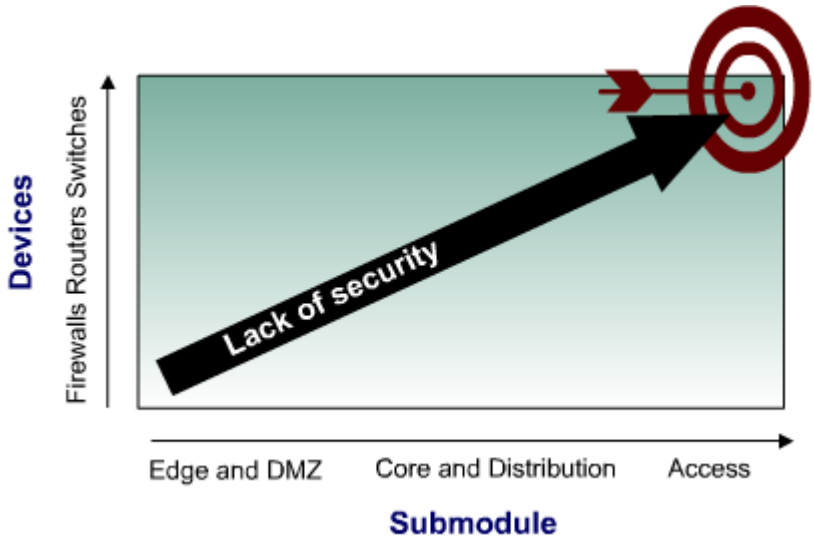
Chương 9 - Giảm Thiểu Thất Thoát Dịch Vụ Và Mất Cắp Dữ Liệu Trong Mạng Campus

Module này xác định rủi ro tiềm năng liên quan đến VLAN trong một hệ thống mạng và các giải pháp có thể. Chủ đề bao gồm port security cho của MAC spoofing và flooding, sử dụng PVLAN và VACL để kiểm soát lưu lượng VLAN, VLAN hopping, giả mạo DHCP, ARP spoofing, và các cuộc tấn công STP. Bạn tìm hiểu về nhiều vấn đề tiềm năng và các giải pháp, trong đó, bạn tìm hiểu làm thế nào để bảo vệ truy cập switch bằng cách sử dụng ACL vty và thực hiện SSH.

9.1 Tìm hiểu bảo mật switch

9.1.1 Tổng quan bảo mật switch

Rất nhiều công nghệ tập trung vào bảo mật mạng từ bên ngoài tường lửa của tổ chức và những lớp trên của mô hình OSI. Bảo mật mạng thường tập trung vào các thiết bị edge-routing, bộ lọc gói là chủ yếu,và hoạt động chủ yêu hoạt động dựa vào việc kiểm tra header của lớp 3 và 4 ,port, và trạng thái kết nối của gói. Tất cả các truy cập từ internet vào trong mạng sẽ được kiểm tra từ lớp 3 trở lên. Do vậy công nghệ bảo mật mạng ít tập trung vào các thiết bị truy cập Campus và sự lưu thông mạng ở lớp 2.



Hình 9.1.1-1: Mức độ an toàn của các thiết bị

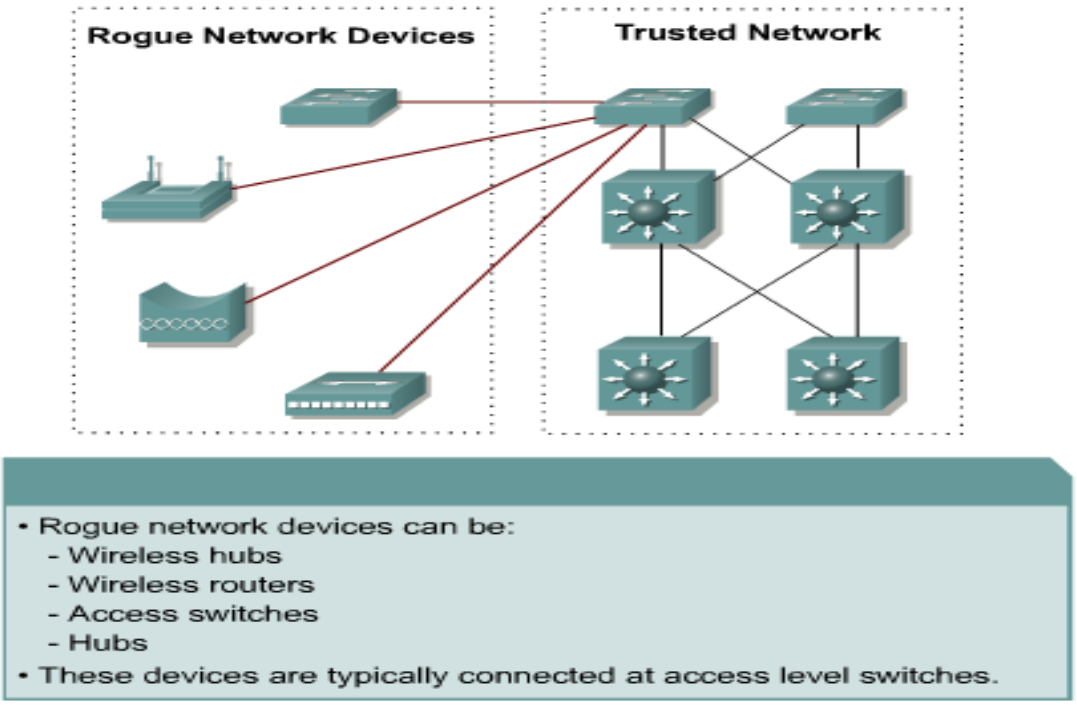
Mặc định các thiết bị mạng chủ yếu kiểm soát các truy cập từ bên ngoài và mở truy cập cho các giao tiếp bên trong nội mạng. Tường lửa được đặt ở biên giữa tổ chức với mạng internet bên ngoài, mặc định tường lửa không cho phép

giao tiếp cho đến khi cấu hình được thực thi. Chế độ cấu hình mặc định của các router và switch bên trong mạng cho phép giao tiếp với nhau và chuyển tất cả các traffic. Điều này chính là kết quả của cấu hình bảo mật thiếu và yếu, những thiết bị này sẽ trở thành đối tượng cho các hoạt động tấn công. Nếu các cuộc xâm nhập đã tấn công các thiết bị truy cập CAMPUS thì các thiết bị còn lại trong mạng sẽ nhanh chóng bị kiểm soát mà rất khó phát hiện.

Nhiều tính năng bảo mật có sẵn trên switch và router, nhưng những đặc tính này cần phải được cấu hình để đặt được hiệu quả. Với lớp 3 các mối đe dọa càng tăng do vậy do vậy cần phải được cấu hình bảo mật nghiêm ngặt đồng thời triển khai phương pháp bảo mật để bảo vệ các hoạt động nguy hại ở lớp 2. Bảo mật mạng cần phải tập trung vào các vụ thâm nhập dựa vào hoạt động của switch lớp 2. Giống như ACLs, một chính sách bảo mật cần được thiết lập và cấu hình những đặc tính bảo mật phù hợp nhắm mục đích vừa chống lại các hoạt động đe dọa vừa đảm bảo sự vận hành của hệ thống mạng.

9.1.2 Truy cập trái phép với các thiệt bị Rogue

Truy cập rogue gồm có nhiều hình thức. Ví dụ, các điểm truy cập rogue ít tốn kém và sẵn có nên đôi khi nhân viên cắm vào hệ thống mạng LAN và xây dựng mạng ad hoc mà không thông qua quản trị mạng. Các điểm truy cập rogue có thể vi phạm nghiêm trọng trong bảo mật mạng, vì rất có thể các điểm truy cập rogue cắm phía trong tường lửa.



Hình 9.1.2-1: Truy cập trái phép từ các thiết bị ngoài mạng

Nhân viên thường không triển khai cấu hình bảo mật trên các thiết bị truy cập rogue. Vì vậy các thiết bị này cho phép truy cập không chứng thực

Hiện tại thì rủi ro và thách thức ngày càng lớn đến từ các điểm truy cập rogue độc hại. Vì các điểm truy cập này ẩn trong mô hình mạng. Các điểm truy cập rogue độc hại được cắm vào mạng LAN sẽ làm tăng độ nguy hại, và rủi ro cho hệ thống.

Switch lớp hai cũng là một thiết bị rogue độc hại. Kẻ tấn công có truy cập vật lí đến rogue switch, thì chúng có thể thực hiện STP, hop VLAN, Sniff traffic…Rogue switch này trở thành trạm hoạt động có khã năng trunk và tham gia các hoạt động lưu thông mạng ở lớp 2.

Để giảm thiểu thao tác STP sử dụng lệnh roo-guard và BPDU guard trên các root bridge trong mô hình mạng và trong STP domain border. STP BPDU guard cho phép các nhà thiết kế mạng có thể dự đoán mô hình hoạt động của mạng. Trong khi BPDU guard trông có vẽ không cần thiết đối với người quản trị khi cài đặt bridge priority về 0. Khi đó vẫn chưa đảm bảo Switch đó sẽ được chọn làm root bridge. Bởi vì rất có thể trong mạng có một Switch khác có bridge priority là 0 và có chỉ số bridge thấp hơn. BPDU guard là cách tốt nhất để chống sự mở rộng của switch rogue.

9.1.3 Tấn công Switch

Các cuộc tấn công nguy hiểm lớp 2 thường là sự xâm nhập bằng một thiết bị kết nối trực tiếp đến mạng CAMpus. Có thể là một thiết bị rogue vật lí được đặt trong mạng hoặc sự xâm nhập bên ngoài bị kiểm soát và tấn công từ các thiết bị tin cậy trong mạng.

Các hình thức tấn công layer 2 và tấn công switch:

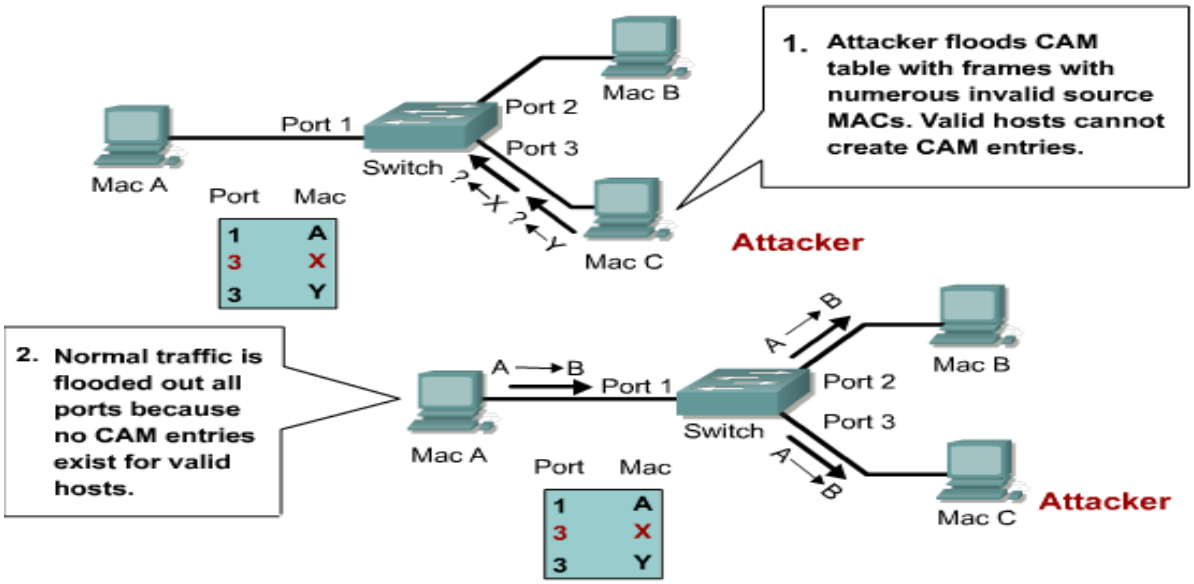
- MAC layer attacks
- VLAN attacks
- Spoof attacks

Kỹ thuật	Mô tả	Giải pháp
Mac layer attack		
MAC address flooding	Các gói tin có địa chỉ MAC giả mạo sẽ flood đến switch, trong Switch có bản CAM (content addressable memory) để lưu lại địa chỉ MAC. Do giới hạn bộ nhớ không cho phép bản CAM ghi thêm những địa chỉ MAC của các gói tin thực trong mạng, do vậy khi gói tin đến nó sẽ được flood ra tất cả các port của switch	Port security MAC address VLAN access maps
VLAN Attacks		
VLAN hoping	Thay đổi VLAN ID của các packet dành cho trunking. Các thiết bị tấn công có thể gửi và nhận các gói tin của nhiều VLAN khác nhau, và vượt qua được mức bảo mật ở lớp 3	Cấu hình trunk tốt và thỏa thuận trạng thái của những port không dùng. Cấu hình những port không dùng vào các common VLAN
Attacks between devices on common VLAN	Thiết bị cần được bảo vệ thậm chí là các thiết bị này được cấu hình nằm trong các common VLAN. Đặc biệt là các nhà cung ứng dịch vụ phân loại các thiết bị hỗ trợ đối với nhiều loại khách hàng	Triển khai Private VLAN (PVLAN)
Spoofing attack		
DHCP starvation DHCP spoofing	Thiết bị tấn công có thể yêu cầu không gian địa chỉ IP cho một khoảng thời gian xác định. Hoặc các thiết bị này có thể hoạt động như	DHCP snooping

	một DHCP server trong trường hợp tấn công man in the midle	
Spanning tree compromises	Thiết bị tấn công sẽ spoof root bridge trong mô hình STP	Cấu hình backup root device và bật root guard
MAC spoofing	Thiết bị tấn công sẽ thay đổi địa chỉ MAC của một host thực trong bảng CAM bằng một địa chỉ MAC của thiết bị tấn công, như vậy thay vì switch chuyển gói tin đến host thực nhưng gói tin sẽ đi đến attacking device	DHCP snooping Port security
ARP spoofing	Attacking device sẽ dùng kỹ thuật để trả lời các gói ARP cho các host. Như vậy địa chỉ MAC của attacking device sẽ được các thiết bị bên trong mạng sử dụng để đóng frame.	Dynamic ARP inspection DHCP snooping Port security
Switch device attacks		
CDP(cisco discovery protocol)	Thông tin được gửi thông qua CDP ở dạng cleartext và không có chứng thực vì vậy có thể dễ dàng bắt gói để biết thông tin	Disable CDP trên các port.
SSH và telnet attacks	Gói tin telnet có thể đọc đượ do nó ở dạng cleartext. SSH v1 không bảo mật	Sử dụng SSHv2 Sử dụng telnet với VTY(virtual terminal) ACLs

9.1.4 MAC Flooding Attack

Tân công lớp 2 hoặc tấn công Switch là MAC flooding, kỹ thuật tấn công này làm cho bảng CAM ngập lụt và kết quả là các frame đến switch sẽ được chuyển ra đến tất cả các port. Kỹ thuật tấn công này được dùng để thu thập mẫu traffic bên trong mạng hoặc tấn công từ chối dịch vụ(DoS).



Hình 9.1.4-1: Tấn công MAC flooding

Bảng CAM của switch có giới hạn về dung lượng bộ nhớ, vì vậy chỉ có thể chứa một số lượng địa chỉ MAC có giới hạn ở một thời điểm nhất định. Kẻ tấn công mạng có thể làm ngập lụt một switch bằng cách gửi một số lượng lớn các frame có địa chỉ MAC không có thực trong mạng. Khi bảng CAM chứa đủ dung lượng thì địa chỉ MAC của các frame đến sau sẽ không được ghi vào bảng. Như vậy khi một frame cần một thiết bị nào đó trong mạng mà địa chỉ MAC không có trong bảng CAM thì gói frame đó sẽ được chuyển đến tất cả các port của switch. Tác hại:

- Traffic lưu thông hiệu quả kém
- Các thiết bị xâm nhập dễ dàng kết nối và bắt gói tin ở tất cả các port của switch

Nếu cuộc tấn công triển khai vào thời điểm buổi sáng thì dung lượng của bảng CAM trong switch sẽ đầy. Vì vậy khi các thiết bị trong mạng khởi động, địa chỉ MAC nguồn sẽ không được ghi vào trong bảng CAM. Nếu số lượng thiết bị này càng lớn thì số lượng địa chỉ MAC dành cho traffic bị ngập lụt sẽ càng cao. Các port của switch sẽ bị ngập lụt frame từ một lượng lớn các thiết bị trong mạng.

Nếu sự ngập lụt bảng CAM chỉ diễn ra một lần, sau một thời gian cấu hình nhất định switch sẽ loại bỏ và các thiết bị mạng hợp lệ sẽ có thể tạo ra các entry để ghi vào bảng CAM, trong khi đó thì kẻ xâm nhập đã bắt được một lượng lớn traffic từ trong mạng.

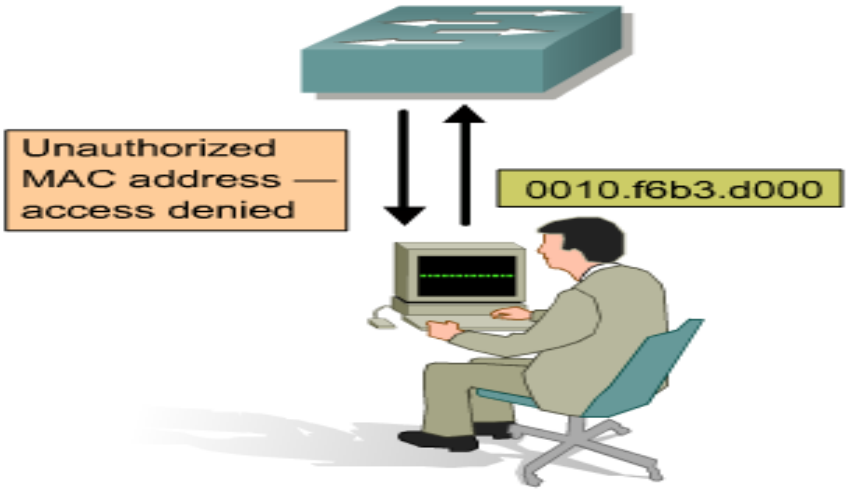
Qui trình tấn công ngập lụt địa chỉ MAC:

- Switch thực hiện forward dựa vào bảng CAM hợp lệ
- Kẻ tấn công gửi ra ngoài một lượng lớn các gói có địa chỉ source khác nhau.
- Sau một thời gian thì bảng CAM của switch trở nên đầy và không ghi thêm được nữa. Cuộc tấn công vẫn duy trì và bảng CAM sẽ được duy trì ở trạng thái full với các địa chỉ giả mạo.
- Switch bắt đầu flood tất cả các packet mà nó nhận được từ tất cả các port. Ví dụ một frame từ host A gửi đến host B cũng được flood ra tất cả các port còn lại của switch.

Để hạn chế MAC flooding yêu cầu cấu hình port security. Cấu hình port security được cấu hình để chỉ ra địa chỉ MAC nào và số lượng cho phép hoạt động trên mỗi port.

9.1.5 Port Security

Cisco Catalyst switches có tích hợp port security. Port security giới hạn địa chỉ MAC nào? Và số lượng địa chỉ MAC hoạt động trên mỗi port của switch.



Hình 9.1.5-1: Từ chối truy cập của các địa chỉ MAC không hợp lệ

Địa chỉ sẽ được cấu hình hoặc học hỏi tự động, chỉ có những địa chỉ này mới được phép hoạt động trên port đã được cấu hình port security. Nếu số lượng địa chỉ giới hạn được cấu hình là 4 mà không chỉ rõ những địa chỉ MAC nào? port sẽ tự động học 4 địa chỉ MAC bất kì.

Một đặc tính của port security gọi là sticky learning, đặc tính này là sự kết hợp giữa cấu hình tĩnh và tự học của thiết bị. Khi đặc tính này được cấu hình trên

interface và interface sẽ chuyển sang học địa chỉ tự động để “sticky secure” địa chỉ. Những địa đã được học tự động được thêm vào trong cấu hình chạy giống như chúng đã được cấu hình sử dụng lệnh: switchport port-security mac-address.

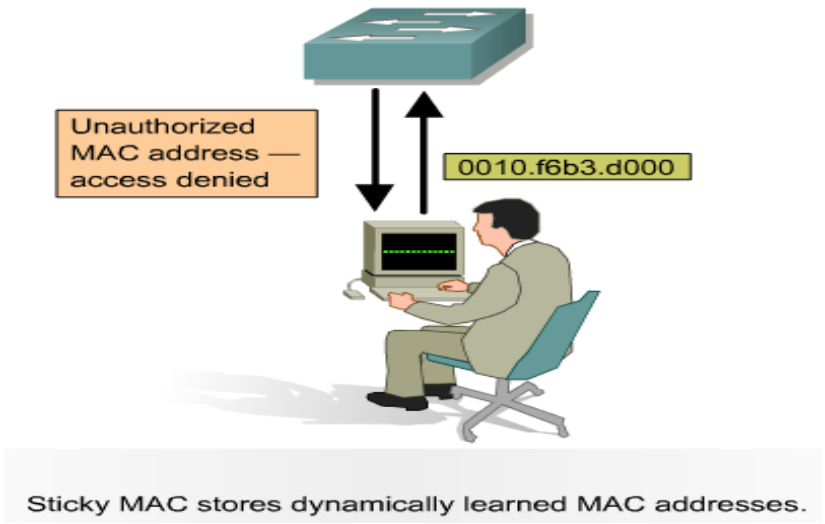
Bảng sau mô tả tiến trình này:

Bước	Hoạt động	Ghi chú
1	Cấu hình port security	Cấu hình port security cho phép chỉ 5 kết nối trênport đó. Cấu hình một entry cho mỗi một cái trong năm địa chỉ được cho phép. Tác dụng của điều này gán vào bảng địa chỉ MAC năm entry cho port đó van không cho phép add thêm entry nào được học tự động.
2	Cho phép các frame được thực thi.	Khi các frame đến port của Switch địa chỉ MAC nguồn của chúng được kiểm tra trong bảng địa chỉ MAC. Nếu frame có địa chỉ nguồn khớp với một entry trong bảng cho part đó, frame se được chuyển vào Switch để tiếp tục tiến trình như các frame khác trên Switch.
3	Một địa chỉ mới không được phép tạo một entry mới trong bảng địa chỉ MAC	Khi các frame đến port của Switch địa chỉ MAC nguồn của chúng được kiểm tra trong bảng địa chỉ MAC. Nếu frame có địa chỉ nguồn khớp với một entry trong bảng cho part đó, frame se được chuyển vào Switch để tiếp tục tiến trình như các frame khác trên Switch.
4	Switch thực hiện hành động với các frame không hợp lệ.	Switch không cho phép vào port van thực hiện một trong các biện pháp được cấu hình sau: (a) port bị shut down; (b) từ chối truy nhập của địa chỉ MAC này và ghi lại lỗi; (c) từ chối truy nhập của địa chỉ MAC này và không có thông báo lỗi.

Lưu ý: port security không được cấu hình trên port trunk, nơi mà địa chỉ sẽ thay đổi thường xuyên.

9.1.6 Port security với sticky MAC address

Port security được sử dụng để giảm thiểu rủi ro trước các cuộc tấn công giả mạo bằng cách giới hạn truy cập trên các port switch. Ngăn chặn được những kẻ xâm nhập sử dụng nhiều địa chỉ MAC trong một khoảng thời gian, nhưng không giới hạn port truy cập đến một địa chỉ MAC xác định. Hầu hết các triển khai giới hạn port security đều chỉ rõ chính xác địa chỉ MAC của một thiết bị, thiết bị sẽ được truy cập thông qua port. Tuy nhiên đê triên khai mức bảo mật này thì yêu cầu một chi phí đáng kể.



Hình 9.1.6-1: Port security có thuộc tính Sticky

Port security có thuộc tính gọi là “sticky MAC address”, đặc tính này giới hạn truy cập đến một địa chỉ MAC.

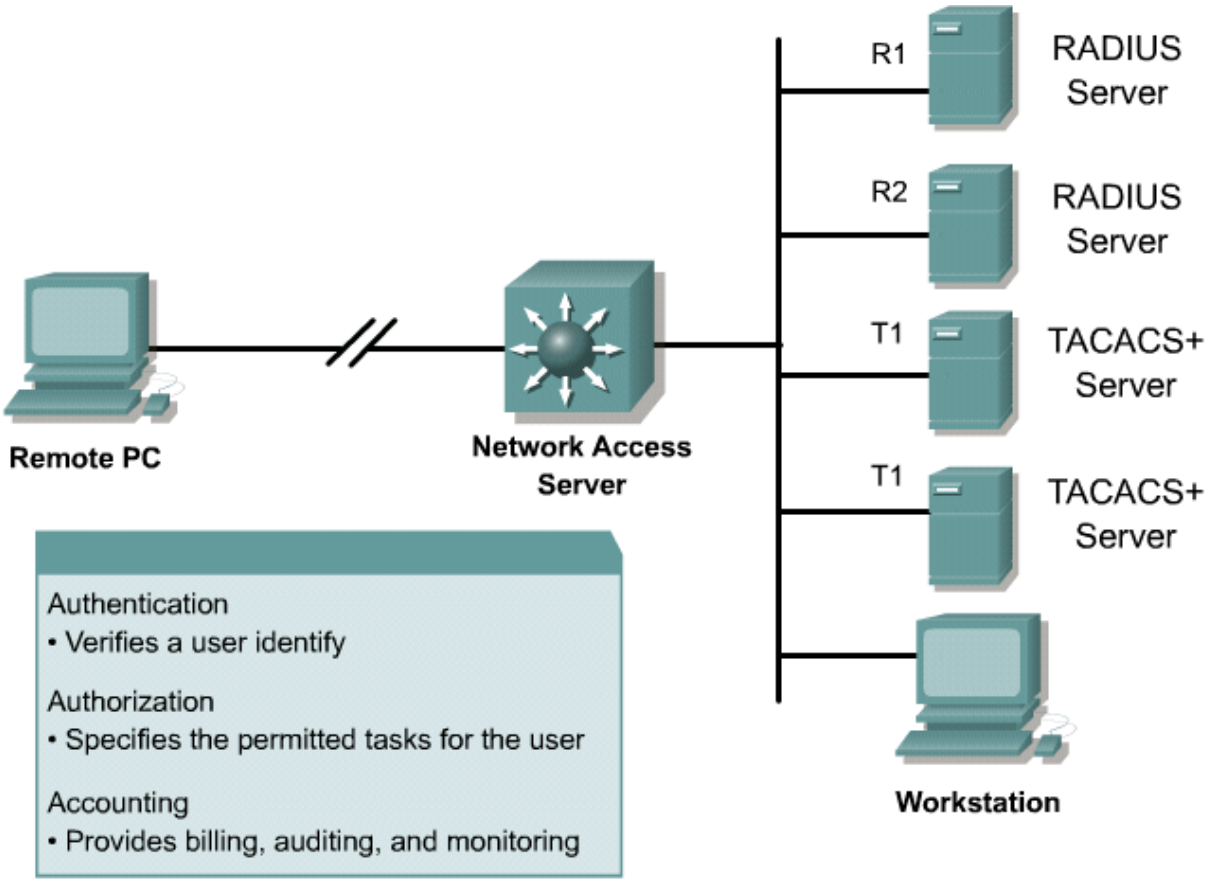
Sticky MAC address được sử dụng, thì switch port sẽ chuyển sang học tự động các địa chỉ MAC để sticky địa chỉ MAC và thêm những địa chỉ này vào cấu hình đang chạy giống như cấu hình tĩnh(port security) cho một địa chỉ MAC. Sticky MAC address được thêm vào trong cấu hình chạy nhưng vẫn chưa có trong file start up. Trừ khi cấu hình chạy được sao chép vào file startup config sau khi những địa chỉ đã được học thì switch sẽ không cần phải học lại khi khởi động lại.

Những lệnh dưới đây dùng để covert dynamic port security-learned MAC address sang sticky secure MAC address:

switchport port-security mac-address sticky

Lưu ý: lệnh này không được dùng trong VLAN voice.

9.1.7 Authentication, Authorization, và Accounting.



Hình 9.1.7-1: Mô hình bảo mật AAA

Dịch vụ bảo mật AAA cung cấp dịch vụ bảo vệ framework thông qua điều khiển truy cập được cài đặt trên switch. AAA là một khung bảo mật cho phép cấu hình cài đặt 3 chức năng bảo mật độc lập nhất quán.

Authentication là cách người dùng được xác định trước khi được phép truy cập mạng và dịch vụ mạng. chứng thực AAA được cấu hình bằng cách định nghĩa một danh sách các phương pháp xác thực được đặt tên và sau đó áp dụng danh sách này để các interface khác nhau. Danh sách các phương pháp xác định phương thức xác thực sẽ được thực hiện và thực hiện theo trình tự. Danh sách các phương pháp phải được áp dụng cho một interface cụ thể trước khi có bất kì phương pháp xác thực nào khác thực thi. Nếu không có danh sách các phương pháp xác định, phương pháp danh sách mặc định (có tên là "default") được áp dụng. Danh sách các phương thức được định nghĩa sẽ được ghi đè lên danh sách mặc đinh.

Trong nhiều trường hợp AAA sử dụng giao thức chứng thực như: RADIUS, TACACS+, hoặc 802. 1x để quản lí chức năng bảo mật. Nếu Switch hoạt động

như một máy chủ truy cập mạng, AAA là phương thức mà qua đó switch thiết lập giao tiếp giữa các máy chủ truy cập mạng và RADIUS, TACACS +, hoặc máy chủ an ninh 802. 1x.

9.1.8 Các Phương Thức Chứng Thực

Dịch vụ AAA mang lại nhiều phương thức chứng thực login.

Cấu trúc lệnh tạo một danh sách chứng thực cục bộ:

Switch(config)# aaa authentication login {default | list-name} method1 [method2….]

Cisco IOS AAA hỗ trợ các phương thức chứng thực:

- Enable password
- Kerberos 5
- Kerberos 5-Telnet authentication
- Line password
- Local database
- Local database with case sensitivily
- No authentication
- RADIUS
- TACACS+

Tham số list-name là tên của danh sách, tham số method chỉ đến thuật toán xác định. Các phươn thức xác thực bổ sung chỉ được dùng khi phương thức trước đó bị lỗi.

Ví dụ để dùng RADIUS làm phương pháp chứng thực trong suốt quá trình login, cấu hình các lệnh sau: aaa authentication dot1x default group radius

Các bước cấu hình AAA:

- **Bước 1:** enable AAA: aaa new-model

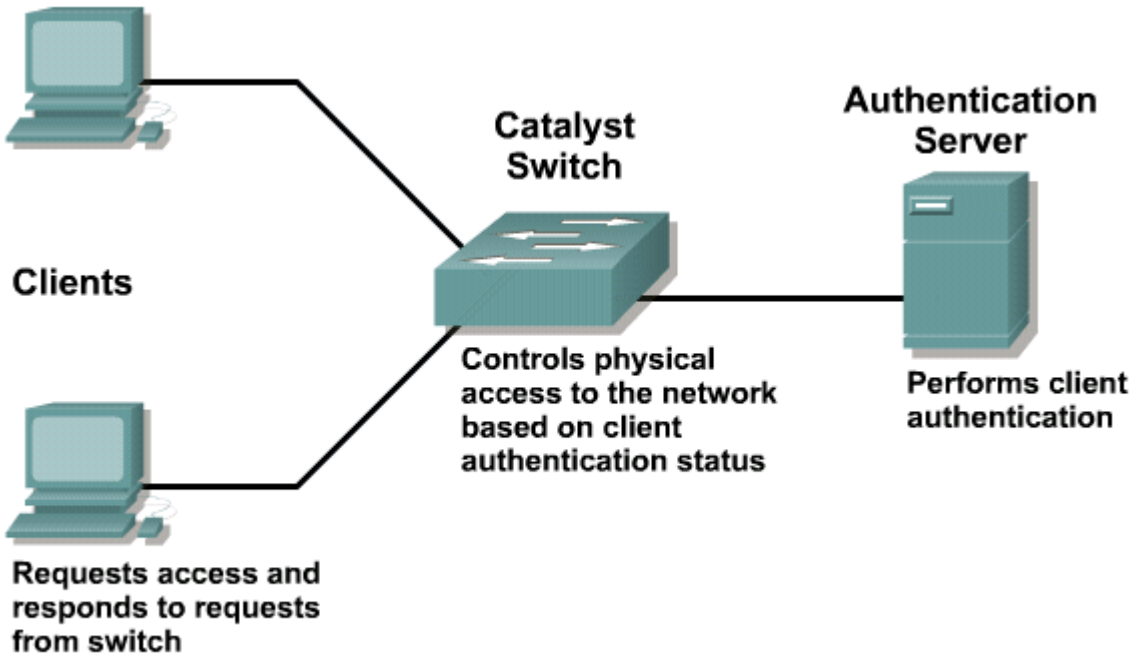
- **Bước 2:** Cấu hình phương thức chứng thực: RADIUS, TACAS+, hoặc Kerberos

- **Bước 3:** Cấu hình danh sách các phương thức dùng cho chứng thực: aaa athentication

9.1.9 Chứng thực 802. 1x Port Based

Chuẩn 802. 1x định nghĩa giao thức chứng thực và điều khiển truy cập port based, giao thức này ngăn chặn các thiệt bị không hợp lệ có thể truy cập vào mạng LAN thông qua switch. Server chứng thực chứng thực các máy trạm kết nối đến port switch trước khi các máy trạm này sử dụng dịch vụ.

Cho đến khi nào máy trạm được chứng thực,thì lúc này 802. 1x điều khiển truy cập mới chỉ cho phép traffic EAPOL đi qua port switch đi đến những máy trạm khác đã được kết nối. Sau khi chứng thực thành công, thì traffic thông thương có thể đi qua port switch.



Hình 9.1.9-1: Chứng thực Port Based

Với chứng thực 802. 1x port based, Các thiết bị trong mạng có vai trò như sau:

Client: là máy trạm yêu cầu truy cập đến dịch vụ LAN và Switch, đồng thời phản hồi các yêu cầu từ Switch. Máy trạm có thể chạy gói 802. 1x compliant client, ưu tiên dùng trong các máy có hệ điều hành Win XP và Win Vista.

Server chứng thực: Thực hiện chứng client. Các máy chủ chứng thực xác nhận danh tính của khách hàng và thông báo đến switch có hoặc không, client được ủy quyền để truy cập vào mạng LAN và các dịch vụ switch. Bởi vì switch hoạt động như Proxy, nên dịch vụ chứng thực sẽ trong suốt đối với client. Hệ thống bảo mật RADIUS với EAP chỉ hổ trợ chứng thực Server.

Switch: Điều khiển truy cập vật lý đến mạng dựa vào điều kiện chứng thực của client. Switch hoạt động như một proxy giữa client và server. Thông tin yêu cầu từ client sẽ được chứng thực ở server, server phản hồi thông tin đến client. Switch được cài đặt một gói phần mềm RADIUS agent, gói này chịu trách nhiệm cho việc đóng gói và mở gói theo định dạng EAP và tương tác với server chứng thực.

Switch port state xác định client nào sẽ được truy cập vào mạng. Với port state không cho phép traffic đi vào hoặc đi ra ngoại trừ gói tin có định dạng theo giao thức 802. 1x. Khi chứng thực thành công, cho tất cả các traffic lưu thông bình thường.

Nếu switch yêu cầu thức thực nhưng client không có hổ trợ giao thức 802. 1x. Do vậy port vẫn chưa được chứng thực và client cũng sẽ không truy cập được vào mạng.

Ngược lại nếu client chạy giao thức 802. 1x, client sẽ gửi một frame EAPOL start đến switch(không có chạy giao thức 802. 1x), Client sẽ không nhận được phản hồi và client gửi frame đến switch giống như port đã được chứng thực.

Bạn có thể điều khiển trạng thái chứng thực của port: sử dụng lệnh dotx port-control một số keywords:

Force-authorized: Tắt chứng thực theo giao thức 802. 1x, vì vậy port sẽ chuyển sang trạng thái authorized state không cần yêu gửi chứng thực. Port sẽ gửi và nhận traffic không cần chứng thực 802. 1x. Force-authorized là tùy chọn mặc định.

For-authorized: là lí do mà port vẫn còn ở trạng thái unauthorized state. Switch port bỏ qua tất cả các yêu cầu chứng thức. Switch không hổ trợ dịch vụ chưng thực clien thông qua interface.

Auto: Enable 802. 1x port-based authentication và nguyên nhân làm cho port khởi động với trạng thái unauthorized state, chỉ cho phép frame có định dạng theo EAPOL lưu thông qua port. Quá trình chứng thực chỉ được bắt đầu khi trạng thái của port từ down sang up và khi frame EAPOL-start được nhận. Switch yêu

cầu xác thực client và phản hồi lại thông điệp chứng thực giữa client và server chứng thực. Switch các định mỗi client thử truy cập ứng với địa chỉ MAC của client.

Khi client log off, client sẽ gửi EAPOL–logoff message, port sẽ chuyển sang trạng thái unauthorized state

Cấu hình 802. 1x:

```
Switch(config)#aaa new-model
```
• Enables AAA

```
Switch(config)#aaa authentication dot1x {default} method1
[method2...]
```
• Creates an 802.1x port-based authentication method list

```
Switch(config)#dot1x system-auth-control
```
• Globally enables 802.1x port-based authentication

```
Switch(config)#interface type slot/port
```
• Enters interface configuration mode

```
Switch(config-if)#dot1x port-control auto
```
• Enables 802.1x port-based authentication on the interface

Hình 9.1.9-2: Các dòng lệnh cấu hình 802. 1x

Triển khai 802. 1x port-based authentication:

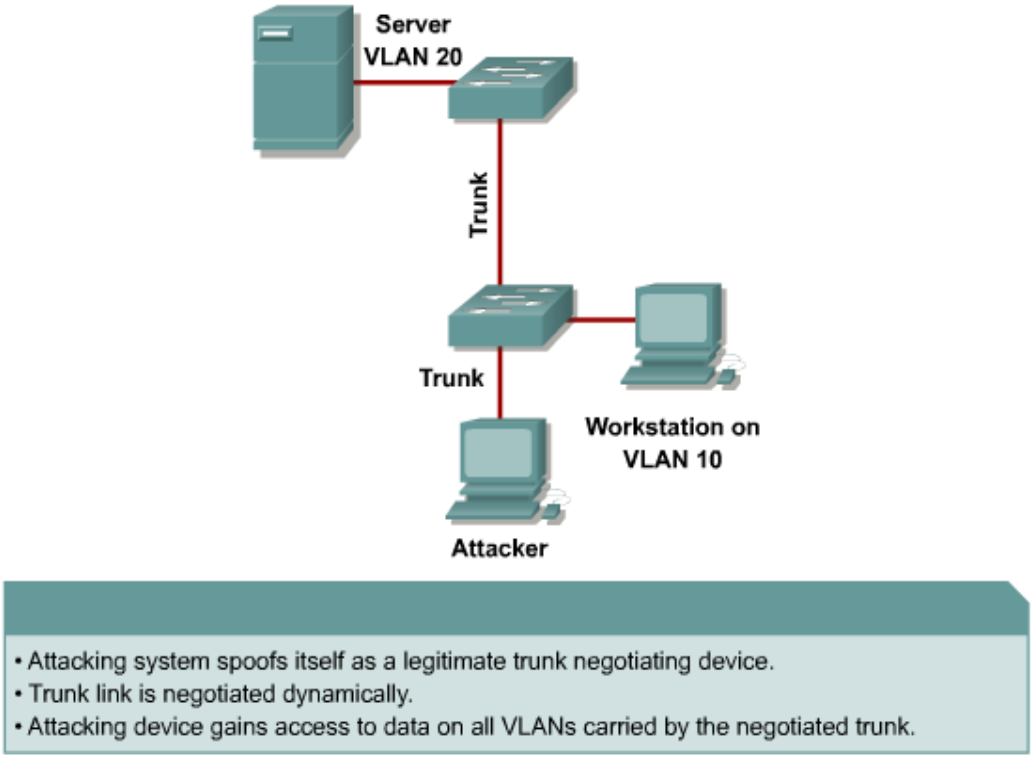
Step	Description
1.	Enable AAA. `Switch(config)#aaa new-model`
2.	Create an 802.1x port-based authentication method list. `Switch(config)#aaa authentication dot1x {default} method1 [method2...]`
3.	Globally enable 802.1x port-based authentication. `Switch(config)#dot1x system-auth-control`
4.	Enter interface configuration mode and specify the interface to be enabled for 802.1x port-based authentication. `Switch(config)#interface type slot/port`
5.	Enable 802.1x port-based authentication on the interface. `Switch(config-if)#dot1x port-control auto`
6.	Return to privileged EXEC mode. `Switch(config)#end`

Hình 9.1.9-3: Triển khai 802. 1x port-based authentication

9.2 Protecting Against VLAN Attacks

9.2.1 Explaining VLAN Hopping

VLAN hopping là một cuộc tấn công mạng, theo đó một hệ thống đầu cuối gửi packet đến, hoặc thu thập các packet , một VLAN không nên được truy cập vào hệ thống đầu cuối



Hình 9.2.1-1: Tấn công VLAN hopping

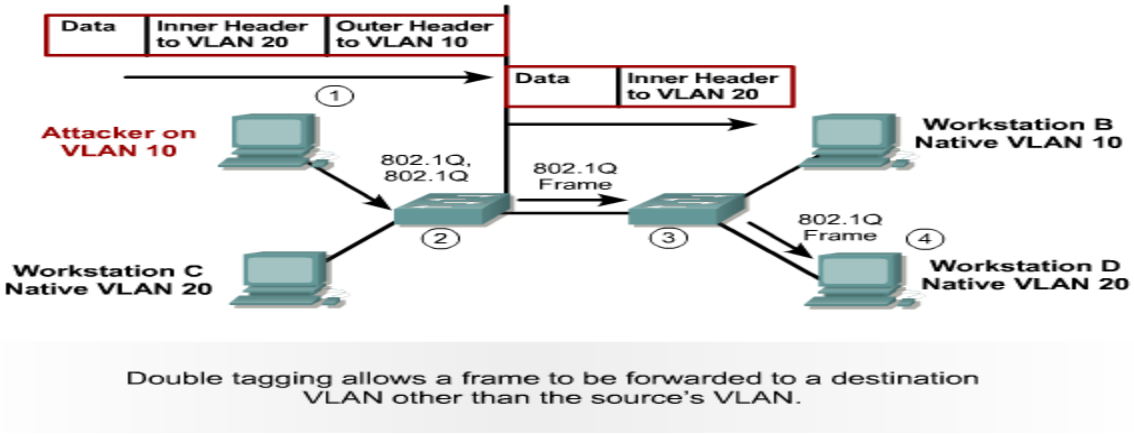
Điều này được thực hiện bằng cách gán invasive traffic với một VLAN ID hoặc bằng cách thỏa thuận một liên kết trunk để gửi hoặc nhận packet trên VLAN xâm nhập. VLAN hopping có thể được thực hiện bằng cách switch spoofing hoặc double tagging.

Trong một cuộc tấn công switch spoofing, những kẻ tấn công mạng cấu hình một hệ thống để spoof chính nó như là một chuyển đổi bằng cách thực hiện Inter-Switch Link (ISL) hoặc trunking 802.1Q, cùng với Dynamic Trunking Protocol (DTP), để thiết lập kết nối trunk đến switch . Bất kỳ switch port cấu hình như DTP tự động có thể trở thành một trunk port khi DTP packet tạo ra bởi các thiết bị tấn công nhận được, và do đó truy cập traffic đích cho bất kỳ VLAN hỗ trợ trunk. Các thiết bị gây hại có thể gửi packet, hoặc thu thập các packet từ, bất kỳ VLAN trên trunk.

Bảng sau mô tả quá trình xảy ra switch spoofing

Bước	Mô tả
1.	Kẻ tấn công được quyền truy cập vào một port trên switch và gởi thỏa thuận DTP vào một switch đang chạy DTP và tự động kích hoạt thỏa thuận (thường là, cấu hình mặc định.
2.	Kẻ tấn công và switch thiết lập trunking.
3.	Switch cho phép tất cả các VLAN (mặc định) di chuyển qua đường trunk.
4.	Kẻ tấn công gởi hoặc thu thập dữ liệu từ tất cả các VLAN trên đường trunk

Một phương thức khác của VLAN hopping là cho một workstation phát sinh frames với header 802.1Q để switch forward frame trên VLAN mà có thể không truy cập được để kẻ tấn công thông qua các phương tiện hợp pháp.



Hình 9.2.1-2: Tấn công VLAN hopping khác

Nếu double tagging frame là multicast, broadcast, hoặc là unknown destination,switch nhận frame ra tất cả các port có cùng VLAN(VLAN 10) như attacker's port native LAN. Switch lấy VLAN tag đầu tiên trước khi forward,cung cấp tag này kết hợp với VLAN của port mà nó được nhận. Bất kỳ truy cập port trên switch này đầu tiên được giao đến VLAN 10 sẽ nhận được khung với các tag VLAN thứ hai. Nếu trunk port cùng native VLAN(VLAN 10),switch không re-tag frame và đi đến việc chuyển đổi switch kế tiếp với tag VLAN thứ hai. Switch thứ hai tin rằng nguồn gốc frame từ VLAN khác (VLAN 20) và sau đó tràn ra tất cả các port active trong VLAN thứ hai. Switch nên forward frame trên đường trunk hoạt động VLAN thứ hai.

Nếu trunk port trên switch đầu tiên được gán một VLAN khác với của kẻ tấn công port,frame đơn giản là tràn ra tất cả các port hoạt động trong VLAN 10

trên cả hai switch (không có VLAN hopping). Lý do switch đầu tiên nên có tag 802.1Q frame với attacker's port để gửi qua trunk.

Bảng sau mô tả phương thức double-tagging của VLAN hopping

Bước	Mô tả
1.	Máy trạm A (native VLAN 10) gởi frame với header 802.1Q đến switch 1.
2	Switch 1 tháo tag ngoài và chuyển đến tất cả các port có cùng native VLAN.
3.	Switch 2 xác định frame theo thông tin tag trong khớp với VLAN ID 20
4.	Switch 2 chuyển frame ra ngoài tất cả các port thích hợp với VLAN 20, bao gồm port trunk.

Bảng 9.2.1-1 : Bảng mô tả phương thức double-tagging của VLAN hopping

9.2.2 Mitigating VLAN hopping

Các biện pháp để bảo vệ mạng từ VLAN hopping bao gồm một loạt các thực hành tốt nhất cho tất cả các cổng switch và một bộ các thông số để làm theo khi thiết lập một trunk port.

- Cấu hình tất cả các port chưa sử dụng như là các port truy cập để trunking mà không thể được thỏa thuận trên các liên kết này.
- Đặt tất cả các port chưa sử dụng ở tình trạng shutdown và liên kết với một VLAN chỉ cho port không sử dụng, không mang dữ liệu .
- Khi thành lập một liên kết trunk, cấu hình như sau:
    - Làm cho VLAN nguồn gốc khác nhau từ bất kỳ dữ liệu VLAN
    - Thiết lập trunking là "on", hơn là thỏa thuận
    - Xác định phạm vi VLAN để được tiến hành trên trunk.

```
Switch(config)#interface-range type mod/port-port
```
- Selects a range of interfaces to configure

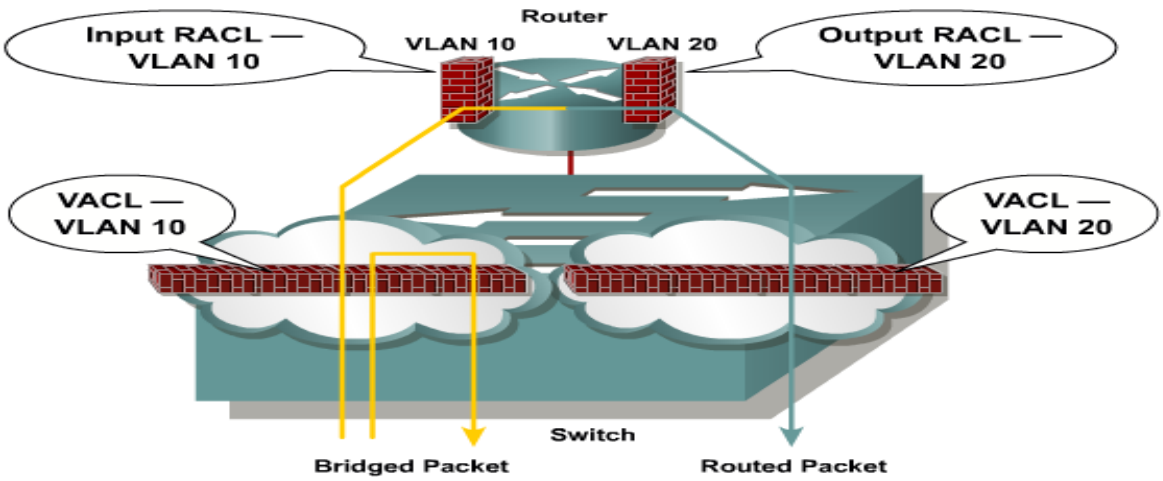
```
Switch(config-if)#switchport mode access
```
- Configures the ports as access ports and turns off DTP

```
Switch(config-if)#switchport access vlan vlan-id
```
- Statically assigns the ports to specific unused VLAN

Hình 9.2.2-1: Cấu hình mode access cho các port

Chú ý: Các lệnh cấu hình trong hình 1 không làm việc trên các port truy cập có hỗ trợ VoIP, vì họ sẽ được cấu hình như là trunk port. Tuy vậy, trên tất cả các port truy cập khác, tốt nhất là thực hành để áp dụng các lệnh này để giảm thiểu VLAN hopping.

9.2.3 VLAN Access Control List



Hình 9.2.3-1: Các ACL

Swich Cisco hỗ trợ 3 loại ACL:

- **Router access control list (RACL):** Áp dụng cho tầng 3 như là SVI hoặc là L3 routed port. Điều khiển truy cập đường đi traffic giữa VLAN. RACLs áp dụng trên interface định rõ hướng(inbound hoặc outbound). Chúng ta có thể truy cập một access list trên mỗi hướng. Để nâng cao thực thi trong Switch, RACLs được hỗ trợ trong bộ nhớ địa chỉ (TCAM)

- **Port access control list (PACL):** Áp dụng trên Layer 2 switch port,trunk port,trên EtherChannel port. PACLs thực thi access control trên traffic vào tại Layer 2. Với PACLs,chúng ta có filter IP traffic bằng cách sử dụng IP access list và non-IP traffic bằng sử dụng MAC address. Khi chúng ta áp

dụng PACL đến trunk port,filter traffic trên tất cả các VLAN hiện diện trên trunk port.

- **VLAN access control list (VACL):** Hổ trợ phần mềm Cisco multiplayer switch. Filtering dựa trên Layer 2 hoặc Layer 3 với VLAN. Không giống như RACLs, VACLs không được xác định bởi hướng

Catalyst switch hỗ trợ bốn ACL tra cứu cho mỗi packet: an toàn ACL cho input và output, và input và output Quality of Service (QoS) ACL.

Catalyst switch sử dụng hai phương pháp thực hiện một hợp nhất: độc lập và phụ thuộc. Với lệnh hợp nhất độc lập, ACLs được chuyển đổi từ một loạt các hành động tự-phụ thuộc vào một tập các lệnh độc lập mask và pattern. Việc truy cập kết quả kiểm soát nhập cảnh (ACE) có thể rất lớn. Việc hợp nhất là bộ xử lý và bộ nhớ chuyên sâu.

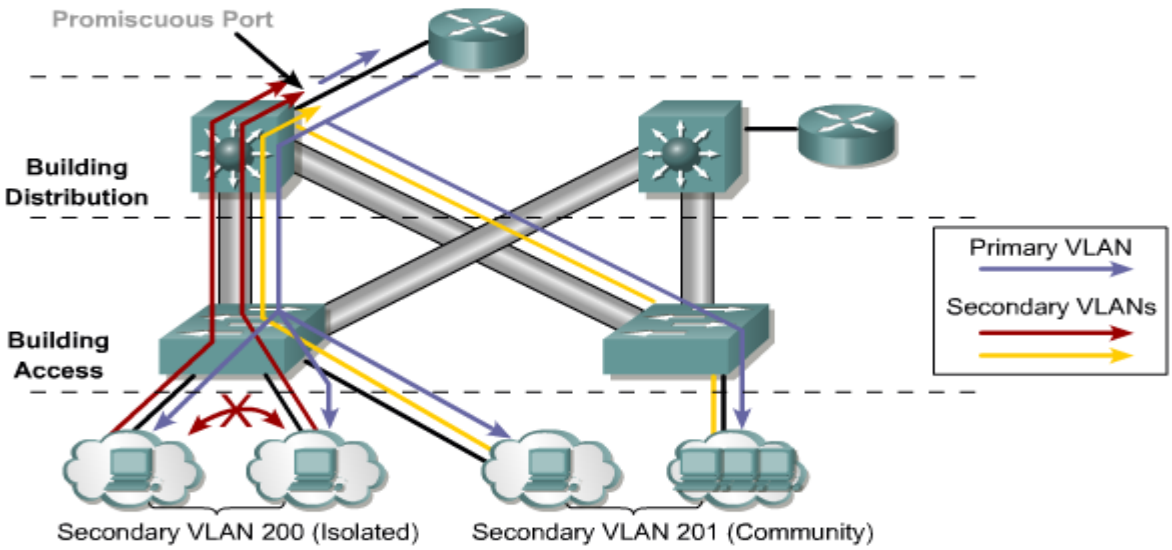
Kết hợp các order-dependent được nâng cao trên một số Catalyst switch trong đó giữ lại một số khía cạnh về order-dependent. Các tính toán là nhanh hơn nhiều và ít bộ xử lý chuyên sâu.

RACLs được hỗ trợ trong phần cứng thông qua các tiêu chuẩn IP ACLs và IP ACLs mở rộng, với permit và deny actions. Quy trình ACL là một phần bên trong của quá trình xử lý gói tin. ACL được lập trình trong phần cứng. Tra cứu xảy ra trong pipeline ACL được cấu hình hay không. Với RACLs, thống kê danh sách truy cập và đăng nhập không được hỗ trợ.

9.2.4 Private VLANs and Protected Ports

Internet service providers (ISP) thường có nhiều thiết bị từ khách hàng, cũng như các máy chủ riêng của họ, trên một khu phi quân sự (DMZ) phân đoạn hoặc VLAN. Như vấn đề an ninh, sẽ trở thành cần thiết để cung cấp traffice riêng biệt giữa các thiết bị, mặc dù chúng có thể tồn tại trên Layer 3 và VLAN.

Catalyst 6500/4500/3750/3560 switches thực thi VLAN riêng để một số switch share và một số riêng biệt,mặc dù các port tồn tại trên cùng VLAN.



Hình 9.2.4-1: Switch 2960 hỗ trợ "protected ports" (tương tự như PVLAN trên các switch cơ bản)

Các giải pháp truyền thống để giải quyết các yêu cầu này là ISP cung cấp một VLAN cho mỗi khách hàng, với mỗi VLAN có subnet riêng của IP của nó. Một Layer 3 sau đó cung cấp thiết bị tương liên giữa các VLAN và các điểm đến Internet.

Đây là những thách thức với các giải pháp truyền thống này:

- Hỗ trợ một VLAN riêng biệt cho mỗi khách hàng có thể yêu cầu một số lượng lớn interfaces trên các thiết bị nhà cung cấp dịch vụ mạng.
- Spanning tree trở nên phức tạp hơn với nhiều lần lặp VLAN.
- Network address phải được chia thành nhiều subnet.
- Nhiều ứng dụng ACL được yêu cầu để duy trì an ninh trên nhiều VLAN, kết quả là tăng phức tạp trong quản lý.

PVLANs và protecteds ports cung cấp riêng biệt cho Layer 2 giữa các port cùng VLAN. Riêng biệt này giúp loại bỏ sự cần thiết cho một VLAN riêng biệt và subnet IP cho mỗi khách hàng.

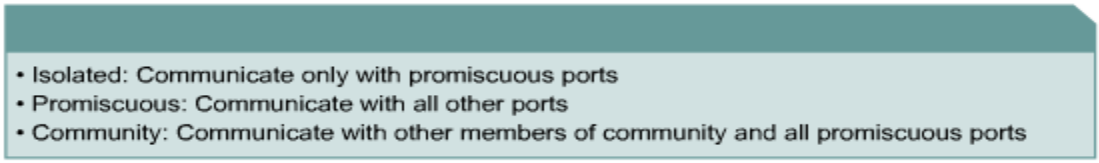
Một protected port không forward nhiều traffic (unicast,broadcast,multicast) đến port bất kỳ là proteced port. Traffic không được forward giữa các protected ports tại Layer 2;tất cả traffic qua giữa các protected port phải được forward qua

thiết bị Layer 3. Cách hành xử forward giữa các protected port và non-protected port không bị ảnh hưởng và xử lý bình thường.

Ví dụ trong hình cho thấy làm thế nào để cấu hình Fast Ethernet 0 / 1 interface như là một protected port và kiểm tra cấu hình.

PVLANs được hỗ trợ trên Catalyst 3. 560, 3. 750, 4. 500 và 6. 500 Switch.

Một port trong PVLAN có thể được một trong ba loại:



Hình 9.2.4-2: Các loại port trong PVLAN

- Isolated: Layer 2 tách từ các port khác cùng VLAN,ngoại trừ port promiscuous(không phân loại). Traffic được nhận từ isolated port chỉ được forward đến promiscuous ports.

- Promiscuous: giao tiếp với tất cả các port trong PVLAN,bao gồm community và isolated port. Default gateway cho segment có thể lưu trữ trên promiscuous ports, cho rằng tất cả các thiết bị trong các PVLAN nhu cầu giao tiếp với port đó.

- Community: Giao tiếp với nhau và với cổng promiscuous của họ. Các interfaces này đang bị cô lập ở Layer 2 từ tất cả interfaces khác trong các community khác, hoặc tại isolated port trong PVLAN.

Lưu ý: Trunks có thể hỗ trợ VLAN mang traffic giữa các isolated,community,và promiscuous ports,isolated và community port traffic phải được vào hoặc rời switch qua trunk interface.

Ports PVLAN được liên kết với một tập hợp các hỗ trợ VLANs được sử dụng để tạo cấu trúc PVLAN. PVLAN A sử dụng VLAN theo ba cách:

- **Primary VLAN:** Mang traffic từ promiscuous port đến isolated port,community và promiscuous ports khác trong cùng primary VLAN.

- **Isolated VLAN:** Mang traffic từ isolated ports đến promiscuous port.

- **Community VLAN:** Mang traffic giữa các community ports và đến promiscuous ports. Chúng ta có thể cấu hình nhiều VLANs trong PVLAN.

Isolated và community VLANs được gọi là VLANs secondary. Chúng ta có thể mở rộng PVLans qua nhiều thiết bị bằng cách trunking priamry,isolated,và community VLANs đến các thiết bị khác hổ trợ PVLANs.

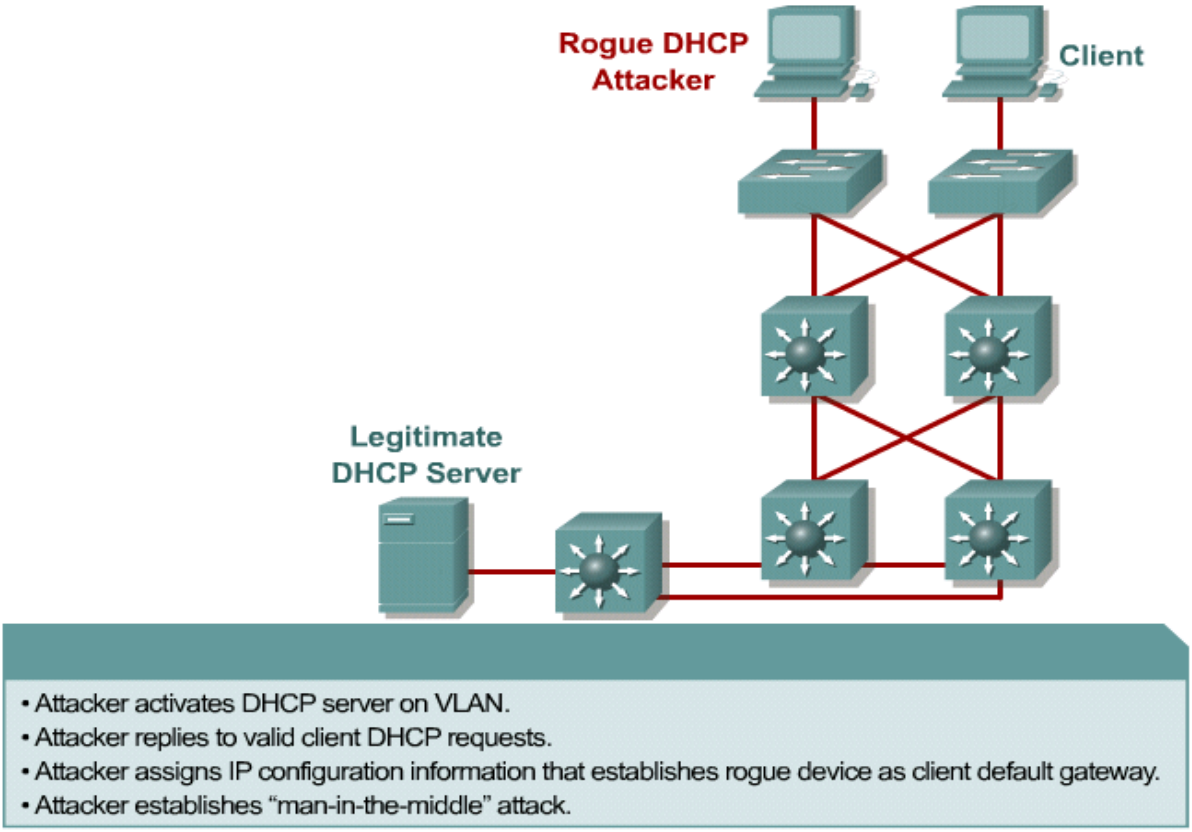
Chú ý: Một promiscuous port chỉ phục vụ trên primary VLAN. Một promiscuous port có thể phục vụ một isolated hoặc nhiều community VLANs.

Với promiscuous port,chúng ta có thể kết nối một loạt các thiết bị như access points đế có PVLAN. Ví dụ: bạn có thể kết nối một port promiscuous vào port server để kết nối một VLAN riêng biệt hoặc một số community VLAN cho server. Một cân bằng tải có thể được sử dụng để cân bằng tải các máy chủ hiện diện trong community hoặc cô lập VLAN, hoặc bạn có thể sử dụng một promiscuous port để theo dõi hoặc sao lưu tất cả các máy chủ PVLAN từ adminstration workstation.

9.3 Protecting Against Spoof Attacks

9.3.1 Describing a DHCP Spoof Attack

Một trong những cách một mà kẻ tấn công có thể được truy cập vào mạng lưới là để các đáp ứng spoof đó sẽ được gửi bởi một máy chủ DHCP hợp lệ. Các thiết bị giả mạo DHCP trả lời cho khách hàng yêu cầu DHCP. Các máy chủ hợp pháp có thể trả lời là tốt, nhưng nếu các thiết bị giả mạo là trên phân đoạn tương tự như khách hàng, trả lời của mình cho khách hàng có thể đến đầu tiên. DHCP trả lời của kẻ xâm nhập cung cấp một địa chỉ IP và hỗ trợ thông tin chỉ định kẻ đột nhập như là default gateway hoặc Domain Name System (DNS) server. Trong trường hợp của gateway, các khách hàng chuyển tiếp các gói tin đến thiết bị bị tấn công, mà lần lượt gửi chúng đến đích mong muốn. Điều này được gọi là một cuộc tấn công "kẻ ở giữa”, và nó có thể đi hoàn toàn không bị phát hiện có kẻ xâm nhập chặn dòng chảy dữ liệu qua mạng.



Hình 9.3.1-1: Tấn công DHCP Spoof

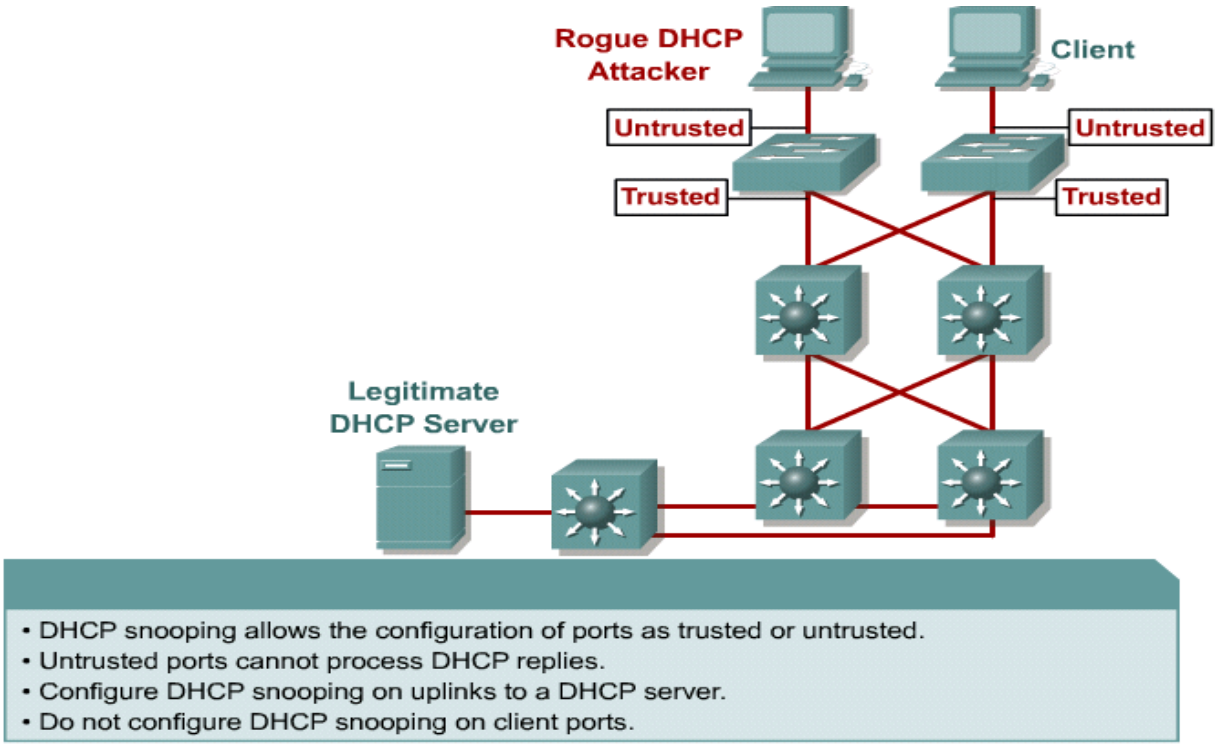
Bảng sau mô tả cách thức DHCP giả mạo tấn công:

Bước	Mô tả
1.	Kẻ tấn công giả làm một DHCP server của switch port
2.	Client broadcast một yêu cầu cho cấu hình DHCP
3.	DHCP server đểu đáp ứng trước DHCP server thật, gán một IP do kẻ tấn công đặt ra cho thông tin cấu hình
4.	Các gói tin của host thì được chuyển hướng đến địa chỉ của kẻ tấn công như là nó giả lập một default gateway làm cho lầm lẫn cung cấp địa chỉ DHCP cho client

Bảng 9.3.1-1 : Bảng mô tả cách thức DHCP giả mạo tấn công:

9.3.2 Describing DHCP Snooping

DHCP snooping là một chức năng của Cisco Catalyst xác định các cổng chuyển đổi có thể đáp ứng các yêu cầu DHCP.



Hình 9.3.2-1: Mô tả DHCP Snooping

Port được xác định là đáng tin cậy và không tin cậy. Port tin cậy có thể có nguồn tất cả các tin nhắnDHCP, trong khi port không tin cậy chỉ có nguồn của tin nhắn yêu cầu. Port tin cậy có thể là DHCP server hoặc có thể là một đường lên phía máy chủ DHCP. Nếu một thiết bị giả mạo trên một port không tin cậy gửi một đáp ứng DHCP vào mạng, port bị shut down.

Port không tin cậy là những port không được cấu hình đáng tin cậy. Một bảng DHCP ràng buộc được xây dựng cho các port không tin cậy. Mỗi entry chứa địa chỉ MAC client, địa chỉ IP, thời gian cho thuê, loại ràng buộc, số lượng VLAN, port ID được ghi nhận khi client thực hiện các yêu cầu DHCP. Bảng này sau đó được sử dụng để lọc dữ liệu DHCP. Từ một snooping DHCP, port không đáng tin cậy không được gửi bất kỳ đáp ứng DHCP, như DHCPOFFER, DHCPACK, hoặc DHCPNAK.

Với tính năng DHCP-82 tùy chọn kích hoạt trên switch, port-to-port DHCP broadcast thực hiện khi các port của client có một VLAN duy nhất. Trong quá trình trao đổi từ client đến máy chủ, việc broadcast các yêu cầu từ client đến với port access trên VLAN dược chặn bởi một đại lý relay chạy trên switch và không flood cho các client khác trên cùng một VLAN. Các relay agent chèn thêm các thông tin vào bên trong các gói yêu cầu DHCP, chẳng hạn như port yêu cầu có nguồn gốc từ đâu, và sau đó chuyển tiếp nó tới máy chủ DHCP. Trong quá trình trao đổi máy chủ đến khách hàng, các DHCP server (kích hoạt tùy chọn-82) gửi một gói trả lời

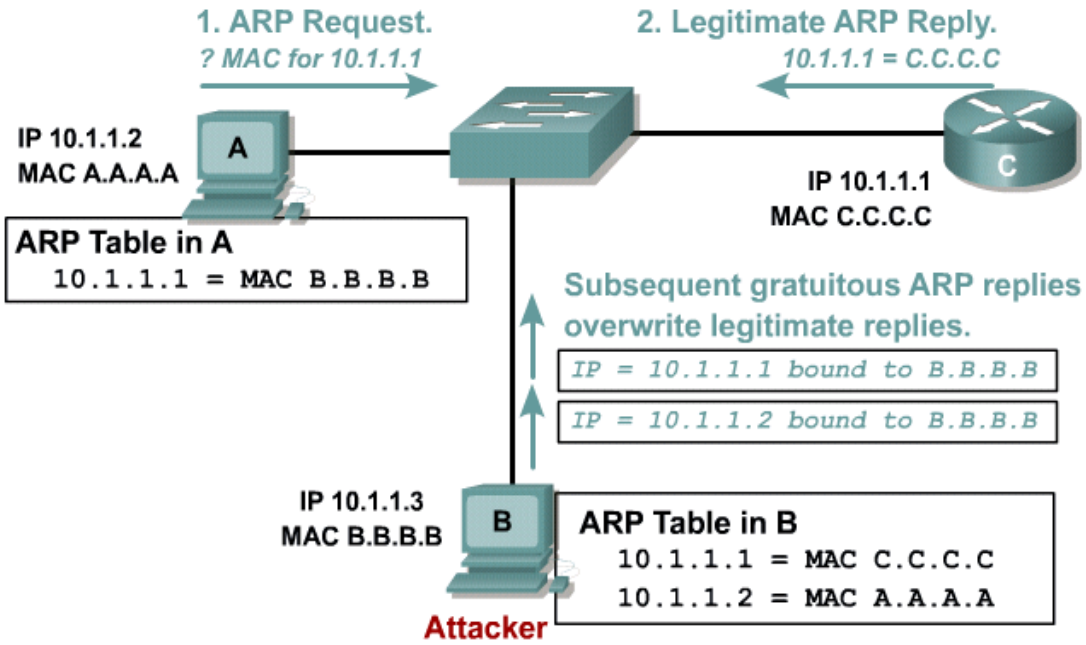
có chứa tùy chọn-82. Các relay agent sử dụng thông tin này để xác định được port kết nối với các khách hàng yêu cầu và tránh chuyển tiếp các trả lời cho toàn bộ VLAN.

Ngữ cảnh cấu hình	Mô tả
1.	Cấu hình DHCP snooping toàn bộ.
2.	Cấu hình port tin cậy
3.	Cấu hình gán tùy chọn-82 (mặc định kích hoạt ở bước 2)
4	Cấu hình tỷ lệ giới hạn trên port không tin cậy
5.	Cấu hình DHCP snooping cho các VLAN được chọn

Bảng 9.3.2-1 : Bảng mô tả cấu hình chống DHCP Snooping

9.3.3 Describing ARP Spoofing

Trong một hoạt động ARP bình thường, một host gửi một broadcast để xác định địa chỉ MAC của một host khác với một địa chỉ IP cụ thể. Các thiết bị với địa chỉ IP đó trả lời địa chỉ MAC của nó. Các host nguồn lưu giữ các đáp ứng ARP, sử dụng nó để gán header Layer 2 của gói tin gửi đến địa chỉ IP. Bằng cách giả mạo một trả lời ARP từ một thiết bị hợp pháp với một ARP cho không, thiết bị tấn công giả như là đích mả người gởi cần gởi . Các trả lời ARP từ kẻ tấn công làm cho người gửi lưu trữ các địa chỉ MAC của thông tin của tấn công trong bộ nhớ cache ARP của nó. Tất cả các gói tin gởi cho đại chỉ IP này được chuyển tiếp qua cho kẻ tấn công.



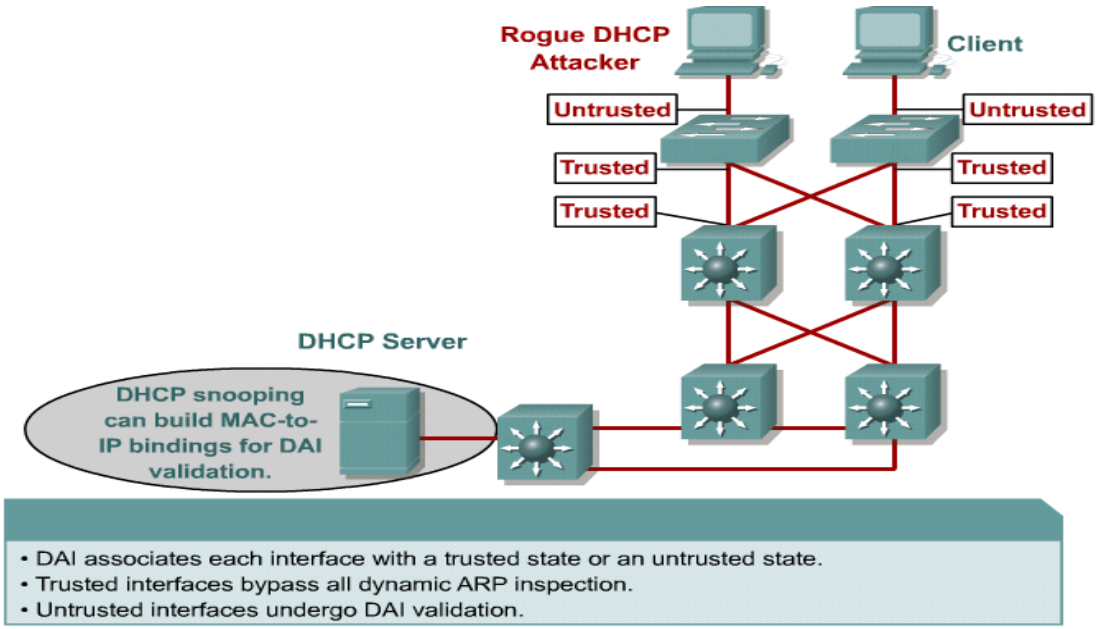
Hình 9.3.3-1: Mô tả ARP Spoofing

Bước	Mô tả
1.	Host A gởi yêu cầu ARP cho địa chỉ MAC của host C.
2.	Router C trả lời với địa chỉ MAC van IP của nó. C cũng cập nhật bộ nhớ đệm ARP của nó
3.	Host A gắn địa chỉ MAC của host C với địa chỉ IP trên bộ nhớ đệm ARP của nó.
4.	Host B (kẻ tấn công) gởi một ARP có gắn địa chỉ MAC của B với IP của C
5.	Host A cập nhật ARP với địa chỉ MAC cua B được gán với IP của C.
6.	Host B gởi một ARP gán địa chỉ MAC cua B với IP của A
7.	Router C cập nhật ARP cache với địa chỉ MAC của B gán cho IP của A
8.	Gói tin bây giờ vận chuyển ngang qua kẻ tấn công (B)

Bảng 9.3.3-1 : Bảng mô tả Mô tả ARP Spoofing

9.3.4 Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) xác định tính hợp lệ của một gói ARP dựa trên địa chỉ MAC-gán địa chỉ IP được lưu trữ trong một cơ sở dữ liệu DHCP snooping. Thêm vào đó, DAI có thể xác nhận các gói tin ARP dựa trên ACL với host cấu hình cấu hình địa chỉ IP tĩnh.



Hình 9.3.4-1: Mô tả DAI(Dynamic ARP Inspection)

Để ngăn chặn ARP spoofing hay "nhiễm độc", một switch phải đảm bảo rằng chỉ có yêu cầu van đáp ứng ARP hợp lệ được chuyển tiếp. Để đảm bảo rằng chỉ có yêu cầu và đáp ứng ARP hợp lệ DAI có những hành động sau đây:

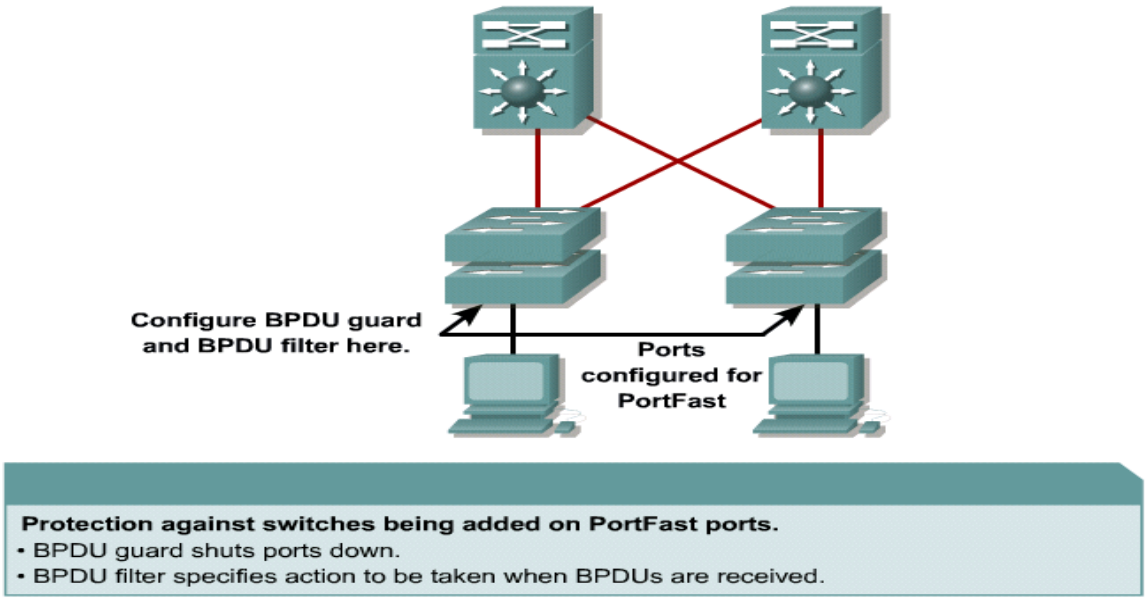
- Chuyển tiếp gói tin ARP nhận được trên interface đáng tin cậy mà không có bất kỳ kiểm tra
- Chặn tất cả các gói ARP trên các cổng không tin cậy
- Kiểm tra mỗi gói tin bị chặn xem có một chuyển đổi rang buộc IP-tới-MAC hợp lệ trước khi chuyển tiếp các gói tin có thể cập nhật bộ nhớ cache ARP địa phương.
- Hủy, ghi chú, hoặc hủy và ghi chú các gói tin ARP không hợp lệ. Nói chung, tất cả các access switch nên được cấu hình như không tin cậy và tất cả các port trên switch kết nối tới switch khác là đáng tin cậy. Tất cả các gói tin ARP đi vào mạng từ một distribution hay core switch có thể bỏ qua kiểm tra không cần xác nhận thêm.

Bạn cũng có thể sử dụng DAI để thiết lập giới hạn tốc độ của các gói ARP và sau đó vô hiệu hóa interface nếu vượt quá tỷ lệ.

9.4 STP Security Mechanisms

9.4.1 Protecting the Operation of STP

Cisco cung cấp các tính năng chống loop cho spanning tree bằng cách tạo port được kích hoạt chế độ PortFast. Trong một cấu hình đúng, PortFast sẽ được kích hoạt chỉ trên các thiết bị hỗ trợ thiết bị đầu cuối chẳng hạn như máy chủ và máy trạm. Chắc rằng gói BPDU từ một switch không được nhận được trên một interface PortFast. Tuy nhiên, điều này phải xảy ra, BPDU guard và BPDU filter cung cấp bảo vệ. Cả BPDU guard và BPDU filter có thể được cấu hình trên hoàn toàn trên tất cả các port được cấu hình PortFast hoặc trên các port độc lập.



Hình 9.4.1-1: Cấu hình BPDU guard và BPDU filter trên các port

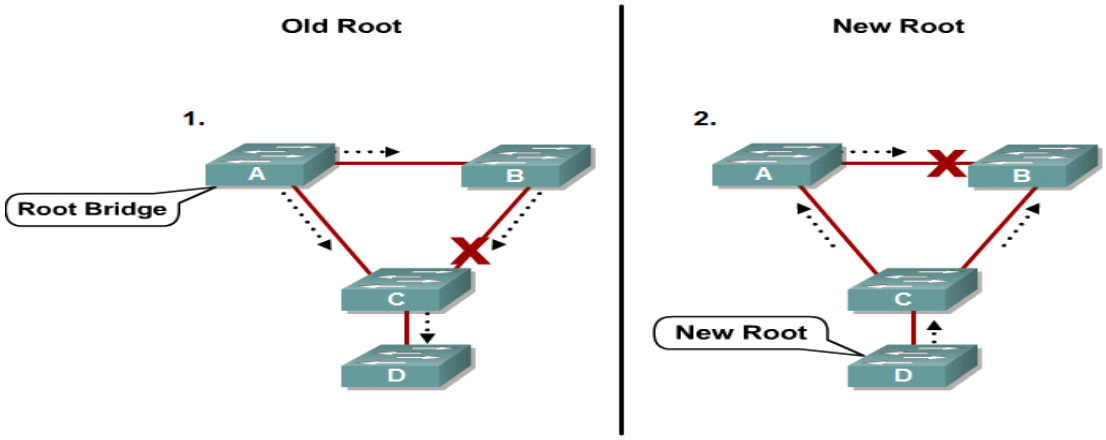
BPDU guard bảo vệ các mạng chuyển từ những vấn đề mà có thể được gây ra bởi việc nhận các gói BPDU trên port mà không cần phải nhận được chúng. Việc nhận BPDUs bất ngờ có thể được tình cờ hoặc có thể là một phần của một nỗ lực bất hợp pháp để thêm một switch vào mạng.

PortFast BPDU filter có tác dụng như thế switch xác nhận các gói BPDU được nhận trên port cấu hình PortFast. Chức năng của nó khác nếu nó được cấu hình trên toàn bộ hoặc cho mỗi cổng cơ sở.

Root guard bảo vệ chống lại các switch bên ngoài mạng cố gắng để trở thành root brigde bằng cách chặn truy cập của nó cho đến khi nhận BPDUs của nó chấm dứt.

9.4.2 Root Guard

Root guard giới hạn các port out trên switch root bridge. Nếu một port được thiết lập root guard nhận các gói BPDU được gởi bởi root bridge, port đó chuyển sang trạng thái root-inconsistent, có tác dụng như trạng thái listening của STP. Không có dữ liệu sẽ được chuyển qua port này.



Hình 9.4.2-1: Thay đổi port bị block khi có Root mới

Trong hình trên, switch A và B ở lớp core của mạng. Switch A là root bridge cho một VLAN. Switch C là một switch ở lớp access. Mối liên hệ giữa B và C là chặn ở bên C. Đường đi của các gói STP BPDU được hiển thị với mũi tên. Bên trái, thiết bị D bắt đầu tham gia vào STP. Nếu độ ưu tiên của switch D thấp hơn so với root bridge hiện hành, switch D sẽ được bầu làm root bridge. Điều này sẽ làm cho các liên kết kết nối switch A và B bị chặn, làm cho tất cả lưu lượng từ switch B đến C trong lớp access, rõ ràng là không thuận lợi. Nếu root guard được cấu hình trên port của switch C mà switch D kết nối vào, switch D sẽ không bao giờ được bầu làm root bridge.

Root guard được cấu hình cho mỗi port cơ sở. Nếu một gói BPDU cấp trên được nhận vào port, root guard đặt port vào trạng thái root-inconsistent. Khi switch D dừng gởi các gói BPDU cấp trên, port được unblock và chuyển sang các trạng thái của STP như các port khác. Phục hồi không cần can thiệp. Một port root guard là port ở trạng thái designated. Khi root guard được kích hoạt trên một port, switch không cho phép post đó trở thành một root port trong STP. Port trở lại thành designated port trong STP.

Root guard cần được kích hoạt trên tất cả các cổng, nơi root bridge không phải là dự đoán. Trong ví dụ, root guard nên được cho phép như sau:

- Switch A: cổng kết nối đến switch C
- Chuyển sang B: cổng kết nối đến switch C
- Chuyển sang C: cổng kết nối đến switch D

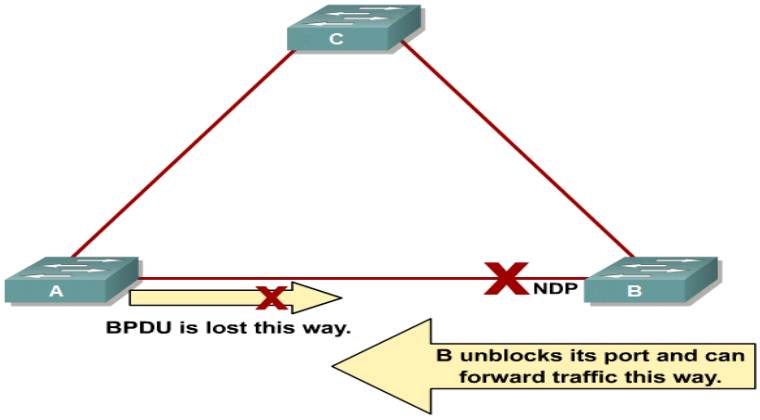
Khi root guard khóa một port thì xuất hiện tin nhắn:

%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77. Moved to root-inconsistent state

9.5 Preventing STP Forwarding Loops

9.5.1 Unidirectional Link Detection

Một liên kết đơn hướng xảy ra khi lưu lượng được truyền đi giữa các láng giềng theo một hướng duy nhất. Đơn hướng có thể gây ra loop trong spanning tree. Unidirectional Link Detection (UDLD-Dò tìm lien kết đơn hướng) cho phép các thiết bị phát hiện các tình trạng liên kết đơn hướng khi cơ chế Layer 1 không làm, và cung cấp khả năng tắt các interface bị ảnh hưởng.



Hình 9.5.1-1: Mất gói BPDU nếu được gởi trên một liên kết đơn hướng

UDLD là một giao thức ở Lớp 2 làm việc với các cơ chế Lớp 1 để xác định tình trạng vật lý của một liên kết. Ví dụ, nếu một sợi cáp quang trong cặp một là bị ngắt kết nối, cơ chế tự đàm phán Lớp 1 sẽ không cho phép liên kết hoạt động hoặc ở lại. Nhưng nếu cả hai sợi hoạt động, UDLD quyết định nếu lưu lượng truyền hai chiều giữa những neighbor phù hợp.

Switch định kỳ truyền các gói tin UDLD trên một interface có kích hoạt UDLD. Nếu các gói tin không trở lại trong một khoảng thời gian cụ thể, liên kết được gắn cờ là đơn hướng, và interface được tắt. Các thiết bị trên cả hai đầu của

liên kết phải hỗ trợ UDLD để thành công xác định và vô hiệu hóa lien kết đơn hướng.

Chức năng của UDLD là để ngăn chặn truyền thông một chiều giữa các thiết bị lân cận. Khi UDLD phát hiện một giao tiếp một chiều, nó có thể làm một trong hai điều, tuỳ thuộc vào việc UDLD được cấu hình trong chế độ bình thường hay tích cực. Trong chế độ bình thường, UDLD thay đổi port được kích hoạt UDLD thành trạng thái chưa xác định khi nó dừng lại nhận được tin nhắn UDLD từ hàng xóm trực tiếp kết nối của nó. Chế độ tích cực thực hiện tám nỗ lực để thiết lập lại mối quan hệ hàng xóm UDLD trước khi vô hiệu hóa các port. Chế độ tích cực là phương pháp thích hợp của cấu hình UDLD và là chế độ duy nhất có thể phát hiện tình trạng của UDLD trên cáp xoắn đôi.

UDLD đích sử dụng MAC đích 01-00-0C-cc-cc-cc với loại giao thức SNAP HDLC 0x0111.

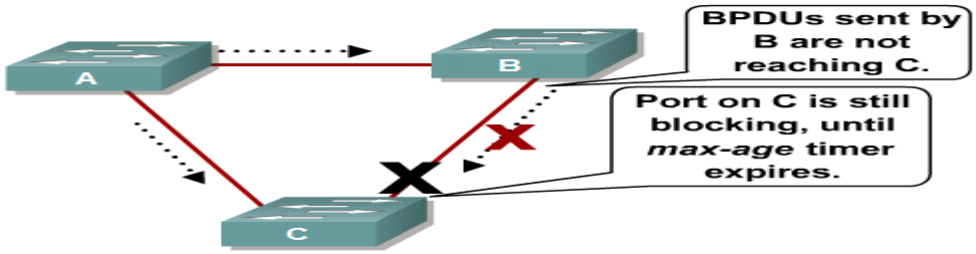
Bảng mô tả các trạng thái mặc định cho các UDLD trên cơ sở toàn bộ và interface.

Đặc điểm	**Mặc định**
Kích hoạt trang thái UDLD toàn bộ	Không kích hoạt toàn bộ
Kích hoạt UDLD trên mỗi interface cho môi trường cáp quang	Kích hoạt trên tất cả các interface Ethernet có cáp quang
Kích hoạt UDLD cho mỗi interface cho môi trường cáp xoắn đôi	Không có kích hoạt trên tất cả các interface Ethernet 10/100 van 1000BASE-TS

Bảng 9.5.1-1 : Bảng mô tả các trạng thái mặc định cho các UDLD trên cơ sở toàn bộ và interface.

9.5.2 Loop Guard

Giống như UDLD, loop guard cung cấp bảo vệ cho STP khi một liên kết là đơn hướng và BPDUs đang được gửi đi, nhưng không nhận được, vào một liên kết được xem là hoạt động.



Hình 9.5.2-1: Gói tin từ B không gởi tới được C vì C vẫn đang bị block

Nếu không có loop guard, một port bị block sẽ chuyển sang trạng thái forwarding khi nó ngừng nhận các gói BPDU. Nếu loop guard được kích hoạt và liên kết không nhận BPDUs, interface chuyển vào trạng thái loop-inconsistent blocking. Khi loop guard khóa một port, thông báo này được tạo ra hoặc log file:

SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.

Khi một gói BPDU được nhận trên một port có cấu hình loop guard ,port mà đang ở trạng thái loop-inconsistent, port chuyển sang trạng thái phù hợp được xác định bởi các chức năng bình thường của spanning tree. Phục hồi này không đòi hỏi có sự can thiệp của người dùng. Sau khi phục hồi có thông báo này:

SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.

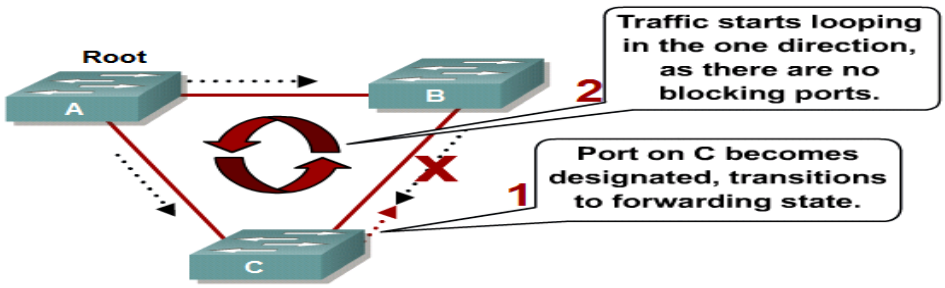
Các tính năng của loop guard bảo vệ chống lại loop spanning tree bằng cách phát hiện một liên kết đơn hướng. Với một liên kết đơn hướng, một port trong những liên kết thành viên thì hoạt động trong trạng thái up và truyền nhưng không nhận được lưu lượng. Đồng thời, các liên kết thành viên khác hoạt động chính xác. Loop guard được kích hoạt trên các port được tham gia spanning tree và đang dự phòng ở Lớp 2. Khi switch dừng tiếp nhận các gói BPDU vào root port hoặc blocking port của nó, nó chuyển trạng thái port thành loop-inconsistent, không cho lưu lượng vượt qua.

Loop guard được cấu hình trên mỗi cổng trên các phiên bản hệ điều hành sớm hơn so với hệ điều hành Catalyst 7.1 (1).

Loop guard không tương thích với root guard. Ngoài ra, loop guard không nên được kích hoạt trên port PortFast.

Trong một bó EtherChannel, UDLD tắt chỉ liên kết vật lý bị lỗi. Loop guard, tuy nhiên, hành xử khác nhau bởi vì port hoạt động đầu tiên EtherChannel được sử dụng cho BPDU và các port khác thì không. Nếu port đầu tiên có một liên kết

đơn hướng lỗi, loop guard chuyển trạng thái của tất cả các liên kết trong kênh thành loop-inconsistent. Đây không phải là một kết quả mong muốn, bởi vì sự kế thừa dự phòng có được thông qua kênh bị mất.

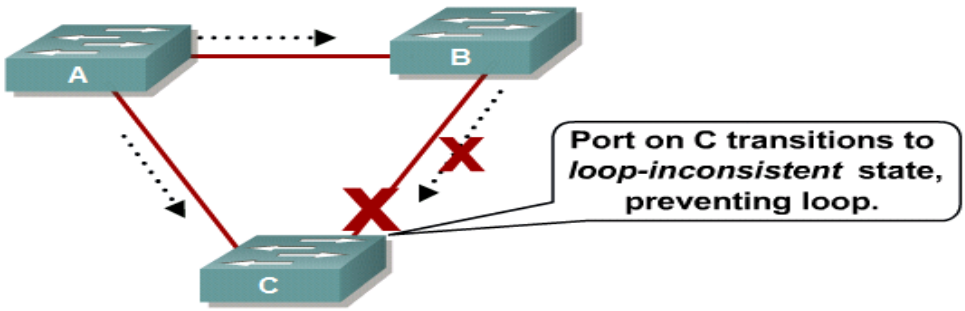


Hình 9.5.2-2: Trafic dang bị loop

Trong ví dụ minh họa trong hình trên, switch A là root bidge. Do một lỗi liên kết đơn trên kết nối giữa các switch B và C, switch C không nhận các gói BPDU từ switch B.

Nếu không có loop guard, port blocking trên C chuyển sang trạng thái listening STP khi bộ đếm thời gian hết hạn tuổi tối đa và sau đó sang trạng thái forwarding trong hai lần trì hoãn thời gian chuyển tiếp, và một vòng lặp được tạo ra.

Hình sau thể hiện loop guard hoạt động như thế nào để ngăn chặn loop trong một lỗi liên kết đơn



Hình 9.5.2-3: Port tren switch C chuyển trạng thái để ngăn loop

Với loop guard được kích hoạt, các blocking port trên switch C chuyển vào trạng thái loop-inconsistent khi hết thời gian max age. Bởi vì một port ở trạng thái loop-consistent không cho lưu lượng người dùng vượt qua, không có loop được tạo ra. Trạng thái loop-inconsistent là hiệu quả như blocking port.

9.5.3 Preventing STP Failures Due to Unidirectional Links

Các chức năng của UDLD và loop guard là các phần cùng nhau ngăn chặn các lỗi STP do liên kết đơn hướng gây ra. Hai tính năng này là khác nhau trong cách giải quyết vấn đề và cũng trong các chức năng.

Bảng sau nêu ra các sự khác biệt quan trọng :

	Loop guard	**UDLD**
Cấu hình	Mỗi port	Mỗi port
Hành động chi tiết	Mỗi VLAN	Mỗi port
Tự động phục hồi	Có	Có, với ngắt kích hoạt lỗi hết giờ
Bảo vệ chống lại các lỗi STP gây ra bởi liên kết đơn hướng	Có, khi kích hoạt trên tất cả root van alternative port trong mô hình dự phòng	Có, khi kích hoạt trên tất cả trên các link trong mạng dự phòng.
Bảo vệ chống lại các lội gây ra bởi những vấn đề phần mềm, hậu quả là các designated switch không gởi gói BPDU	Có	Không
Bảo vệ khỏi mất dây	Không	Có

Tùy thuộc vào yêu cầu thiết kế, bạn có thể chọn một trong hai UDLD hoặc loop guard. UDLD không cung cấp bảo vệ cho các lỗi STP gây ra bởi phần mềm như là designated switch không gửi các gói BPDU. Đây là loại thất bại, tuy nhiên, là những ít phổ biến hơn do lỗi phần cứng.

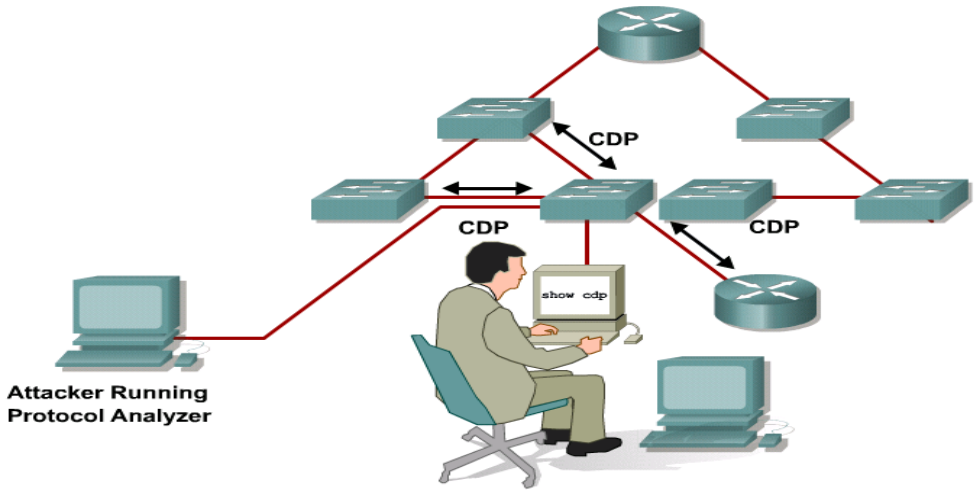
Trên một bó EtherChannel, UDLD vô hiệu hóa các liên kết cá nhân thất bại. Các kênh chính nó vẫn còn chức năng nếu các liên kết khác vẫn hoạt động. Loop guard sẽ đặt toàn bộ kênh ở trạng thái loop-inconsistent nếu không nhận được các gói BPDU qua EtherChannel.

Loop guard không làm việc trên các liên kết chia sẻ hoặc một liên kết đã bị làm đơn hướng kể từ khi bắt đầu. Tạo điều kiện cho cả hai UDLD và loop guard cung cấp mức cao nhất của bảo vệ.

9.6 Securing Network Switches

9.6.1 Describing Vulnerabilities in CDP

Kẻ tấn công có kiến thức về cách thức CDP hoạt động có thể tìm cách để tận dụng lợi thế của các văn bản rõ ràng của CDP để đạt được kiến thức về mạng. CDP chạy ở Layer 2 và cho phép thiết bị Cisco để xác định chính nó với các thiết bị Cisco khác. Tuy nhiên, các thông tin gửi qua CDP được truyền đi dưới dạng văn bản rõ ràng và không được chứng thực. Bằng cách sử dụng một bộ phân tích gói tin, kẻ tấn công có thể thu thập thông tin về các thiết bị mạng từ các gói tin quảng bá CDP.



Hình 9.6.1-1: Sử dụng CDP để tìm hiểu và tấn công

CDP là cần thiết cho các ứng dụng quản lý và không thể bị vô hiệu hoá mà không có sự bất tương thích với một số ứng dụng quản lý mạng. Tuy nhiên, CDP có thể được vô hiệu hóa có chọn lọc trên interface, nơi quản lý không được thực hiện. Lệnh no cdp enable cho phép vô hiệu hóa CDP trên một interface độc lập.

Bảng mô tả cách CDP có thể được bị lợi dụng :

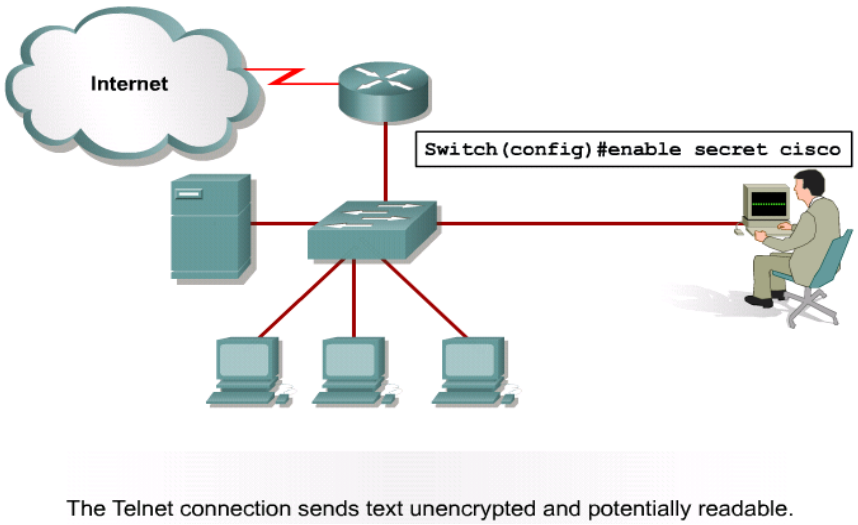
	Mô tả
1	Quản trị hệ thống sử dụng CDP để xem thông tin láng giềng
2	Kẻ tấn công sử dụng phân tích gói tin để chặn lấy các thông tin CDP
3	Kẻ tấn công phân tích thông tin trong gói tin CDP để biết địa chỉ mạng và thông tin thiết bị
4	Kẻ tấn công dự tính phương thức tấn công dựa trên có thông tin có được.

Bảng 9.6.1-1 : Bảng mô tả các CDP bị lợi dụng để tấn công

9.6.2 Telnet Protocol Vulnerabilities

Telnet có các lỗ hổng sau đây:

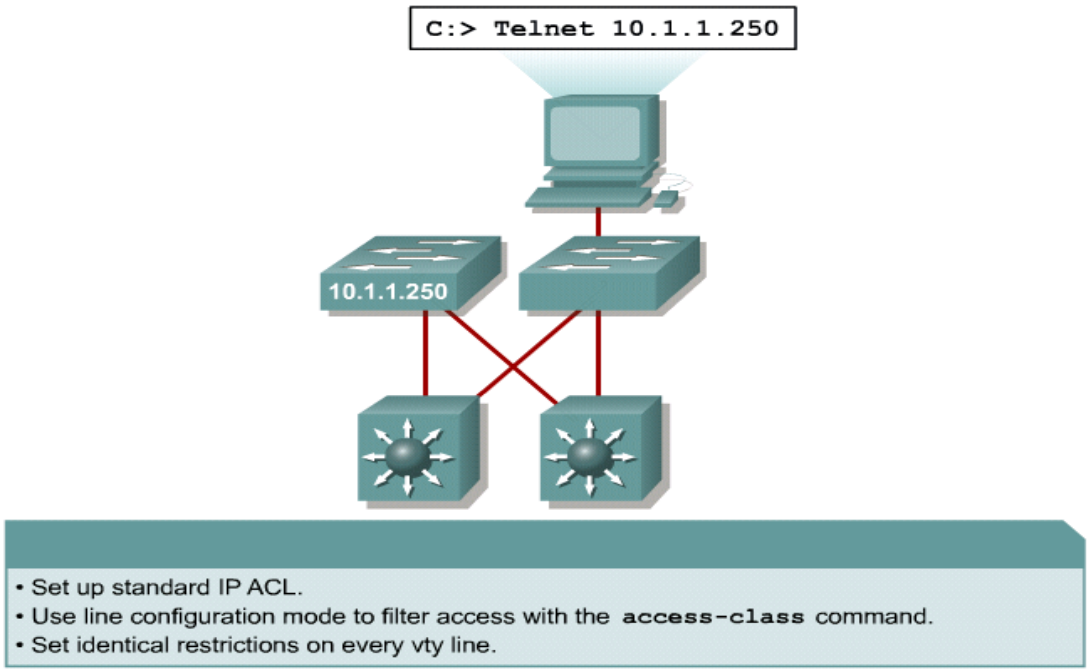
- Tất cả tên người dùng, mật khẩu, và các dữ liệu gửi qua mạng công cộng dưới dạng văn bản rõ ràng thì dễ bị tổn thương.
- Một người dùng với một tài khoản trên hệ thống có thể đạt được các đặc quyền nâng cao.
- Một kẻ tấn công từ xa có thể làm sụp đổ các dịch vụ Telnet, ngăn chặn việc sử dụng hợp pháp của dịch vụ đó.
- Một kẻ tấn công từ xa có thể tìm thấy một tài khoản khách được kích hoạt từ đó có thể có mặt bất cứ nơi nào trong các domain tin cậy của máy chủ.



Hình 9.6.2-1: Kết nối telnet gởi dữ liệu không được mã hóa

9.6.3 vty ACL

Cisco cung cấp ACL để cho phép hoặc từ chối Telnet truy cập vào cổng vty của một switch. Các thiết bị Cisco khác nhau về số lượng các cổng vty có sẵn theo mặc định. Khi cấu hình ACL cho vty, đảm bảo rằng tất cả các port mặc định được loại bỏ hoặc có một ACL vty cụ thể.



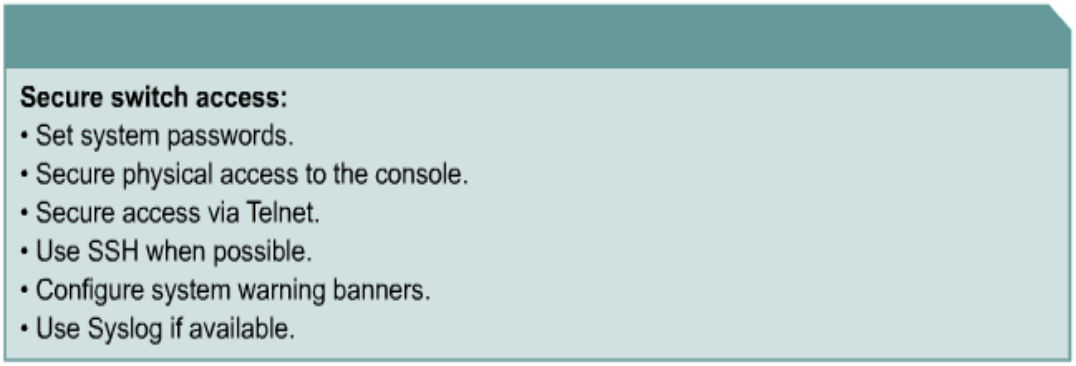
Hình 9.6.3-1: Mô tả cấu hình vty ACL

Lọc Telnet thường được coi là một chức năng của IP ACL mở rộng vì nó được lọc một giao thức cấp cao hơn. Tuy nhiên, do câu lệnh access-class lọc các phiên Telnet theo địa chỉ nguồn và áp dụng trên đường vty, bạn có thể sử dụng IP ACL cơ bản để kiểm soát truy cập vty. Lệnh access-class cũng áp dụng lọc IP ACL cơ sở lên đường vty cho các phiên Telnet có nguồn gốc từ switch.

Bạn có thể áp dụng các ACL vty cho bất kỳ sự kết hợp của đường vty nào. Bạn có thể áp dụng cùng một ACL cho tất cả các đường vty hoặc cụ thể với từng đuòng vty đặc biệt. Thường là dùng một ACL cho tất cả các đường vty.

9.6.4 Best Practices for Switch Security

Lỗ hổng bảo mật mạng bao gồm mất sự riêng tư, ăn cắp dữ liệu, mạo danh, và mất toàn vẹn. các biện pháp bảo mật cơ bản cần được thực hiện trên mạng để giảm thiểu tác động tiêu cực của người sử dụng sự sơ suất hoặc hành vi của mục đích xấu.



Hình 9.6.4-1: Bảo mật cho Switch

Các bước sau đây cần được thực hiện bất cứ khi nào đặt thiết bị mới:

- Bước 1 Xem xét hoặc thiết lập các chính sách an ninh của tổ chức.
- Bước 2 Secure các switch.
- Bước 3 Secure giao thức trên switch.
- Bước 4 Giảm thiểu các thỏa hiệp thông qua witch

Bạn nên xem xét các chính sách của một tổ chức khi xác định được mức độ và loại hình an ninh để thực hiện. Bạn phải cân bằng mục tiêu của an ninh mạng hợp lý với phí hành chính của các biện pháp an ninh rất hạn chế.

Một chính sách thiết lập an ninh tốt những đặc điểm:

Cung cấp một quá trình kiểm tra an ninh mạng hiện có

- Cung cấp một khuôn khổ an ninh chung để thực hiện an ninh mạng
- Định nghĩa hành vi không được phép đối với dữ liệu điện tử
- Xác định mà các công cụ và phương thức cần thiết cho tổ chức
- Tạo sự đồng thuận giữa nhóm người tạo key và xác định trách nhiệm của người sử dụng và quản trị viên
- Định nghĩa một quá trình xử lý sự cố an ninh mạng
- Cho phép mở rộng doanh nghiệp, thực hiệnbảo mật và kế hoạch thực thi.

Thực hiện theo các thông lệ tốt nhất để truy cập an toànswitch:

- **Đặt mật khẩu hệ thống:** Sử dụng câu lệnh enable secret để thiết lập mật khẩu cho phép truy cập vào các hệ thống Cisco IOS. Bởi vì câu lệnh enable secret cho phép thực hiện mã hóa Message Digest 5 (MD5) hash mật khẩu cấu hình, mật khẩu vẫn còn dễ bị tấn công từ điển. Vì vậy, áp dụng các tiêu chuẩn trong việc lựa chọn một mật khẩu khả thi. Hãy thử chọn mật khẩu có chứa chữ cái, số, và các ký tự đặc biệt, ví dụ, "$ pecia1 $" thay vì "đặc biệt", nơi mà các “s" đã được thay thế bằng "$", và l”" đã được thay thế với "1" (một).

- **An toàn truy cập vào giao diện điều khiển (console):** điều khiển truy cập đòi hỏi một mức tối thiểu của an ninh cả vật lý và luận lý. Một cá nhân truy cập vào một hệ thống có thể phục hồi hoặc thiết lập lại mật khẩu của hệ thống, do đó cho phép người đó để bỏ qua tất cả các bảo đảm khác thực hiện trên hệ thống đó. Do đó, bắt buộc để đảm bảo quyền truy cập vào giao diện điều khiển.

- **Bảo mật truy cập vào đường vty:** Các bước tối thiểu được đề nghị đối với việc bảo vệ truy cập Telnet là:

    - Áp dụng các ACL cơ bản cho tất cả các đường vty.

    - Cấu hình một mật khẩu cho tất cả các dòng line vty.

- **Sử dụng SSH:** Các giao thức SSH và ứng dụng cung cấp một kết nối an toàn từ xa đến switch. Nó mã hóa tất cả lưu lượng, bao gồm cả mật khẩu, giữa một giao diện điều khiển từ xa và switch. Bởi vì SSH không gửi dữ liệu trong văn bản rõ ràng, quản trị mạng có thể tiến hành phiên truy cập từ xa mà kẻ theo dõi không thể biết. Các máy chủ SSH trong phần mềm Cisco IOS làm việc công khai và thương mại cho khách hàng SSH.

- **Cấu hình các biểu ngữ cảnh báo hệ thống:** Đối với cả hai mục đích pháp lý và hành chính, hiển thị một biểu ngữ hệ thống cảnh báo trước khi đăng nhập là một cách thuận tiện và hiệu quả của việc tăng cường an ninh và chính sách sử dụng nói chung. Bởi trong đó nêu rõ quyền sở hữu, sử dụng, truy cập, và các chính sách bảo hộ trước khi đăng nhập, bạn cung cấp sao lưu thêm cho chắc chắn.

- **Vô hiệu hoá dịch vụ không cần thiết:** Theo mặc định, các thiết bị Cisco hỗ trợ nhiều TCP và User Datagram Protocol (UDP) máy chủ để tạo điều kiện quản lý và hội nhập vào môi trường hiện tại. Đối với hầu hết các cài đặt, các dịch vụ này thường không cần thiết, và vô hiệu hoá chúng rất có

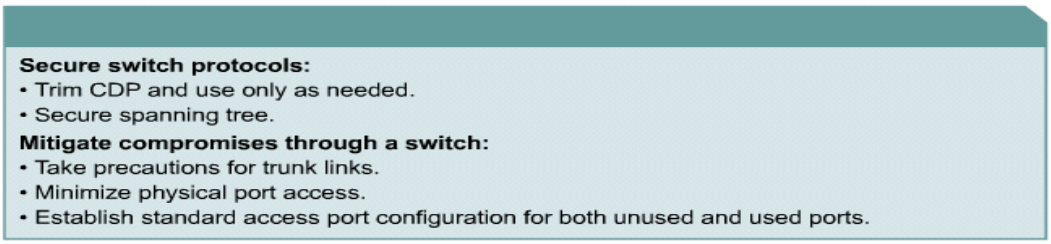
thể giảm tiếp xúc an ninh tổng thể. Những lệnh này dùn để vô hiệu hóa dịch vụ không cần thiết được sử dụng:

- no service tcp-small-servers
- no service udp-small-servers
- no service finger
- no service config

- **Vô hiệu hoá việc tích hợp HTTP daemon nếu không sử dụng:** Mặc dù phần mềm Cisco IOS cung cấp một máy chủ HTTP tích hợp cho quản lý, nhưng đề nghị nó nên bị vô hiệu hóa để giảm thiểu tiếp xúc tổng thể. Nếu truy cập HTTP switch là hoàn toàn cần thiết, sử dụng ACL cơ bản để cho phép truy cập từ chỉ mạng con tin cậy.

- **Cấu hình logging cơ bản:** Để hỗ trợ và đơn giản hóa vấn đề và điều tra xử lý sự cố an ninh, điều khiển hoạt động hệ thống thông tin nhận được từ chức năng loggin. Xem thông tin xuất ra trong hệ thống bộ nhớ đệm loggin. Để tăng hoạt động hệ thống, tăng kích thước bộ đệm mặc định.

  Thực hiện theo các bước tốt nhất cho an ninh switch:



Hình 9.6.4-2: Các bước tốt nhất cho an ninh switch

- **Sử dụng CDP chỉ khi cần thiết:** CDP không tiết lộ thông tin bảo mật cụ thể, nhưng nó có thể để cho một kẻ tấn công khai thác thông tin trong một cuộc tấn công trinh sát, theo đó những kẻ tấn công biết được thiết bị và thông tin địa chỉ IP cho mục đích phát động tấn công khác. Hai hướng dẫn thực hành nên được thiết lập cho CDP.

  - Nếu CDP là không cần thiết, hoặc thiết bị nằm trong một môi trường không an toàn, nên vô hiệu hóa toàn cầu hình CDP trên thiết bị.

- Nếu CDP là bắt buộc, vô hiệu hóa CDP trên một mỗi interface trên các port kết nối với các mạng không tin cậy. Bởi vì CDP là một giao thức liên kết cấp, nó không phải là thoáng qua trên một mạng (trừ khi một cơ chế đường hầm Lớp 2 được đặt ra). Giới hạn nó chạy chỉ giữa các thiết bị tin cậy và vô hiệu hóa nó ở các nơi khác. Tuy nhiên, CDP được yêu cầu trên bất kỳ cổng truy cập khi bạn gắn một điện thoại Cisco để thiết lập một mối quan hệ tin tưởng.

- **Secure topo của spanning tree:** Điều quan trọng là bảo vệ quá trình STP của các switch bao gồm cơ sở hạ tầng. Các gói BPDU vô hoặc độc hại có thể dùng để tấn công một thiết bị hoặc gây ra một cuộc tấn công DoS. Bước đầu tiên trong việc ổn định một cài đặt spanning tree là tích cực xác định các root brigde trong thiết kế và thiết lập cứng các ưu tiên STP để chấp nhận giá trị root. Làm tương tự cho các root bigde backup. Những hành động này bảo vệ chống lại sự thay đổi vô ý trong STP do không kiểm soát được các gói giới thiệu của switch mới.

Trên một số nền tảng, tính năng bảo vệ BPDU có thể sẵn có. Nếu có, cho phép nó truy cập vào portkết hợp với các tính năng PortFast để bảo vệ mạng từ lưu lượng BPDU truy cập không mong muốn. Khi nhận được BPDU, tính năng tự động vô hiệu hóa các port.

Thực hiện theo các thao tác tốt nhất để giảm thiểu sự thỏa hiệp qua một switch:

- Chủ động cấu hình các port router và switch không sử dụng:
  - Thực hiện lệnh shut vào tất cả các port và interface chưa sử dụng.
  - Đặt tất cả các port không sử dụng trong một VLAN được sử dụng đặc biệt để nhóm các port không sử dụng cho đến khi chúng được chủ động đặt vào dịch vụ.
  - Cấu hình tất cả các cổng chưa sửp dụng như là ở mode access, không cho phép tự động đàm phán trunk.

- Vô hiệu hoá tự động đàm phán trunk: Theo mặc định, thiết bị chuyển mạch Cisco Catalyst Cisco IOS đang chạy phần mềm được cấu hình để tự động thương lượng khả năng trunking. Vấn đề này đặt ra một mối nguy hiểm nghiêm trọng cho cơ sở hạ tầng, vì một thiết bị của bên thứ ba không có

bảo đảm có thể được giới thiệu đến mạng như một thành phần cơ sở hạ tầng hợp lệ. Các khả năng bị tấn bao gồm chặn traffic, chuyển hướng lưu lượng truy cập, và DoS. Để tránh nguy cơ này, vô hiệu hoá tự động đàm phán trunking và tự kích hoạt nó trên các liên kết có yêu cầu nó. Đảm bảo rằng đường trunk sử dụng một native VLAN được dành riêng cho trunking.

- **Kiểm soát truy cập thiết bị vật lý:** Tránh các thiết bị đểu truy cập trực tiếp port.

- **Xây dựng bảo vệ trên port:** các biện pháp cụ thể phải được thực hiện trên tất cả các port truy cập của bất kỳ switch được đặt vào dịch vụ. Đảm bảo rằng chính sách được đặt ra cho cả port dùng van không dùng trên switch. Đối với các cổng kích hoạt cho thiết bị đầu cuối truy cập, macro switchport host thực hiện các hành động khi hoạt động trên một port cụ thể:

    - Đặt chế độ accesscho port
    - Kích hoạt spanning tree PortFast
    - Vô hiệu hóa kênh nhóm.

Lưu ý : Lệnh switchport host là một macro thực hiện nhiều câu lệnh cấu hình. Nó không có hình thức “no” để vô hiệu hóa nó. Để trở về giao diện để cấu hình mặc định của nó, sử dụng lệnh default interface interface-id.