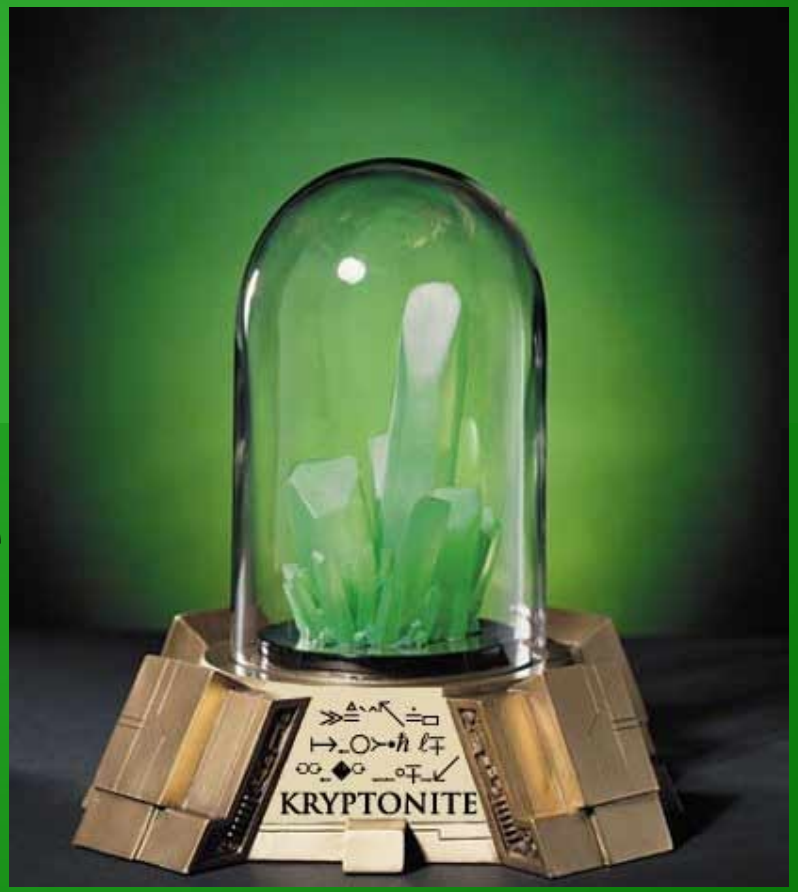
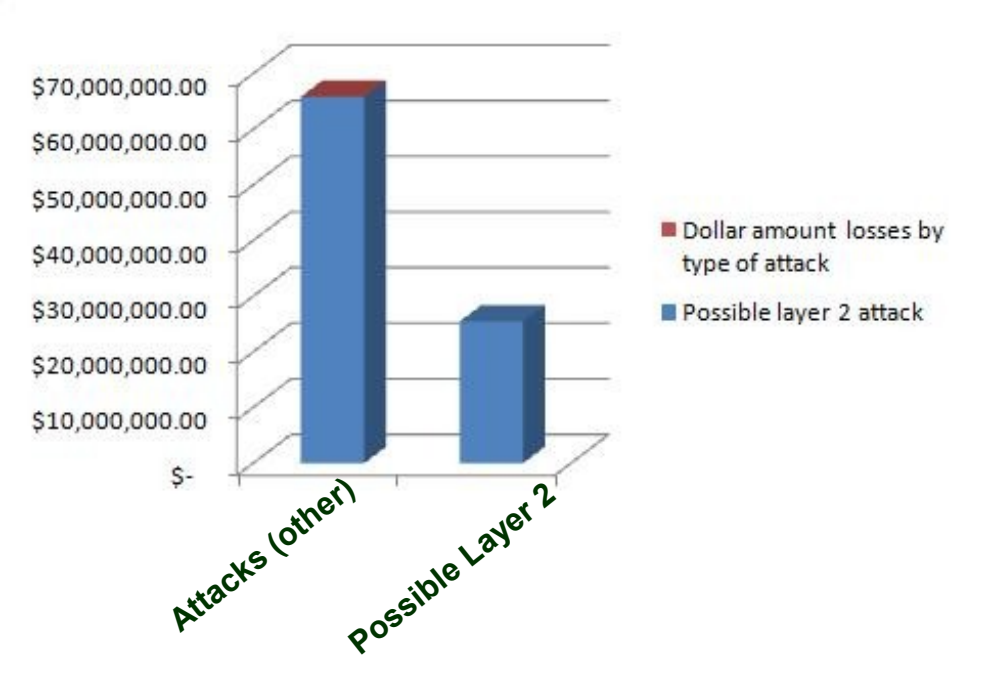
VLANs Layer 2 Attacks:

Their Relevance and Their Kryptonite



Justification for this Research

- Security is only as strong as the weakest link
- Layer 2 attacks are timeworn but still relevant in today's networking environment
- Crime and security survey show different types of attacks for the year of 2007. CSI / FBI surveys also show that 9 of 19 types of attacks could target routers and switches



Equipment, Attacks and Tools Used

Equipment

- Cisco 3600, 2600 routers
- Cisco 2900, 3500, 4006 switches
- Wifi Netgear & Cisco-Linksys

Attacks

- ARP Attacks
- MAC Flooding Attack/ CAM Table Overflow Attacks
- DHCP Starvation Attack
- CDP Attack
- Spanning-Tree Attack
- Multicast Brute Force
- VLAN Trunking Protocol Attack
- Private VLAN Attack
- VLAN Hopping Attack
- Double-Encapsulated 802.1Q/Nested VLAN Attack
- VLAN Management Policy server VMPS/ VLAN Query Protocol VQP Attack

Tools

- Scapy
- Yersinia
- Macof
- TCPDump
- Cain & Abel
- EtterCap
- Ethereal

Cisco Lab Setup

How to get a lab for testing purposes



Is Layer 2 out of date?

- Just ask HD Moore's ISP
- Someone was ARP poisoning the IP address

Example: Metasploit.com ISP PIMPED!

13:04:39.768055 00:15:f2:4b:cd:3a > 00:15:f2:4b:d0:c9, ethertype ARP (0x0806), length 60: arp reply 216.75.15.1 is-at 00:15:f2:4b:cd:3a
13:04:40.397616 00:15:f2:4b:cd:3a > 00:15:f2:4b:d0:c9, ethertype ARP (0x0806), length 60: arp reply 216.75.15.1 is-at 00:05:dc:0c:84:00
13:04:40.397686 00:15:f2:4b:cd:3a > 00:15:f2:4b:d0:c9, ethertype ARP (0x0806), length 60: arp reply 216.75.15.1 is-at 00:15:f2:4b:cd:3a

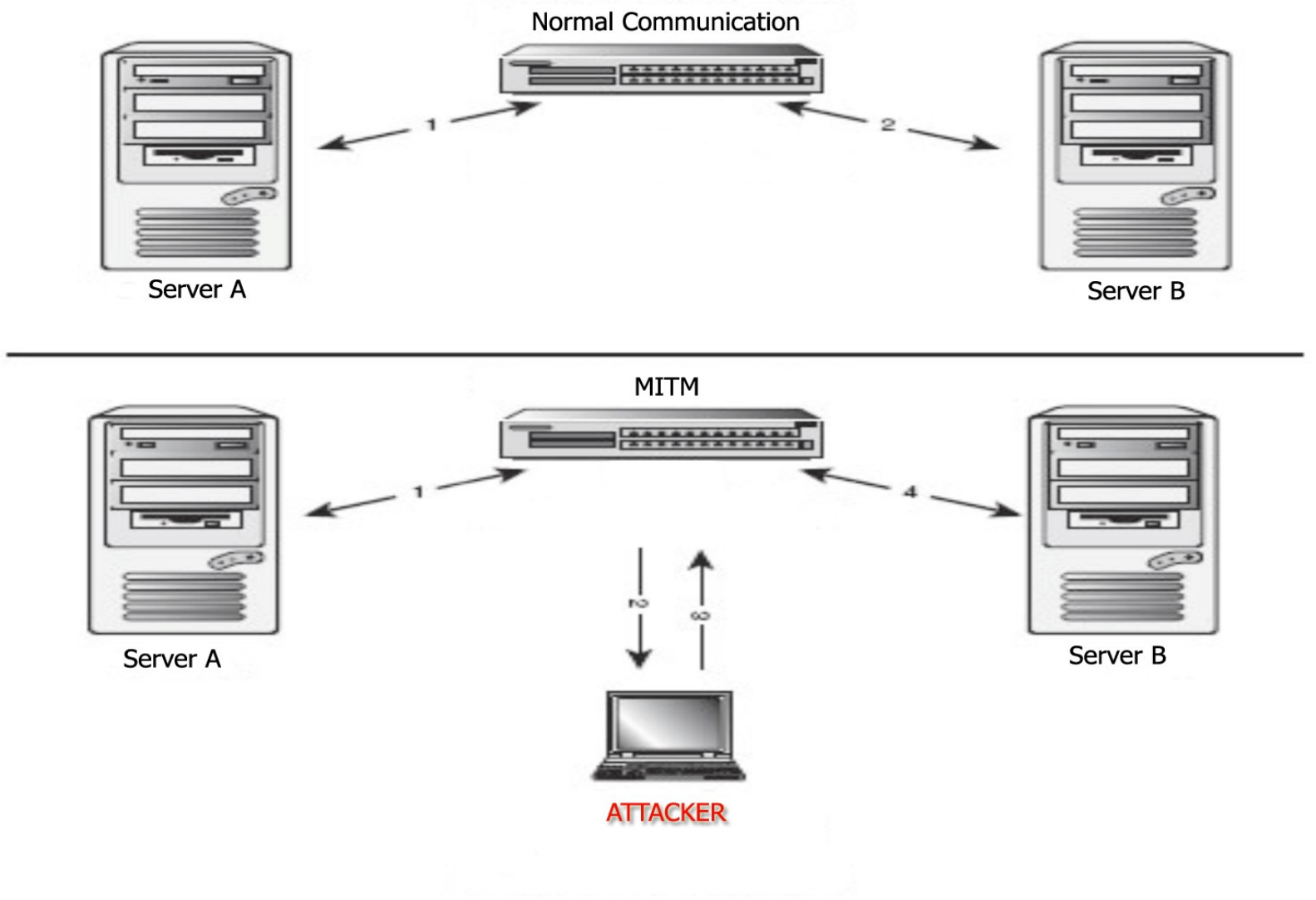




Back to the Basics - ARP Attacks

- ARP Poisoning: Simple and effective
- ARP may be used most but least respected
- 250 other servers are hosted on the same local network at the same service provider metasploit.com that were still vulnerable a month ago
- No authentication built into protocol
- Information leakage

ARP Attacks


Normal Communication
1
2
Server A
Server B
MITM
1
4
2
3
Server A
Server B
ATTACKER

ARP Attacks

- ARP attack demo

Example:

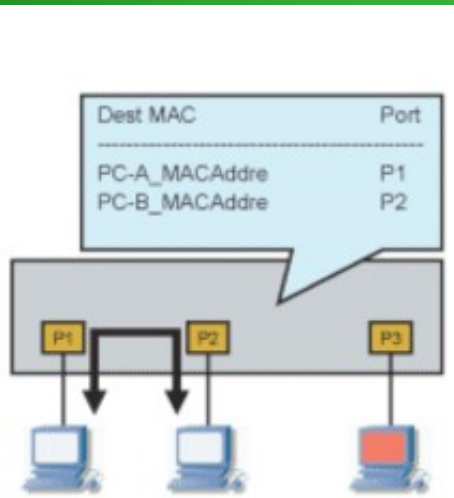
1st of its kind. Human ARP attack

ARP Attack Mitigation

- **Port Security**
  - **Non changing ARP entries (don't waste your time)**
  - **DHCP Snooping (the network device maintains a record of the MAC address that are connected to ARP port)**
  - **Arpwatch (listens to arp replies)**
  - **ArpON**

MAC Flooding/CAM Table Overflow Attack

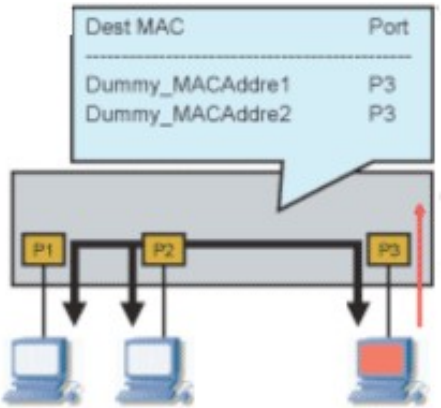
- MAC flooding attacks are often ignored in the corporate environment.
- MAC flooding – switch ports act like a hub when overloaded
- CAM table - table fills and the switch begins to echo any received frame to all port (traffic bleeds out).
- Tools to perform this attack:
  - Dsniff
  - Macof
  - Cain & Able
  - Ettercap



CAM TABLE

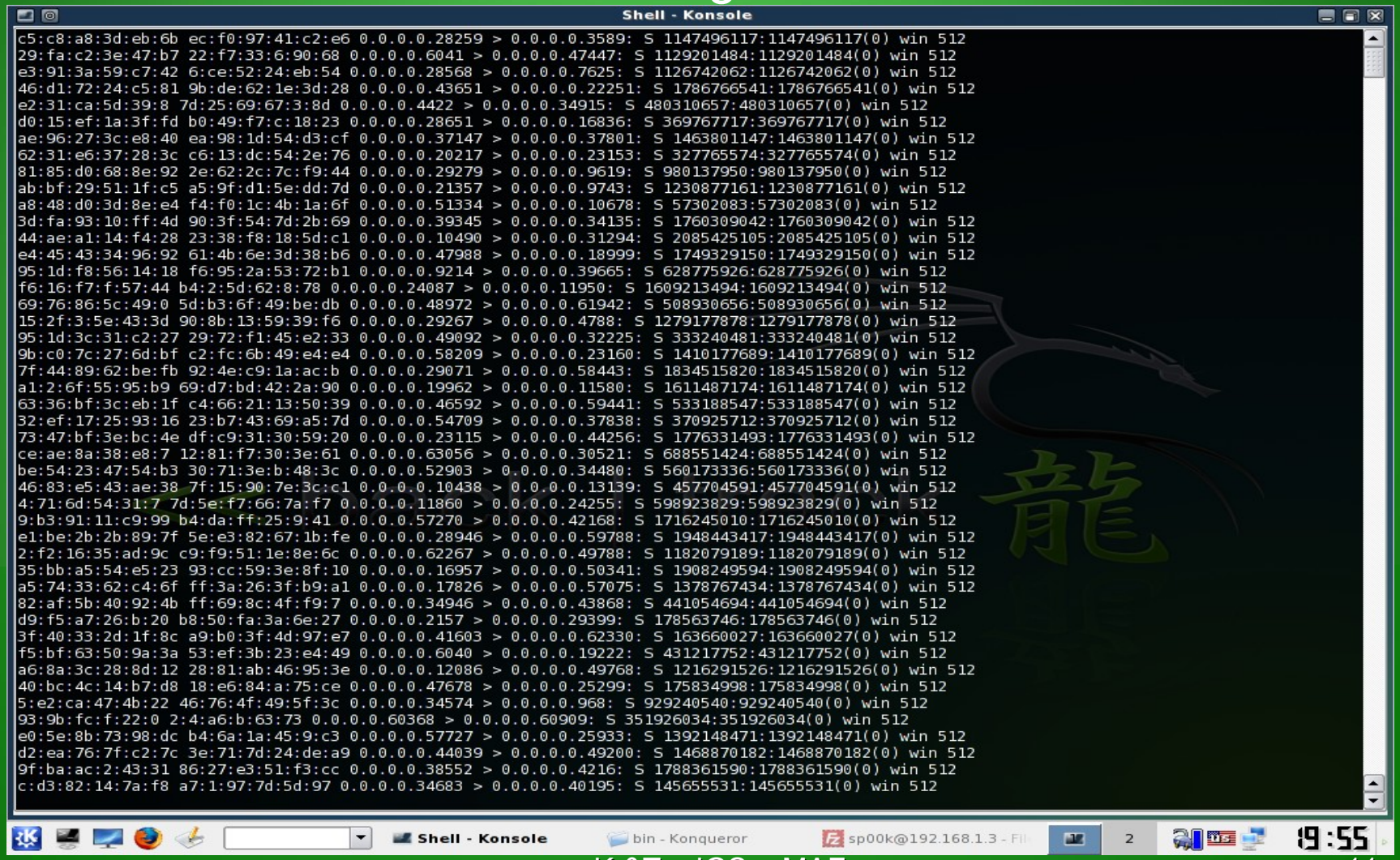
Vlan	Mac Address	Type	Ports
All	0014.1c40.b080	STATIC	CPU
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0100.0cdd.dddd	STATIC	CPU
1	0000.aa70.d9b9	DYNAMIC	Fa0/1
1	0004.00d5.285d	DYNAMIC	Fa0/9
1	0009.0f0a.6974	DYNAMIC	Fa0/1
1	000b.db12.a3f9	DYNAMIC	Fa0/1
1	000b.db2c.a66a	DYNAMIC	Fa0/1
1	000d.5652.c0d4	DYNAMIC	Fa0/1
1	000d.5652.e2d7	DYNAMIC	Fa0/1
1	000f.1fdd.bb2a	DYNAMIC	Fa0/1
1	000f.1fe6.c8d2	DYNAMIC	Fa0/1
1	000f.1fe6.cb0a	DYNAMIC	Fa0/1
1	000f.3daa.7fb1	DYNAMIC	Fa0/1
1	0011.1114.6ded	DYNAMIC	Fa0/1
1	0011.85fb.b0f1	DYNAMIC	Fa0/10
1	0012.3f85.ced1	DYNAMIC	Fa0/1
1	0012.3fed.417a	DYNAMIC	Fa0/24
1	0013.72ba.1b72	DYNAMIC	Fa0/1
1	0013.72ba.1c9b	DYNAMIC	Fa0/1
1	0014.1c53.39c1	DYNAMIC	Fa0/1
1	0030.055d.b106	DYNAMIC	Fa0/1
1	0030.803d.0ba0	DYNAMIC	Fa0/13
1	00c0.9f41.907d	DYNAMIC	Fa0/1
1	00c0.b768.5409	DYNAMIC	Fa0/14

Total Mac_Addresses for this criterion: 26



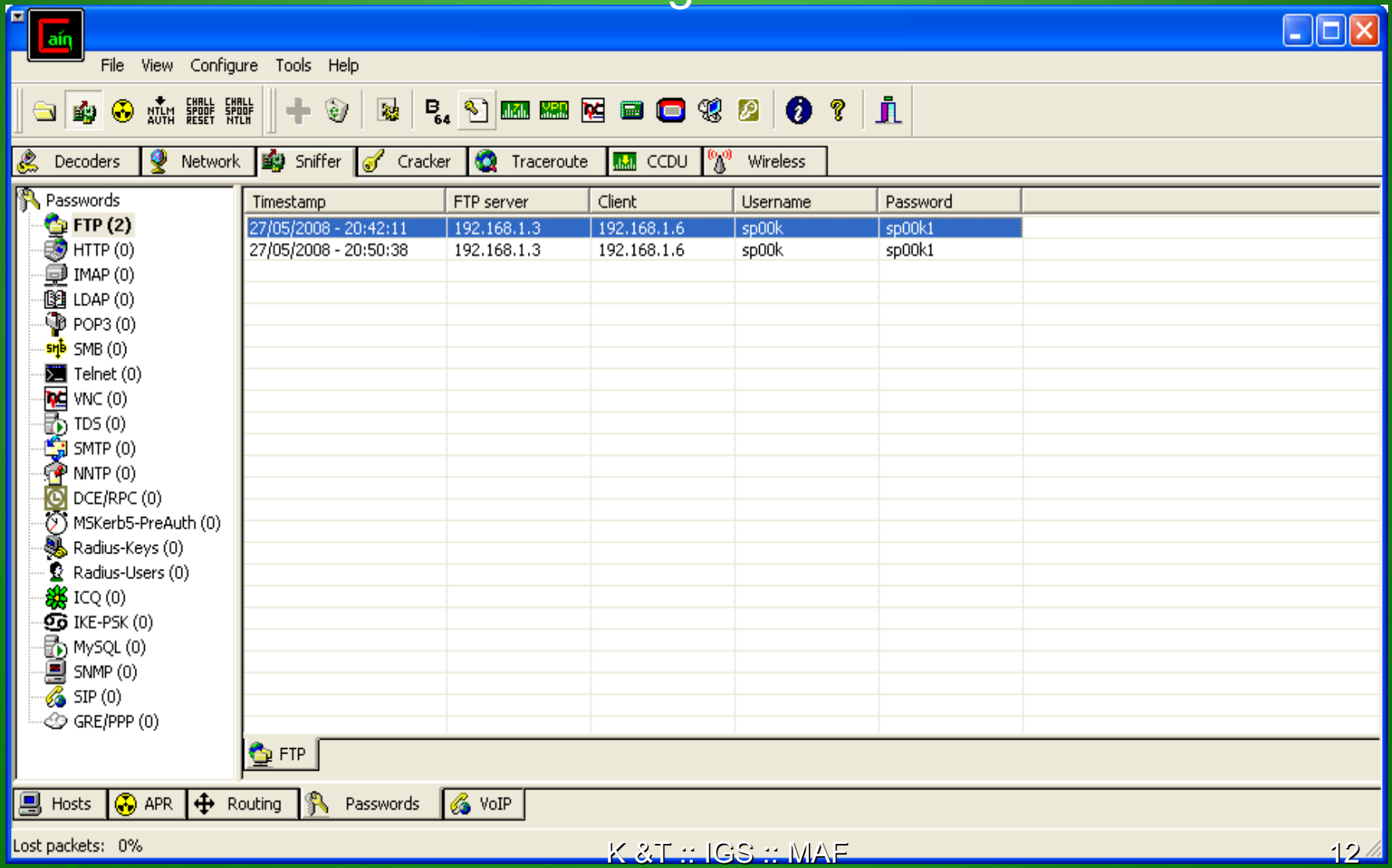
MAC Flooding/CAM Table Overflow Attack

Macof at work flooding the Cisco switch



Sniffing for the good stuff

Switch is bleeding out the traffic



MAC Flooding/CAM Table Overflow Attack Mitigation

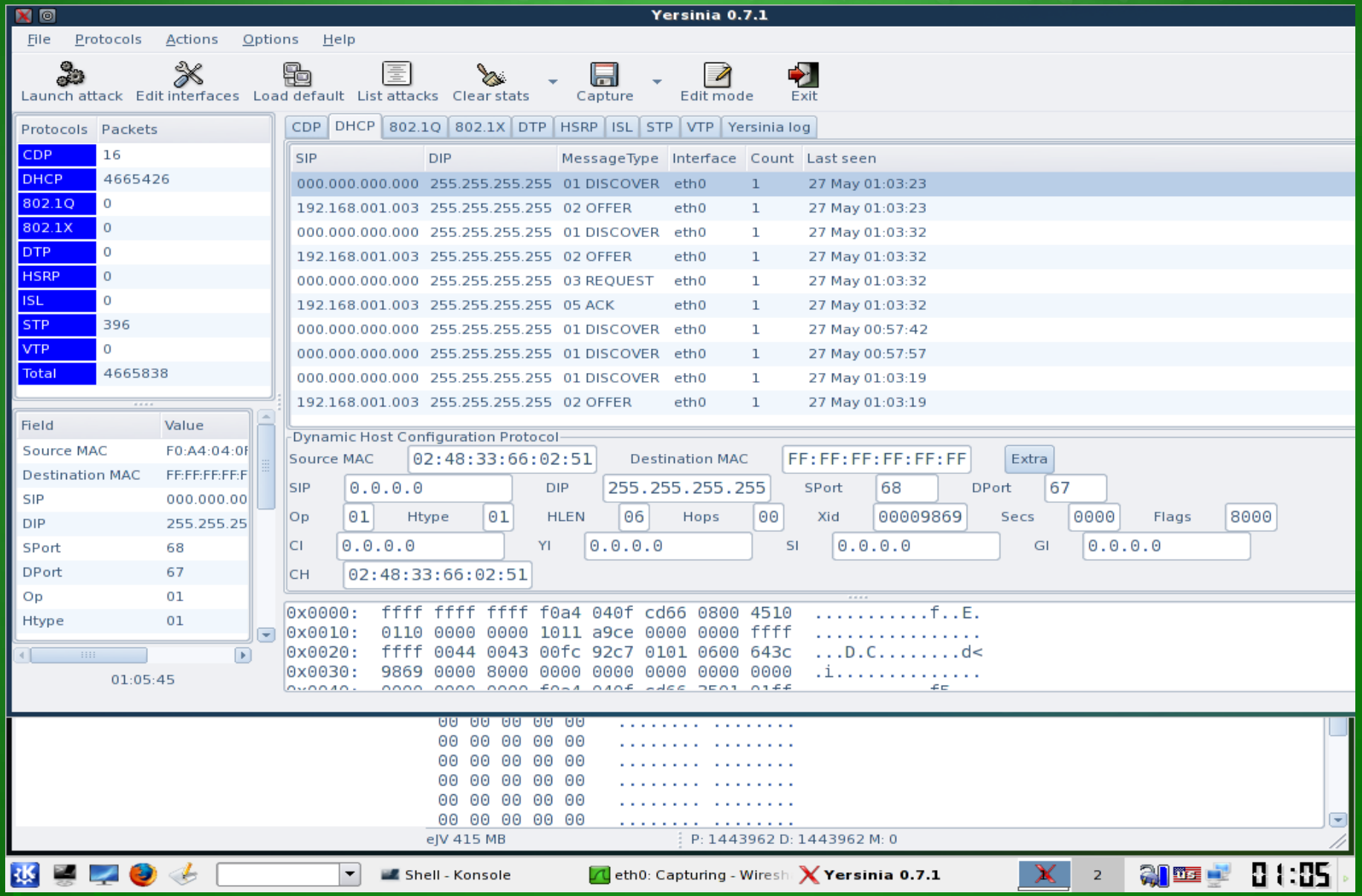
- Same as the ARP attack mitigation
- Limit amount of MAC addresses to be learned / port.
- Static MAC addresses configuration (not scalable but most secure).

DHCP Starvation Attacks

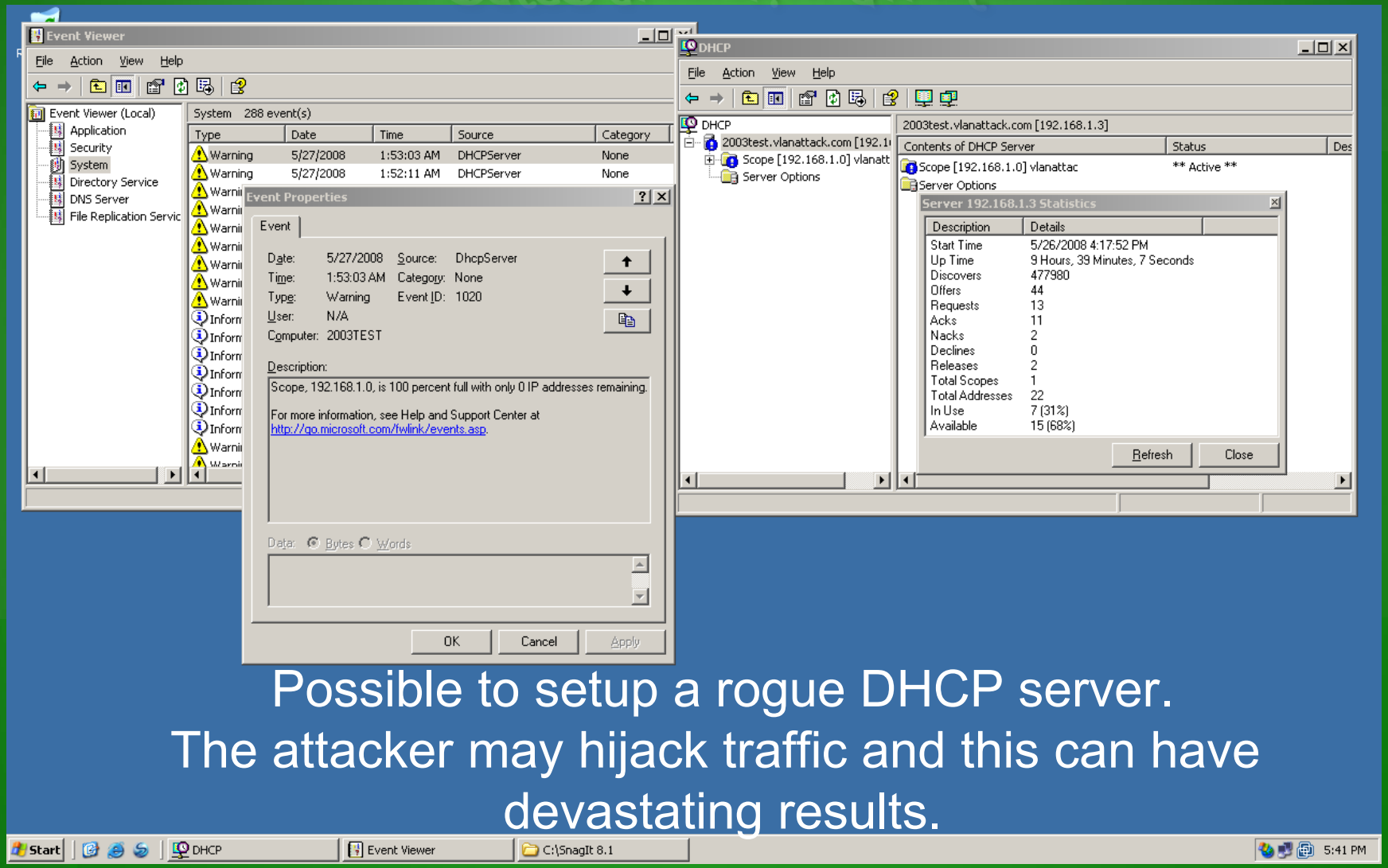
- A DHCP Scope exhaustion (client spoofs other clients)
- Installation of a rogue DHCP server
- Tools
  - Yersinia
  - Gobbler

VLAN Layer 2 Attacks

DHCP Starvation Attacks with Yersinia



DHCP Starvation Attacks



Possible to setup a rogue DHCP server.
The attacker may hijack traffic and this can have devastating results.

DHCP Starvation Attacks

- Demo Time
  - DHCP Starvation Demo

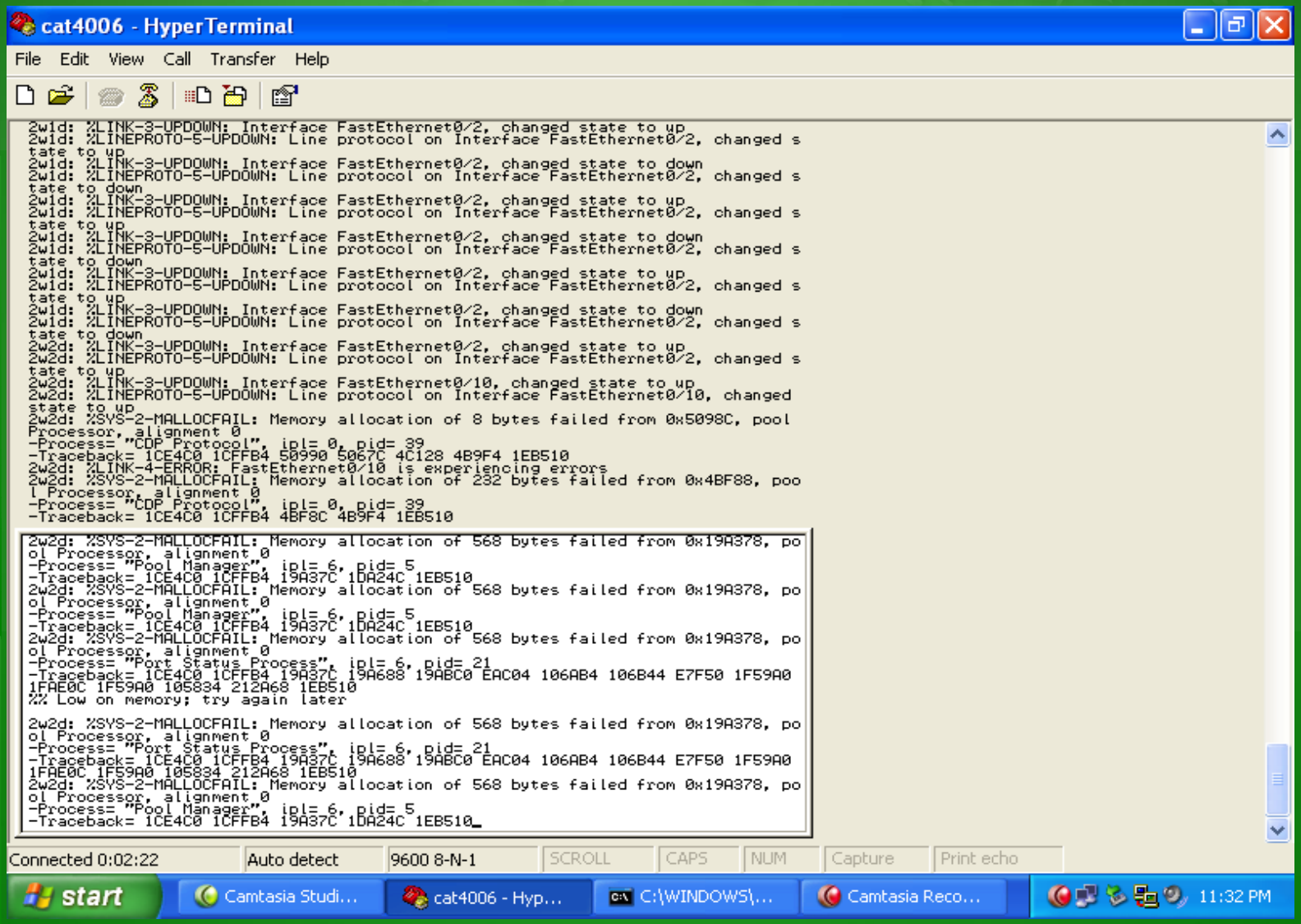
DHCP Starvation Attacks Mitigation

- By limiting the number of MAC addresses on a switch port will reduce the risk of DHCP starvation attacks.
- DHCP Snooping – monitors and restricts DHCP

Cisco Discovery Protocol (CDP) Attack

- Cisco Discovery Protocol allows Cisco devices to communicate amongst one another (IP address, software version, router model, etc) CDP is clear text and unauthenticated.
- CDP Denial Of Service (Many companies do not upgrade their IOS often enough to 12.2.x and current versions of CatOS)
- CDP cache overflow – a software bug can reset the switch
- Power exhaustion – claiming to be a VoIP phone an attacker can reserve electrical power
- CDP cache pollution – CDP table becomes unusable because it contains a lot of false information

Cisco Discovery Protocol (CDP) Attack



CDP Attack Mitigation

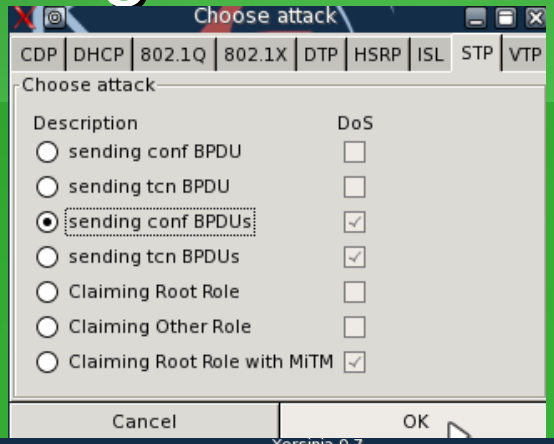
- Turn the sh*t off
- Router # no cdp enable
- Switch (enable) set cdp disable 1/23
- The question is why is CDP enabled on a network? IP phones are popular, CDP is used in order to determine the actual power requirement for the phone.

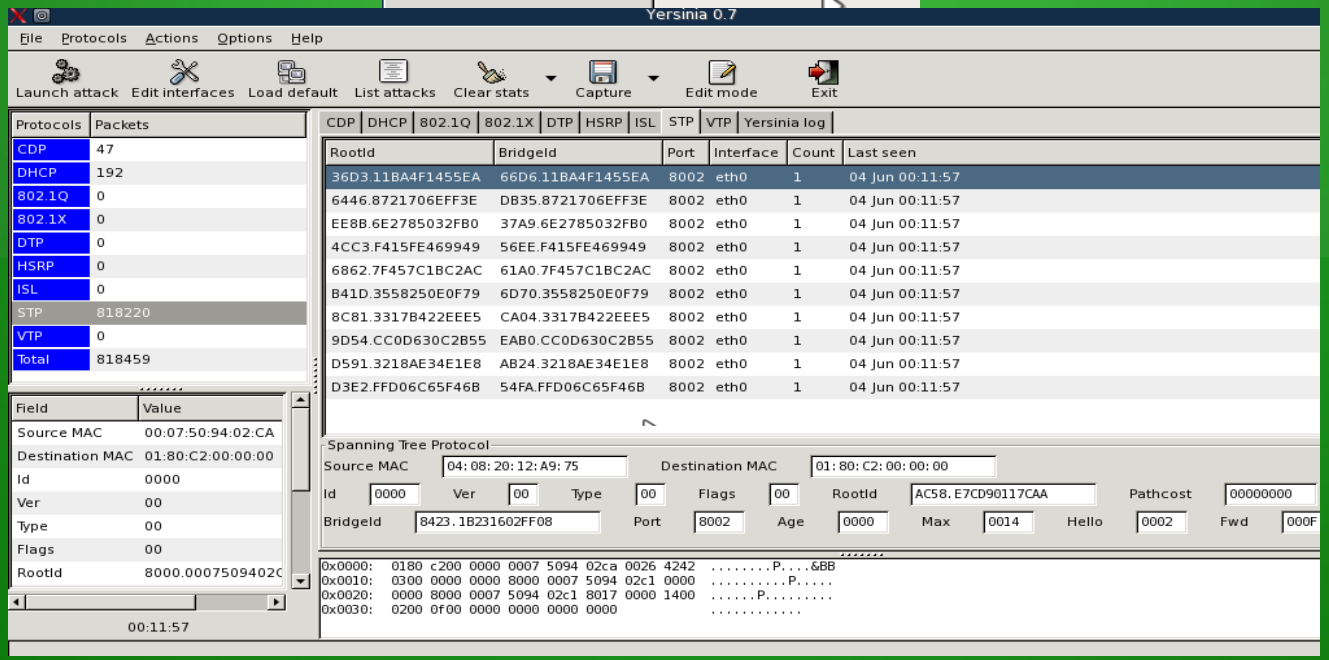
Spanning-Tree Protocol(STP) Attack

- STP Attack – involves an attacker spoofing the root bridge in the topology
- Attacks
  - Sending RAW Configuration BPDU
  - Sending RAW TCN BPDU
  - DoS sending RAW Configuration BPDU
  - DoS Sending RAW TCN BPDU
  - Claiming Root Role
  - Claiming Other Role
  - Claiming Root Role Dual-Home (MITM)

Spanning-Tree Protocol(STP) Attack

- STP sending conf BPDUs DoS





Spanning-Tree Protocol(STP) Attack

- Spanning tree functions must be disabled on all user interfaces but maintained for Network to Network Interfaces to avoid a network loop.
- Enable **root guard** on Cisco equipment, or BPDU guard on users ports to disable the thus of priority zero and hence becoming a root bridge.

Example:

```
#spanning-tree portfast dbduguard
#interface fa0/10
#spanning-tree guard root
```

Multicast Brute Force Attack

- This involves spoofing, in rapid succession, a series of multicast frames
- Frames leak into other VLANs if the routing mechanism in place between the VLANS
- Injecting packets into multicast also can cause a DoS scenario

Multicast Brute Force Attack Mitigation

- Buy more capable switches!
- The Layer 2 multicast packets should be constrained within the ingress VLAN. No packets should be 'leaked' to other VLANs.

VLAN Trunking Protocol (VTP) Attack

- VTP has the ability to add and remove VLAN from the network. (Someone will get fired if this happens!)
- VTP involves a station sending VTP messages through the network, advertising that there are no VLANs.
- All client VTP switches erase their VLANs once receiving the message
- Attacks:
  - Sending VTP Packet
  - Deleting all VTP VLANs
  - Deleting one VLAN
  - Adding one VLAN

(VTP) Attack Mitigation

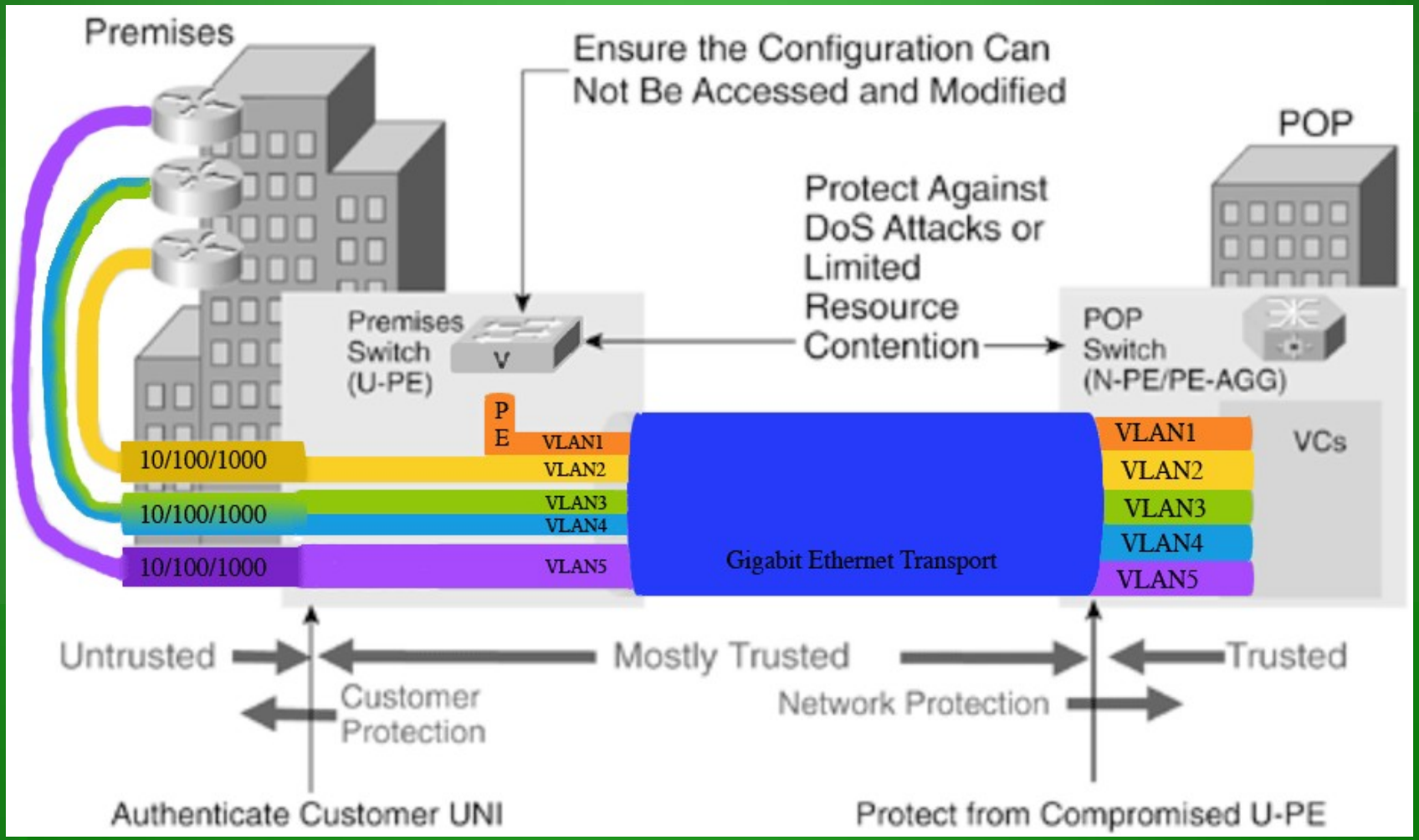
- If you like your job don't use VTP!



Private VLAN Attack

- Private VLANs only isolate traffic at Layer 2
- Forward all traffic via Layer 3 to get to the private VLAN
- Scapy is your best friend!

Private VLAN Attack



Private VLAN Attack Mitigation

- Configure VLAN access lists on the router interface

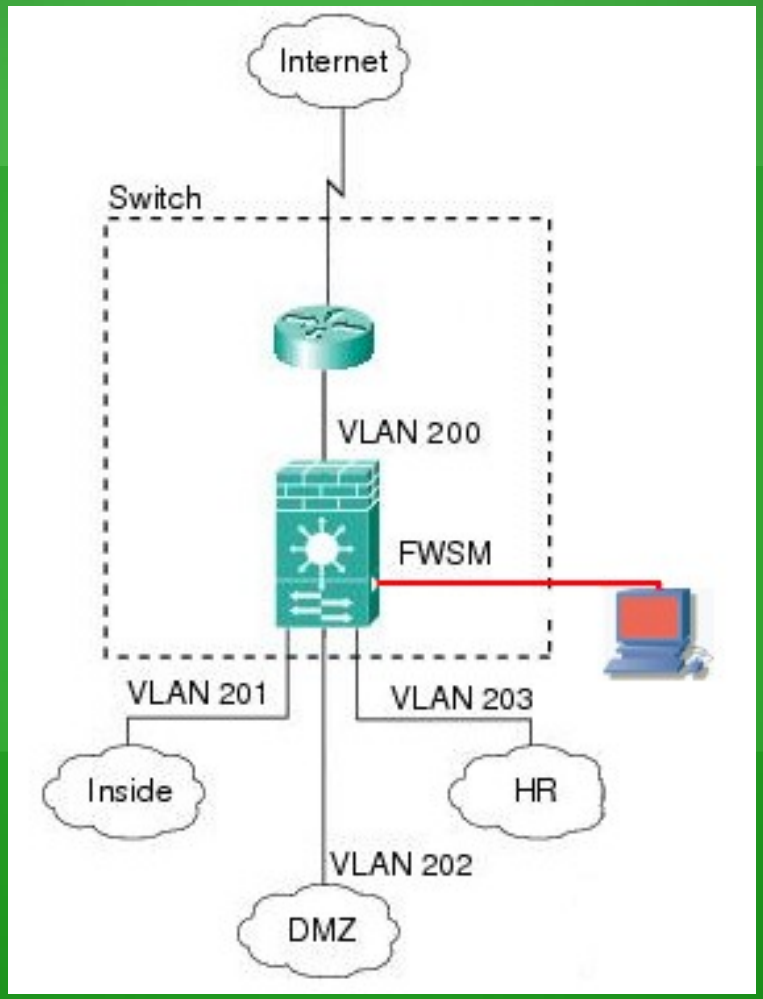
Example:

vlan access-map map_name (0-65535)

VLAN Hopping Attack

- Attacker configures a system to spoof itself as a switch by emulating either 802.1q or ISL
- Another variation involves tagging transmitted frames with two 802.1q headers.

VLAN Hopping Attack



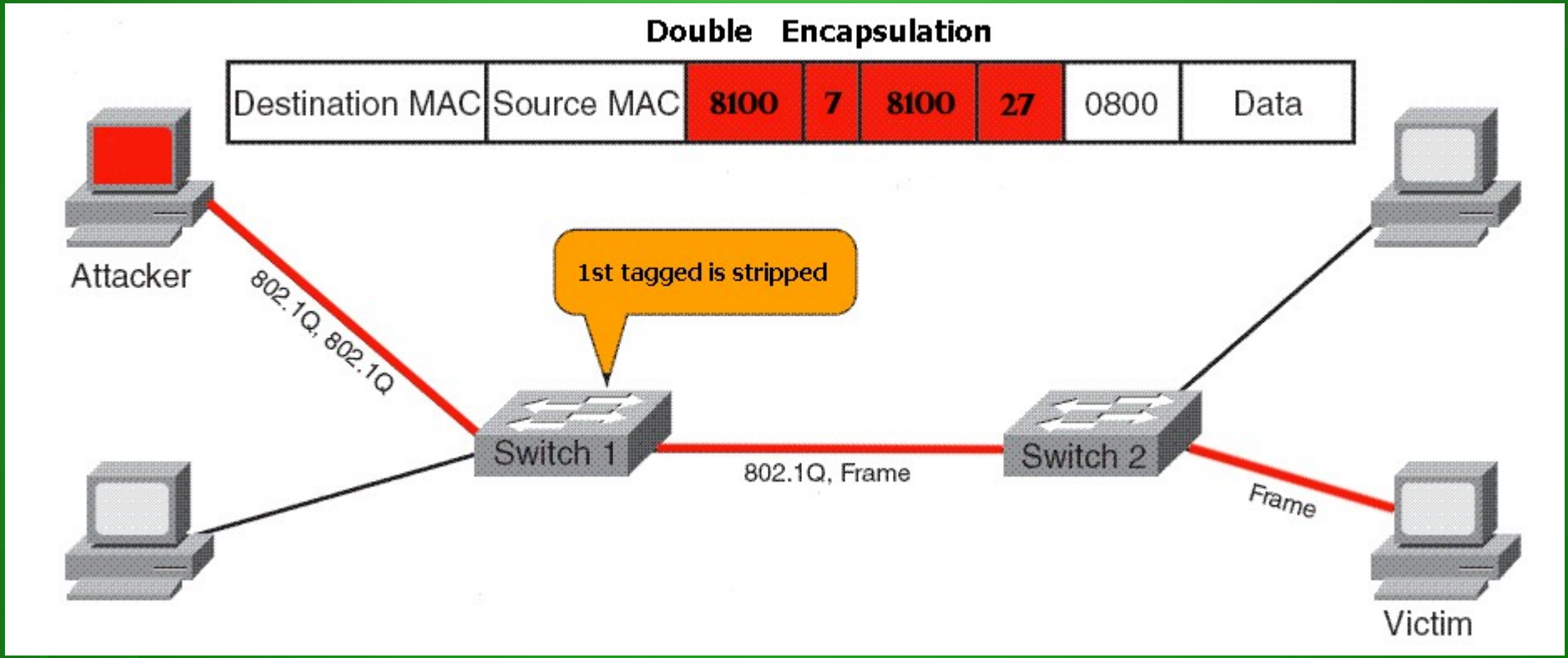
VLAN Hopping Attack Mitigatione

- Disable auto-trunking
- Unused ports, other than trunk port should be removed.
- For backbone switch to switch connections, explicitly configure trunking
- Do not use the user native VLAN as the trunk port native VLAN
- Do not use VLAN 1 as the switch management VLAN

Double Encapsulation 802.1q and ISL Tagging Attack

- VLAN numbers and identification are carried in a special extended format.
- Instead, outside of a switch, the tagging rules are dictated by standards such as ISL or 802.1Q.
- This allows the forwarding path to maintain VLAN isolation from end to end without loss of information.

Double Encapsulation 802.1q and ISL Tagging Attack



Double Encapsulation 802.1q and ISL Tagging Attack Mitigation

- Ensure that the native VLAN is not assigned to any port
- Force all traffic on the trunk to always carry a tag

VLAN Management Policy Server (VMPS) / VLAN Query Protocol (VQP) Attack

- The VLAN Management Policy Server is for assigning dynamically created VLANs based on MAC/IP address or HTTP authentication (URT). VMPS is a centralized host information database which is can be downloaded to servers via TFTP.
- All VMPS traffic is in clear text, unauthenticated and over UDP, and may be misused for hijacking purposes

VMPS / VQP Attack Mitigation

- VMPS traffic shall be transmitted on a Out Of Band basis (user traffic separate network) or not used.

Conclusion

- Manage switches in as secure a manner as possible (SSH, OOB, permit lists, etc.)
- Always use a dedicated VLAN ID for all trunk ports. Be paranoid: do not use VLAN 1 for anything.
- Deploy port security.
- Set users ports to a non trunking state.
- Deploy port-security whenever possible for user ports.
- Selectively use SNMP and treat community strings like root passwords.
- Have a plan for the ARP security issues in your network.
- Use private VLANS where appropriate to further divide L2 networks. Disable all unused ports and put them in an unused VLAN.
- Consider 802.1X for the future and ARP inspection
- Use BPDU guard, Root guard
- Disable CDP whenever possible
- Ensure DHCP attack prevention