mạng và phía Server tiếp nhận các yêu cầu từ phía Client và cung cấp các dịch vụ một cách thông suốt cho người sử dụng.

1.3. Tổng quan về VLAN

1.3.1. Định nghĩa

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập

dựa trên các yếu tố như chức năng, bộ phận, ứng dụng… của công ty. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch.



Hình 1.4: Mô hình VLAN

1.3.2. Ưu điểm

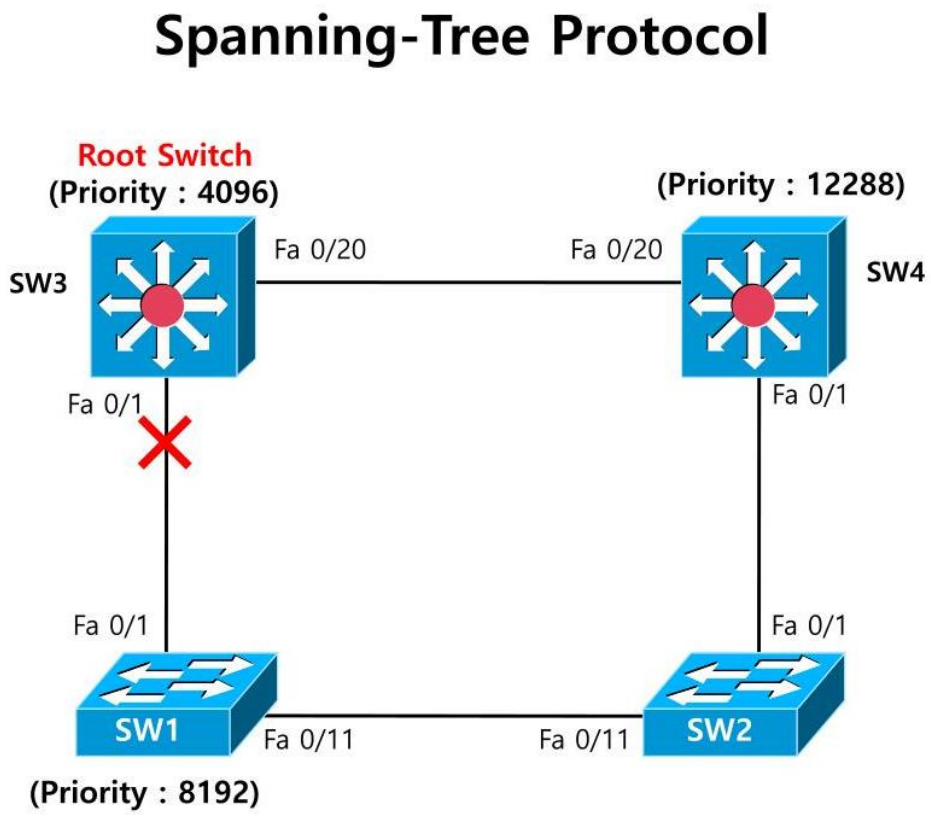
- **Tiết kiệm băng thông của hệ thống mạng**: VLAN chia mạng LAN thành nhiều đoạn (segment) nhỏ, mỗi đoạn đó là một vùng quảng bá (broadcast domain). Khi có gói tin quảng bá (broadcast), nó sẽ được truyền duy nhất trong VLAN tương ứng. Do đó việc chia VLAN giúp tiết kiệm băng thông của hệ thống mạng.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

1.3.3. Phân loại

- **Port - based VLAN**: là cách cấu hình VLAN đơn giản và phổ biến. Mỗi cổng của Switch được gắn với một VLAN xác định (mặc định là VLAN 1), do vậy bất cứ thiết bị host nào gắn vào cổng đó đều thuộc một VLAN nào đó.
- **MAC address based VLAN**: Cách cấu hình này ít được sử dụng do có nhiều bất tiện trong việc quản lý. Mỗi địa chỉ MAC được đánh dấu với một VLAN xác định.
- **Protocol – based VLAN**: Cách cấu hình này gần giống như MAC Address based, nhưng sử dụng một địa chỉ logic hay địa chỉ IP thay thế cho địa chỉ MAC. Cách cấu hình không còn thông dụng nhờ sử dụng giao thức DHCP

1.4. Tổng quan về giao thức Spanning-Tree (STP)

1.4.1. Định nghĩa



Hình 1.5: Giao thức Spanning-Tree

Theo IEEE 802.1D, giao thức Spanning Tree (STP) là một giao thức ngăn ngừa vòng lặp cho phép các thiết bị chuyển mạch giao tiếp với nhau để tìm ra các vòng lặp vật lý trong mạng.

STP chỉ định thuật toán mà bộ chuyển mạch có thể sử dụng khi tìm thấy vòng lặp để tạo cấu trúc liên kết logic không có vòng lặp.

1.4.2. Các bước ra quyết định của giao thức Spanning-Stree

STP sử dụng quy trình gồm bốn bước dưới đây nhằm tạo cấu trúc liên kết logic không có vòng lặp:

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

SW sử dụng frame đặc biệt được gọi là Bridge Protocol Data Units (BPDU) để trao đổi thông tin STP. Sau khi đánh giá các BPDU nhận được trên một cổng thì BPDU tốt nhất được lưu trữ. Kiểm tra theo trình tự bốn bước với mọi BPDU nhận được trên một cổng và so sánh với các BPDU được lưu.

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.

1.4.3. Sự hội tụ ban đầu của giao thức Spanning-Tree

Quá trình hội tụ STP ban đầu được thực hiện theo ba bước sau:

- **Bước 1: Chọn một Root Bridge**: Công tắc phân tích các BPDU nhận được và tìm kiếm công tắc có BID thấp nhất
- **Bước 2: Chọn Root Ports**: Một Root Port trên switch là port gần Root Bridge nhất. Mỗi switch ngoại trừ Root Bridge phải chọn một Root Port. Các thiết bị chuyển mạch sử dụng khái niệm chi phí để xác định khoảng cách giữa chúng với các thiết bị chuyển mạch khác. Root Path Cost là chi phí tích lũy của tất cả các liên kết đến Root Bridge
- **Bước 3: Chọn cổng được chỉ định**. Mỗi phân đoạn trong cấu trúc liên kết Lớp 2 có một Cổng được chỉ định. Cổng này gửi và nhận lưu lượng truy cập đến và từ phân đoạn đó và Root Bridge. Chỉ một cổng xử lý lưu lượng cho mỗi liên kết, đảm bảo cấu trúc liên kết không có vòng lặp. Cầu chứa Cổng được chỉ định cho một phân đoạn nhất định được coi là Công tắc được chỉ định trên phân đoạn đó.

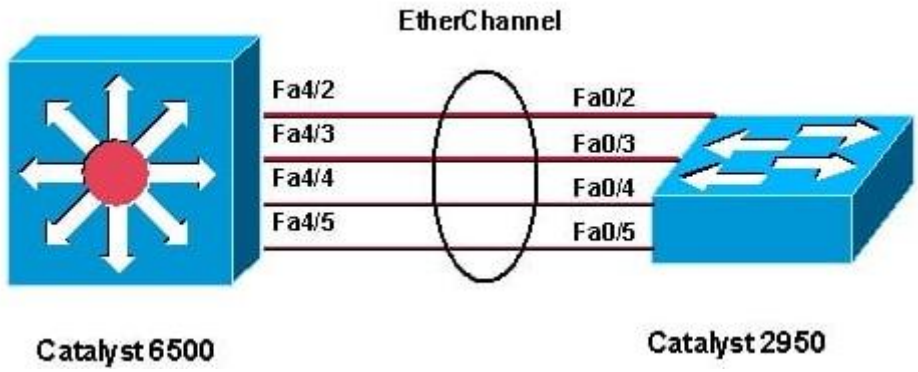
1.4.4. Các trạng thái trong một tiến trình Spanning-Tree

- **Disabled**: Cổng bị vô hiệu hoá về mặt quản trị.
- **Blocking**: Chỉ nhận các BPDU. Chuyển sang trạng thái listening khi không còn nhận được BPDU ở một thời gian nhất định.
- **Listening**: Chỉ gửi và nhận các BPDU để xác định cấu trúc liên kết Lớp 2. Đây là giai đoạn diễn ra cuộc bầu chọn Root Bridge, Root Ports và Designated Ports.
- **Learning**: Các cổng được chỉ định hoặc Cổng gốc sau 15 giây sẽ chuyển sang trạng thái Học và trong khoảng thời gian 15 giây khác, cầu nối sẽ xây dựng bảng địa chỉ MAC của nó nhưng không chuyển tiếp dữ liệu người dùng.
- **Forwarding**: Sau khoảng thời gian 15 giây, cổng chuyển sang trạng thái Chuyển tiếp, trong đó nó gửi và nhận các khung dữ liệu.

1.5. Tổng quan về EtherChannel

1.5.1. Định nghĩa

EtherChannel là 1 liên kết Logic, hay còn gọi là Virtual Interface, được sử dụng để giao tiếp giữa 2 thiết bị, có thể là giữa 2 switch, switch với server hoặc bất kỳ thiết bị nào có hỗ trợ công nghệ này. EtherChannel tổng hợp nhiều link vật lý thành 1 link logic để cung cấp băng thông cao hơn, cân bằng tải traffic và dự phòng các liên kết.



Hình 1.6: Mô hình EtherChannel

1.5.2. Ưu điểm

- Hầu hết các cấu hình được thực trên cấu hình EtherChannel đảm bảo tính nhất quán trong suốt liên kết.
- Dựa trên các cổng Switch có sẵn – không cần nâng cấp.
- Cân bằng tải giữa các liên kết trên cùng một EtherChannnel.
- Tạo ra một tập hợp được xem như là một liên kết logic bởi STP.

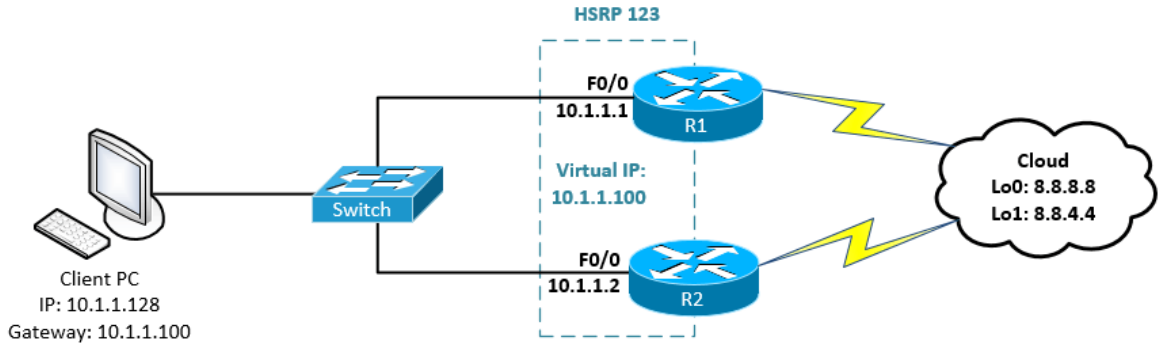
- Cung cấp khả năng dự phòng bởi vì liên kết tổng thể được xem như là 1 kết nối logic. Nếu 1 liên kết vật lý trong kênh hỏng, điều này không gây ra sự thay đổi trong cấu trúc liên kết và không đòi hỏi tính toán lại STP.

1.6. Tổng quan về giao thức Host Standy Router Protocol (HSRP)

1.6.1. Định nghĩa

Hot Standby Router Protocol (HSRP) là một chuẩn của Cisco, HSRP ra đời từ nhưng năm 1990 nhằm cung cấp tính sẵn sàng làm việc cao của hệ thống mạng bằng cách đưa ra sự dự phòng cho các host trên một mạng LAN đã được cấu hình với một địa chỉ IP default gateway.

HSRP cho phép nhiều router cùng chia sẽ một địa chỉ IP ảo và các địa chỉ MAC sao cho các máy của người dùng (user) sẽ không nhận ra khi nào có sự cố mạng xảy ra đối với Active router.



Hình 1.7: Giao thức HSRP

1.6.2. Đặc điểm

- Địa chỉ IP là ảo và địa chỉ MAC cũng ảo trên router actine.
- Các router dự phòng sẽ lắng nghe các gói hello từ router đang active, mặc định mỗi 3 giây và 10 giây cho khoảng thời gian dead.
- Độ ưu tiên cao nhất (mặc định là 100, trong tầm từ 1-255) sẽ xác định router, với cơ chế pre-emption bị tắt.
- Hỗ trợ tính năng tracking, trong đó độ ưu tiên của một router sẽ bị giảm khi một interface đang bị theo dõi bị hỏng hóc.
- Có thể có tối đa 255 nhóm HSRP trên mỗi interface, cho phép một hình thức cân bằng tải.
- Địa chỉ MAC ảo có dạng 0000.0C07.Acxx trong đó xx là chỉ số của nhóm HSRP.
- Địa chỉ của IP ảo phải trong cùng giá trị subnet của cổng của router trong LAN.

- Địa chỉ của IP ảo phải khác với bất kỳ một địa chỉ thật nào của các cổng tham gia vào HSRP.

1.6.3. Cách hoạt động

HSRP hoạt động dựa trên việc tạo ra một gateway ảo. Gateway ảo trên cụng có thể hiểu như là một công việc hay vai trò mà HSRP có trách nhiệm đảm nhận cung cấp cho các máy bên trong mạng LAN. Trong một nhóm các routers chạy HSRP, sẽ có một router đứng ra đảm trách vai trò làm gateway nói trên. Router đó được gọi là ACTIVE router. IP của gateway ảo được gọi là IP ma (phantom IP). Các routers không active sẽ bị rơi vào trạng thái standby.

Active Router sẽ định tuyến các gói tin; còn Standby Router là router sẽ được làm nhiệm vụ thay thế Active Router khi mà Active Rouer bị lỗi hoặc do những điều kiện mà người quản trị mạng đã cấu hình trước.

HSRP sẽ tự động được tìm thấy khi mà Active Router bị lỗi, và một Standby Router sẽ được lựa chọn để điều khiển địa chỉ IP và địa chỉ MAC của nhóm Hot Standby đó. Một Standby Router mới cũng sẽ được chọn lại trong thời điểm này.

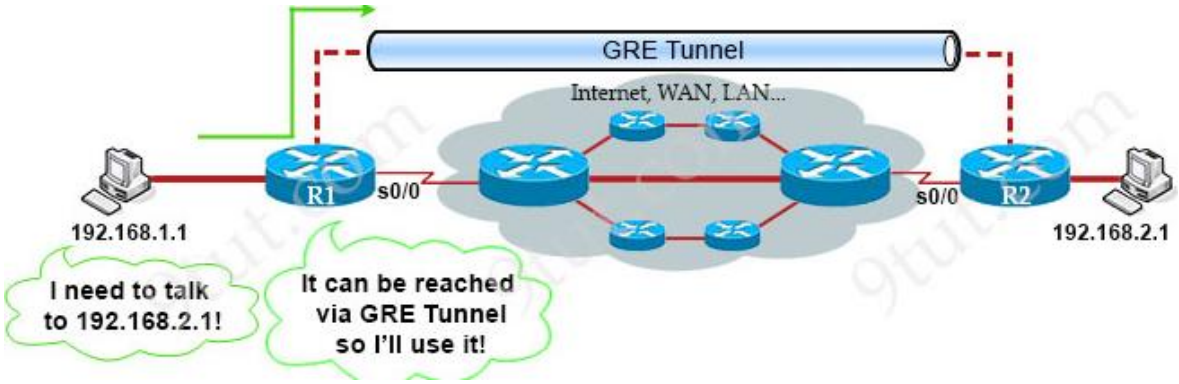
Những thiết bị đang chạy HSRP sẽ gửi và nhận các gói tin hello dưới dạng địa chỉ Multicast để có khả năng xác định được router bị lỗi và xác định được Active Router và Standby Router. Khi HSRP được cấu hình trên một interface, thì thông điệp ICMP redirect sẽ bị disable theo mặc định trên tất cả các interface.

1.7. Tổng quan về GRE VPN

1.7.1. Định nghĩa

GRE là viết tắt của Generic Routing Encapsulation, là giao thức được phát triển bởi Cisco, cho phép đóng gói nhiều loại giao thức lớp Network trong các liên kết Point-to-Point. Một GRE Tunnel được sử dụng khi các gói dữ liệu cần được gửi giữa các mạng khác nhau thông qua internet. Với GRE được cấu hình, 1 đường hầm ảo được tạo giữa 2 Router và các gói tin gửi giữa 2 mạng nội bộ sẽ được truyền qua GRE Tunnel.

Có 2 loại GRE, GRE truyền thống là point-to-point, còn mGRE là sự mở rộng khái niệm này bằng việc cho phép một tunnel có thể đến được nhiều điểm đích, mGRE tunnel là thành phần cơ bản nhất trong DMVPN.



Hình 1.8: Mô hình GRE VPN

1.7.2. Ưu điểm

- Cho phép đóng gói nhiều giao thức và truyền thông qua một giao thức backbone (IP protocol).
- Cung cấp cách giải quyết cho các mạng bị hạn chế hop (hạn chế số hop di chuyển tối đa trong một mạng).
- Kết nối các mạng con gián tiếp.
- Yêu cầu ít tài nguyên hơn các giải pháp tunnel khác. (ví dụ Ipsec VPN).

1.7.3. Nhược điểm

- Không có cơ chế mã hóa.
- Không có cơ chế hashing
- Không có cách nào xác thực nguồn gốc của VPN peer.

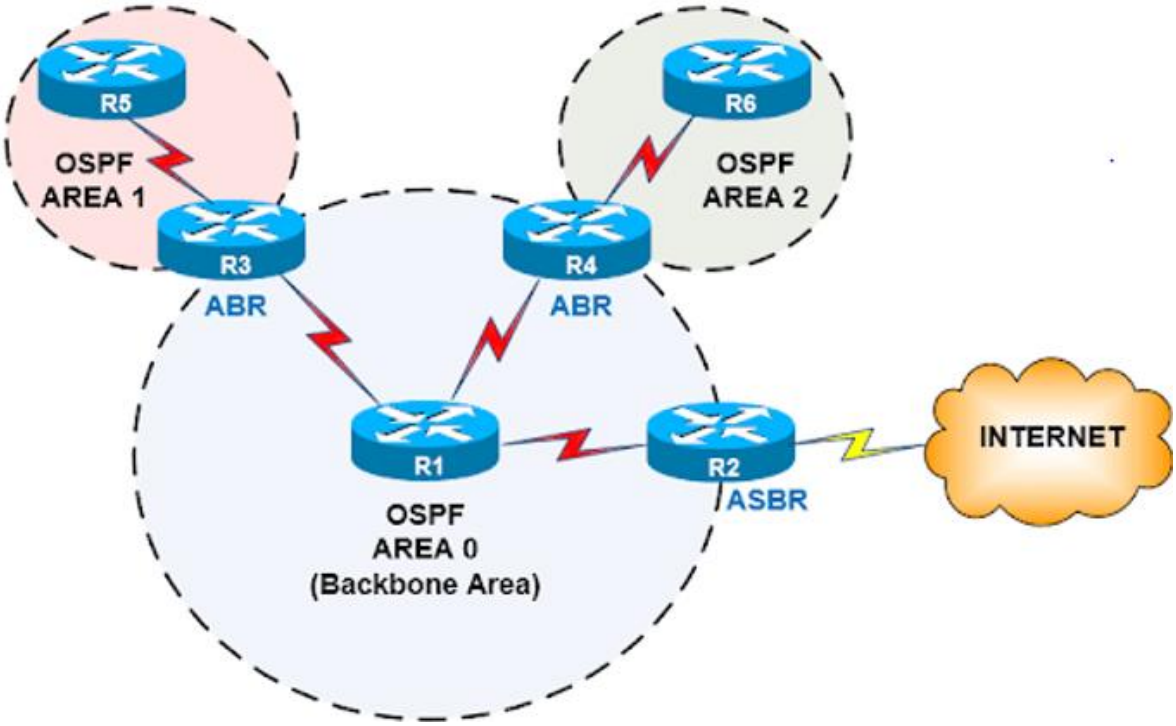
1.8. Tổng quan về giao thức định tuyến OSPF

1.8.1. Định nghĩa

OSPF (Open Shortest Path First) là một giao thức định tuyến nội dựa trên thuật toán link state routing được sử dụng trong một hệ thống mạng hay một khu vực xác định. Mỗi bộ định tuyến của OSPF sẽ chứa thông tin của tất cả các tên miền để có thể dựa vào đó và xác định được quãng đường đi ngắn nhất và tốt nhất giữa bộ định tuyến nguồn và đích. Do đó, mục tiêu chính của giao thức này là tìm hiểu về các tuyến đường.

Giao thức OSPF đạt được mục tiêu của nó bằng cách tìm hiểu mọi bộ định tuyến và các mạng con có trong toàn bộ hệ thống mạng. Các bộ định tuyến này đều chứa những thông tin về mạng tương tự nhau và được bộ định tuyến tìm hiểu bằng cách gửi Link State Advertisement (LSA). Mọi thông tin về bộ định tuyến, mạng con và những thông tin khác đều được chứa trong LSA. Khi LSA đầy, OSPF sẽ thực hiện

việc lưu trữ thông tin trong LSDB (cơ sở dữ liệu có trạng thái liên kết) một cách đồng nhất.



Hình 1.9: Giao thức OSPF

1.8.2 Cách hoạt động

Router chạy bằng định tuyến OSPF thông qua các bước cơ bản như sau :

Bước 1: Chọn Router ID: Để giao thức OSPF có thể hoạt động được thì người dùng phải tạo ra một định danh gọi là Router ID.

- **Cách 1: Router tự tạo định danh**: Router xem xét các interface để tự động lấy Router có IP cao nhất làm Router ID.
- **Cách 2: Người dùng tự cấu hình định danh**: Router sẽ không cần định danh Router ID bằng cách chọn IP có sẵn trên interface mà chỉ cần tự tạo ra nó.

Bước 2: Thiết lập mối quan hệ láng giềng: Hai router được xem là láng giềng nếu chúng đáp ứng được các điều kiện sau:

- **Cùng Area-ID**: Một hệ thống mạng lớn sẽ được chia thành nhiều khu vực để giảm thiểu tối đa những ảnh hưởng khi xuất hiện sự cố, mỗi vùng là một Area-ID. Trong đó, vùng trung tâm sẽ có Area-Id bằng 0 còn những vùng khác muốn truyền được dữ liệu phải có đường truyền trực tiếp về cùng trung tâm.

- **Cùng Subnet**: Hai IP phải có cùng Subnet thì mới có thể ping và thực hiện trao đổi thông tin lẫn nhau.
- **Cùng thông số**: Mặc định dead time hoặc hello trên hai cổng là 10s/40s.
- **Cùng xác thực trên hai cổng**: Đây là điều kiện dành cho mạng lớn bởi khi đặt xác thực thì các router khác sẽ không lấy được thông tin.

Bước 3: Trao đổi LSDB: Với vai trò như tấm bản đồ, LSDB chính là căn cứ để Router tính toán định tuyến. Mỗi Router sẽ tiến hành giao tiếp và trao đổi với nhau theo từng đơn vị thông tin LSA.

Bước 4: Tính toán trong giao thức OSPF bảng định tuyến.

1.8.3. Ưu điểm

- Chi phí được dùng làm thông số định tuyến để chọn đường đi chính xác trong hệ thống mạng.
- Router có thể dễ dàng lựa chọn đường đi bằng cách sử dụng những thông tin mới nhất.
- Giao thức định tuyến OSPF có khả năng hỗ trợ CIDR và VLSM.
- Mỗi Router sẽ đồng bộ về toàn bộ cấu trúc hệ thống mạng và một bộ hồ sơ đầy đủ nên chúng rất khó bị lặp vòng.

1.8.4. Nhược điểm

- OSPF tốn nhiều bộ nhớ và yêu cầu năng lực xử lý cao hơn nên chi phí đầu tư sẽ không phù hợp với các tổ chức nhỏ có thiết bị cũ hay chi phí hạn hẹp.
- Hệ thống mạng phải chia thành nhiều vùng nhỏ để giảm độ phức tạp và độ lớn của cơ sở dữ liệu.
- OSPF đòi hỏi người quản trị phải nắm rõ giao thức.

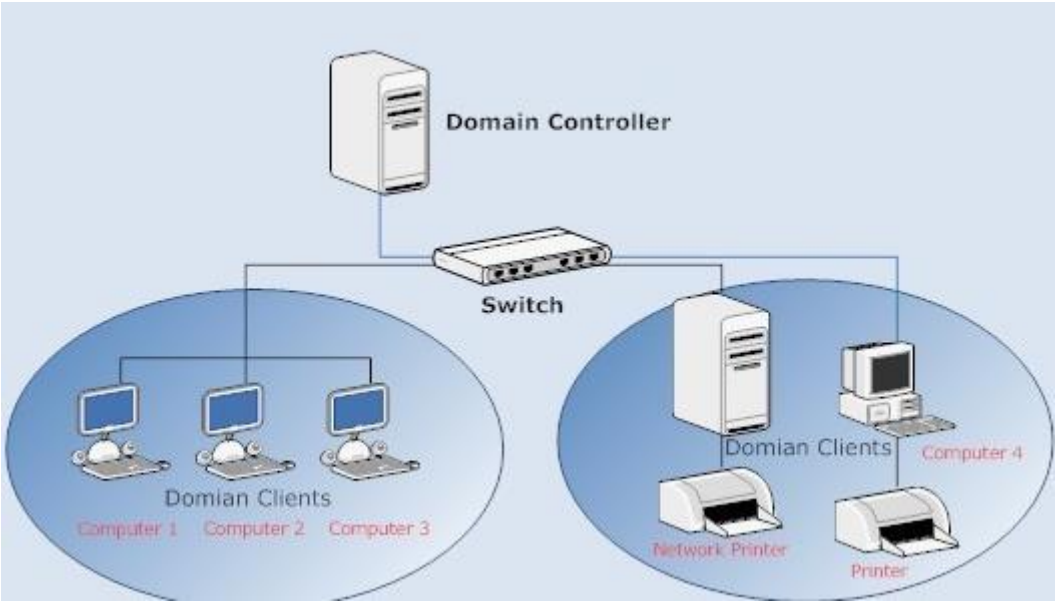
1.8.5. Những trạng thái của OSPF

- **Down**: Tại trạng thái này, trên giao diện sẽ không nhận bất kỳ gói tin HELLO nào nếu thiết bị ở trạng thái ngừng hoạt động (quá trình OSPF chưa bắt đầu).
- **Init**: Thiết bị của bạn ở trạng thái Init sẽ đồng nghĩa với việc thiết bị đã nhận được gói HELLO từ một bộ định tuyến khác.
- **2WAY**: Nếu thiết bị của bạn trong trạng thái này thì cả hai bộ định tuyến đều đã nhận được gói tin HELLO từ bộ định tuyến khác và giữa những bộ định tuyến này đã được hình thành liên kết.

- **Exstart**: Cả hai bộ định tuyến sẽ chuyển sang trạng thái khởi động khi quá trình trao đổi giữa chúng bắt đầu. Cả chủ và khách tại trạng thái này sẽ được chọn dựa trên ID của bộ định tuyến.
- **Exchange**: Cả hai bộ định tuyến trong trạng thái trao đổi sẽ gửi danh sách các LSA có chứa mô tả cơ sở dữ liệu cho nhau.
- **Loading**: LSR, LSU và LSA tại trạng thái tải sẽ tiến hành trao đổi cho nhau.
- **Full**: Sau khi LSA hoàn tất việc trao đổi, các bộ định tuyến sẽ ngay lập tức chuyển sang trạng thái đầy đủ này.

1.9. Tổng quan về Domain Controller

1.9.1. Định nghĩa



Hình 1.10: Sơ đồ hệ thống Domain Controller

Domain Controller (DC) là máy tính của máy chủ (server) được thiết lập với mục đích quản lý Domain. Một Domain Controller là một máy chủ chịu trách nhiệm quản lý vấn đề an ninh mạng, nó giống như một "người gác cổng" làm nhiệm vụ xác thực và ủy quyền User.

Khái niệm Active Directory hình thành dựa trên mối liên hệ với các mạng Windows NT cũ, được giới thiệu lần đầu bởi Microsoft. Domain Controller đáp ứng nhu cầu về một giải pháp hữu hiệu để kiểm soát quyền truy cập vào các tài nguyên trong một Domain.

Một Server muốn trở thành Domain Controller phải cài đặt và khởi tạo Active Directory ("AD"). Domain Controller quản lý Domain thông qua Active Directory đã khởi tạo trước đó.

1.9.2. Phân loại

Có hai kiểu Domain Controller được sử dụng phổ biến nhất hiện nay đó là Backup Domain Controllers (BDC) (tùy chọn) và Primary Domain Controller (PDC). Trong đó:

- Primary Domain Controller (PDC): Toàn bộ tin tức bảo mật của domain sẽ được lưu trữ trong thư mục chính đó là Windows server.
- Backup Domain Controllers (BDC): Một BDC sẽ được đẩy lên PDC khi PDC gặp lỗi. PDC này được đẩy lên này sẽ giúp cân bằng khối lượng công việc trong các tình huống tắc nghẽn mạng. Tương ứng với mỗi chu kỳ của BDC thì PCD sẽ tự động sao chép cơ sở dữ liệu bên trong các thư mục chính.

1.9.3. Các bước triển khai Domain Controller

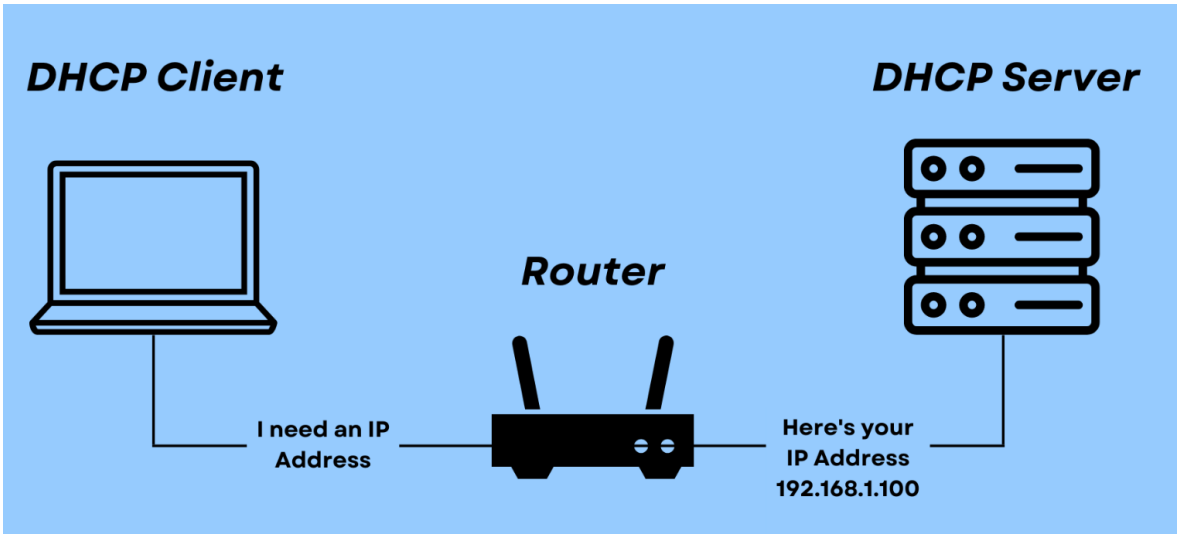
Để có được mô hình Domain Controller, các bạn cần thực hiện theo các bước cơ bản sau đây:

- **Bước 1:** Tiến hành đặt IP tĩnh cho máy được lựa chọn làm Domain Controller.
- **Bước 2:** Xây dựng Domain Controller trên máy Server đã được chọn làm Domain Controller.
- **Bước 3:** Tạo user trong Domain Controller cho các máy Client.
- **Bước 4**: Đặt địa chỉ IP và Join các Client vào Domain.
- **Bước 5:** Đăng nhập máy Client sau đó kiểm tra Domain Controller.

1.10. Tổng về DHCP

1.10.1. Định nghĩa

DHCP viết tắt của Dynamic Host Configuration Protocol, là giao thức tự động cấp phát địa chỉ IP đến các thiết bị trong mạng. Bên cạnh đó, nó cũng đảm bảo không có trường hợp hai hoặc nhiều thiết bị có cùng IP và còn cung cấp các thông tin cấu hình như DNS, subnet mask, default gateway.



Hình 1.11: Ví dụ về DHCP

1.10.2. Cách hoạt động

Nguyên lý hoạt động của DHCP về cơ bản khá dễ hiểu, khi có một thiết bị cần truy cập mạng, nó sẽ gửi yêu cầu từ một router và được router gán cho một địa chỉ IP khả dụng.

Cách router hoạt động như một máy chủ DHCP đối với các mô hình mạng nhỏ hoặc hộ gia đình. Đối với các mạng lớn hơn một router không thể quản lý số lượng lớn các thiết bị nên sẽ có một máy chủ chuyên dụng để cấp IP.

Cụ thể hơn về cách thức hoạt động của DHCP:

- Khi muốn kết nối với mạng thiết bị sẽ gửi yêu cầu DHCP DISCOVER đến máy chủ. Máy chủ DHCP sẽ tìm địa chỉ IP khả dụng rồi cung cấp cho thiết bị cùng với gói DHCP OFFER.
- Sau khi nhận được địa chỉ, thiết bị sẽ phản hồi với máy chủ bằng một gói tin DHCP REQUEST.
- Đây là lúc chấp nhận yêu cầu, máy chủ sẽ gửi tin báo nhận (ACK) xác nhận thiết bị đã có IP và thời gian sử dụng IP đến khi có địa chỉ mới.

1.10.3. Ưu điểm

- Giúp các thiết bị như máy tính, laptop, điện thoại, máy tính bảng…kết nối mạng nhanh chóng.
- Quản lý địa chỉ IP một cách khoa học, tránh trường hợp trùng IP trên nhiều, đảm bảo cấu hình tự động cho mọi thiết bị kết nối mạng.
- Quản lý địa chỉ IP và các tham số TCP/IP dễ dàng qua các trạm.

- Các nhà quản trị mạng có thể thay đổi cấu hình và thông số của IP để nâng cấp cơ sở hạ tầng.
- Các thiết bị có thể di chuyển tự do từ mạng này sang mạng khác và nhận IP mới tự động.

1.11. Tổng quan về DNS

1.11.1. Định nghĩa

Hệ thống phân giải tên miền (DNS) về căn bản là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ (dạng ký tự, ví dụ www.example.com) sang địa chỉ IP vật lý (dạng số, ví dụ 123.11.5.19) tương ứng của tên miền đó. DNS giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

1.11.2 Nguyên tắc làm việc

Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server riêng của mình, gồm những máy bên trong phần riêng của mỗi nhà cung cấp dịch vụ đó trong internet.

Nghĩa là, DNS server phân giải tên website của một trình duyệt tìm kiếm địa chỉ bất kỳ phải là DNS server của chúng tổ chức quản lý trang web đó chứ không là của một tổ chức hay nhà cung cấp dịch vụ nào khác.

Internet Network Information Center (INTERNIC) chịu trách nhiệm theo dõi các DNS server và các tên miền tương ứng. INTERNIC là một tổ chức được thành lập bởi AT & T, National Science Foundation và Network Solution, có trách nhiệm đăng ký các tên miền của internet. INTERNIC không có nhiệm vụ phân giải tên cho từng địa chỉ mà chỉ có nhiệm vụ quản lý tất cả các DNS server trên internet.

Để có được một cái tên đã được phân giải, DNS có khả năng tra vấn các DNS server khác. Thường, DNS server của mỗi tên miền có hai việc khác biệt. Gồm việc chịu trách nhiệm phân giải tên từ các máy bên trong miền về địa chỉ internet, cả bên trong và nên ngoài miền nó quản lý. Việc thứ hai là chúng trả lời các DNS server bên ngoài đang cố gắng phân giải những cái tên bên trong miền nó quản lý. DNS server có khả năng ghi nhớ lại những tên vừa phân giải để sử dụng cho những yêu cầu phân giải lần sau. Tùy thuộc vào quy mô của từng DNS để lưu lại số lượng những tên phân giải.

CHƯƠNG II : PHÂN TÍCH THIẾT KẾ HỆ THỐNG

2.1 Khảo sát doanh nghiệp

Công ty Cổ phần Novatech với 2 lĩnh vực kinh doanh cốt lõi gồm : Công nghệ và Viễn thông. Hiện tại công ty đã hoạt động được 2 năm và muốn xây dựng hệ thống mạng nội bộ mô hình domain cho công ty.

Thông qua việc thực hiện cuộc khảo sát tại doanh nghiệp có một trụ sở chính và ba chi nhánh.

Trụ sở chính gồm các phòng ban :

- Phòng Giám đốc
- Phòng Kinh doanh
- Phòng Kế toán
- Phòng Kỹ thuật
- Phòng Máy chủ

2.2 Yêu cầu thiết kế hệ thống mạng LAN

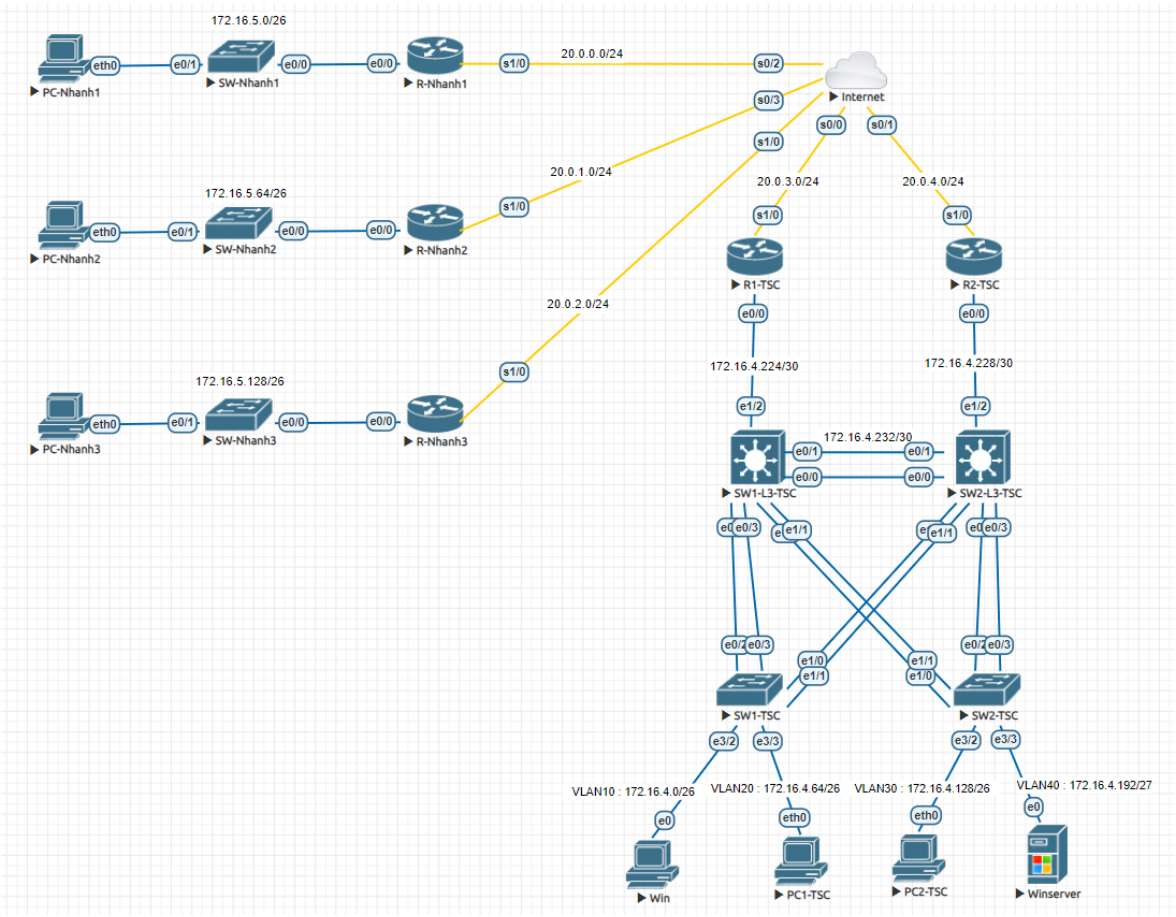
- Doanh nghiệp có nhu cầu triển khai hệ thống mạng Intranet cho một trụ sở chính và 3 chi nhánh. Số lượng host trong mỗi chi nhánh không ít hơn 50. Số lượng host tại trụ sở chính không ít hơn 150.
- Dải IP cấp phát : 172.16.4.0
- Tại vùng Server phải có ít nhất 1 DC và 1 Server cài đặt DNS và DHCP, cấp phát IP động cho tất cả 4 nhánh theo từng vùng.

2.3 Đề xuất phương án triển khai

Sau khi đã nắm rõ được tổng quan về kiến trúc và nhu cầu của công ty thì có thể đưa ra một số hướng giải quyết như sau:

- Thiết kế sơ đồ logic cho hệ thống mạng dựa trên hạ tầng của công ty.
- Đề xuất các thiết bị xây dựng mạng và bảng dự toán chi phí.
- Thiết lập dải IP cho từng phòng ban theo số lượng các thiết bị cần thiết.
- Lập bảng IP cho các thiết bị.
- Triển khai cấu hình các thiết bị để hệ thống có thể chạy
- Chạy thử nghiệm một số dịch vụ đã cấu hình cho công ty.

2.4 Sơ đồ triển khai trên phần mềm EVE-NG :



Hình 2.1: Sơ đồ triển khai hệ thống trên phần mềm EVE-NG

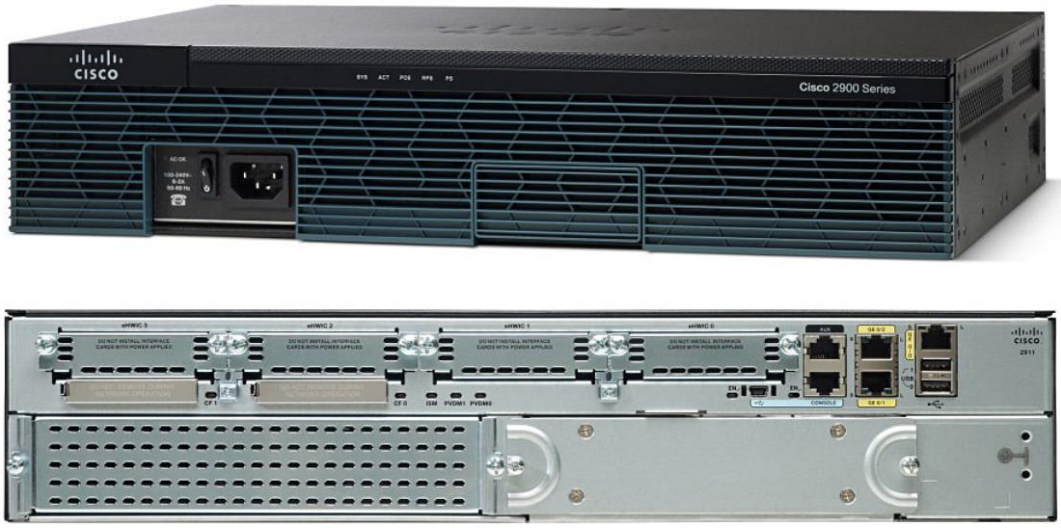
2.5 Quy hoạch IP cho hệ thống mạng

Tên	Địa chỉ mạng	Dải địa chỉ khả dụng	Ghi chú
VLAN 10	172.16.4.0/26	172.16.4.1 – 172.16.4.62	Trụ sở chính
VLAN 20	172.16.4.64/26	172.16.4.65 – 172.16.4.126	Trụ sở chính
VLAN 30	172.16.4.128/26	172.16.4.129 – 172.16.4.190	Trụ sở chính
VLAN 40	172.16.4.192/27	172.16.4.193 – 172.16.4.222	Trụ sở chính

R1-TCS => SW1-L3-TCS	172.16.4.224/30	172.16.4.225 – 172.16.4.226	Trụ sở chính
R2-TCS => SW2-L3-TCS	172.16.4.228/30	172.16.4.229 – 172.16.4.230	Trụ sở chính
SW1-L3-TCS => SW2-L3-TCS	172.16.4.232/30	172.16.4.233 – 172.16.4.234	Trụ sở chính
R-Nhanh1	172.16.5.0/26	172.16.5.1 – 172.16.5.62	Nhánh 1
R-Nhanh2	172.16.5.64/26	172.16.5.65 – 172.16.5.126	Nhánh 2
R-Nhanh3	172.16.5.128/26	172.16.5.129 – 172.16.5.190	Nhánh 3
Internet => R-Nhanh1	20.0.0.0/24	20.0.0.1 – 20.0.0.254	Internet
Internet => R-Nhanh2	20.0.1.0/24	20.0.1.1 – 20.0.1.254	Internet
Internet => R-Nhanh3	20.0.2.0/24	20.0.2.1 – 20.0.2.254	Internet
Internet => R1-TSC	20.0.3.0/24	20.0.3.1 – 20.0.3.254	Internet
Internet => R2-TSC	20.0.4.0/24	20.0.4.1 – 20.0.4.254	Internet

CHƯƠNG III : PHƯƠNG ÁN LỰA CHỌN THIẾT BỊ

3.1 Thiết bị Router Cisco 2911 SEC/K9



Hình 3.1: Router Cisco 2911 SEC/K9

Thông số kỹ thuật :

- Cisco 2911 CISCO2911-SEC/K9 Security Bundle w/SEC license PAK
- Giao thức kết nối dữ liệu: Ethernet, Fast Ethernet, Gigabit Ethernet
- Định tuyến: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, static IPv4 IPv6 routing
- Giao thức mạng: IPSec
- Bộ nhớ DRAM: 512 MB (installed) / 2 GB (max)
- Bộ nhớ flash: 256 MB (installed) / 8 GB (max)

3.2 Thiết bị Switch Layer 3 Cisco CBS250-16T-2G-EU

Hình 3.2: Switch Cisco CBS250-16T-2G-EU Smart 16-PORT GE, 2X1G SFP

Thông số kỹ thuật :

- Switch thông minh Gigabit Ethernet 18 cổng CBS250-16T-2G-EU
- Hỗ trợ 16 cổng Gigabit Ethernet và 2 cổng Small Form-Factor Pluggable
- Dung lượng chuyển mạch: 36.0Gbps.
- Khung Jumbo: Kích thước khung lên tới 9K byte. MTU mặc định 2K byte.
- Bảng MAC: 8K địa chỉ.
- Cáp: Unshielded Twisted Pair (UTP) Category 5e hoặc 1000BASE-T trở lên
- Bộ nhớ flash: 256 MB.
- CPU:800MHz ARM
- RAM:512 MB

3.3 Thiết bị Switch Layer 2 Cisco CBS250-48T-4G-EU

Hình 3.3: Swtich Cisco CBS250-48T-4G-EU Smart 48-PORT GE, 4X1G SFP

Thông số kỹ thuật :

- Cổng RJ-45 : 48 cổng PoE +
- Cổng kết hợp (RJ-45 + SFP) : 4 Gigabit SFP
- Nguồn dành riêng cho PoE : 370W
- Số cổng hỗ trợ PoE : 48
- Flash : 256 MB
- CPU : 800 MHz ARM
- Bộ nhớ CPU : 512 MB
- Bộ đệm gói : 3 MB
- Kích thước đơn vị (W x H x D) : 445 x 350 x 44 mm (17,5 x 13,78 x 1,73 in)

3.4 Máy tính nhân viên

Hình 3.4: Máy tính nhân viên

Thông số kỹ thuật :

- CPU: Intel Pentium Gold G6400
- Mainboard: GIGABYTE H410M-H V2
- RAM: Kingston 1x 8GB
- Ổ cứng: Dung lượng 1TB HDD
- PSU: Công suất thực 350W
- Màn hình: 22 Inch tấm nền IPS
- Bàn phím: Full Size
- Mouse: Chuột quang RGB

3.5 Bảng chi phí dự tính

Tên thiết bị	Số lượng	Đơn giá	Thành tiền
Router Cisco 2911 SEC/K9	5	19.200.000	96.000.000
Switch Cisco CBS250-16T-2G-EU	2	6.800.000	13.600.000
Switch Layer 2 Cisco CBS250-48T-4G-EU	5	13.000.000	65.000.000
Máy tính nhân viên	300	6.000.000	1.800.000.000
Cáp mạng UTP cho hệ thống mạng LAN	1500 m	10.000	15.000.000
TỔNG			1.989.600.000

Hình 3.5: Bảng chi phí dự tính

- Tổng chi phí dự tính khoảng 1.989.600.000 VNĐ (Chưa tính chi phí phát sinh)

CHƯƠNG IV : THỰC NGHIỆM TRIỂN KHAI MÔ PHỎNG TRÊN PHẦN MỀM EVE-NG

4.1 Thông số cấu hình trên thiết bị mạng

4.1.1 Cấu hình Switch SW1-L3-TSC

Cấu hình IP ,Trunking và tạo EtherChannel cho interface :

```
!
interface Ethernet0/0
 no switchport
 no ip address
 duplex auto
 channel-group 1 mode desirable
!
interface Ethernet0/1
 no switchport
 no ip address
 duplex auto
 channel-group 1 mode desirable
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/2
 no switchport
 ip address 172.16.4.226 255.255.255.252
 ip helper-address 172.16.4.221
 duplex auto
```

Hình 4.1: Cấu hình Ip, Trunking và tạo EtherChannel cho interface

Cấu hình EtherChannel :

```
interface Port-channel1
 no switchport
 ip address 172.16.4.233 255.255.255.252
 ip helper-address 172.16.4.221
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Hình 4.2: Cấu hình EtherChannel

Cấu hình VLAN , HSRP và DCHP Relay :

```
interface Vlan10
 ip address 172.16.4.1 255.255.255.192
 ip helper-address 172.16.4.221
 standby 10 ip 172.16.4.62
 standby 10 priority 150
 standby 10 preempt
!
interface Vlan20
 ip address 172.16.4.65 255.255.255.192
 ip helper-address 172.16.4.221
 standby 20 ip 172.16.4.126
 standby 20 priority 150
 standby 20 preempt
!
interface Vlan30
 ip address 172.16.4.129 255.255.255.192
 ip helper-address 172.16.4.221
 standby 30 ip 172.16.4.190
 standby 30 preempt
!
interface Vlan40
 ip address 172.16.4.193 255.255.255.224
 ip helper-address 172.16.4.221
 standby 40 ip 172.16.4.222
 standby 40 preempt
!
```

Hình 4.3: Cấu hình VLAN , HSRP và DHCP Relay

Cấu hình VTP :

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.16.4.226 on interface Et1/2 (first layer3 interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

Hình 4.4: Cấu hình VTP

Cấu hình Spanning-tree :

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10,20 priority 24576
spanning-tree vlan 30,40 priority 28672
!
vlan internal allocation policy ascending
!
```

Hình 4.5: Cấu hình Spanning-stree

Cấu hình hình OSPF :

```
!
router ospf 1
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 passive-interface Vlan40
 network 172.16.4.0 0.0.0.255 area 0
!
```

Hình 4.6: Cấu hình OSPF

4.1.2 Cấu hình Switch SW2-L3-TSC

Cấu hình IP, Trunking và tạo EtherChannel :

```
interface Ethernet0/0
 no switchport
 no ip address
 duplex auto
 channel-group 1 mode desirable
!
interface Ethernet0/1
 no switchport
 no ip address
 duplex auto
 channel-group 1 mode desirable
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/2
 no switchport
 ip address 172.16.4.230 255.255.255.252
 ip helper-address 172.16.4.221
 duplex auto
```

Hình 4.7: Cấu hình IP, Trunking và tạo EtherChannel cho interface

Cấu hình EtherChannel :

```
interface Port-channel1
 no switchport
 ip address 172.16.4.234 255.255.255.252
 ip helper-address 172.16.4.221
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Hình 4.8: Cấu hình EtherChannel

Cấu hình VLAN, HSRP và DHCP Relay :

```
interface Vlan10
 ip address 172.16.4.2 255.255.255.192
 ip helper-address 172.16.4.221
 standby 10 ip 172.16.4.62
 standby 10 preempt
!
interface Vlan20
 ip address 172.16.4.66 255.255.255.192
 ip helper-address 172.16.4.221
 standby 20 ip 172.16.4.126
 standby 20 preempt
!
interface Vlan30
 ip address 172.16.4.130 255.255.255.192
 ip helper-address 172.16.4.221
 standby 30 ip 172.16.4.190
 standby 30 priority 150
 standby 30 preempt
!
interface Vlan40
 ip address 172.16.4.194 255.255.255.224
 ip helper-address 172.16.4.221
 standby 40 ip 172.16.4.222
 standby 40 priority 150
 standby 40 preempt
```

Hình 4.9: Cấu hình VLAN, HSRP và DCHP Relay

Cấu hình VTP :

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.1000
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.16.4.226 on interface Et1/2 (first layer3 interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                    0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC
```

Hình 4.10: Cấu hình VTP

Cấu hình Spanning-tree :

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10,20 priority 28672
spanning-tree vlan 30,40 priority 24576
!
```

Hình 4.11: Cấu hình Spanning-tree

Cấu hình OSPF :

```
!
router ospf 1
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 passive-interface Vlan40
 network 172.16.4.0 0.0.0.255 area 0
!
```

Hình 4.12: Cấu hình OSPF

4.1.3 Cấu hình Switch SW1-TSC

Cấu hình Trunking và tạo EtherChannel :

```
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
```

Hình 4.13: Cấu hình Trunking và tạo EtherChannel

Cấu hình EtherChannel :

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Hình 4.14: Cấu hình EtherChannel

Cấu hình Access port :

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1
10   VLAN0010                         active    Et3/2
20   VLAN0020                         active    Et3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Hình 4.15: Cấu hình Access Port

Cấu hình VTP :

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.3000
Configuration last modified by 0.0.0.0 at 9-30-23 09:32:09

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xB2 0x7C 0xEB 0x44 0xB9 0x61 0x2A 0x3F
                                    0x8A 0xFD 0x1B 0x4B 0xBB 0xC0 0x41 0x01
```

Hình 4.16: Cấu hình VTP

4.1.4 Cấu hình Switch SW2-TSC

Cấu hình Trunking và tạo EtherChannel :

```
!
interface Ethernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode desirable
!
interface Ethernet1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
interface Ethernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode desirable
!
```

Hình 4.17: Cấu hình Trunking và tạo EtherChannel

Cấu hình EtherChannel :

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Hình 4.18: Cấu hình EtherChannel

Cấu hình Access Port :

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1
30   VLAN0030                         active    Et3/2
40   VLAN0040                         active    Et3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Hình 4.19: Cấu hình Access Port

Cấu hình VTP :

```
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.4000
Configuration last modified by 0.0.0.0 at 9-30-23 09:55:26

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xAA 0x0A 0x0E 0xAA 0xAB 0x6E 0xE3 0x3A
                                    0x7E 0xE8 0xDD 0xD8 0x14 0xC8 0xBC 0x2B
```

Hình 4.20: Cấu hình TCP

4.1.5 Cấu hình R1-TSC

Cấu hình IP , DHCP Relay và GRE VPN :

```
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.0.2
!
interface Tunnel1
 ip address 10.0.1.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.1.2
!
interface Tunnel2
 ip address 10.0.2.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.2.2
!
interface Ethernet0/0
 ip address 172.16.4.225 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
interface Serial1/0
 ip address 20.0.3.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 serial restart-delay 0
!
```

Hình 4.21: Cấu hình IP, DHCP Relay và GRE VPN

Cấu hình OSPF :

```
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.4.0 0.0.0.255 area 0
 default-information originate metric-type 1
!
```

Hình 4.22: Cấu hình OSPF

Cấu hình Default route và NAT :

```
ip nat inside source list 1 interface Serial1/0 overload
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
ipv6 ioam timestamp
!
!
access-list 1 permit any
```

Hình 4.23: Cấu hình Default route và NAT

4.1.6 Cấu hình R2-TSC

Cấu hình OSPF :

```
router ospf 1
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.4.0 0.0.0.255 area 0
 default-information originate metric-type 1
!
```

Hình 4.24: Cấu hình OSPF

Cấu hình Default route và NAT :

```
ip nat inside source list 1 interface Serial1/0 overload
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
ipv6 ioam timestamp
!
!
access-list 1 permit any
```

Hình 4.25: Cấu hình Default route và NAT

Cấu hình IP và GRE VPN :

```
interface Tunnel10
 ip address 10.0.10.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.0.2
!
interface Tunnel11
 ip address 10.0.11.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.1.2
!
interface Tunnel12
 ip address 10.0.12.1 255.255.255.0
 ip helper-address 172.16.4.221
 tunnel source Serial1/0
 tunnel destination 20.0.2.2
!
interface Ethernet0/0
 ip address 172.16.4.229 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
interface Serial1/0
 ip address 20.0.4.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 serial restart-delay 0
```

Hình 4.26: Cấu hình IP, DCHP Relay và GRE VPN

4.1.7 Cấu hình R-Nhanh1

Cấu hình IP, DHCP Relay và GRE VPN :

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.3.2
!
interface Tunnel10
 ip address 10.0.10.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.4.2
!
interface Ethernet0/0
 ip address 172.16.5.1 255.255.255.192
 ip helper-address 172.16.4.221
 ip nat inside
 ip virtual-reassembly in
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
interface Serial1/0
 ip address 20.0.0.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 serial restart-delay 0
```

Hình 4.27: Cấu hình IP, DHCP Relay và GRE VPN

Cấu hình OSPF :

```
router ospf 1
 passive-interface Ethernet0/0
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
!
```

Hình 4.28: Cấu hình OSPF

Cấu hình Default route và NAT :

```
ip nat inside source list 1 interface Serial1/0 overload
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
ipv6 ioam timestamp
!
!
access-list 1 permit any
```

Hình 4.29: Cấu hình Default route và NAT

4.1.8 Cấu hình R2-Nhanh2

Cấu hình OSPF :

```
router ospf 1
 passive-interface Ethernet0/0
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
```

Hình 4.30: Cấu hình OSPF

Cấu hình Default route và NAT

```
ip nat inside source list 1 interface Serial1/0 overload
ip route 0.0.0.0 0.0.0.0 Serial1/0
!
ipv6 ioam timestamp
!
!
access-list 1 permit any
```

Hình 4.31: Cấu hình Default route và NAT

Cấu hình IP, DHCP Relay và GRE VPN

```
interface Tunnel1
 ip address 10.0.1.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.3.2
!
interface Tunnel11
 ip address 10.0.11.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.4.2
!
interface Ethernet0/0
 ip address 172.16.5.65 255.255.255.192
 ip helper-address 172.16.4.221
 ip nat inside
 ip virtual-reassembly in
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
interface Serial1/0
 ip address 20.0.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 serial restart-delay 0
```

Hình 4.32: Cấu hình IP, DHCP Relay và GRE VPN

4.1.9 Cấu hình R3-Nhanh3

Cấu hình IP, DHCP Relay và GRE VPN

```
interface Tunnel2
 ip address 10.0.2.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.3.2
!
interface Tunnel12
 ip address 10.0.12.2 255.255.255.0
 tunnel source Serial1/0
 tunnel destination 20.0.4.2
!
interface Ethernet0/0
 ip address 172.16.5.129 255.255.255.192
 ip helper-address 172.16.4.221
 ip nat inside
 ip virtual-reassembly in
 duplex auto
!
interface Ethernet0/1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/2
 no ip address
 shutdown
 duplex auto
!
interface Ethernet0/3
 no ip address
 shutdown
 duplex auto
!
interface Serial1/0
 ip address 20.0.2.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 serial restart-delay 0
```

Hình 4.33: Cấu hình IP, DHCP Relay và GRE VPN

Cấu hình OSPF :

```
router ospf 1
 passive-interface Ethernet0/0
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
!
```

Hình 4.34: Cấu hình OSPF

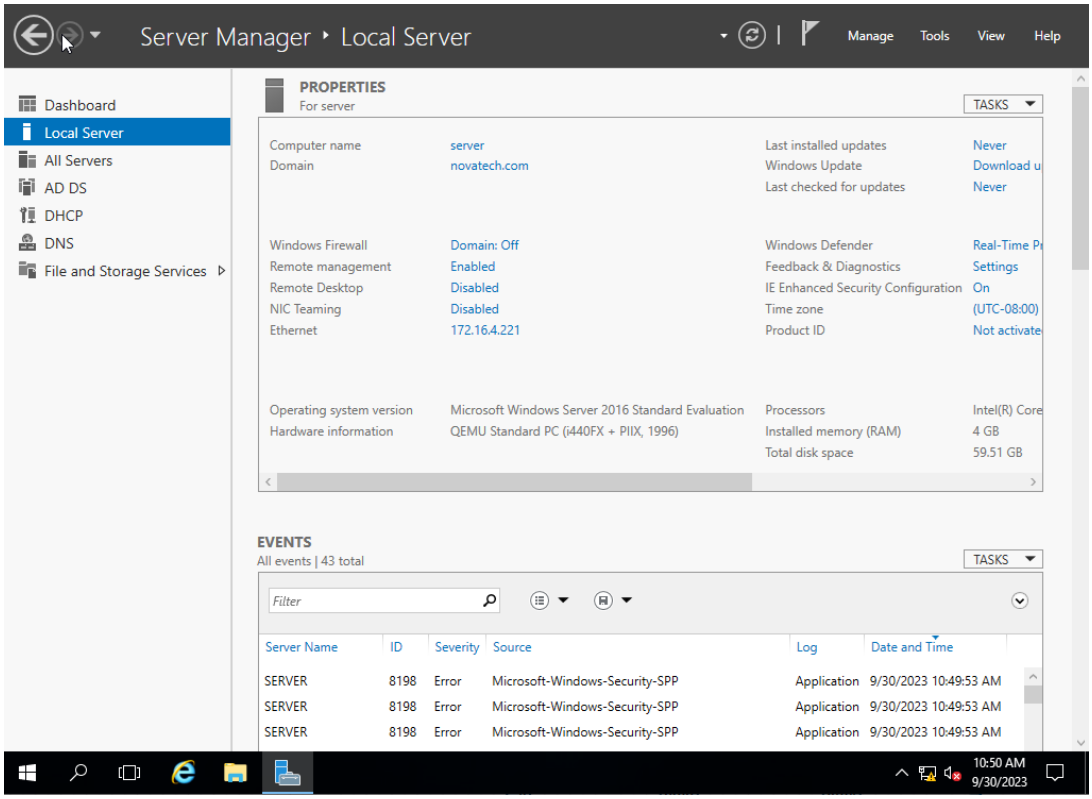
Cấu hình Default route và NAT :

```
router ospf 1
 passive-interface Ethernet0/0
 network 10.0.0.0 0.0.255.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
!
```

Hình 4.35: Cấu hình Default route và NAT

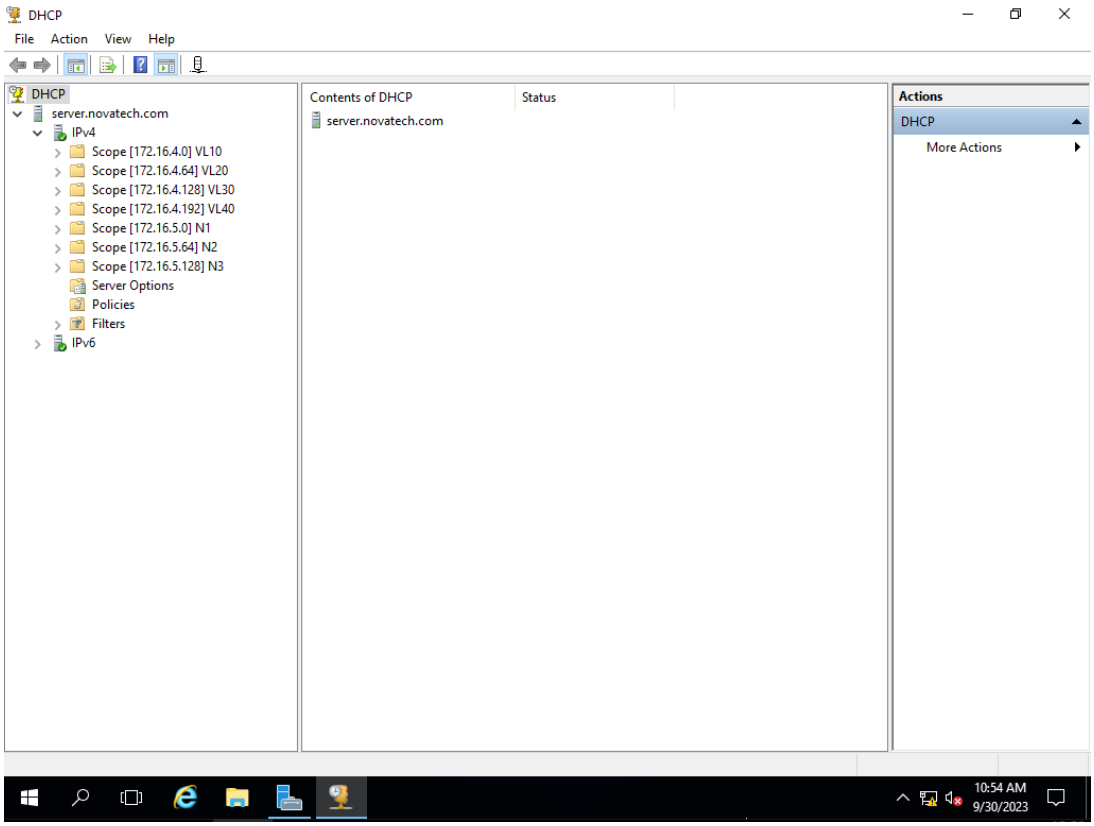
4.2 Các dịch vụ triển khai trên Server

4.2.1 Tạo máy chủ ADDS



Hình 4.36: Tạo máy chủ ADDS với tên miền novatech.com

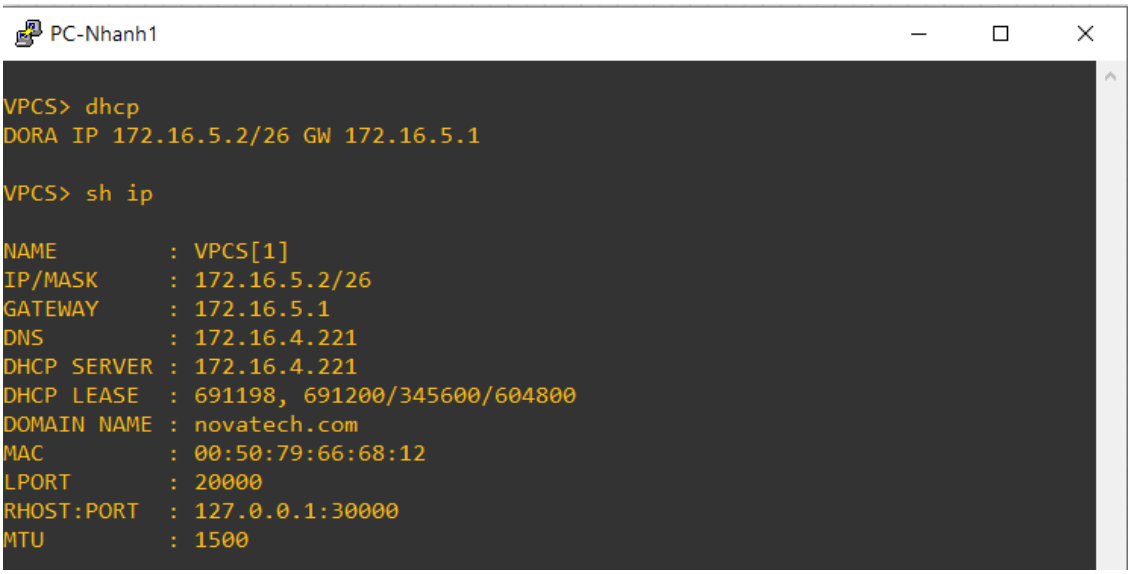
4.2.2 Cấu hình dịch vụ DHCP



Hình 4.37: Cấu hình dịch vụ DHCP

4.3 Kiểm tra cấu hình

4.3.1 Kiểm tra dịch vụ DHCP



Hình 4.38: Kiểm tra dịch vụ DHCP

4.3.2 Kiểm tra kết nối giữa các chi nhánh

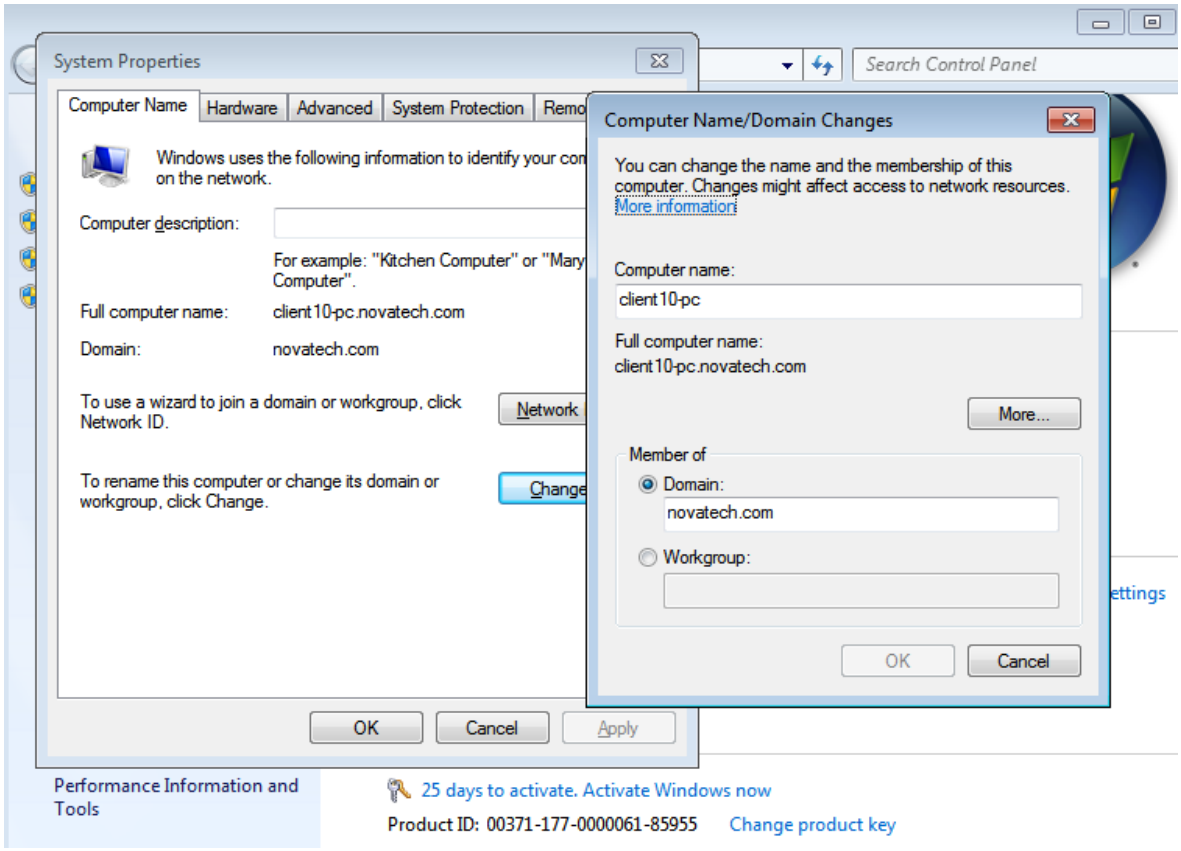
```
VPCS> ping 172.16.4.3

84 bytes from 172.16.4.3 icmp_seq=1 ttl=125 time=20.903 ms
84 bytes from 172.16.4.3 icmp_seq=2 ttl=125 time=23.048 ms
84 bytes from 172.16.4.3 icmp_seq=3 ttl=125 time=23.232 ms
84 bytes from 172.16.4.3 icmp_seq=4 ttl=125 time=20.648 ms
84 bytes from 172.16.4.3 icmp_seq=5 ttl=125 time=21.252 ms

VPCS>
```

Hình 4.39: Kiểm tra kết nối giữa Trụ sở chính và Chi Nhánh 1

4.3.3 Kiểm tra gia nhập Domain trên win 7



Hình 4.40: Kiểm tra gia nhập Domain trên win 7

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Những kết quả đạt được trong đề tài:

- Thành công trong việc triển khai mạng cho doanh nghiệp trên EVE-NG
- Áp dụng được các chính sách doanh nghiệp đề ra
- Đảm bảo dự phòng cho hệ thống mạng
- Đảm bảo lưu lượng băng thông cho toàn bộ hệ thống
- Sử dụng VLAN và VTP để quản lý và tối ưu hoá hệ thống mạng

Những việc chưa hoàng thành :

- Chưa áp dụng được các tính năng bảo mật cho hệ thống
- Chi phí dành cho thiết bị mạng chưa được tối ưu

Hướng phát triển :

Từ những nội dung đã làm được tiếp tục phát triển và nghiên cứu thêm để hoàn thiện tốt hơn cũng như nghiên cứu thêm cách vận hành các thiết bị bảo mật cũng như triển khai những tính năng bảo mật trên các thiết bị mạng để giúp cho hệ thống mạng thiết kế được an toàn hơn trước các mối đe dọa về bảo mật của những cuộc tấn công mạng nhằm đánh cắp dữ liệu và phá hủy hệ thống.