AN TOÀN LỚP 2

Nguyen Hong Son

Giới thiệu

- Tập trung an toàn tại lớp data link, đặc biệt quan tâm đến switch security
- Các dịch vụ lớp 2: flow control, acknowledgment, error recovery, maintenance (activation and deactivation) of the link
- Data link technologies:
  - ATM
  - Ethernet
  - Fiber Distributed Data Interface (FDDI)
  - Multi Protocol Label Switching (MPLS)
  - Point-to-Point Protocol (PPP)
  - Token ring
  - High-Level Data Link Control (HDLC)

Tại sao Switch Security là quan trọng

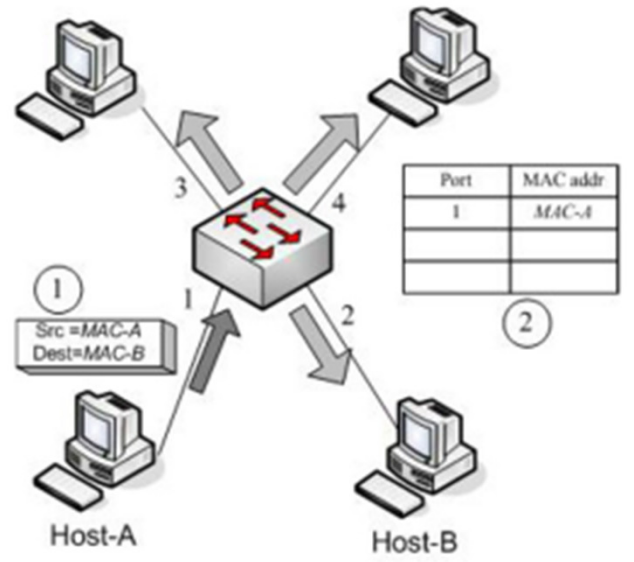
- Toàn bộ communication session sẽ bị xâm hại nếu switch mất an toàn
- Các liên kết trong môi trường WAN thường an toàn hơn so với môi trường LAN
- Với các tool hiện có, một máy tính có thể phát ra các thông điệp điều khiển hay quảng cáo gây phương hại đến các thiết bị lớp 2.
- Một Linux machine + BRIDGE-UTILS package có thể phát sinh các Bridge Protocol Data Units (BPDU) frame

Switch có thể bị tấn công như thế nào?

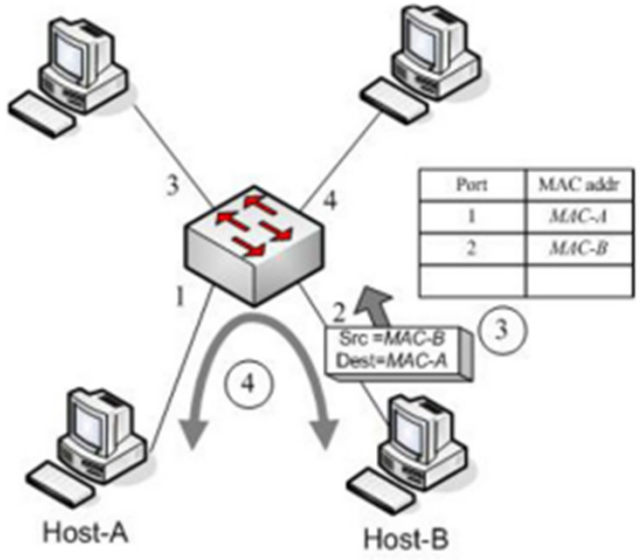
- MAC Flooding
- ARP Spoofing
- STP attacks
- VLAN attacks

MAC Flooding

- MAC flooding attack làm cho switch chuyển hoạt động sang broadcast mode, tác động giống như một hub, giúp sniffing có thể thực hiện dễ dàng
- CAM (Content Addressable Memory) Table
- Thông thường một switch chỉ chuyển lưu lượng đến cổng nối đến host đích, các host khác không sẽ không thấy được lưu lượng giữa hai máy nguồn và đích đang giao tiếp.



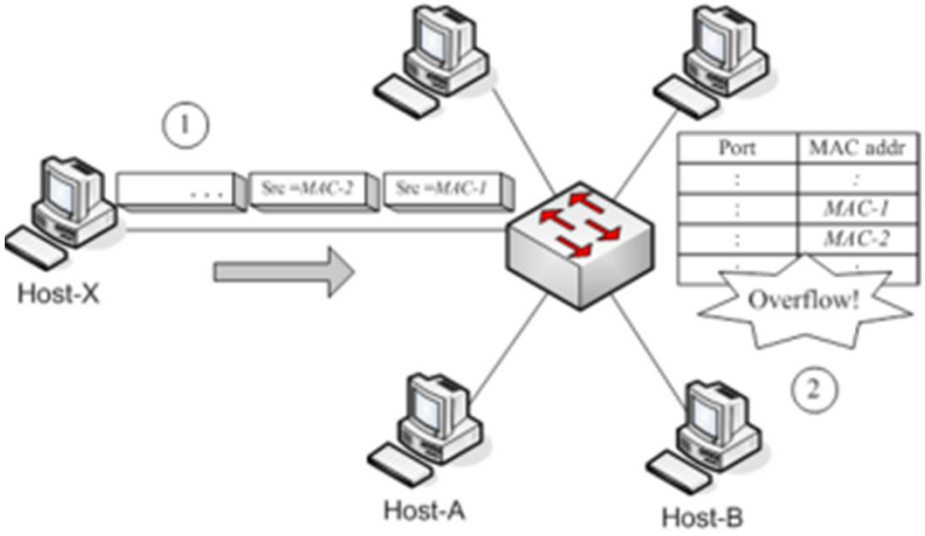
a.

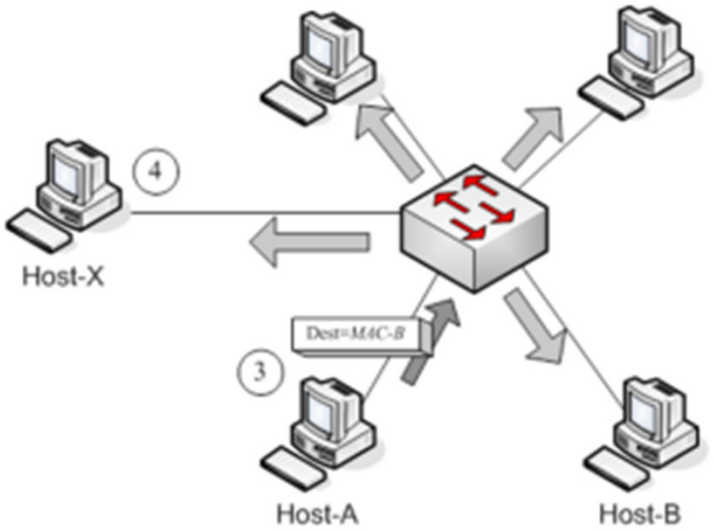


b

MAC Flooding

- Kích thước của bảng CAM là giới hạn. Khi bảng bị tràn switch sẽ quảng bá lưu lượng giống như hub.
- Attacker chỉ cần phát ra hàng hoạt các frame với địa chỉ MAC giả.





MAC Flooding: Giải pháp

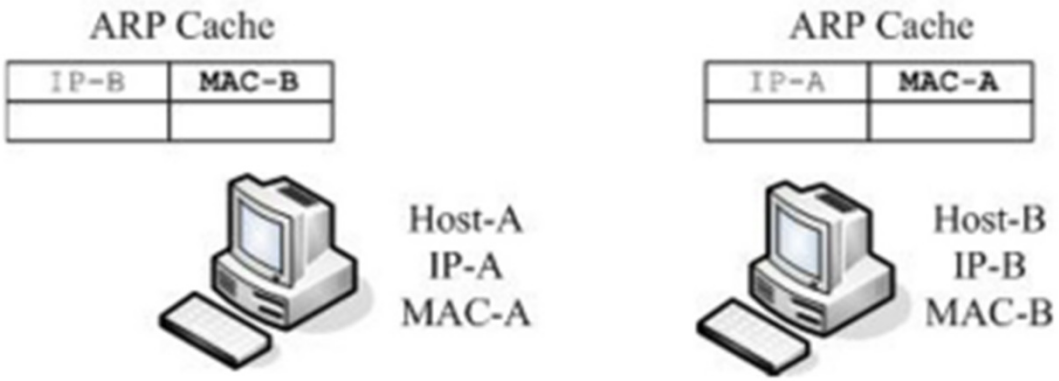
- Cách phổ biến nhằm ngăn chặn MAC flooding attack là giới hạn địa chỉ MAC có thể đăng ký vào một switch port. Đặc tính này được gọi là ***port security***

ARP Spoofing

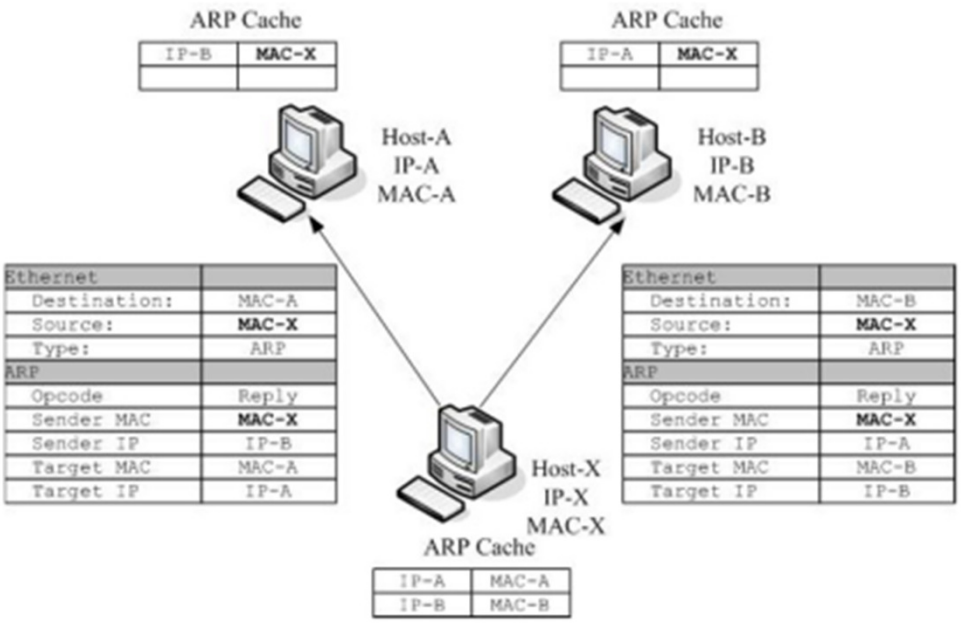
- Một attacker có thể đầu độc một ARP cache với ánh xạ IP-MAC mapping giả mạo, làm chuyển hướng lưu lượng đến đích do hacker chọn.
- Quá trình này được gọi là ARP spoofing

ARP Spoofing

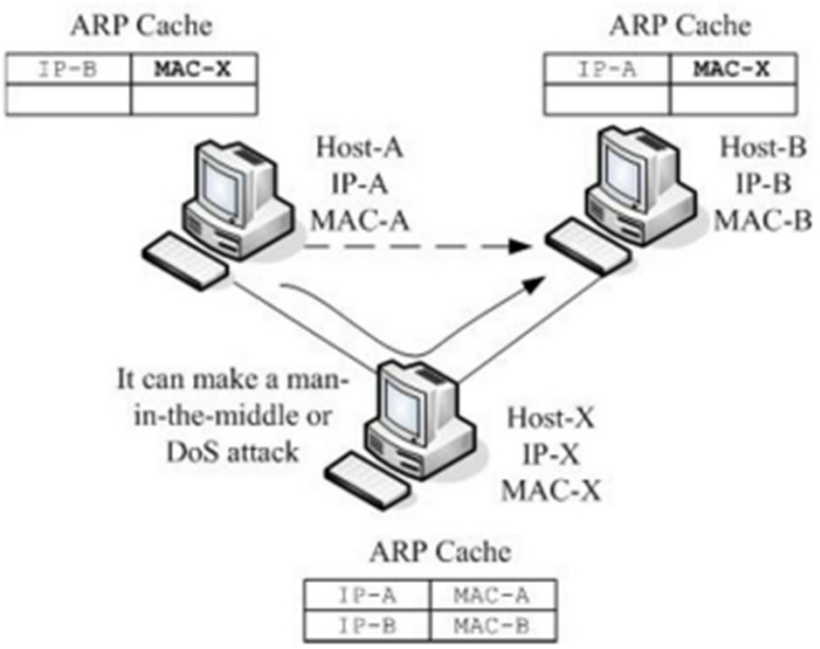
- *Bất cứ khi nào host nhận một ARP reply, nó sẽ cập nhật ARP cache ánh xạ mới IP-MAC mapping*. Điều này có thể bị lợi dụng để đầu độc cache



ARP Spoofing



Host-X đầu độc ARP caches của Host-A và Host-B.



Lưu lượng giữa Host-A và Host-B sẽ đi qua Host-X.

ARP Spoofing

- Sau khi thực hiện ARP spoofing, các tấn công khác có thể được xúc tiến:
  - Man-in-the-middle
  - DoS
  - Hijacking
  - Spoofing WAN Traffic: Nếu một trong hai host là default gateway

Câu hỏi

- Cách tấn công ARP có những hạn chế gì không?

ARP Spoofing: Giải pháp

- Static ARP Entries
- Detection: ARPWatch
- No Cache Update: Chỉ chấp nhận ARP reply và cập nhật các ánh xạ trong cache khi ánh xạ hết hạn sử dụng.

STP attacks

- Thế nào là STP ?
- STP làm việc như thế nào ?

STP: Topology Change (1/5)

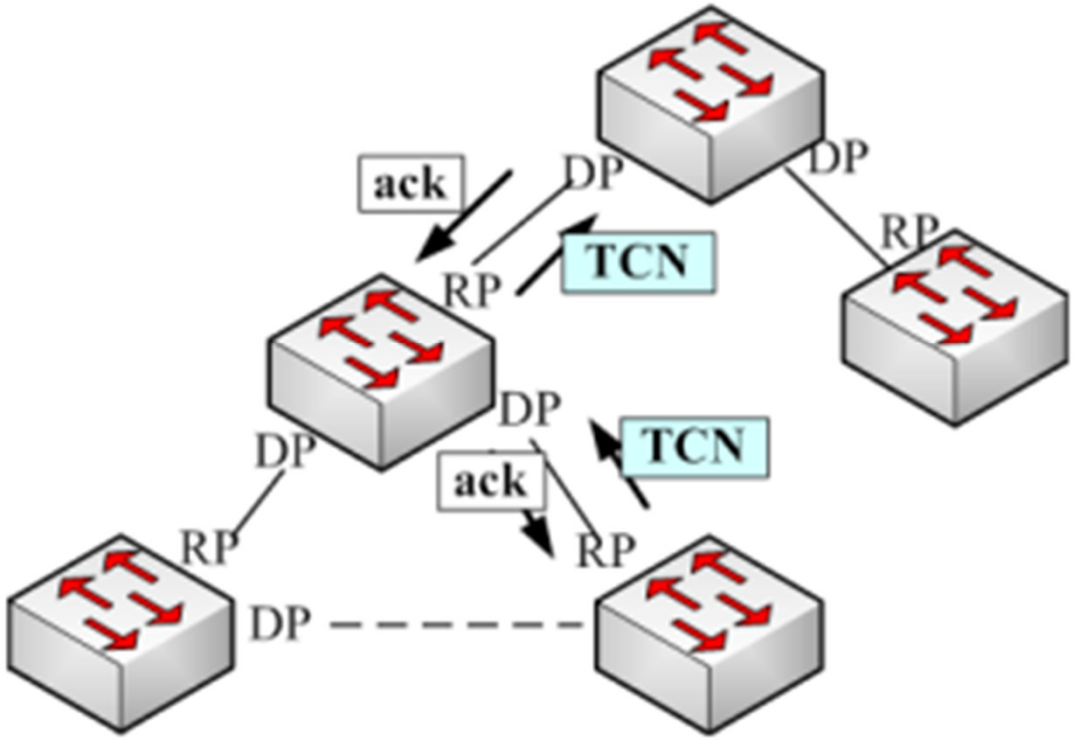
- Tất cả các switch đều tiếp nhận các Hello BPDUs từ Root Bridge một cách định kỳ.
- Nếu một sw không nhận được Hello BPDU trong khoảng thời gian tối đa (Max Age Time- 20s by default), sẽ khởi động quá trình tái cấu hình topo mạng bằng cách gửi Topology Change Notification BPDUs

STP : Topology Change (2/5)

- Khi một sw phát hiện topo thay đổi:

1. Đầu tiên sẽ quảng cáo Topology Change Notification (TCN) BPDU qua root port dẫn đến designated bridge của nó. (được gửi cách nhau bởi thời khoảng hello interval cho đến khi nhận được báo nhận từ upstream bridge.)
2. Sau khi nhận TCN BPDU, designated bridge báo nhận bằng cách replying một Configuration BPDU cờ TCA flag được dựng lên. Bridge này sau đó phát sinh một TCN BPDU khác qua root port của nó để thông báo cho upstream bridge.
3. Quá trình này tiếp tục cho đến khi TCN BPDU gặp Root Bridge

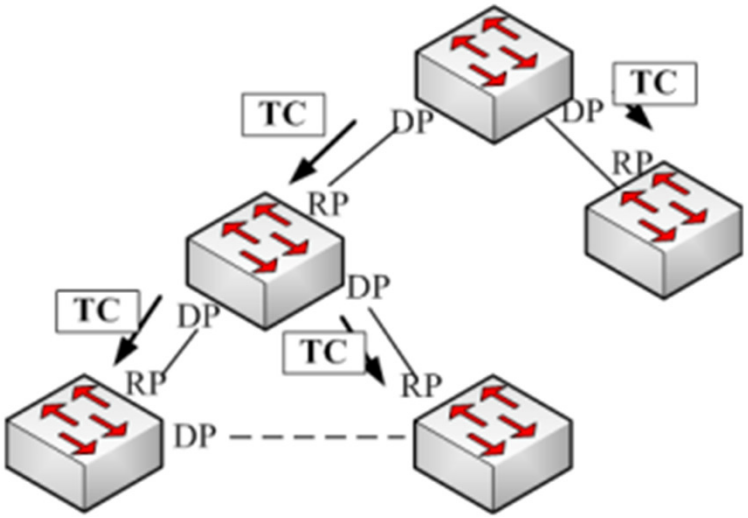
STP : Topology Change (3/5)



STP : Topology Change (4/5)

4. Khi root nhận TCN BPDU, dựng cờ topology change (TC) flag trong tất cả các Configuration BPDU được gửi xuống (trong khoảng thời gian Forward Delay+MaxAge).

5. Các Configuration BPDU với TC flag được dựng sẽ lan truyền trên toàn bộ cây trải rộng (spanning tree). Kết quả là tất cả các sw đều nhận thức được sự thay đổi topo này.



STP: Topology Change (5/5)

- Khi các sw phát hiện TC flag, nó nhanh chóng vô hiệu các mục của bảng CAM.
- Trong thời gian quá độ sự gián đoạn kết nối hay loop cí thể xảy ra.
- Sau khi root hạ cờ TC, các non-root sw bắt đầu các hoạt động học và chuyển lưu lượng theo topo mới. Quá trình mất khoảng 30-50 giây để hội tụ trở lại.

STP attacks: Root claim and MITM

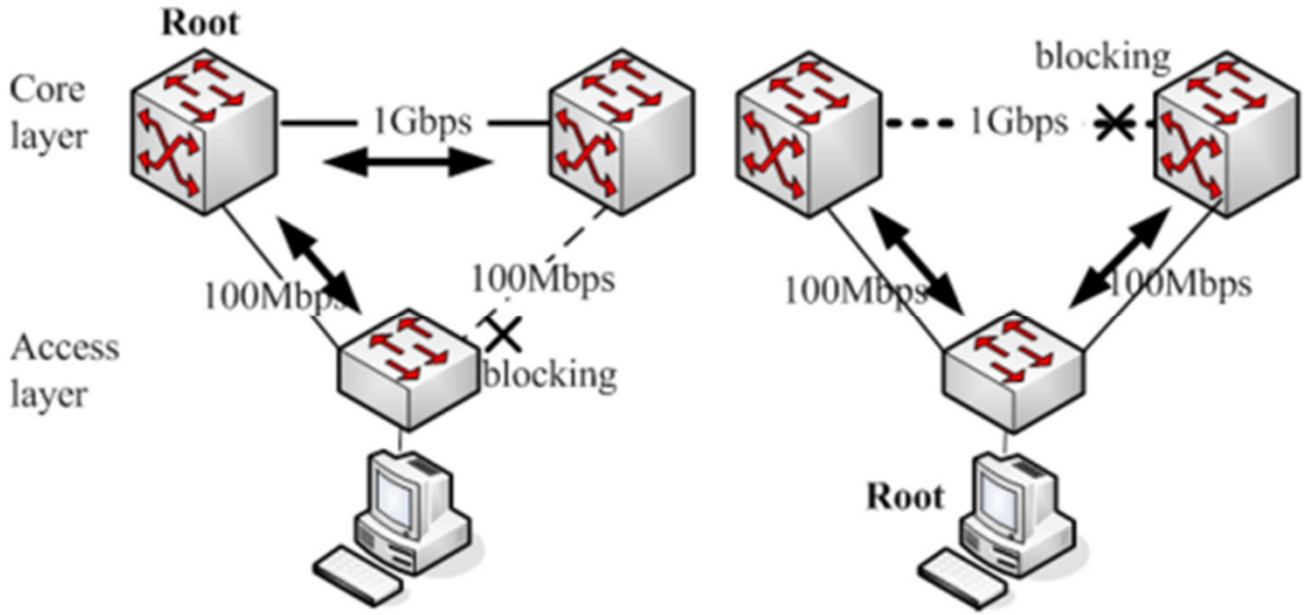
- Bằng cách gửi một BPDU giả mạo với Bridge ID nhỏ nhất, attacker station sẽ được bầu thành new root bridge
- New root có thể sniff tất cả các frame chuyển qua nó, vì nó là “middle” of the spanning tree network (MITM)
- Nếu nó cố ý bỏ qua các TCN, các sw trong mạng sẽ không điều chỉnh theo bất kỳ sự thay đổi nào. Trong trường hợp này STP không đảm bảo một topo không loop.

STP attacks: Eternal root election

- Gây ra sự mất ổn định mạng bằng cách ép mạng ở trạng thái chọn root.
  - Attacker đầu tiên học id của root bridge, root_id (dùng một sniffer)
  - Chèn vào một BPDU với id=root_id – 1
  - Lặp lại quá trình
- Một TCN BPDU từ một sw có thể khiến cho root quảng bá các BPDU với cờ TC flag được dựng, và trên cơ sở nhận các BPDU này các non-root bridge sẽ làm vô hiệu nhanh chóng các bảng CAM.
  - Bằng cách gửi dòng TCN đều đặn, một attacker có thể khiến cho mỗi sw của mạng gây ra tình trạng vô hiệu liên tục.

STP attacks: Affecting network performance

- Bằng cách lấy vai trò root trong cây, một attacker có thể thay đổi luồng lưu lượng trong mạng chuyển mạch



Đường Gigabit link sẽ bị khóa. Tất cả data sẽ được dẫn qua đường 100Mbps link

STP attacks: Giải pháp

- BPDU Guard: Các cổng có BPDU Gaurd được cài đặt sẽ không cho phép các host phía sau nó gửi BPDU
- Root Guard: Các cổng có cấu hình Root Guard không thể trở thành Root Ports

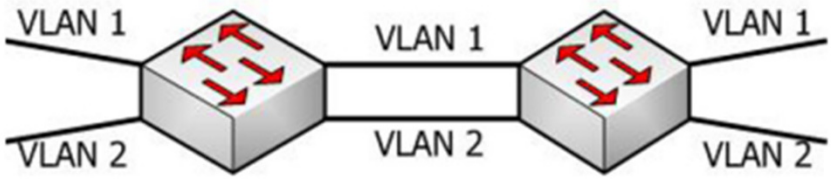
Yêu cầu sinh viên:

-Giải thích tại sao các giải pháp trên có thể hạn chế được tấn công STP

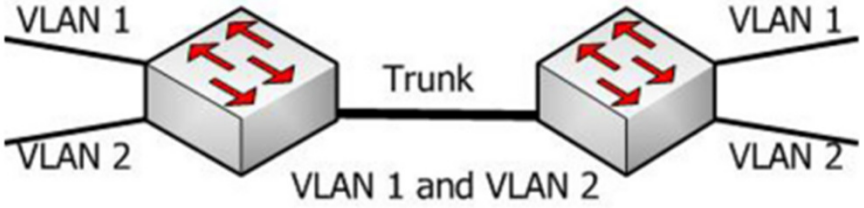
-Tìm thêm thông tin

VLAN attacks

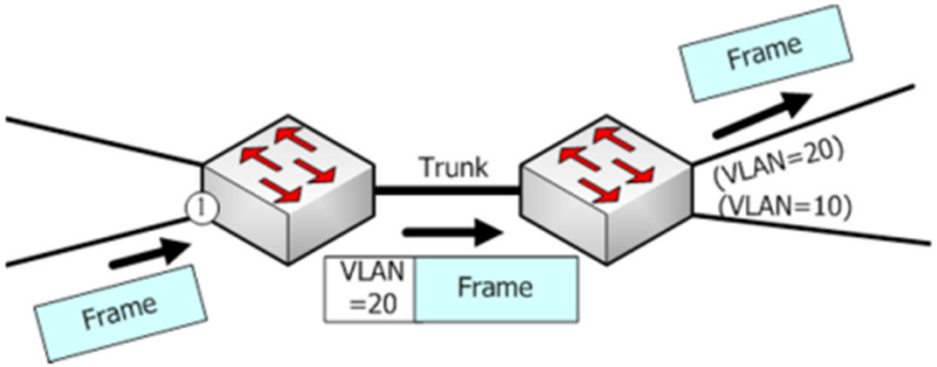
- Thế nào là VLAN?
- VLAN hoạt động như thế nào?
  - Frame Tagging?



a. With out Trunking

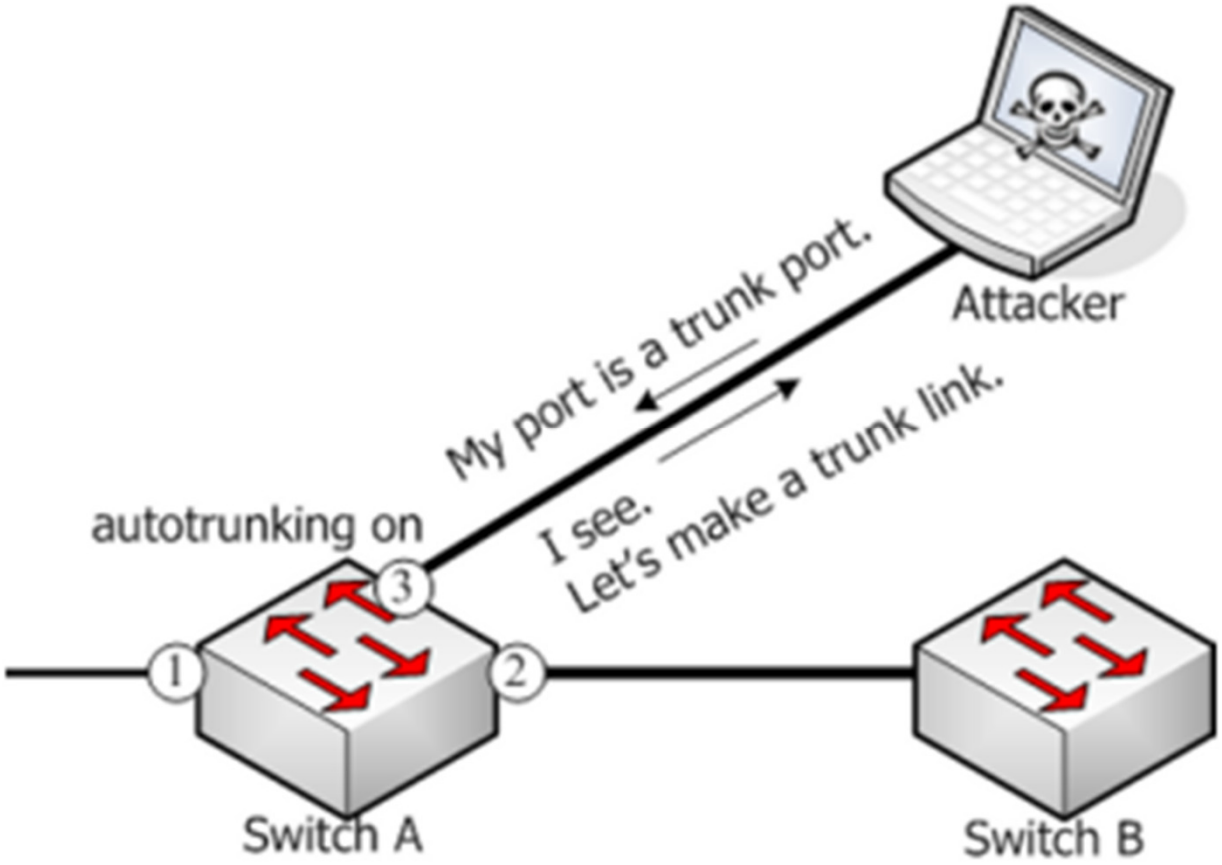


b. With Trunking



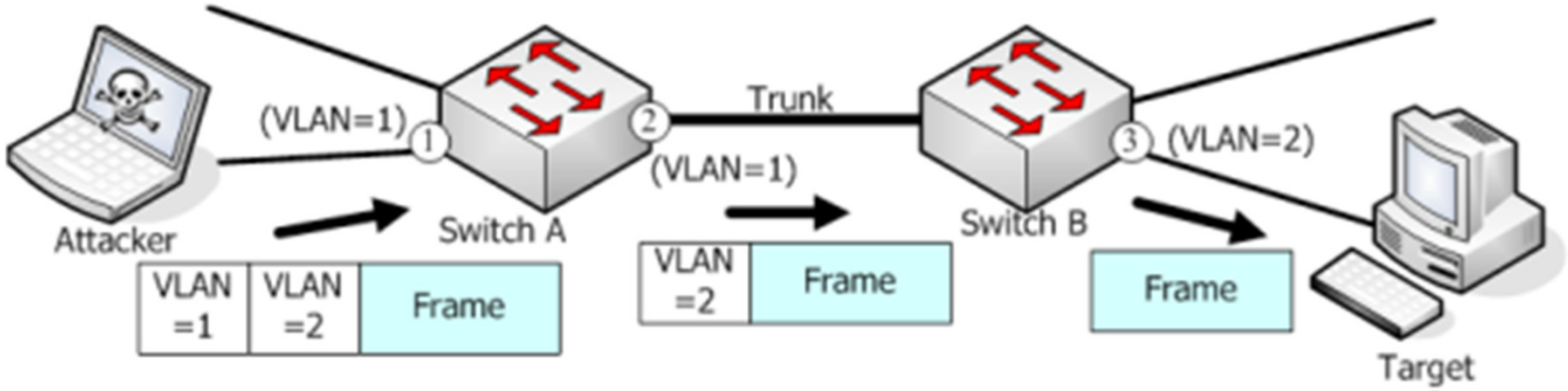
VLAN attacks: VLAN Hopping

- Tách biệt subnets hay zones. Nếu có thể gửi data xuyên qua các zone khác nhau (hopping), chức năng tách biệt của VLAN không hữu hiệu → **VLAN hopping**
- Sw giả mạo nối vào một trong các sw thật, thiết lập trunk link. Hacker có thể nhận các frame từ VLAN và gửi các frame đến các VLAN thông qua trunk port bị lợi dụng.


My port is a trunk port.
I see.
Let's make a trunk link.
Attacker
autotrunking on
3
1
2
Switch A
Switch B

VLAN attacks: Double tagging

- Nếu attacker thêm hai tag vào mỗi frame, có thể đạt được VLAN hopping.



VLAN attacks: Double tagging

- Điều kiện cần để dạng tấn công này thành công:
  - attacker và nạn nhân phải ở trên các sw khác biệt.
  - attacker biết trước địa chỉ MAC của máy nạn nhân.
  - attacker có cùng native VLAN với trunk link. Ví dụ ports 1 và 2 cùng thuộc VLAN 1 là native VLAN theo mặc định.

VLAN attacks: Double tagging

- Một số câu hỏi nghiên cứu :
  - Tại sao Switch A chấp nhận tagged frame từ attacker trên một port (ví dụ port 1 trên hình) không nối trunk ở vị trí đầu tiên?
  - Tại sao Switch A không bổ sung tag vào frame khi gửi ra trunk?
  - Tại sao Switch A không kiểm tra các frame đến xem có nhiều hơn một tag hay không?

Các tấn công VLAN khác

- Đề nghị tham khảo tài liệu:

Steve A. Rouiller, **"Virtual LAN Security: weaknesses and countermeasures**," SANS Institute

HẾT BÀI 3