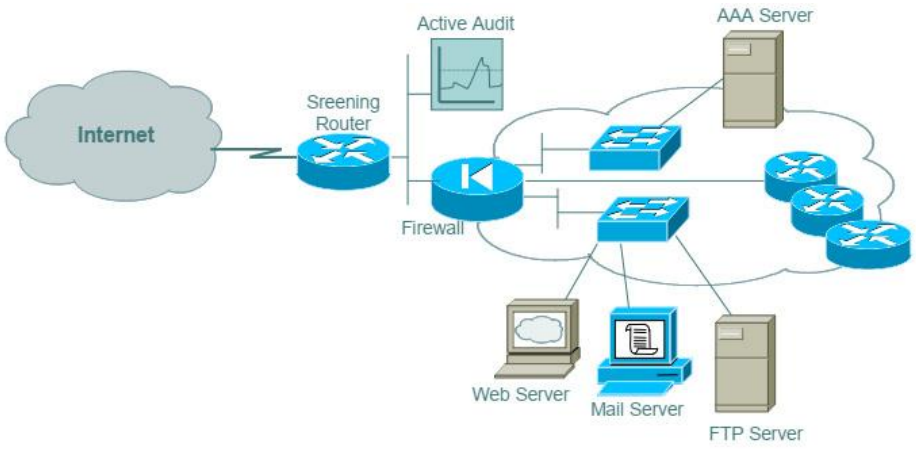
An toàn cơ sở hạ tầng mạng

Các thành phần hạ tầng mạng

- Phần cứng: router, switch, card…
- Phần mềm: HĐH, ứng dụng mạng…
- Dịch vụ
- Có thể chứa các lỗ hổng bảo mật



Các mối đe dọa của hạ tầng mạng

Threat	Mô tả
Interruption	ngăn các gói tin đến các điểm đến được ủy quyền
Interception	truy cập trái phép vào nội dung gói tin
Modification	thay đổi nội dung gói tin
Fabrication	xây dựng các gói tin trông giống như gói tin nguồn từ người dùng được ủy quyền
Replication	phát lại các gói tin
Routing table poisoning	cố tình gửi thông tin không có thật để đầu độc bảng định tuyến của bộ định tuyến.
Packet mistreatment	thay đổi hành vi bình thường của traffic
Address Spoofing	giả mạo bất hợp pháp địa chỉ để che giấu danh tính của kẻ tấn công
Server compromising	xâm nhập máy chủ để sửa đổi cấu hình của nó

Hậu quả của tấn công cơ sở hạ tầng mạng

Problem	Mô tả
Sub-optimal routes	Các gói tin sẽ đi qua một con đường kém tối ưu hơn, dẫn đến độ trễ lâu hơn.
Routing loops	Con đường chuyển tải các gói tin tạo thành một vòng lặp, ngăn không cho các gói đến đích.
Congestion	Các gói tin được chuyển tiếp một cách độc hại đến các liên kết hoặc mạng cụ thể, làm cho quá tải, dẫn đến độ trễ cao và thậm chí các gói bị giảm.
Network partition	Một mạng đơn lẻ sẽ bị phân tách giả tạo thành hai hoặc nhiều phân vùng, làm cho các máy chủ thuộc một phân vùng không thể giao tiếp với máy chủ thuộc các phân vùng khác.
Blackhole	Một khu vực của mạng nơi các gói tin đi vào nhưng không đi ra.
Denial of Service	Do lượng truy cập khổng lồ bất thường, các bộ định tuyến bị quá tải và không thể phục vụ các yêu cầu hợp pháp.
Traffic subversion	Lưu lượng được chuyển hướng để đi qua một liên kết nhất định để kẻ tấn công có thể nghe trộm hoặc sửa đổi dữ liệu, mặc dù lưu lượng sẽ vẫn được chuyển tiếp đến đúng đích.

Một số phương pháp bảo mật hạ tầng mạng

- Xác thực và giám sát phần cứng, phần mềm
- Truy cập bảo mật động
  - Cấp độ truy cập của các thành viên
  - Quản lý đặc quyền truy cập và xác thực động
- Phân khu vực có cấu trúc
  - Giảm thiểu sự lây lan của các mối đe dọa tiềm ẩn
    - Một phân đoạn bị tấn công → các phân đoạn khác được tắt hoặc ngăn chặn

Thách thức an toàn hạ tầng mạng

- Thiết kế bảo mật từ đầu
- Chí phí cao cho thay đổi giải pháp
- Đánh đổi bảo mật và hiệu suất
- Khó bảo mật hoàn toàn trên internet

Switch

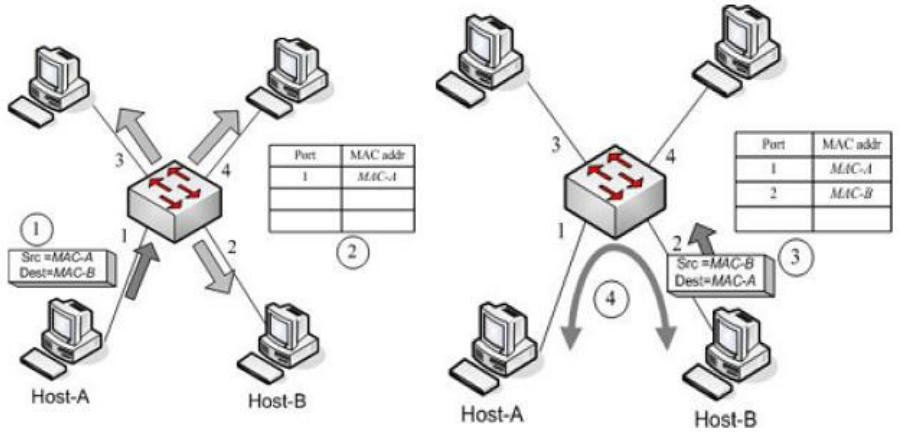
- Hoạt động ở tầng data link
- Xử lý dữ liệu dạng frame
- Hỗ trợ thiết lập VLAN, STP, Port-security...
- Switch layer3/multilayer switch

Nguy cơ của switch

- Độc lập của các tầng
  - Khi một tầng bị tấn công thì các tầng khác không biết
- Tin tưởng
  - Quản trị viên thường tin tưởng các mạng tầng 2 đáng tin cậy nên chủ quan
- Khó phát hiện tấn công
  - Cần có kiến thức về hoạt động của các giao thức tầng datalink như ARP, STP

Tấn công trên switch

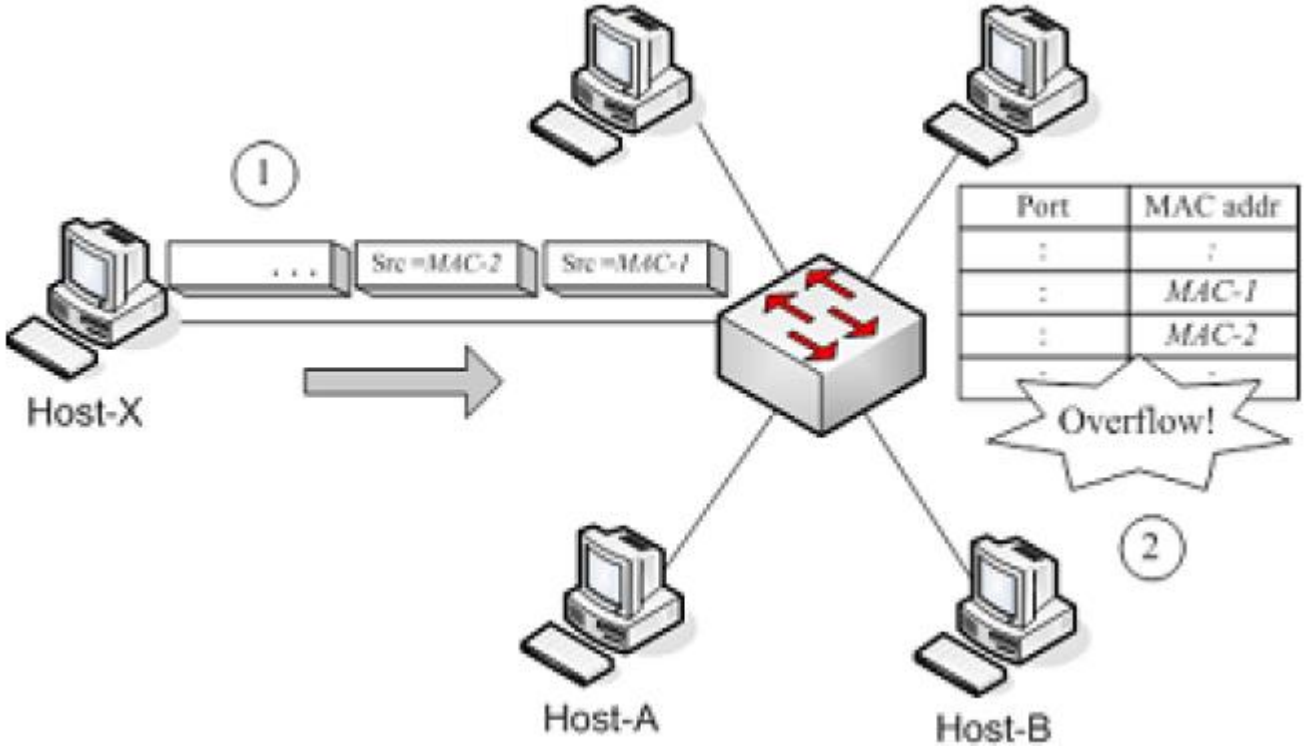
- Tấn công MAC flooding
  - Lưu trữ thông tin chuyển mạch: bảng CAM
  - Xây dựng bảng CAM: trích xuất địa chỉ MAC nguồn từ frame được truyền trên mỗi cổng
- MAC flooding: tấn công làm tràn bảng CAM
  - CAM chỉ chứa được một số hữu hạn ánh xạ (sau n giây, địa chỉ nào không dùng sẽ bị xóa khỏi CAM)

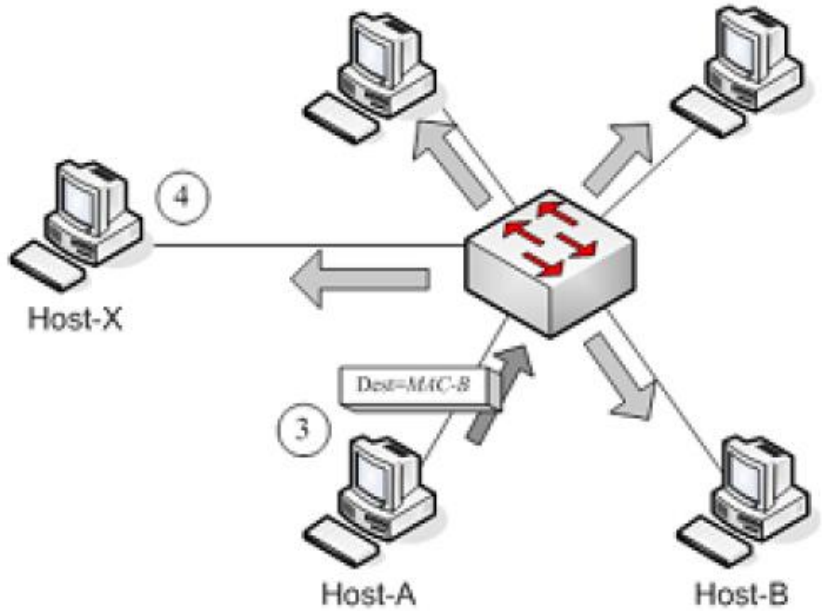


Tấn công trên switch

- Tấn công MAC flooding

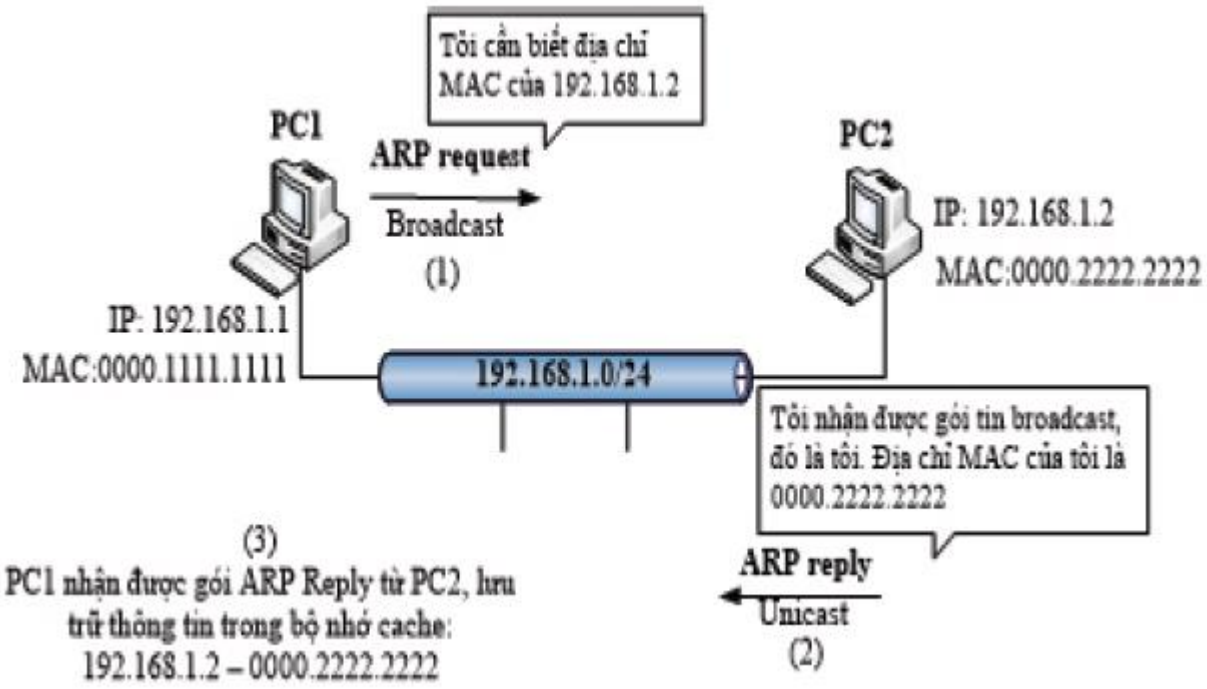
Ngăn chặn:
Port security: chỉ định số lượng MAC có thể được kết nối với 1 cổng switch hoặc chỉ định địa chỉ MAC nào có thể truy cập vào một cổng cụ thể, nếu vi phạm, cổng tương ứng sẽ bị tắt





Tấn công trên switch

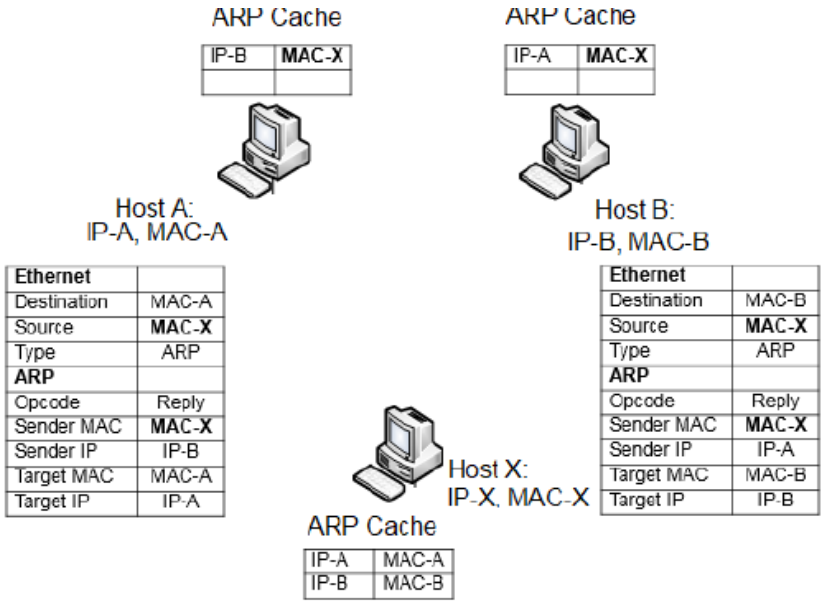
- Tấn công ARP poisoning
- Giao thức ARP

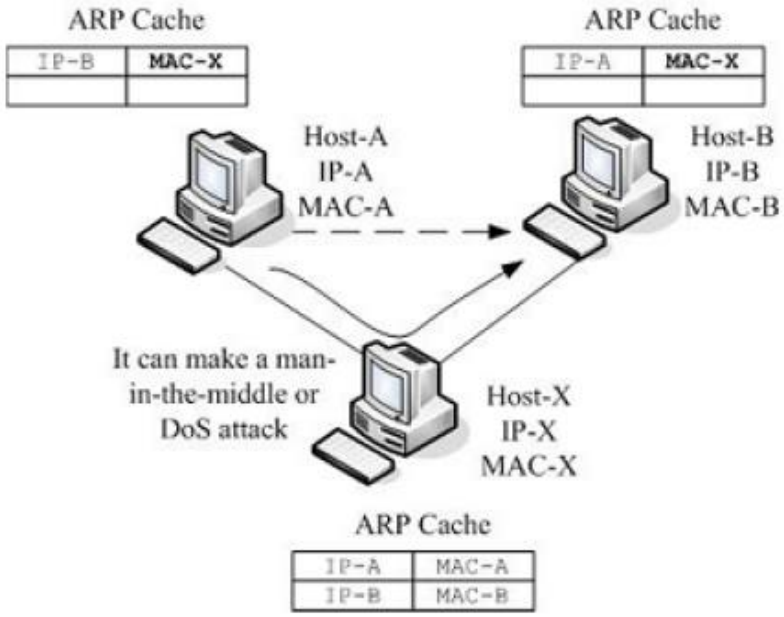


Để giảm số lượng yêu cầu ARP, hệ điều hành thường lưu vào bộ nhớ cache các địa chỉ MAC đã phân giải được trong một khoảng thời gian ngắn. Do đó, trước khi thực hiện yêu cầu ARP, máy chủ sẽ kiểm tra bộ nhớ cache ARP để xem liệu ánh xạ IP-MAC được yêu cầu có tồn tại hay không.
Nếu ánh xạ tồn tại, nó sẽ lấy địa chỉ MAC tương ứng từ bộ nhớ đệm mà không cần thực hiện yêu cầu ARP mới.
Nguy cơ của ARP là hacker sẽ đầu độc bảng Cache ARP của các host bằng tấn công ARP Poisoning

Tấn công trên switch

- Tấn công ARP poisoning





Hacker đầu độc các máy khác bằng cách gửi một gói ARP Reply với thông tin sai. Vì ARP không yêu cầu xác thực nên bất cứ khi nào máy tính nhận được phản hồi ARP, nó sẽ cập nhật bộ nhớ cache của nó bất kể nó đã gửi yêu cầu ARP hay chưa. Do đó, hacker có thể dễ dàng gửi ARP Reply sai – tạo các ánh xạ IP của các máy nạn nhân tương ứng với địa chỉ MAC của máy tấn công

Sau khi bộ cache ARP bị cập nhật sai, mọi traffic giữa 2 host này sẽ bị chuyển hướng qua máy tấn công Host-X thay vì đi trực tiếp tới Host-A hay Host-B như ban đầu. Khi đó Host-X sẽ đọc được hết thông tin đã được trao đổi giữa Host-A và Host B, nó có thể chặn traffic giữa chúng

Tấn công trên switch

- Sau khi đầu độc ARP, hacker sử dụng cache để tiếp tục tấn công
  - Tấn công man in the middle
    - Nếu Host X định tuyến lại các gói tin đến chính xác theo hai hướng thì Host A và Host B không biết rằng lưu lượng giữa chúng đang bị theo dõi hoặc chỉnh sửa
  - Tấn công DoS
    - Nếu không định tuyến lại các gói tin thì Host X sẽ khởi động tấn công DoS (vì Host A và Host B không thể giao tiếp với nhau). Tuy nhiên vì không có lưu lượng giữa A và B nên các mục tương ứng trong bộ nhớ đệm ARP sẽ hết thời gian chờ, do đó để tiếp tục từ chối dịch vụ, Host X phải tiếp tục đầu độc bộ nhớ cache ARP

Tấn công trên switch

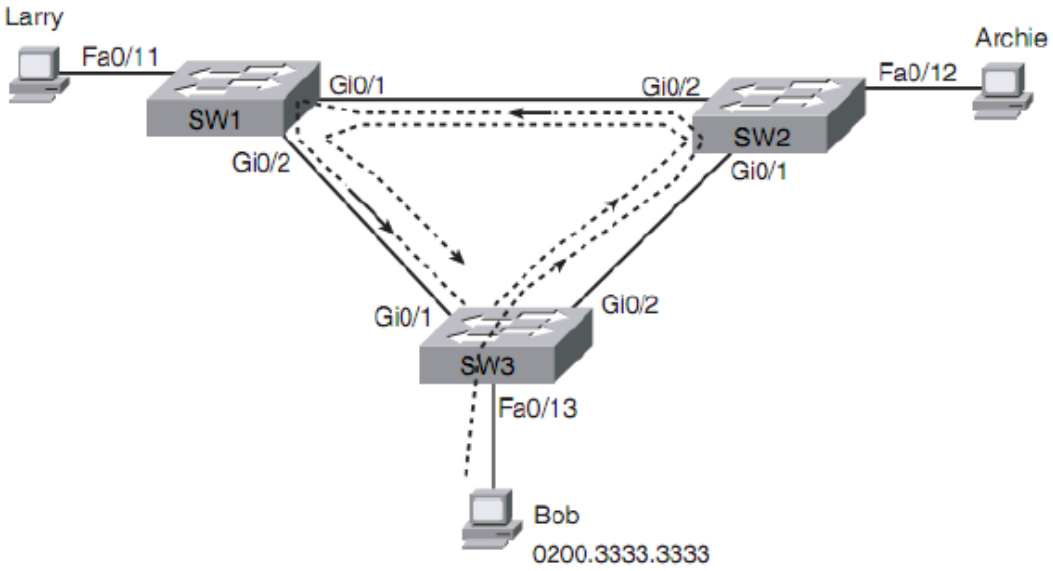
- Sau khi đầu độc ARP, hacker sử dụng cache để tiếp tục tấn công
  - Tấn công Hijacking
    - Giả sử Host B là máy chủ, khi Host X nhận gói tin từ Host A, nó sẽ đưa gói tin của chính mình vào Host A, giả vờ mình là Host B. Khi đó Host X kiểm soát kết nối và cả A và B đều không biết mình bị kiểm soát
  - Tấn công Spoofing WAN traffic
    - Default gateway trong LAN: kết nối các máy cục bộ với internet
    - Để tiếp cận các máy chủ trên internet, các máy chủ trong mạng LAN gửi các gói tin đến default gateway của nó (MAC đích = MAC của default gateway)
    - Default gateway định tuyến các gói đến bước tiếp theo và tiếp tục đến đích
    - Khi các gói tin trở lại từ internet, default gateway gửi chúng đến máy chủ trong LAN
    - Ví dụ Host A hoặc Host B là default gateway, hacker sẽ đánh hơi được lưu lượng truy cập internet của máy chủ lưu trữ

Tấn công trên switch

- Phòng chống tấn công ARP poisoning
  - Dùng mục nhập ARP tĩnh
    - Bộ đệm ARP có thể lưu trữ các ánh xạ IP-MAC tĩnh nên các mục nhập không thay đổi, do đó các câu trả lời giả mạo ARP sẽ bị bỏ qua
  - Giám sát để phát hiện
    - ARPWatch: khi có bất cứ thay đổi đáng ngờ nào của ánh xạ, sẽ thông báo cho admin
  - Không cập nhật bộ nhớ cache ARP
    - Chỉ chấp nhận các câu trả lời ARP và cập nhật các mục nhập trong bộ nhờ cache khi chúng hết hạn
    - Do đó để đầu độc bộ nhớ cache ARP, hacker phải gửi gói trả lời ARP nhanh hơn so với máy chủ hợp pháp, làm cho quá trình giả mạo khó khăn hơn

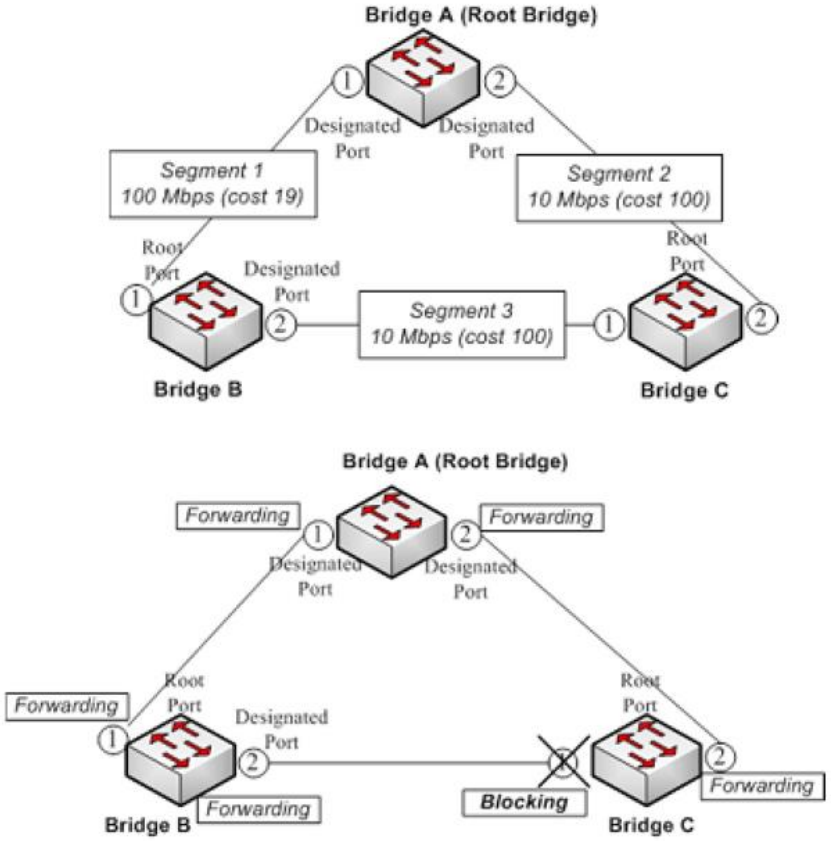
Tấn công trên switch

- Tấn công STP
  - Thiết kế kết nối dư thừa làm tăng khả năng dự phòng cho hệ thống
  - Problem: bão quảng bá, nhiều gói tin nhận được giống nhau và bảng địa chỉ MAC trên các switch không ổn định (switching loop)
  - Giao thức STP khóa tạm thời một hoặc một số cổng để tránh tình trạng switching loop
  - STP hoạt động dựa trên thông báo BPDU để giao tiếp với các bridge láng giềng
  - 2 loại BPDU: configuration BPDU và Topology Change Notification



Tấn công trên switch

- Tấn công STP
  - Hoạt động của STP
    - Bầu chọn Root Switch (Root Bridge): mỗi switch có một giá trị Bridge ID gồm 2 trường Bridge priority và MAC address được đặt vào trong BPDU và gửi quảng bá cho các switch khác 2s một lần
    - Switch được chọn làm Root Bridge là switch có Bridge ID nhỏ nhất (so sánh Bridge priority trước, nếu bằng nhau thì so sánh MAC addr)
    - Chọn Root port: các port trên Root Bridge đều là Root port. Trên các switch còn lại, dựa vào chi phí nhỏ nhất tính từ mỗi port đến Root Bridge
    - Chọn designed port: trên mỗi segment mạng, dựa vào chi phí nhỏ nhất tính từ mỗi segment đến Root Bridge, cổng còn lại gọi là Nondesigned port



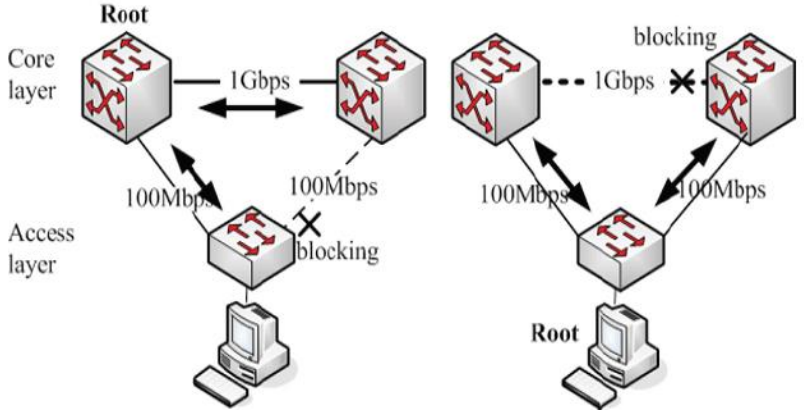
Tấn công trên switch

- Tấn công STP
  - Do việc thiếu xác thực với các bản tin BPDU trong STP, bất cứ máy chủ nào đang chạy phần mềm Bridging đều có thể tham gia vào STP (ví dụ bất cứ máy Linux nào cũng có thể được cấu hình thành một bridge dựa trên phần mềm bằng cách sử dụng gói BRIDGE-UTILS, có thể dựa vào đó để gửi BPDU giả mạo để tấn công STP)
  - Root Claim và MITM: bằng cách gửi một BPDU giả mạo với Bridge ID thấp nhất, bridge của hacker sẽ được bầu làm Root bridge mới.
    - Root bridge độc hại này có thể thực hiện các cuộc tấn công khác nhau: đánh hơi các khung dữ liệu đi qua nó
    - Root bridge này có thể là bất cứ máy tính nào đang chạy phần mềm bridge và máy tính đó dễ dàng đánh hơi các khung dữ liệu

Tấn công trên switch

- Tấn công STP
  - Tấn công DoS STP: mỗi lần chiếm quyền Root Bridge với Bridge ID thấp nhất sẽ làm cho các thiết bị chuyển mạch tính toán lại cấu trúc liên kết, nếu liên tục thực hiện việc chiếm quyền Root Bridge thì các thiết bị chuyển mạch liên tục tính toán lại cấu trúc liên kết, việc này sẽ làm gián đoạn hoạt động của mạng, dẫn đến từ chối dịch vụ. Cuộc tấn công này gọi là bầu cử vĩnh viễn, tức là liên tục bầu cử, các công của switch không bao giờ trở thành trạng thái chuyển tiếp, làm cho mạng mất ổn định hoặc vô hiệu hóa

Tấn công trên switch



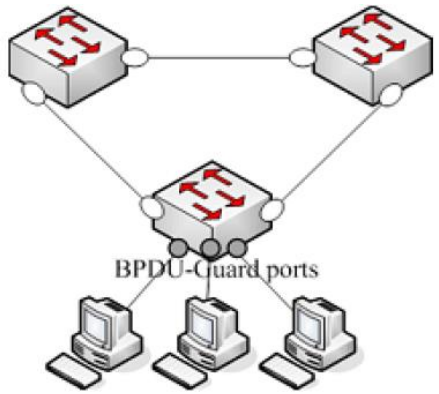
- Tấn công STP
  - Thông báo TCN liên tục: bằng cách giành được vai trò Root Bridge mạng Spanning Tree, hacker có thể thay đổi luồng lưu lượng trong mạng chuyển mạch
  - Các thiết bị chuyển mạch trong lớp lõi có băng thông cao hơn nhiều so với lớp truy cập
  - Nếu máy tính ở lớp Access Switch chạy ứng dụng Bridging và tuyên bố nó là Root Bridge bằng cách quảng cáo một BPDU có Bridge ID thấp nhất, ST sẽ được tạo lại và liên kết Gigabit sẽ bị chặn → lưu lượng sẽ đi qua liên kết 100Mbps → giảm hiệu suất

Tấn công trên switch

- Phòng chống tấn công STP
  - Dùng BPDU guard – tính năng Portfrast BPDU guard là một trong những cải tiến của CISCO để chống lại tấn công STP
  - Các cổng có bật BPDU guard không cho phép các máy tính phía sau chúng gửi BPDU (ngay khi các cổng đó nhận BPDU thì sẽ bị chặn)
  - Khi đó các máy tính phía sau các cổng BPDU guard không thể ảnh hưởng đến cấu trúc liên kết STP đang hoạt động và chỉ gửi các khung dữ liệu bình thường

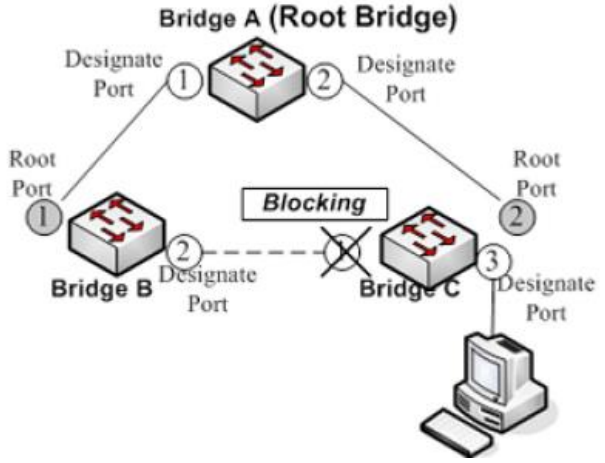
```
SW1(config)#int fastEthernet 0/7
 SW1(config-if)#spanning-tree bpduguard enable
```

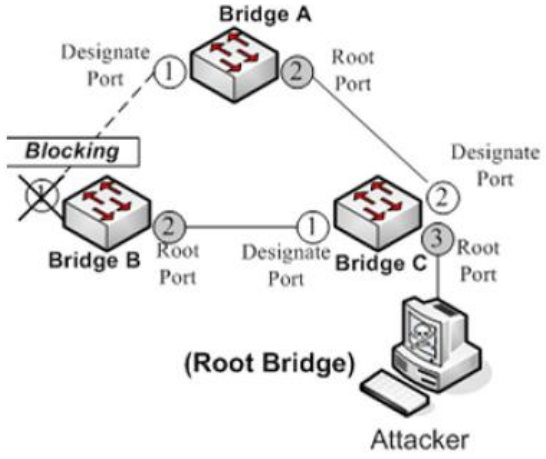
```
SW1(config)#spanning-tree portfast bpdufilter default
 SW1(config)#interface GigabitEthernet0/6
 SW1(config-if)#spanning-tree portfast
```



Tấn công trên switch

- Phòng chống tấn công STP
  - Dùng Root guard: thực hiện vị trí cầu nối trong mạng
  - Khi một cuộc tấn công chiếm vai trò Root trong mạng, cấu trúc cây thay đổi và các cổng của các bridge trong mạng sẽ được cấu hình lại cho phù hợp

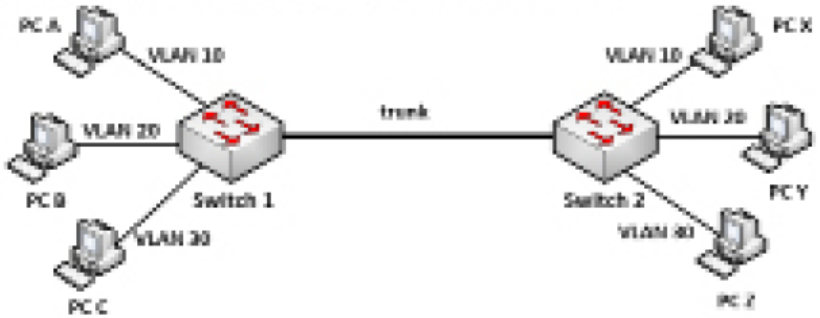




Root guard được cấu hình trên mỗi cổng. Các cổng đó không thể trở thành Root port mà phải là designed port. Nếu các cổng này nhận được các BPDU, chúng sẽ chuyển sang trạng thái STP không phù hợp gốc (thay vì trở thành Root port) và không có lưu lượng nào chuyển tiếp qua chúng

Tấn công trên switch

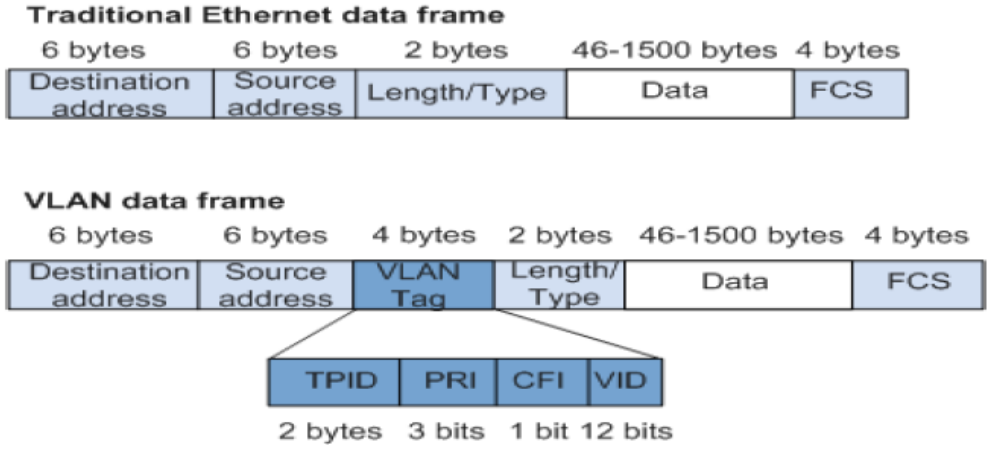
- Tấn công VLAN
  - Trong VLAN, khi một gói tin quảng bá được gửi từ một thiết bị trong VLAN thì sẽ được chuyển đến các thiết bị trong VLAN đó
  - Để thực hiện trao đổi giữa các VLAN phải sử dụng trunk
  - Kết nối trunk là kết nối point-to-point giữa các cổng trên switch với router hoặc switch khác
  - Kết nối trunk sẽ vận chuyển dữ liệu của nhiều VLAN thông qua một liên kết đơn và cho phép mở rộng VLAN trên hệ thống mạng



Dùng một dây nối switch 1 với switch 2, các thành viên trong cùng VLAN ở các switch khác nhau vẫn có thể giao tiếp với nhau -> liên kết trunk lớp 2

Tấn công trên switch

- Tấn công VLAN
  - Kỹ thuật trunk cho phép dùng chung một kết nối vật lý cho dữ liệu của các VLAN đi qua nên để phân biệt được chúng là dữ liệu của VLAN nào, người ta gắn vào các gói tin một dấu hiệu “tagging”.
  - Các tag được thêm vào trên đường gói tin đi ra/vào đường trunk và được bỏ đi khi ra khỏi đường trunk (giao thức 802.1Q (dot1q)
  - Giao thức này nhận dạng các VLAN bằng cách thêm “Frame Header” (gắn thẻ cho VLAN – Frame tagging)



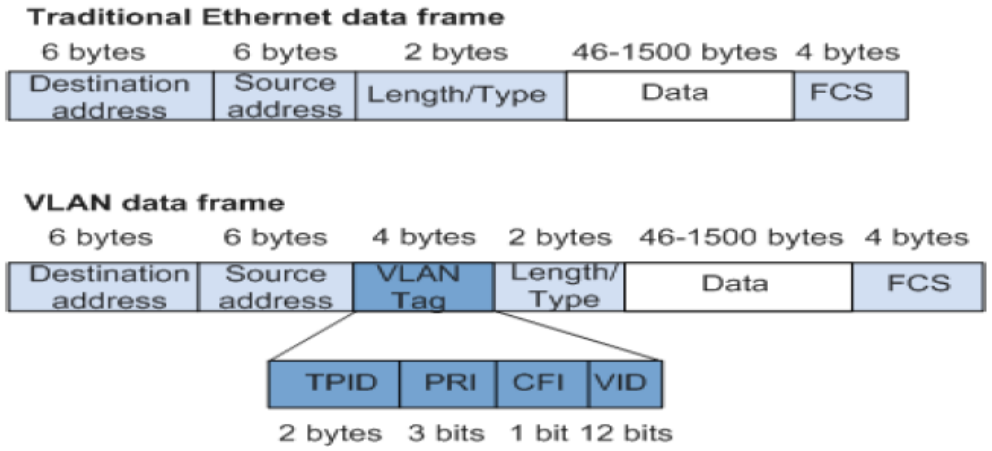
Tấn công trên switch

- Tấn công VLAN
  - Kỹ thuật trunk cho phép dùng chung một kết nối vật lý cho dữ liệu của các VLAN đi qua nên để phân biệt được chúng là dữ liệu của VLAN nào, người ta gắn vào các gói tin một dấu hiệu “tagging”.
  - Các tag được thêm vào trên đường gói tin đi ra/vào đường trunk và được bỏ đi khi ra khỏi đường trunk (giao thức 802.1Q (dot1q)
  - Giao thức này nhận dạng các VLAN bằng cách thêm “Frame Header” (gắn thẻ cho VLAN – Frame tagging)

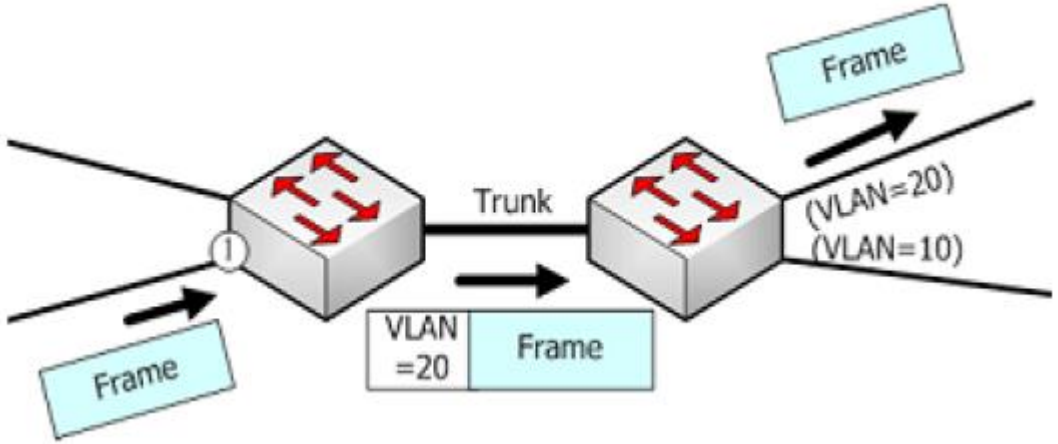
TPID (Tag Protocol ID): ID giao thức thẻ được sử dụng để xác định khung là khung IEEE 802.1q. Giá trị được đặt thành 0x8100.

PRI (User priority): cho biết mức độ ưu tiên của khung. Giá trị 0 là nỗ lực tốt nhất và 7 là cao nhất và 1 đại diện cho mức độ ưu tiên thấp nhất.

CFI (Canonical format identifier): được sử dụng với mức độ ưu tiên của người dùng để đánh dấu các gói có thể bị loại bỏ trong trường hợp tắc nghẽn.



Tấn công trên switch



- Tấn công VLAN
  - Mỗi switch duy trì một bảng chuyển mạch riêng biệt cho môi VLAN
  - Khi một switch nhận được một frame dữ liệu trên một cổng nào đó, nó sẽ kiểm tra bảng chuyển mạch của VLAN để xem có chứa cổng đó không nhằm biết liệu máy tính mục tiêu có được gắn vào cùng một bộ chuyển mạch hay không
  - Ở hình trên cổng 1 của switch thuộc về VLAN 20
  - Nếu đúng, bảng chuyển mạch của VLAN có chứa cổng nhận frame Switch thực hiện kết nối nội bộ giữa nguồn và các trạm đích
  - Nếu không đúng, frame sẽ được thêm một thẻ IEEE 802.1Q chỉ định thành viên của VLAN. Frame gắn thẻ được chuyển tiếp đến switch liền kề qua trunk
  - Khi nhận, switch sẽ loại bỏ thẻ trước khi chuyển tiếp nó đến máy tính cuối

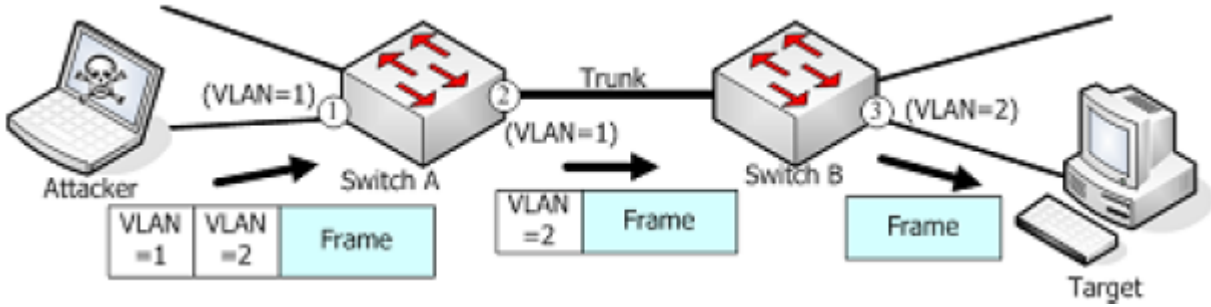
Tấn công trên switch

- Tấn công VLAN
  - Tấn công VLAN hopping cho phép lưu lượng từ một VLAN truy cập tới những VLAN khác mà không cần định tuyến
  - Hacker có thể thay đổi VLAN ID trên các khung dữ liệu được đóng gói để kết nối vào một trong các switch và thiết lập đường trunk để nghe trộm traffic trên các VLAN khác và gửi frame đến các VLAN thông qua trunk bị lợi dụng → tấn công VLAN hopping
  - Ví dụ: hai VLAN thực hiện hai mức bảo mật thấp và cao, một máy trong VLAN bảo mật thấp có thể tấn công dos đối với các máy trong VLAN bảo mật cao

Tấn công trên switch

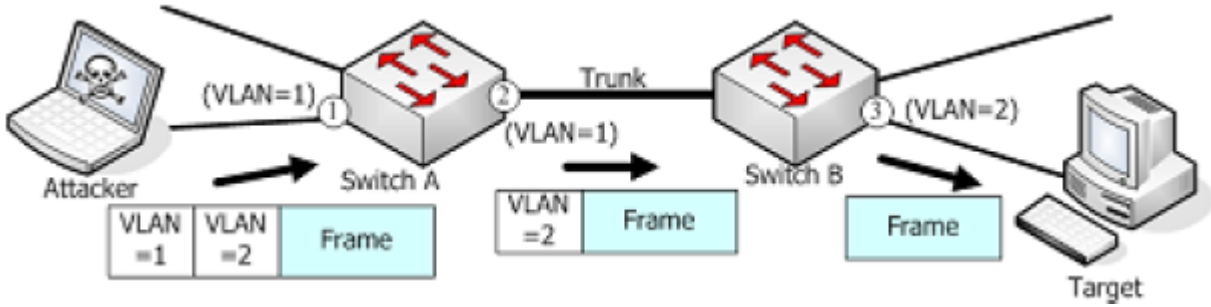
- Tấn công VLAN
  - Tấn công VLAN hopping dùng switch spoofing
  - Hacker sử dụng một máy tính có cài phần mềm giả lập biến máy tính này thành một switch giả mạo và bật tính năng trunking
  - Nếu port kết nối với máy tính này trên switch thật có bật tính năng auto trunking thì switch giả trên sẽ trở thành một thành viên của tất cả các VLAN → máy tính hacker có thể liên lạc với mọi VLAN trong hệ thống

Tấn công trên switch



- Tấn công VLAN
  - Tấn công VLAN hopping dùng double tagging
  - VLAN hopping có thể thực hiện ngay cả khi đã tắt trunking trên tất cả các cổng mà không cần trunking
  - Hacker có thể thêm hai tag thay vì một tag vào mỗi frame để tấn công VLAN hopping
  - Hacker dùng phần mềm sửa đổi frame gán 2 tag vào ethernet frame trước khi gửi đến switch 1. Outer tag cho thấy VLAN của hacker là VLAN 1 và trùng với Native VLAN của đường trunk, trong khi đó inner tag cho thấy VLAN của nạn nhân là VLAN 2
  - Khi frame giả này được gửi đi, switch A nhận frame này sẽ xóa outer tag và gửi nó đi đến các port thuộc outer VLAN và kể cả đường trunk

Tấn công trên switch



- Tấn công VLAN
  - Tấn công VLAN hopping dùng double tagging
  - Vì outer tag cho biết VLAN trùng với native VLAN của đường trunk nên switch A không thêm tag nào vào frame của hacker
  - Khi frame đến switch B, switch này xem tag inner và thấy frame này cần được chuyển đến VLAN ghi trong inner tag (VLAN 2) và nó chuyển frame này đến cổng thuộc VLAN 2 (cổng của máy nạn nhân)
  - Điều kiện để tấn công thành công
    - Hacker và nạn nhân ở 2 switch khác nhau
    - Hacker biết MAC nạn nhân
    - Hacker có cùng một VLAN gốc với liên kết trunking

Tấn công trên switch

- Phòng chống tấn công VLAN
  - Tấn công VLAN hopping
    - Tấn công này lợi dụng các cổng có chế độ chạy autotrunking mặc định
    - Tắt auto trunking trên các cổng và cả port trunk
    - Chỉ cấu hình tĩnh
  - Tấn công VLAN double tagging
    - Tấn công xảy ra khi native VLAN trên đường trunk trùng với VLAN mà hacker sử dụng để tấn công
    - Set native trên các đường trunk là 1 VLAN không có user nào sử dụng (không có port nào gán vào VLAN này – unused VLAN)

Định tuyến

- Xác định đường đi của các gói tin từ nguồn tới đích
- Router dựa vào địa chỉ IP đích trong các gói tin và sử dụng bảng định tuyến để xác định đường đi
- Trong bảng định tuyến, mỗi mạng mà router có thể chuyển đi được để trên một dòng (mỗi mạng này có được có thể do kết nối trực tiếp với router hay router học được thông qua cấu hình định tuyến)
- Định tuyến tĩnh: router sử dụng các tuyến đường tĩnh để chuyển dữ liệu
- Định tuyến động: sử dụng các tuyến đường di động, do các giao thức định tuyến động trao đổi thông tin định tuyến tạo ra (RIP, OSPF, BGP…)

Một số lỗ hổng trong giao thức định tuyến

- Cập nhật định tuyến bị sửa đổi hoặc xóa có chủ đích → bảng định tuyến chứa các mục sai → sự cố của một hoặc nhiều miền internet
- Thiếu xác minh thông tin định tuyến
  - Không có cơ chế xác minh tính đúng đắn thông tin hàng xóm gửi
  - Thông tin sai sẽ chuyển từ bộ định tuyến này sang bộ định tuyến khác, đánh lừa các bộ định tuyến trong toàn mạng
  - Ví dụ cơ chế xác thực trong RIP và OSPF là mật khẩu văn bản, có thể bị phá bằng phần mềm phân tích gói
- Khi bộ định tuyến bị tấn công, toàn bộ hệ thống mạng sẽ bị ảnh hưởng

Hậu quả khi bộ định tuyến bị tấn công

- Vòng lặp: quảng cáo định tuyến không chính xác
- Độ trễ: định tuyến sai làm quãng đường dài hơn
- Không truy cập được đích đến: gói tin có thể chuyển hướng đến hố đen
- Tắc nghẽn liên kết: liên kết quảng cáo sai vì có băng thông cao hơn giá trị ban đầu của nó
- Tải mạng cao: vòng lặp và truyền lại làm tăng tải trọng tổng thể của mạng

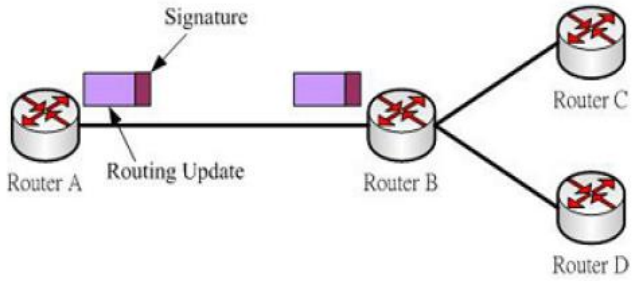
Tấn công external

- Tấn công liên kết, hacker chiếm quyền truy cập vào liên kết giao tiếp giữa hai bộ định tuyến, từ đó có thể thay đổi, định tuyến lưu lượng qua liên kết

Threat	Mô tả	Ảnh hưởng	Giải pháp
Interruption	Ngăn cập nhật định tuyến đến các bộ định tuyến được ủy quyền	Bị hạn chế	Xác nhận đã nhận được thông báo
Modification	Thay đổi nội dung của các bản cập nhật định tuyến	Nguy hiểm	Chữ ký số
Fabrication	Tạo bản cập nhật định tuyến giống như đến từ một bộ định tuyến hợp pháp	Nguy hiểm	Chữ ký số
Replication	Nắm giữ bản cập nhật định tuyến và phát lại sau	Bị hạn chế	Đánh số thứ tự cho thông báo

Chống tấn công external bằng chữ ký số

- Có tổ chức phát hành chứng chỉ được tin cậy bởi tất cả các bộ định tuyến
- Tổ chức này cấp cặp public key và private key cho tất cả các bộ định tuyến
- Mỗi bộ định tuyến giữ khóa private và cung cấp public key
- Bảo vệ private key trong mạng cục bộ, phân phối khóa public có thể dựa vào một giao thức hoặc cơ chế độc lập để chuyển tải khóa



- Router A dùng khóa Public của Router B để mã hóa thông điệp cập nhật định tuyến, đồng thời đính kèm chữ ký đã được mã hóa bởi khóa Private của Router A để gửi đi.
- Router B nhận được thông tin sẽ dùng khóa Public của Router A để giải mã chữ ký, sau đó dùng khóa Private của Router B để giải mã thông tin cập nhật định tuyến.
- Sử dụng chữ ký số làm tăng chi phí băng thông mạng + chi phí xử lý

Tấn công internal

- Thông tin định tuyến không chính xác
- Masquerading routers:
  - Giả mạo IP để giả mạo một bộ định tuyến nhằm gửi thông tin sai lệch
- Subverted routers
  - Làm lỗi bộ định tuyến bằng cách khai thác lỗi trong hệ điều hành của router, cấu hình sai các file hệ thống hoặc cấu hình để nhận file độc hại
- Unauthorized routers
  - Một bộ định tuyến không được phép nhưng cố tình tham gia vào mạng định tuyến và trao đổi giao thức định tuyến

Một số cách kiểm soát bộ định tuyến

- Xâm nhập hệ điều hành của router
- Lộ file cấu hình
- Bẻ khóa mật khẩu
- Lạm dụng khôi phục mật khẩu

Tấn công giao thức RIP

- RIP – giao thức vector định tuyến khoảng cách đại diện
  - Nếu có một bộ định tuyến độc hại thông báo cập nhật định tuyến quảng cáo với thông tin không chính xác -> các thông báo này chuyển tới toàn bộ các bộ định tuyến trong mạng -> cập nhật bảng định tuyến -> có thể tắc nghẽn mạng...
- Phòng chống
  - Chạy thuật toán dựa vào đường đi trong các bộ định tuyến: kiểm tra tính nhất quán và thuật toán dựa trên pivot để khôi phục sự không nhất quán

Tấn công giao thức OSPF

- OSPF – giao thức trạng thái liên kết
  - Các router sẽ trao đổi các LSA (quảng cáo link state) với nhau để xây dựng và duy trì cơ sở dữ liệu về trạng thái các đường liên kết (CSDL về cấu trúc mạng)
  - Các thông tin trao đổi dưới dạng multicast -> các router có cái nhìn đầy đủ và cụ thể về cấu trúc hệ thống mạng. Từ đó các router sẽ dùng thuật toán tìm đường đi ngắn nhất để tính toán đường đi. Các router không cập nhật định kỳ mà chỉ cập nhật khi có sự thay đổi
- Nguy cơ
  - Khi các router quảng cáo LSA, nó có thể làm ngập các thông báo trong toàn bộ miền định tuyến. Quá trình ngập lụt diễn ra bất cứ khi nào thông tin nó mang theo thay đổi (một liên kết bị xóa)
  - Nếu nhận được một LSA độc hại, nội dung CSDL trạng thái liên kết và các đường dẫn ngắn nhất được tính toán sẽ không chính xác

Bảo vệ OSPF

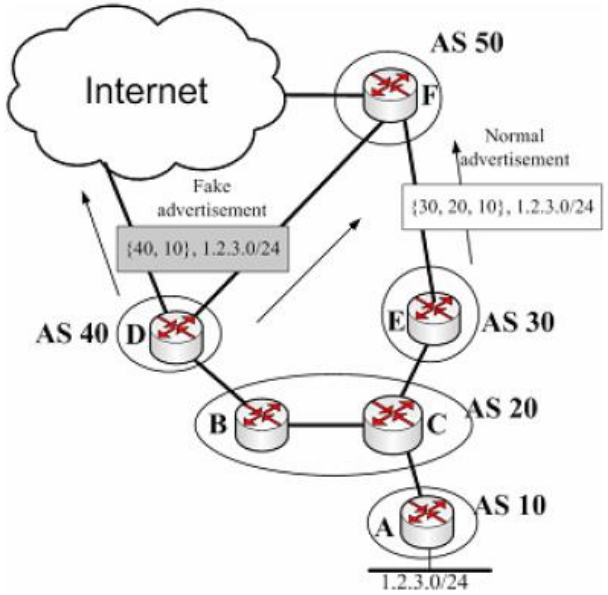
- Mã hóa trạng thái liên kết
  - Thêm chữ ký số vào mọi bản quảng cáo trạng thái liên kết của OSPF
- Giải pháp băm SLS
  - Sử dụng một choỗi băm duy nhất làm mã thông báo xác thực. Để tạo choỗi băm, phải tạo một đại lượng bí mật ngẫu nhiên R, sau đó R được băm n lần sử dụng hàm băm một chiều (SHA, MD5)
- Giải pháp băm FLS
  - Sử dụng hai choỗi băm cho mỗi liên kết. Hai hàm băm khác nhau được sử dụng cho hai choỗi này

Tấn công BGP

- Giao thức định tuyến dạng vector đường đi. Hoạt động dựa trên cập nhật một bảng chứa các địa chỉ mạng cho biết mối liên hệ giữa các hệ thống tự trị AS (autonomous system), tập hợp các hệ thống mạng dưới cùng sự điều hành của một nhà quản trị mạng (ISP) -> chọn đường bằng một tập chính sách và luật
- Lỗ hổng trong BGP
  - Không bảo vệ tính toàn vẹn của dữ liệu và cung cấp xác thực nguồn
  - Không xác thực quyền sở hữu tiền tố của một hệ thống tự trị
  - Không xác thực tính đúng đắn của các thuộc tính đường đi được AS công bố
  - Mục tiêu tấn công
    - Tạo hố đen
    - Chuyển hướng lưu lượng mạng
    - Lật đổ lưu lượng
    - Tính không ổn định

Tấn công BGP

- Prefix hijacking, sử dụng thông báo UPDATE để cung cấp bản cập nhật định tuyến cho các bộ định tuyến BGP khác. Thông báo UPDATE sai có thể bị sử dụng để chiếm quyền prefix



Router D tấn công A

1. Router D chuẩn bị một thông báo UPDATE giả mạo tuyên bố rằng nó có kết nối trực tiếp đến AS10 bằng cách thêm số AS của nó ngay trước AS10 trong đường dẫn AS ({40,10}). Sau đó, Router D gửi thông báo tới AS50 và Internet.

2. Khi AS50 nhận được thông báo giả mạo, nó nhận thấy rằng thông báo có chứa một đường dẫn AS ngắn hơn với độ dài là 2 (nodes) so với thông báo từ AS30 có độ dài là 3 (nodes).

3. Trong trường hợp này, vì đường đi ngắn hơn được ưu tiên, AS50 sẽ chuyển tiếp tất cả lưu lượng dành cho AS10 sang AS40 thay vì AS30. Do đó, lưu lượng sẽ đi qua Router D, giúp nó có thể thực hiện bất kỳ hành động độc hại nào về lưu lượng như nghe trộm và sửa đổi gói tin.

4. Nếu Router D chuyển tiếp lưu lượng đến đích chính xác là AS10, cuộc tấn công này sẽ trở nên rất khó bị phát hiện

Tấn công BGP

- Prefix de-aggregation
- Tấn công quảng cáo mâu thuẫn
- Khai thác việc giảm xóc tuyến đường
- Đối phó với tấn công BGP
  - Secure BGP, Secure origin BGP, interdomain routing validation: đảm bảo tính toàn vẹn của Hop (tin nhắn ko bị sửa đổi), xác thực nguồn gốc, xác thực đường đi
  - Giải pháp lọc đường đi

Tấn công DHCP

- Tấn công DoS DHCP Server dùng Address Stavation
  - Gửi số lượng lớn yêu cầu DHCP với các địa chỉ MAC giả mạo khác nhau đến DHCP server
  - Vì server coi mỗi yêu cầu với MAC mới là từ máy client mới và gán cho nó một địa chỉ IP nên khi hacker gửi số lượng yêu cầu lớn thì dải địa chỉ của server sẽ được cấp phát hết -> hết IP cho các máy client hợp pháp
- Tấn công MIMT dùng DHCP server giả mạo
  - Hacker thiết lập DHCP server giả mạo là máy chủ hợp pháp và trả lại client địa chỉ default gateway giả mạo, hacker có thể chặn các lưu lượng mạng
- Tấn công chuyển hướng DNS dùng DHCP server giả mạo
  - Tương tự MIMT, thay vì default gateway không có thật, máy chủ DHCP giả mạo sẽ gửi máy chủ DNS không có thật.
  - Máy chủ DNS chứa các ánh xạ địa chỉ giả mạo được kiểm soát bởi hacker