www.crysys.hu

Layer 2 Security

Tamás Holczer
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
holczer@crysys.hu

Outline

- Intro
- Attacks and countermeasures:
  - VLAN
  - MAC
  - DHCP
  - ARP
  - IP/MAC Spoofing
  - STP
  - VTP
  - CDP
  - HSRP
  - PVLAN
  - IEEE 802.1AE
- Control questions

Layer 2 basics

- Data Link Layer
- Protocol: Ethernet widely used (most common)
- Other protocols: ARP, ATM, CDP, DTP, FR, LLDP, PPP, VLAN …
- Focus of this lecture
  - switched network (hubs disappeared, but WLAN…)
  - manaegable switch
  - IPv4
- Compromise of L2 can cause problems in upper layers

- Attacker must be on the LAN to be attacked

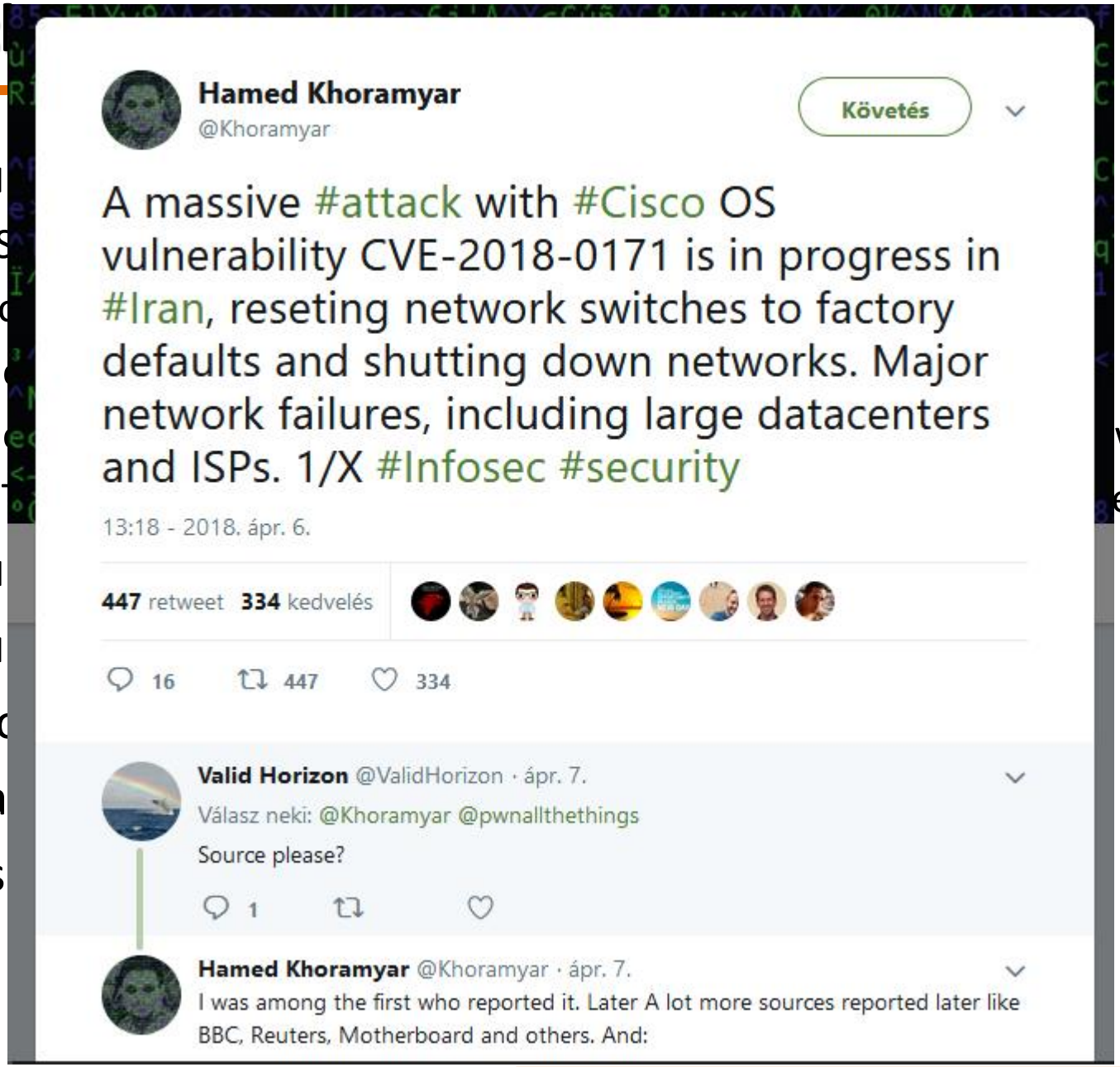
- Most examples are from Cisco (sorry, I am a Cisco instructor…), but similar applies to other vendors

Switch security

- Secure remote management
  - SSH
  - Consol (local)
  - No aux
  - No insecure protocols: SNMP, TFTP, Telnet, FTP (widely used in switches)
  - HTTPS (no http) with proper version, crypto etc. (problematic lifetime)
- Secure image storage
- Secure configuration management
- Up to date OS/firmware
- Separate VLAN for management
- ACLs for management

Switc

- Secu
  - SS
  - Co
  - N
  - N witches)
  - H etime)
- Secu
- Secu
- Up to
- Sepa
- ACLs



CVE-2018-0171

Critical

Advisory ID:	cisco-sa-20180328-smi2	CVE-2018-0171	Download CVRF
First Published:	2018 March 28 16:00 GMT	CWE-20	Download PDF
Last Updated:	2018 April 6 19:35 GMT		Email
Version 1.3:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvg76186		
CVSS Score:	Base 9.8		

Summary

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device.

The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts:

- Triggering a reload of the device
- Allowing the attacker to execute arbitrary code on the device
- Causing an indefinite loop on the affected device that triggers a watchdog crash

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

CVE-2018-0171

- https://thehackernews.com/2018/04/hacking-cisco-smart-install.html

Cisco Smart Install (CVE-2018-0171)

Search for Port:4786 Cisco returned 165,650 results on 08-04-2018

Top Countries

1. United States	46,338
2. Russian Federation	12,302
3. China	10,032
4. Japan	9,356
5. Korea, Republic of	8,014
6. United Kingdom	7,959
7. Taiwan	5,216
8. France	4,324
9. Canada	4,031
10. India	3,934

According to Internet scanning engine Shodan, more than 165,000 systems are still exposed on the Internet running Cisco Smart Install Client over TCP port 4786.

Don’t mess with our elections

- Attack based on Cisco Smart Install itself (no vuln)
- Lack of authentication
- Mitigation: disable Cisco Smart Install

Don’t n

- Attack
- Lack of
- Mitigat

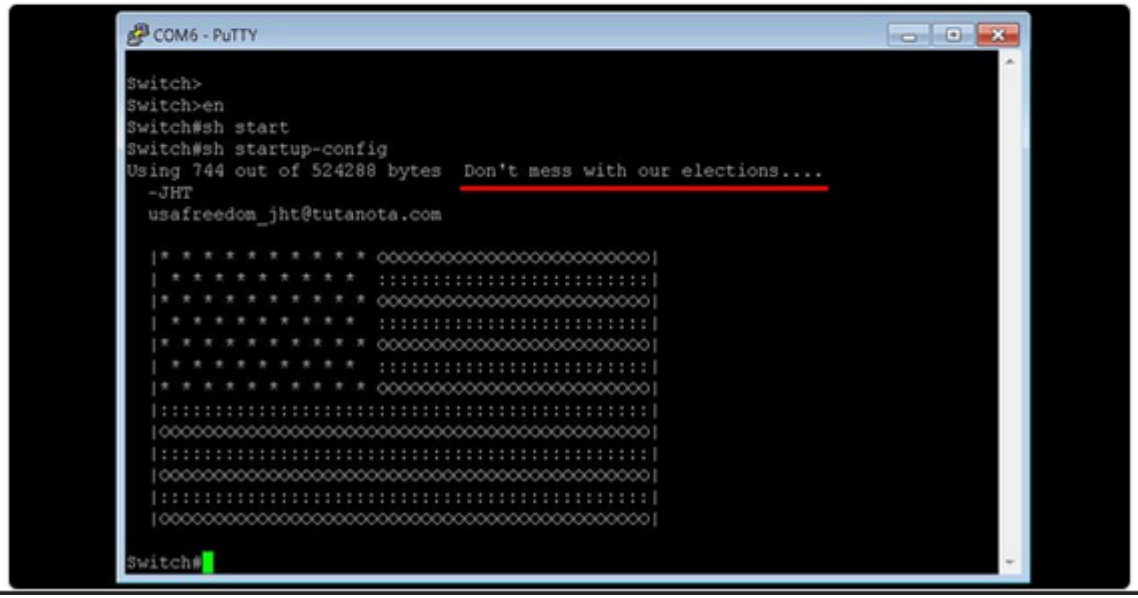
The Hacker News
@TheHackersNews

Követés

Here’s how thousands of Cisco Network Switches in Russia & Iran were hacked to display 'Don't Mess with our Elections' message

thehackernews.com/2018/04/hackin ...

Researchers confirm it has nothing to do with a recently disclosed RCE exploit (CVE-2018-0171) for Cisco Smart Install Client

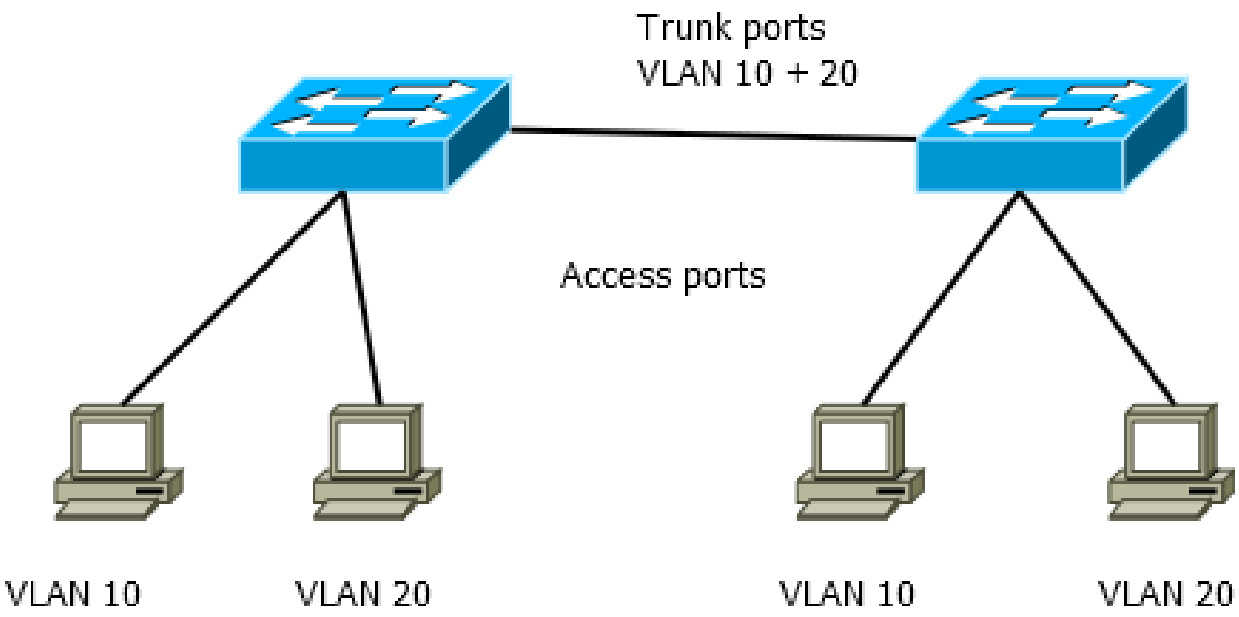


VLANs perspectives

Questions	NetOPS	SecOPS
• Security Policy for VLANs	• We have L2 security issues?	• I handle it at L3 and above
• Do you use VLANS often	• I use them all the time	• I have no idea how often
• Do you use VLANs for security?	• Routing in and out of the same switch are fine, that is why we have a Layer 3 switch	• It is a switch, why would I care?
• What addresses are assigned per VLAN?	• Security Guy asks for a segment, I make a VLAN and give it	• I ask NetOPS they, they give me Ports and addresses

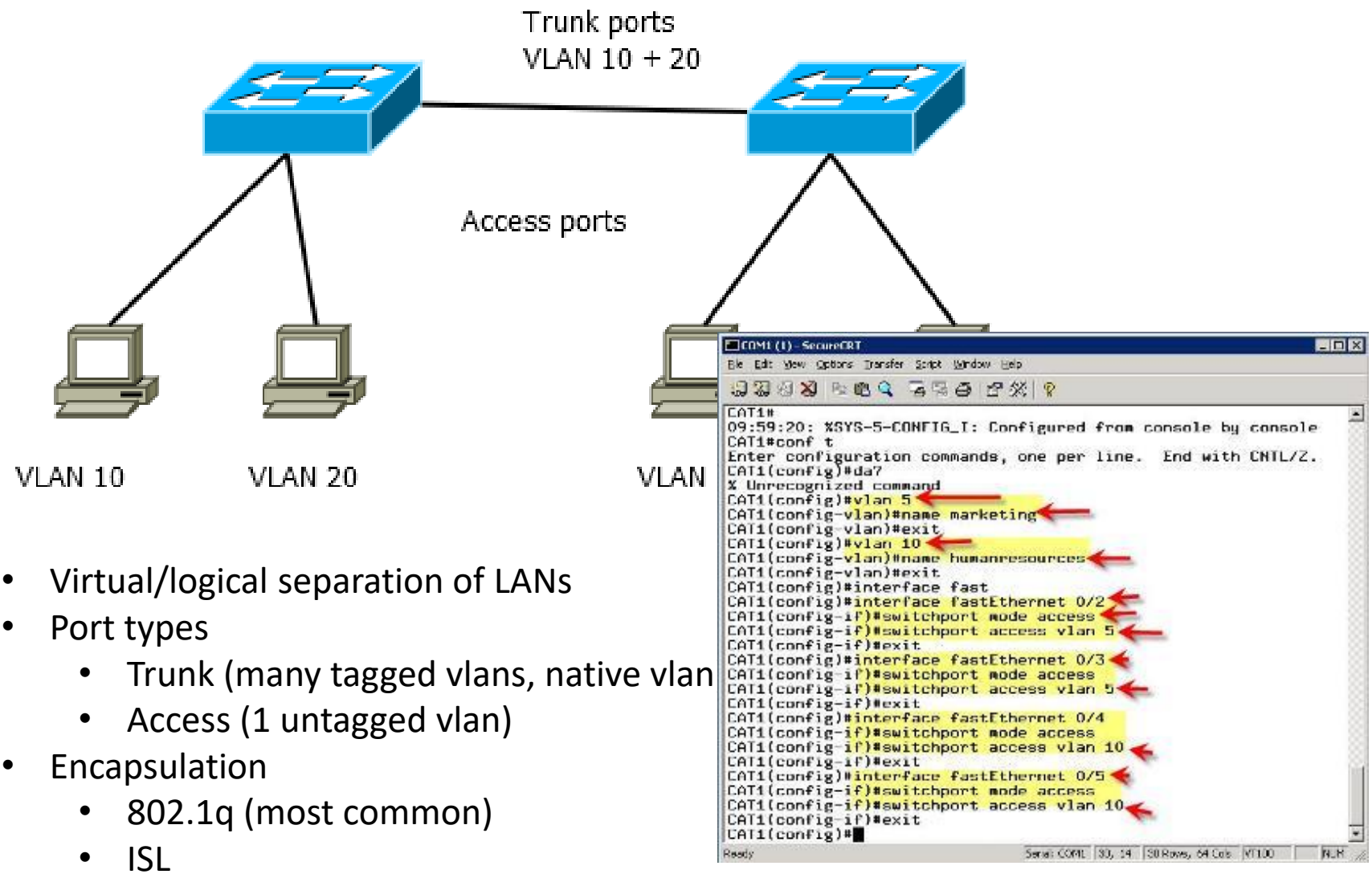
From Yusuf Bhaiji

VLANs



- Virtual/logical separation of LANs
- Port types
  - Trunk (many tagged vlans, native vlan)
  - Access (1 untagged vlan)
- Encapsulation
  - 802.1q (most common)
  - ISL
- DTP/VTP to share VLAN info

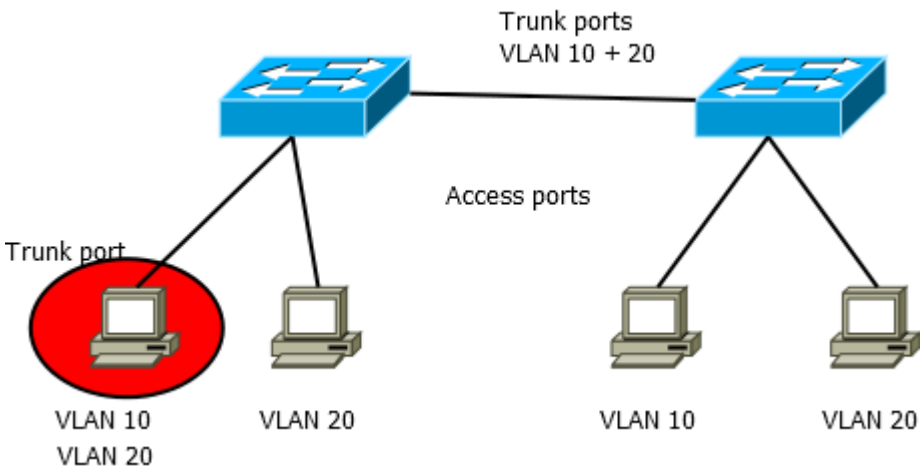
VLANs



- Virtual/logical separation of LANs
- Port types
  - Trunk (many tagged vlans, native vlan
  - Access (1 untagged vlan)
- Encapsulation
  - 802.1q (most common)
  - ISL
- DTP/VTP to share VLAN info

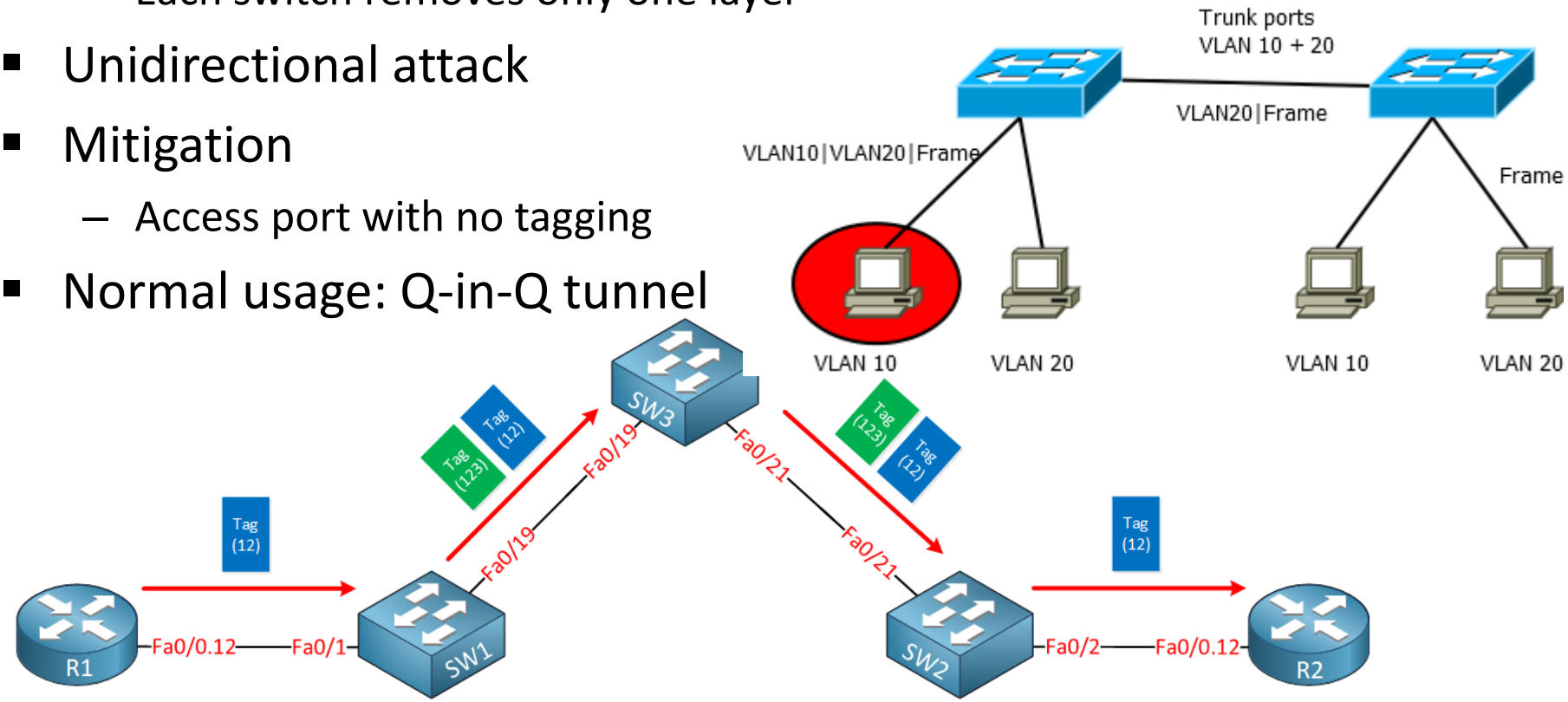
Basic VLAN hopping

- DTP: Dynamic Trunk Protocol
  - Switch can negotiate with neighbors VLAN information
- Attacker sends DTP frames to become all VLAN member
  - Attacker can inject frames to any VLAN
- Solution
  - DTP Off on access ports



Double encapsulation VLAN hopping

- DTP: Dynamic Trunk Protocol
  - Switch can negotiate with neighbors VLAN information
- Attacker sends double encapsulation
  - Each switch removes only one layer
- Unidirectional attack
- Mitigation
  - Access port with no tagging
- Normal usage: Q-in-Q tunnel

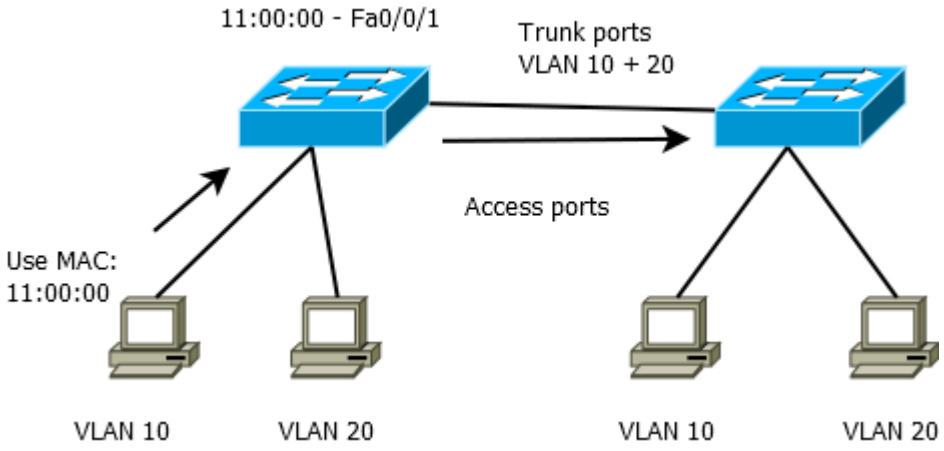


VLAN hardening tips

- Disable unused ports and put them in an unused VLAN
- DTP off for access ports
- Access mode on user facing ports
- Do not use DTP or VTP (but harder to maintain)
- Explicitly configure trunking
- Do not use default vlan (VLAN 1) for anything

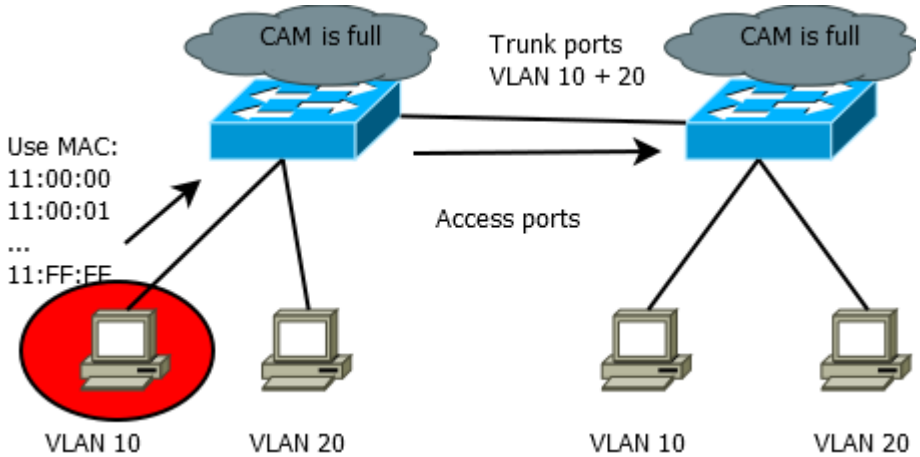
MAC table flooding 1.

- Each switch has a MAC table (CAM – Content Adressable Memory) with fixed size
  - Special (expensive) hardware for efficient lookup
  - MAC – Port – VLAN information
  - Can be addresed by content



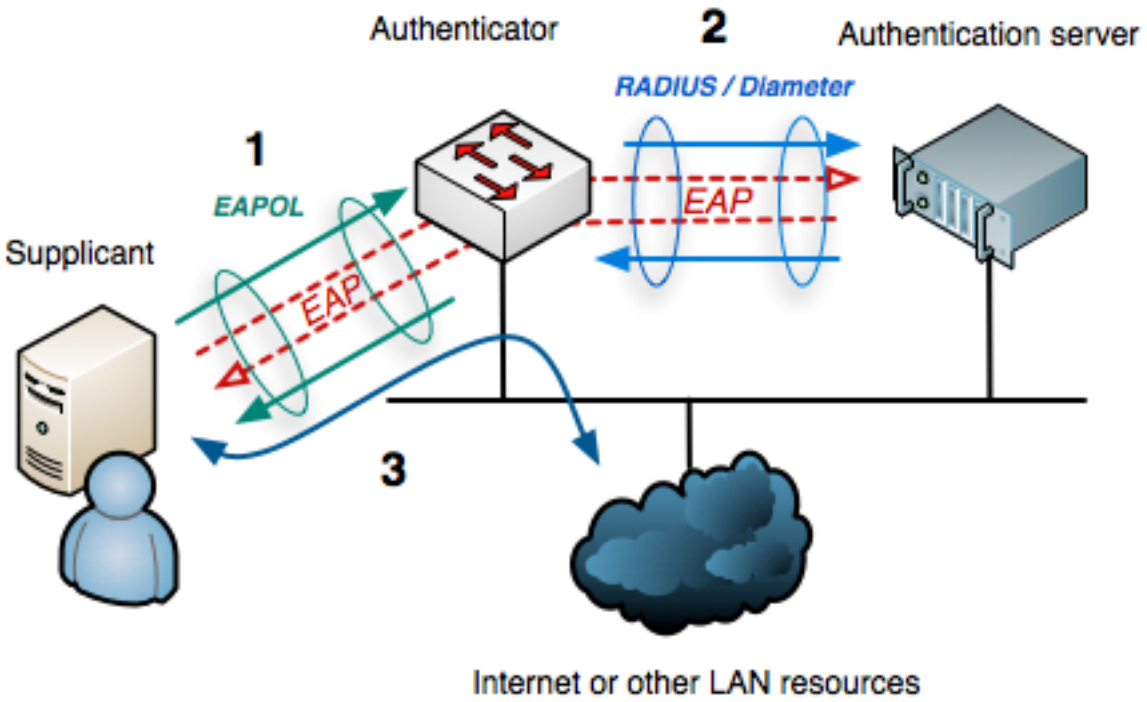
MAC table flooding 2.

- Attack: fill the table with random data
  - Switch is degraded to hub functionality (still no inter vlan traffic)
  - Neighboring switches are filled by the victim switch
- Mitigation: Port security
  - Configure mac – port pairs in advance (admin nightmare)
  - Sticky learning (still…)
  - Configured max number of values
  - Can cause 99% CPU utilization



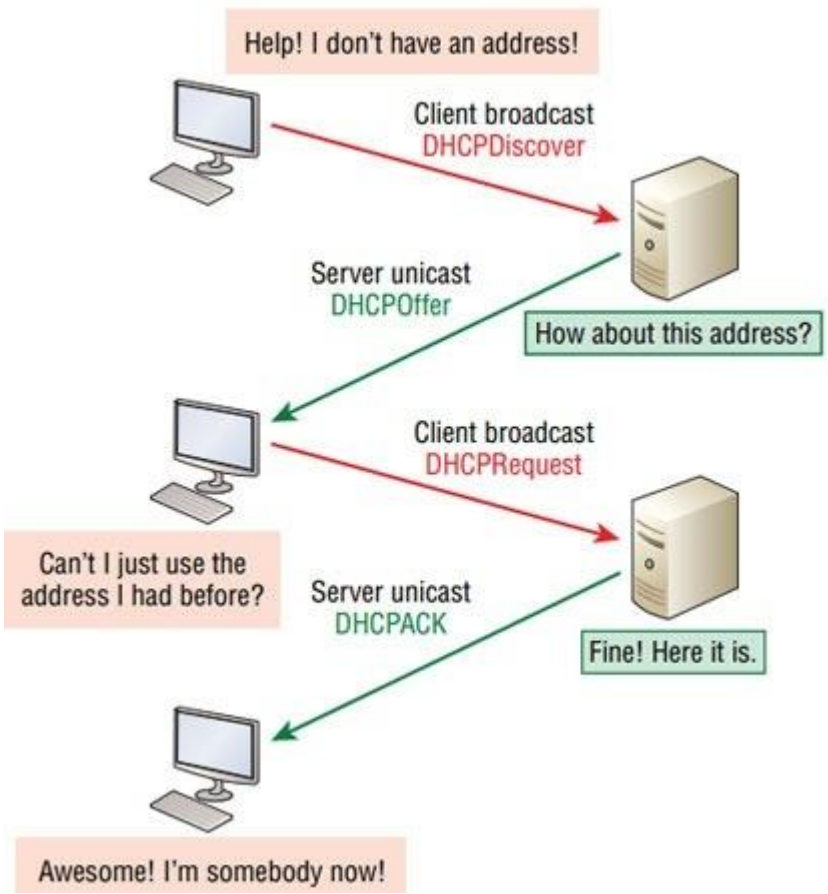
Mitigation: 802.1X

- Port based Network Access Control
- EAP over LAN
- Certificate based normally
- Username/password can be used



DHCP Attacks 1.

- RFC 2131
- Assigns IP addresses on demand
  - IP address
  - Netmask
  - Lease time
  - Server IP
- Uses addresses from pool
- Multiple DHCP servers can coexist in one network
- Other info:
  - Default gateway
  - DNS
  - …



https://fossbytes.com/dhcp-how-does-it-work/

DHCP Attacks 2. Starvation

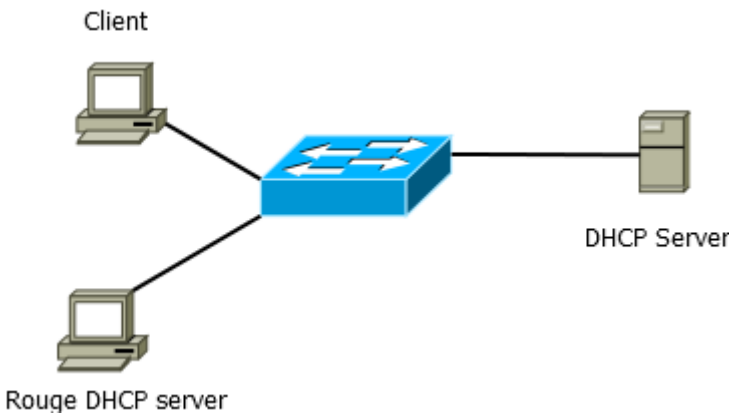
- Other message types
  - DHCPNAK (S → C) address is incorrect
  - DHCPDECLINE (C → S) address is already in use
  - DHCPRELEASE (C → S) client cancelling remaining lease
  - DHCPINFORM (C → S) client already has an address, but ask for other info

- Starvation attack:
  - One client asks for many addresses
  - Newcomer cannot be served
  - DoS type attack

- Mitigation: Port security (see MAC table flooding)
  - Still problem if pool is small and port security is not strict

DHCP attacks 3. Rouge Server

- Rouge DHCP server:
  - Simple PC runs a DHCP server
- Potential problems:
  - IP address collision (DoS)
  - Attacker is the default gateway
  - Attacker is the DNS server
  - Routing problems
  - Typcial when installing a Wifi AP with DHCP enabled in a wired infrastructure

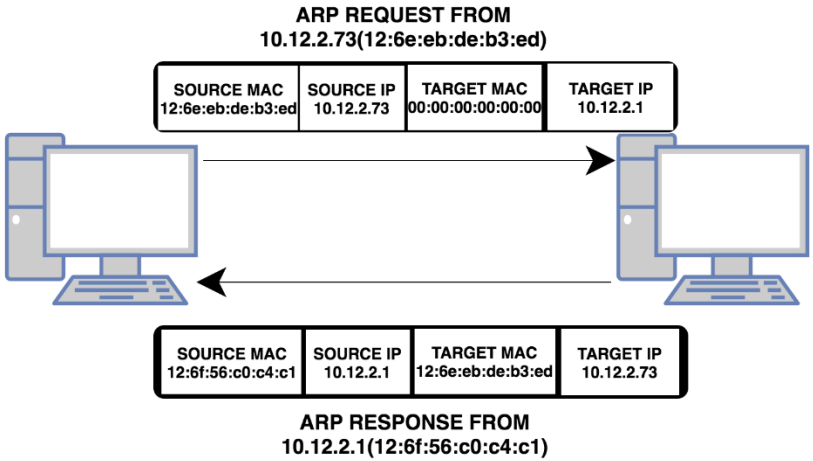


DHCP attacks 4. DHCP Snooping

- Interface: Trusted or Untrusted
- Default: Untrusted
- Per VLAN configuration
- Untrusted: client interface
- Trusted: Uplink or DHCP Server
- Drop traffic:
  - DHCP server messages from untrusted interface
  - Ethernet MAC and DHCP MAC mismatch
  - Release or decline messages from wrong interface (not from expected)
- Problems:
  - Rigid topology
  - client uses 2 interfaces inconsistently
  - Limited DHCP Binding table size

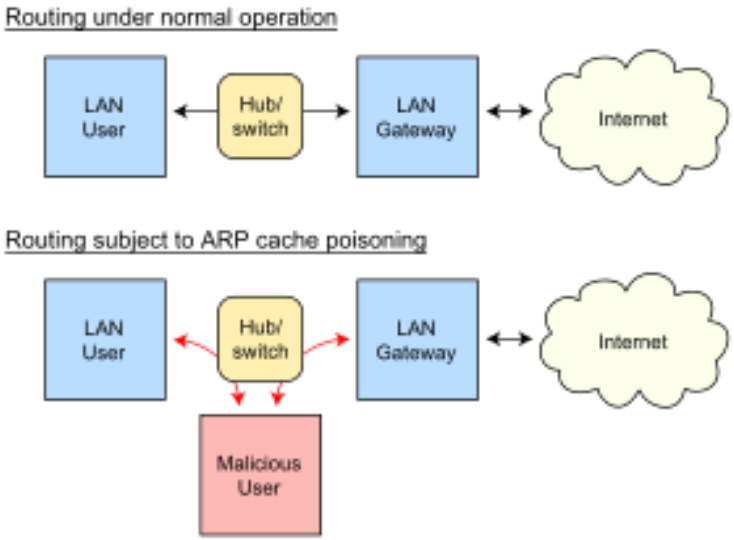
ARP

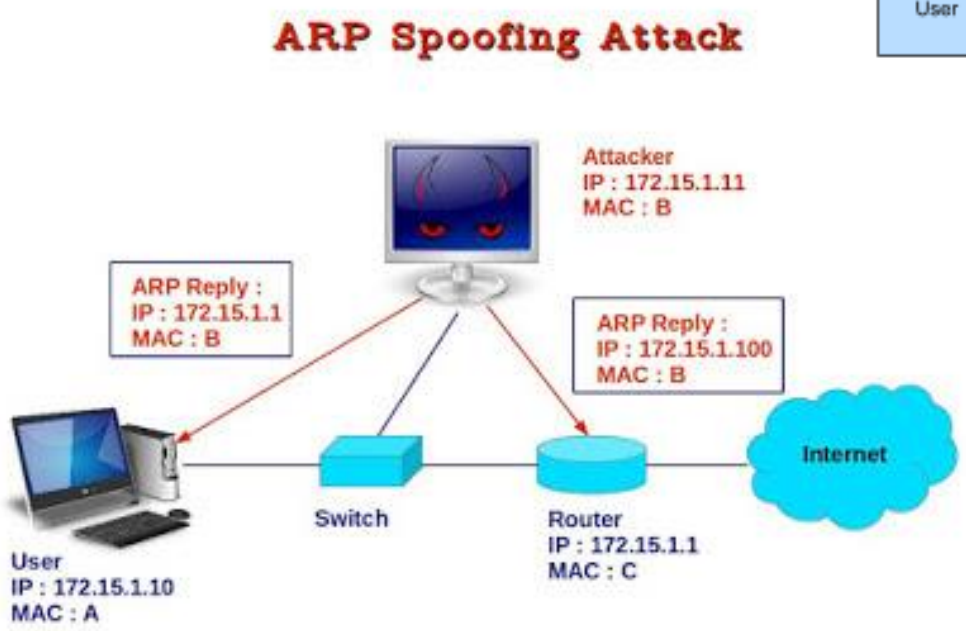
- RFC 826 (1982: An Ethernet Address Resolution Protocol)
- Look up MAC address based on IP address
- Request: broadcast
- Reply: unicast
- Gratuitous ARP: request/reply that is not normally needed according to the ARP specification (ARP *request* or ARP *reply*)
  - request (srcIP=dstIP): to detect IP conflict
  - reply: moved stations
  - update CAM table
  - indication of boot up / reboot



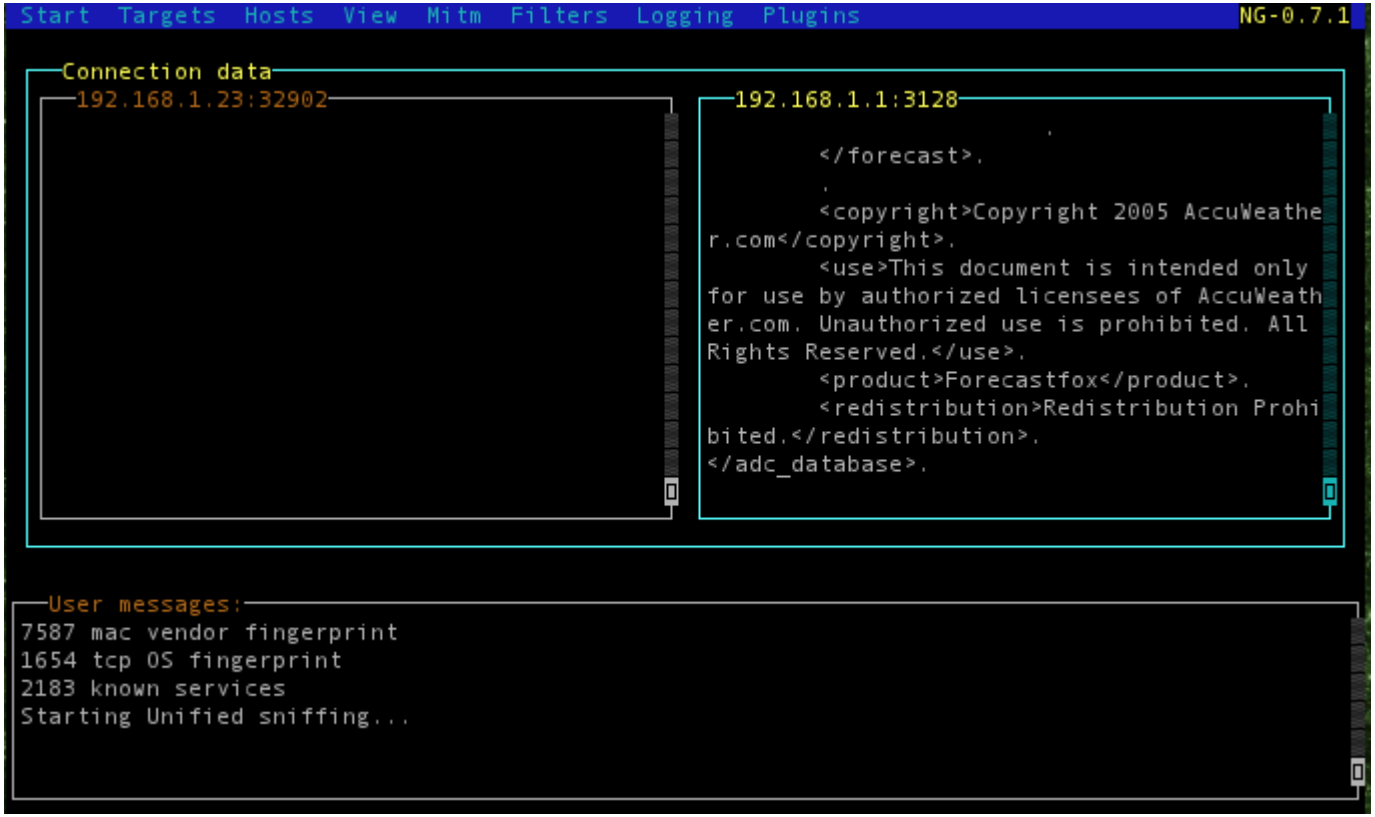
ARP attacks

- Easy to use tools
- Uses gratuitous ARP
- Problem?



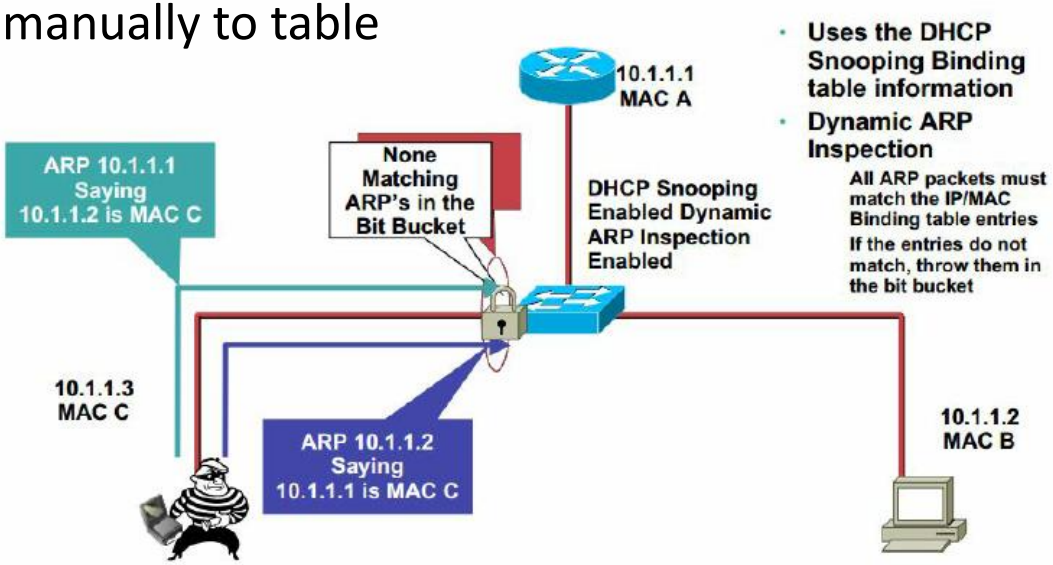


ARP: Ettercap



ARP: Dynamic ARP Inspection & ARPWatch

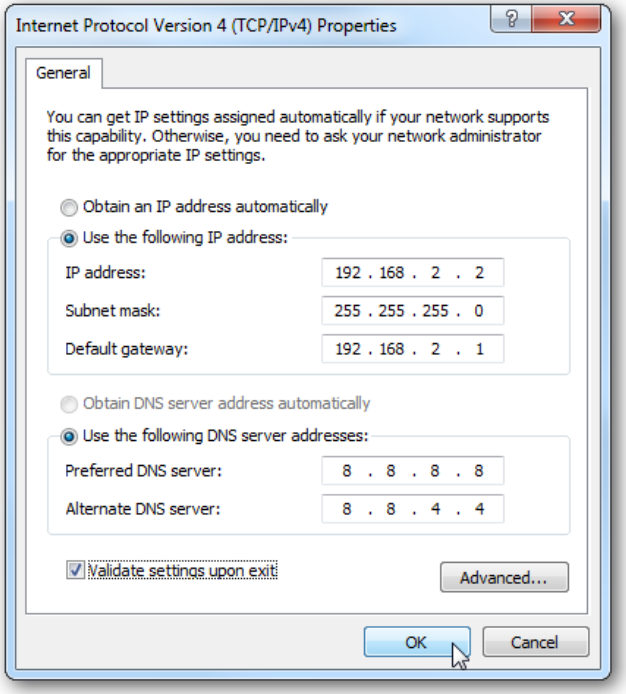
- Based on DHCP Snooping Binding table
- Drop if ARP reply does not match DHCP Snooping Binding table
  - Difference in MAC IP binding
  - Missing record
- Problem with static addresses
  - Must add static addresses manually to table
  - Easy to forget to add
  - Easy to forget to remove

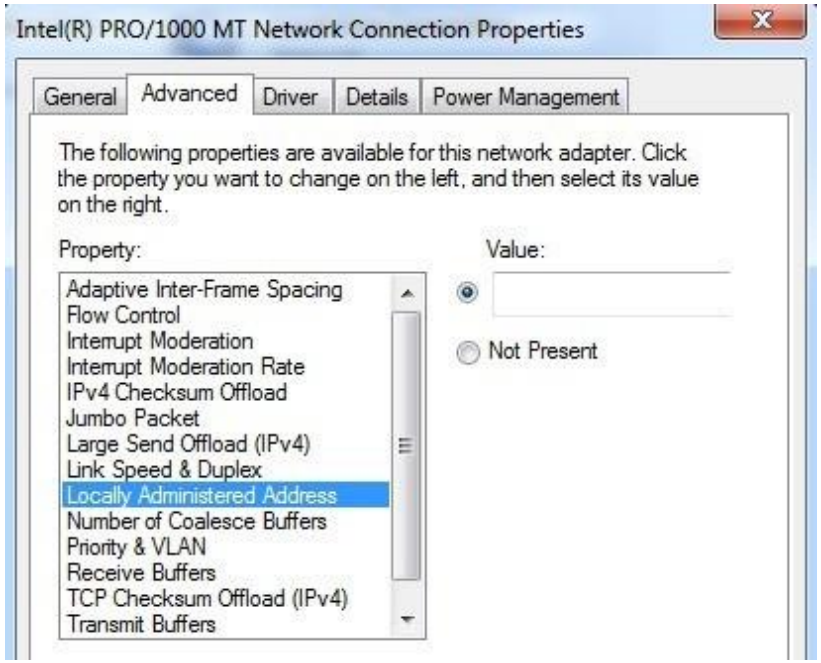


- ARPWatch:
  - Free tool
  - Server/VLAN
  - Lot of false alerts

MAC/IP Spoofing

- Send traffic with altered MAC address
  - Easy with Linux, Windows, OS X …
- Send traffic with altered IP address
  - Easy with Linux, Windows, OS X …





MAC/IP Spoofing mitigation: IPSG

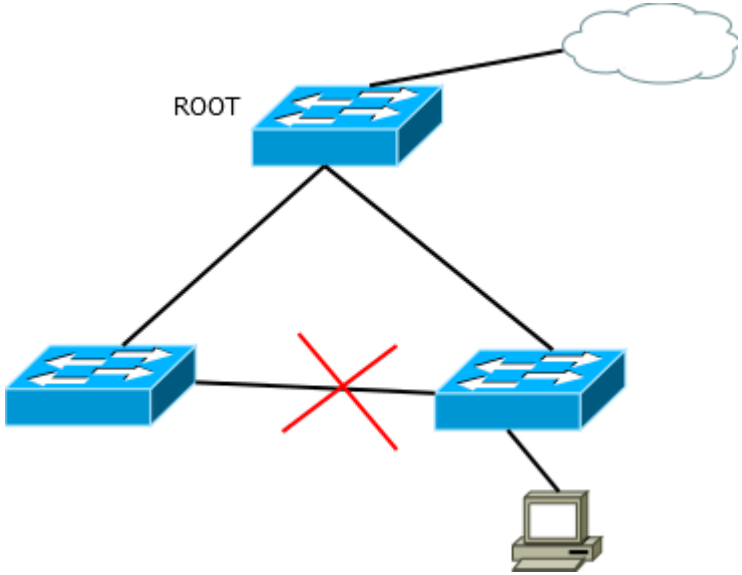
- IP Source Guard
- Based on DHCP Snooping Binding table
- Similar to Dynamic ARP Inspection but checks every IP packet
- Drop if IP packet does not match DHCP Snooping Binding table
  - Difference in MAC IP binding
  - Missing record
- Problem with static addresses…

MAC/IP Spoofing mitigation: DHCP Option 82

- DHCP relay agent information option
- Information about the „physical attachment” of the client
- Operation:
  - Switch inserts 82 info option into DHCP requests
  - Server uses that information
  - Switch strips from response the 82 Option
- Parts:
  - Circuit ID = interface, VLAN (e.g.: ge-0/0/10:vlan1)
  - Remote ID
  - Vendor ID
- Microsoft does not support option 82

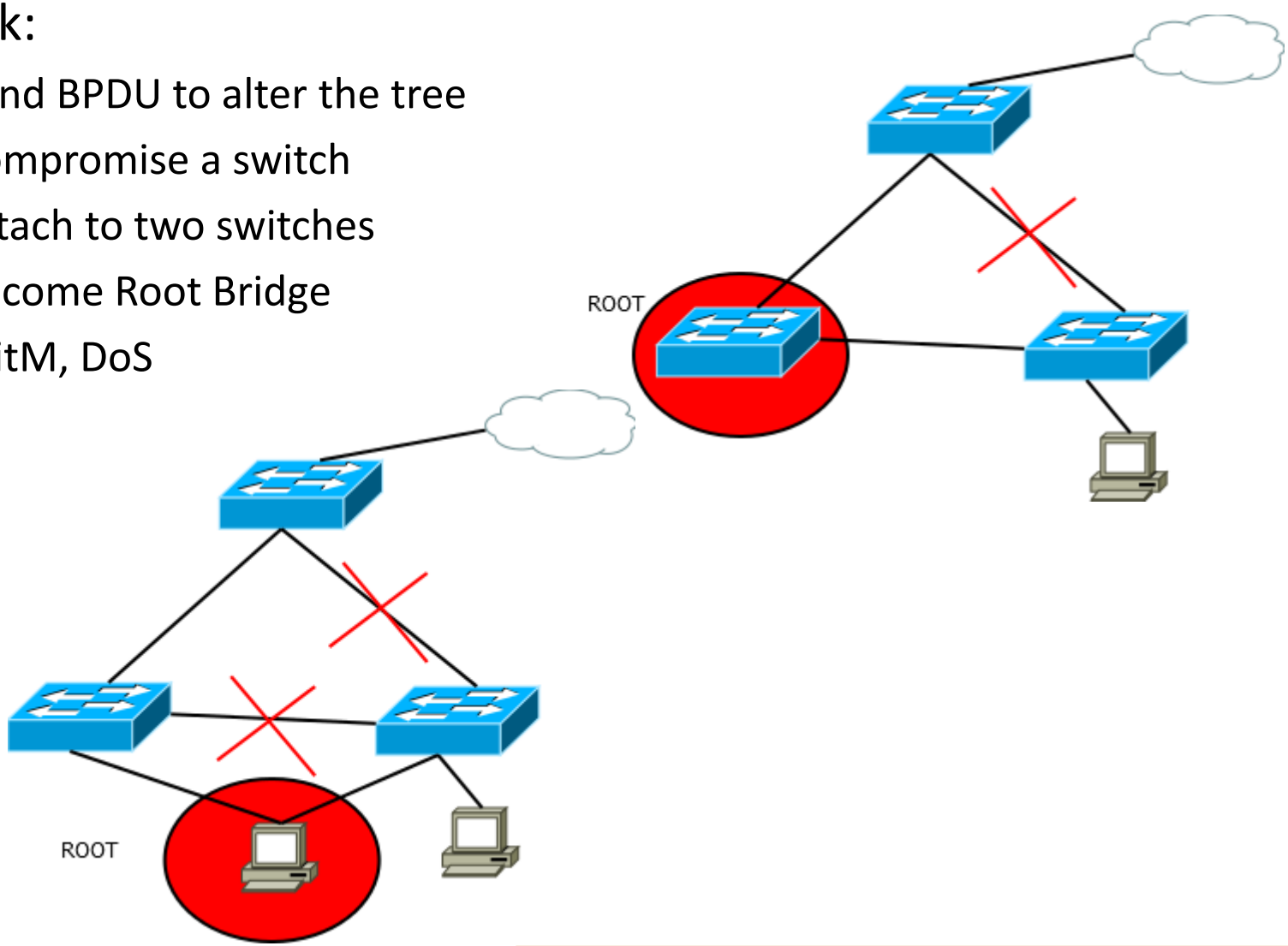
STP basics

- Spanning tree protocol
- Maintain loop free topology
- Goal: avoid (broadcast) storms
- Protocol
  - Elects Root bridge (the head)
  - Switches off links to avoid
    - » Loops
    - » Parallel links



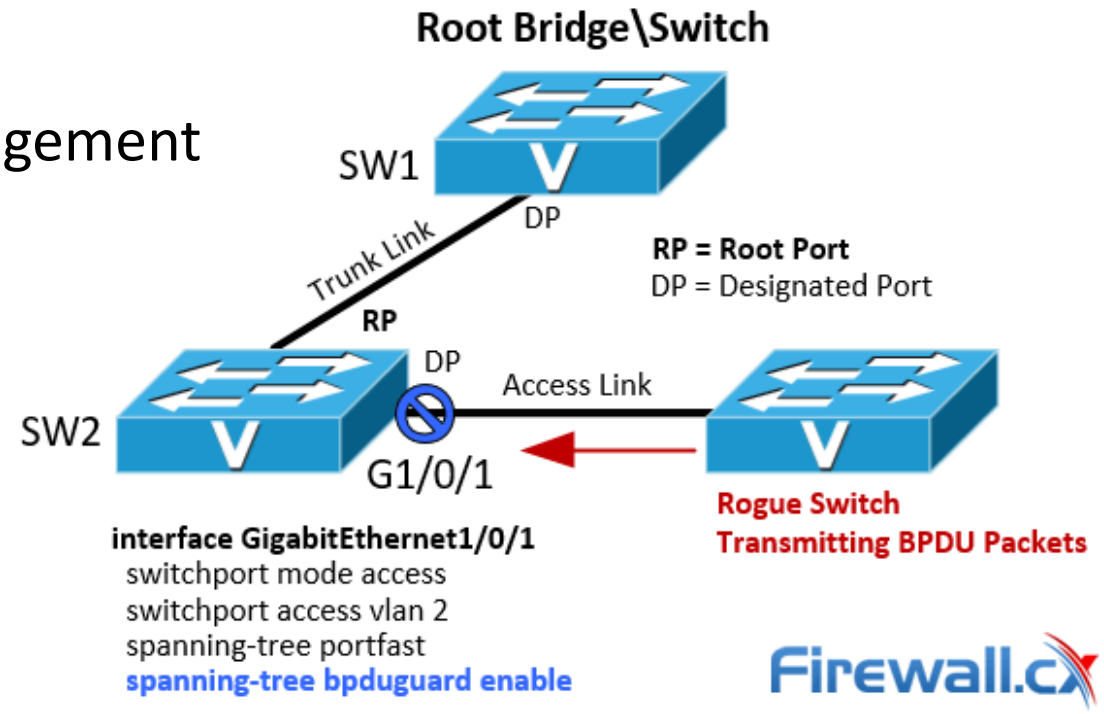
STP attacks

- Attack:
  - Send BPDU to alter the tree
  - Compromise a switch
  - Attach to two switches
  - Become Root Bridge
  - MitM, DoS



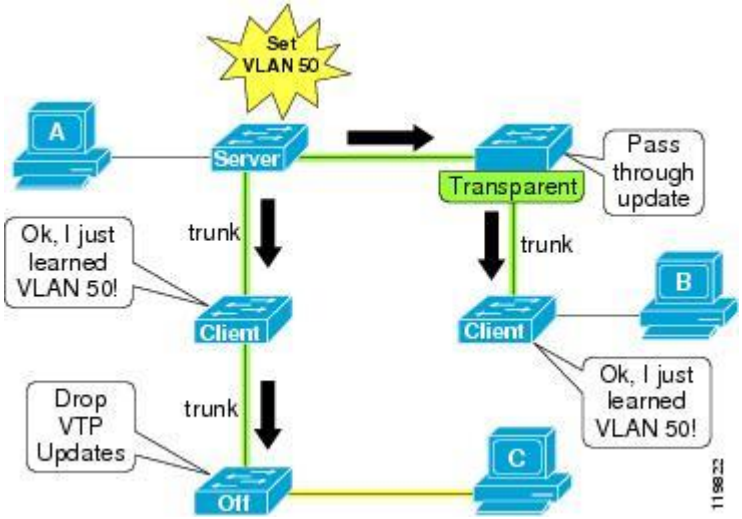
STP attacks, mitigations

- Use loop free topology (but what about redundancy?)
- BPDU guard: no BPDU traffic from client facing ports
- Root guard: port remains designated port (no RP)
- Secure communication with network devices
- Password policy
- Separate VLAN for management



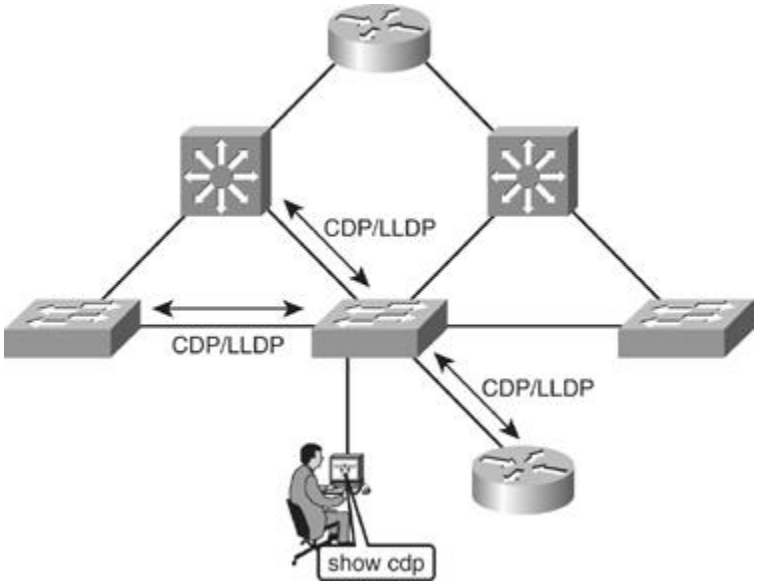
VTP

- VTP (VLAN Trunking Protocol)
  - Cisco proprietary
  - VLAN information is distributed from VTP servers
  - Messages are not protected
  - Attacker can send any VLAN list (e.g. empty list –> delete VLANs)
  - Mitigation:
    - » Disable VTP
    - » Use passwords for MD5 authentication



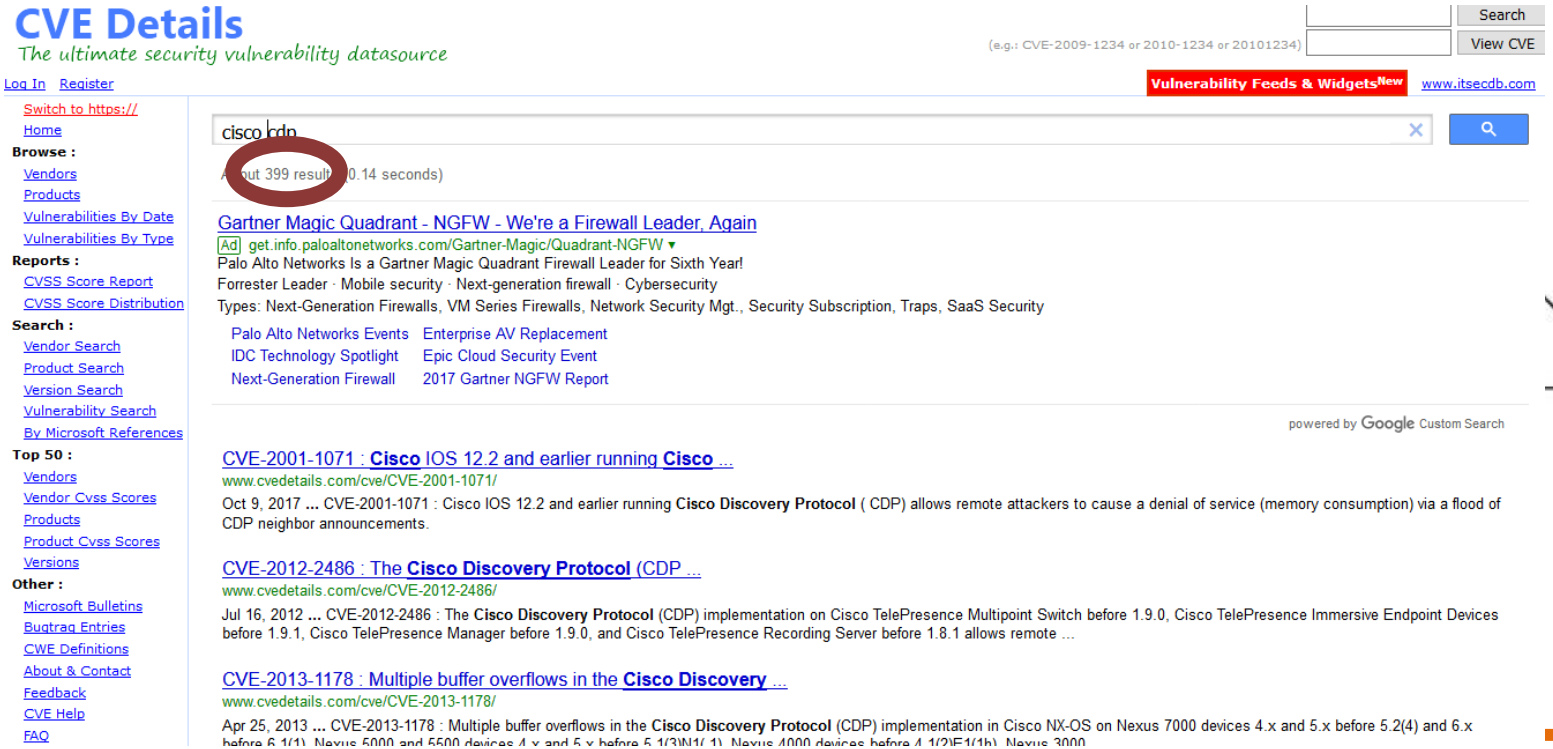
CDP

- CDP (Cisco Discovery Protocol)
  - Share information about neighbors
  - Collect sensitive information (IP, version, firmware etc.)
  - Mitigation:
    - » Disable CDP (but in some cases, it is used, e.g VoIP Phones)



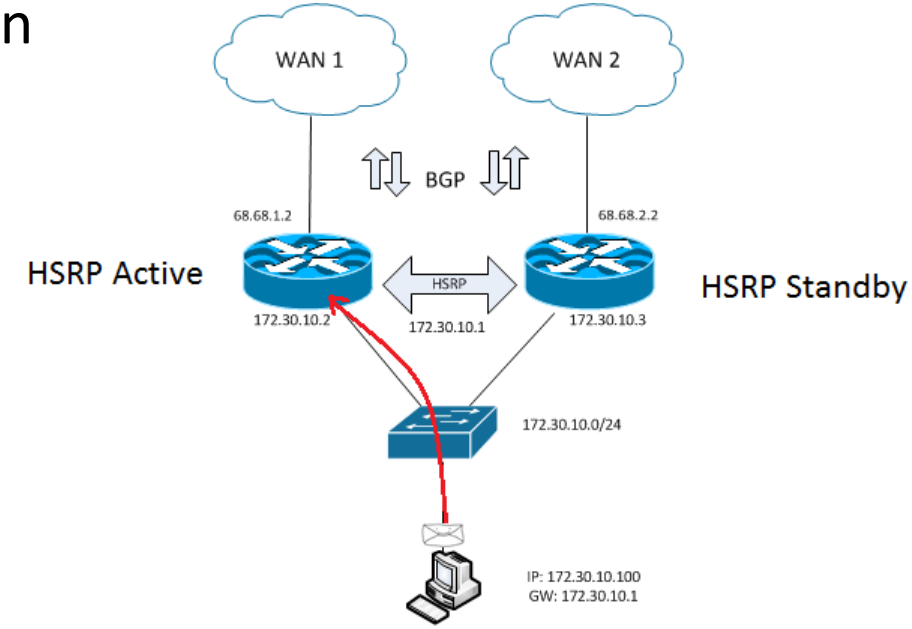
CDP

- CDP (Cisco Discovery Protocol)
  - Share information about neighbors
  - Collect sensitive information (IP, version, firmware etc.)
  - Mitigation:
    - » Disable CDP (but in some cases, it is used, e.g VoIP Phones)



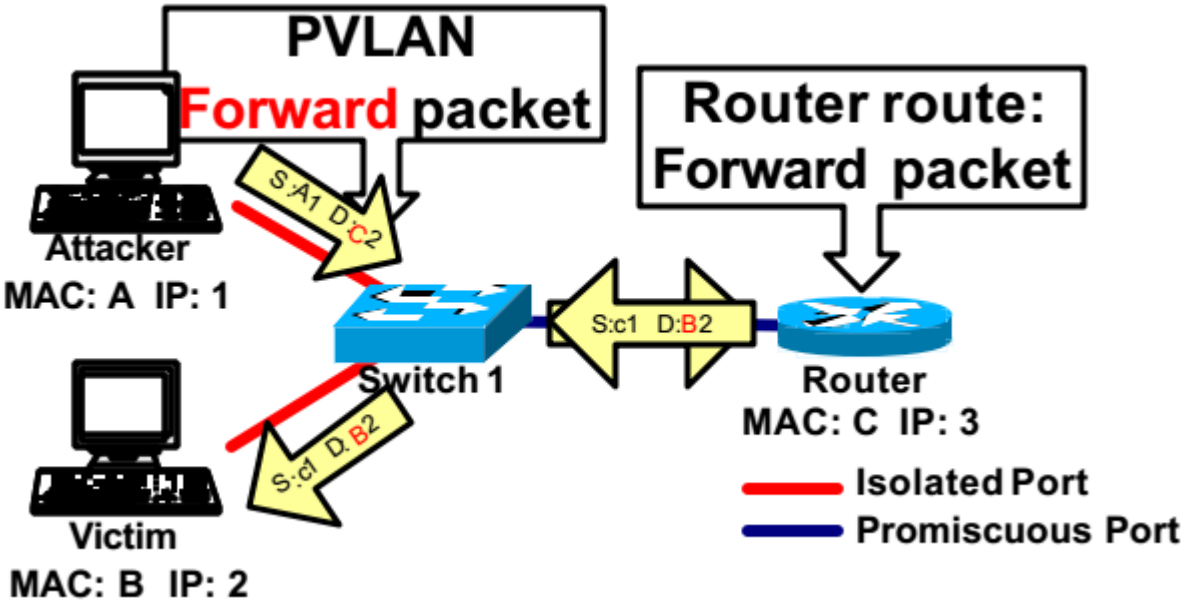
HSRP

- Hot Standby Router Protocol
- HA between devices (virtual IP, router/WAN problems)
- Password in plain (beacon)
- Attack: send raw HSRP packet and become Active
- Mitigation: MD5 authentication



PVLAN attacks

- No traffic between ports in same VLAN is allowed (e.g.: hotel, no traffic between rooms)
- Traffic possible using a L3 router
- Attack: send traffic through the router
- Mitigation: (V)ACL on Router



IEEE 802.1AE

- Layer 2 encryption
- Provides confidentality and integrity between Layer 2 Ethernet ports at wire speed (1-100 Gb)
- Galois/Counter Mode, symmetric key algorithm (GCM-AES-128)
- Standard since 2006
- Key management: 802.1X-2010
- Similar frame format as Ethernet, extra:
  - Message authentication code
  - Packet number
  - Association number

- You can buy compatible switch or NIC

Control Questions

- What is VLAN hopping?
- How to avoid CAM table flooding?
- Describe attacks against STP!
- Describe attacks against DHCP!
- How to mitigate ARP attacks?
- What is IEEE 802.1AE for?

Further Reading, Sources

- Steve A. Rouiller: Virtual LAN Security: weaknesses and countermeasures, SANS
- Yusuf Bhaiji: Understanding, Preventing, and Defending Against Layer 2 Attacks, Cisco 2009
- http://www.ciscopress.com/articles/article.asp?p=1181682
- https://www.juniper.net/documentation/en_US/junos/topics/concept/ex-series-security-overview.html
-