

# Network Security on OSI Layer 2 and 3

Enno Rey, [erey@ernw.de](mailto:erey@ernw.de)  
BS 7799 LA, CISSP/ISSAP, CISA



# Who I am

---

- “Old-school networker“
- Started working on Layer 2–4 in the early 90s
- With special focus on security since 1997
- (Co-) Author of several books, articles and whitepapers and regular speaker on international conferences (incl. Black Hat, Hack In The Box, FutureNet)
- Founder (2001) and CTO of a highly specialized IT security consultancy [[www.ernw.de](http://www.ernw.de)] with 12 employees, based in Heidelberg/Germany and Lisbon/PT



# Agenda

- **The Architect's View: The Building Blocks of Network Sec**
- **The Security Officer's (or Hacker's) View: Attacks, Tools, Mitigating Controls on Layer 2**
- **The Security Officer's (or Hacker's) View: Attacks, Tools, Mitigating Controls on Layer 3**
- **The Auditor's View: How to Evaluate the Whole Stuff**
- **The Speaker's View: Some Notes on the Future**

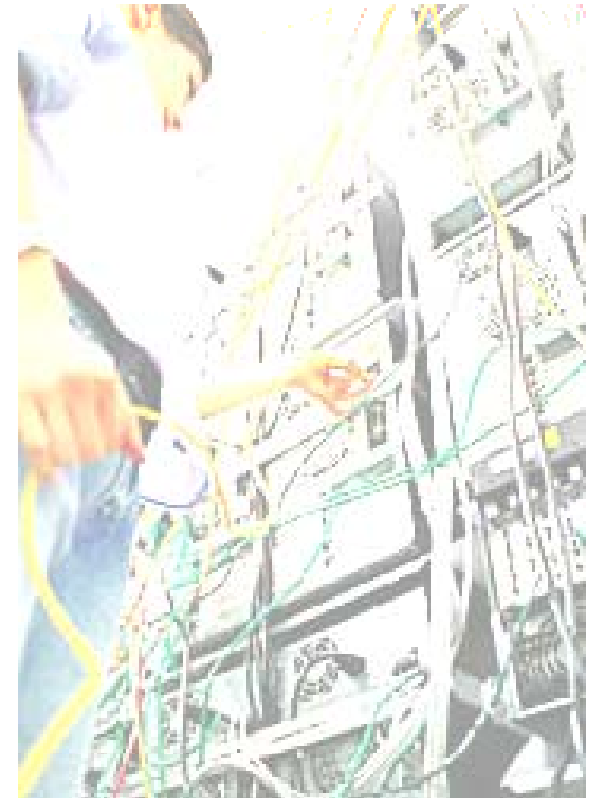


# Some Notes on the Motivation of my Talk

- Depending on the customer I work as a network planner, engineer, operator or auditor/evaluator  
=> I sit on “both sides of the table“.
- This can be pretty frustrating...
- Listening to auditors telling us (operators) things like “You should use SNMPv3 on all devices“.
- Telling (as an auditor) the network guys things like “You shouldn’t use SNMP *private* as a RW community“  
... just to hear “We can’t change that, for operational reasons“
- This talk aims to give an overview of threats and techniques, to “bridge the gap“ mentioned above in a realistic way.



## The Building Blocks of Network Security



# Definition

- **RFC 3871, sect. 1.4:**

**A secure network is one in which:**

- o **The network keeps passing legitimate customer traffic (availability).**
- o **Traffic goes where it is supposed to go, and only where it is supposed to go (availability, confidentiality).**
- o **The network elements remain manageable (availability).**
- o **Only authorized users can manage network elements (authorization).**
- o **There is a record of all security related events (accountability).**
- o **The network operator has the necessary tools to detect and respond to illegitimate traffic.**



# The Building Blocks

---

- **Isolation / Segmentation**
- **Restriction / Filtering**
- **Access Control / Authentication**
- **Encryption**
- **Hardening of Infrastructure Services**
- **Secure Management**
- **Logging / Monitoring**
  
- **Policy**



## Why don't you mention “Design“ here?

- **Not a technique in itself, but – in some sense – based on the building blocks.**
- **Must follow risk analysis. However in most cases doesn't...**
- **Unfortunately design is not easy to change once implemented.**
- **And not easy to audit either... how do you measure “good design“??**



# Isolation / Segmentation

---

- **If some traffic (based on network design, routing config and/or traffic's properties) can't reach a destination... you won't have a problem there...**
- **Isolation / Segmentation should be based on**
  - Different protection needs
  - Different threat potential [that's why one uses "DMZs"]
- **Overall most important network security mechanism.**
- **Often combined with filtering.**



# Restriction / Filtering

- If you don't want that some traffic reaches some destination... filter it!
- Preferably implemented on existing hardware than on dedicated one (which would add complexity).
- If conflict *manageability* vs. 'security' arises, opt for manageability (fewer + coarse rules better than more + accurate rules).
- Think about *Infrastructure ACLs*.



# Access Control / Authentication

- **Control who is able to access / take part in the network.**
- **Preventative mechanism  
=> as such a good thing**
- **But might be administrative nightmare**
  
- **MAC address based (*Port Security*)**
- **Certificate based**
- **802.1x**
- **NAC/NAP (?)**



# Some Remarks on NAC/NAP here

- **NAC/NAP solutions address mainly two problems:**
  - Missing patches
  - Outdated AV signatures
- **In a perfect world both problems would not exist due to**
  - Good patch management
  - Good signature distribution
- **In an even better world both processes would not be necessary as a result of**
  - Software that doesn't need to be patched every some days
  - Users behaving sensibly



# Some Remarks on NAC/NAP here

So...

- **NAC/NAP address deficiencies in processes ... which address deficiencies in some “info processing entities“.**
- **Kind of *the medicine for the symptom of the medicine for the symptom.***
- **Think about that when thinking about spending money on this stuff...**
- **\$\$\$ spent for NAC/NAP might be spent much better elsewhere.**
- **See also: [http://www.ernw.de/content/e7/e181/e566/download569/bh07-europe\\_nacattack\\_03\\_ger.pdf](http://www.ernw.de/content/e7/e181/e566/download569/bh07-europe_nacattack_03_ger.pdf)**



# Encryption

- **Best (and mostly) only method if you don't trust the transport path.**
- **Again: manageability is key.**
- **Think about key mgmt processes *before* deploying.**
- **Performance might be a factor, too.**  
**=> Undertake risk analysis if highest key length needed.**



# Infrastructure Hardening [devices, protocols]

---

- **Unsecure devices (still) one of the weakest points in many environments.**
- **It's not rocket science to harden nw devices, basic rules apply...**
- **And don't forget all those protocols**
  - Routing protocols
  - Layer 2 (STP, VTP/DTP, LLDP etc.)
  - NTP, syslog
  - DNS, DHCP
  - LDAP / AD stuff



# Secure Management

---

- **Restriction of source addresses authorized for mgmt access.**
- **Choice of protocols (SSH vs. Telnet, HTTPS vs. HTTP, SNMPv3 vs. community-based SNMP).**
- **Use of good passwords and personalized accounts (for accountability)**

**Should SNMP community strings be subject to corporate pw policy? In most cases: no!**

**Corporate password change policy vs. operational impact.**

- **Logging of all successful/failed logins and – if possible – performed actions.**



# Controls as for SNMP

---

- **Check if SNMPv3 possible**

**If using community based SNMP:**

- **Restrict authorized managers, use mgmt segments**
- **Use good community strings (length!)**
- **Enable logging:**

```
hdz-core-002(config)#logging snmp-auth
Logging of %SNMP-3-AUTHFAIL is enabled
hdz-core-002(config)#exi
```

- **Think (at least) twice about RW access**
- **Restrict views**
- **See also:**

**[http://www.ernw.de/content/e7/e181/e671/download690/ERNW\\_026\\_SNMP\\_HitB\\_Dubai\\_2007\\_ger.pdf](http://www.ernw.de/content/e7/e181/e671/download690/ERNW_026_SNMP_HitB_Dubai_2007_ger.pdf)**



# Logging / Monitoring

- You do this extensively for *compliance reasons*, don't you? ;-)
- If you can't really prevent/control stuff you should at least be able to detect or track.



- Ask yourselves: would you notice if the configuration of a network device was modified?
- Lots of free and powerful tools available, usually no need to “buy another appliance“...



## General Use

---

- **The building blocks can be “applied“ to all components / technologies / protocols.**

**Just ask:**

- **What is the “scope“? Can it be limited?**
- **Can (the traffic) be filtered / restricted?**
- **Are there authentication mechanisms?**
- **How’s the stuff being managed?**
- **Any hardening (of a device or service) possible?**
- **What about logging / monitoring?**



# Policy

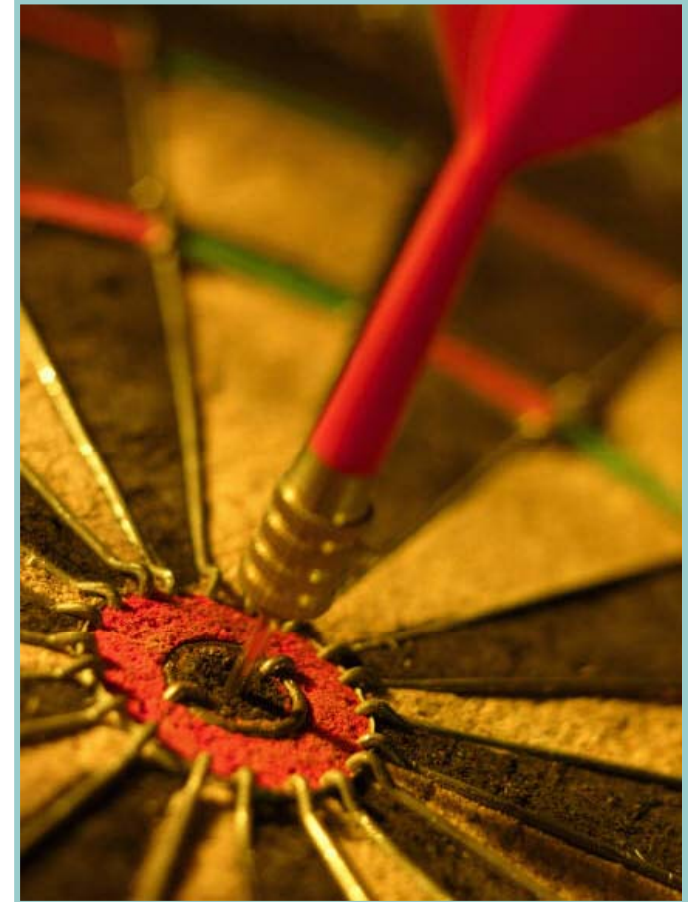
- Network security depends *highly* on operational processes & procedures.
- => Guidance necessary... and usually very efficient.
- Many nw people can still think only of technical controls. But lots of problems must (at least complementarily) be addressed by policy.

## Example

- Question: “What can I do to prevent sniffing in my network?”
- Answer: “First step: Forbid it by policy!”



## Network Security on Layer 2



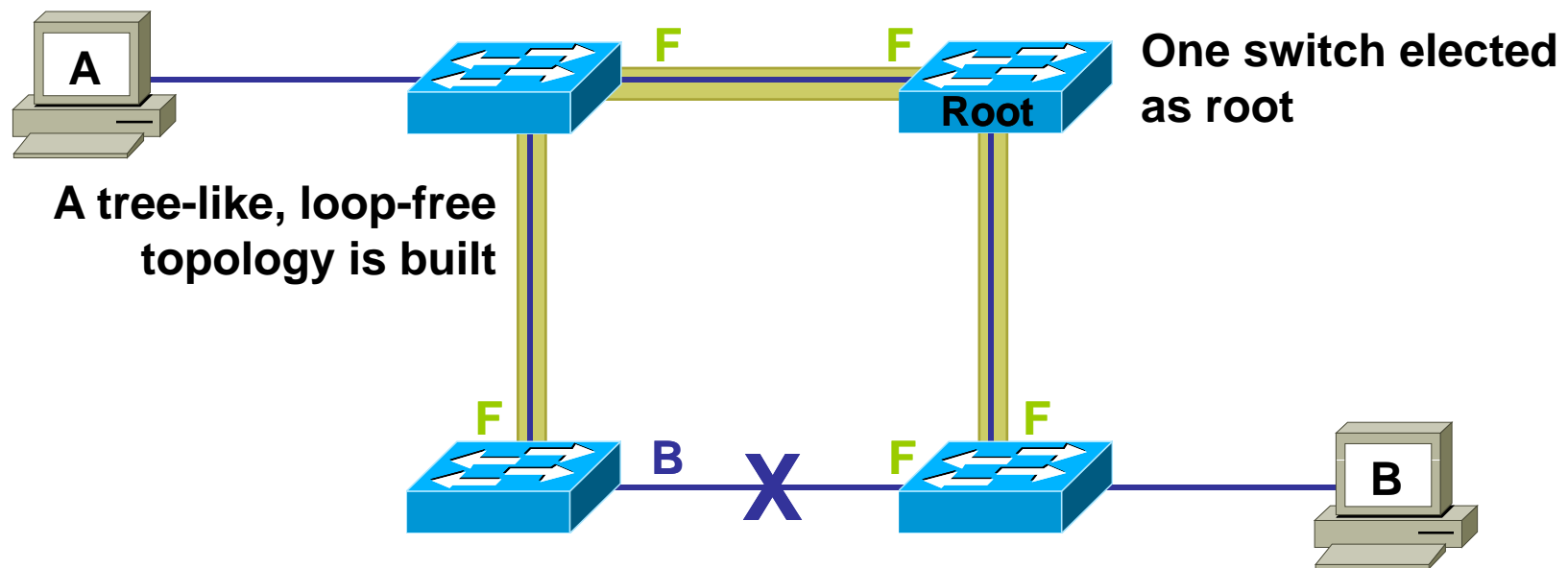
# Layer 2

## There are three main classes of attacks

- **Spanning Tree (STP)**
- **Cisco VLAN/Trunking Protocols (VTP/DTP)**
- **Other (CDP, 802.1x, potentially against new L2 protocols)**
  
- **Main impact (depending on type of attack):**
  - Denial of Service
  - Eavesdropping, potentially of multiple VLANs



# Spanning Tree



# Attacks against STP

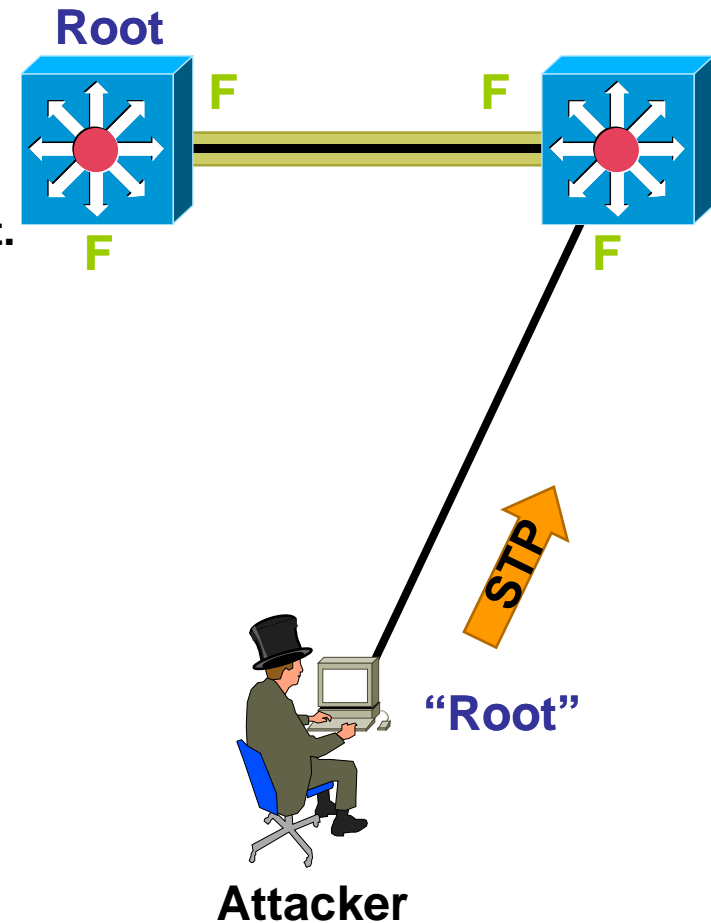
---

- **Impact mostly over-estimated**
- **DoS possible, but may be limited to one VLAN**
- **Traffic redirection possible under rare circumstances**
- **Main tool: *yersinia***



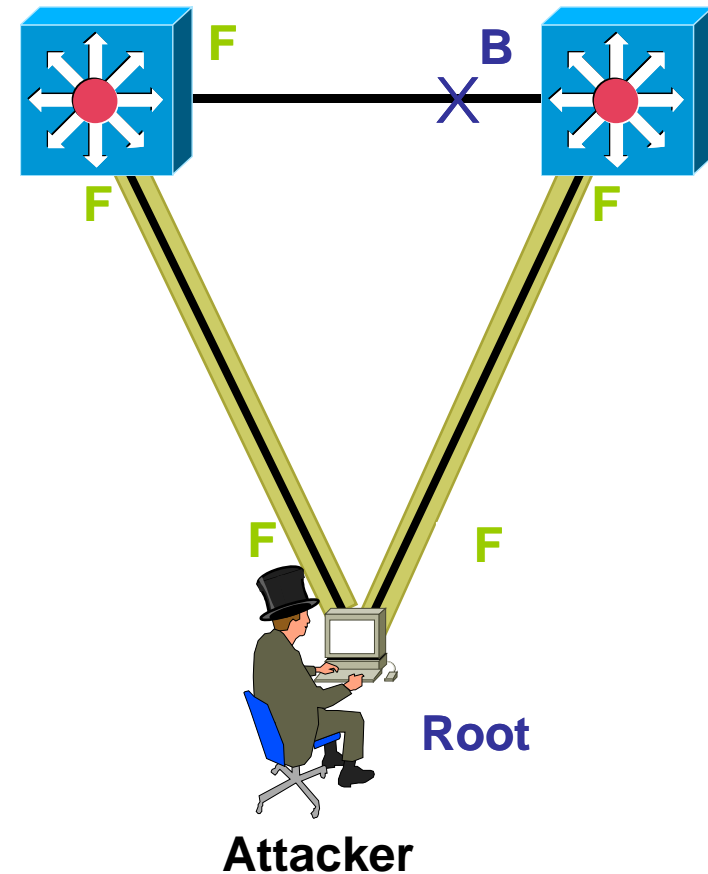
# Spanning-Tree, DoS Attack

- Attacker sends BPDUs to enforce recalculation
- Impact mostly DoS
- If *Rapid Spanning Tree* is used much less impact.

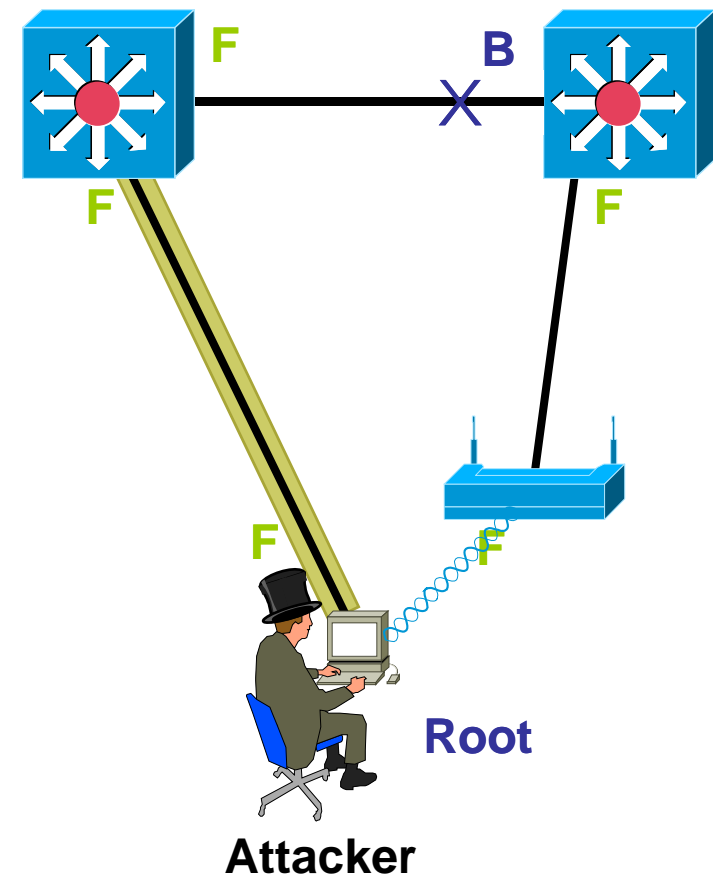


# Spanning-Tree, MiTM

- Attacker sends BPDUs to become root herself.
- If connected to *two* devices MiTM position achieved.  
=> large scale eavesdropping possible.
- Problem: usually attacker does not dispose of connection to two devices.



- In the age of WLANs some new paths arise.
- Usually access points are not connected to the same switch as wired connection of attacker.
  - => MiTM position via STP possible (if AP participates in STP)
- => Attacker can eavesdrop.



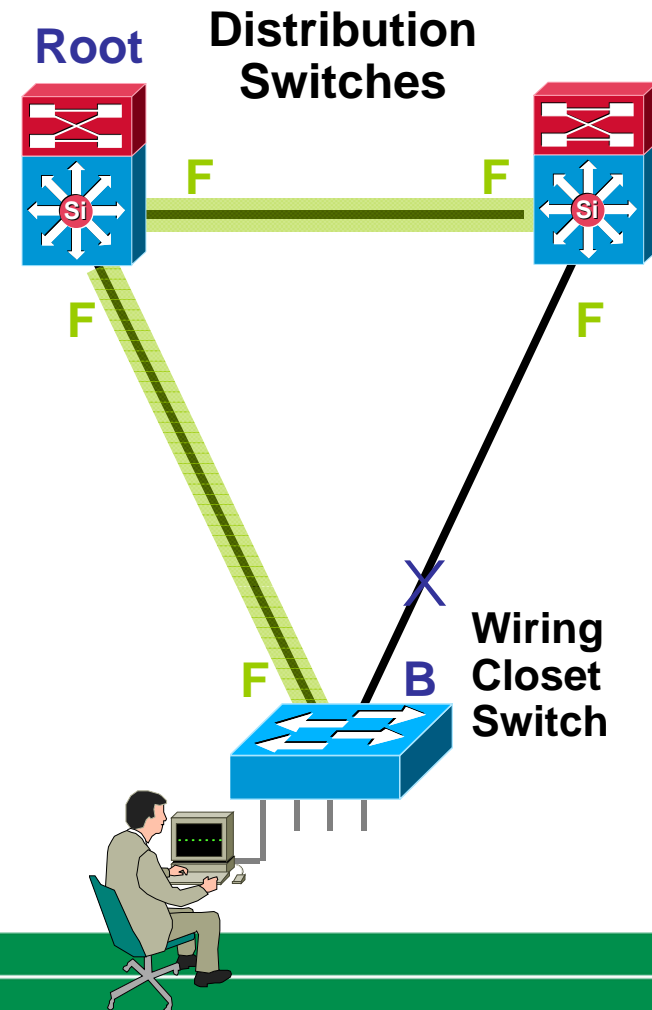
# STP Attacks, Mitigating Controls

- ***Rapid Spanning Tree*** for faster re-calculation.
- **Cisco: *BPDU Guard* and/or *Root Guard*.**
- ***Port Security*** against MiTM attack, as redirected packets get blocked then.



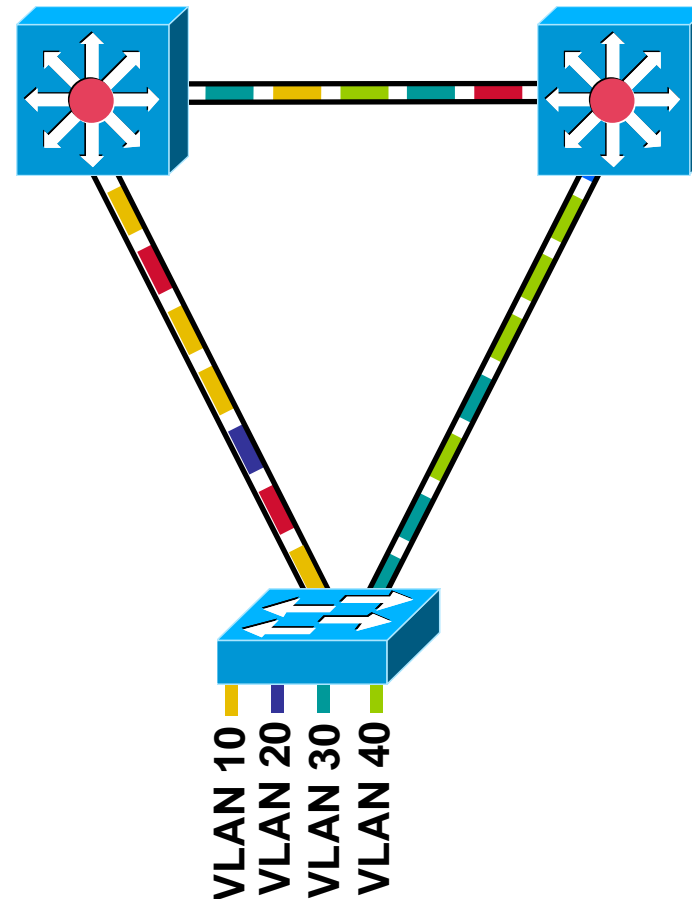
# Spanning Tree Toolkit (Cisco)

- **PortFast\***: Bypass listening-learning phase for access port
- **UplinkFast**: Three to five seconds convergence after link failure
- **BackboneFast**: Cuts convergence time by Max\_Age for indirect failure
- **LoopGuard\***: Prevents alternate or root port to become designated in absence of BPDUs
- **RootGuard\***: Prevents external switches from becoming root
- **BPDUGuard\***: Disable PortFast enabled port if a BPDU is received
- **BPDUFILTER\***: Do not send or receive BPDUs on PortFast enabled ports



# Trunking

- With *trunk* ports VLANs can be implemented across several switches.
- HP language: *tagged ports*.
- In *Cisco* space trunking state may be negotiated by a special protocol (DTP).



# Security problems with DTP

„The key thing to remember about DTP is the default mode on most switches is *Auto*.” [5]

- DTP usually enabled by default.
- This does not change after typical config performed by many admins:

```
interface FastEthernet0/2
switchport access vlan 27
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 27
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 27
spanning-tree portfast
```

- =>even on (alleged) *access ports* trunking possible.



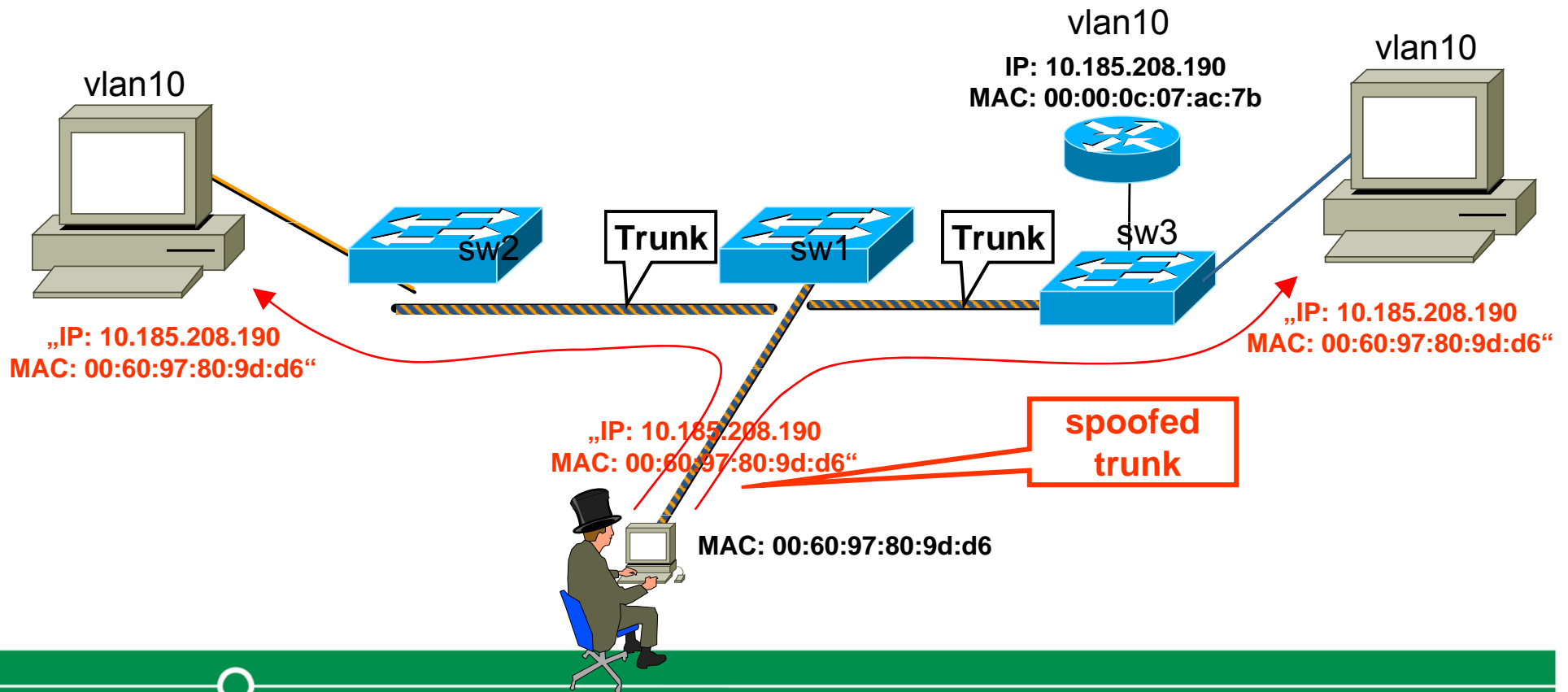
# Attack against DTP

```
erey@mobile:~  
----- yersinia 0.5.3 by Slay & tomac - DTP mode ----- [17:43:54]  
Neighbor-ID  Status      Domain      Iface  Last seen  
000BFDB648AF  03 (ACCESS/DESIRABLE)  ernw   eth0   08 May 17:40:46  
048D226BAE78  03 (ACCESS/DESIRABLE)  ernw   eth0   08 May 17:40:55  
000BFDB648AF  83 (TRUNK/DESIRABLE)  ernw   eth0   08 May 17:43:26  
048D226BAE78  83 (TRUNK/DESIRABLE)  ernw   eth0   08 May 17:43:29  
----- Attack Panel -----  
No  DoS  Description  
0   0    sending DTP packet  
1   1    enabling trunking  
-----  
Total Packets: 0  
Those strange: 0  
----- DTP Fields -----  
Source MAC 04: 000BFDB648AF  
Version 01  Domain  
Status 03  Type A5  Neighbor-ID 048D226BAE78  
-----  
Select attack to launch ('q' to quit)  
-----  
Spoofing [X]
```

Attacker will now be able to participate in all VLANs.



# ARP spoofing across VLAN boundaries



# VTP

- ***VLAN Trunking Protocol***
- **Cisco proprietary protocol to propagate VLAN information between switches.**
- **VTP packets only exchanged on trunk ports...**



# Attacks against VTP

```
erey@mobile:~  
----- yersinia 0.5.3 by Slay & tomac - VTP mode ----- [17:44:44]  
Code      Domain      MD5      Iface Last seen  
04 (JOIN)  ernw        eth0     08 May 17:40:56  
04 (JOIN)  ernw        eth0     08 May 17:40:56  
04 (JOIN)  ernw        eth0     08 May 17:41:22  
01 (SUMMARY) e  
04 (JOIN)  e  
04 (JOIN)  e  
----- Attack Panel -----  
No  DoS  Description  
0   0    sending VTP packet  
1   X    deleting all VTP vlans  
2   X    deleting one vlan  
3   0    adding one vlan  
-----  
Total Packets  
Those strange  
VTP Fields  
Source MAC 00: _____ Select attack to launch ('q' to quit) _____ 00  
Version 00 Code 00 Domain  
MD5 00000000000000000000000000000000 Updater 000.000.000.000  
Revision 00000000 Timestamp Start value 00000000  
Followers 000 Sequence 000 VLAN
```

Do I really have to discuss the impact of this?



# DTP / VTP

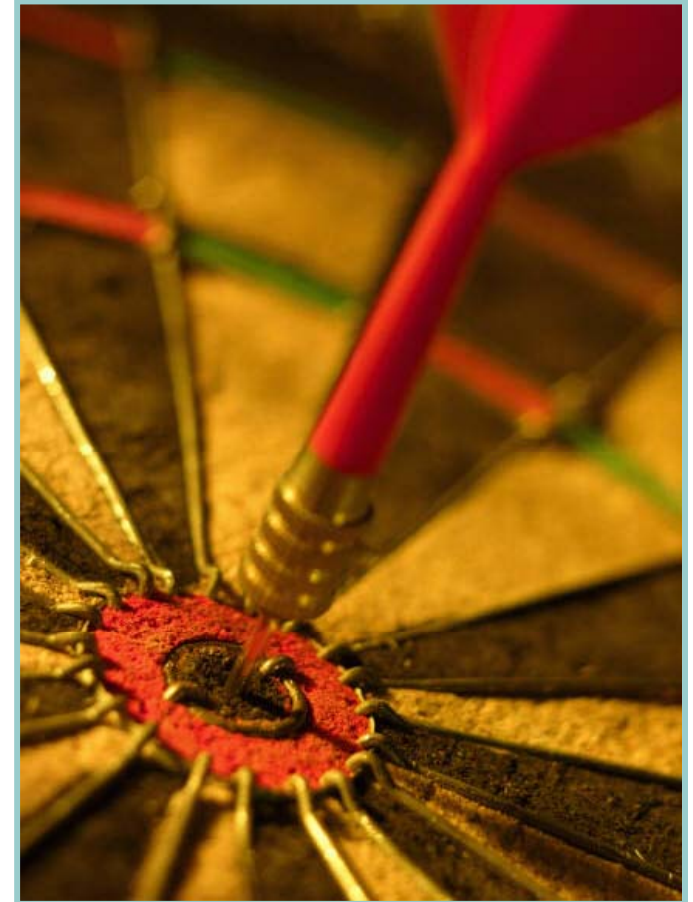
## Mitigating Controls

---

- **Disable DTP on all access ports:**  
**IOS: switchport mode access**  
**CatOS: set trunk *mod/port* off**
- **Use VTP passwords**
- **VTPv3 may help**



## Network Security on Layer 3



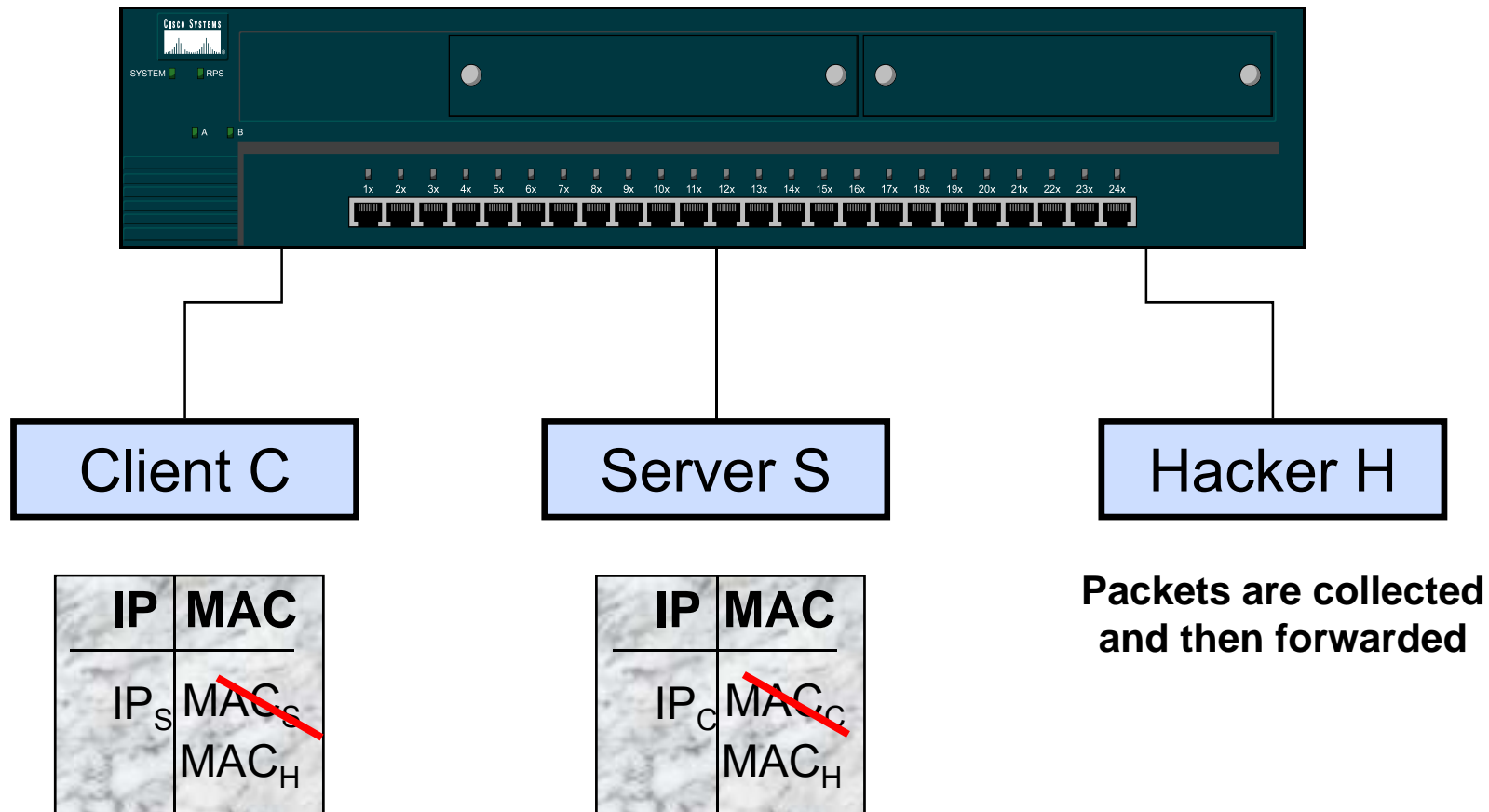
# Layer 3

## Two main attack paths:

- **Attacks against ARP (still one of the major problems)**
- **Attacks against routing protocols (rare, but efficient)**



# ARP Spoofing



# dsniff

- **DSNIFF(8)**

**NAME**

`dsniff - password sniffer`

- **SYNOPSIS**

```
dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen]
[-f services] [-t trigger[,...]] [-r|-w savefile]
[expression]
```

- **DESCRIPTION**

`dsniff` is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.

- `dsniff` automatically detects and minimally parses each application protocol, only saving the interesting bits, and uses Berkeley DB as its output file format, only logging unique authentication attempts. Full TCP/IP reassembly is provided by `libnids(3)`.



# *dsniff* in Action

```
-----  
02/13/03 17:28:38 udp 192.1.29.9.1052 -> 192.16.15.143.161 (snmp)  
[version 1]  
20isx02  
  
-----  
02/13/03 17:28:38 udp 192.1.29.9.2465 -> 192.1.50.2.161 (snmp)  
[version 1]  
19xvi95  
  
-----  
02/13/03 19:35:22 tcp 192.1.29.200.3334 -> 192.1.20.111.8080 (http)  
GET http://www.winnetmag.com/globals/images/header_net_link.gif HTTP/1.1  
Host: www.winnetmag.com  
Proxy-Authorization: Basic aXVoZWE6SGVmZVdlaXplbg== [iutea:HefeWeizen]  
  
-----  
02/13/03 20:05:49 tcp 192.1.29.144.1331 -> 192.1.20.71.143 (imap)  
LOGIN "iutm" "mecano"  
  
-----  
02/13/03 20:06:24 tcp 192.1.29.74.3120 -> 192.1.20.71.143 (imap)  
LOGIN "iulnm" "qweyxc00"  
  
-----  
02/13/03 20:06:37 tcp 192.1.29.123.33812 -> 192.1.20.163.23 (telnet)  
root  
hp
```



# ARP Attacks, Mitigating Controls

---

## Still difficult, mostly:

- **Network segmentation (ARP stuff only possible in subnet).**
- **Encryption**
- **Potentially static ARP entries (effective, but mgmt nightmare). Does not work very well in *Windows* space.**
- **New techniques, see below**



# Some New Techniques

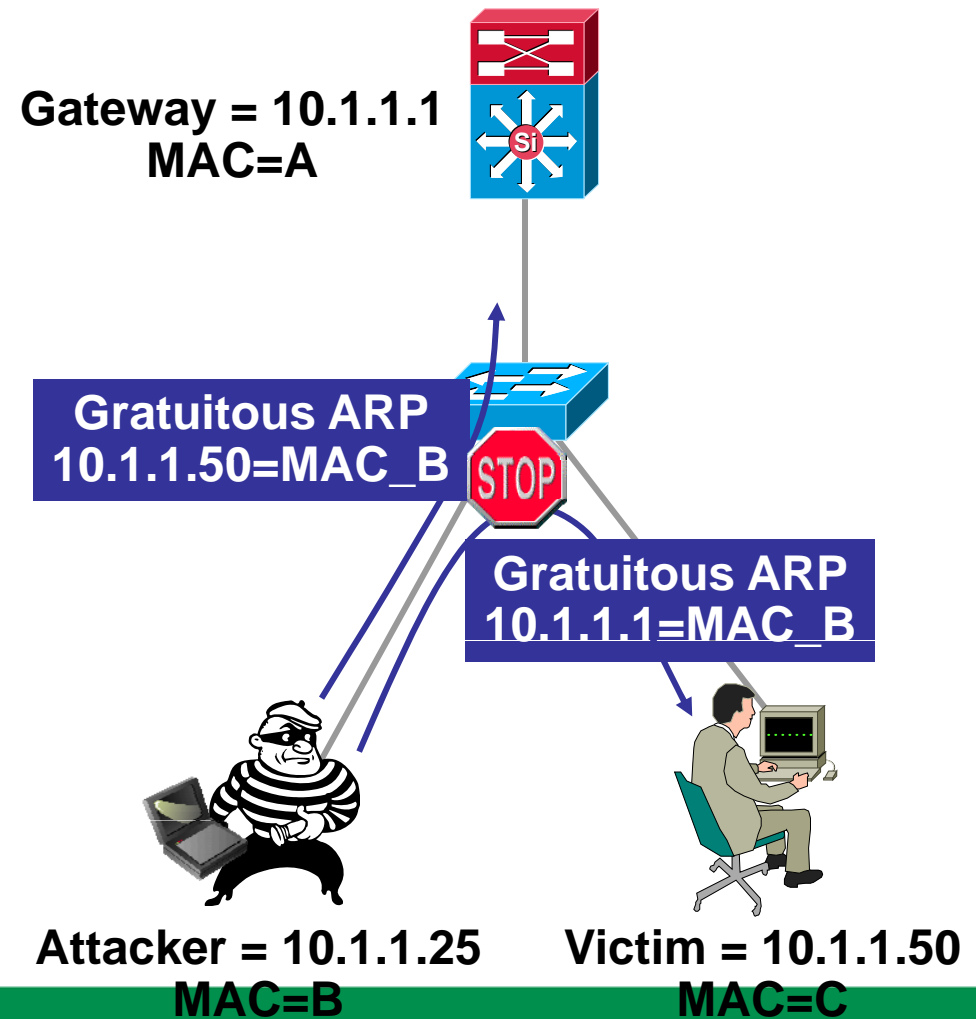
---

- **Cisco proprietary**
- **Interesting approaches to address some problems**
- **Working reliably in the interim**
- **Should be reconsidered**
- **But must be deployed with caution  
=> Risk Analysis ;-)**

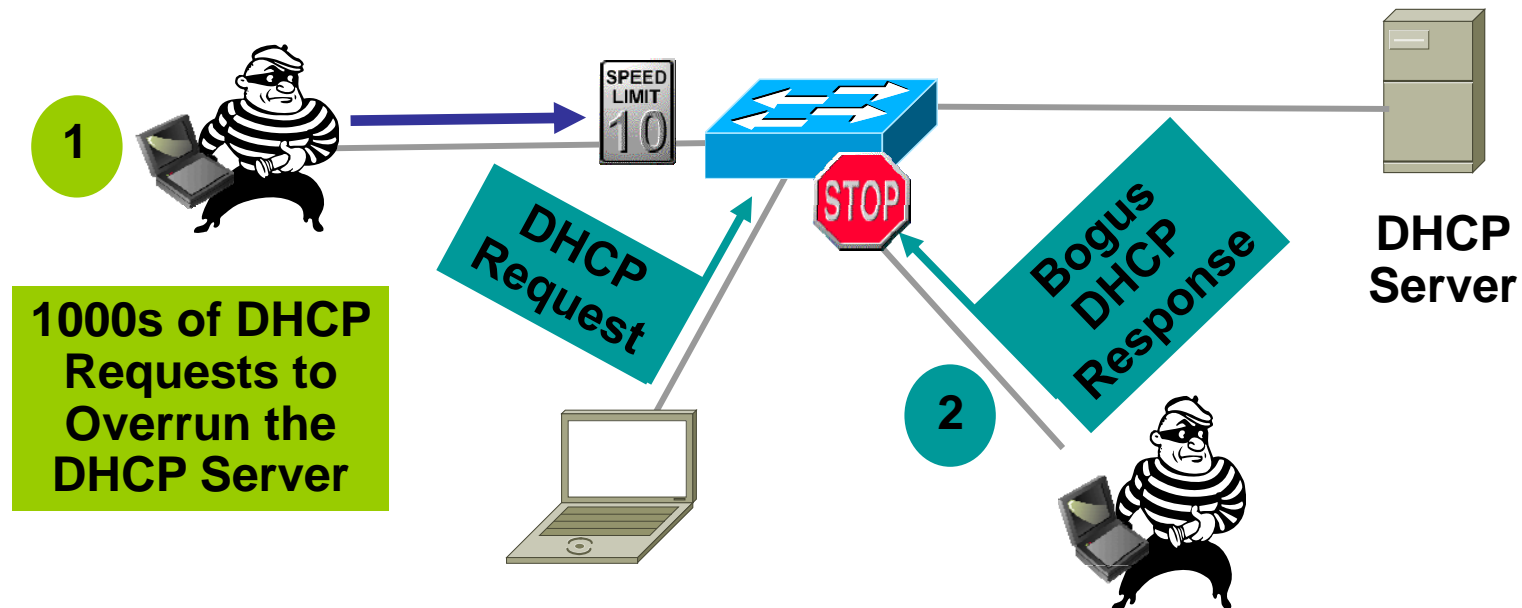


# Protection Against ARP Poisoning

- *Dynamic ARP inspection* protects against ARP poisoning (ettercap, dsniff, arpspoof)
- Uses the DHCP snooping binding table
- Tracks MAC to IP from DHCP transactions
- Rate-limits ARP requests from client ports; stop port scanning
- Drop BOGUS gratuitous ARP's; stop ARP poisoning/MIM attacks



# DHCP Snooping

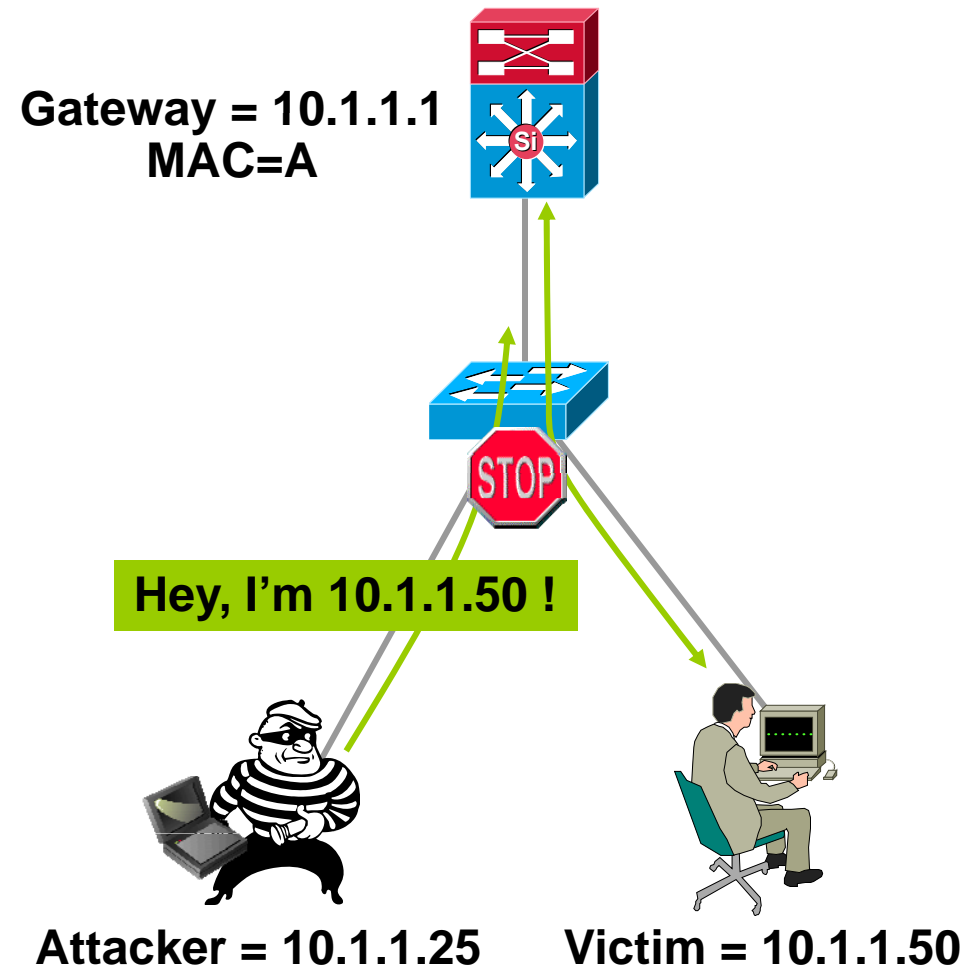


- DHCP requests (discover) and responses (offer) tracked
- Rate-limit requests on trusted interfaces; limits DOS attacks on DHCP server
- Deny responses (offers) on non trusted interfaces; stop malicious or errant DHCP server



# IP Source Guard

- IP source guard protects against spoofed IP addresses
- Uses the DHCP snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP



# Attacks Against Routing Protocols

- **Very efficient for large scale traffic redirection if used “appropriately“**
- **Still regarded not feasible in many networks**
- **Recent research proves otherwise**
- **Again: risk analysis needed.**
  
- **See also:**  
***[http://www.ernw.de/content/e7/e181/e520/download523/ospf-sec\\_02\\_dr\\_ger.pdf](http://www.ernw.de/content/e7/e181/e520/download523/ospf-sec_02_dr_ger.pdf)*** &  
***RFC 4953: Generic Threats to Routing Protocols***



# Attacks against Routing, Mitigating Controls

---

- **See *Building Blocks* and use your brain cells ;-)**



## How to Evaluate the Whole Stuff



# The Auditor's Problem

---

- **Given the span between “pure security“ and operational requirements there are no “general checklists“.**
- **There are not too many “Universal Best Practices“.**
- **Those that exist are not followed.**
  
- **Most important question (as always ;- ) during an audit:**

**Did you perform proper risk analysis?**

**If so, show the documents.**

**If not, justify why you don't follow *Best Practices*.**

**[Problem for auditor: What are those? Answer: see below]**

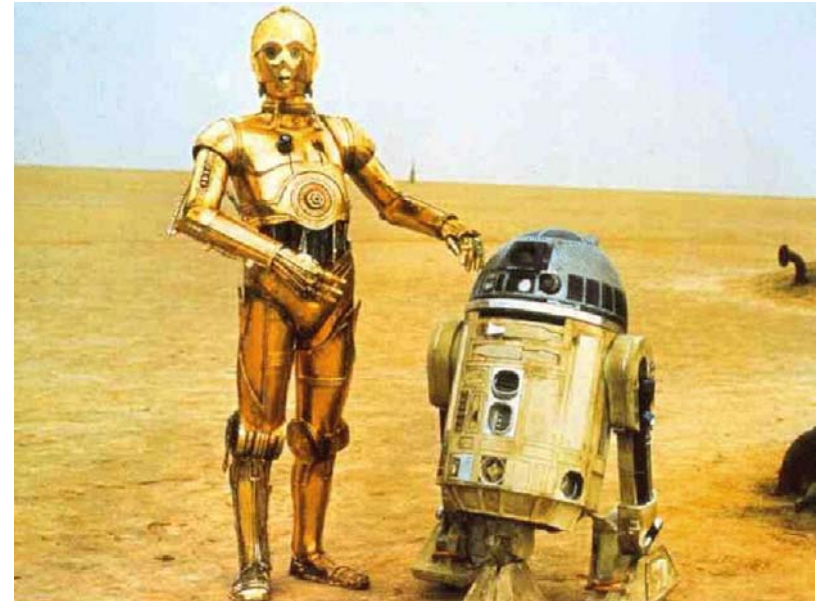


# Checklists

- **It *is* still possible to compile reasonable checklists for some areas. I'll list the most important base material here.**
- **Device Hardening:**  
<http://www.cymru.com/Documents/secure-ios-template.html>  
<http://www.mirrors.wiretapped.net/security/info/reference/nsa-guides/cisco/cisco-ios-switch-security-configuration-guide.pdf>
- **Management Procedures:**  
<http://www.ietf.org/rfc/rfc4778.txt>
- **Routing Protocols:**  
[http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/sfblp\\_wp.pdf](http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/sfblp_wp.pdf)



## Some Notes on the Future



# Two Main Trends as for Layer 2 / 3 Security

- **New protocols on Layer 2 and 3, mainly introduced by Windows Vista**
  - Link Layer Topology Discovery (LLTD)
  - Link Local Multicast Name Resolution (LLMNR)
  - Peer Name Resolution Protocol (PNRP)
  - Teredo
  - etc.
  
- **End-to-end Ethernet Services across WAN**
  - Metro Ethernet
  - EoMPLS
  - Virtual Private LAN Service (VPLS)



# New Protocols

---

- **Whole new bunch of protocols emerged recently**
- **Still very little understood, especially as for sec aspects**
- **Some enabled by default in Win Vista**
- **Most probably we will see “interesting stuff“ here...**



# Ethernet Services

- **More and more carrier offerings that do not provide ethernet as an “access medium“, but as a service.**
- **=> (Mostly) transparent *ethernet* connections across WAN possible.**
- **Might be interesting for quite some corporations (world wide VLANs possible, easy multicast communication etc.).**
- **Will then bring “merger of Layer 2 and Layer 3“.**
- **With some new security problems...**



- **Transparent LAN Service (TLS)** provides

- Intra-company Connectivity
- Full transparency of control protocols (BPDUs)

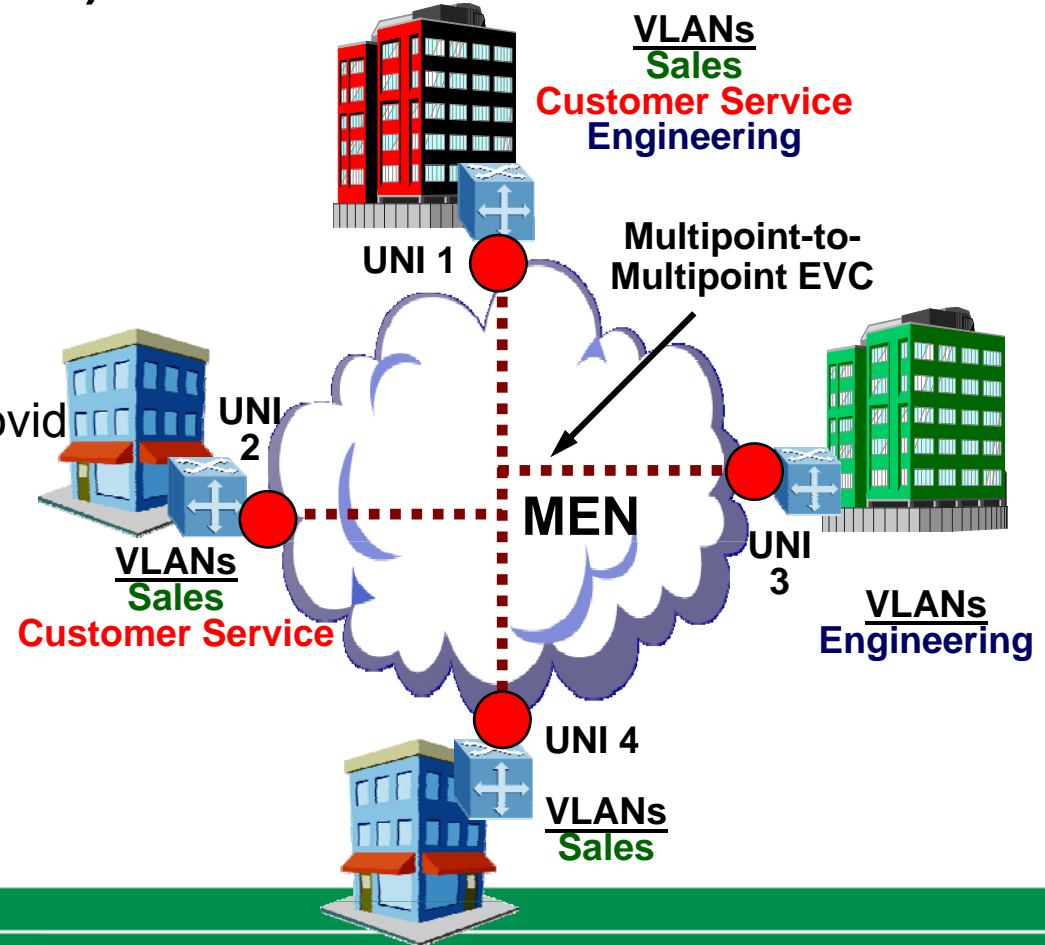
- **New VLANs added**

- without coordination with provider

!!!

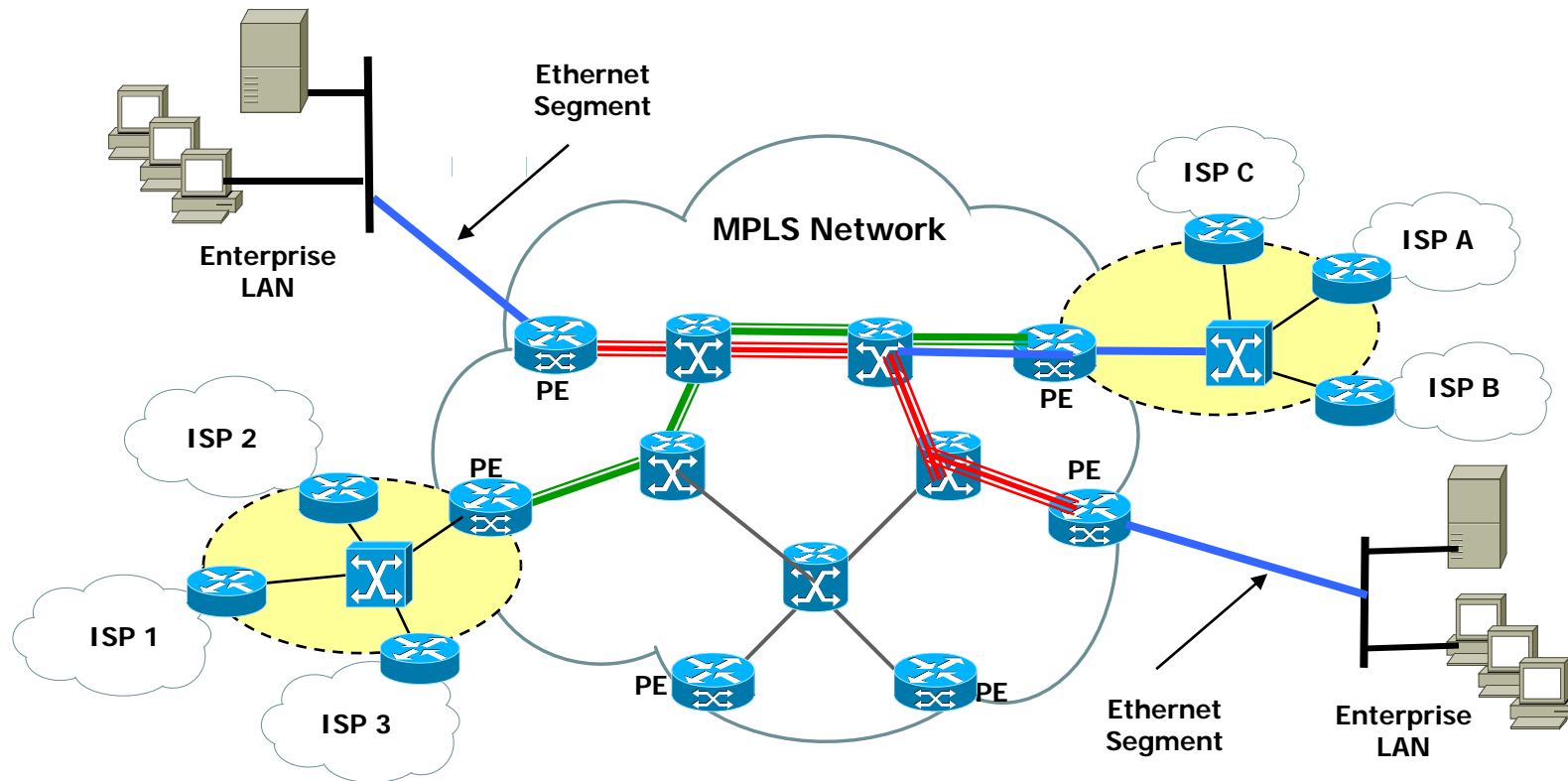
TLS makes the MEN look like a LAN

## Transparent LAN Service

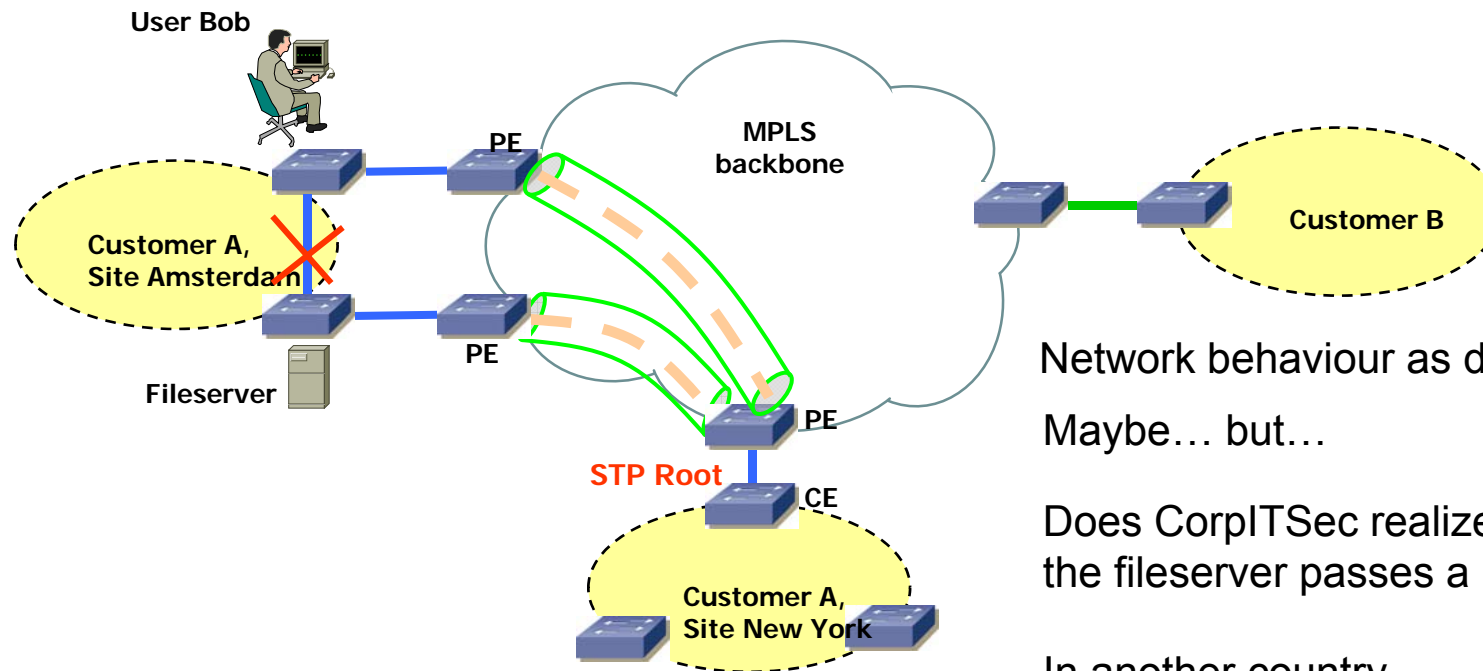


# Technology

## *Ethernet over MPLS*



## Example of Potential Problem



Network behaviour as designed?

Maybe... but...

Does CorpITSec realize that Bob's access to the fileserver passes a provider backbone?

In another country...

where *Carnivore/DCS 1000* applies (or a different 'understanding of intellectual property' exists)...

Unencrypted!



# Summary

- **In the field of network security there's a strong opposition between "theoretical security" & operational requirements.**
- **However there are some general building blocks of network security that can be universally applied.**
- **Several attacks exist on Layer 2 and Layer 3 that can lead to loss of availability or breach of confidentiality.**
- **Due to a multitude of new protocols and due to "ethernet convergence" we'll see new classes of attacks.**



# Final Words

**Whatever you do... always remember the following**

- **Ross Callon in *RFC 1925*:**

**“Some things in networking can never be fully understood by someone who neither builds commercial networking equipment nor runs an operational network.”**

**=> If really interested in this stuff get your hands on some devices ;-)**

- ***Simplicity Principle* from  
<http://tools.ietf.org/html/draft-ymbk-arch-guidelines-05>**



# Questions?



Thanks for your  
attention!



# References

---

- [2] VLAN Hopping: <http://www.sans.org/resources/idfaq/vlan.php>
- [3] System Requirements to Implement Trunking:  
[http://www.cisco.com/en/US/tech/tk389/tk390/technologies\\_tech\\_note09186a008017f86a.shtml](http://www.cisco.com/en/US/tech/tk389/tk390/technologies_tech_note09186a008017f86a.shtml)
- [4] Tool *Yersinia*: <http://yersinia.sourceforge.net>
- [5] Cisco Packet Magazine, "Layer 2 -- The Weakest Link":  
[http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac222/about\\_cisco\\_packet\\_feature09186a0080142deb.html](http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac222/about_cisco_packet_feature09186a0080142deb.html)
- [7] Andreas Aurand: IOS Router Security:  
[http://www.decus.de/slides/sy2003/09\\_04/2g05.pdf](http://www.decus.de/slides/sy2003/09_04/2g05.pdf)



# Appendix A

## Important Standards

---

- ISO 18028 *Information technology — Security techniques — IT network security*
- ISO 17799:2005 *Information technology — Security techniques — Code of practice for information security management*  
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT  
11 ACCESS CONTROL
- RFC 3871 – Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
- RFC 4778 – Current Operational Security Practices in Internet Service Provider Environments
- RFC 3013 – Recommended Internet Service Provider Security Services and Procedures

