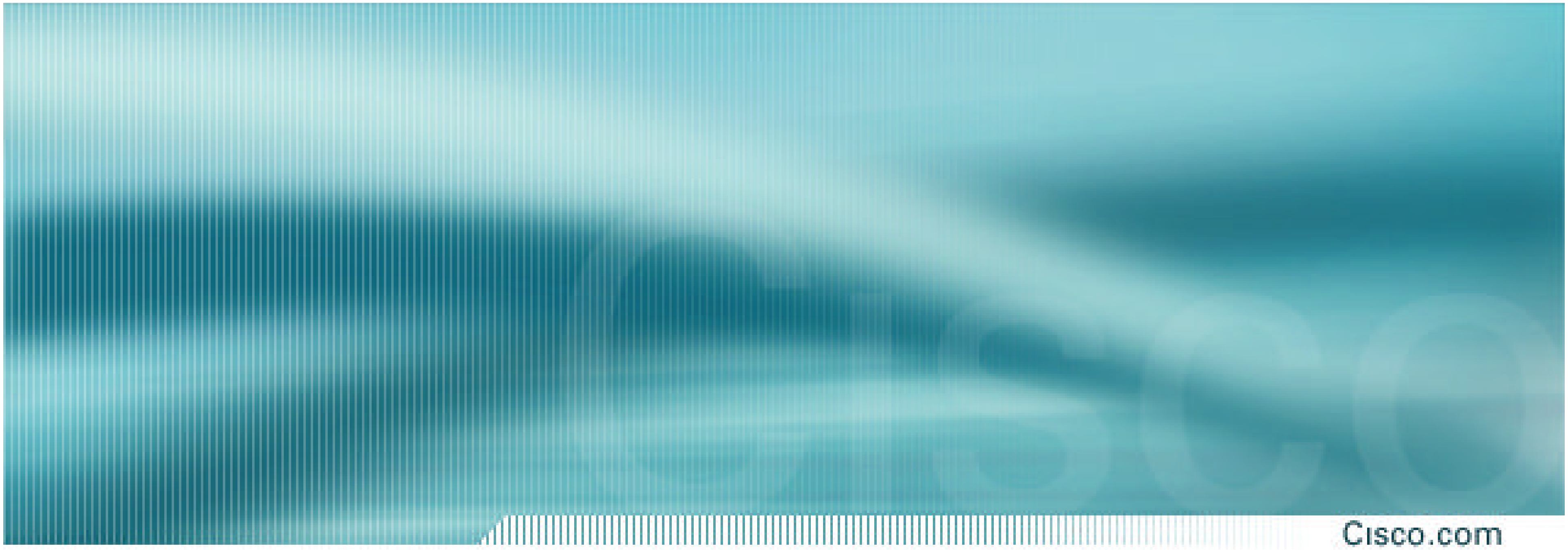


Layer 2 Attacks and Their Mitigation

Louis Senecal

lsenecal@cisco.com

Agenda

- MAC Attacks
- VLAN “Hopping” Attacks
- GARP Attacks
- Spanning Tree Attacks
- Layer 2 Port Authentication
- Summary

Caveats

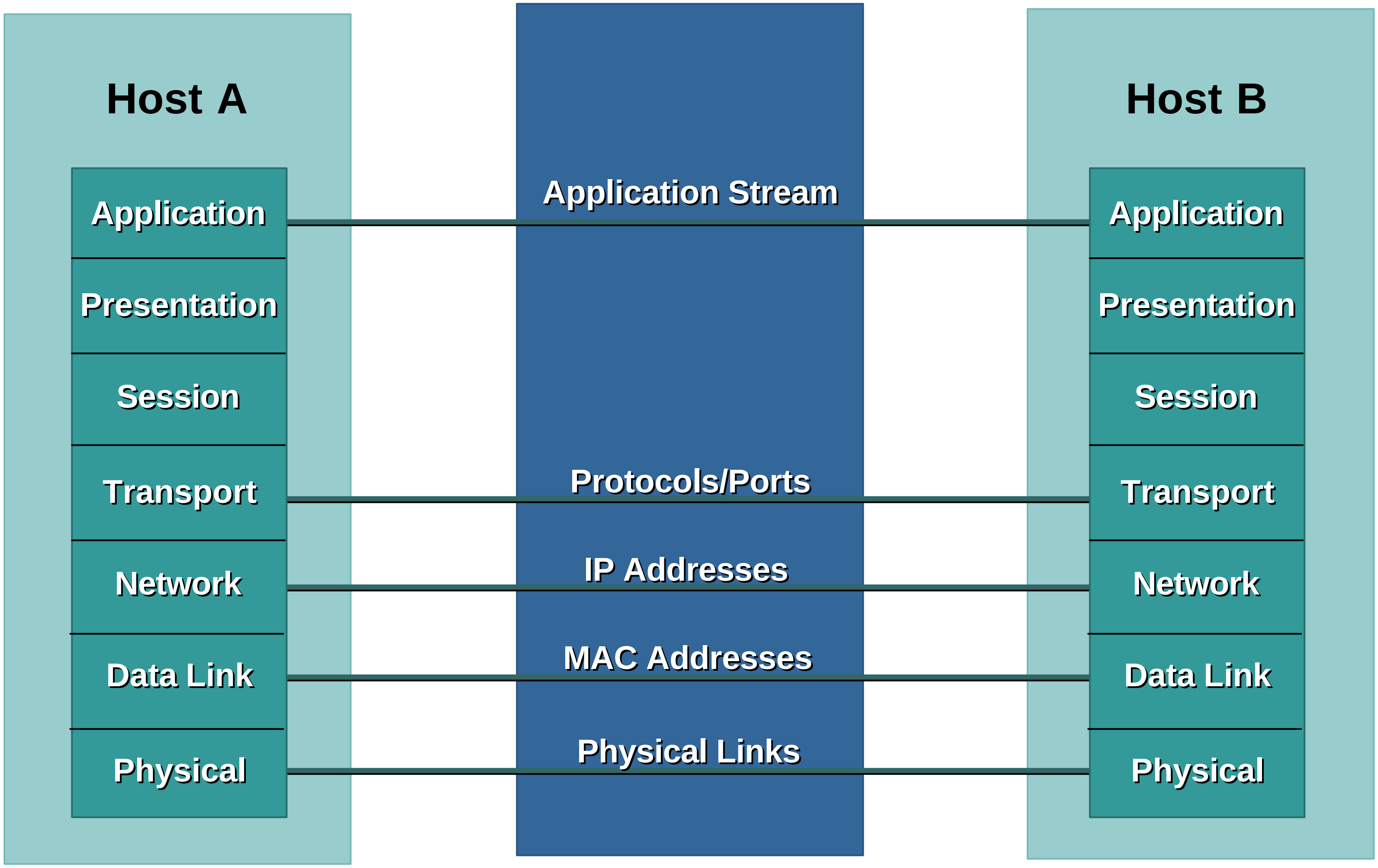
- **All attacks and mitigation techniques assume a switched Ethernet network running IP**

    If shared Ethernet access is used (WLAN, Hub, etc.) most of these attacks get much easier☺

- **Hackers are a creative bunch, attacks in the “theoretical” category can move to the practical in a matter of days**
- **This is not a comprehensive talk on configuring Ethernet switches for security; the focus is on L2 attacks and their mitigation**

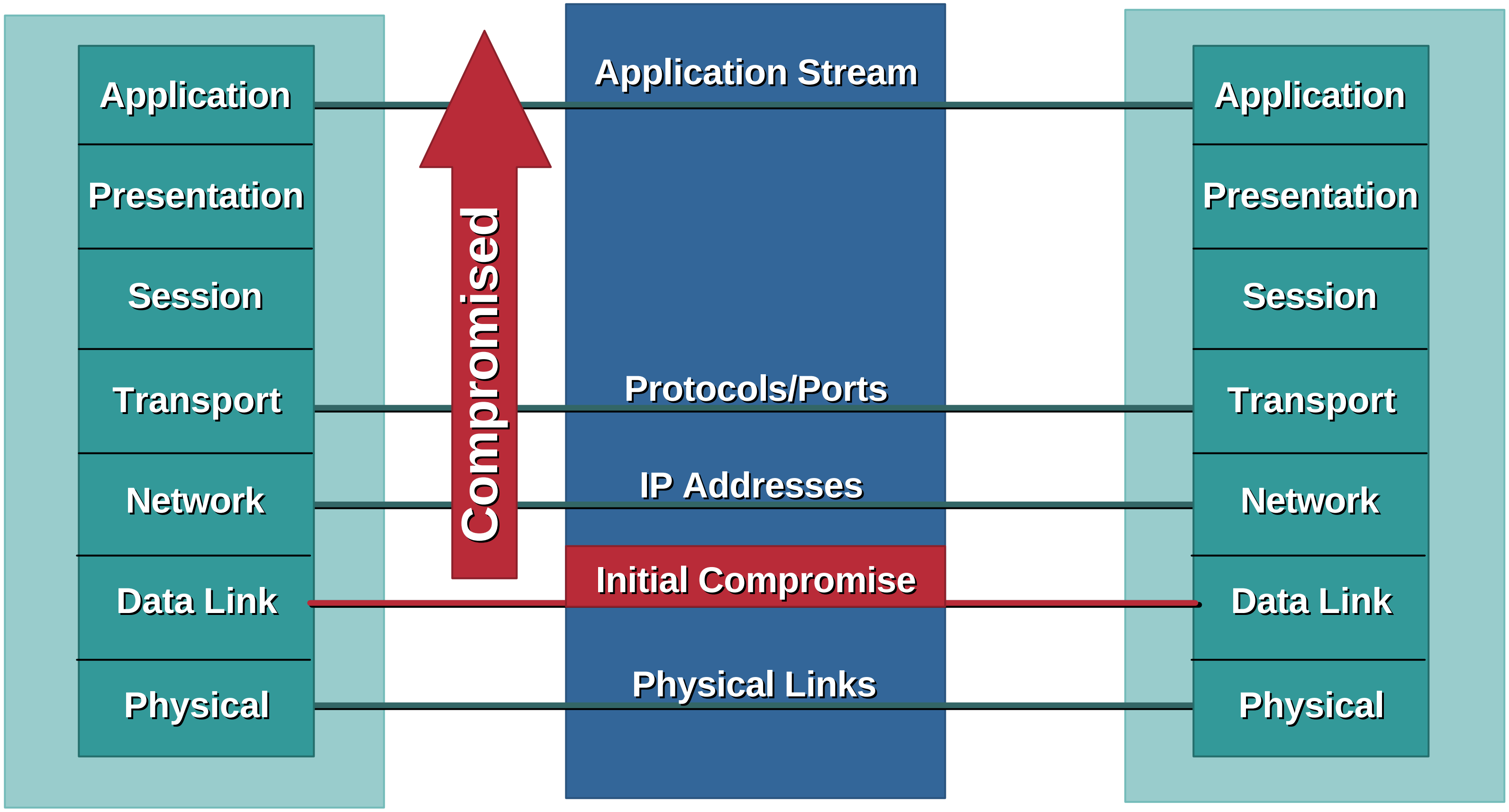
Why Worry about Layer 2 Security?

OSI Was Built to Allow Different Layers to Work without Knowledge of Each Other



The Domino Effect

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem
- Security is only as strong as your weakest link
- When it comes to networking, layer 2 can be a VERY weak link



NetOPS/SecOPS, Who’s Problem Is It?

Questions:

- What is your stance on L2 security issues?
- Do you use VLANs often?
- Do you ever put different security levels on the same switch using VLANs?
- What is the process for allocating addresses for segments?

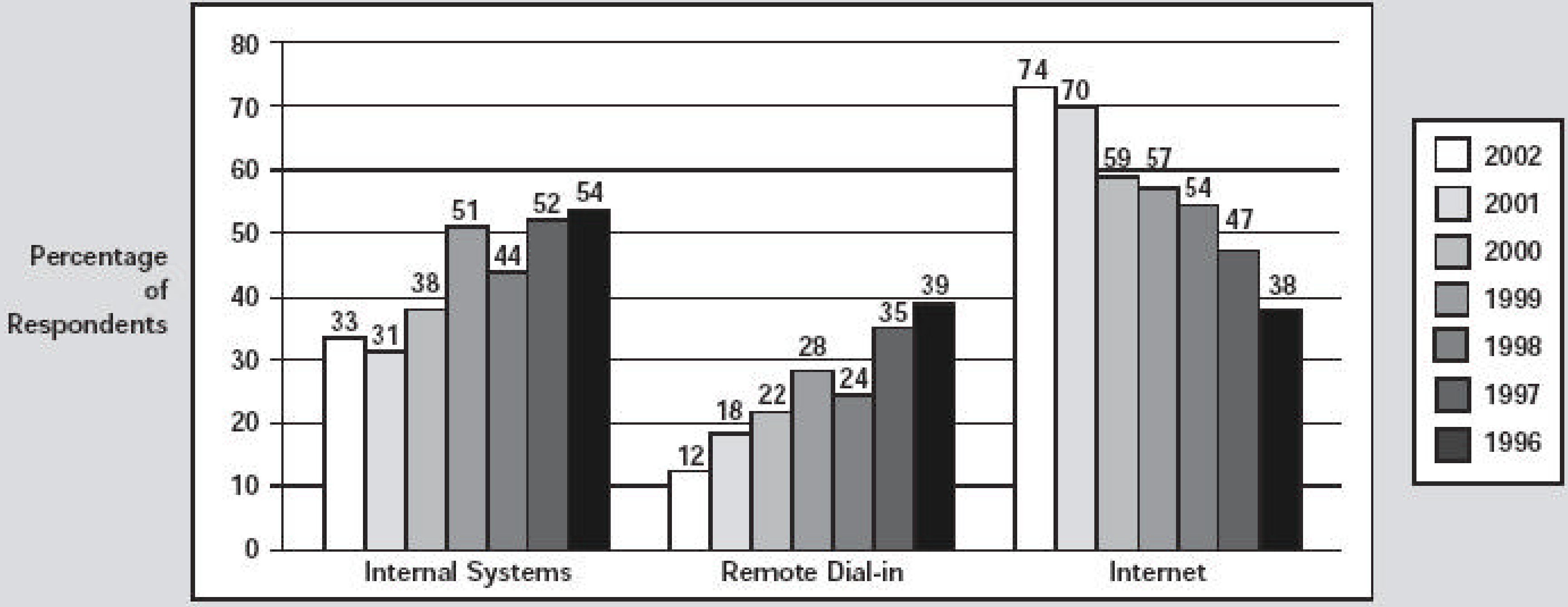
Most NetOPS

- There are L2 Security issues?
- I use VLANs all the time
- Routing in and out of the same switch is OK by me! That’s what VLANs are for
- The security guy asks me for a new segment, I create a VLAN and assign him an address space

Most SecOPS

- I handle security issues at L3 and above
- I have no idea if we are using VLANs
- Why would I care what the network guy does with the switch?
- I ask Netops for a segment, they give me ports and addresses

The Numbers from CSI/FBI



2002:	481 Respondents/96%
2001:	384 Respondents/72%
2000:	443 Respondents/68%
1999:	324 Respondents/62%
1998:	279 Respondents/54%
1997:	391 Respondents/69%
1996:	174 Respondents/40%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

MAC Attack

MAC Address/CAM Table Review

48 Bit Hexadecimal (Base16) Unique Layer Two Address

1234.5678.9ABC

First 24 bits = Manufacture Code
Assigned by IEEE

0000.0cXX.XXXX

Second 24 bits = Specific Interface,
Assigned by Manufacture

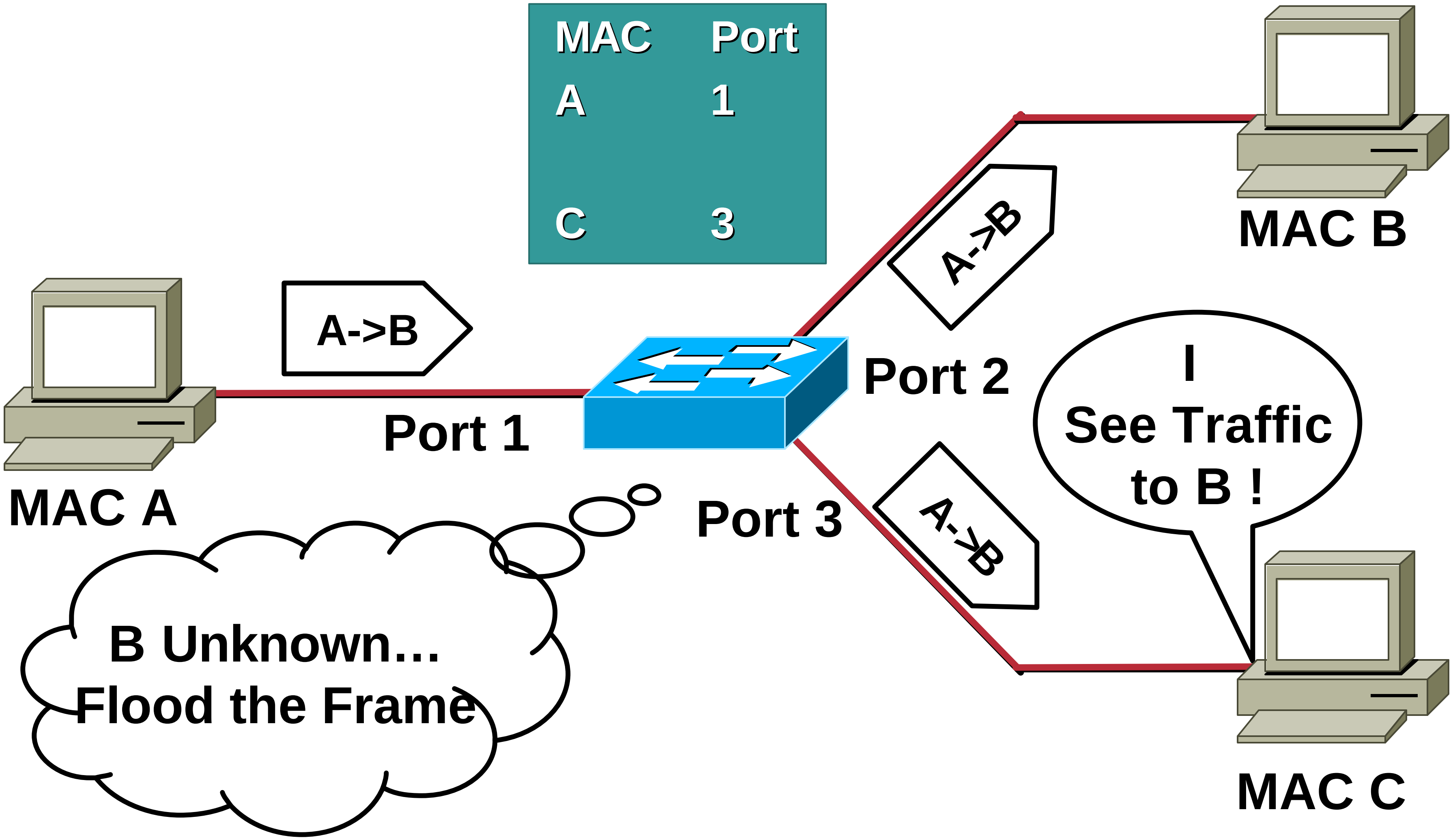
XXXX.XX00.0001

All F’s = Broadcast

FFFF.FFFF.FFFF

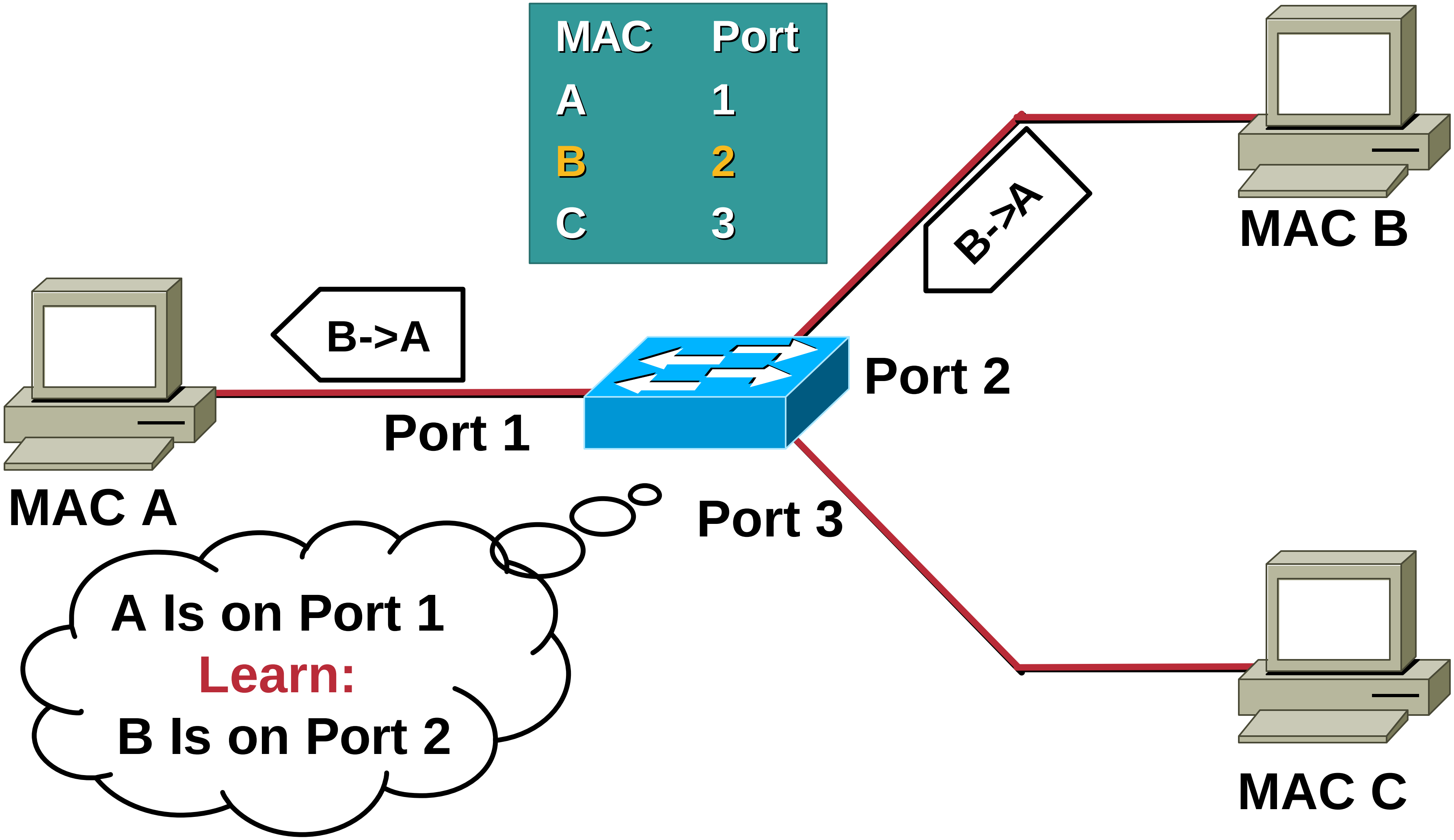
- CAM Table stands for Content Addressable Memory
- The CAM Table stores information such as MAC addresses available on physical ports with their associated VLAN parameters
- CAM Tables have a fixed size

Normal CAM Behaviour 1/3



MAC	Port
A	1
C	3

Normal CAM Behaviour 2/3



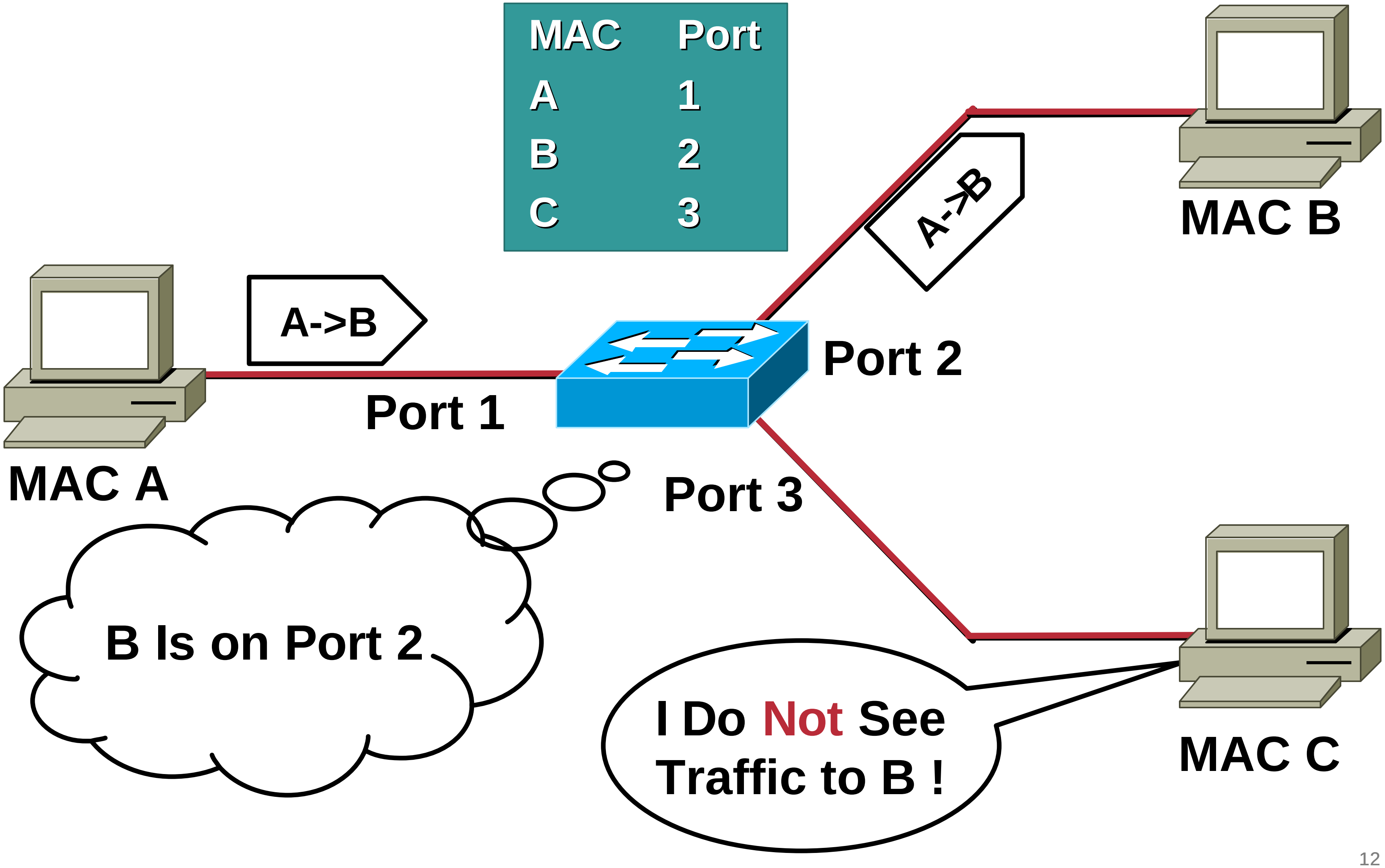
MAC	Port
A	1
B	2
C	3

A Is on Port 1

Learn:

B Is on Port 2

Normal CAM Behaviour 3/3

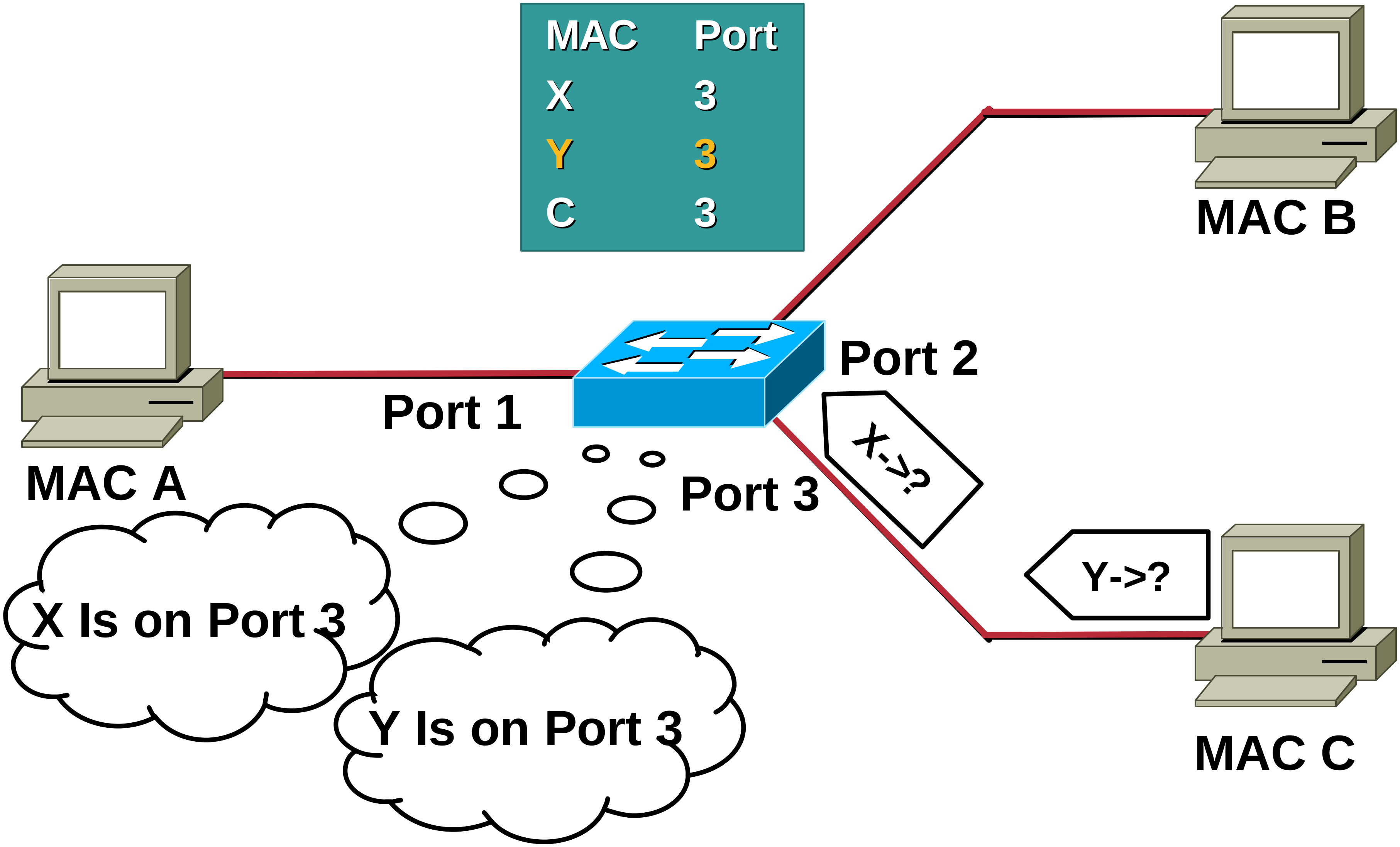


MAC	Port
A	1
B	2
C	3

CAM Overflow 1/3

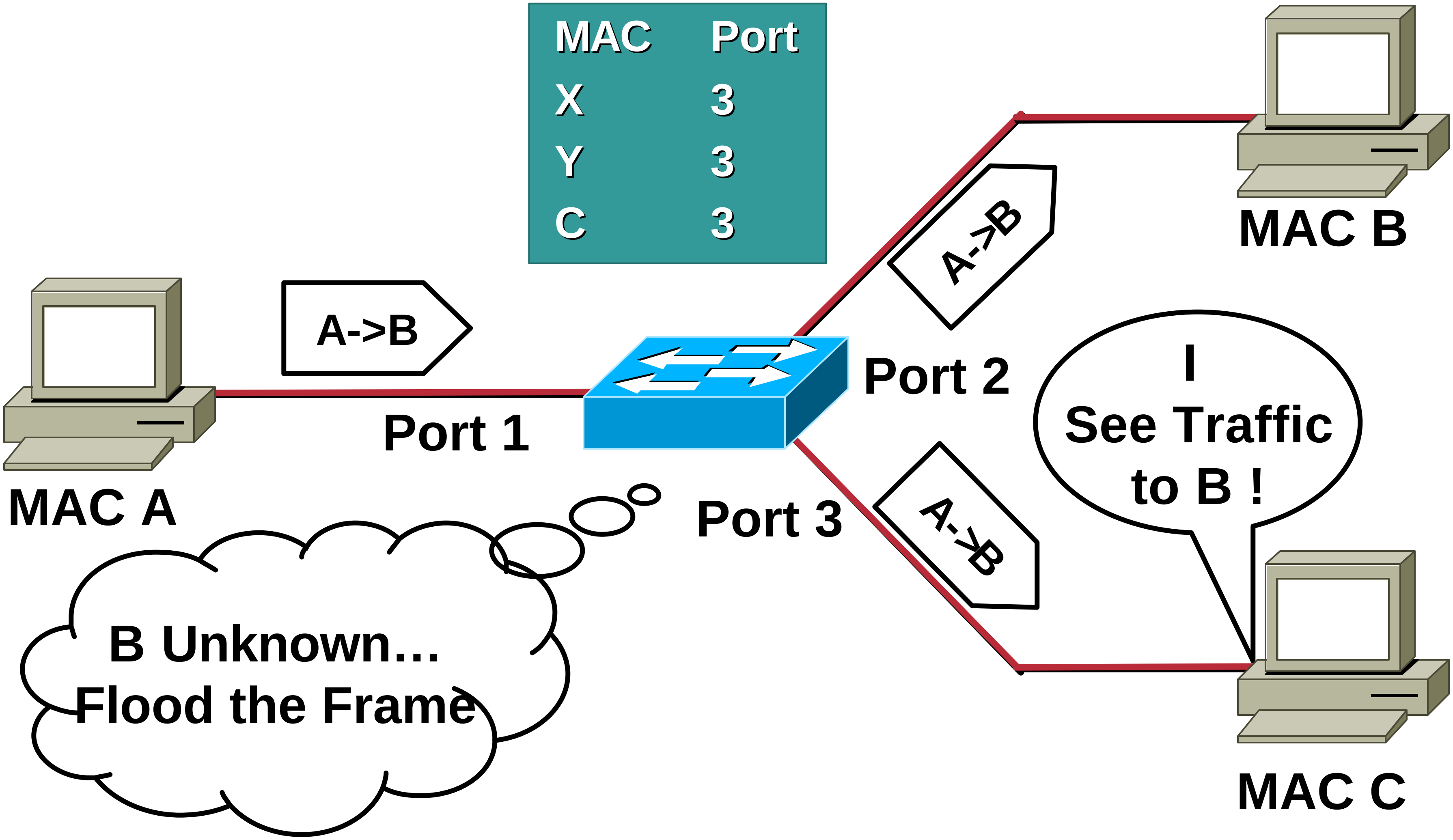
- Theoretical attack until May 1999
- *macof* tool since May 1999 (about 100 lines of perl)
- Based on CAM Table’s limited size

CAM Overflow 2/3



MAC	Port
X	3
Y	3
C	3

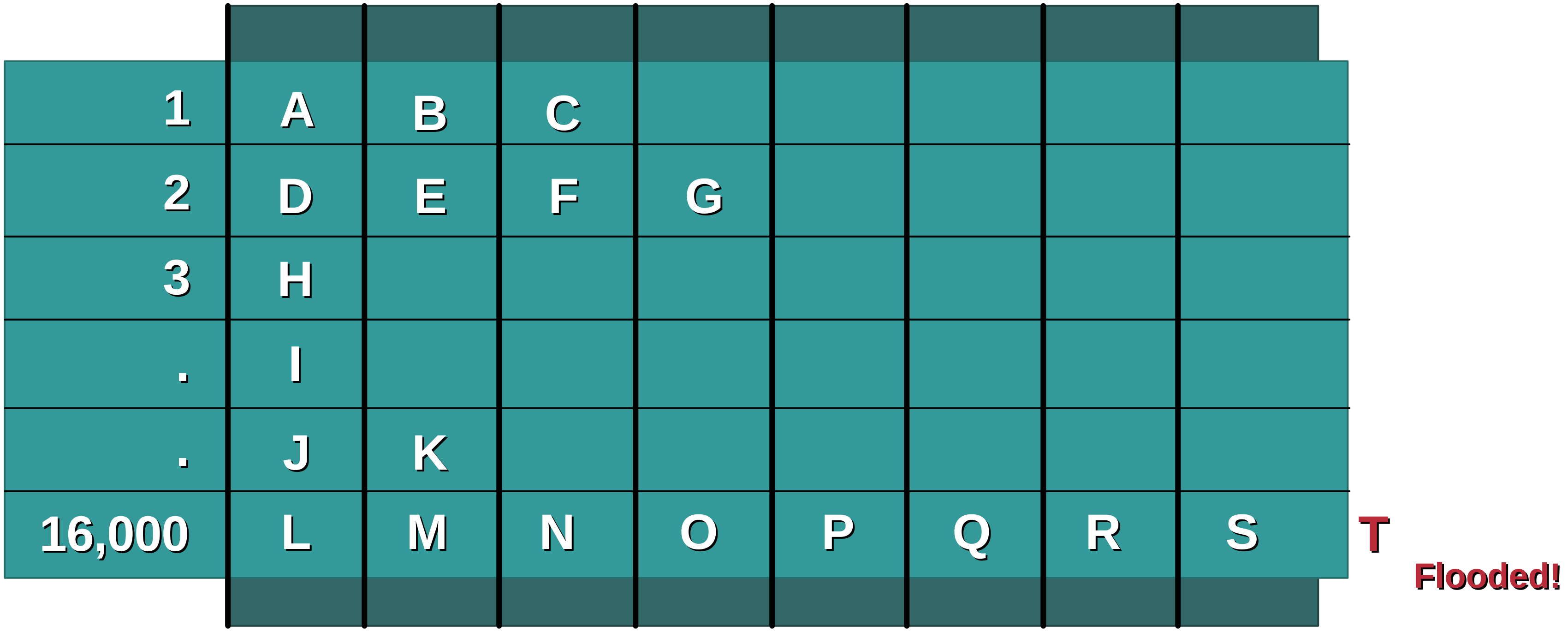
CAM Overflow 3/3



MAC	Port
X	3
Y	3
C	3

Catalyst CAM Tables

- Catalyst switches use hash to place MAC in CAM table



1	A	B	C					
2	D	E	F	G				
3	H							
.	I							
.	J	K						
16,000	L	M	N	O	P	Q	R	S

T

Flooded!

- 63 bits of source (MAC, VLAN, misc) creates a 17 bit hash value
  - If the value is the same there are 8 columns to place CAM entries, if all 8 are filled the packet is flooded

MAC Flooding Switches with Macof

```
[root@hacker-lnx ds
b5:cf:65:4b:d5:59 2c:01                                 318(0) win 512
68:2a:55:6c:1c:1c bb:33                                 9777(0) win 512
1e:95:26:5e:ab:4f d7:80                                 866876(0) win 512
51:b5:4a:7a:03:b3 70:a9                                 4740(0) win 512
51:75:2e:22:c6:31 91:a1                                 621419(0) win 512
7b:fc:69:5b:47:e2 e7:65                                 935(0) win 512
19:14:72:73:6f:ff 8d:ba                                 98(0) win 512
63:c8:58:03:4e:f8 82:b6                                 135783(0) win 512
33:d7:e0:2a:77:70 48:96                                 100617(0) win 512
f2:7f:96:6f:d1:bd c6:15                                 931(0) win 512
22:6a:3c:4b:05:7f 1a:78                                 802199(0) win 512
f6:60:da:3d:07:5b 3d:db                                 461959(0) win 512
bc:fd:c0:17:52:95 8d:c1                                 9994(0) win 512
bb:c9:48:4c:06:2e 37:12                                 5491(0) win 512
e6:23:b5:47:46:e7 78:11                                 268(0) win 512
c9:89:97:4b:62:2a c3:4a                                 820794(0) win 512
56:30:ac:0b:d0:ef 1a:11                                 090777(0) win 512
```

```
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 42
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 36314
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 62213
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 88874
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 104683
ottlab-sm6509a> (enable) sh cam count dy
…
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 130997
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 131001
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 131006
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 131008
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 131009
ottlab-sm6509a> (enable) sh cam count dy
Total Matching CAM Entries = 131009
```

CAM Table Full!

- Dsniff (macof) can generate 480,000 MAC entries on a switch per minute 8000/s*60
- Assuming a perfect hash function the CAM table will total out at 128,000 (16,000 x 8) 131,052 to be exact

  Since hash isn’t perfect it actually takes 70 seconds to fill the CAM table

```
OTTLAB-SM (enable) sho cam count dynamic

Total Matching CAM Entries = 131052
```

- Once table is full, traffic without a CAM entry floods on the VLAN, but NOT existing traffic with an existing CAM entry

Snoop output on non-SPAN port 15.1.1.50

```
10.1.1.22 -> (broadcast)  ARP C Who is 15.1.1.1, 15.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 15.1.1.19, 15.1.1.19 ?
15.1.1.26 -> 15.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
15.1.1.25 -> 15.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

MAC Flooding Attack Mitigation
- Port Security

```
ottlab-3524a#sh mac count
Dyn
Secu
Stati
Syst
Tota
```

```
ottlab-3524a(config)#int fa 0/7
ottlab-3524a(config-if)#port security max-mac-count 2
ottlab-3524a(config-if)#port security action shutdown
```

```
00:22:08: %PORT_SECURITY-2-SECURITYREJECT: Security violation occurred on module 0 port 7
caused by MAC address e03a.2209.8dd4
00:22:08: %PORT_SECURITY-2-SECURITYREJECT: Security violation occurred on module 0 port 7
caused by MAC address ccad.1943.de45
00:22:08: %PORT_SECURITY-2-SECURITYREJECT: Security violation occurred on module 0 port 7
 caused by MAC address 8af0.9f02.febe
00:22:08: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
```

http://cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/config/sec_port.htm

Port Security Details

- Beware management burden and performance hit
- Lots of platform specific options besides just “ON/OFF”

```
CatOS> (enable) set port security mod/ports... [enable | disable]
[mac_addr] [age {age_time}] [maximum {num_ of_mac}] [shutdown
{shutdown_time}] [violation{shutdown | restrict}]
```

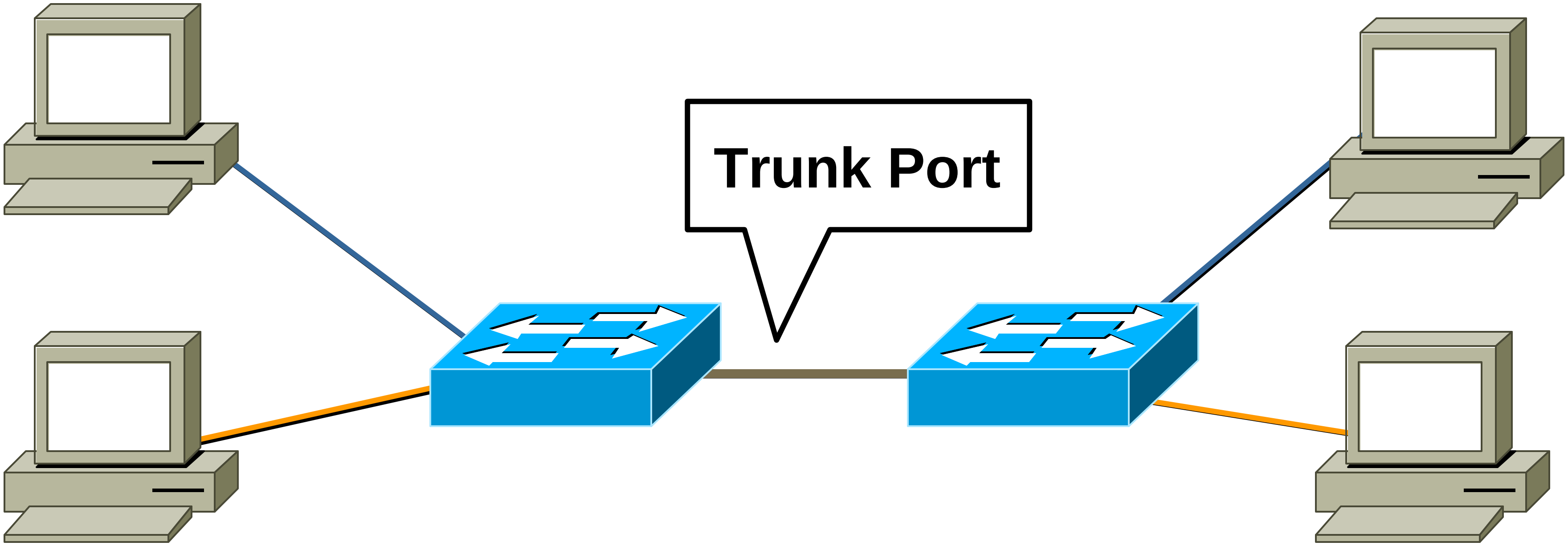
- MAC Tables do not have unlimited size (platform dependant)

```
2002 Apr 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:Port 3/21 shutdown due to no space
```

Available in Cat 29XX, 4K, 5K, and 6K in CatOS 5.2; 29/3500XL in 11.2(8)SA; 2950 in 12.0(5.2)WC(1); 3550 in 12.1(4)EA1

VLAN “Hopping” Attacks

Trunk Port Refresher



- Trunk ports have access to all VLANs by default
- Used to route traffic for multiple VLANs across the same physical link (generally used between switches)
- Encapsulation can be 802.1Q or ISL

Dynamic Trunk Protocol (DTP)

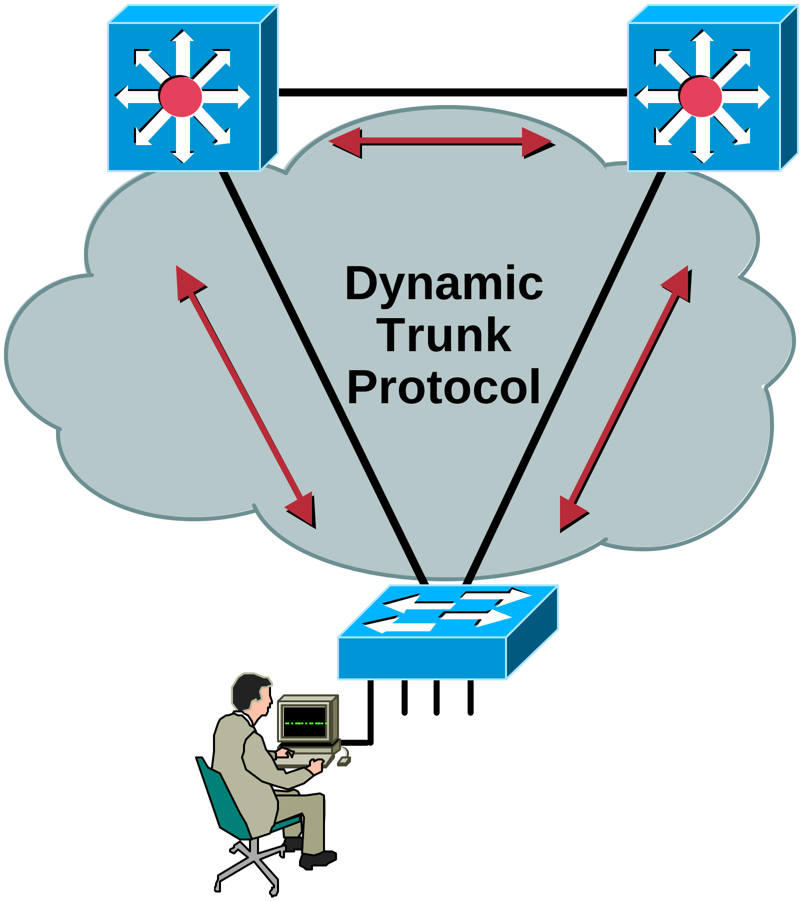
- What is DTP?

  Automates ISL/802.1Q trunk configuration

  Operates between switches

  Does not operate on routers

- DTP synchronizes the trunking mode on link ends
- DTP prevents the need for management intervention on both sides
- DTP state on ISL/1Q trunking port can be set to “Auto”, “On”, “Off”, “Desirable”, or “Non-Negotiate”



DTP Administrative States

- Administrator configurable trunk states

ON I want to be a trunk and I don’t care what you think! (Used when the other end does not understand DTP)

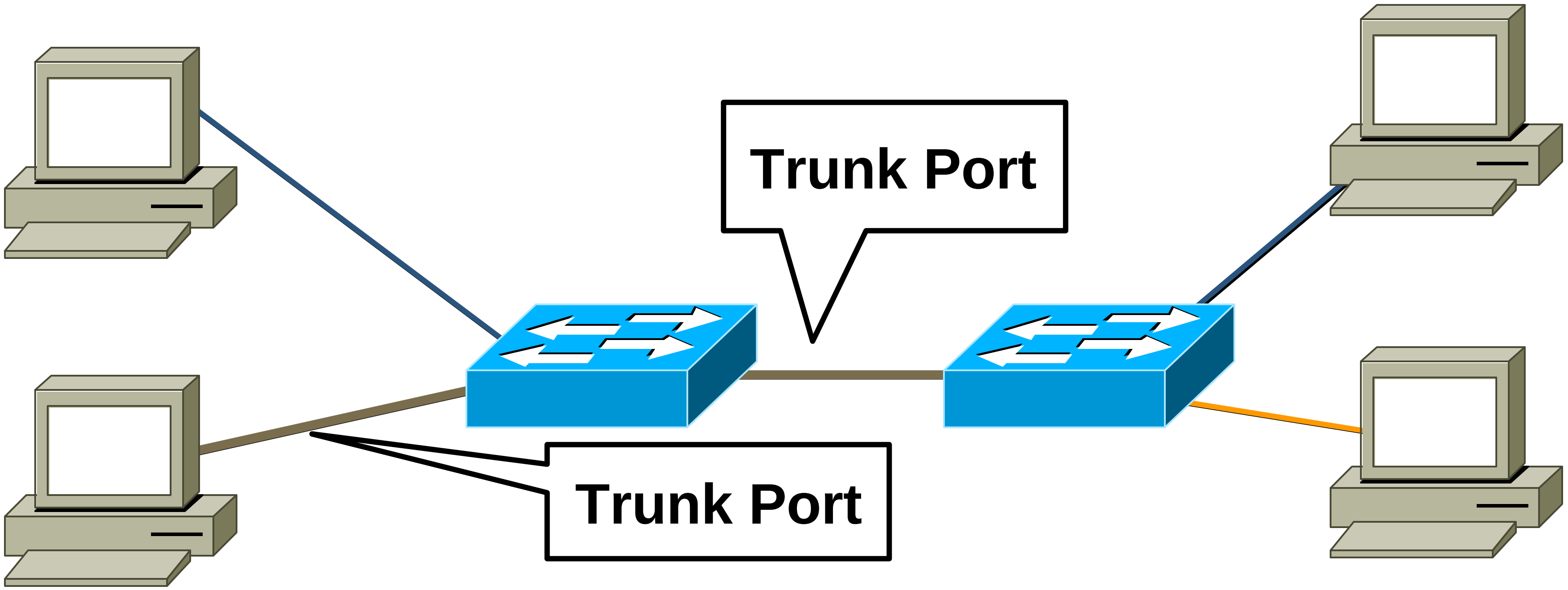
OFF I don’t want to be a trunk and I don’t care what you think! (Used when the other end cannot do ISL or .1Q)

Desirable I’m willing to become a VLAN trunk; are you interested? (Used when you are interested in being a trunk)

Auto I’m willing to go with whatever you want! (This is the default on many switches!)

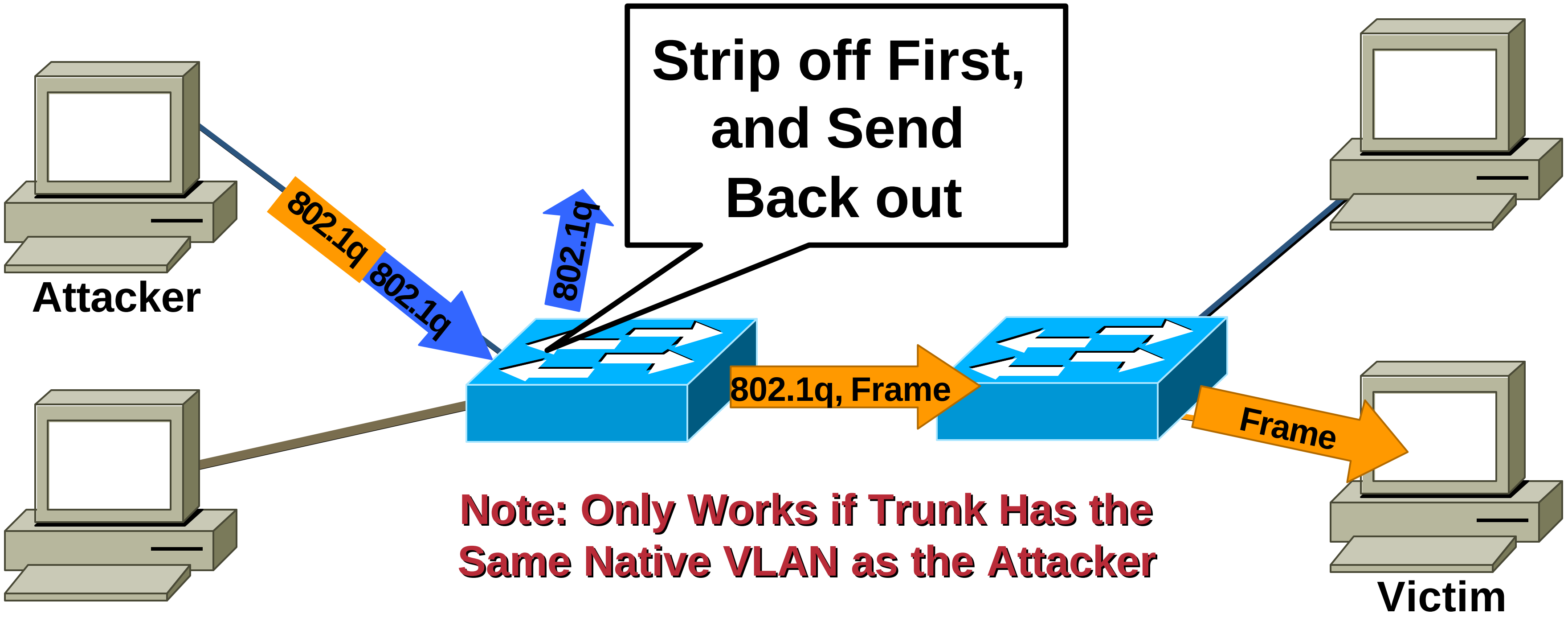
Non-Negotiate I want to trunk, and this is what kind of trunk I will be! (Used when you want a specific type of trunk ISL or .1Q)

Basic VLAN Hopping Attack



- A station can spoof as a switch with ISL or 802.1Q signaling (DTP signaling is usually required as well)
- The station is then member of all VLANs
- Requires a trunking favorable setting on the port (the SANS paper is two years old)

Double Encapsulated 802.1q VLAN Hopping Attack



Note: Only Works if Trunk Has the Same Native VLAN as the Attacker

- Send double encapsulated 802.1Q frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Disabling Auto-Trunking

```
CatOS> (enable) set trunk <mod/port> off
IOS(config-if)#switchport mode access
```

- **Defaults change depending on switch; always check:**

  From the Cisco docs: “The default mode is dependent on the platform…”

  To check from the CLI:

```
CatOS> (enable) show trunk [mod|mod/port]
IOS#show interface type number switchport
```

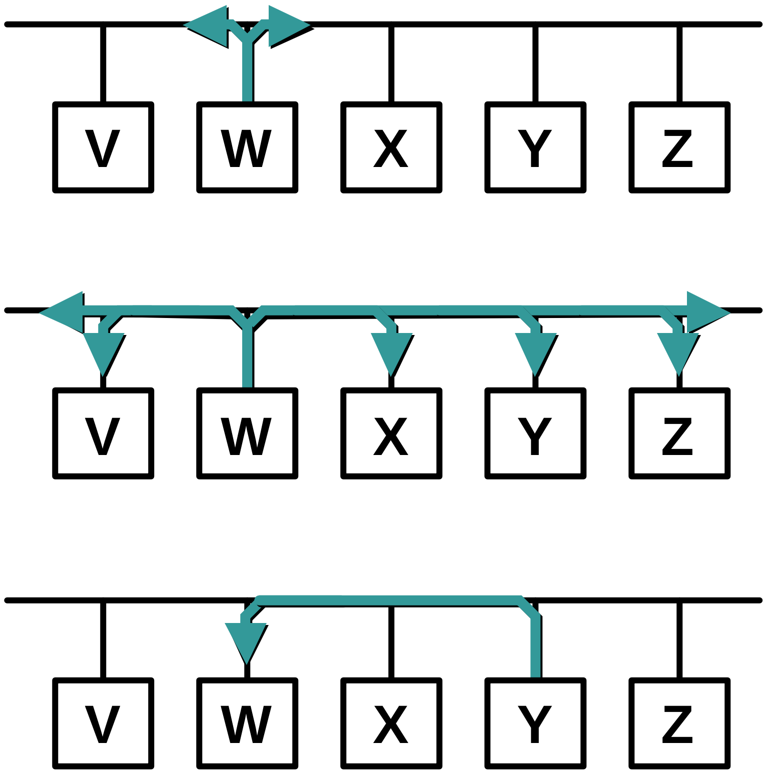
Security Best Practices for VLANs and Trunking

- Always use a dedicated VLAN ID for all trunk ports
- Disable unused ports and put them in an unused VLAN
- Be paranoid: Do not use VLAN 1 for anything
- Set all user ports to non-trunking (DTP Off)

GARP Attacks

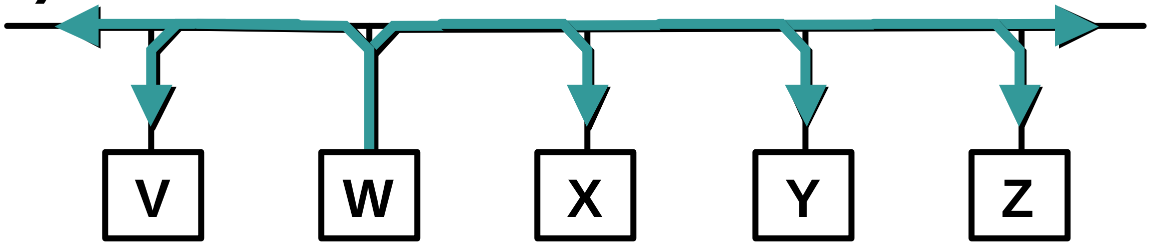
ARP Refresher

- An ARP request message should be placed in a frame and broadcast to all computers on the network
- Each computer receives the request and examines the IP address
- The computer mentioned in the request sends a response; all other computers process and discard the request without sending a response



Gratuitous ARP

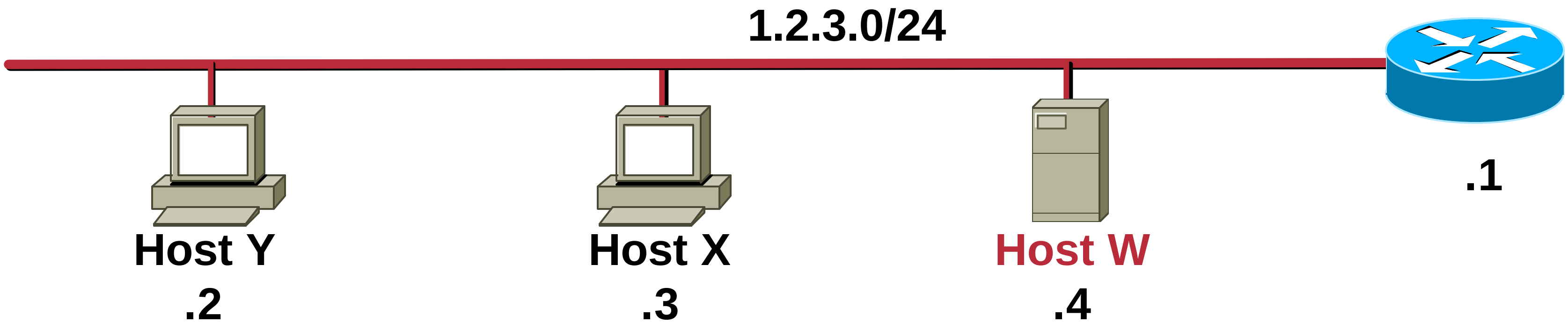
- Gratuitous ARP is used by hosts to “announce” their IP address to the local network and avoid duplicate IP addresses on the network; routers and other network hardware may use cache information gained from gratuitous ARPs
- Gratuitous ARP is a broadcast packet (like an ARP request)



- HOST W: Hey everyone I’m host W and my IP Address is 1.2.3.4 and my MAC address is 12:34:56:78:9A:BC

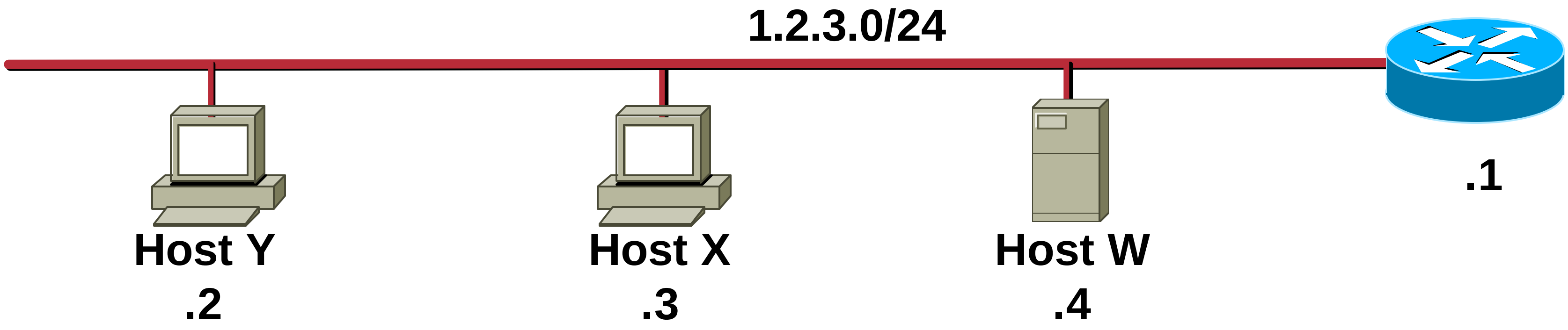
Misuse of Gratuitous ARP

- ARP has no security or ownership of IP or MAC addresses
- What if we did the following?



- Host W broadcasts I'm 1.2.3.1 with MAC 12:34:56:78:9A:BC
- (Wait 5 seconds)
- Host W broadcasts I'm 1.2.3.1 with MAC 12:34:56:78:9A:BC

A Test in the Lab



- When host Y requests the MAC of 1.2.3.1 the real router will reply and communications will work until host W sends a gratuitous ARP again
- Even a static ARP entry for 1.2.3.1 on Y will get overwritten by the Gratuitous ARP on some OSs (NT4,WIN2K for sure)

Dsniff—A Collection of Tools to Do:

- ARP Spoof
- MAC flooding
- Selective sniffing
- SSH/SSL interception

Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff/

Arpspoof in Action

```
[root@hacker-lnx dsniff-2.3]# ./arpspoof 15.1.1.1
```

```
C:\>test

C:\>arp -d 15.1.1.1

C:\>ping -n 1 15.1.1.1

Pinging 15.1.1.1 with 32 bytes of data:

Reply from 15.1.1.1: bytes=32 time<10ms TTL=255

C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-04-4e-f2-d8-01     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-10-83-34-29-72     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
```

More on Arpspoof

- All traffic now flows through machine running dsniff in a half-duplex manner

  Not quite a sniffer but fairly close

- Port security doesn’t help
- Static ARP doesn’t help
- Note that attack could be generated in the opposite direction by spoofing the destination host when the router sends its ARP request

Static ARP Doesn’t Help

```
C:\>arp -s 10.85.139.1 00-00-0c-07-ac-01       <====== Setting the static Entry
C:\>arp -a

Interface: 10.85.139.33 on Interface 0x1000004
  Internet Address      Physical Address      Type
  10.85.139.1           00-00-0c-07-ac-01     static            <===========  MAC is the real one of the router

C:\>arp -a

Interface: 10.85.139.33 on Interface 0x1000004
  Internet Address      Physical Address      Type
  10.85.139.1           00-d0-59-bc-0c-ad     static       <========= The static has been changed by Hacker
  10.85.139.2           00-d0-59-bc-0c-ad     dynamic
  10.85.139.3           00-d0-59-bc-0c-ad     dynamic

C:\>arp -a

Interface: 10.85.139.33 on Interface 0x1000004
  Internet Address      Physical Address      Type
  10.85.139.1           00-00-0c-07-ac-01     static                <======== Hacker is gone
  10.85.139.2           00-05-5f-08-a8-0a     dynamic
```

Selective Sniffing

- Once the dsniff box has started the arpspoof process, the magic begins:

```
[root@hacker-lnx dsniff-2.3]# ./dsniff -c
dsniff: listening on eth0
-----------------
07/17/01 10:09:48 tcp 15.1.1.26.1126 -> wwwin-abc.cisco.com.80 (http)
GET /SERVICE/Paging/page/ HTTP/1.1
Host: wwwin-abc.cisco.com
Authorization: Basic c2NvdlghV9UNMRH4lejDmaA== [myuser:mypassword]
```

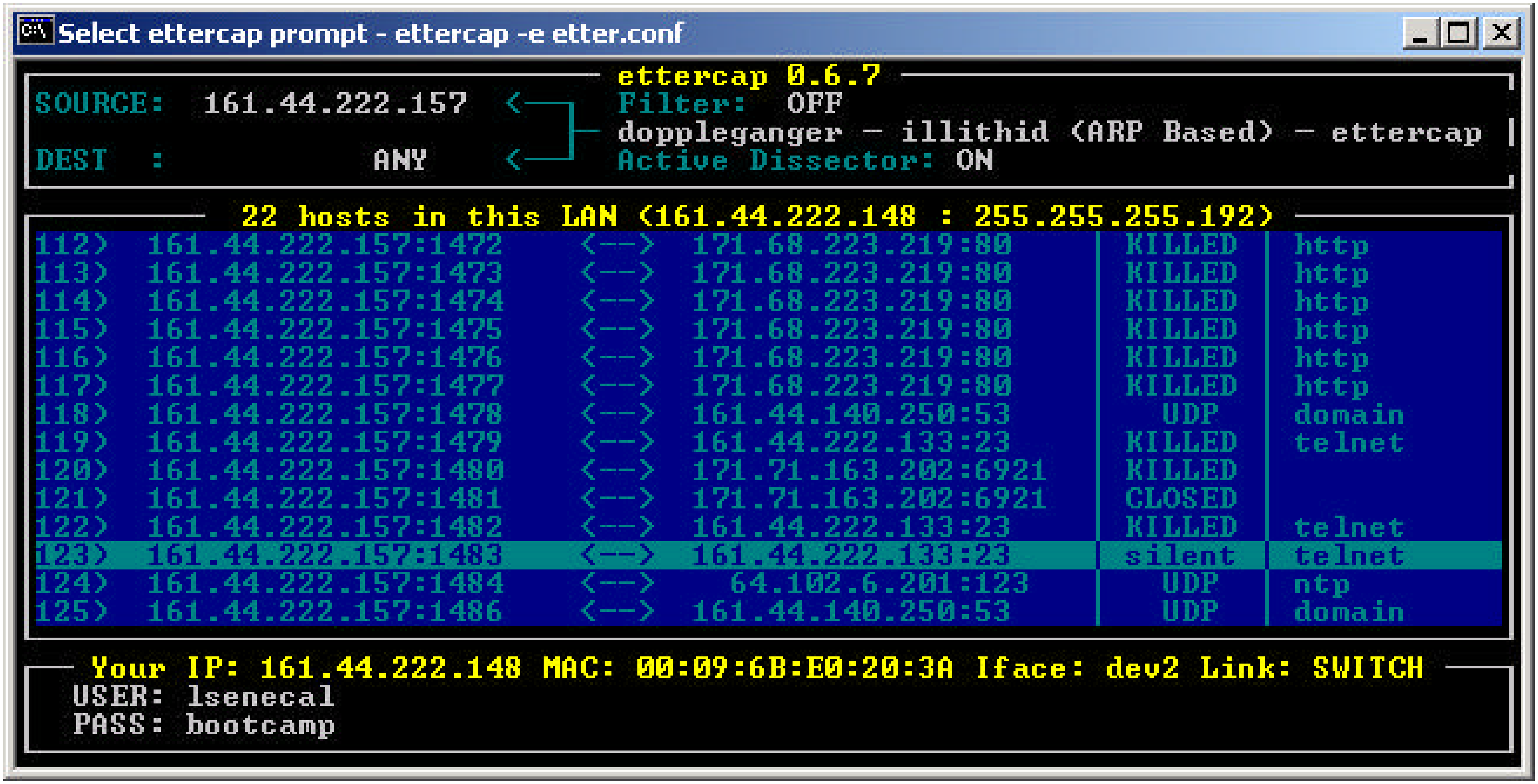
Supports More than 30 Standardized/Proprietary Protocols:

FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL

New Toy in Town: Ettercap

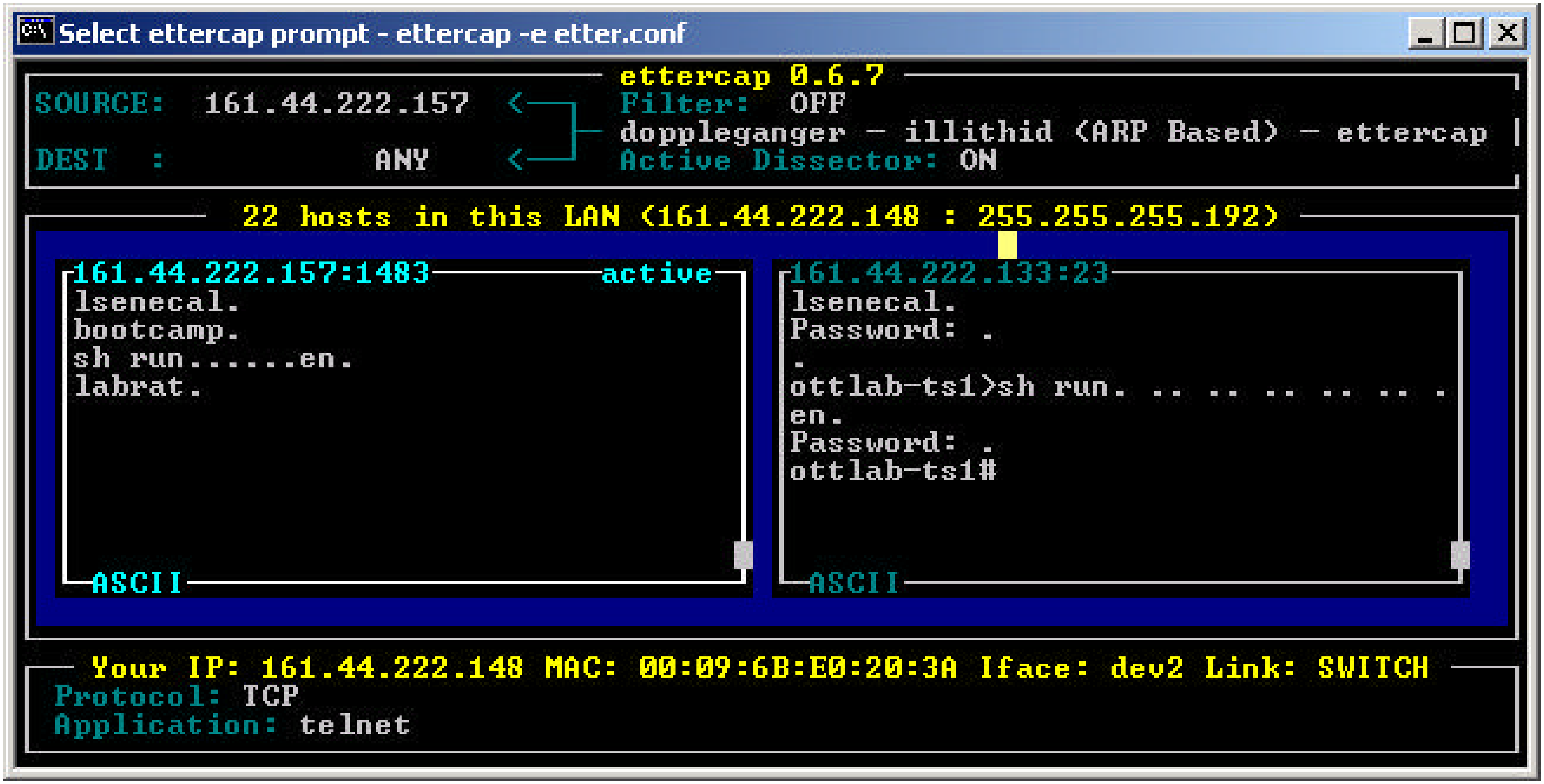
- Similar to dsniff though not as many protocols supported for sniffing
- Can ARP spoof both sides of a session to achieve full-duplex sniffing
- Allows command insertion into persistent TCP sessions
- Menu driven interface
- http://ettercap.sourceforge.net

Can It Get Much Easier?



```
                                        ettercap 0.6.7
SOURCE:  161.44.222.157   <--+          Filter:  OFF
                             |--        doppleganger - illithid (ARP Based) - ettercap
DEST  :             ANY   <--+          Active Dissector: ON

            22 hosts in this LAN (161.44.222.148 : 255.255.255.192)
112)  161.44.222.157:1472    <-->  171.68.223.219:80     | KILLED | http
113)  161.44.222.157:1473    <-->  171.68.223.219:80     | KILLED | http
114)  161.44.222.157:1474    <-->  171.68.223.219:80     | KILLED | http
115)  161.44.222.157:1475    <-->  171.68.223.219:80     | KILLED | http
116)  161.44.222.157:1476    <-->  171.68.223.219:80     | KILLED | http
117)  161.44.222.157:1477    <-->  171.68.223.219:80     | KILLED | http
118)  161.44.222.157:1478    <-->  161.44.140.250:53     |   UDP  | domain
119)  161.44.222.157:1479    <-->  161.44.222.133:23     | KILLED | telnet
120)  161.44.222.157:1480    <-->  171.71.163.202:6921   | KILLED |
121)  161.44.222.157:1481    <-->  171.71.163.202:6921   | CLOSED |
122)  161.44.222.157:1482    <-->  161.44.222.133:23     | KILLED | telnet
123)  161.44.222.157:1483    <-->  161.44.222.133:23     | silent | telnet
124)  161.44.222.157:1484    <-->    64.102.6.201:123    |   UDP  | ntp
125)  161.44.222.157:1486    <-->  161.44.140.250:53     |   UDP  | domain

  Your IP: 161.44.222.148 MAC: 00:09:6B:E0:20:3A Iface: dev2 Link: SWITCH
  USER: lsenecal
  PASS: bootcamp
```

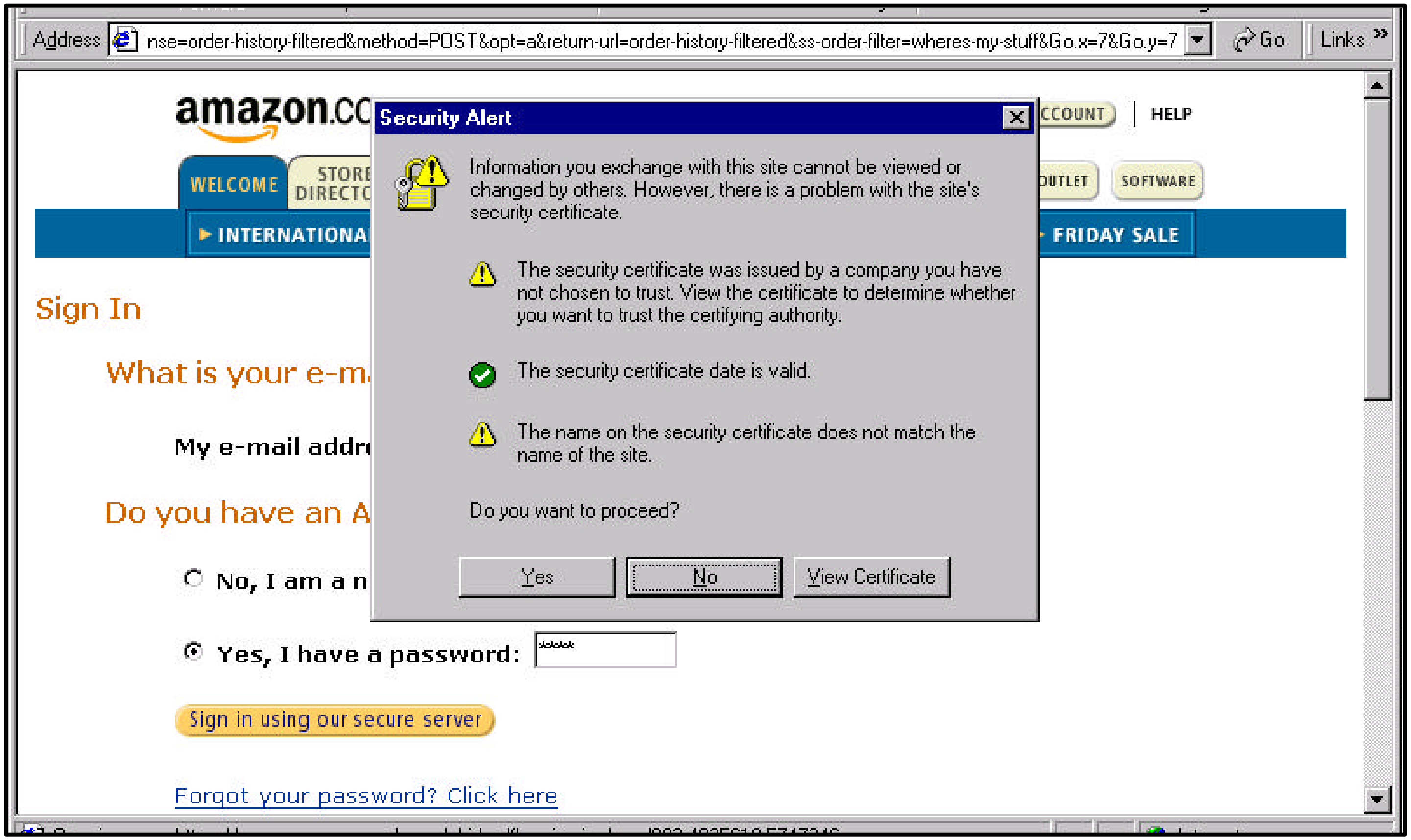
Password and Username



```
SOURCE:  161.44.222.157  <┐   ettercap 0.6.7
                           │   Filter:  OFF
                           ├─ doppleganger - illithid (ARP Based) - ettercap
DEST   :             ANY  <┘   Active Dissector: ON

     22 hosts in this LAN (161.44.222.148 : 255.255.255.192)

161.44.222.157:1483          active     161.44.222.133:23
lsenecal.                               lsenecal.
bootcamp.                               Password: .
sh run......en.                         .
labrat.                                 ottlab-ts1>sh run. .. .. .. .. .. .
                                        en.
                                        Password: .
                                        ottlab-ts1#

  ASCII                                   ASCII

Your IP: 161.44.222.148 MAC: 00:09:6B:E0:20:3A Iface: dev2 Link: SWITCH
Protocol: TCP
Application: telnet
```

SSL/SSH Interception

- Using Ettercap/Dsniff (webmitm) most SSL sessions can be intercepted and bogus certificate credentials can be presented



Address
nse=order-history-filtered&method=POST&opt=a&return-url=order-history-filtered&ss-order-filter=wheres-my-stuff&Go.x=7&Go.y=7
Go
Links
amazon.co
WELCOME
STORE DIRECTO
CCOUNT
HELP
OUTLET
SOFTWARE
INTERNATIONA
FRIDAY SALE
Sign In
What is your e-m
My e-mail addr
Do you have an A
No, I am a n
Yes, I have a password:
Sign in using our secure server
Forgot your password? Click here

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

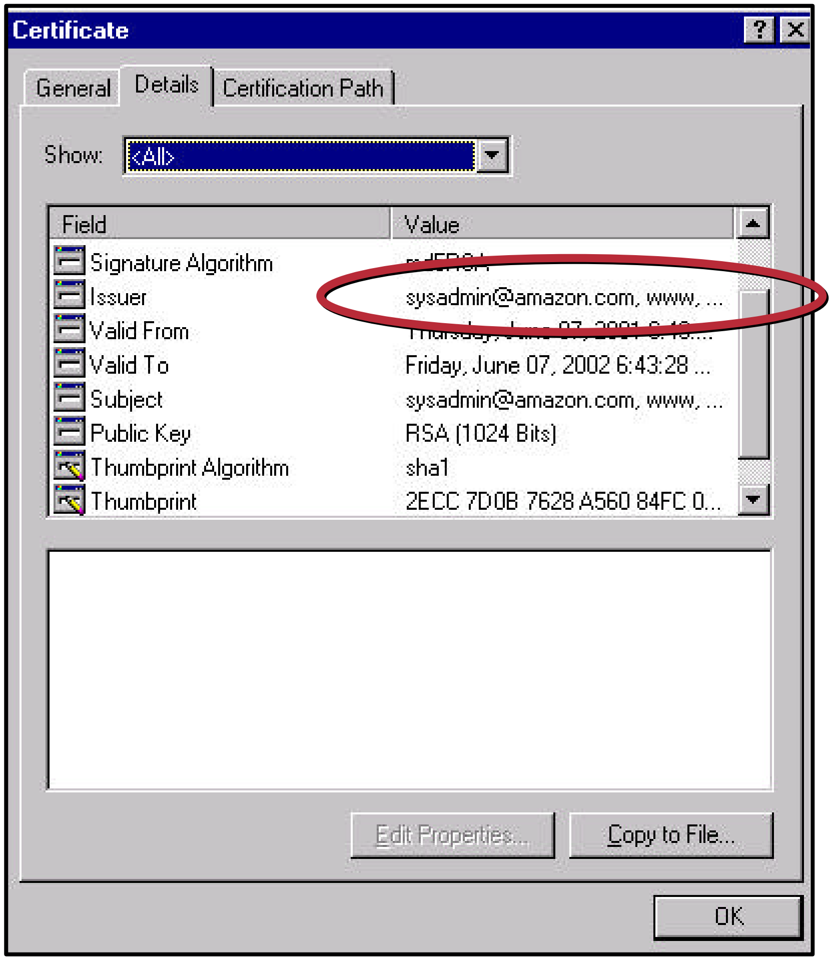
✓ The security certificate date is valid.

⚠ The name on the security certificate does not match the name of the site.

Do you want to proceed?

SSL/SSH Interception

- **Upon inspection they will look invalid but they would likely fool most users**



Show: <All>

Field	Value
Signature Algorithm	md5RSA
Issuer	sysadmin@amazon.com, www, ...
Valid From	Thursday, June 07, 2001 6:43:...
Valid To	Friday, June 07, 2002 6:43:28 ...
Subject	sysadmin@amazon.com, www, ...
Public Key	RSA (1024 Bits)
Thumbprint Algorithm	sha1
Thumbprint	2ECC 7D0B 7628 A560 84FC 0...

invalid

ARP Spoof Mitigation: Private VLANs

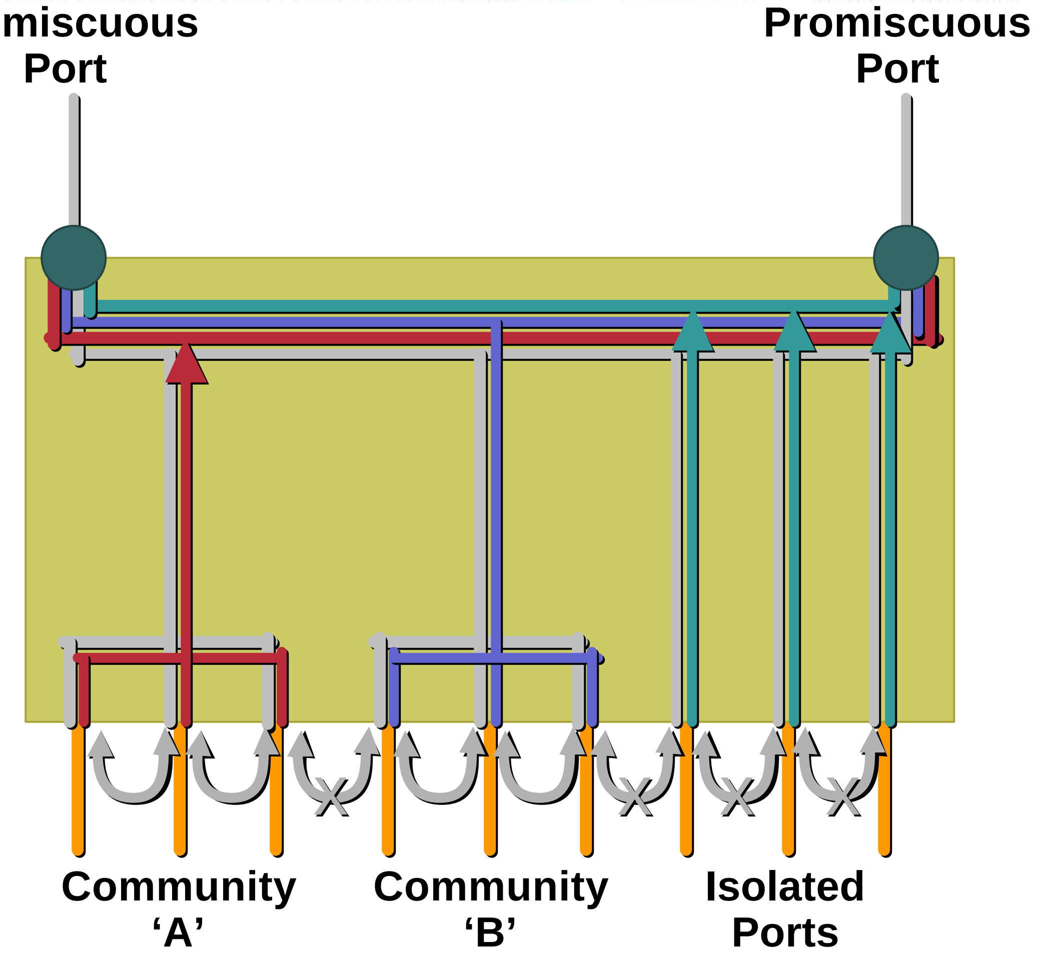
Only One Subnet!

⬜ Primary VLAN

🟥 Community VLAN

🟦 Community VLAN

🟩 Isolated VLAN



- **PVLANs isolate traffic in specific communities to create distinct "networks" within a normal VLAN**
- **Note: Most inter-host communication is disabled with PVLANs turned on**

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_7_1/conf_gd/vlans.htm#xtocid854519

All PVLANs Are Not Created Equal

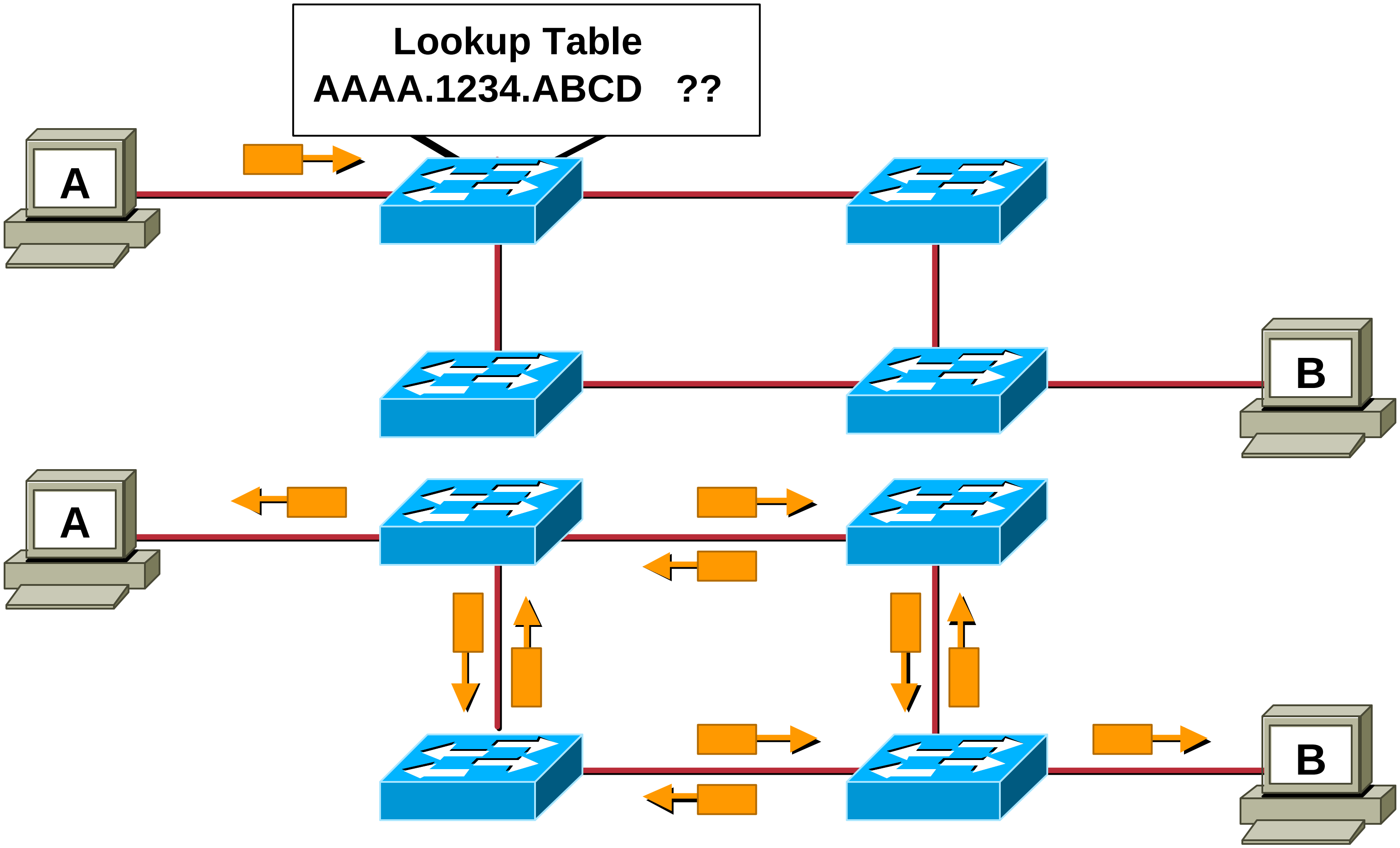
- On CAT 4K, 6K they are called Private VLANs
- On CAT 2K, 3K they are called Private VLAN edge or port protected
- CAT 4K,6K PVLANs support the following exclusive features:
    - Sticky ARP to mitigate default gateway attacks
        - ARP Entries do not age out
        - Changing ARP bindings requires manual intervention
    - PVLANs spanning multiple switches
    - Community Ports
- PVLANs are only compatible with Port Security on Cat 4K and 6K

Spanning Tree Attacks

Spanning Tree

- **Purpose: To maintain loop-free topologies in a redundant Layer 2 infrastructure**
- **Provides path recovery services**
- **Hackers are just starting to play around with STP; the “dsniff” of STP attacks has yet to be released**

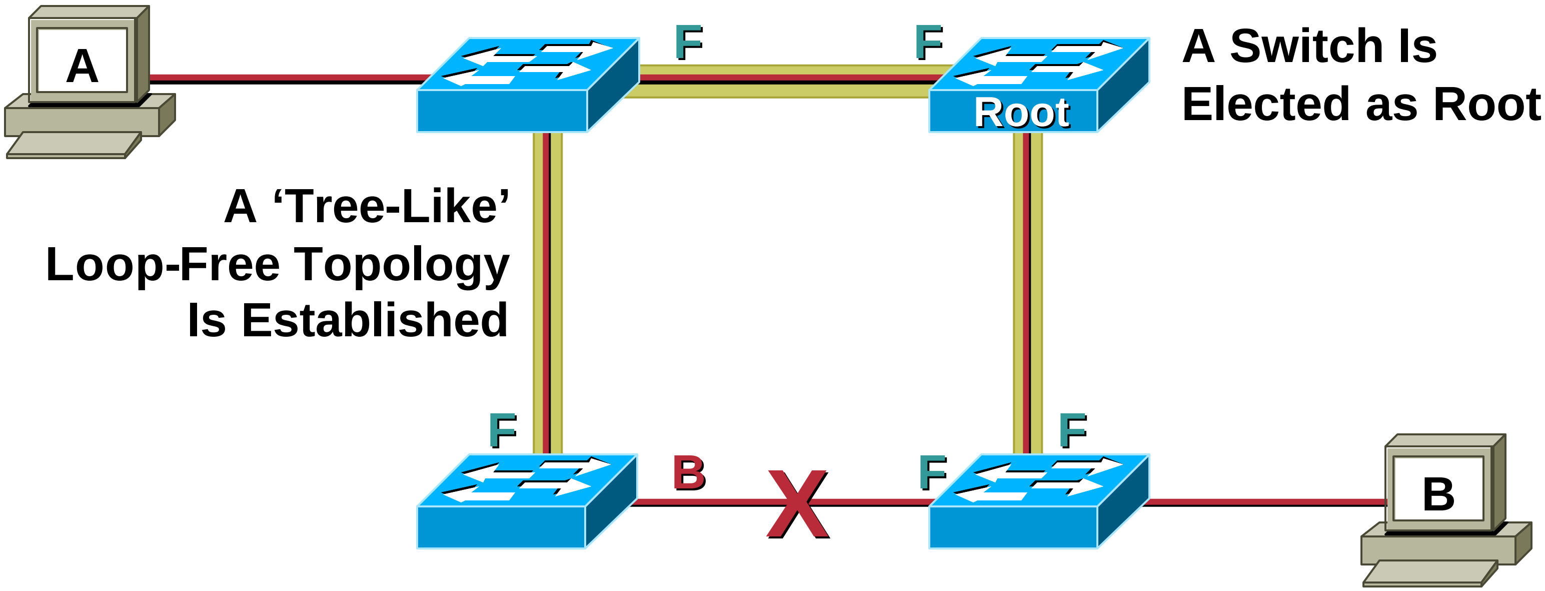
What Happens without Spanning Tree



Lookup Table
AAAA.1234.ABCD ??

Broadcasts Would Become Storms

Spanning Tree Basics



A Switch Is Elected as Root

A ‘Tree-Like’ Loop-Free Topology Is Established

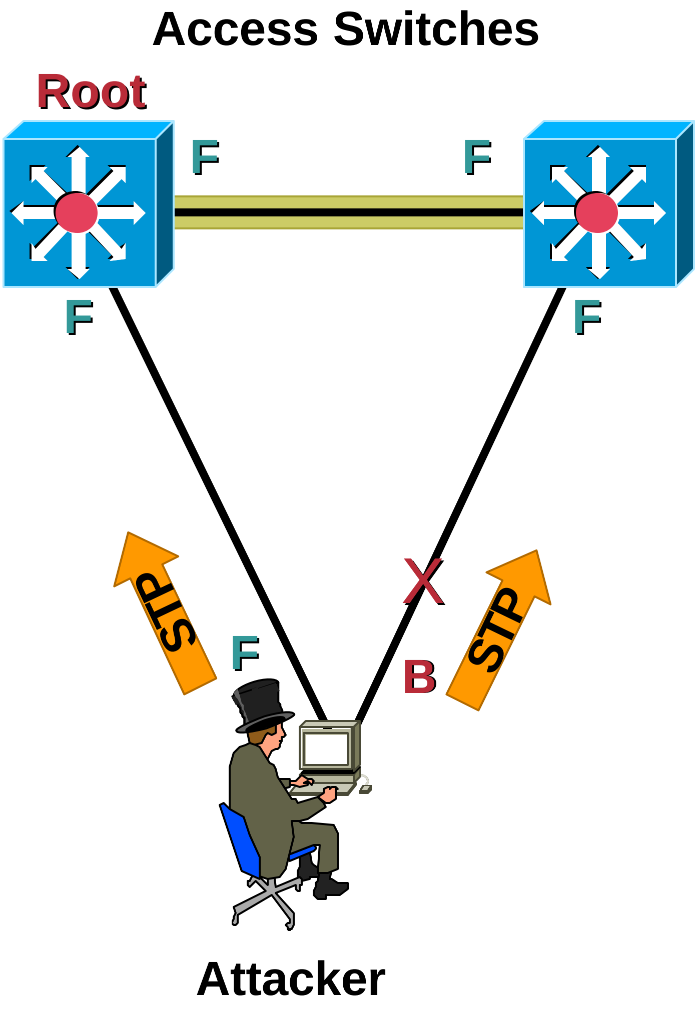
Loop-Free Connectivity

Spanning Tree Attack Example 1/2

- Send BPDU messages from attacker to force spanning tree recalculations

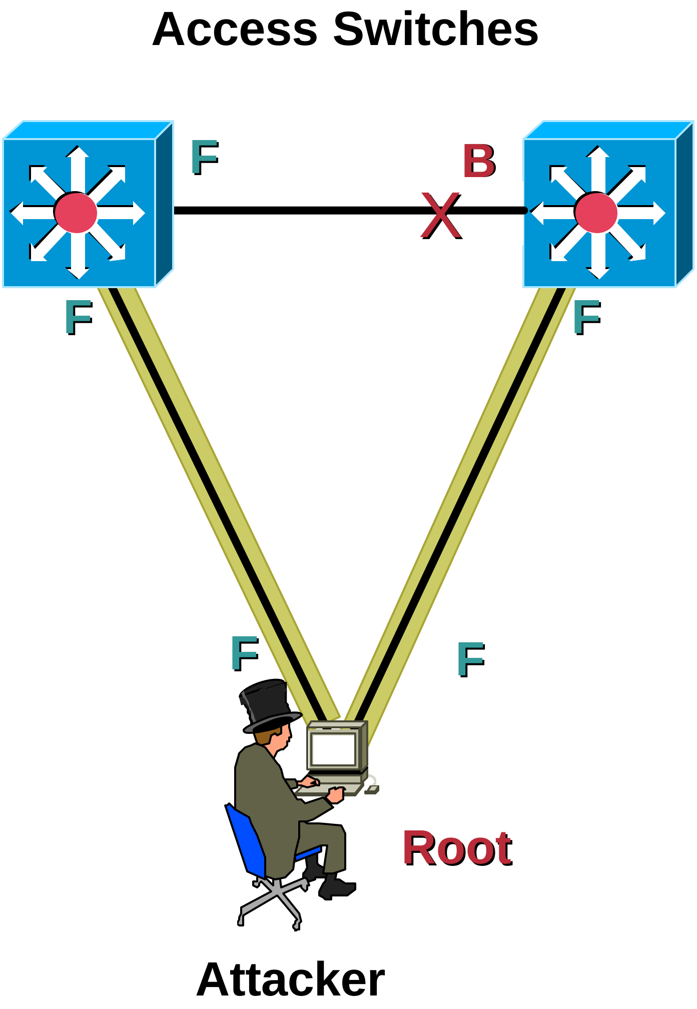
    Impact likely to be DoS

- Send BPDU messages to become root bridge



Spanning Tree Attack Example 2/2

- **Send BPDU messages from attacker to force spanning tree recalculations**
  - **Impact likely to be DoS**
- **Send BPDU messages to become root bridge**
  - **The hacker then sees frames he shouldn't**
    - **MITM, DoS, etc. all possible**
    - **Any attack is very sensitive to the original topology, trunking, PVST, etc.**
    - **Requires attacker to be dual homed to two different switches**



Spanning Tree DoS Example

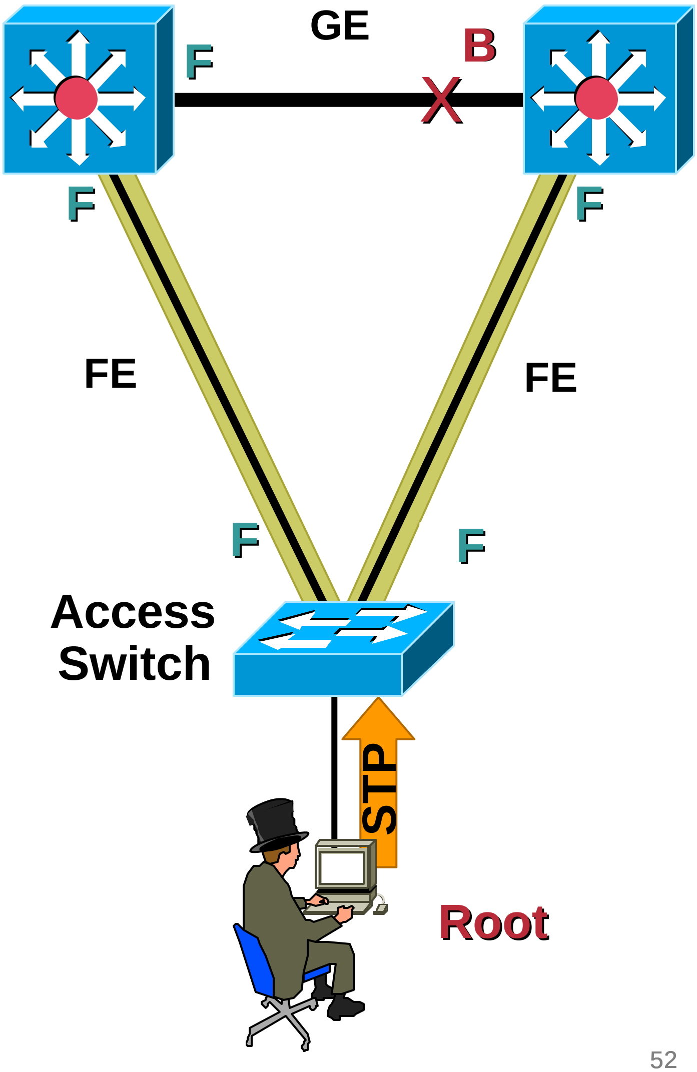
- **Attacker sends BPDU advertising itself with a bridge priority of zero**

  Attacker becomes root bridge

  Spanning Tree recalculates

  GE backbone becomes FE ☹

  If attack is combined with macof, it could yield more packets available to sniff



STP Attack Mitigation

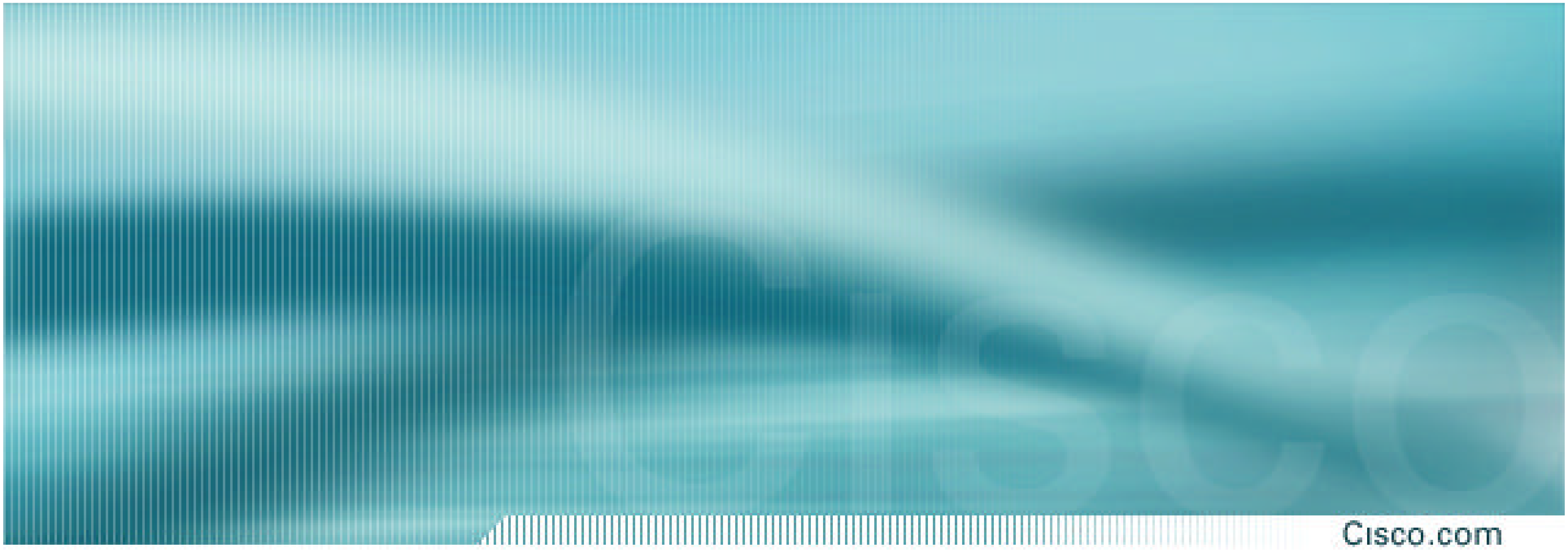
- Disable STP (It is not needed in loop free topologies)
- BPDU Guard
  - Disables ports using portfast upon detection of a BPDU message on the port
  - Globally enabled on all ports running portfast
  - Available in CatOS 5.4.1 for Cat 2K, 4K, 5K, and 6K; 12.0XE for native IOS 6K; 12.1(8a)EW for 4K Sup III; 12.1(4)EA1 for 3550; 12.1(6)EA2 for 2950

```
CatOS> (enable)set spantree portfast bpdu-guard enable

IOS(config)#spanning-tree portfast bpduguard
```

- Root Guard
  - Disables ports who would become the root bridge due to their BPDU advertisement
  - Configured on a per port basis
  - Available in CatOS 6.1.1 for Cat 29XX, 4K, 5K, and 6K; 12.0(7) XE for native IOS 6K, 12.1(8a)EW for 4K Sup III; 29/3500XL in 12.0(5)XU; 3550 in 12.1(4)EA1; 2950 in 12.1(6)EA2

```
CatOS> (enable) set spantree guard root 1/1

IOS(config)#spanning-tree guard root (or rootguard)
```

http://www.cisco.com/warp/public/473/65.pdf



Layer 2 Port Authentication

Dynamic VLAN Access Ports

- VLAN assignment based on MAC address or HTTP Auth (URT) is possible with a VLAN Management Policy Server (VMPS)
- Requires VLAN to MAC database which is downloaded via TFTP to the VMPS server
- VMPS uses VLAN Query Protocol (VQP) which is unauthenticated and runs over UDP
- Can restrict certain VLANs to certain physical ports
- During access violation, switch can send either an "access denied" response or shutdown the port (depends on configuration)
- If a VLAN in the database does not match the current VLAN on the port and active hosts are on the port, VMPS sends an access denied or a port shutdown response (depends on configuration)
- Server and client
  - Available in Cat 29XX, 4K, 5K, and 6K in CatOS 5.2
- Client only
  - Available in 3550 and 2950 in 12.1(4)EA1; 29/3500XL in 11.2(8)SA4

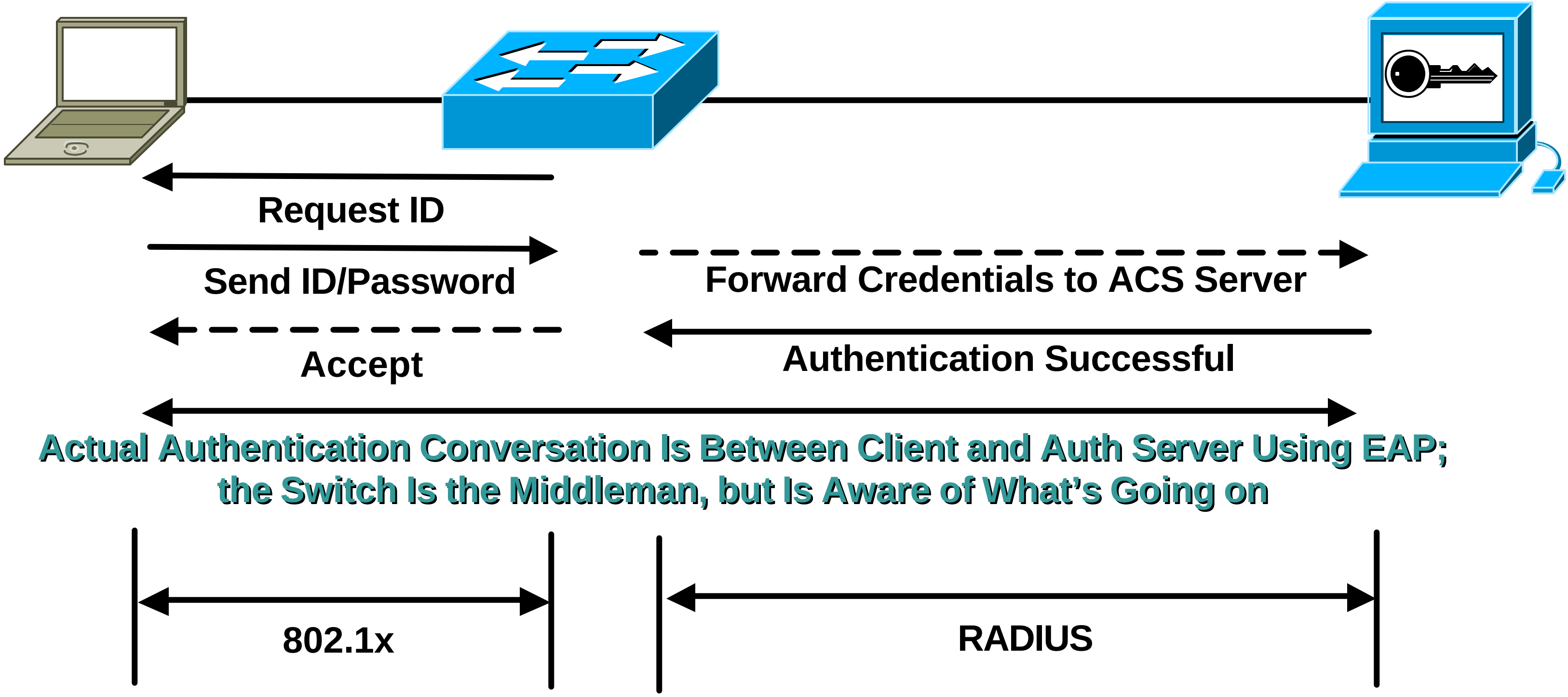
802.1x/EAP Switch Authentication

- **802.1x and EAP (Extensible Authentication Protocol) can authenticate a device before allowing access to a switch and can assign a VLAN after authentication**

  EAP allows different authentication types to use the same format (TLS, MD5, OTP)

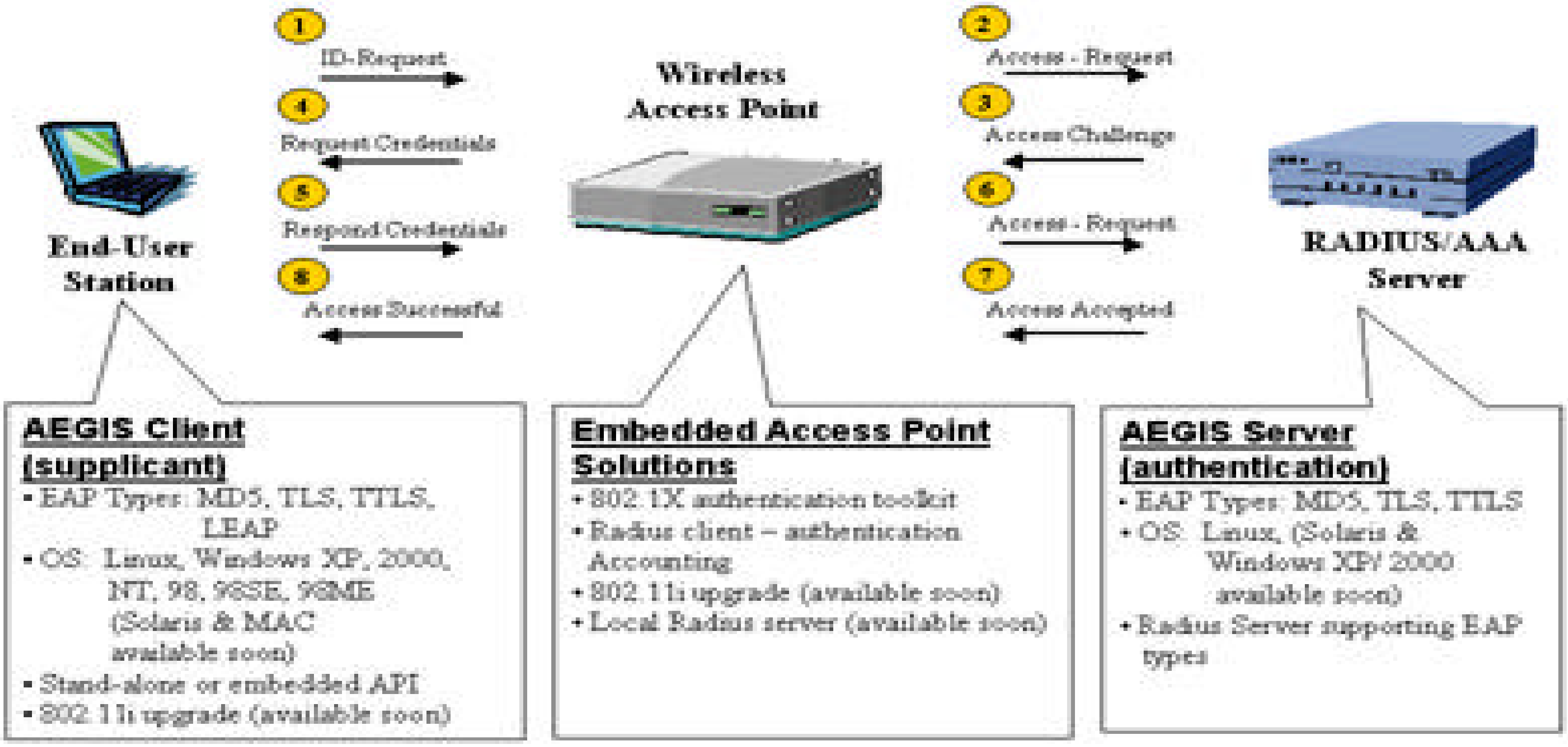
- **Works between the supplicant (client) and the authenticator (network device)**
- **Maintains backend communication to an authentication (RADIUS) server**
- **The authenticator (switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information**
- **Available on Cat 2900,4K,6K in CatOS 6.2; Cat 3550 in 12.1(4)EA1; Cat 2950 in 12.1(6)EA2**

802.1X Port Authentication



Actual Authentication Conversation Is Between Client and Auth Server Using EAP; the Switch Is the Middleman, but Is Aware of What's Going on

Meetinghouse Data Communication 802.1x Client



AEGIS Client (supplicant)

- EAP Types: MD5, TLS, TTLS, LEAP
- OS: Linux, Windows XP, 2000, NT, 98, 98SE, 98ME (Solaris & MAC available soon)
- Stand-alone or embedded API
- 802.11i upgrade (available soon)

Embedded Access Point Solutions

- 802.1X authentication toolkit
- Radius client – authentication Accounting
- 802.11i upgrade (available soon)
- Local Radius server (available soon)

AEGIS Server (authentication)

- EAP Types: MD5, TLS, TTLS
- OS: Linux, (Solaris & Windows XP/ 2000 available soon)
- Radius Server supporting EAP types

http://www.mtghouse.com/products/client/index.shtml

Other Attacks
CDP
HSRP
DHCP Starvation
DNS Spoofing
ETC.

Summary

Layer 2 Security Best Practices 1/2

- 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
- Set all user ports to non trunking
- Deploy port-security where 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

Layer 2 Security Best Practices 2/2

- Enable STP attack mitigation (BPDU Guard, Root Guard)
- 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

Catalyst Switch Feature Support

	Cat 2900 XL	Cat 3500 XL	Cat 2950	Cat 3550	Cat 29XX G	CatOS 4000	CatOS 6000	IOS 4000	IOS 6000
Port Security	X	X	X	X	X	X	X	X	
Private VLANs	X	X	X	X		X	X	X	X
STP BPDU Guard			X	X		X	X	X	X
STP Root Guard	X	X	X	X	X	X	X	X	X
SSH Support			X	X	X	X	X	X	X
VMPS Client	X	X	X	X	X	X	X	X	X
VMPS Server					X	X	X		
802.1X Auth			X	X	X	X	X	X	
Wire Rate ACLs			X	X		X	X	X	X

X:Q1FY03

Lessons Learned

- Still a need for intelligent L2 Switch
- Security ? Price Per Pond L2
- Evaluate your security policy while considering the other issues raised in this session
  - Is there room for improvement?
  - What campus risks are acceptable based on your policy?
- Deploy, where appropriate, L2 security best practices