CỤC TMĐT-CNTT
TRUNG TÂM TIN HỌC

ĐỀ TÀI

Nghiên cứu các giải pháp tăng cường chất lượng dịch vụ mạng sử dụng mạng Lan ảo và phát triển dịch vụ truy nhập từ xa vào mạng nội bộ thông qua internet

CHỦ NHIỆM ĐỀ TÀI

HUỲNH ĐỨC NGHĨA

7059
05/01/2009

Hà Nội, Tháng 12 năm 2008.

MỤC LỤC

LỜI NHÓM TÁC GIẢ

Nhóm tác giả thực hiện đề tài xin được dành vị trí trân trọng nhất để bày tỏ sự biết ơn chân thành đến Lãnh đạo Bộ Công Thương,Vụ Khoa học và Công nghệ, Trung tâm Tin học đã hết lòng tạo điều kiện, động viên, khuyến khích chúng tôi trong thời gian thực hiện đề tài này.

Nhóm tác giả cũng xin bày tỏ lời cảm ơn chân thành đến các anh chị, đồng nghiệp, là những người trực tiếp tham gia, hỗ trợ kiến thức, chia sẻ kinh nghiệm quý báu trong quá trình tìm hiểu công tác nghiệp vụ, đồng thời cũng là những chuyên gia tư vấn về hệ thống, những người trực tiếp hỗ trợ, thu thập, cung cấp tài liệu, kiểm tra và đánh giá trong giai đoạn thực hiện đề tài.

TÓM TẮT ĐỀ TÀI

Đề tài "***Nghiên cứu các giải pháp tăng cường chất lượng dịch vụ mạng sử dụng mạng Lan ảo và phát triển dịch vụ truy nhập từ xa vào mạng nội bộ thông qua internet*** " được thực hiện căn cứ theo Quyết định số 1999/QĐ-BCT ngày 03/12/2007 của Bộ trưởng Bộ Công Thương về việc giao kế hoạch khoa học và công nghệ năm 2008

Mục đích chính của đề tài

1. Khảo sát hiện trạng hệ thống mạng nội bộ cơ quan Bộ.
2. Nghiên cứu xây dựng 5 mạng Lan ảo tại Bộ Công Thương và 4 mạng Lan ảo tại các đơn vị kết nối đến Bộ để tăng cường sự ổn định và chất lượng dịch vụ mạng máy tính Bộ Công Thương.
3. Nghiên cứu sử dụng công nghệ VPN để cung cấp khả năng kết nối từ xa vào mạng nội bộ thông qua internet.

Kết quả thực hiện của đề tài

1. Báo cáo tìm hiểu công nghệ Lan ảo (VLAN)
2. Triển khai 5 mạng Lan ảo tại cơ quan Bộ Công Thương và 4 mạng Lan ảo cho các đơn vị kết nối đến Bộ
3. Triển khai cung cấp dịch vụ kết nối mạng nôi bộ từ xa qua Internet.

CÁC TỪ VIẾT TẮT

STT	Viết tắt	Diễn giải
1	VLAN	Virtual Local area network: Mạng Lan ảo
2	VPN	Virtual Private Network: Mạng riêng ảo
3	BCT	Bộ Công Thương
4	CNTT	Công Nghệ Thông Tin
5	IP	Internet Protocol
6	OSI	Open System Interconnection
7	MAC	Media Access Control

CHƯƠNG I: GIỚI THIỆU ĐỀ TÀI

1.1Cơ sở pháp lý xuất xứ đề tài:

Đề tài "***Nghiên cứu các giải pháp tăng cường chất lượng dịch vụ mạng sử dụng mạng Lan ảo và phát triển dịch vụ truy nhập từ xa vào mạng nội bộ thông qua internet*** " được thực hiện căn cứ theo Quyết định số 1999/QĐ-BCT ngày 03/12/2007 của Bộ trưởng Bộ Công Thương về việc giao kế hoạch khoa học và công nghệ năm 2008

1.2 Tính cấp thiết và mục tiêu nghiên cứu của đề tài:

Ngày nay, với sự phát triển lớn mạnh của Công nghệ Thông tin đặc biệt là ứng dụng hệ thống Công nghệ Thông tin trong công việc quản lý hành chính. Công nghệ Thông tin đã trở thành một công cụ đắc lực, nó giúp giảm chi phí về thời gian và tiền của, mang lại sự thuận tiện.

Mục tiêu nghiên cứu xuyên suốt của đề tài là làm sao nắm bắt được công nghệ Vlan, nghiên cứu các đặc tính nổi bật của Vlan từ đó ứng dụng vào mô hình hệ thống mạng của Bộ Công Thương. Đồng thời nghiên cứu công nghệ mạng truy cập từ xa Virtual private network. Kết quả phải đạt được là:

- Báo cáo tìm hiểu về công nghệ Lan ảo(Vlan).

- Triển khai 5 mạng Lan ảo tại cơ quan Bộ Công Thương và 4 mạng Lan ảo cho các đơn vị ngoài Bộ kết nối vào.

- Triển khai cung cấp dịch vụ kết nối mạng từ xa qua internet.

1.3 Đối tượng, phạm vi và nội dung nghiên cứu:

Đề tài "Nghiên cứu các giải pháp tăng cường chất lượng dịch vụ mạng sử dụng mạng Lan ảo và phát triển dịch vụ truy nhập từ xa vào mạng nội bộ thông qua internet'' với mục đích chính là triển khai hai dịch vụ cơ bản cho người dùng cơ quan Bộ Công Thương và một số các đơn vị kết nối vào Bộ. Do đó, phạm vi nghiên cứu và thực hiện đề tài là trong cơ quan Bộ Công Thương và triển khai cấu hình thiết bị ngay tại trụ sơ cơ quan Bộ.

Trong quá trình thực hiện đề tài, nhóm thực hiện đề tài thu thập nguồn tài liệu từ các nguồn tài liệu của các tổ chức nổi tiếng trên thế giới. Áp dụng mô hình của họ vào mô hình thực tiễn của Bộ Công Thương. Tham khảo một số mô hình các đơn vị có uy tín về Công nghệ thông tin trong nước và khu vực.

Nội dung của đề tài được tập trung vào hai nhiệm vụ chính là nghiên cứu triển khai hai dịch vụ mạng Lan ảo và mạng truy nhập từ xa đáp ứng nhu cầu dịch vụ cho người dùng, tiện lợi cho quản trị viên trong quá trình vận hành giám sát hệ thống mọi lúc mọi nơi. Qua đó các công việc phải làm là:

- ❖ Khảo sát hiện trạng hệ thống mạng nội bộ cơ quan Bộ.
- ❖ Nghiên cứu xây dựng 5 mạng Lan ảo tại Bộ Công Thương và 4 mạng Lan ảo tại các đơn vị kết nối đến Bộ để tăng cường sự ổn định và chất lượng dịch vụ mạng máy tính Bộ Công Thương.
- ❖ Nghiên cứu sử dụng công nghệ VPN để cung cấp khả năng kết nối từ xa vào mạng nội bộ thông qua internet.

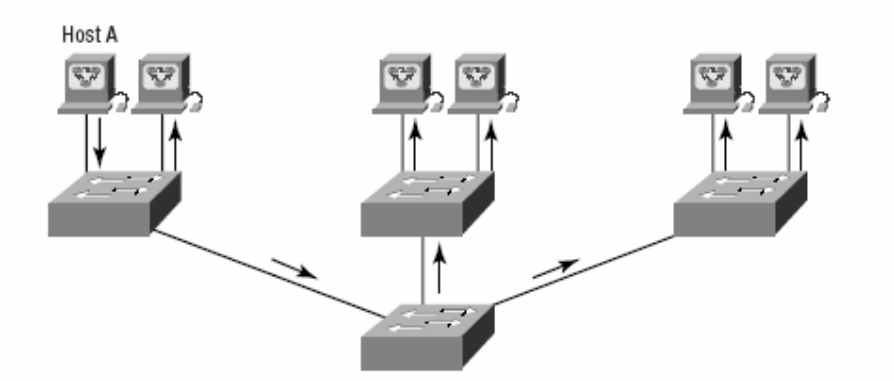
1.4 Tổng quan tình hình nghiên cứu trong và ngoài nước:

Tình hình nghiên cứu trong và ngoài nước: Với sự phát triển của Công nghệ thông tin trong nước và ngoài nước, việc áp dụng vào quản lý nhà nước là tất yếu. Việc áp dụng CNTT làm đơn giản hóa quản lý, giúp cho người dùng có nhiều công cụ thuận tiện trong quản lý và sử dụng. Với sự phát triển trong cũng như ngoài nước, công nghệ mạng Lan ảo và công nghệ mạng riêng ảo là sự lựa chọn hàng đầu. Nó phục vụ cho người dùng và đơn giản hóa công việc nhưng vẫn tiết kiệm được chi phí xây dựng và quản lý. Mô hình mạng Lan ảo giúp cho các đơn vị phát triển các chi nhánh một cách thuận tiện, nó giảm tối đa về chi phí đầu tư mà vẫn mang lại thuận tiện cho người sử dụng. Ngoài ra công nghệ mạng Lan ảo còn giúp tiện kiệm về băng thông của hệ thống, giúp cho trao đổi dữ liệu nhanh hơn. Cũng như vậy, công nghệ mạng riêng ảo mang lại cho người sử dụng một công cụ truy nhập từ xa vào tài nguyên chia sẻ. Phục vụ một cách nhanh chóng và thuận tiện cho người dùng.

Do đó, với sự phát triển CNTT của Bộ Công Thương thì việc áp dụng mô hình mạng Lan ảo và mạng riêng ảo là rất cấp thiết.

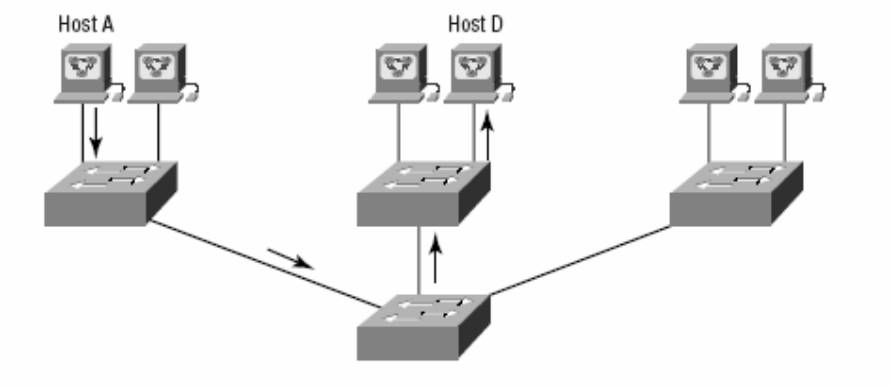
- Cơ sở lý thuyết:

+ Cơ sở lý thuyết Công nghệ mạng Lan ảo: Như chúng ta đã biết, trong mạng máy tính quá trình truyền thông tin dữ liệu được chia thành 7 bước (tức 7 lớp trong mô hình OSI) . Ở lớp 2 của mô hình OSI, là lớp mà Switch hoạt động, thường thì Switch hoạt động trong một mạng Flat (tức mạng ngang hàng,không có phân quyền). Toàn bộ thông tin truyền trên mạng sẽ Broadcast trên toàn mạng, có nghĩa là ai cũng có quyền như nhau, do đó nó chỉ có 1 miền Broadcast .



Hình 1: Mô hình mạng máy tính

Thông tin từ một máy HostA truyền trên mạng sẽ truyền đến cho hết các máy trong mạng LAN, sau đó máy nào có địa chỉ MAC, IP thích hợp sẽ nhận thông tin, còn các máy khác sẽ discard.



Hình 2: Mô hình truyền dữ liệu giữa các máy tính

Còn khi chúng ta đã có được các tính năng lớp 3 trong Switch thì chúng ta sẽ thấy rằng: khi dữ liệu gửi từ Host A tới Host D, thì chỉ host D nhận được yêu cầu nhận. Và lúc đó thông tin trên mạng sẽ không bị dư thừa.

Để có được những tính năng trên chúng ta phải nói đến VLAN:

- Vlan mang lại Bảo mật trong mạng.
- Phân quyền người dùng truy nhập vào cơ sở dữ liệu, theo chức năng, nhiệm vụ….
- Tăng số vùng Broadcast, nhưng lại giảm dung lượng kích cỡ của chúng.

❖ **Các loại Vlan:**

- **Static Vlan:**

Là một kiểu Vlan mà chúng ta sẽ không phải cấu hình, theo đó thì tất cả các port của Switch sẽ thuộc Vlan1. Trong kiểu Vlan này thì nó có đầy đủ các tính năng có của Vlan. Cái khác ở đây là tất cả các port sẽ thuộc một Vlan, như vậy sẽ xảy ra trường hợp thừa port trong đó lại thiếu Vlan để phân quyền.

- **Dynamic Vlan:**

Là một kiểu Vlan mà chúng dựa vào địa chỉ Mac, giao thức, ứng dụng. Việc dựa vào địa chỉ Mac có ý nghĩa rất quan trọng, chúng ta thử lấy một ví dụ sau:

Một máy Host A được phân vào một VLan x nào đó, nghĩa là máy A chỉ vào được mạng Lan khi máy A cắm đúng vào port của switch, qua đó ta sẽ thấy sự bất tiện là nếu máy A muốn di chuyển đến nơi khác thì sẽ gặp vấn đề.

Người ta đã có giải pháp là dùng VLan gán địa chỉ Mac của máy A cho Vlan mà nó thuộc vào. Vì địa chỉ MAC thì không bao giờ thay đổi và nó có tính chất đơn nhất trên toàn cầu. Từ đó việc di chuyển máy A đến các địa điểm khác nhau không còn vấn đề. Switch chỉ cần nhận biết trong NvRam của nó rằng cứ với một địa chỉ Mac này của máy A sẽ tương ứng với việc nó thuộc VLan đã ấn định sẵn mà không cần quan tâm nó được gán vào port nào của Switch.

❖ **Nhận dạng Vlan:**

- **Các kiểu kết nối:**

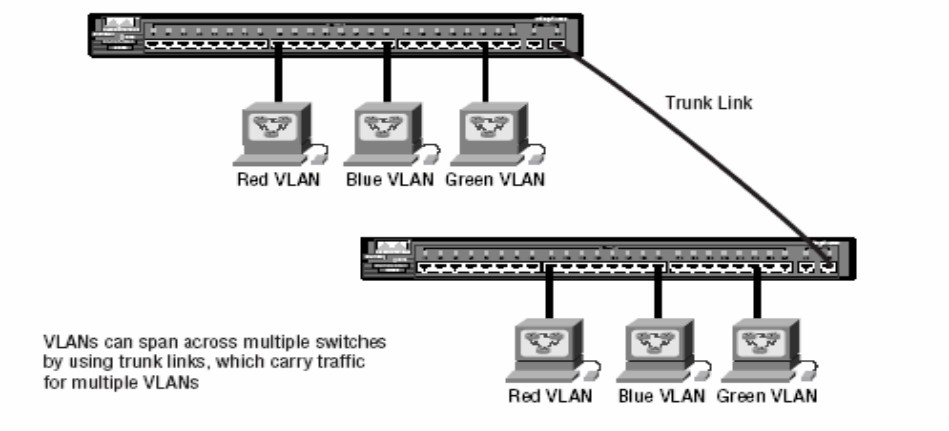
Có hai loại kế nối(link) trong môi trường Vlan:

a. Access link:

Thực chất nó chính là các liên kết port trong switch, các Vlan không thể nói chuyện với nhau nếu chúng không có một lien kết khác mà chúng ta muốn đề cập đến đây là Trunk link.

b. Trunk link:

Tác dụng chính của trunk link là cho phép các Vlan có thể nói chuyện với nhau,tốc độ của nó có thể lên tới:100--1000Mbps và có thể định tuyến 1--1005 Vlan cùng một lúc. Chúng ta sẽ đề cập tới vấn đề này trong phần sau:



Hình 3: Mô hình mạng Lan ảo

Nhìn trên hình vẽ chúng ta có thể thấy được là:

- Có 3 Vlan: **Red Vlan**

  Blue Vlan

  Green Vlan

- Các máy trong 1 Vlan nối với nhau qua đường Access link.
- Việc kết nối các Vlan với nhau qua đường Trunk Link.
- Các máy thuộc Vlan khác nhau có thể ở trên các Switch khác nhau mà việc liên kết không gặp vấn đề. **Việc này khá quan trọng!!**

❖ **Các phương pháp đóng gói trong Vlan:**

- **Inter-Switch Link (ISL):** Là sản phẩm của Cisco,chỉ dùng cho các sản phẩm của cisco.
- **IEEE 802.1Q**: Có thể hoạt động trên các sản phẩm của các hãng khác nhau.

❖ **VLAN Trunking Protocol (VTP):** Nó cho phép quản lý kết nối liên mạng trên các Vlan, thêm bớt, thay đổi tên Vlan.

❖ **Các loại VTP:**

a. Server:

Loại VTP Server luôn là cấu hình mặc định cho các Switch (khi chúng ta mua về, nó đã được gán là thuộc kiểu VTP Server).

Đặc điểm nổi bật của VTP Server là:

- Có thể tạo thêm Vlan, xoá Vlan
- Thay đổi các cấu hình
- Đóng vai trò Switch chủ

b. Client:

Loại VTP Client, Switch sẽ nhận thông tin từ các VTP Server và gửi cũng như nhận các thông tin updates.

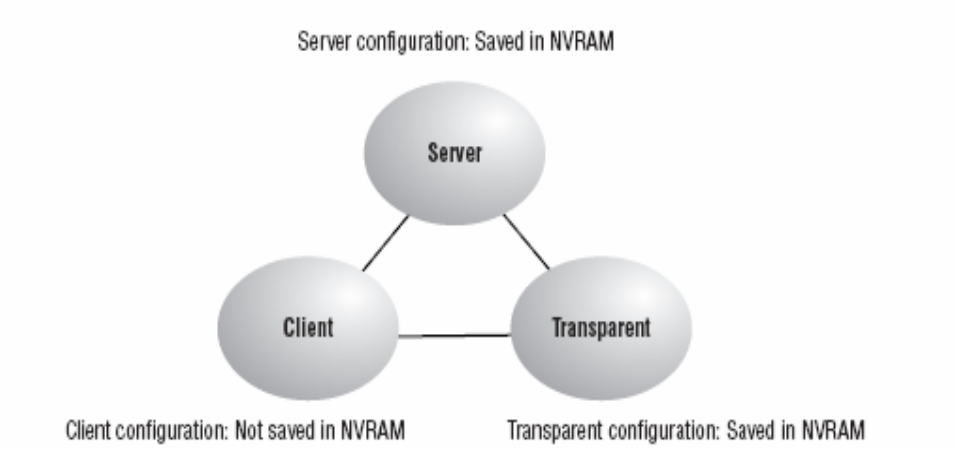
Đặc điểm nổi bật của VTP Client là:

- Không thể thay đổi cấu hình trên Switch.
- Nó chỉ đóng vai trò Switch khách.
- Khi chúng ta muốn chuyển một Switch thành Switch Server thì chúng ta nên chuyển Switch đó thành kiểu Client trước vì khi ở kiểu Client thì Switch sẽ nhận mọi thông tin về Vlan. Sau đó chúng ta chuyển thành Server thì sẽ hiệu quả hơn.
- Một đặc điểm quan trọng nữa của Client VTP là Switch sẽ nhận thông tin mà không lưu trữ trên NVRam, có nghĩa là toàn bộ thông tin sẽ bị mất nếu chúng ta Reset lại Switch.

c. Transparent:

- Switch sẽ chỉ truyền (forward) thông tin.
- Không thể thay đổi thông tin về Vlan.
- Thông tin được lưu trữ trong NVRam .

- Nhiệm vụ chính của chế độ Transparent là cho phép các Switch từ xa nhận thông tin cơ sở dữ liệu của Vlan từ VTP Server qua một Switch mà nó không thuộc cùng Vlan.



Hình 4: Các kiểu mạng Lan ảo

❖ **Định tuyến giữa các Vlan :**

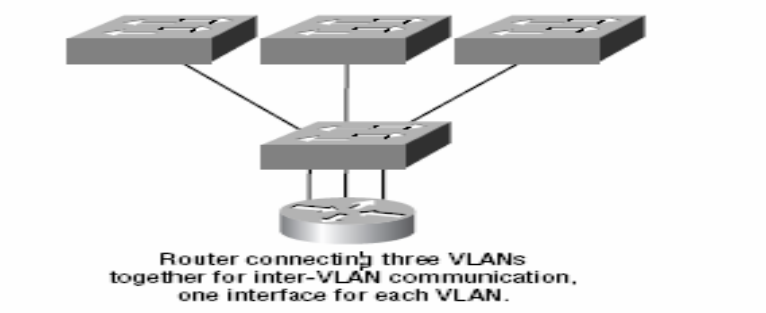
Để định tuyến thông tin trên các Vlan chúng ta cần có sự hỗ trợ của Router. Vì thông tin giữa các Vlan thuộc các miền Broadcast khác nhau nên để các Vlan khác nhau nói chuyện được với nhau thì chúng ta phải có Router để định tuyến thông tin lớp 3.

Vậy thì câu hỏi đặt ra là:

- Các Switch nối với nhau kiểu gì?
- Các Switch là router nối với nhau qua đường nào?

Chúng ta thử xem hai mô hình dưới đây:

- **Kiểu 1:**



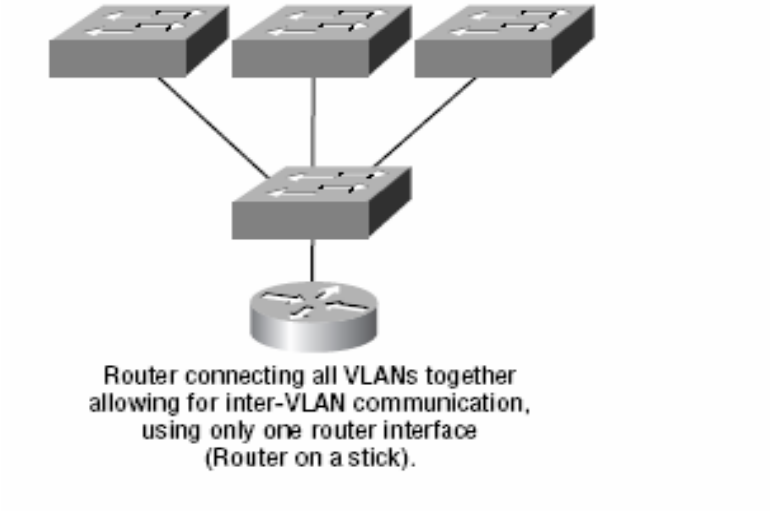
Hình 5: Mô hình mạng Lan ảo 1

Có 3 Vlan và các Vlan này được nối với router qua 3 interface (Ethernet). Vậy thì sẽ đặt ra câu hỏi là nếu mà có nhiều Vlan thì làm sao có đủ cổng Ethernet cho router (Vì cổng router thường chỉ có 2 cổng, nếu lắp thêm thì cũng không được nhiều).

- **Kiểu 2:**

Giải pháp cho Kiểu 1 là chúng ta chỉ cần một cổng Ethernet nhưng chúng ta sẽ dùng Subinterface.

Ở kiểu Subinterface thì sẽ chia một cổng Physical (vật lý) thành các cổng con có cùng đặc tính và được gọi là cổng Logical. Mỗi cổng ảo đó sẽ đảm nhiệm cho một Vlan.

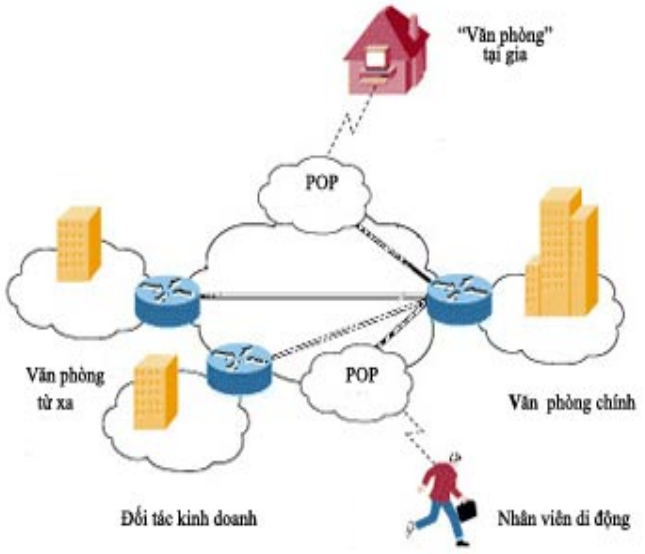


Hình 6: Mô hình mạng Lan ảo 2

Trên hình vẽ chúng ta có thể thấy được chỉ có một cổng vật lý nối giữa router và Switch. Trong khi đó có những 3 Vlan (hoặc nhiều hơn).

+ Cơ sở lý thuyết công nghệ mạng riêng ảo:

Giải pháp VPN (Virtual Private Network) được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn nên tiết kiệm được được chi phí và thời gian. Do đó, mô hình mạng riêng ảo được triển khai tại Bộ Công Thương để mang lại tiện ích truy nhập từ xa tới hệ thống mạng của Bộ thông qua kết nối internet.



Hình 7: Một mạng VPN điển hình bao gồm mạng LAN chính tại trụ sở (Văn phòng chính), các mạng LAN khác tại những văn phòng từ xa, các điểm kết nối (như 'Văn phòng' tại gia) hoặc người sử dụng (Nhân viên di động) truy cập đến từ bên ngoài.

- Khái niệm:

Về cơ bản, VPN là một mạng riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các địa điểm hoặc người sử dụng từ xa với một mạng LAN ở trụ sở trung tâm. Thay vì dùng kết nối thật khá phức tạp như

đường dây thuê bao số, VPN tạo ra các liên kết ảo được truyền qua Internet giữa mạng riêng của một tổ chức với địa điểm hoặc người sử dụng ở xa.

- Các loại VPN

Có hai loại phổ biến hiện nay là VPN truy cập từ xa (Remote-Access) và VPN điểm-nối-điểm (site-to-site). VPN truy cập từ xa còn được gọi là mạng Dial-up riêng ảo (VPDN), là một kết nối người dùng-đến-LAN, thường là nhu cầu của một tổ chức có nhiều nhân viên cần liên hệ với mạng riêng của mình từ rất nhiều địa điểm ở xa. Ví dụ như công ty muốn thiết lập một VPN lớn phải cần đến một nhà cung cấp dịch vụ doanh nghiệp (ESP). ESP này tạo ra một máy chủ truy cập mạng (NAS) và cung cấp cho những người sử dụng từ xa một phần mềm máy khách cho máy tính của họ. Sau đó, người sử dụng có thể gọi một số miễn phí để liên hệ với NAS và dùng phần mềm VPN máy khách để truy cập vào mạng riêng của công ty. Loại VPN này cho phép các kết nối an toàn, có mật mã.

Hình minh họa cho thấy kết nối giữa Văn phòng chính và "Văn phòng" tại gia hoặc nhân viên di động là loại VPN truy cập từ xa).

VPN điểm-nối-điểm là việc sử dụng mật mã dành cho nhiều người để kết nối nhiều điểm cố định với nhau thông qua một mạng công cộng như Internet. Loại này có thể dựa trên Intranet hoặc Extranet. Loại dựa trên Intranet: Nếu một công ty có vài địa điểm từ xa muốn tham gia vào một mạng riêng duy nhất, họ có thể tạo ra một VPN intranet (VPN nội bộ) để nối LAN với LAN. Loại dựa trên Extranet: Khi một công ty có mối quan hệ mật thiết với một công ty khác (ví dụ như đối tác cung cấp, khách hàng...), họ có thể xây dựng một VPN extranet (VPN mở rộng) kết nối LAN với LAN để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung.

Trong hình minh họa trên, kết nối giữa Văn phòng chính và Văn phòng từ xa là loại VPN Intranet, kết nối giữa Văn phòng chính với Đối tác kinh doanh là VPN Extranet.

- Bảo mật trong VPN:

Tường lửa (firewall) là rào chắn vững chắc giữa mạng riêng và Internet. Bạn có thể thiết lập các tường lửa để hạn chế số lượng cổng mở, loại gói tin và giao thức được chuyển qua. Một số sản phẩm dùng cho VPN như router 1700 của Cisco có thể nâng cấp để gộp những tính năng của tường lửa bằng cách chạy hệ điều hành Internet Cisco IOS thích hợp. Tốt nhất là hãy cài tường lửa thật tốt trước khi thiết lập VPN.

Mật mã truy cập là khi một máy tính mã hóa dữ liệu và gửi nó tới một máy tính khác thì chỉ có máy đó mới giải mã được. Có hai loại là mật mã riêng và mật mã chung.

Mật mã riêng (Symmetric-Key Encryption): Mỗi máy tính đều có một mã bí mật để mã hóa gói tin trước khi gửi tới máy tính khác trong mạng. Mã riêng yêu cầu bạn phải biết mình đang liên hệ với những máy tính nào để có thể cài mã lên đó, để máy tính của người nhận có thể giải mã được.

Mật mã chung (Public-Key Encryption) kết hợp mã riêng và một mã công cộng. Mã riêng này chỉ có máy của bạn nhận biết, còn mã chung thì do máy của bạn cấp cho bất kỳ máy nào muốn liên hệ (một cách an toàn) với nó. Để giải mã một message, máy tính phải dùng mã chung được máy tính nguồn cung cấp, đồng thời cần đến mã riêng của nó nữa. Có một ứng dụng loại này được dùng rất phổ biến là Pretty Good Privacy (PGP), cho phép bạn mã hóa hầu như bất cứ thứ gì.

Giao thức bảo mật giao thức Internet (IPSec) cung cấp những tính năng an ninh cao cấp như các thuật toán mã hóa tốt hơn, quá trình thẩm định quyền đăng nhập toàn diện hơn.

IPSec có hai cơ chế mã hóa là Tunnel và Transport. Tunnel mã hóa tiêu đề (header) và kích thước của mỗi gói tin còn Transport chỉ mã hóa kích thước. Chỉ những hệ thống nào hỗ trợ IPSec mới có thể tận dụng được giao thức này. Ngoài ra, tất cả các thiết bị phải sử dụng một mã khóa chung và các tường lửa trên mỗi hệ thống phải có các thiết lập bảo mật giống nhau. IPSec có thể mã hóa dữ liệu giữa nhiều thiết bị khác nhau như router với router, firewall với router, PC với router, PC với máy chủ.

- Máy chủ AAA:

AAA là viết tắt của ba chữ Authentication (thẩm định quyền truy cập), Authorization (cho phép) và Accounting (kiểm soát). Các server này được dùng để đảm bảo truy cập an toàn hơn. Khi yêu cầu thiết lập một kết nối được gửi tới từ máy khách, nó sẽ phải qua máy chủ AAA để kiểm tra. Các thông tin về những hoạt động của người sử dụng là hết sức cần thiết để theo dõi vì mục đích an toàn.

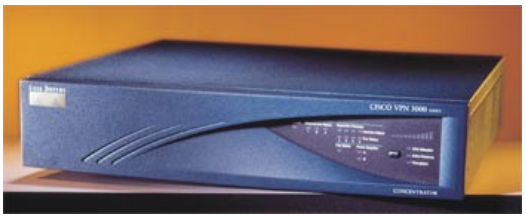
Sản phẩm công nghệ dành cho VPN:

Tùy vào loại VPN (truy cập từ xa hay điểm-nối-điểm), bạn sẽ cần phải cài đặt những bộ phận hợp thành nào đó để thiết lập mạng riêng ảo. Đó có thể là:

- Phần mềm cho desktop của máy khách dành cho người sử dụng từ xa.
- Phần cứng cao cấp như bộ xử lý trung tâm VPN hoặc firewall bảo mật PIX.
- Mạng VPN và trung tâm quản lý.

- Bộ xử lý trung tâm VPN:

Có nhiều loại máy xử lý VPN của các hãng khác nhau, nhưng sản phẩm của Cisco tỏ ra vượt trội ở một số tính năng. Tích hợp các kỹ thuật mã hóa và thẩm định quyền truy cập cao cấp nhất hiện nay, máy xử lý VPN được thiết kế chuyên biệt cho loại mạng này. Chúng chứa các module xử lý mã hóa SEP, cho phép người sử dụng dễ dàng tăng dung lượng và số lượng gói tin truyền tải. Dòng sản phẩm có các model thích hợp cho các mô hình doanh nghiệp từ nhỏ đến lớn (từ 100 cho đến 10.000 điểm kết nối từ xa truy cập cùng lúc).



Hình 8: Bộ xử lý trung tâm VPN số hiệu 3000 của hãng Cisco.

- Router dùng cho VPN:

Thiết bị này cung cấp các tính năng truyền dẫn, bảo mật. Dựa trên hệ điều hành Internet IOS của mình, hãng Cisco phát triển loại router thích hợp cho mọi trường hợp, từ truy cập nhà-tới-văn phòng cho đến nhu cầu của các doanh nghiệp quy mô lớn.

- Tường lửa PIX của Cisco:

Firewall trao đổi Internet riêng (Private Internet Exchange) bao gồm một cơ chế dịch địa chỉ mạng rất mạnh, máy chủ proxy, bộ lọc gói tin, các tính năng VPN và chặn truy cập bất hợp pháp.

Thay vì dùng IOS, thiết bị này có hệ điều hành với khả năng tổ chức cao, xoay sở được với nhiều giao thức, hoạt động rất mạnh bằng cách tập trung vào IP.

Kết luận

Cùng với sự phổ cập ngày càng cao của Internet, doanh nghiệp dần chuyển sang sử dụng Internet như một phương tiện giúp họ mở rộng mạng cục bộ sẵn có. Đầu tiên là intranets, đây là những sites được bảo vệ bằng password và sử dụng trong phạm vi công ty. Còn bây giờ nhiều doanh nghiệp đang thiết lập dịch vụ VPN (virtual private network).

Nhằm thoả mãn nhu cầu kết nối từ xa giữa nhân viên với văn phòng cũng như giữa các văn phòng cách xa.

Một mạng riêng ảo (VPN) tiêu biểu có thể gồm một mạng LAN chính đặt tại trụ sở chính của công ty, các mạng LAN khác tại những văn phòng ở xa, cũng như những nhân viên kết nối từ xa đến mạng nội bộ của công ty.

VPN về cơ bản là một mạng cục bộ sử dụng hệ thống mạng công cộng sẵn có như Internet để kết nối các văn phòng cũng như nhân viên ở xa. Thay vì sử dụng kết nối chuyên biệt và trực tiếp giữa các văn phòng như kênh thuê riêng

leased lines, một VPN (mạng riêng ảo) sử dụng các kết nối ảo được thiết lập trong môi trường Internet từ mạng riêng của công ty tới các văn phòng.

Sự phát triển của dịch vụ tạo mạng riêng ảo trên internet (IP VPN) là một xu thế tất yếu trong quá trình hội tụ giữa internet và các mạng dùng riêng. Có bốn lý do dẫn đến quá trình hội tụ này ở việt nam cũng như trên thế giới:

Sự phát triển về mặt địa lý của thị trường dẫn đến sự gia tăng số lượng nhân viên hoạt động phân tán điều này gây khó khăn trong việc quản lý của các mạng dùng riêng.

Nhu cầu sử dụng tác nghiệp trực tuyến. Sự phát triển của nền kinh tế dẫn đến xu hướng làm việc với nhiều nhà cung cấp dịchvụ, sản phẩm cũng như đối với nhiều đối tượng khách hàng khác nhau. Mỗi nhà cung cấp dịch vụ sản phẩm, khách hàng sử dụng cấu trúc mạng khác nhau (thủ tục, ứng dụng, nhà cung cấp dịch vụ, hệ thống quản trị mạng lưới...). Điều này là một thách thức lớn đối với một mạng dùng riêng trong việc kết nối với tất cả các mạng này.

Chi phí cho việc cài đặt và duy trì một mạng diện rộng là lớn. Nhu cầu tích hợp và đơn giản hoá giao diện cho người sử dụng

Trong tình hình Việt Nam hiện nay cùng với việc phổ cập Internet tốc độ cao (hiện giờ là ADSL và sắp tới là Cable Internet) ngày càng rộng với giá rẻ, cũng như xuất hiện nhiều thiết bị mạng hỗ trợ VPN với chức năng tích hợp đa dạng, giao diện dễ sử dụng và giá hợp lý sẽ là điều kiện tốt để các doanh nghiệp và tổ chức tăng cường sử dụng mạng riêng ảo VPN như một phương thức kết nối từ xa an toàn, tiện dụng và nhanh chóng với chi phí thấp.

Với mô hình mạng hiện tại và nhu cầu của Bộ Công thương. Việc áp dụng giải pháp công nghệ Vlan và Vpn là hợp lý và rất cần thiết. Tuy nhiên, dựa trên các thiết bị sẵn có và dựa trên nhu cầu thực tế. Hệ thống Vlan của Bộ Công Thương sẽ được triển khai trên các thiết bị đã có và hệ thống Vpn sẽ được triển khai trên cơ sở phần mềm ISA 2006 có khả năng đáp ứng. Nhóm thực hiện đề tài cũng đề xuất phát triển hệ thống với các thiết bị chuyên dụng hơn để có thể cung cấp các ứng dụng tốt nhất cho người dùng.

CHƯƠNG 2: THỰC HIỆN ĐỀ TÀI

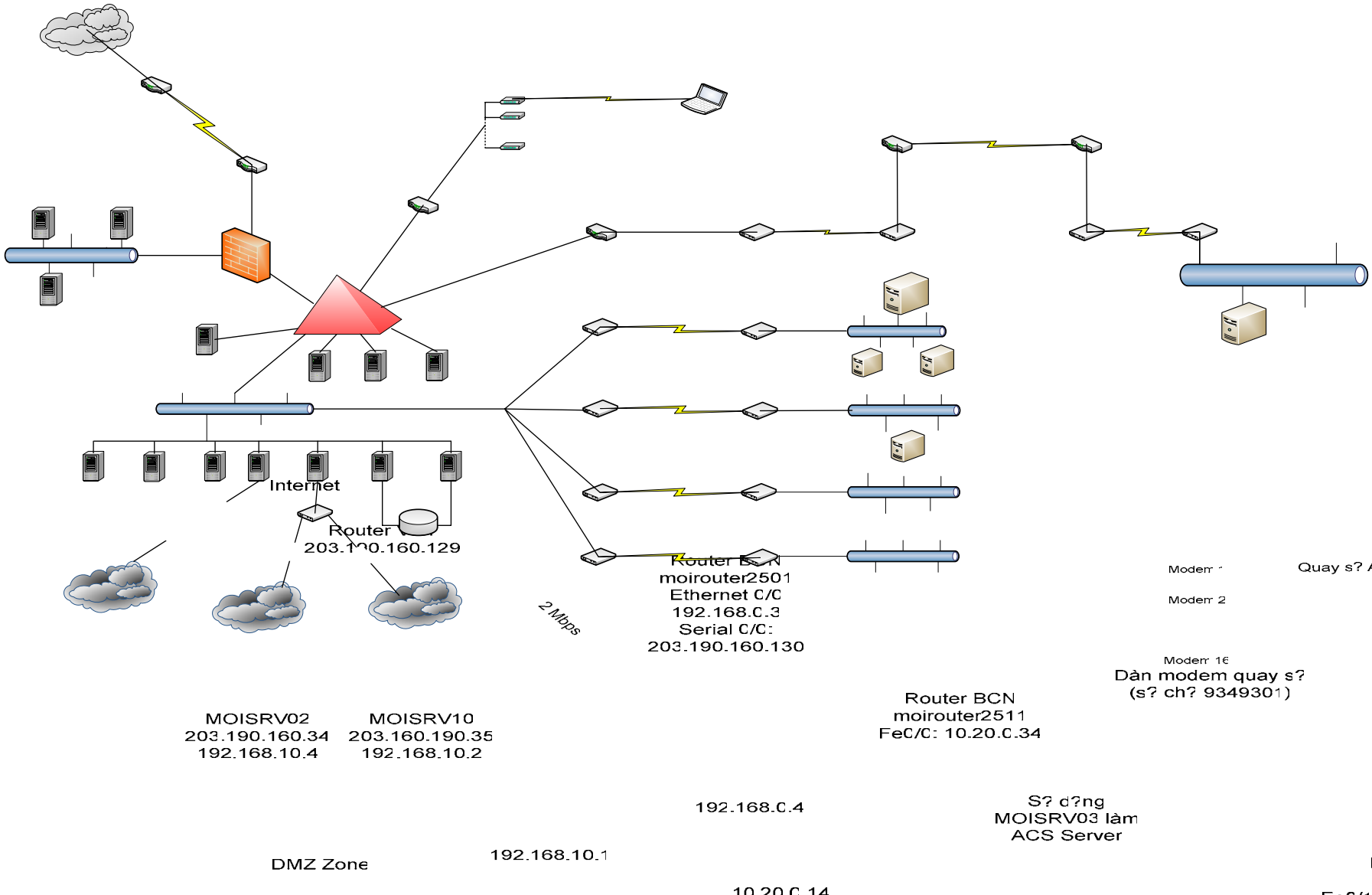
2.1 Phương pháp nghiên cứu:

Trong quá trình nghiên cứu đề tài, nhóm thực hiện đề tài tập hợp toàn bộ sơ đồ hiện trạng của hệ thống, từ đó phân tích đánh giá mô hình hiện trạng hệ thống để đưa ra giải pháp phù hợp cho các ứng dụng. Dựa trên cơ sở thực tiễn những vấn đề thường gặp việc nghiên cứu phát triển một giải pháp hiệu quả dựa trên những nguồn cung cấp tin cậy là thực sự quan trọng và cấp thiết với hiện trạng cơ sở hạ tầng công nghệ thông tin hiện nay. Từ đó đưa ra được phương pháp nghiên cứu triển khai hai hệ thống là hệ thống mạng Lan ảo và hệ thống mạng truy nhập từ xa cho Bộ Công Thương đáp ứng các nhu cầu thiết yếu trong trao đổi thông tin.

Trong quá trình thực hiện đề tài, nhóm thực hiện đề tài thu thập toàn bộ số liệu, mô hình hiện trạng của hệ thống. Từ đó phân tích đánh giá hiện trạng để đưa ra giải pháp thích hợp trong quá trình thực hiện đề tài. Dựa trên các thiết bị hiện có, nhóm thực hiện đề tài nghiên cứu các mô hình của các nước trên thế giới, áp dụng công nghệ mới nhất từ đó nhóm thực hiện đề tài sẽ tổng hợp được các thiết bị tại Bộ Công Thương có thể triển khai được hệ thống Lan ảo và mạng truy cập từ xa. Đồng thời nhóm thực hiện đề tài cũng đưa ra được các thiết bị cần có để thực hiện đề tài.

Qua quá trình nghiên cứu tập hợp tài liệu, nhóm thực hiện đề tài đưa được ra mô hình hiện trạng hệ thống mạng của Bộ Công Thương:

Hình 9: Mô hình mạng Bộ Công Thương trước khi triển khai:



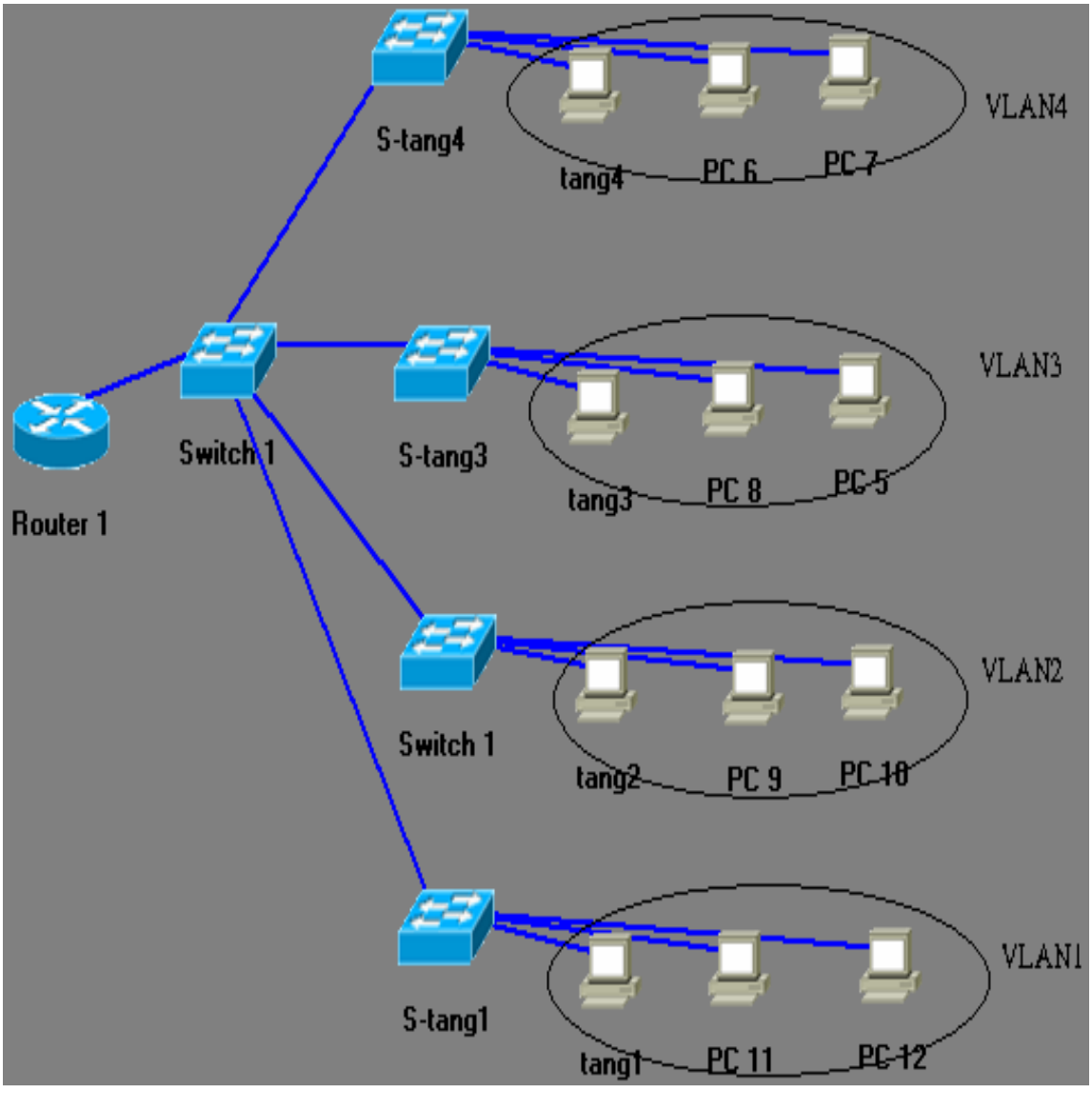
Qua nghiên cứu thực tiễn dựa trên mô hình thực tê, nhóm thực hiện đề tài đã đề xuất hai giải pháp triển khai hệ thống mạng Lan ảo cho Bộ Công Thương như sau:

- Giải pháp 1:Chia mỗi tầng của Bộ là một mạng VLan riêng
- Giải pháp 2:Chia Vlan theo chức năng của mỗi Phòng

- Giải pháp 1:

Với giải pháp 1 thì đó là chia theo địa lý,theo số tầng. Ở giải pháp này thì sẽ tốn ít dây hơn,dễ triển khai hơn,nhưng chỉ có một Vlan tồn tại trong một tầng .

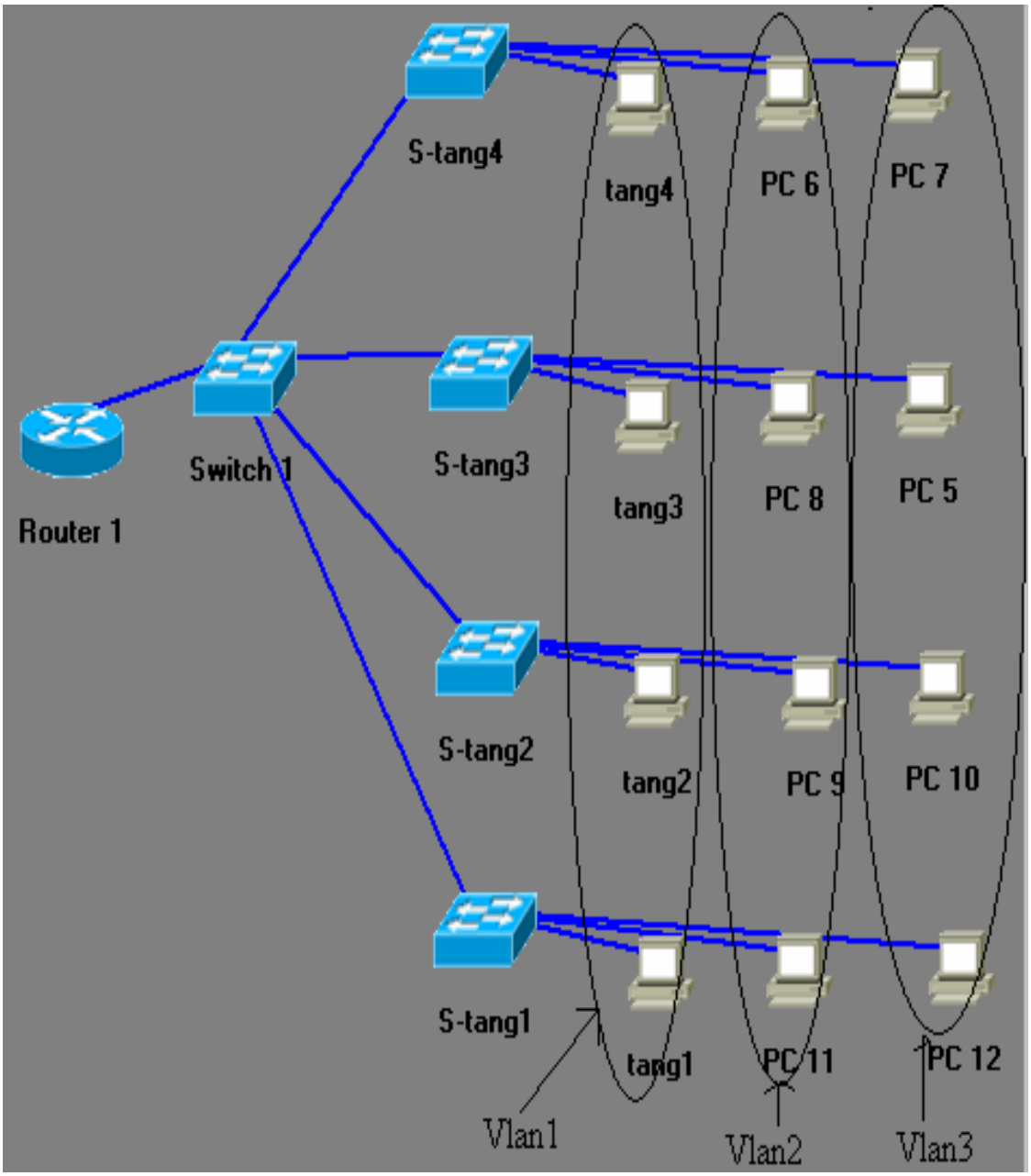
Hình 10: Giải pháp 1 Vlan



-Giải pháp 2:

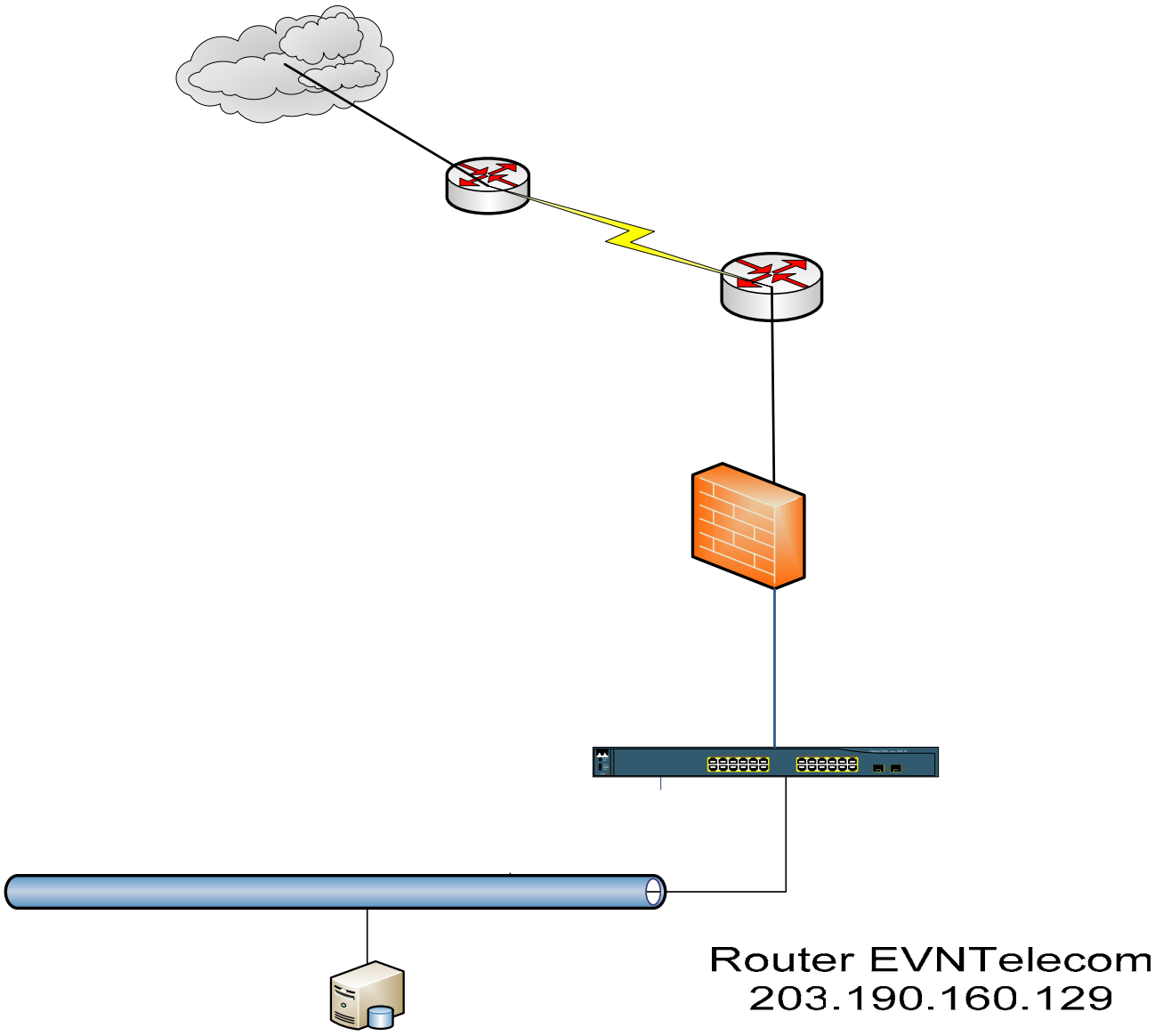
Với giải pháp 2 thì việc đi dây sẽ phức tạp hơn(tốn dây hơn) nhưng nó sẽ cho phép ta có sự linh động trong việc chia VLAN.Có nghĩa là có thể có nhiều hơn 1 Vlan trên một tầng.

Hình 12: Giải pháp 2 Vlan



- Kết luận: Nhóm thực hiện đề tài chọn giải pháp 1 là giải pháp phù hợp với thiết kế hệ thống hiện tại của Bộ Công Thương. Tuy nhiên, với số lượng các thiết bị hiện tại của Bộ Công Thương, việc chia Vlan cho từng tầng chưa thể thực hiện được. Do đó, nhóm thực hiện đề tài sẽ thực hiện chia Vlan cho các trụ sở của Bộ Công Thương và cho các Cục, Viện nối vào.

- Giải pháp triển khai mạng riêng ảo cho Bộ Công Thương:



Hình 13: Mô hình mạng riêng ảo cho Bộ Công Thương

Giải pháp hệ thống mạng truy nhập từ xa của Bộ Công Thương dựa trên các thiết bị:

- Đường truyền internet Leaseline của EVN.
- Máy chủ Moitsrv14 cài ISA 2006 cung cấp dịch vụ VPN.
- Máy chủ Lcssrv cài RRAS chứng thực người dùng.

Giải pháp mạng truy nhập từ xa sử dụng mô hình mạng Clien to Site, khi đó các truy nhập từ internet sẽ được hiểu là Client và mạng Bộ Công Thương sẽ là Site. Đồng thời, sử dụng phần mềm VPN client của Microsoft

2.2 Thiết bị, dụng cụ sử dụng cho nghiên cứu:

Sơ đồ nguyên lý hệ thống mạng:

Hệ thống mạng của Bộ Công Thương sau khi triển khai 2 dịch vụ Mạng Lan ảo và mạng truy nhập từ xa có những thay đổi sau:

- Hệ thống mạng Lan ảo được thiết kế trên cơ sở 2 thiết bị Switch 3560 của Cisco, qua đó cung cấp được các Vlan cho hệ thống nội bộ của Bộ Công Thương và các Vlan cho hệ thống các đơn vị Cục thuộc Bộ Công Thương nối vào.
- Hệ thống mạng truy cập từ xa được thiết kế triển khai trên các thiết bị máy chủ và hệ thống internet Lease line của EVN, cùng với địa chỉ IP tĩnh, người dùng thuộc cơ quan Bộ Công Thương có thể kết nối truy nhập vào mạng Lan của Bộ thông qua internet.

Qua đó, đã đáp ứng được các nhu cầu:

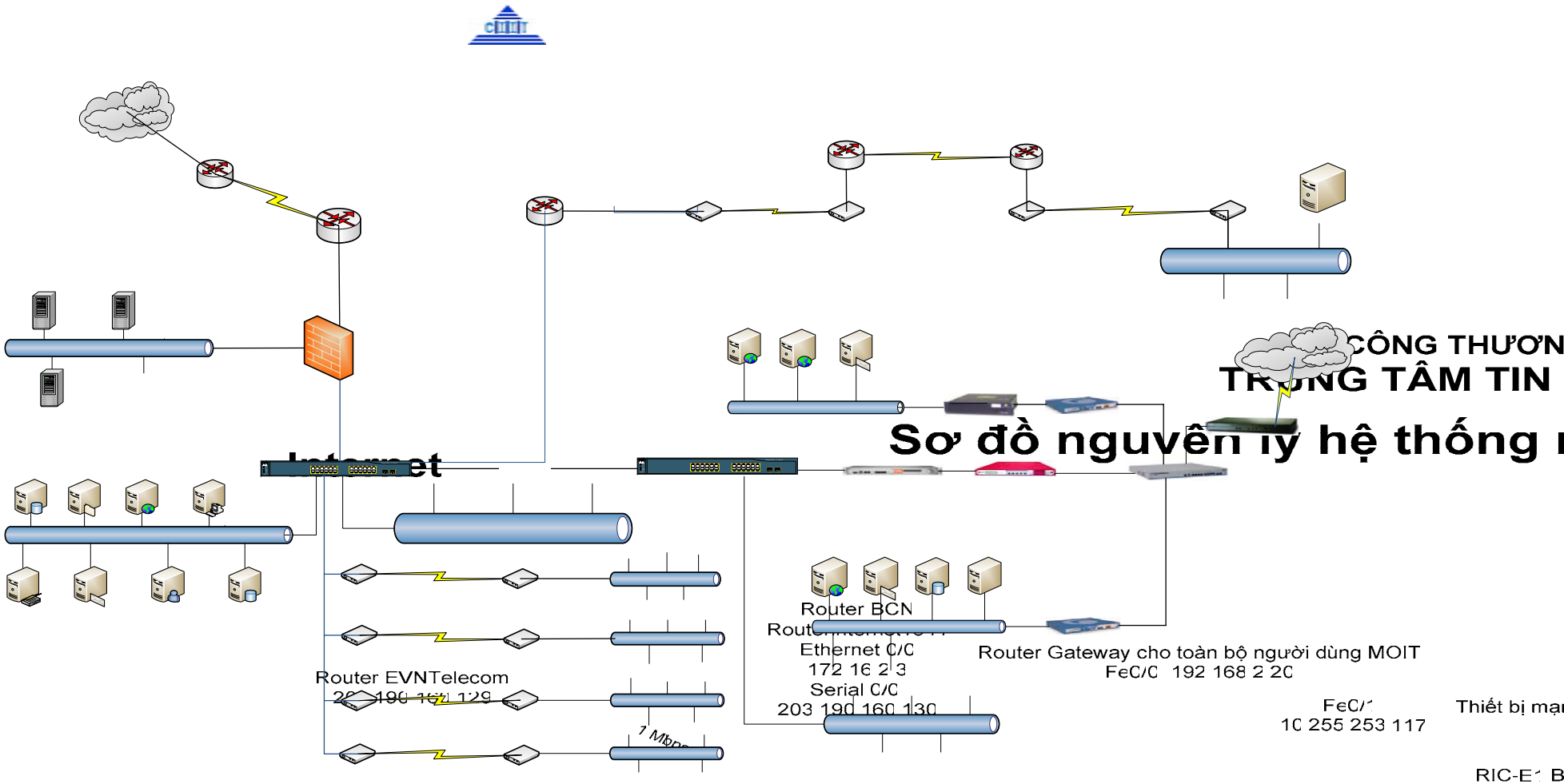
1. Cung cấp dịch vụ truy cập từ xa từ internet.
2. Đảm bảo an toàn thông tin, chứng thực người dùng.
3. Về mạng Lan ảo:

- Tiết kiệm được các chi phí về mua thiết bị.

- Tập trung hóa được quản lý.
- Linh hoạt trong công việc chuyển đổi mô hình hệ thống.
- Tạo nên hệ thống chuẩn, có hệ thống chính, hệ thống backup sao lưu dữ liệu.

Với việc sử dụng các thiết bị có sẵn, cùng với sự tìm hiểu đánh giá hệ thống của nhóm thực hiện đề tài. Hệ thống đã mang lại những lợi ích đáng kể, giúp giảm chi phí về con người và thiết bị. Hệ thống mang Lan ảo sử dụng công nghệ Vlan của Cisco, hệ thống mạng truy cập từ xa dựa trên các đặc tính có sẵn của hệ điều hành Microsoft. Dựa trên hệ thống VPN của phần mềm ISA 2006.

Mô hình sau khi triển khai hệ thống:


CÔNG THƯƠN
TRUNG TÂM TIN
Sơ đồ nguyên lý hệ thống
Internet
Router BCN
Ethernet C/C
172 16 2 3
Serial C/C
203 190 160 130
Router Gateway cho toàn bộ người dùng MOIT
FeC/C 192 168 2 20
Router EVNTelecom
Thiết bị mạ
10 255 253 117
RIC-E
192 168 2 20
172 16 2 3
MOITFRONTEND
203 190 160 34
MOISRV10
203 160 190 35
172 16 2 1

Hiện trạng thiết bị mạng có thể triển khai mạng Lan ảo của Bộ Công Thương:

Như phân tích ở chương 3 mục 3.1, hệ thống hiện tại của Bộ Công Thương có thể tận dụng được các thiết bị có thể triển khai được hệ thống mạng Lan ảo là:

- Hai thiết bị Switch 3560 của Cisco có khả năng chia Vlan.

- Các switch nối các tầng.

- Các module quang, điện.

Hiện trạng thiết bị có thể triển khai truy nhập từ xa qua Internet của Bộ Công Thương:

Như phân tích ở chương 3, mục 3.1, hệ thống hiện tại của Bộ Công Thương có thể tận dụng các thiết bị có thể triển khai được hệ thống mạng truy nhập từ xa từ internet:

- Máy chủ MOITISA14.

- Phần mềm ISA 2006: được cài trên máy chủ Moitisa14.

- Máy chủ MOITLCS: được cài phần mềm RRAS của Windows 2003.

- Thiết bị định tuyến Router 1841.

- Hệ thống internet Lease line của EVN với dải IP tĩnh.

Kết luận đánh giá hiện trạng:

Qua quá trình phân tích đánh giá hiện trạng hệ thống mạng của Bộ Công Thương. Nhóm thực hiện đề tài đã tập hợp ra được các thiết bị có thể triển khai được hai hệ thống mạng Lan ảo và mạng truy nhập từ xa. Trên cơ sở thực tiễn, nhóm thực hiện đề tài đánh giá rất cao những ứng dụng hệ thống hiện tại của Bộ Công Thương mang lại cho người sử dụng. Tuy vậy, nhóm thực hiện đề tài có những đánh giá khách quan sau:

Hệ thống mạng trước khi triển khai thực hiện đề tài:

1. Không đáp ứng các nhu cầu kết nối trong nội bộ và các đơn vị ngoài Bộ Công Thương.
2. Không linh hoạt trong các phương án chuyển đổi hệ thống.
3. Hệ thống không cung cấp dịch vụ truy nhập từ xa cho người dùng.
4. Hệ thống sử dụng các thiết bị định tuyến là máy tính, không đáp ứng được nhu cầu chuyên dụng.

Hệ thống mạng sau khi triển khai thực hiện đề tài:

1. Hệ thống mạng Lan ảo sau khi triển khai đã đáp ứng được nhu cầu kết nối cho hệ thống mạng nội bộ của Bộ Công Thương và các đơn vị ngoài Bộ.
2. Hệ thống mạng Lan ảo sử dụng các thiết bị ddinhh tuyến chuyên dụng, mang lại hiệu quả cao .

Hệ thống mạng riêng ảo cung cấp truy cập từ xa cho người dùng cơ quan Bộ

Kết quả thực nghiệm:

Qua quá trình khảo sát, thu thập tài liệu. Nhóm thực hiện đề thực hiện đánh giá phạm vi ứng dụng và triển khai. Đánh giá tính khả thi và hiệu quả mang lại sau khi triển khai hệ thống. Nhóm thực hiện đề tài thảo luận và đưa ra đánh giá kết luận sau:

Kết quả thực hiện của đề tài

- ❖ Báo cáo tìm hiểu công nghệ Lan ảo (VLAN)
- ❖ Triển khai 5 mạng Lan ảo tại cơ quan Bộ Công Thương và 4 mạng Lan ảo cho các đơn vị kết nối đến Bộ
- ❖ Triển khai cung cấp dịch vụ kết nối mạng nôi bộ từ xa qua Internet.

KẾT LUẬN VÀ KIẾN NGHỊ

Qua quá trình nghiên cứu và triển khai đề tài ***Nghiên cứu các giải pháp tăng cường chất lượng dịch vụ mạng sử dụng mạng Lan ảo và phát triển dịch vụ truy nhập từ xa vào mạng nội bộ thông qua internet*** đã đáp ứng được hết các yêu cầu đặt ra góp phần cung cấp các dịch vụ tiện ích tốt nhất cho người dùng và đảm bảo hệ thống mạng của Bộ Công Thương được vận hành trơn tru, đồng thời nó mở ra hướng phát triển hệ thống của Bộ Công Thương .

Qua báo cáo đề tài này, nhóm nghiên cứu đã đưa ra được cái nhìn tổng quát, những đánh giá về hệ thống để tham mưu cho Bộ Công Thương những giải pháp và kiến trúc cho hệ thống mạng và các dịch vụ tiện ích.

Nhóm thực hiện đề tài cũng xin tiếp tục nghiên cứu hai công nghệ mạng Lan ảo và mạng riêng ảo và có kiến nghị sau:

1. Mở rộng phạm vi sử dụng công nghệ mạng riêng ảo phục vụ kết nối tới các đơn vị tỉnh thành.

2. Triển khai hệ thống mạng Lan ảo áp dụng đến từng tầng, từng Vụ trong Bộ Công Thương và các đơn vị kết nối tới Bộ Công Thương

3. Triển khai hệ thống bảo mật cho hai công nghệ mạng Lan ảo và công nghệ mạng riêng ảo.

Cuối cùng, nhóm thực nhiện đề tài xin chân thành cảm ơn quan tâm của Lãnh đạo Vụ KHCN, của Lãnh đạo Trung tâm Tin học - Cục Thương mại Điện tử và Công nghệ Thông tin đã hết sức động viên và cho ý kiến chỉ đạo kịp thời để kết quả đề tài chính là mạng và dịch vụ truy cập từ xa qua internet đi vào hoạt động tối ưu.

TÀI LIỆU THAM KHẢO

1. Network Perimeter Security Building Defense In Depth 2004
2. Building.and.Implementing.a.Security.Certification.and.Accreditation.Program.Official
3. Wireless.Security.Handbook
4. Bảo mật ứng dụng web.
5. Self.Defending.Networks.The.Next.Generation.of.Network.Security.
6. Computer Network & Internet Security.
7. Ethernet Networks. Design, Implementation, Operation, Management
8. Halting The Hacker A Practical Guide To Computer Security
9. Mastering Web Services Security - 2003 – Wiley
10. Microsoft.Internet.Security.and.Acceleration.ISA.Server.2004
11. Publishing.Firewall.Policies.and.VPN.Configurations

.

PHỤ LỤC

Phụ lục 1: Cài đặt triển khai VLan:

BƯỚC 1:Tạo Vlan và cấu hình tên cho Vlan:

- Switch 1900:

>**en**

#**config t**

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

(config)#**hostname 1900**

1900(config)#**vlan 2 name sales**

1900(config)#**vlan 3 name marketing**

1900(config)#**vlan 4 name mis**

1900(config#exit

Vì Mặc định thì toàn bộ các Port sẽ thuộc Vlan 1:

1900#**sh vlan**

VLAN Name Status Ports

---

1 default Enabled 1-12, AUI, A, B

2 sales Enabled

3 marketing Enabled

4 mis Enabled

1002 fddi-default Suspended

1003 token-ring-defau Suspended

1004 fddinet-default Suspended

1005 trnet-default Suspended

- **Switch 2950:**

Switch>

Switch>**en**

Switch#**config t**

Switch(config)#**vlan 2**

Switch(config-vlan)#

Switch(config-vlan)#**vlan 3**

Switch(config-vlan)#**name Sales**

Switch(config-vlan)#**vlan 4**

Switch(config-vlan)#**name Finance**

Switch(config-vlan)#**^Z**

Switch#

Switch#sh vlan brief

VLAN Name Status Ports

---- -------------------- --------- -------------------------------

1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
			Fa0/7, Fa0/8, Fa0/9, Fa0/10
			Fa0/11, Fa0/12
2 VLAN	0002	active	
3	Sales	active	
4	Finance	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

BƯỚC 2: Gán Cổng cho Vlan:

- **Gán từng cổng :**

Switch(config-if)#**int f0/2**

Switch(config-if)#**switchport access vlan 2**

Switch(config-if)#**int f0/3**

Switch(config-if)#**switchport access vlan 3**

Switch(config-if)#**int f0/4**

Switch(config-if)#**switchport access vlan 4**

Switch(config-if)#

Switch#**sh vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	Fa0/2
3	Sales	active	Fa0/3
4	Finance	active	Fa0/4

BƯỚC 3: Gán Cổng trunk cho Switch:

Switch#**config t**

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

Switch(config)#**int f0/12**

Switch(config-if)#**switchport mode trunk**

Switch(config-if)#^Z

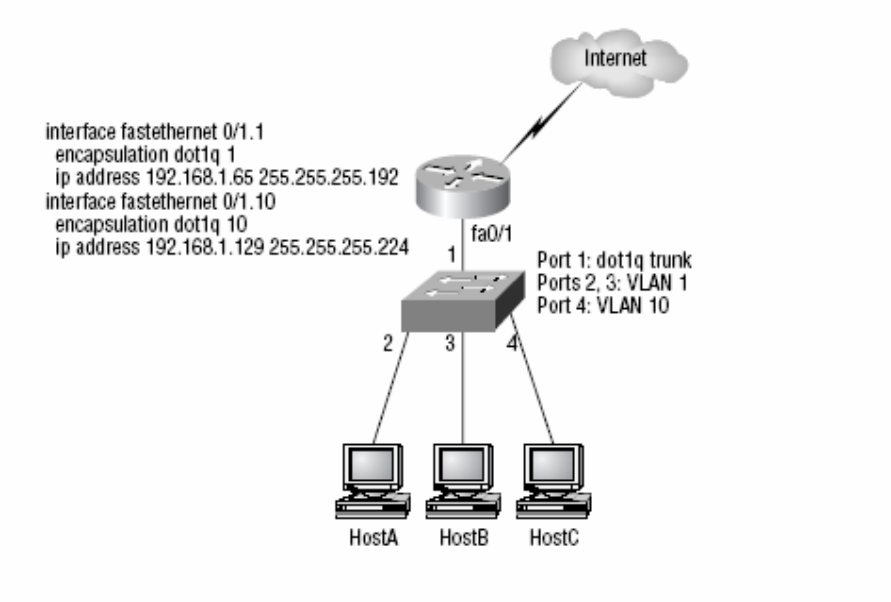
Encapsulation cho Cổng trunk:

Switch(config-if)#**switchport trunk encapsulation ?**

BƯỚC 4: CẤU HÌNH CHO ROUTER:

2600(config)#**int f0/0.1**

2600(config-subif)#**encapsulation dot1q** *vlan#*



B1:Các máy host phải cấu hình Defaul gateway tới địa chỉ VLAN mà nó thuộc vào:

HostA: 192.168.1.66, 255.255.255.192, default gateway 192.168.1.65

HostB: 192.168.1.67, 255.255.255.192, default gateway 192.168.1.65

HostC: 192.168.1.130, 255.255.255.224, default gateway 192.168.1.129

B2:Cổng F0/1 của Switch phải là cổng Trunk:

2950#**config t**

2950(config)#**interface fa0/1**

2950(config-if)#**switchport mode trunk**

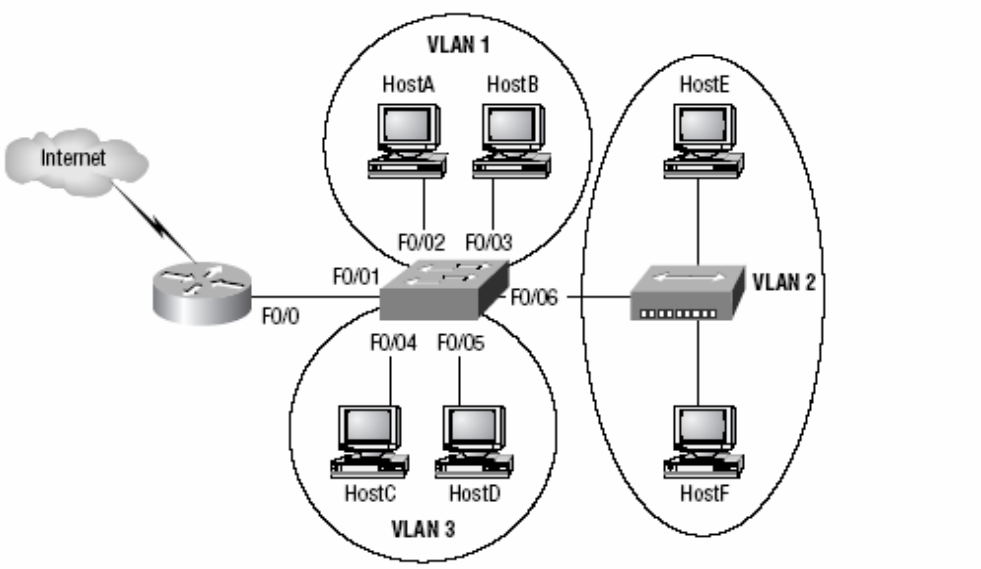
Với Switch 3550:

3550#**config t**

3550(config)#**interface fa0/1**

3550(config-if)#**switchport mode trunk**

3550(config-if)#**switchport trunk encapsulation dot1q**



2950#**config t**

2950(config)#**int f0/1**

2950(config-if)#**switchport mode trunk**

2950(config-if)#**int f0/2**

2950(config-if)#**switchport access vlan 1**

2950(config-if)#**int f0/3**

2950(config-if)#**switchport access vlan 1**

2950(config-if)#**int f0/4**

2950(config-if)#**switchport access vlan 3**

2950(config-if)#**int f0/5**

2950(config-if)#**switchport access vlan 3**

2950(config-if)#**int f0/6**

2950(config-if)#**switchport access vlan 2**

B3:Trước khi đó: ta phải gán địa chỉ Ip cho các Vlan:

2950#**config t**

2950(config)#**int vlan 1**

2950(config-if)#**ip address 172.16.10.2 255.255.255.128**

2950(config-if)#**no shutdown**

VLAN 1: 192.168.10.16/28

VLAN 2: 192.168.10.32/28

VLAN 3: 192.168.10.48/28

B4:Cấu hình cho Router:

Router#**config t**

Router(config)#**int f0/0**

Router(config-if)#**no ip address**

Router(config-if)#**no shutdown**

Router(config-if)#**int f0/0.1**

Router(config-subif)#**encapsulation dot1q 1**

Router(config-subif)#**ip address 192.168.10.17 255.255.255.240**

Router(config-subif)#**int f0/0.2**

Router(config-subif)#**encapsulation dot1q 2**

Router(config-subif)#**ip address 192.168.10.33 255.255.255.240**

Router(config-subif)#**int f0/0.3**

Router(config-subif)#**encapsulation dot1q 3**

Router(config-subif)#**ip address 192.168.10.49 255.255.255.240**

B5:Cấu hình VTP:

1900(config)#**vtp ?**

client VTP client

domain Set VTP domain name

password Set VTP password

pruning VTP pruning

server VTP server

transparent VTP transparent

trap VTP trap

1900(config)#**vtp server**

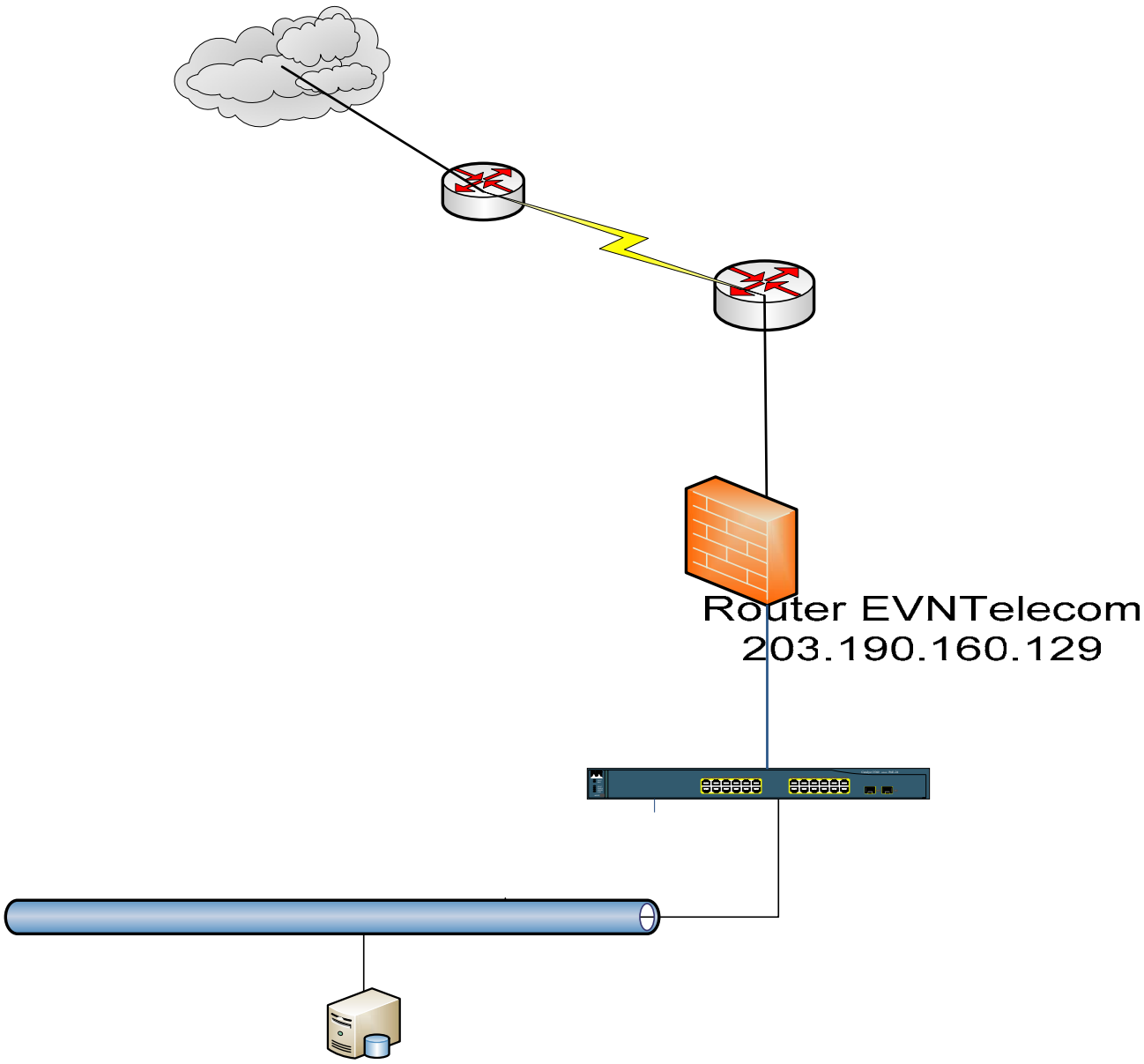
1900(config)#**vtp domain lammle**

1900(config)#**vtp password todd**

Phụ lục 2: Cài đặt triển khai Vpn:

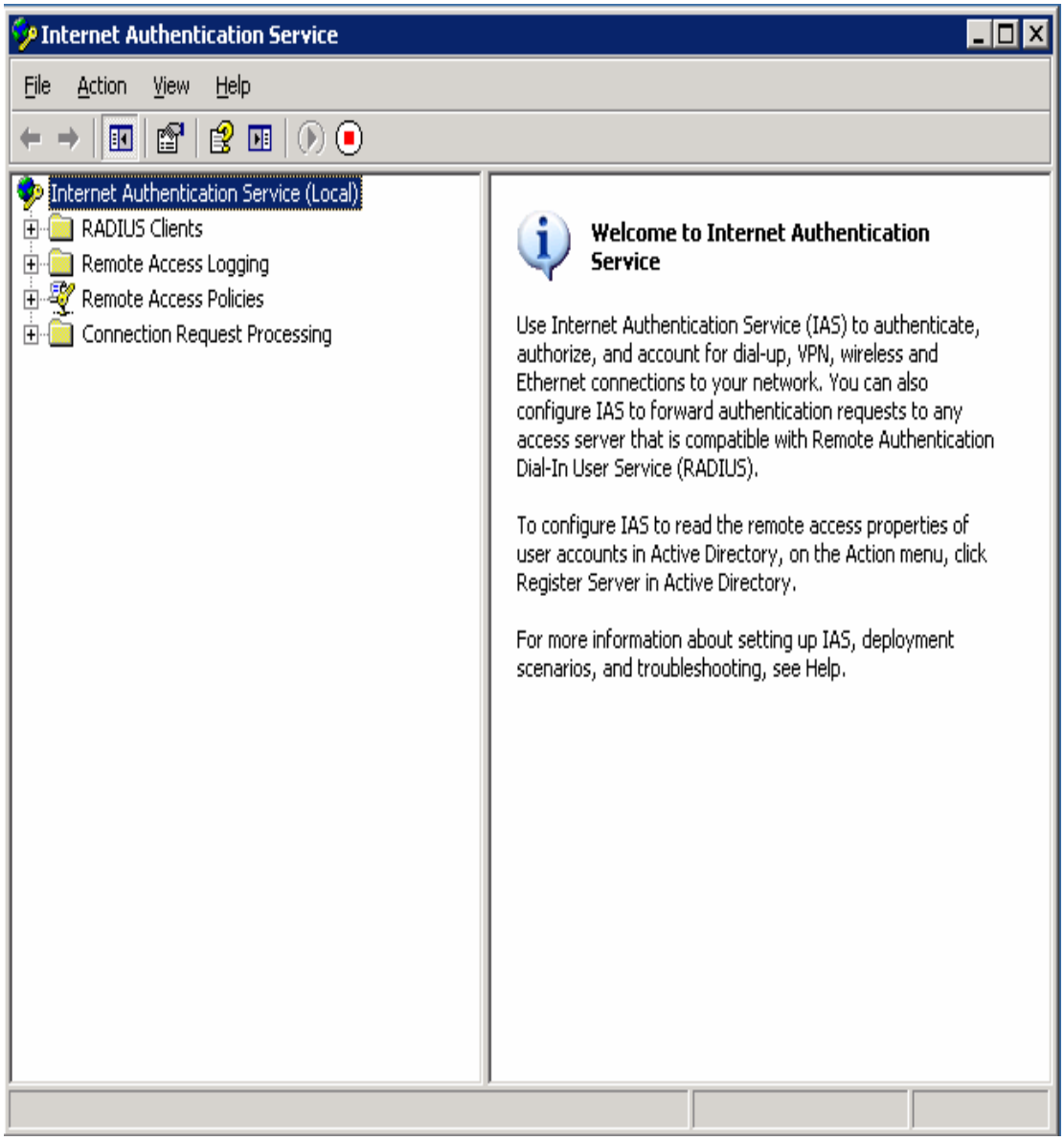
Cấu hình VPN Client to Site trên ISA 2006

Mô hình:

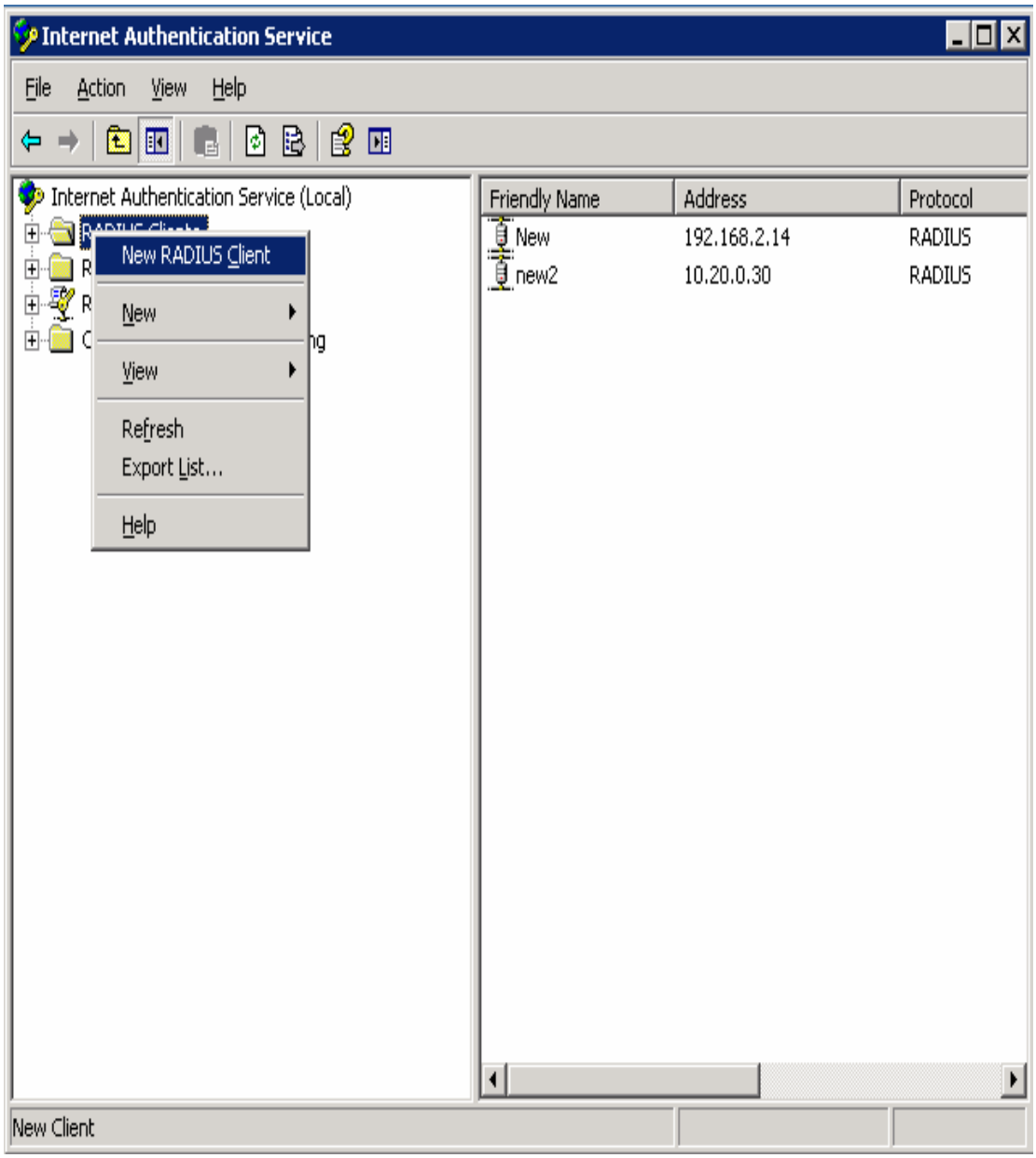


Các bước thực hiện:

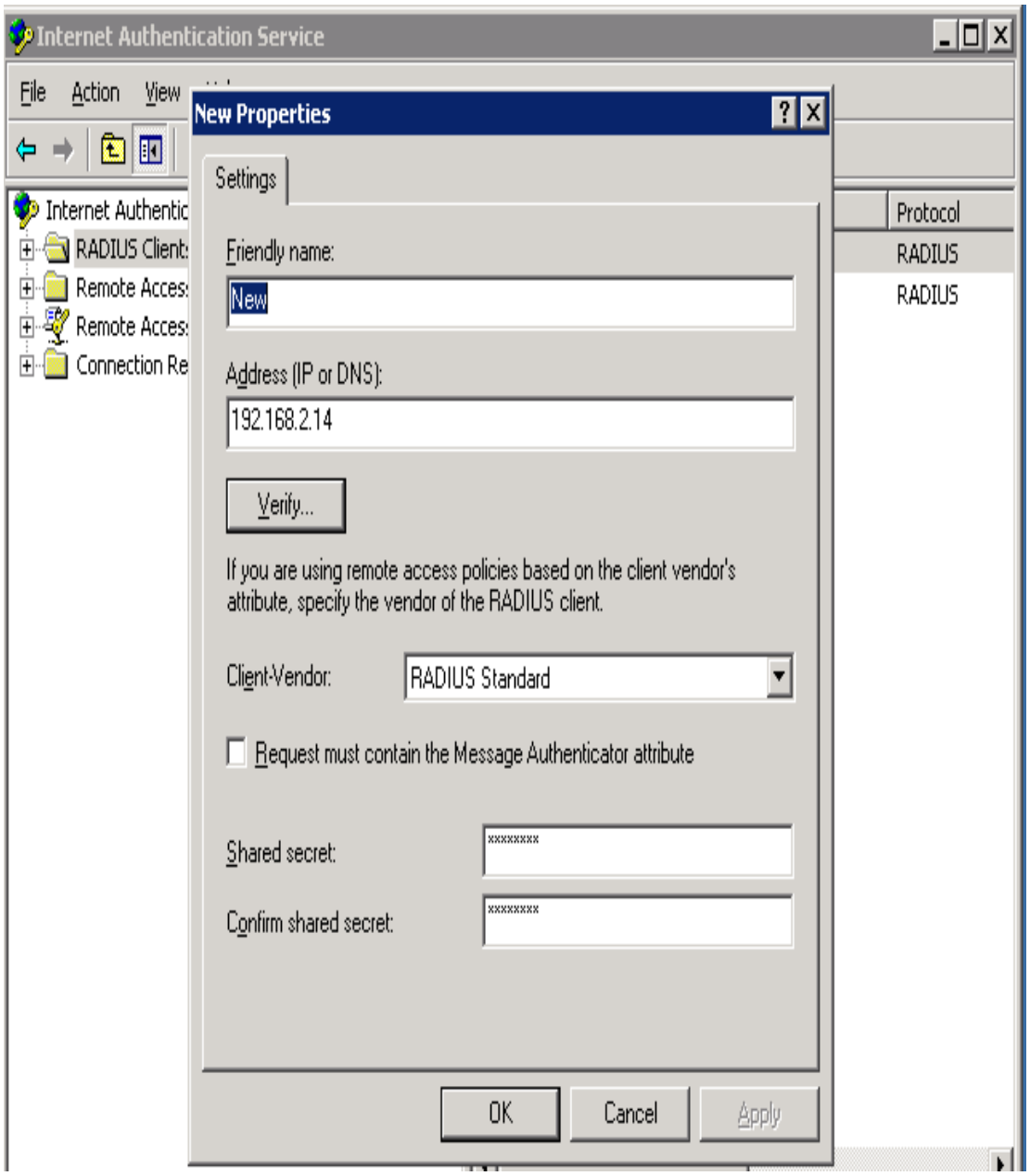
Bước 1: Cấu hình IAS


Internet Authentication Service
File Action View Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Welcome to Internet Authentication Service
Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).
To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.
For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

Tạo Radius client:

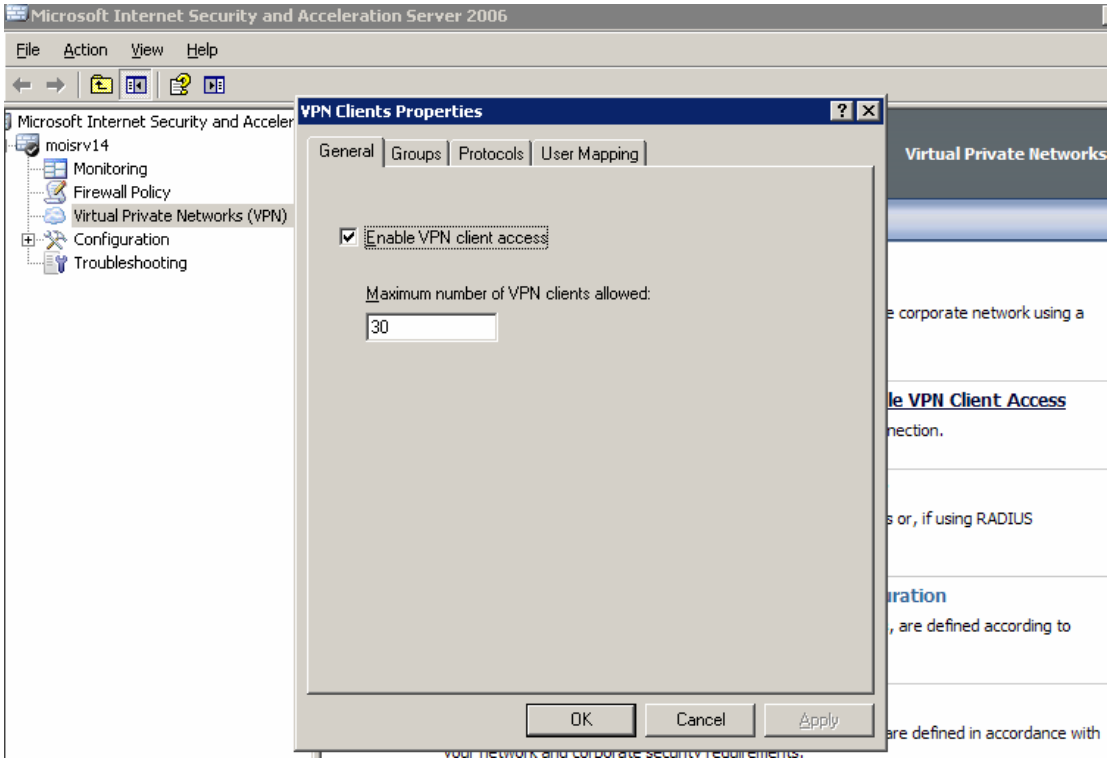


Cấu hình các thông số:

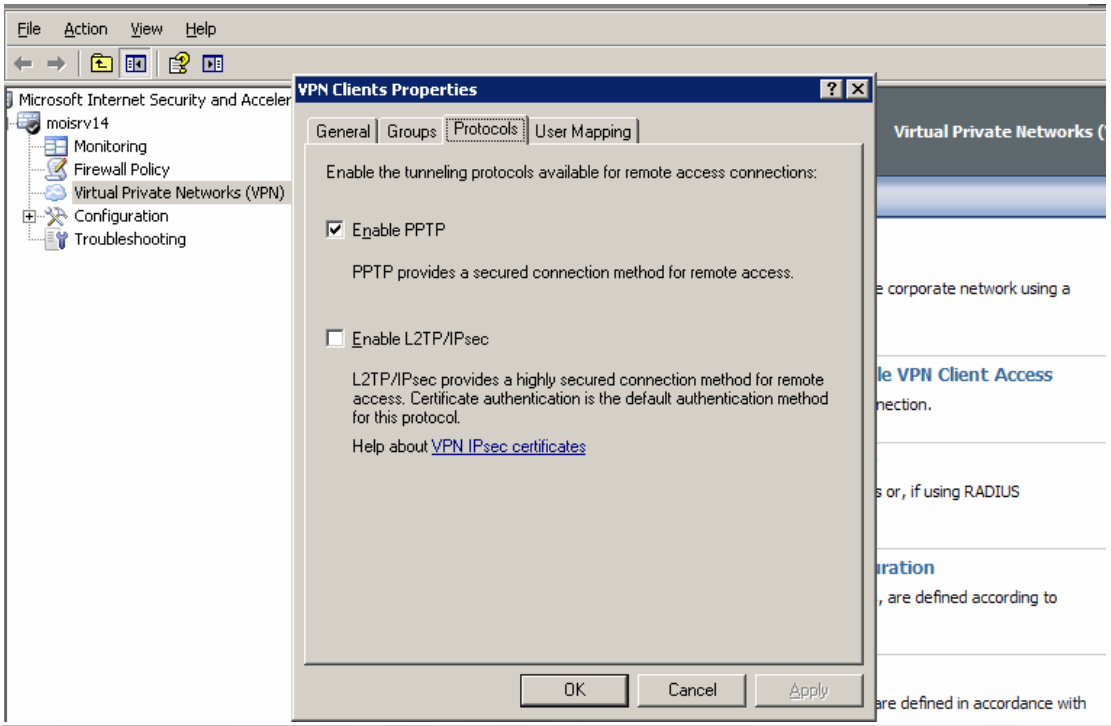


Bước 2: Cấu hình ISA:

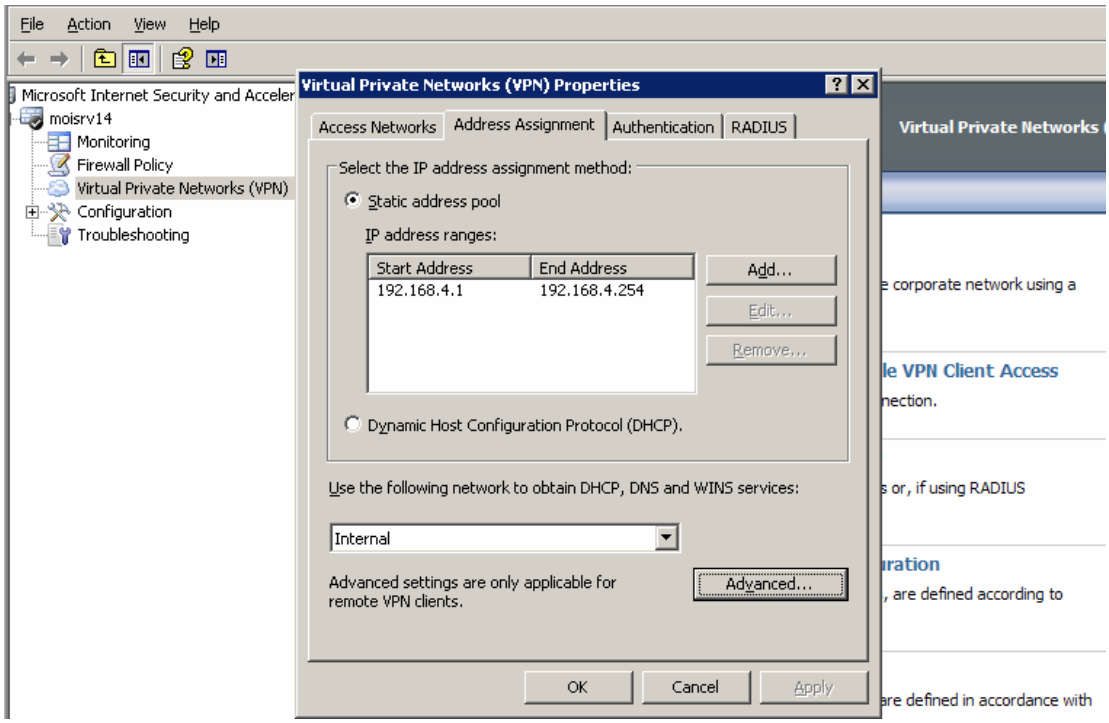
b1. Enable VPN



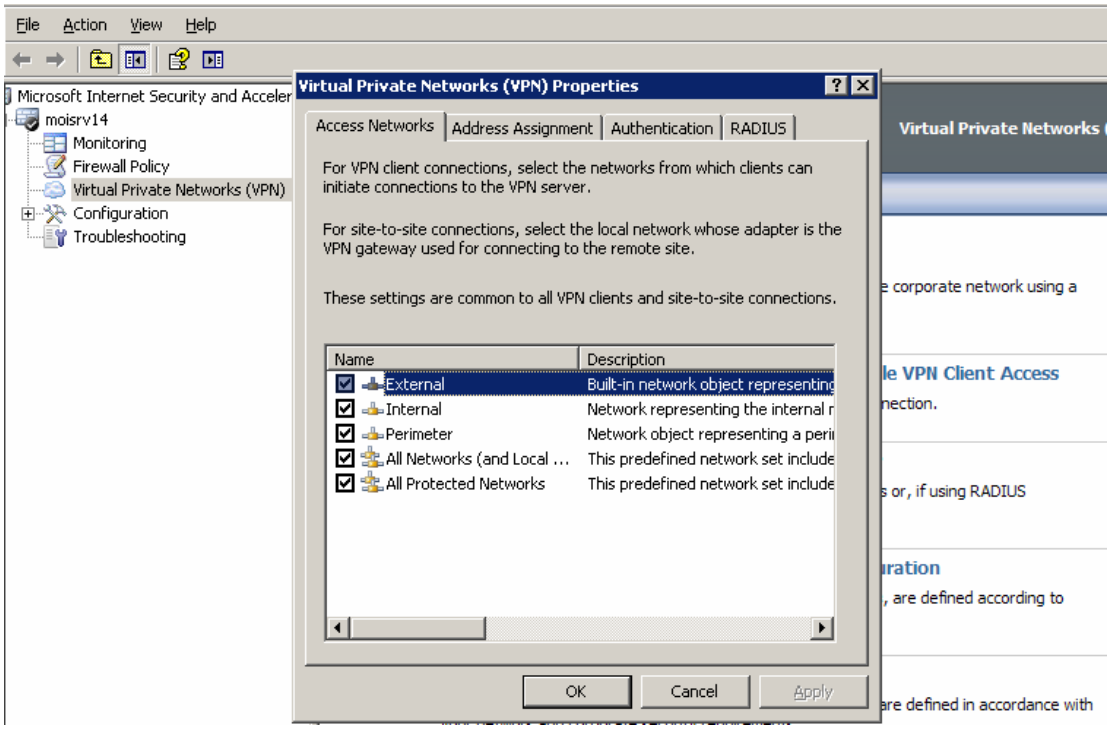
b2. Cấu hình giao thức



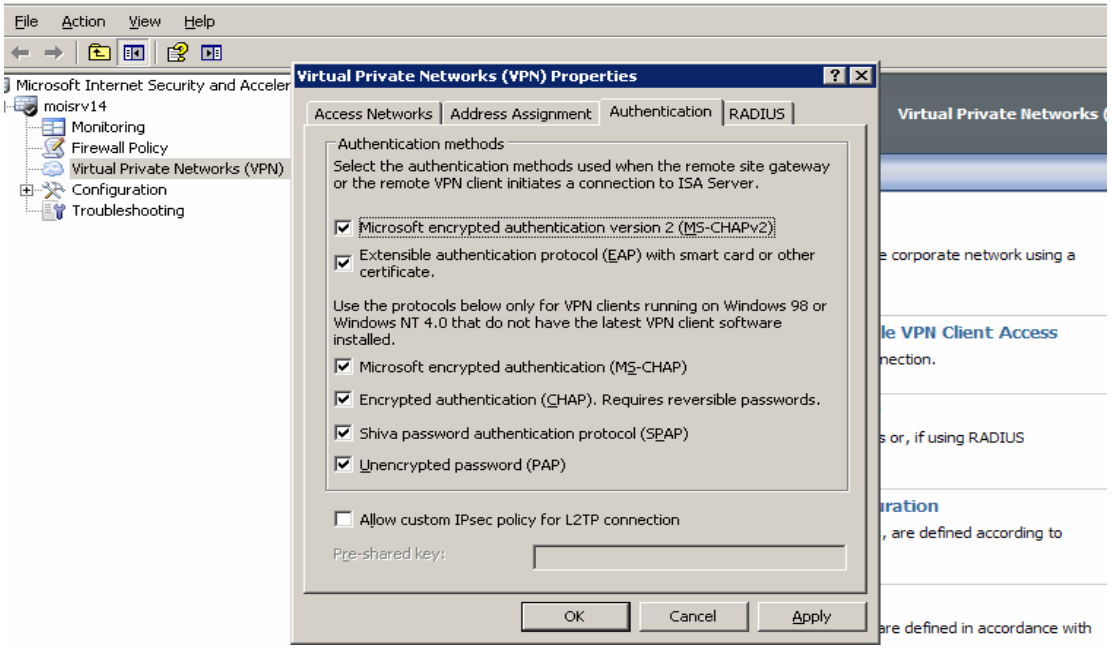
b3. Cấu hình địa chỉ cho Clients

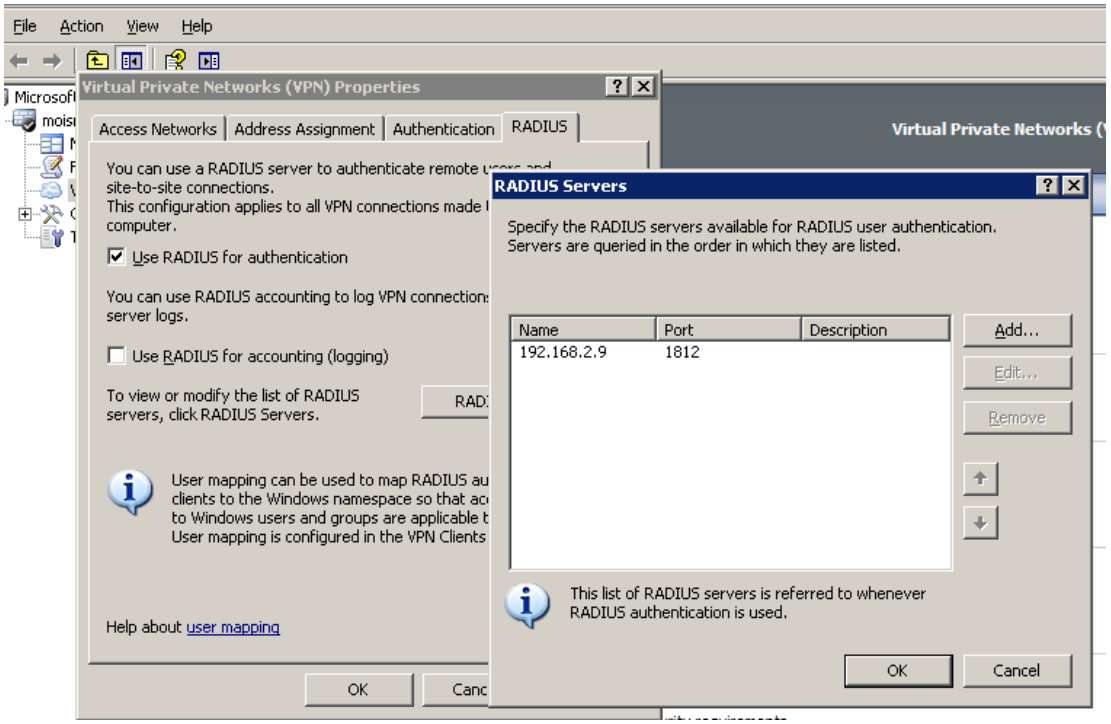


b4. Cấu hình mạng truy nhập cho Clients

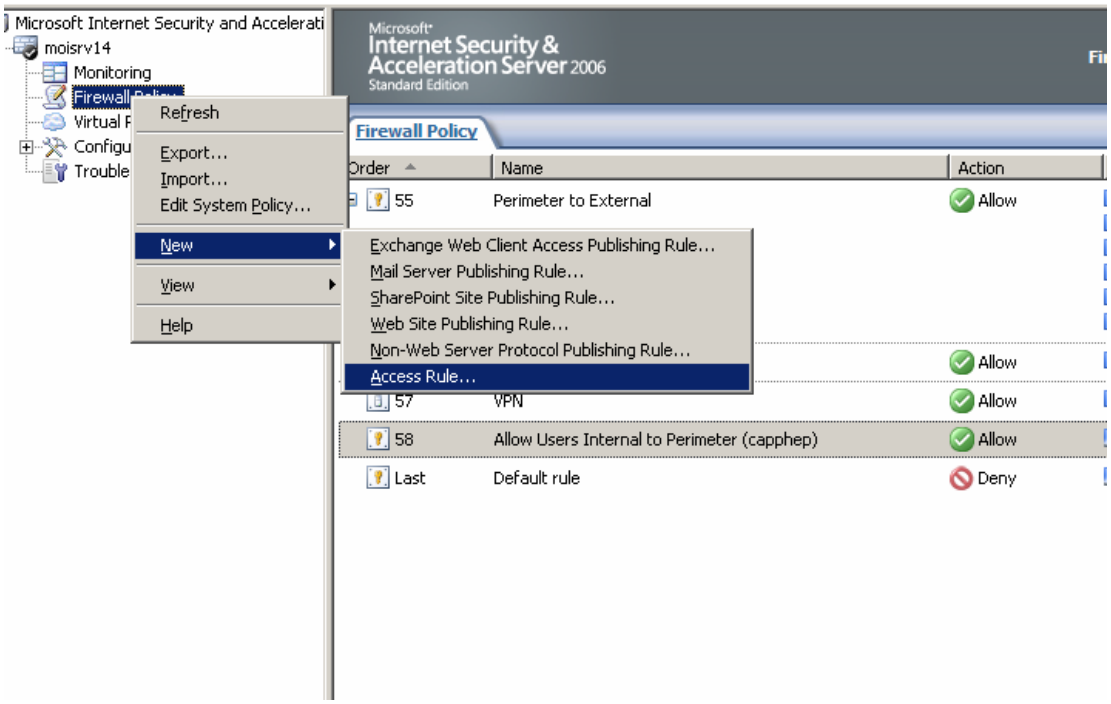


b5. Cấu hình chứng thực

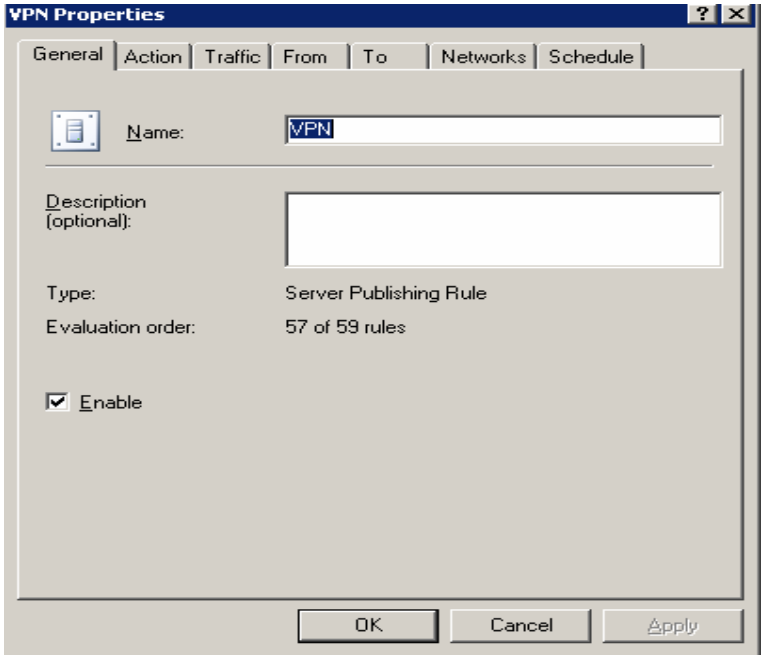


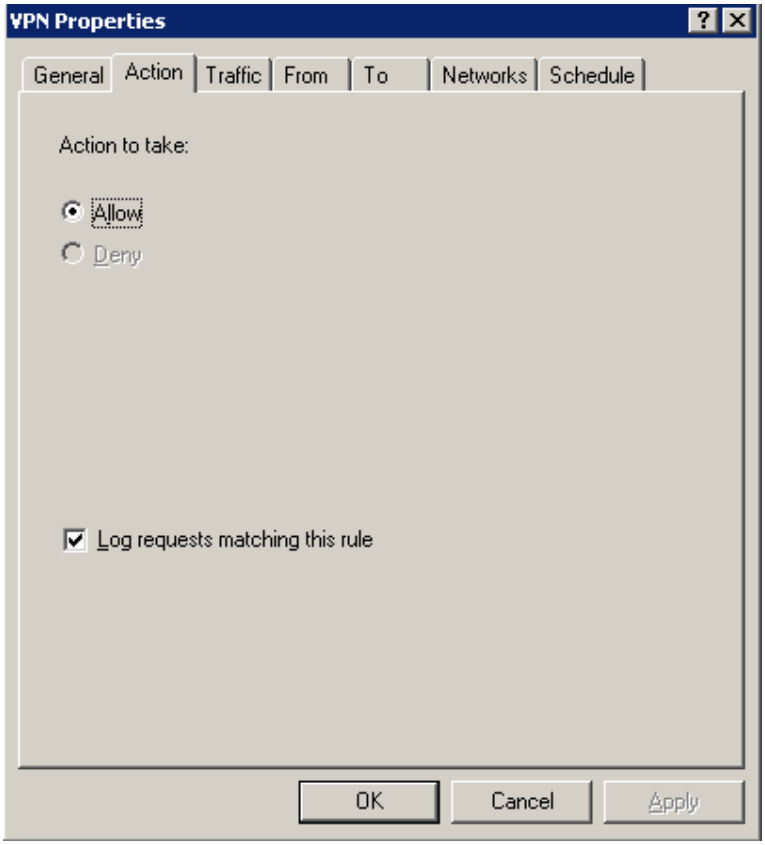


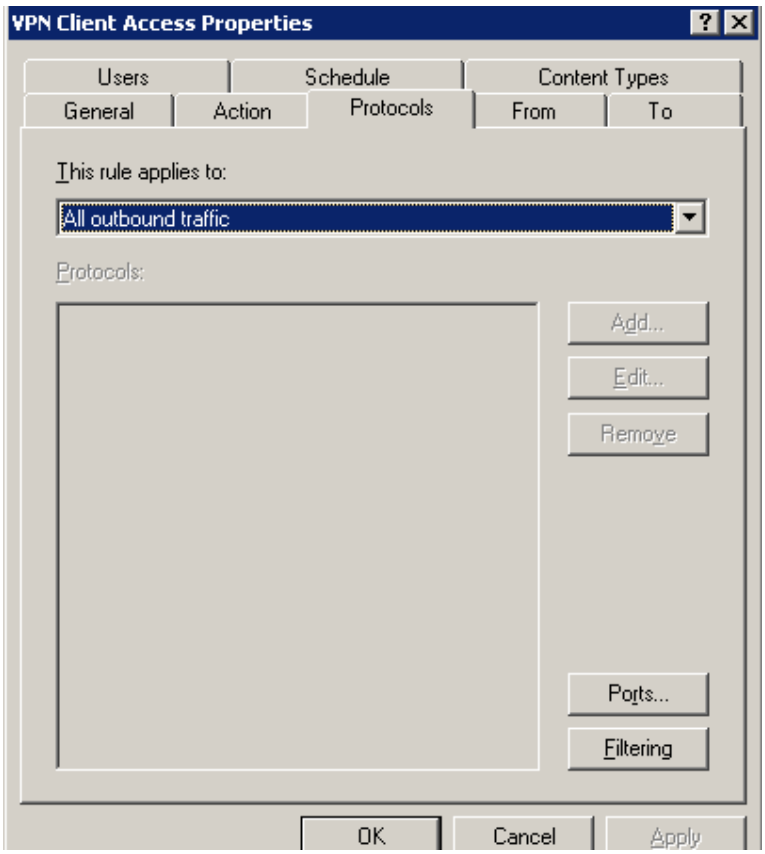
b6. Tạo access rule cho VPN

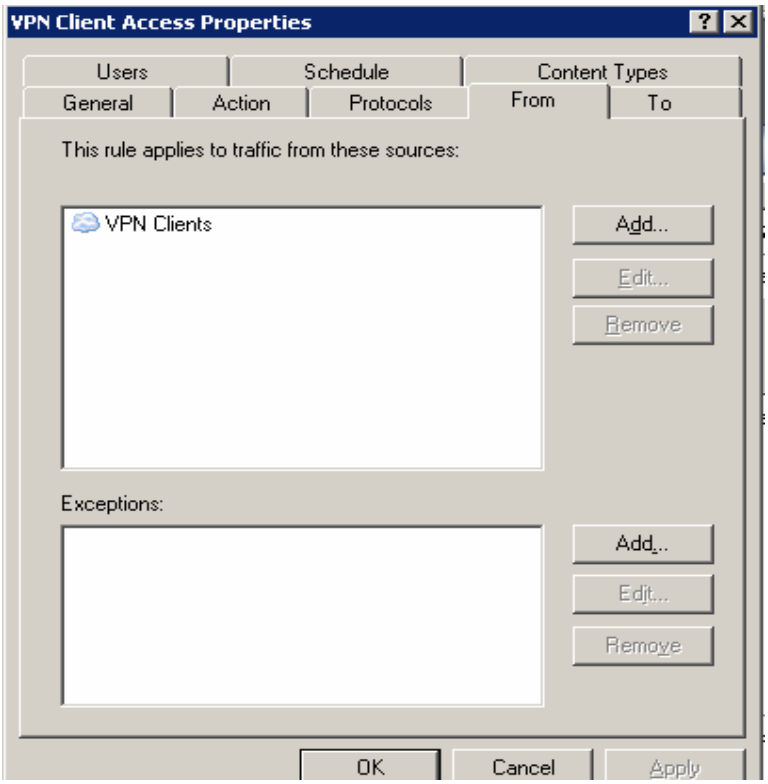


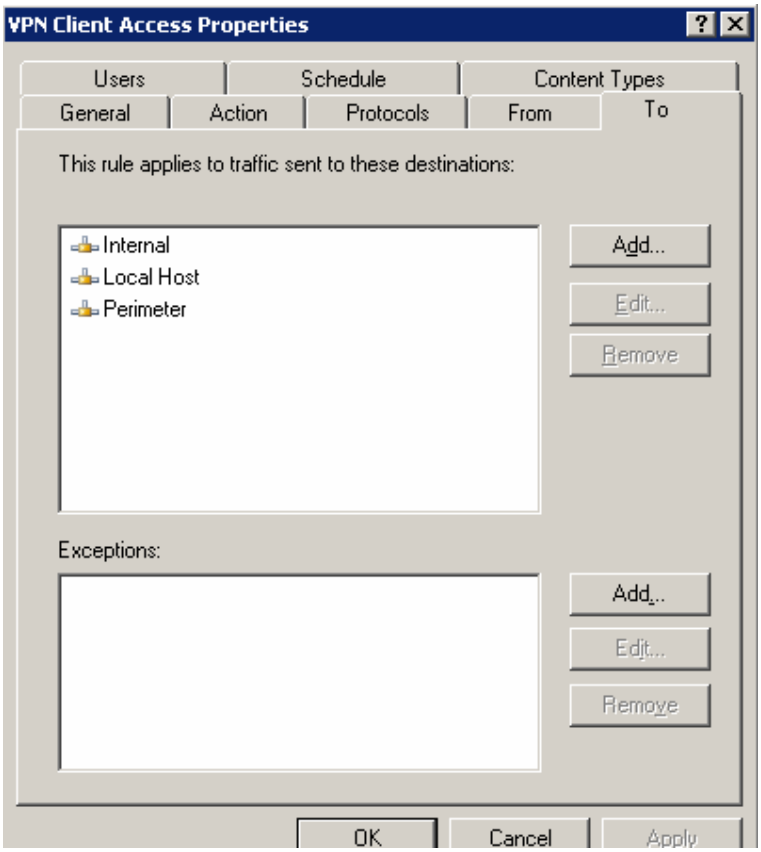
b7. Cấu hình các thông số

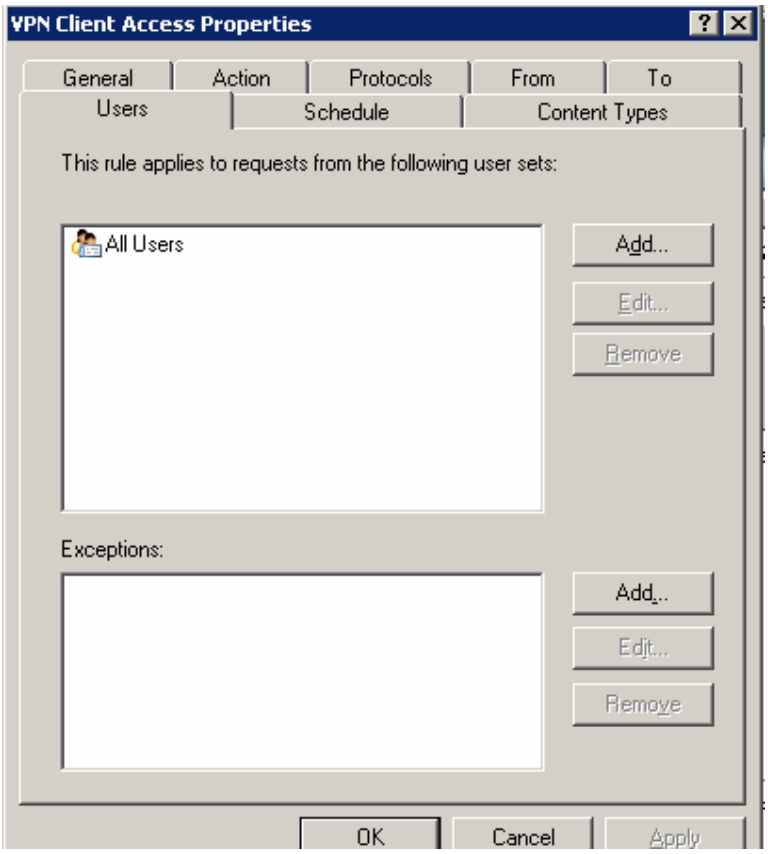



VPN Properties
General
Action
Traffic
From
To
Networks
Schedule
Action to take:
Allow
Deny
Log requests matching this rule
OK
Cancel
Apply


VPN Client Access Properties
Users
Schedule
Content Types
General
Action
Protocols
From
To
This rule applies to:
All outbound traffic
Protocols:
Add...
Edit...
Remove
Ports...
Filtering
OK
Cancel
Apply


VPN Client Access Properties
Users
Schedule
Content Types
General
Action
Protocols
From
To
This rule applies to traffic from these sources:
VPN Clients
Add...
Edit...
Remove
Exceptions:
Add...
Edit...
Remove
OK
Cancel
Apply


VPN Client Access Properties
Users
Schedule
Content Types
General
Action
Protocols
From
To
This rule applies to traffic sent to these destinations:
Internal
Local Host
Perimeter
Add...
Edit...
Remove
Exceptions:
Add...
Edit...
Remove
OK
Cancel
Apply



Phụ lục 3: Hướng dẫn cấu hình sử dụng dịch vụ Vpn

Sau khi cấu hình xong hệ thống VPN, người dùng từ internet muốn sử dụng dịch vụ truy cập từ xa cần phải cấu hình tạo một connection. Phần này, người sử dụng phải làm thành thạo các bước.

Mạng riêng ảo - Virtual Private Networks (VPN) cho phép mở rộng phạm vi mạng nội bộ của Bộ Công Thương bằng cách sử dụng lợi thế của internet. Với việc sử dụng VPN quý vị có thể kết nối máy tính của mình với hệ thống mạng LAN của Bộ Công Thương làm cho nó trở thành một máy tính trong mạng. Khi kết nối được thông suốt, quý vị có thể sử dụng các dịch vụ trong hệ thống thông tin của Bộ Công nghiệp như: trang Thông tin Điều hành tác nghiệp, chương trình Quản lý công văn, Lịch tuần, Tra cứu văn bản pháp luật, Thư điện tử …..

Sau đây là các bước hướng dẫn thực hiện

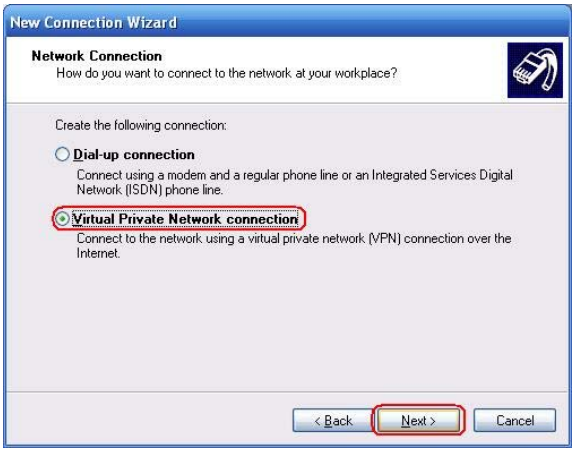
Tạo kết nối

- Kích **Start/Settíng/Control Panel → Network Connections**

Chọn **Create a new Connection Wizard**

Chọn **Next,** Hộp thoại **New Connection Type** xuất hiện

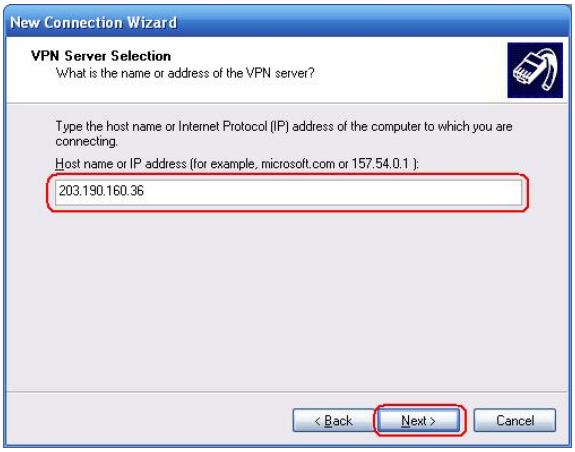
Chọn ô **Connect to the network at my workplace**. Bấm **Next,** hộp thoại **Network Connection** xuất hiện



Chọn ô **Virtual Private Network connection**. Bấm **Next**, hộp thoại **Connection Name** xuất hiện

Mục **Company Name** nhập **Moit**. Bấm **Next**, hộp thoại **Public Network** xuất hiện

Chọn **Do not dial the intial connection**. Bấm **Next**, hộp thoại **VPN Server Selection** xuất hiện



Nhập địa chỉ sau **203.190.160.36** rồi bấm **Next**, hộp thoại **Connection Availability** xuất hiện

Chọn **My use only**. Bấm **Next**, hộp thoại **VPN Server Selection** xuất hiện

Kích chọn **Add a shortcut to this connection to my desktop**. Bấm **Finish**

Kết nối VPN

Kết nối Internet thông qua dialup hoặc ADSL, sau đó chọn kết nối MOIT đã tạo trên desktop.

Trong mục **User name** nhập "**moi\account của quý vị**". VD: moi\tuanld.

Mục **Password**, quý vị nhập vào password của mình.

Sau khi kết nối thành công quý vị có thể sử dụng máy tính như trong hệ thống mạng nội bộ của Bộ Công Thương.