|  |  |
| --- | --- |
| **TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP. HCM**  **KHOA CÔNG NGHỆ THÔNG TIN**  **MÔN: MẠNG MÁY TÍNH NÂNG CAO** | |
|  | |
| BÀI BÁO ĐỒ ÁN CUỐI KÌ | |
| **Sinh viên thực hiện:**  **Phạm Quang Vinh**  **Nguyễn Hoàng Tùng** | **Mã sinh viên:**  **22162057**  **22162053** |
| **Thành Phố Thủ Đức, Ngày 26 Tháng 11 Năm 2024** | |

1. Phân tích và giải thích các nội dung
2. Thiết kế mạng theo mô hình phân lớp

Thiết kế mạng theo mô hình phân lớp là thiết kế để chia mạng thành các lớp riêng biệt, trong đó mỗi lớp có vai trò khác nhau trong mạng theo các chức năng riêng của từng lớp. Thiết kế theo mô hình phân lớp giúp quản lý mạng dễ giàng hơn, đồng thời lưu lượng dữ liệu cục bộ chỉ di chuyển trong cục bộ và chỉ đi lên các lớp cao hơn khi cần hướng tới các mạng khác.

Thông thường thiết kế mạng theo mô hình phân lớp thường bắt đầu bằng phân lớp theo thiết bị vật lý của mạng sau đó cấu hình thiết bị theo mô hình. Mô hình mạng phân lớp thường được thiết kết 3 lớp:

* Lớp mạng trung tâm (hay còn gọi là Core Layer), đây lớp xương sống cho mạng, cung cấp tốc độ truyền tải rất nhanh và đồng thời đây cũng là thường là lớp nhận và truyền tải dữ liệu lớn.
* Lớp phân bổ (Distribution Layer), là lớp nằm giữa lớp trung tâm và lớp truy cập, đây là lớp sử dụng các chính sách mạng để kiểm soát truy cập, các gói tin và lưu lượng mạng. Lớp sử dụng các thuật toán định tuyến để định tuyến các gói tin từ các máy và thường được gọi là lớp “Worksgroup”.
* Lớp truy cập (Access Layer), là lớp bao gồm thiết bị đầu cuối và các máy chủ nội bộ truy cập vào mạng, lớp này còn được gọi là lớp “Workstation”.

1. Triển khai ứng dụng trên môi trường Cloud

Triển khai ứng dụng môi trường đám mây là quá trình triển khai ứng dụng thông qua một hoặc nhiều mô hình khác nhau như: phần mềm dưới dạng dịch vụ (SaaS), nền tảng dưới dạng dịch vụ (PaaS) hay cơ sở hạ tầng dưới dạng dịch vụ (IaaS). Triển khai ứng dụng trên môi trường đám mây mang lợi ích lớn cho các cá nhân, tổ chức và doanh nghiệp trong việc cung cấp các dịch vụ và tài nguyên khác nhau, chẳng hạn như lưu trữ dữ liệu, triển khải máy chủ và cơ sở dữ liệu trực tuyến. Các dịch vụ trên môi trường đám mây cho phép doanh nghiệp sử dụng các dịch vụ, tài nguyên và không gian cần thiết để lưu trữ dữ liệu mà không cần duy trì cơ sở hạ tầng. Các công ty có thể thực hiện các phép tính khổng lồ và cung cấp các dịch vụ hàng đầu nhờ khả năng xử lý một lượng lớn dữ liệu thông qua cơ sở hạ tầng công nghệ thông tin thuộc sở hữu của bên thứ ba đưa ra.

Các loại hình ứng dụng đám mây phổ biến như:

* Phần mềm dưới dạng dịch vụ hay SaaS, phần mềm dưới dạng dịch vụ là một dịch vụ cung cấp một ứng dụng phần mềm được quản lý bởi nhà cung cấp dịch vụ đám mây cho người dùng của mình. Thông thường, các ứng dụng SaaS là các ứng dụng web hoặc di động mà người dùng có thể truy cập thông qua trình duyệt web. SaaS loại bỏ nhu cầu định cấu hình hoặc cài đặt ứng dụng trên thiết bị, cung cấp nhiều phương pháp hơn để truy cập nhóm vào phần mềm. Khắc phục lỗi, cập nhật phần mềm và các hoạt động bảo trì phần mềm chung khác được nhà cung cấp dịch vụ đám mây thực hiện cho người dùng và họ kết nối với các ứng dụng đám mây thông qua bảng điều khiển hoặc API. Việc phát triển ứng dụng đám mây phần mềm dưới dạng dịch vụ có thể được sử dụng cho: Quản lý hệ thống CRM và cơ sở dữ liệu khách hàng, cung cấp các tính năng kiểm toán và công cụ email, tự động hóa dịch vụ và đăng ký sản phẩm, quản lý tài liệu để chia sẻ và cộng tác tệp. Hiện nay, có nhiều công ty hàng đầu cung cấp SaaS như: Salesforce, Microsoft, Adobe Creative Cloud, Google Workspace, Zendesk, v.v.
* Nền tảng dưới dạng dịch vụ (PaaS), đây là dịch vụ cung cấp phần cứng và nền tảng phần mềm, được quản lý bởi nhà cung cấp dịch vụ đám mây, với người dùng xử lý các ứng dụng chạy trên nền tảng và dữ liệu mà ứng dụng dựa vào. Dịch vụ đám mây này cung cấp một nền tảng được chia sẻ để phát triển và quản lý ứng dụng mà không cần tạo và duy trì cơ sở hạ tầng thường liên quan đến quy trình. PaaS có thể được sử dụng cho cơ sở hạ tầng chạy cơ sở dữ liệu, hệ điều hành, công cụ phát triển hay phần mềm trung gian. Các nền tảng đám mây PaaS phổ biến là Windows Azure, OpenShift và Heroku.
* Cơ sở hạ tầng dưới dạng dịch vụ hay IaaS, trong IaaS, nhà cung cấp dịch vụ đám mây quản lý toàn bộ cơ sở hạ tầng kinh doanh, bao gồm mạng, lưu trữ dữ liệu, máy chủ và ảo hóa thông qua kết nối internet. Cơ sở hạ tầng có thể được quản lý bởi đám mây công cộng hoặc đám mây riêng. Người dùng có quyền truy cập thông qua API và quản lý những thứ như hệ điều hành, ứng dụng, dữ liệu và phần mềm trung gian. Nhà cung cấp dịch vụ đám mây cũng chịu trách nhiệm về việc sửa chữa, ngừng hoạt động và các sự cố phần cứng. Cùng với việc kiểm soát tài nguyên, mô hình dịch vụ đám mây IaaS cũng cung cấp các dịch vụ bổ sung cho phát triển ứng dụng dựa trên đám mây như: theo dõi, truy cập nhật ký, khôi phục và sao chép bản sao lưu. Một số ví dụ phổ biến sử dụng dịch vụ đám mây IaaS bao gồm Zoom, Slack, Vimeo và PayPal.

1. Bảo mật hệ thống công nghệ thông tin theo mô hình phân lớp (defense-in-depth)

Mô hình phân lớp (defense-in-depth) trong bảo mật hệ thống công nghệ thông tin là một biện pháp an ninh mạng, mô hình sử dụng nhiều công nghệ, sản phẩm bảo mật khác nhau để bảo vệ mạng lưới, tài nguyên của một công ty, tổ chức. Mô hình phân lớp tổ chức các giải phải bảo mật ở nhiều lớp điều khiển khác nhau như: lớp vật lý, lớp kỹ thuật và lớp quản trị. Một lớp có thể có các sản phẩm là phần mềm hay phần cứng bảo mật để để giải quyết một khía cạnh duy nhất của an toàn mạng. Các sản phẩm có thể rất giống nhau và hướng đến cùng một mục đích, nhưng trong chiến lược bảo mật nhiều lớp đều cần thiết. Sử dụng nhiều sản phẩm trong một lớp có vẻ thừa thãi nhưng sẽ tăng cường khả năng phòng thủ của doanh nghiệp trước các mối đe dọa. Ví dụ như cổng gateway và tường lửa ở lớp kỹ thuật, cả hai đều nhằm mục đích hạn chế quyền truy cập vào một số trang web và ứng dụng nhất định, nhưng vẫn được triển khai trên cùng một lớp và sau khi cả cổng gateway và tường lửa đều đồng ý cho truy cập thì sẽ có thể một sản phẩm bảo mật khác ở lớp khác kiểm tra quyền truy cập cho từng tài nguyên cụ thể.

Mô hình phân lớp ở các doanh nghiệp sẽ được triển khai theo nhiều cách khác nhau để phù hợp nhu cầu và tài nguyên của doanh nghiệp. Tuy vậy, thông thường mô hình phần lớp có các phần mềm bảo mật theo từng loại sau:

* Loại điều khiển lớp vật lý: Dùng để bảo vệ hệ thống IT, tòa nhà công ty, trung tâm dữ liệu và các tài sản vật lý khác khỏi sự can thiệt, trộm cắp và truy cập không hợp lệ. Loại này có thể bao gồm nhiều loại phương pháp kiểm soát ra vào và giám sát khác nhau, chẳng hạn như camera an ninh, hệ thống báo động, máy quét thẻ ID và bảo mật sinh trắc học (ví dụ: đầu đọc dấu vân tay, hệ thống nhận dạng khuôn mặt, v.v.).
* Loại điều khiển lớp kỹ thuật: Loại này bao gồm phần cứng và phần mềm cần thiết để ngăn chặn vi phạm dữ liệu, tấn công DDoS và các mối đe dọa khác nhắm vào mạng, ứng dụng và dữ liệu. Các sản phẩm bảo mật phổ biến ở lớp này bao gồm tường lửa, cổng web an toàn (SWG), hệ thống phát hiện hoặc ngăn chặn xâm nhập (IDS/IPS), công nghệ cô lập trình duyệt, phần mềm phát hiện và phản hồi điểm cuối (EDR), phần mềm ngăn ngừa mất dữ liệu (DLP), tường lửa ứng dụng web (WAF) và phần mềm chống phần mềm độc hại, cùng nhiều phần mềm khác.
* Loại điều khiển lớp quản trị, thường loại này được đề cập đến như các chính sách do quản trị viên hệ thống và nhóm bảo mật đặt ra để kiểm soát quyền truy cập vào hệ thống nội bộ, tài nguyên của công ty và các dữ liệu và ứng dụng nhạy cảm khác. Nó cũng có thể bao gồm đào tạo nhận thức về bảo mật để đảm bảo người dùng thực hiện tốt biện pháp bảo mật, giữ bí mật dữ liệu và tránh để hệ thống, thiết bị và ứng dụng gặp phải những rủi ro không đáng có.

1. Thiết kế mạng theo sơ đồ mạng

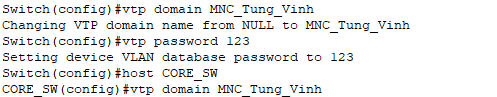
Topology:



1. Cấu hình cơ bản
2. Cấu hình VLAN, VTP, Trunk,…

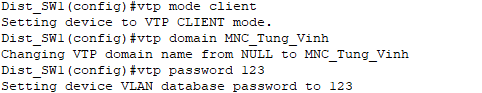
* Cấu hình VTP:

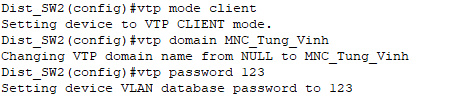
CORE SWITCH:

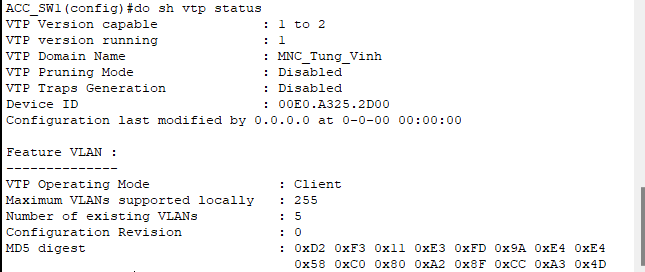


Core switch này sẽ được coi là vtp mode server, nhưng mặc định trên các switch cisco đã là vtp mode server rồi nên dùng lệnh vtp mode server là không cần thiết.

Các switch cấp dưới sẽ được cấu hình vtp mode client:



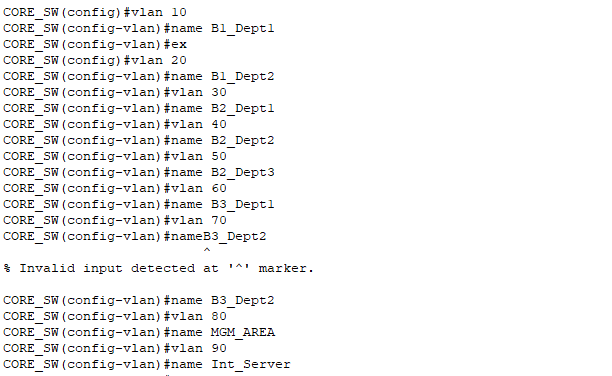




Các Switch access ở Building 2 và Building 3 cấu hình vtp tương tự như ACC\_SW1.

Bước 2: Cấu hình VLAN

Định nghĩa các VLAN trên CORE SWITCH:



Chúng em cấu hình Etherchannel cho các đường dây giữa CORE SWITCH và DIST SWITCH 1,2.

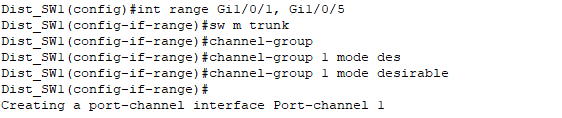
Cấu hình đường kết nối giữa CORE SWITCH và 2 DIST SWITCH sử dụng giao thức PagP:

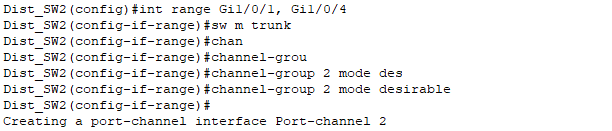






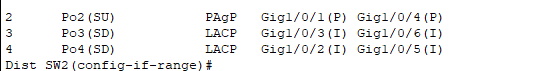


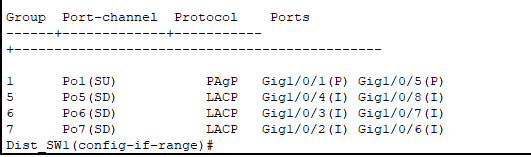




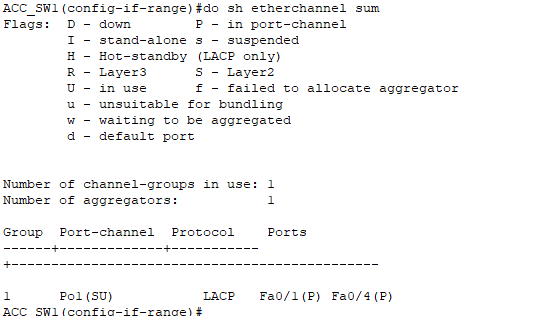
Cấu hình Etherchannel với giao thức LACP giữa các Dist Switch và Access Switch

Xác minh các cấu hình:





Cấu hình tương tự ở phía còn lại (các Access Switch):

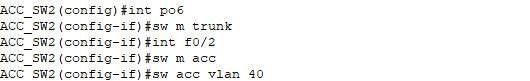


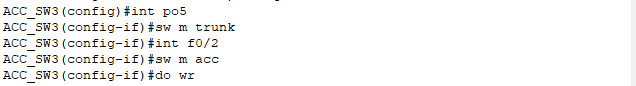
Vì số port channel trên switch 2960 giới hạn chỉ từ 1 đến 6, không thể đặt lên 7 nên switch acces 1 sẽ đặt port channel là 1. Điều này không ảnh hưởng đến cách hoạt động của etherchannel vì channel-group chỉ mang tính cục bộ trên một switch.

Các switch access còn lại cấu hình tương tự.









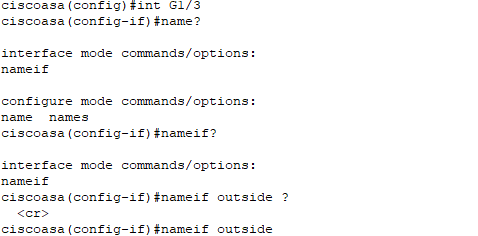


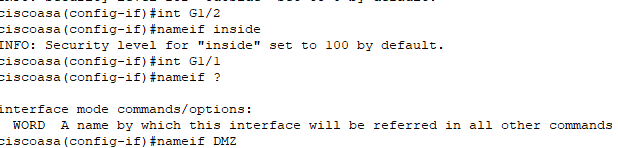


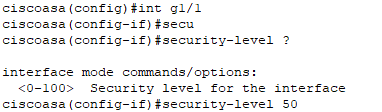
Các switch còn lại chia vlan theo như định nghĩa trong topology.

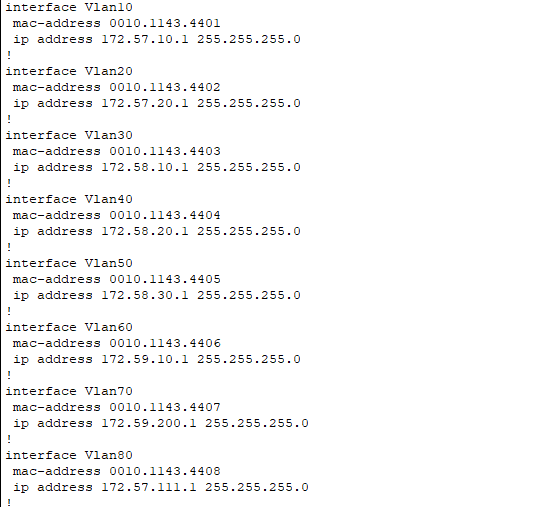
Đặt cổng Gi1/0/2 làm default-gateway cho mạng của các Internal Server.







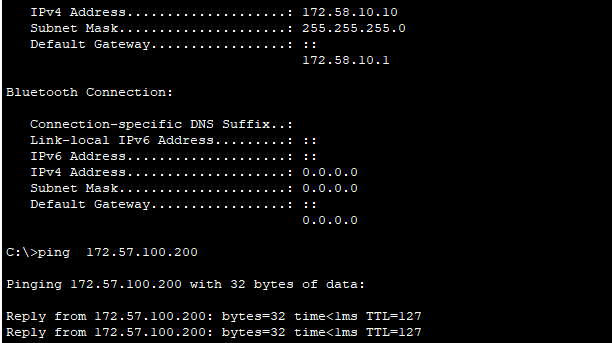




Đặt ip cho các interface vlan, các vlan này có thể giao tiếp với nhau vì kết nối trực tiếp với CORE SWITCH.

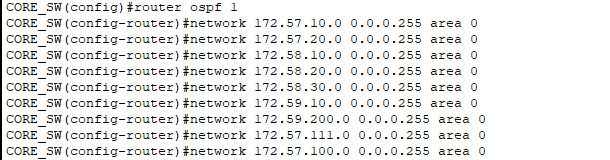
Các máy trong mạng nội bộ đã có thể giao tiếp với nhau:

Từ PC của phòng ban 1 building 2 Đến DHCP Server:

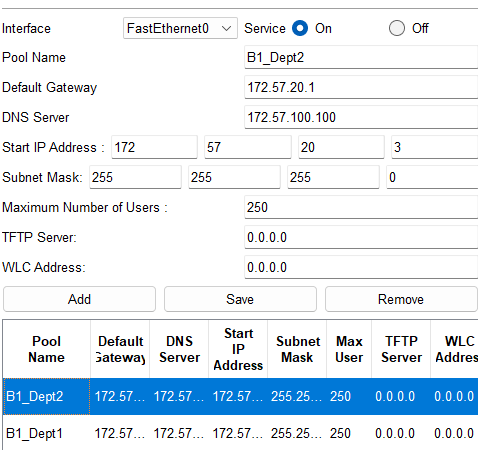


Thực hiện ping các thiết bị khác cũng thu được kết quả tương tự.

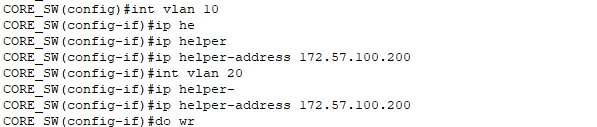
Tiếp theo, chúng em cấu hình định tuyến động trên CORE SWITCH và FW1 để các thiết bị bên dưới cũng có thể liên lạc với khu vực DMZ:



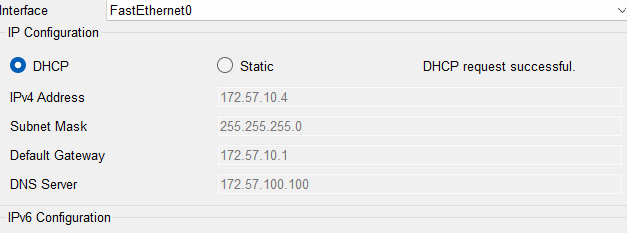
Vì DHCP không thể cấp ip khi cấu hình Etherchannel nên em thực hiện cấu hình DHCP cấp ip cho các phòng ban 1, còn building 2 và 3 sẽ cấp ip tĩnh cho các PC.



Cấu hình ip helper address để cấp ip DHCP cho Building 1:



PC8 ở phòng ban 1 thuộc Building-1 đã nhận ip từ DHCP Server thành công



Tương tự với PC ở phòng ban 2 thuộc Building 1.

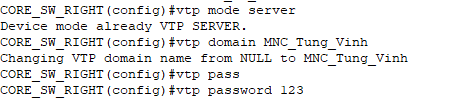
Cấu hình ACL để các máy nội bộ truy cập được ra ngoài internet (sau này cấu hình NAT) và tới các Server trong chi nhánh.

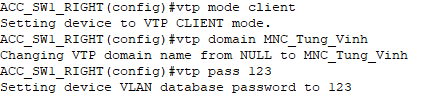




Nhánh mạng bên phải (Chi nhánh 2):

Cấu hình VTP :



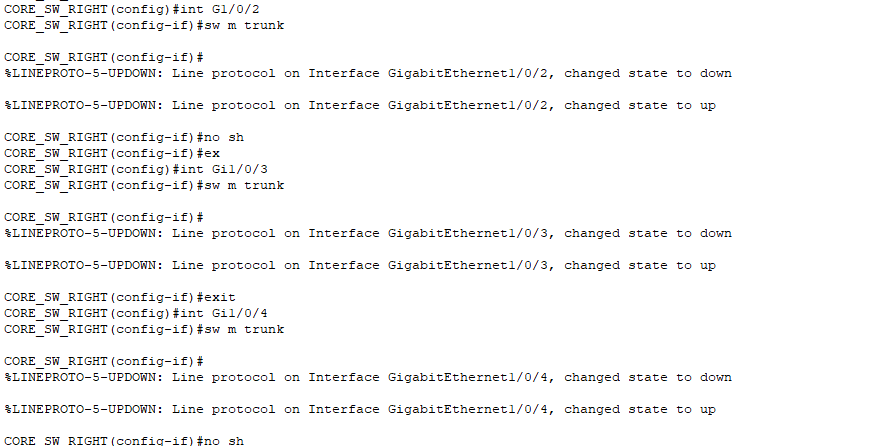


Tương tự với 2 switch access còn lại (từ trái qua phải đặt tên là ACC\_SW1\_RIGHT -> ACC\_SW3\_RIGHT).

Tạo VLAN trên CORE\_SW, sau đó nó cũng quảng bá xuống các access switch:



Cấu hình trunk:

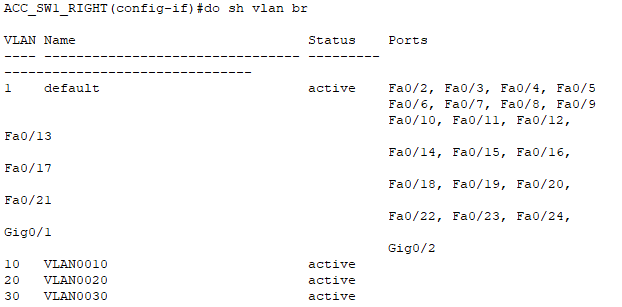








Xác nhận lại các VTP Client đã nhận được các VLAN đã định nghĩa trên CORE SWITCH:



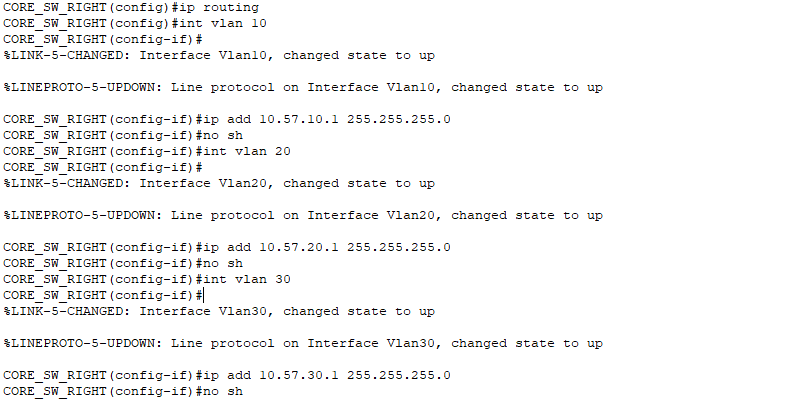
Cấu hình các cổng access:

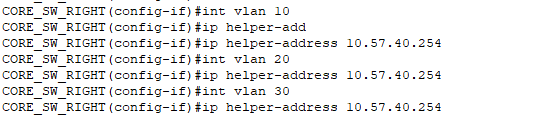




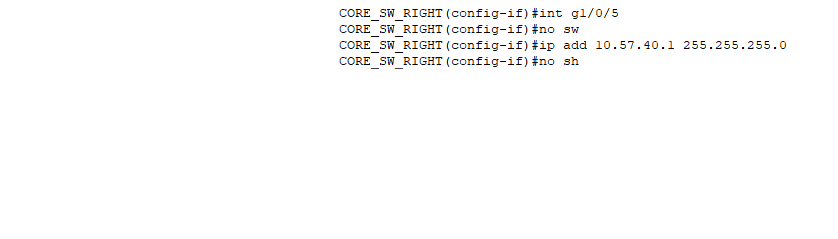


Cấu hình cấp phát ip động:

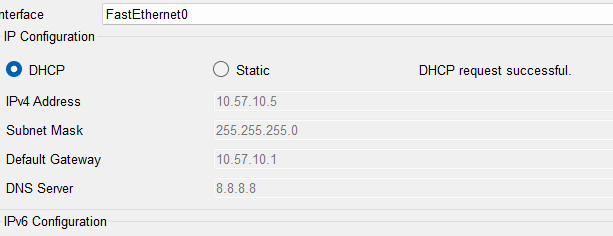
Mở tính năng ip routing trên CORE SWITCH và cấu hình địa chỉ ip, ip helper address để xin ip tới đúng DHCP SERVER của chi nhánh này:  




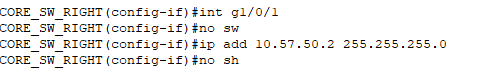
Đặt ip cho gateway của DHCP Server:

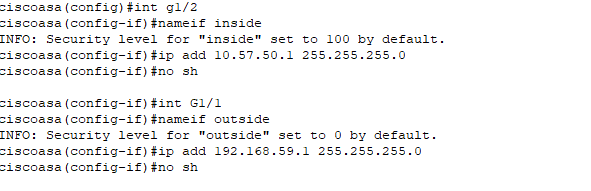


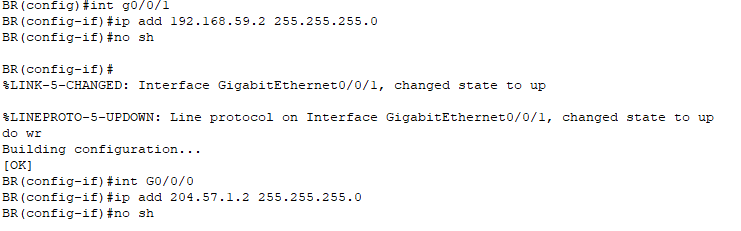
Lấy một PC kiểm tra nhận DHCP được chưa:



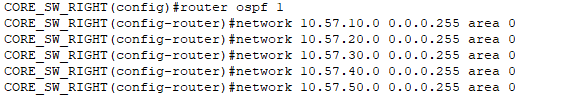
* Kết quả thành công!



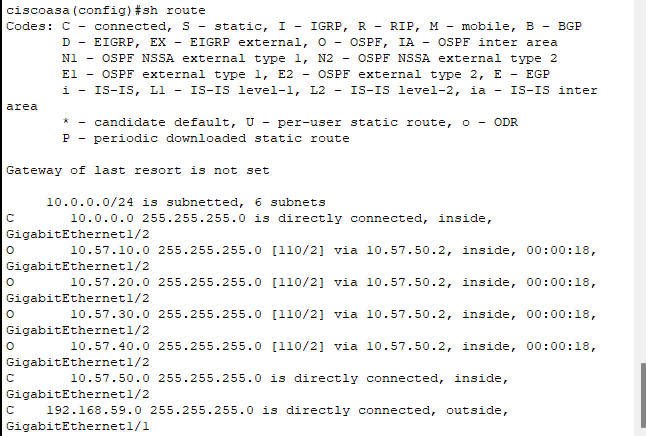




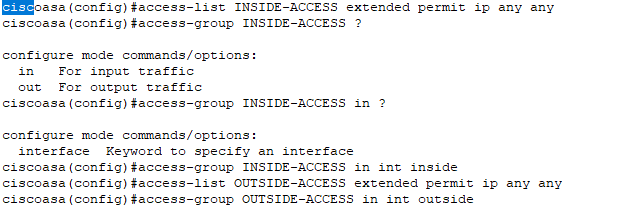
Cấu hình định tuyến:



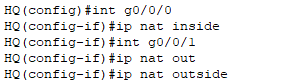




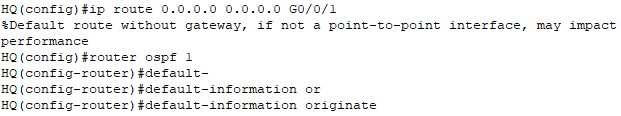
Cấu hình ACL để các PC thuộc VLAN bên dưới ping ra tới Router biên được:

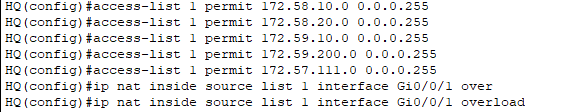












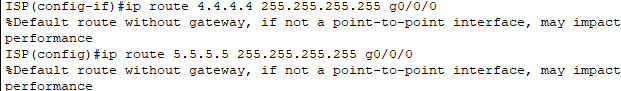




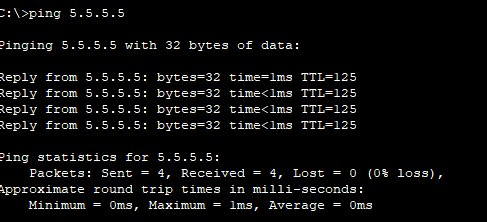


Static NAT cho phép Web Server và Email Server ra ngoài Internet:

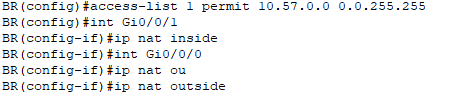




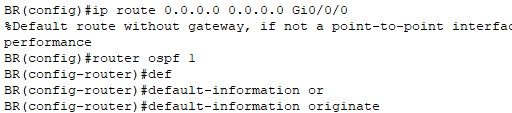
Lấy PC từ ngoài Internet ping vào:

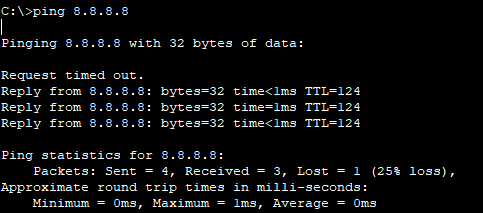


NAT Overloading Chi nhánh 2:







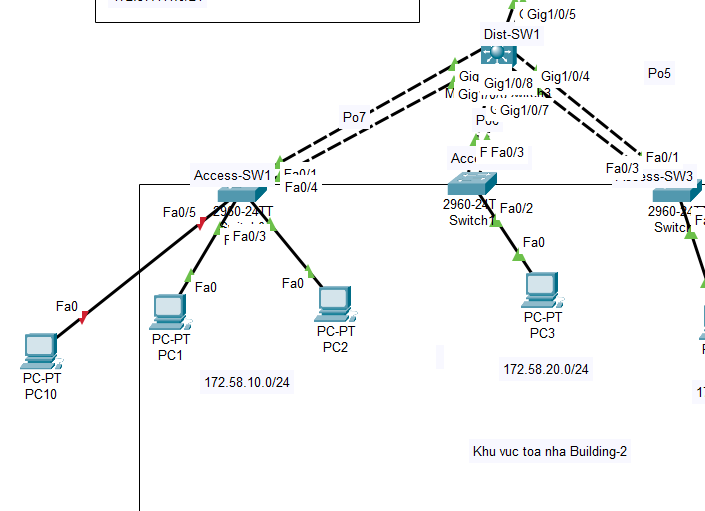


1. Cấu hình bảo mật:
2. 1. Hardening:

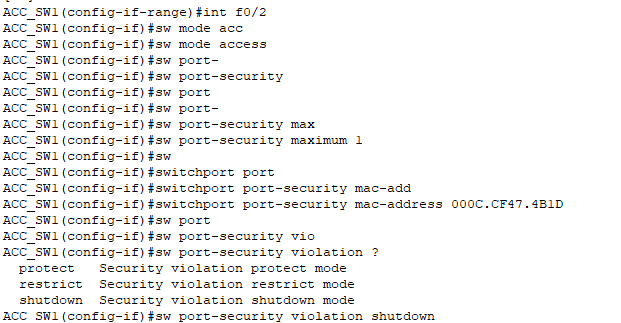




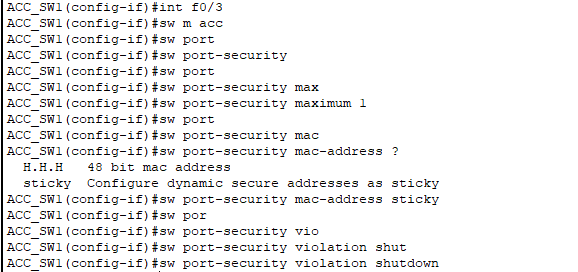
Giả sử có một máy cắm vào, khi này cổng đã bị shutdown:



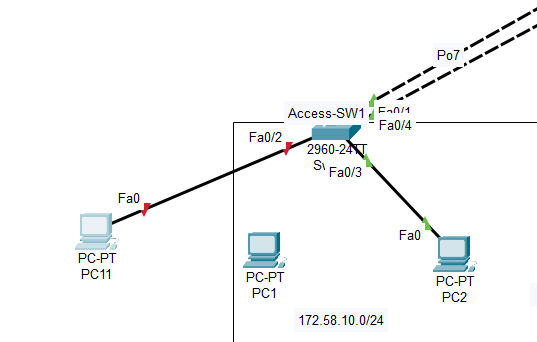
1. Port Security:



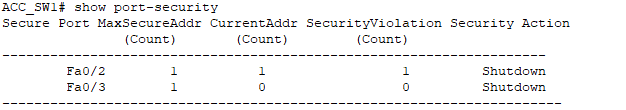
Cho Acc\_SW1 interface fa0/2 học địa chỉ MAC cố định của PC1 đang cắm vào sẵn và interface fa0/3 học địa chỉ MAC tự động.



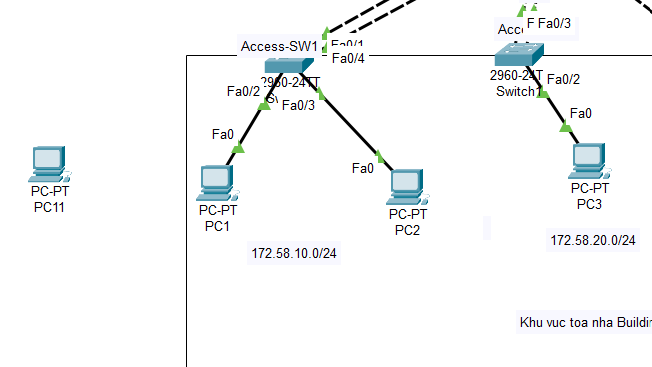
Lúc này giả sử có một PC lạ nào đó cắm vào cổng fa0/2 khi nó đang rảnh, nó sẽ tự động shutdown nếu đó không phải là địa chỉ MAC của PC1:



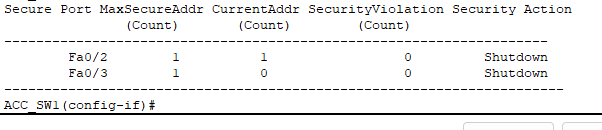
* Cổng fa0/2 lúc này đã tự chuyển sang màu đỏ. Trạng thái shutdown như đã cấu hình.



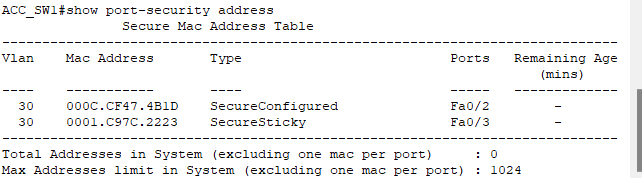
Lúc này một hành vi đã bị vi phạm dẫn đến cổng bị shutdown. Vì đây là thiết bị ảo nên chúng em bắt buộc phải vào cổng, shutdown và no shutdown lại nó mới up trở lại.



* PC1 cắm vào và hoạt động thì nó có đèn xanh trở lại. Lúc này không còn thiết bị nào bị vi phạm nữa:

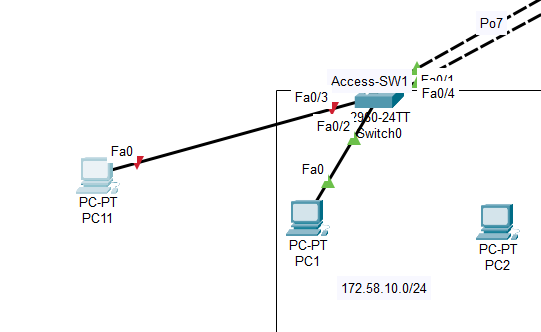


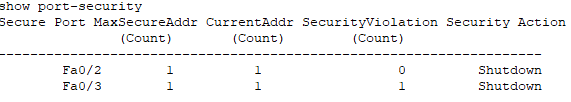
Làm tương tự với sticky, **sticky sẽ học địa chỉ MAC đầu tiên được cắm vào cổng** (nếu chưa có MAC Address nào được học).



0001.C97C.2223 là địa chỉ MAC của PC2.

Thử lại tương tự, nếu cắm PC11 (PC không thuộc hệ thống mạng) vào ACC\_SW1 nó sẽ shutdơn cổng:

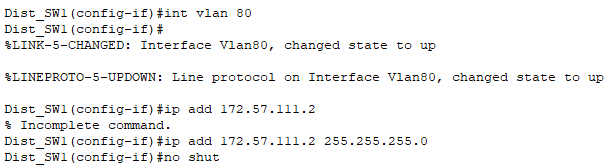




Cổng fa0/3 đã bị tắt, muốn mở lại thì cũng gỡ dây ra gỏi PC11 rồi dùng shutdown sau đó no shutdown như trên.

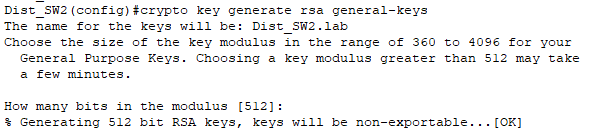
1. Cấu hình truy cập từ xa bằng dịch vụ SSH

Đối với các access switch và distribution switch không có cổng layer 3 để xử lý dịch vụ ssh thì chúng em sẽ sử dụng cổng vlan 80 và đặt địa chỉ ip cho cổng này, từ đó có thể điều khiển từ xa switch. Đối với Core switch thì cần thiết phải tạo thêm cổng vlan 80 vì đã có được cấu hình trước đó.

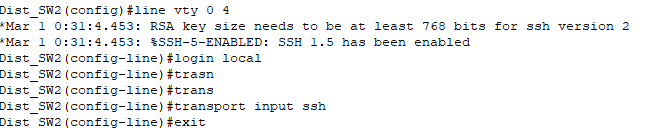


Để có thể sư dụng dịch vụ SSH thì ở các switch phải khai báo tài khoản mật khẩu local hoặc sử dụng aaa từ server để xác thực người điều khiển từ xa, trong bài lab này chúng em sử dụng tài khoản mật khẩu local trên các switch để xác thực tài khoản. Đòng cấu hình thêm tên miền trong lab dùng để theo khóa được tạo ra từ thuật toán rsa (bắt buộc hostname của các switch phải khác tên mặc định), tuy vậy có thể thay thế tên miền bằng các label.

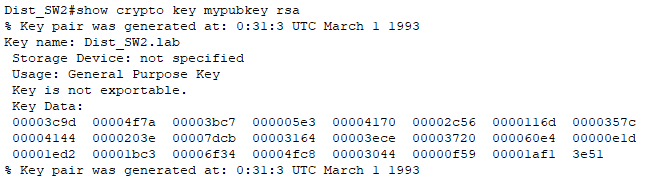


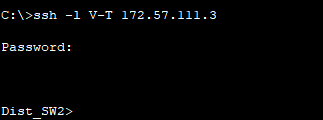


Sau khi cấu hình tên, mật khẩu của tài khoản và cấu hình rsa thì chúng em sẽ cấu hình các cổng remote (ở đây chúng em cho phép remote đồng thời 4 kết nối), cổng sẽ sử dụng dịch vụ SSH làm giao thức điều khiển, tên và mật khẩu để nhập là trên local của các switch.



Sau khi xong cấu hình điều khiển từ xa bằng SSH, chúng em sẽ kiểm tra khóa được tạo trên các switch và thử truy cập điều khiển từ xa bởi các máy tính.

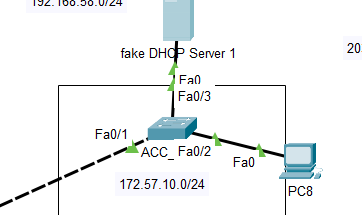




* Thành công trong truy cập từ xa các switch bằng máy tính.

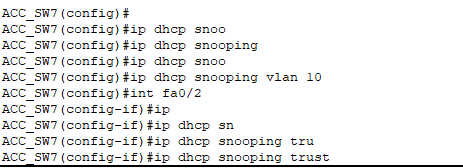
1. Cấu hình DHCP snooping

Đối với các port channel được tạo ra từ công nghệ etherchannel khi gom lại các cổng, trong phần mềm giả lập Cisco Packet Tracer, việc áp lệnh “ip DHCP snooping trust” là không thể, vì thế cho nên chúng em sẽ chỉ cấu hình trên các switch của building 1 trong Hội sở.

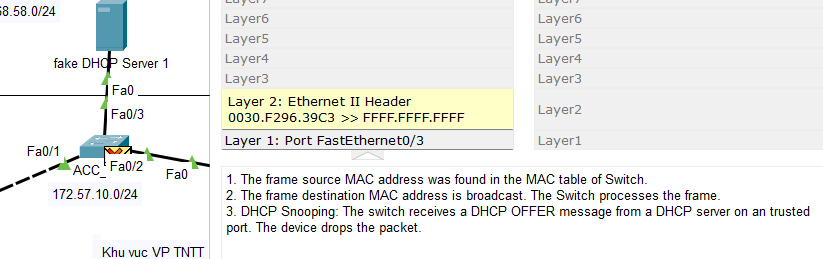


Switch trong building 1 sẽ được cấu hình DHCP snooping

Đầu tiên chúng em bật chế độ DHCP snooping global cho switch và khai báo DHCP snooping sử dụng cho vlan nào, sau đó gán cổng trust cho cổng hướng tới DHCP server.



Sau khi cấu hình ta sẽ kiểm tra nếu xuất hiện một DHCP server giả mạo cùng tồn tại trong cùng VLAN thì switch có từ chối gói DHCP offer từ server giả mạo này không.

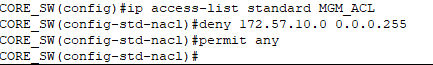


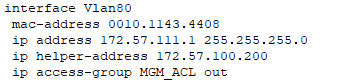
Đối với Core switch thì chúng em không cấu hình DHCP snooping vì đã có lệnh “ip helper-address” xử lý (được cấu hình trước đó).

1. Cấu hình access-list control

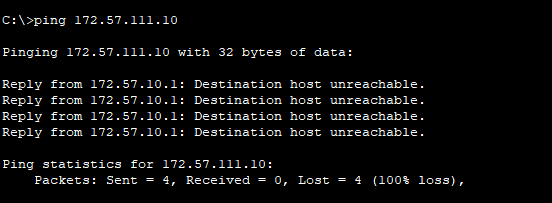
* Cấu hình cấm vlan 10 truy cập vào khu vực quản trị:

Đầu tiên chúng em tạo một ACL để áp dụng vào đầu ra của cổng VLAN 80, ACL sẽ cho phép các mạng ngoài 172.57.10.0 (thuộc vlan 10) truy cập tới khu vực quản trị.

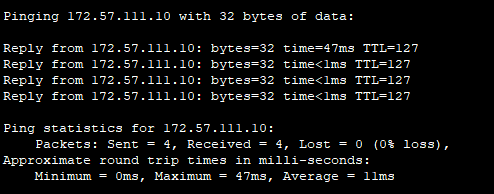




Sau khi cấu hình xong chúng em kiểm tra bằng cách ping từ các máy không thuộc và thuộc vlan 10 tới khu vực quản trị.



Máy thuộc VLAN 10 bị từ chối truy cập khu vực quản trị



Máy không thuộc VLAN ping tới khu vực quản trị

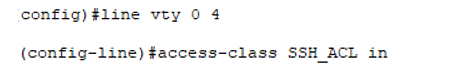
* Cấu hình quyền truy cập từ xa SSH:

Để cho phép chỉ các máy thuộc khu vực quản trị truy cập từ xa, chúng em tạo một ACL và cho phép các gói TCP (lý do là vì SSH sử dụng giao thức TCP ở tầng transport) có địa chỉ IP nguồn thuộc mạng 172.57.111.0/24 SSH tới.

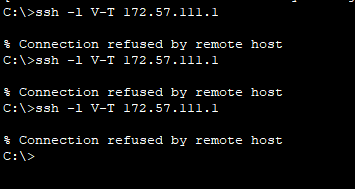




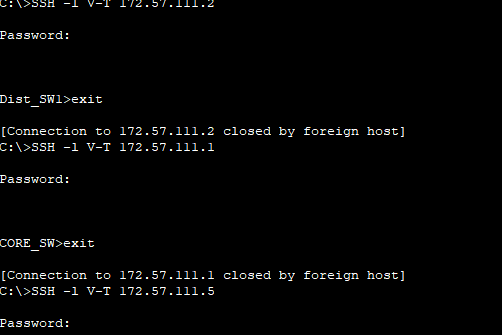
Sau đó gán ACL đã tạo như một filter lọc các địa chỉ IP trên các cổng điều khiển truy cập từ xa với hướng đi của các gói tin là vào.



Sau khi cấu hình xong ACL và cổng trên các switch, chúng em kiểm tra bằng cách điều khiển truy cập từ xa từ các máy không thuộc và thuộc khu vực quản trị tới các switch đã được cấu hình SSH.



Các máy không thuộc khu quản trị bị từ chối điều khiển



Các máy thuộc khu vực quản trị vẫn điều khiển được các Switch

1. Cấu hình Firewall (ở Hội sở)

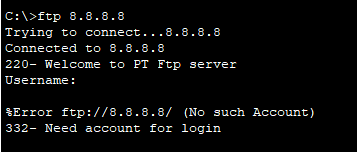
Vì yêu cầu ở mục này là cho phép các máy thuộc VLAN 20 chỉ truy cập ra bên ngoài bằng cách sử dụng Ping và sử dụng FTP, nên chúng em sẽ cấu hình ACL trên tường lửa, ACL này cho phép 2 dịch vụ này với địa chỉ IP nguồn thuộc mạng VLAN 20.

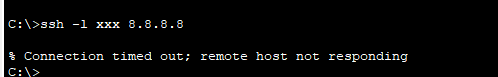












1. Cấu hình Firewall (ở chi nhánh)



1. Cấu hình mạng Wifi ở Hội sở:

