LAYER 2 ATTACKS & MITIGATION TECHNIQUES

SANOG8 – Karachi
1st August 2006

Yusuf Bhaiji
Cisco Systems

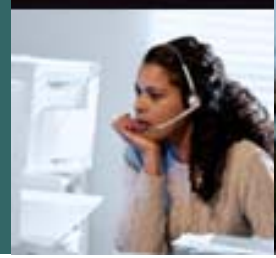
Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - Spanning Tree Attack
  - VLAN “Hopping”
  - MAC Attacks
  - DHCP Attacks
  - ARP Attack
  - Spoofing Attacks
- Summary

Caveats

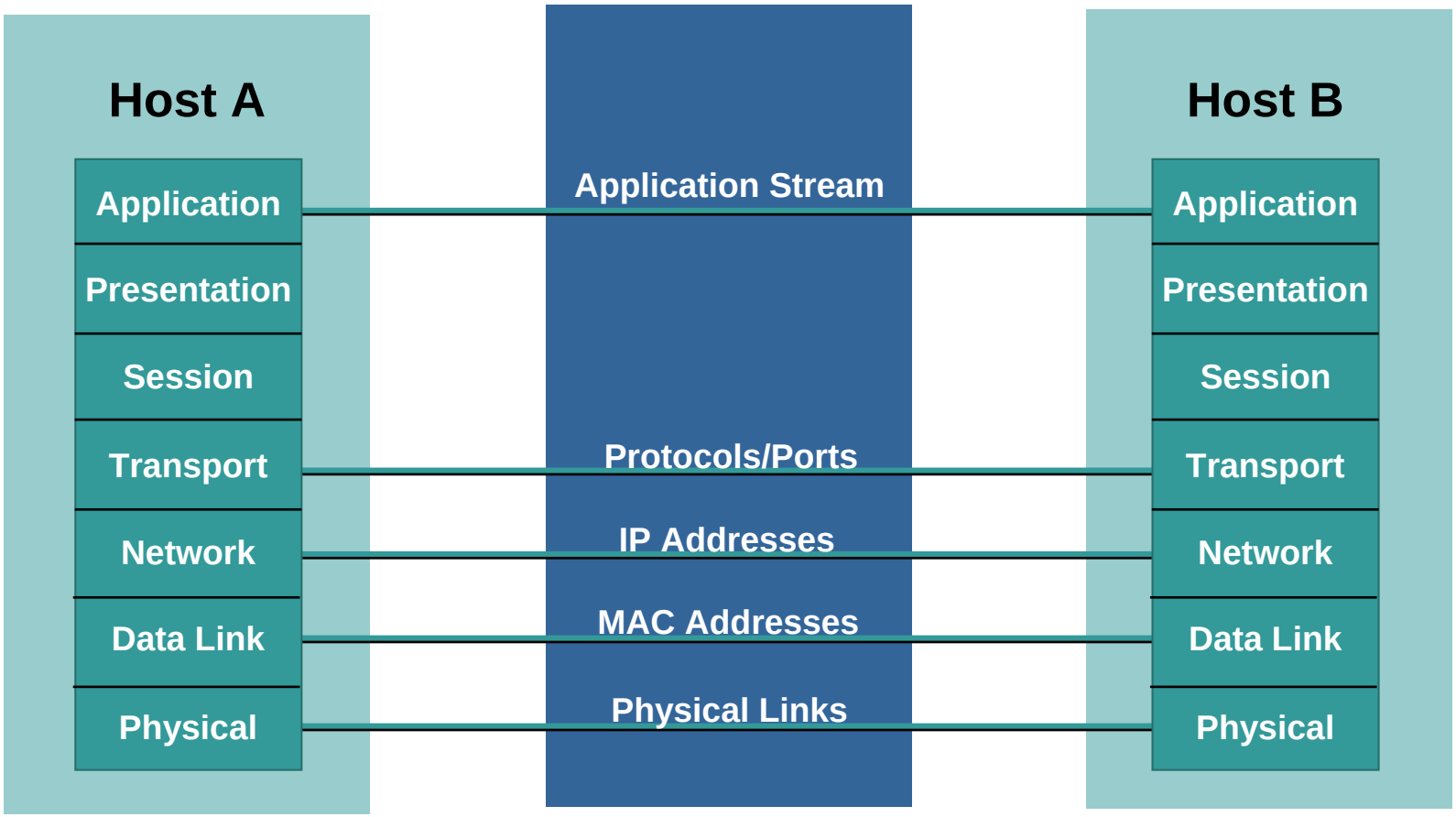
- All attacks and mitigation techniques assume a switched Ethernet network running IP
  - If it is a shared Ethernet access (WLAN, Hub, etc.) most of these attacks get much easier
  - If you are not using Ethernet as your L2 protocol, some of these attacks may not work, but chances are, you are vulnerable to different ones
- New theoretical attacks can move to practical in days
- Ethernet switching attack resilience varies widely from vendor to vendor
- This is not a comprehensive talk on configuring Ethernet switches for security; the focus is mostly access L2 attacks and their mitigation

LAYER 2 ATTACK LANDSCAPE



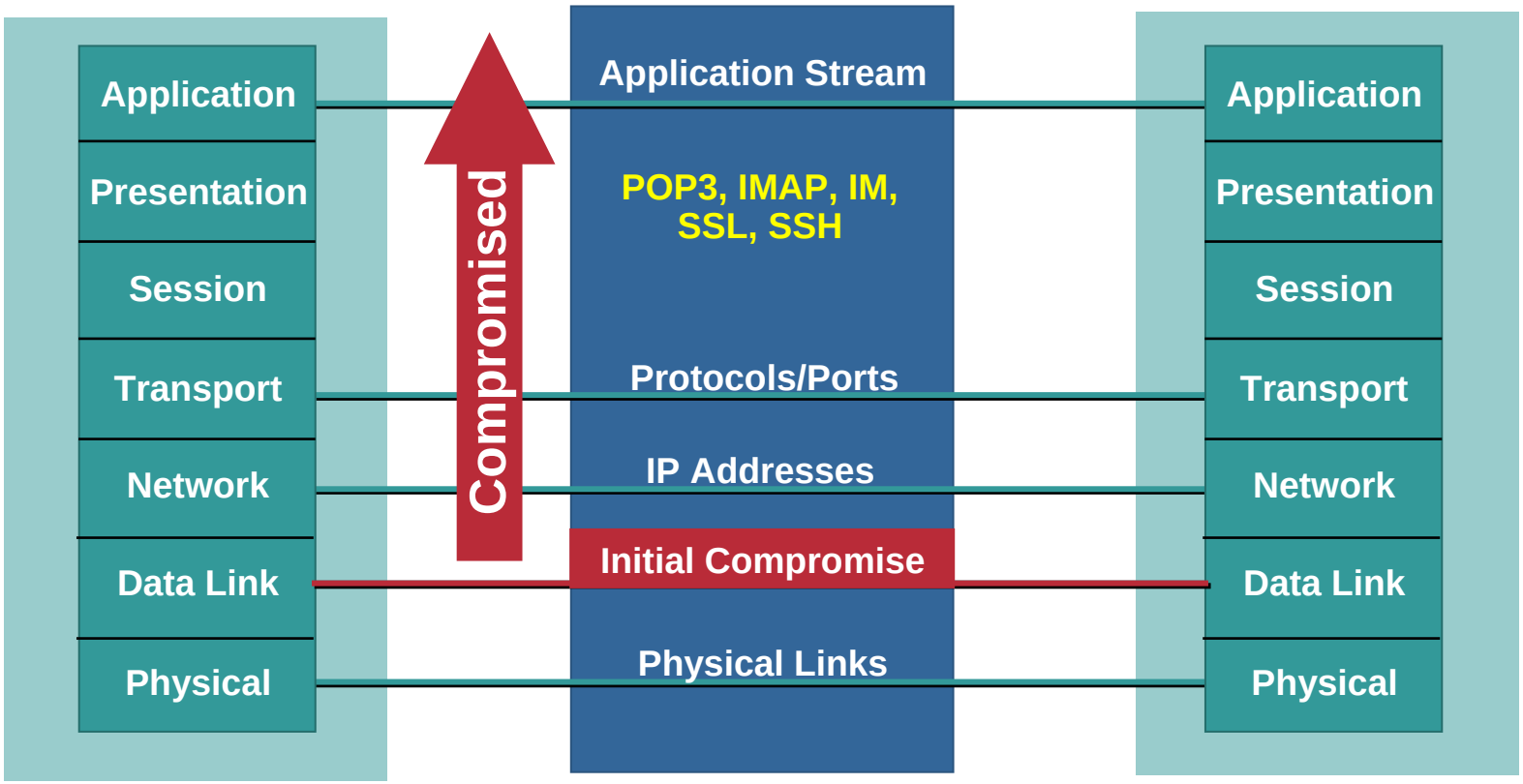
Why Worry About Layer 2 Security?

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



Lower Levels Affect Higher Levels

- 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 the weakest link
- When it comes to networking, layer 2 can be a VERY weak link

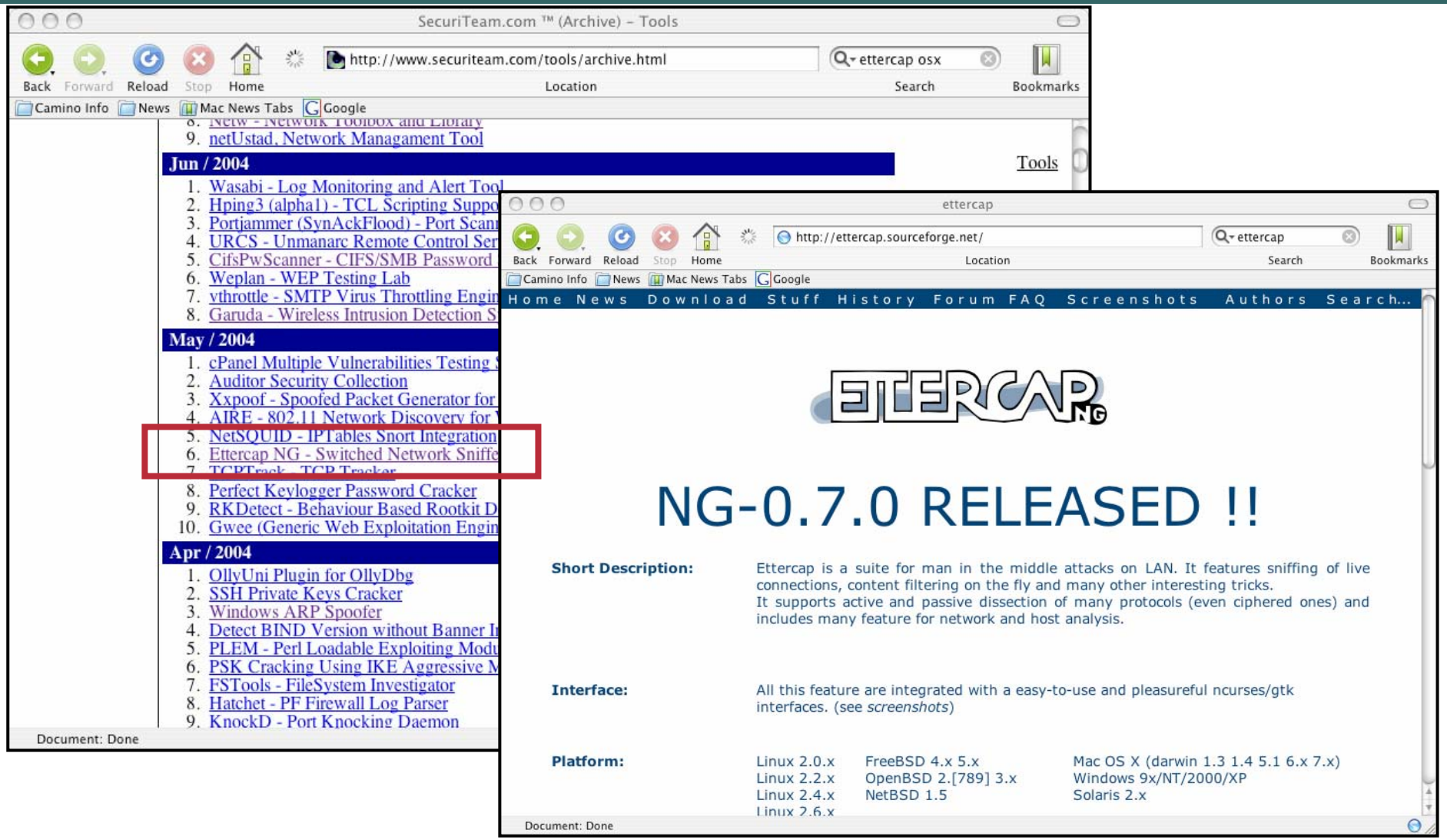


FBI/CSI Risk Assessment*

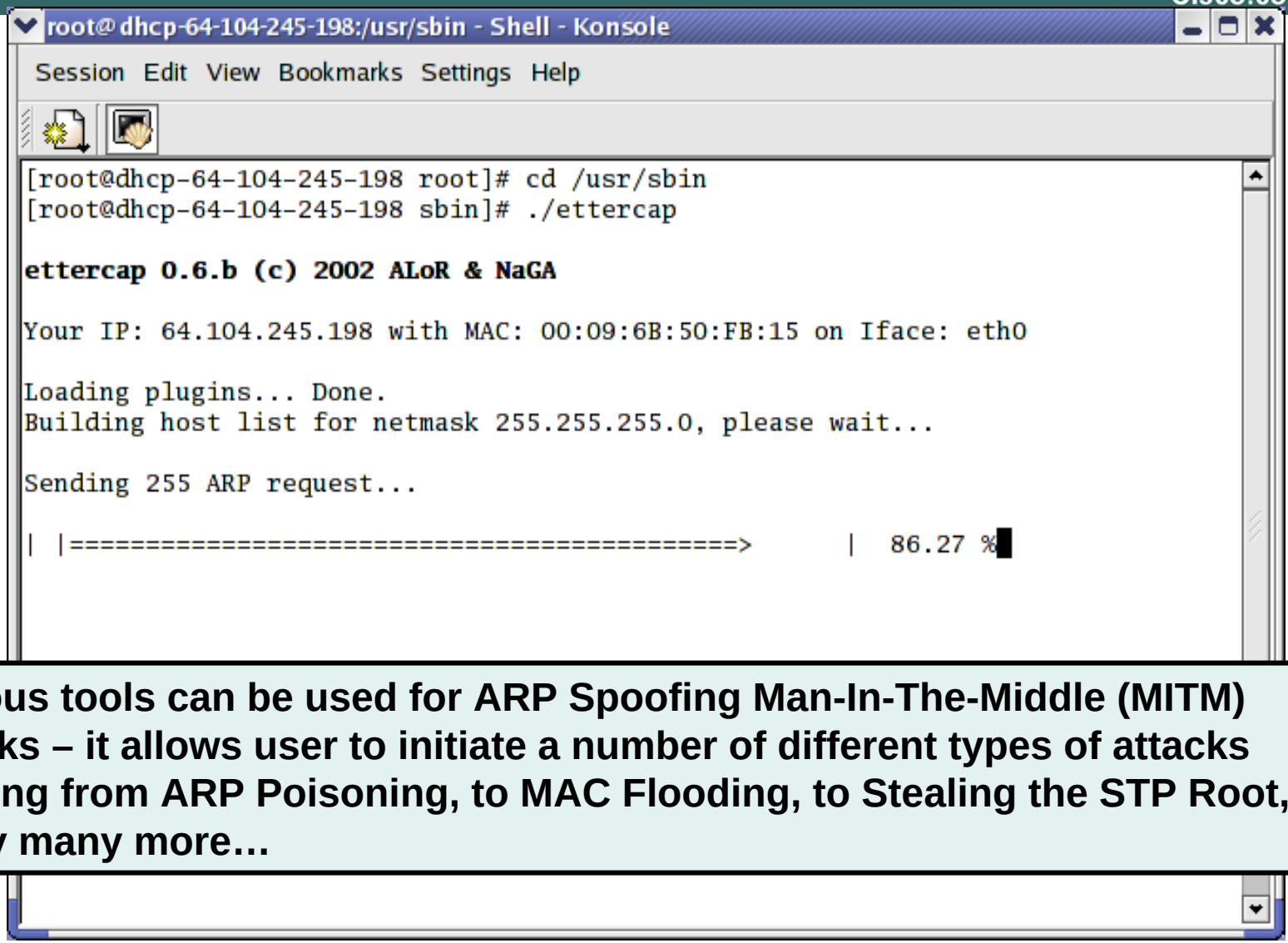
- 99% of all enterprises network ports are OPEN
- Usually any laptop can plug into the network and gain access to the network
- Of companies surveyed total loss was over 141 million
- An average of 11.4 million per incident
- Insider attack by disgruntled employees was listed as likely source by 59% of respondents

*CIS/FBI Computer Crime and Security Survey
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

Layer 2 Attacks
There are lots of tools out there!!!

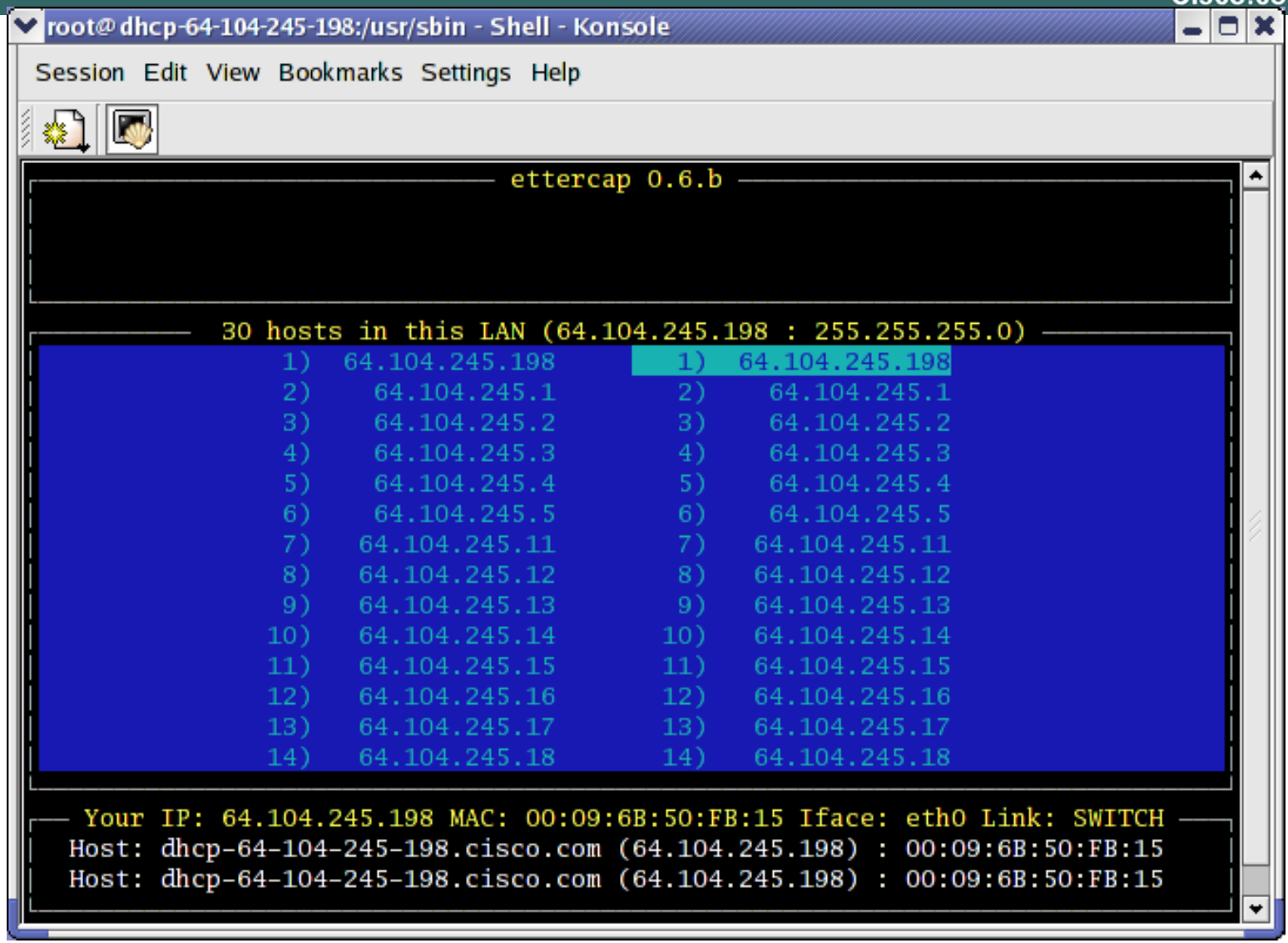


Layer 2 Attacks
ETTERCAP…

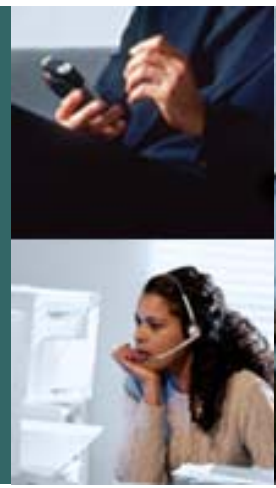


Various tools can be used for ARP Spoofing Man-In-The-Middle (MITM) attacks – it allows user to initiate a number of different types of attacks ranging from ARP Poisoning, to MAC Flooding, to Stealing the STP Root, and many many more…

Layer 2 Attacks
Let the fun begin…



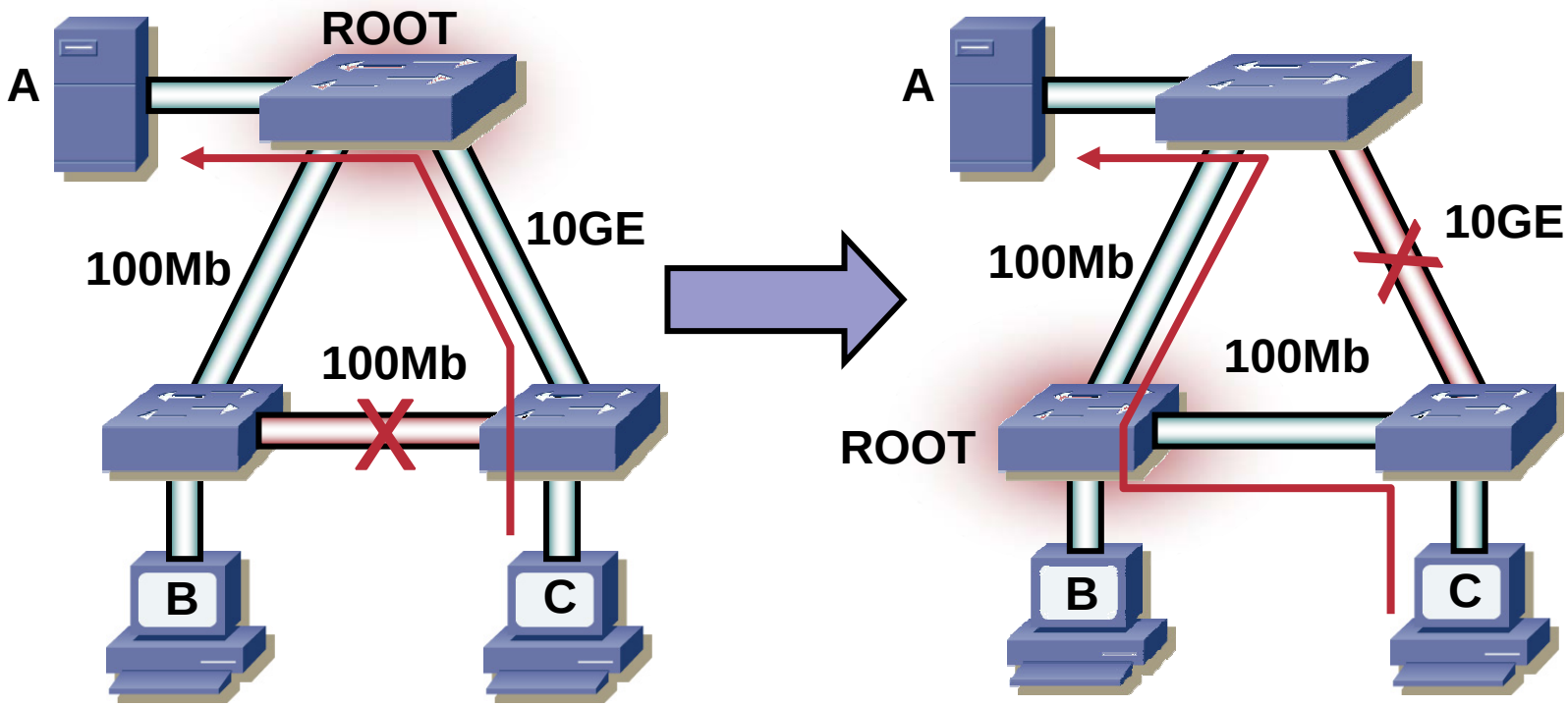
ATTACKS AND COUNTERMEASURES: SPANNING TREE ATTACK



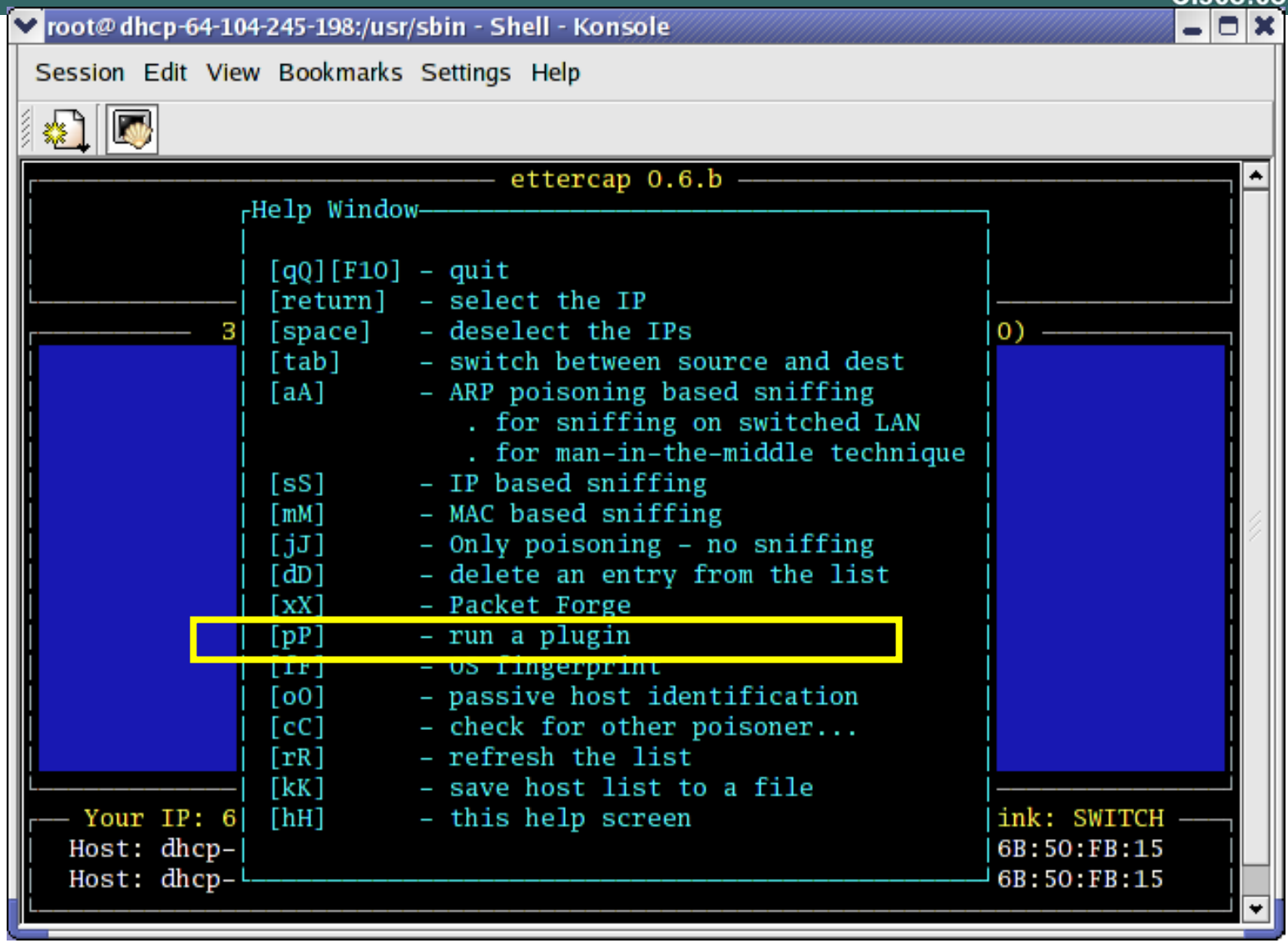
Spanning Tree Attacks

Re-directing traffic while causing disruption…

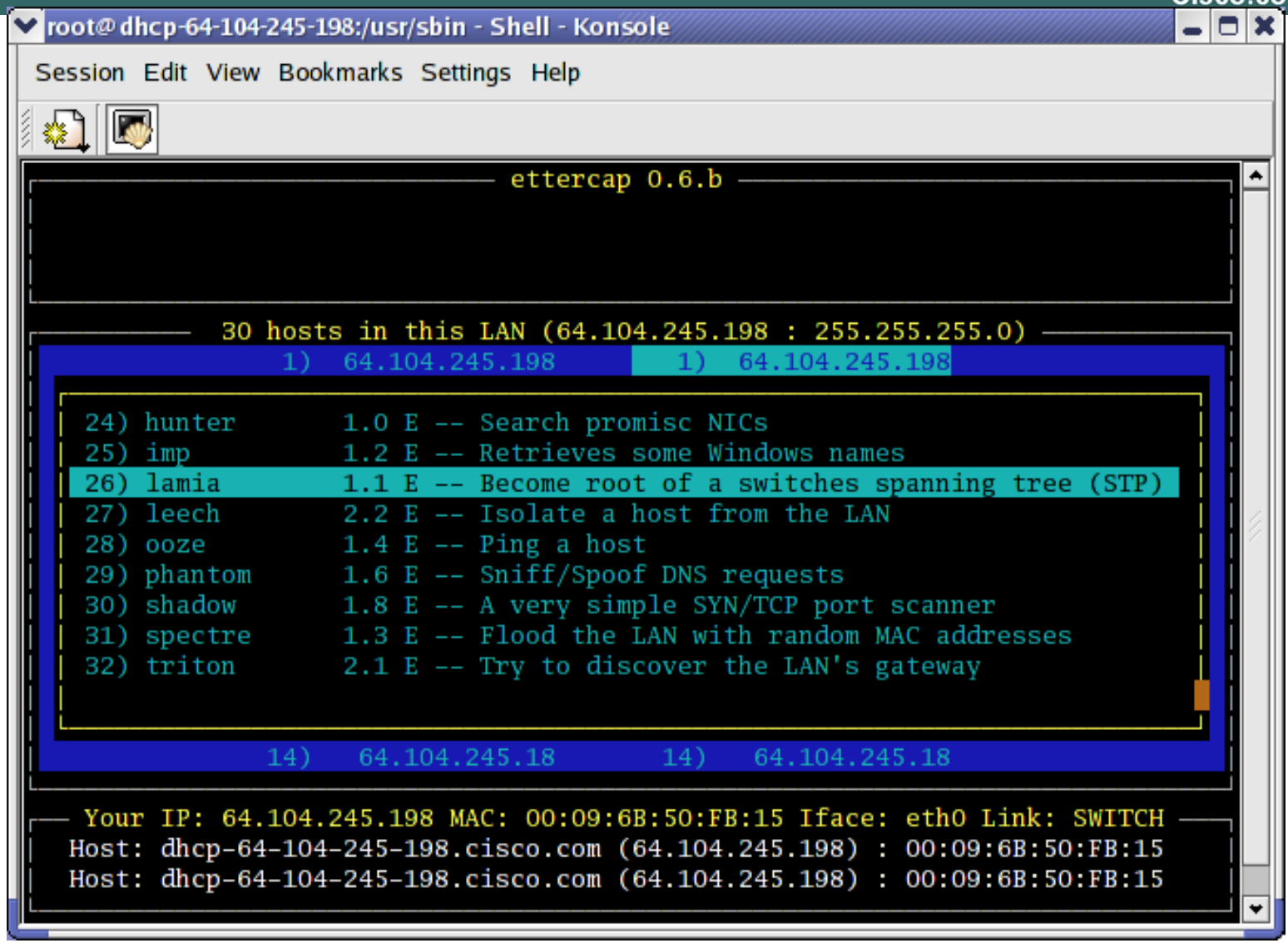
Injecting BPDU packets into the STP domain can cause the entire domain to reconfigure (30-45 second outage) and end up using a less than optimal path for data forwarding – form of Denial of Service attack…



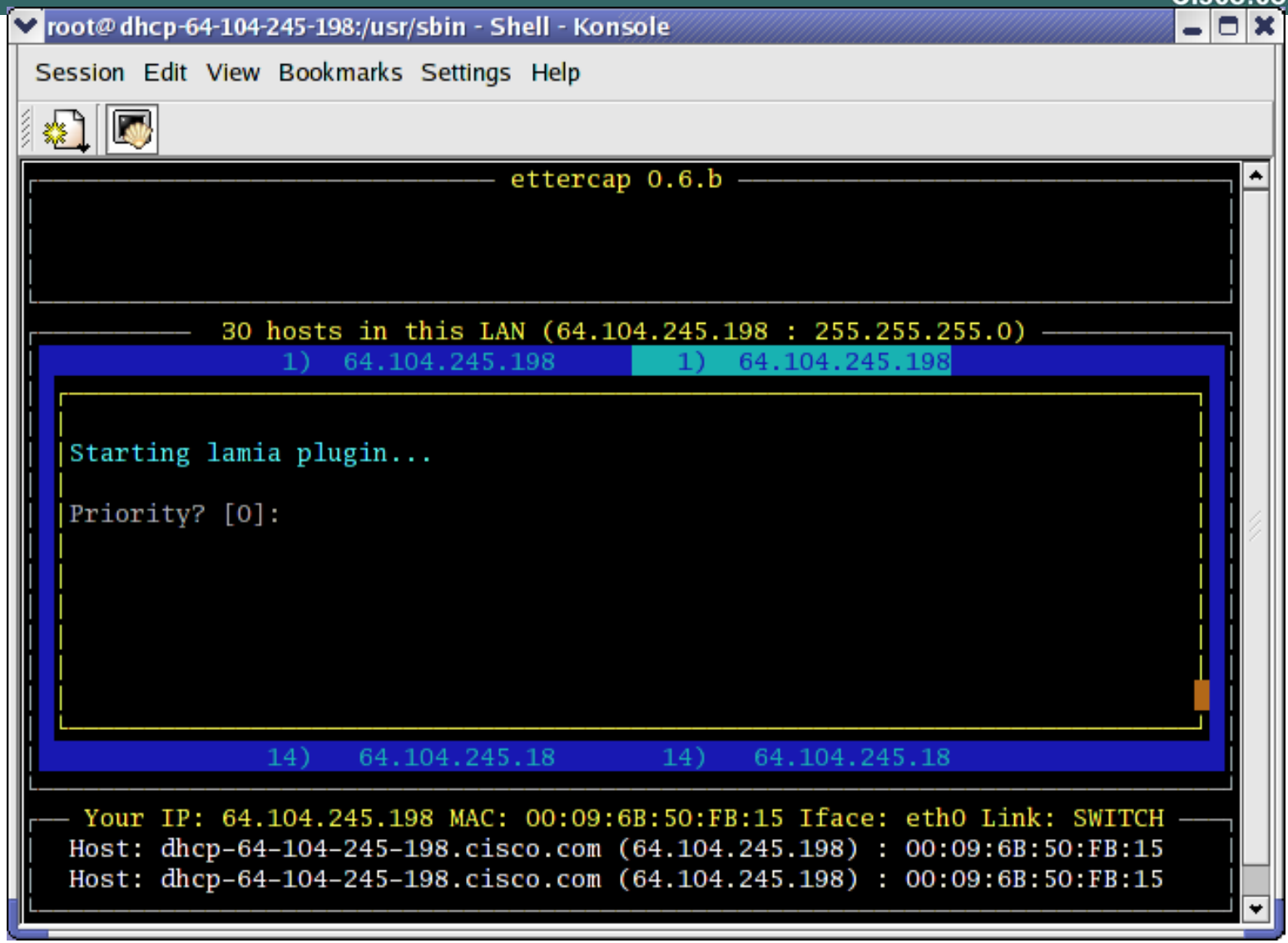
Spanning Tree Attacks
Using Plug-ins…



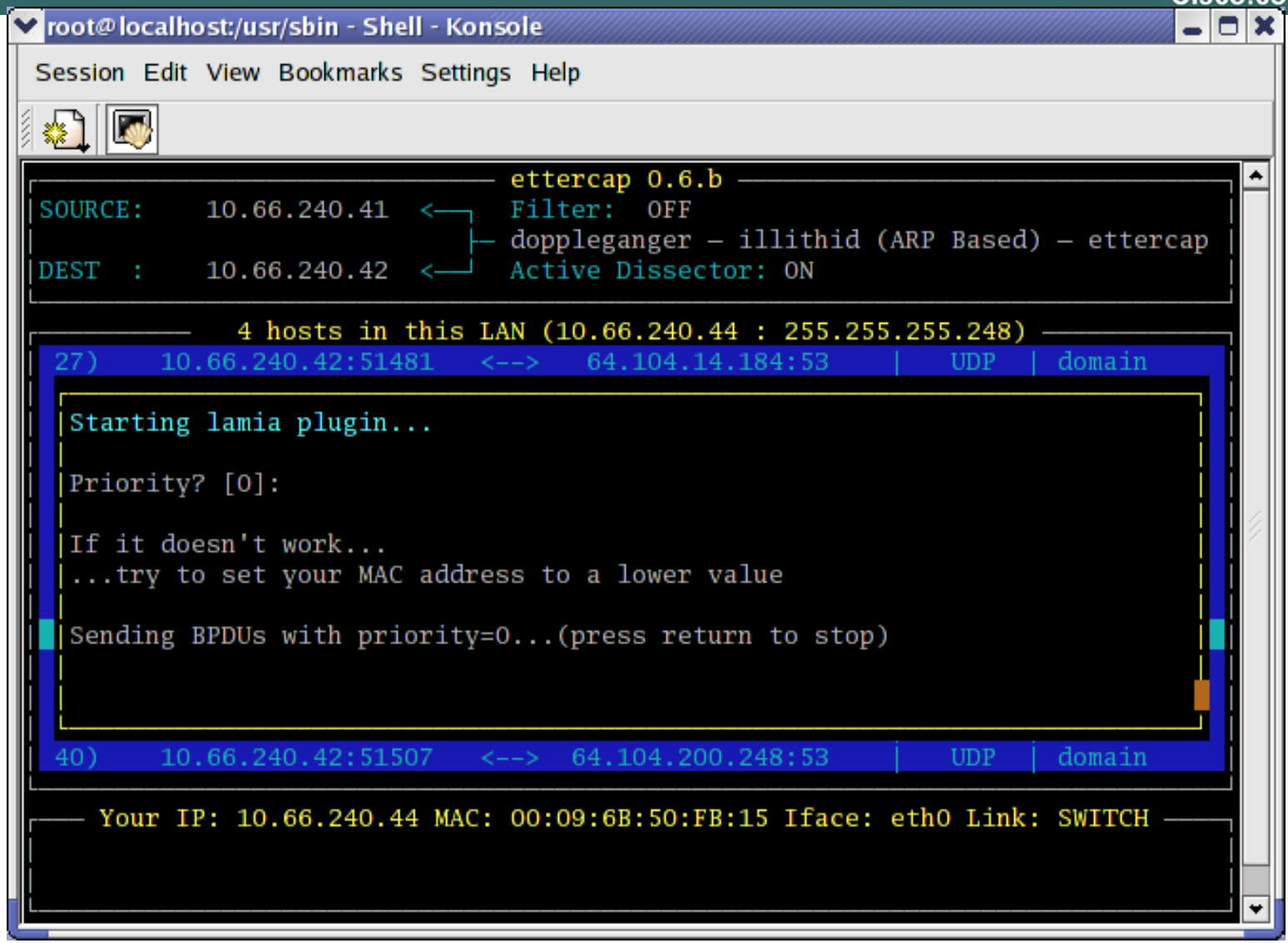
Spanning Tree Attacks
Taking over STP ROOT…



Spanning Tree Attacks
Taking over STP ROOT…



Spanning Tree Attacks
Bingo - you have now become STP Root…

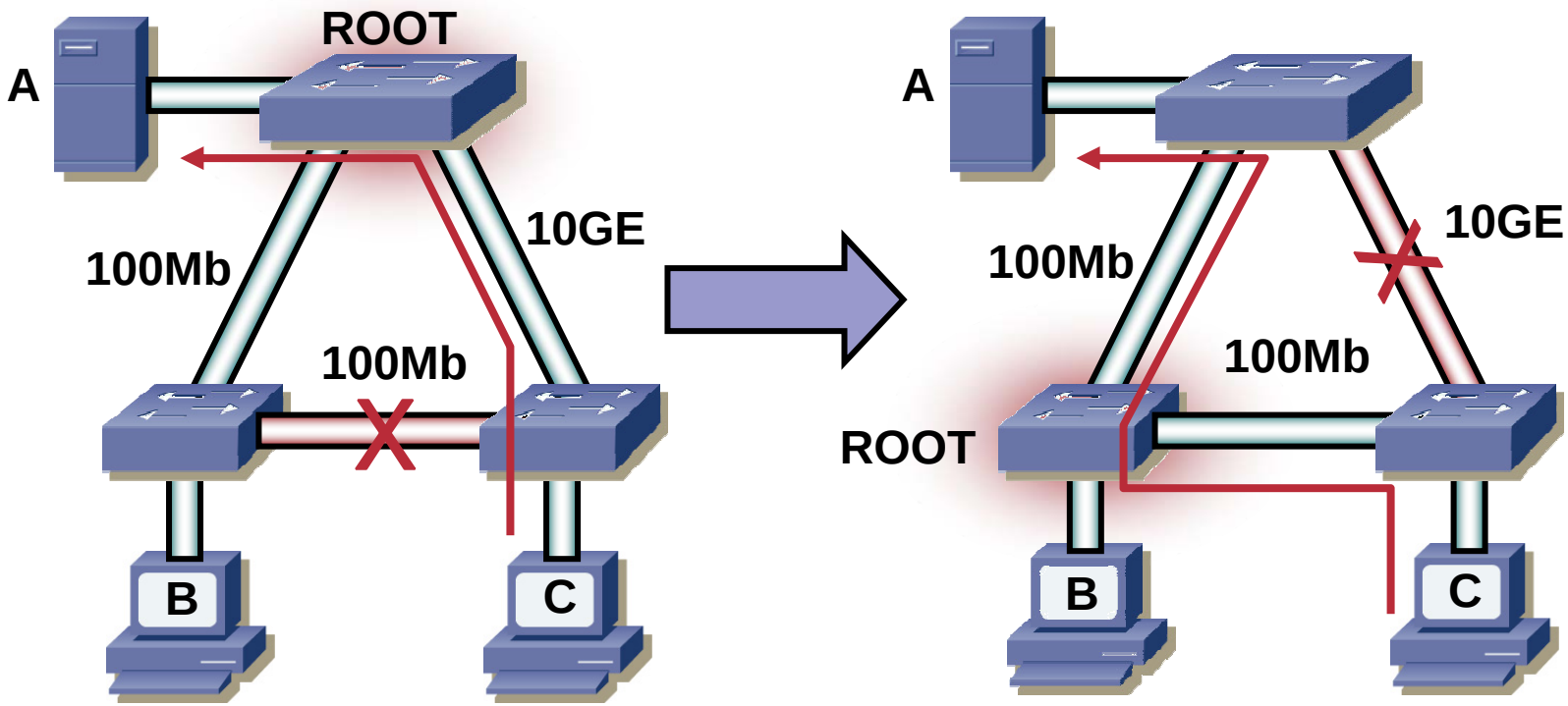


Spanning Tree Attacks

Now traffic is re-directed to you…

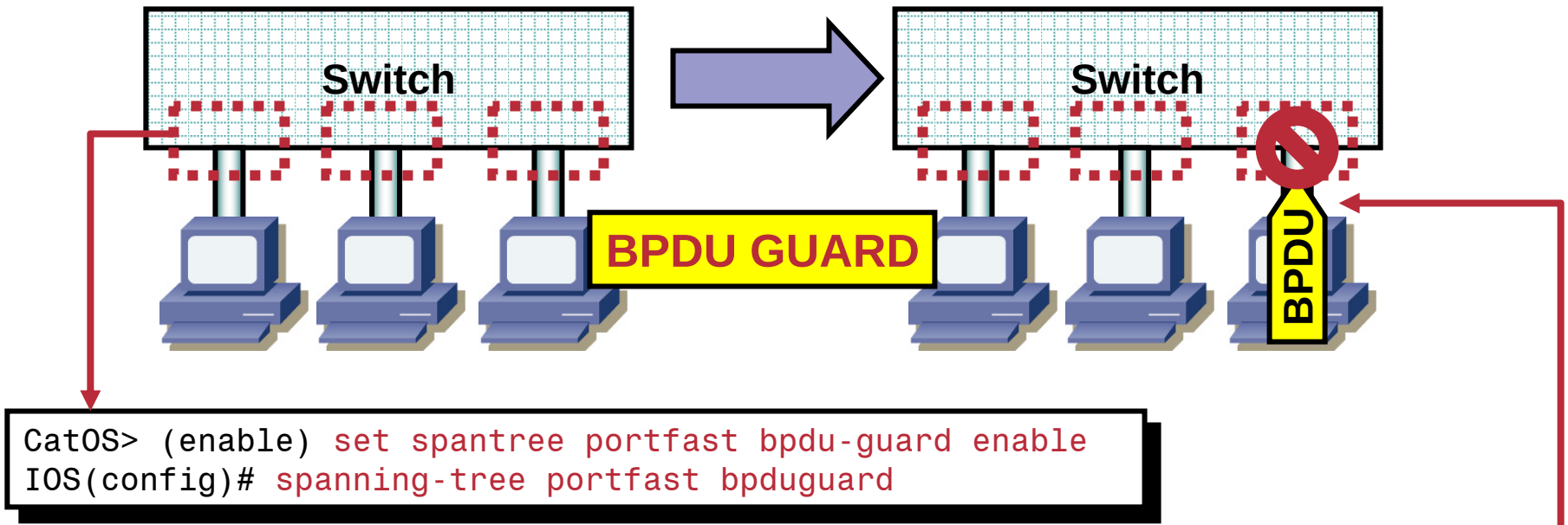
Cisco.com

This attack has resulted in the STP root being moved - now traffic will be diverted via our switch…



Mitigating Spanning Tree Attacks
BPDU Guard…

BPDU Guard is one mechanism to avoid an attacker injecting BPDU packets and becoming the STP Root… applied globally on the switch…



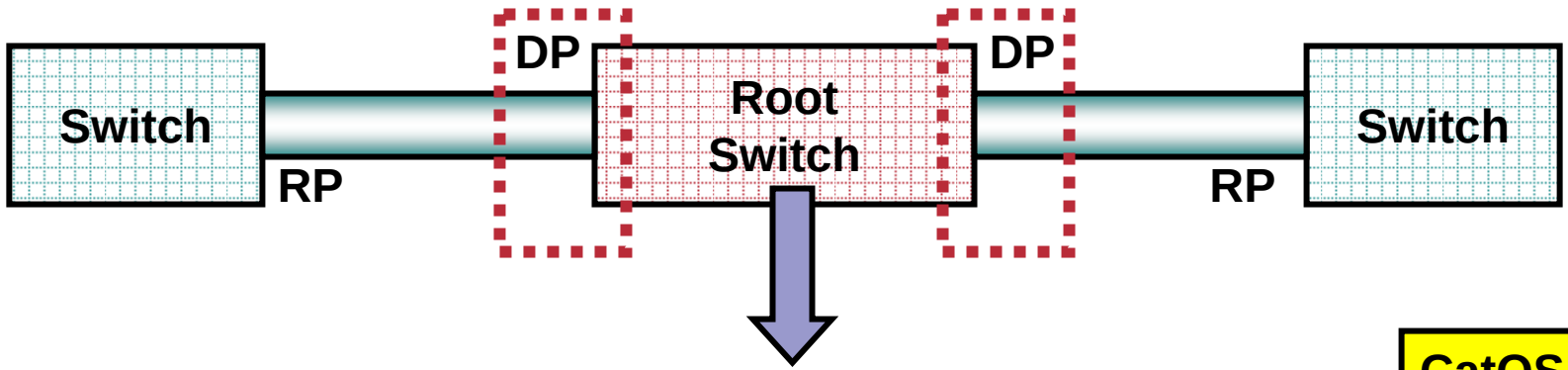

```
CatOS> (enable) set spantree portfast bpdu-guard enable
IOS(config)# spanning-tree portfast bpduguard
```

If a BPDU is detected on a BPDU Guard port, the switchport is shutdown

Mitigating Spanning Tree Attacks
ROOT Guard…

Root Guard is another mechanism to avoid an attacker becoming the STP Root… applied globally on the switch…forces local ports to become "Designated" Ports

DP = Designated Port – Points away from the Root
RP = Root Port – Points towards to Root



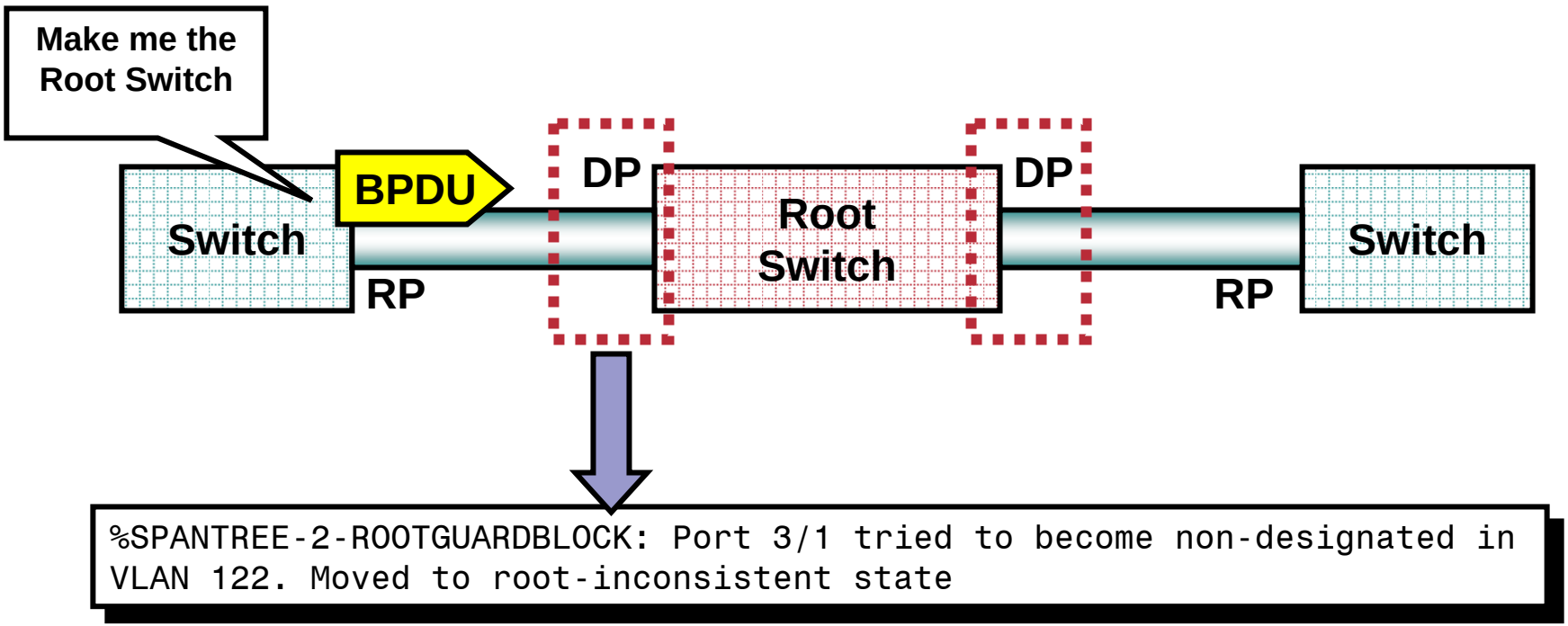
CatOS

```
Switch> (enable) set spantree guard root 3/1
```

IOS

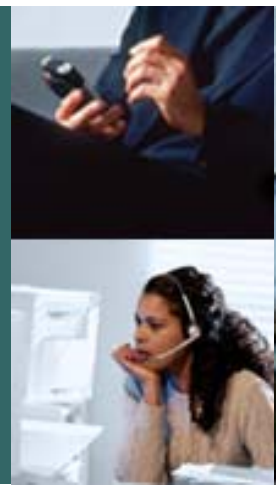
```
Switch(config)# spanning-tree guard root (or rootguard)
```

Mitigating Spanning Tree Attacks
ROOT Guard…



If a root guarded port receives a superior BPDU, the port is moved to a "Root inconsistent STP State" (similar to STP Listening state) and no traffic will be forwarded across that port – thus root switch position maintained

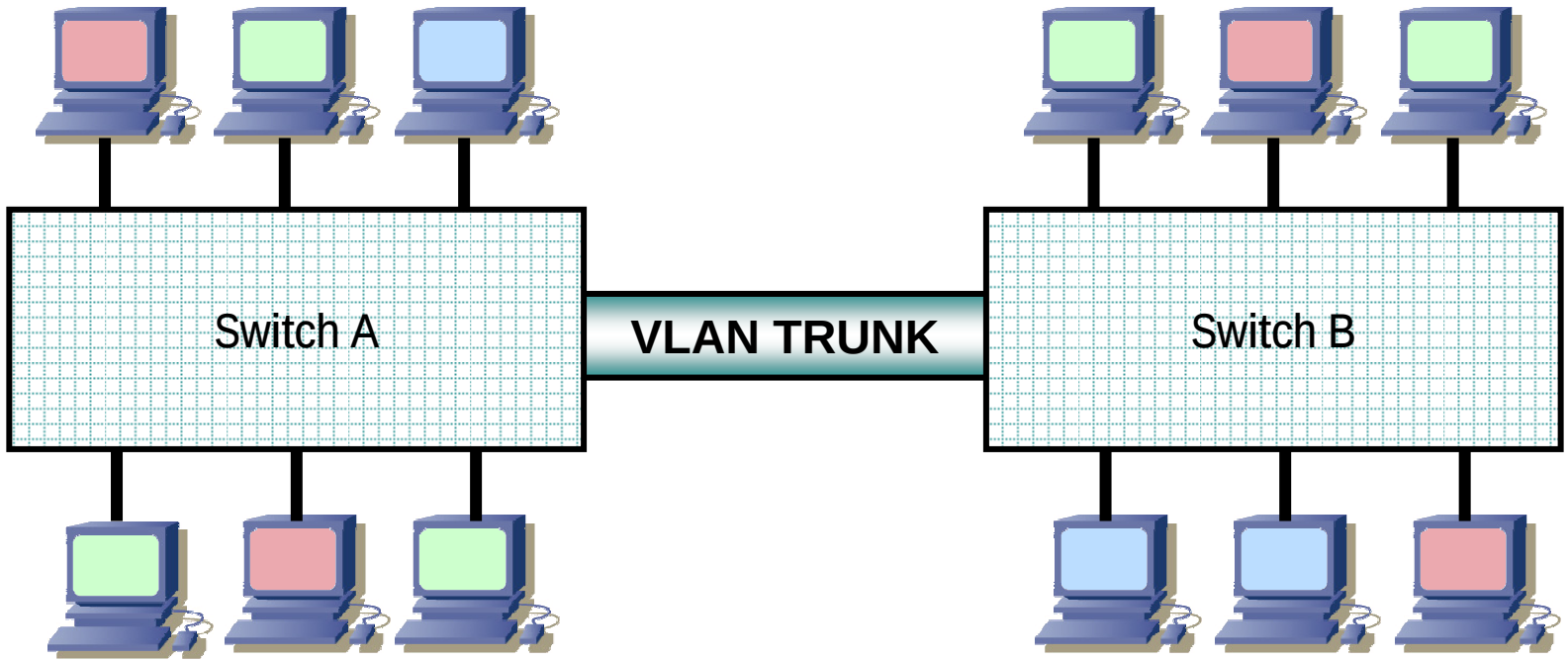
ATTACKS AND COUNTERMEASURES: VLAN HOPPING ATTACKS



© 2005 Cisco Systems, Inc. All rights reserved.

VLAN Trunk Refresher

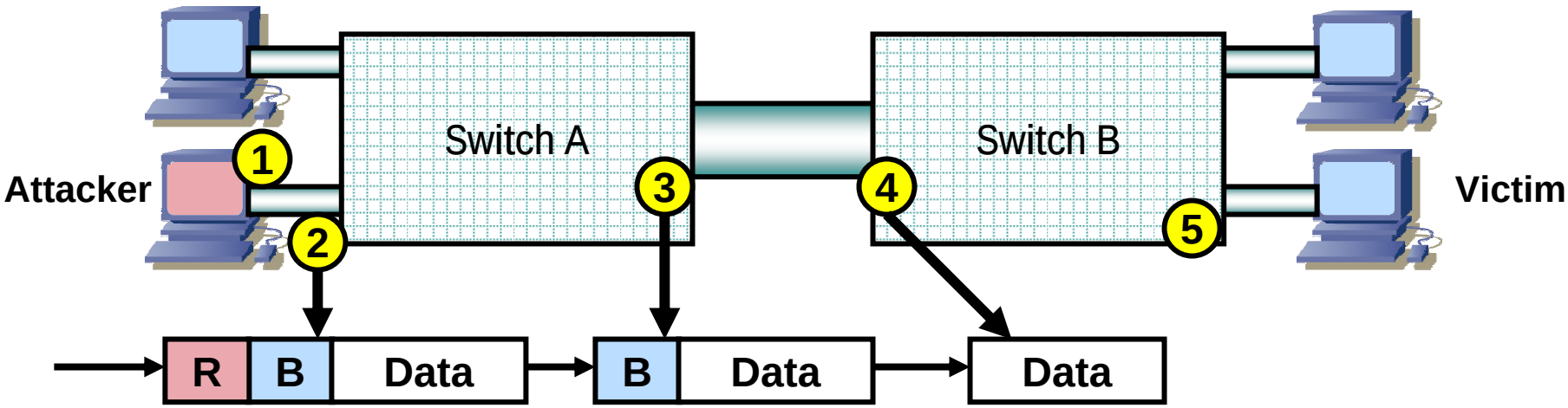
VLAN Trunks are used to forward traffic from multiple VLAN's across a single physical link – Two encapsulation options are available for VLAN Trunking – Cisco ISL and IEEE 802.1Q



In this network, the VLAN Trunk is configured to carry VLAN traffic for the RED, BLUE and GREEN VLAN's

VLAN Hopping Attack

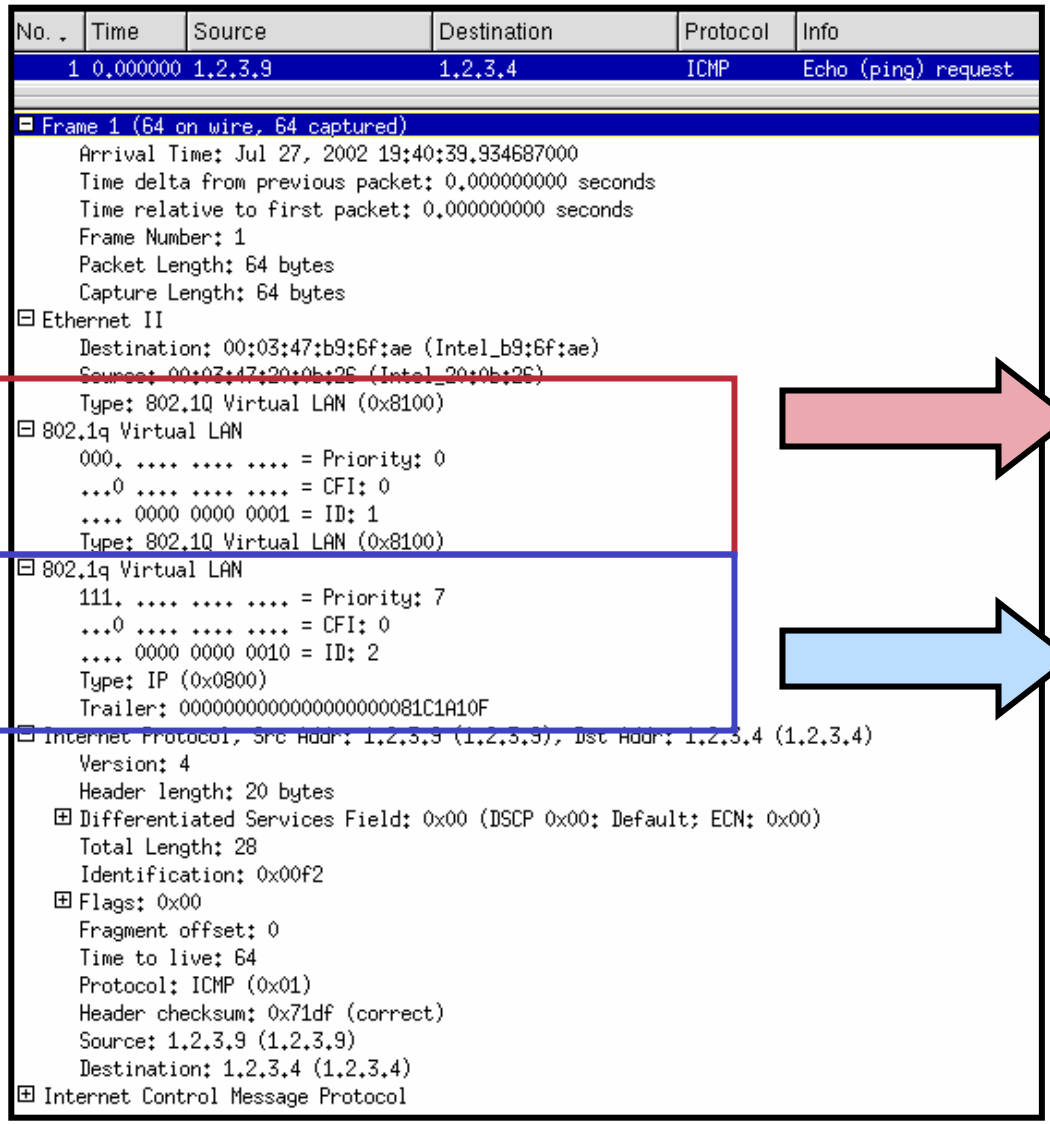
Idea behind the VLAN Hopping attack is to negotiate a VLAN trunk between the switch and host and then send a double tagged packet to the switch



1. Host negotiates Trunk
2. Host sends double tagged frame
3. Switch strips off first frame and forwards to next hop
4. Switch strips off VLAN tag
5. Switch forwards frame in BLUE VLAN to host

Result: VLAN Hopped!!!

Ethereal Capture



First tag shown here is the outside VLAN or the attackers VLAN…

Second tag shown is the inside VLAN or the target VLAN that the attacker wants to hop to…

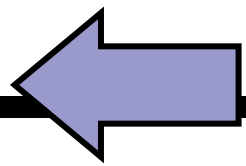
Mitigating VLAN Hopping

Easiest way to stop this from happening is to DISABLE trunking on unnecessary ports

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

CatOS also has a neat feature – a macro command that sets in place a suitable set of parameters for a host port – this command is shown below…

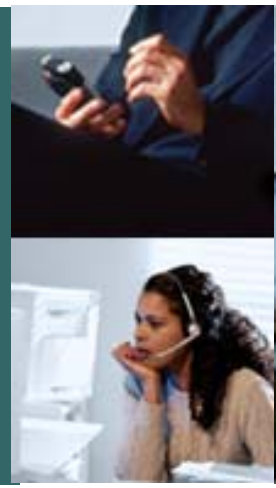
```
C6500> (enable) set port host 6/22
Port(s) 6/22 channel mode set to off.

Warning: Connecting Layer 2 devices to a fast start port can cause
temporary spanning tree loops. Use with caution.

Spantree port  6/22 fast start enabled.
Dot1q tunnel feature disabled on port(s)  6/22.
Port(s)  6/22 trunk mode set to off.
```



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
- Disable auto-trunking on user facing ports (DTP off)
- Explicitly configure trunking on infrastructure ports
- Use all tagged mode for the Native VLAN on trunks

ATTACKS AND COUNTERMEASURES: MAC ATTACKS



MAC Address/CAM Table Review

48 Bit Hexadecimal Number Creates 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

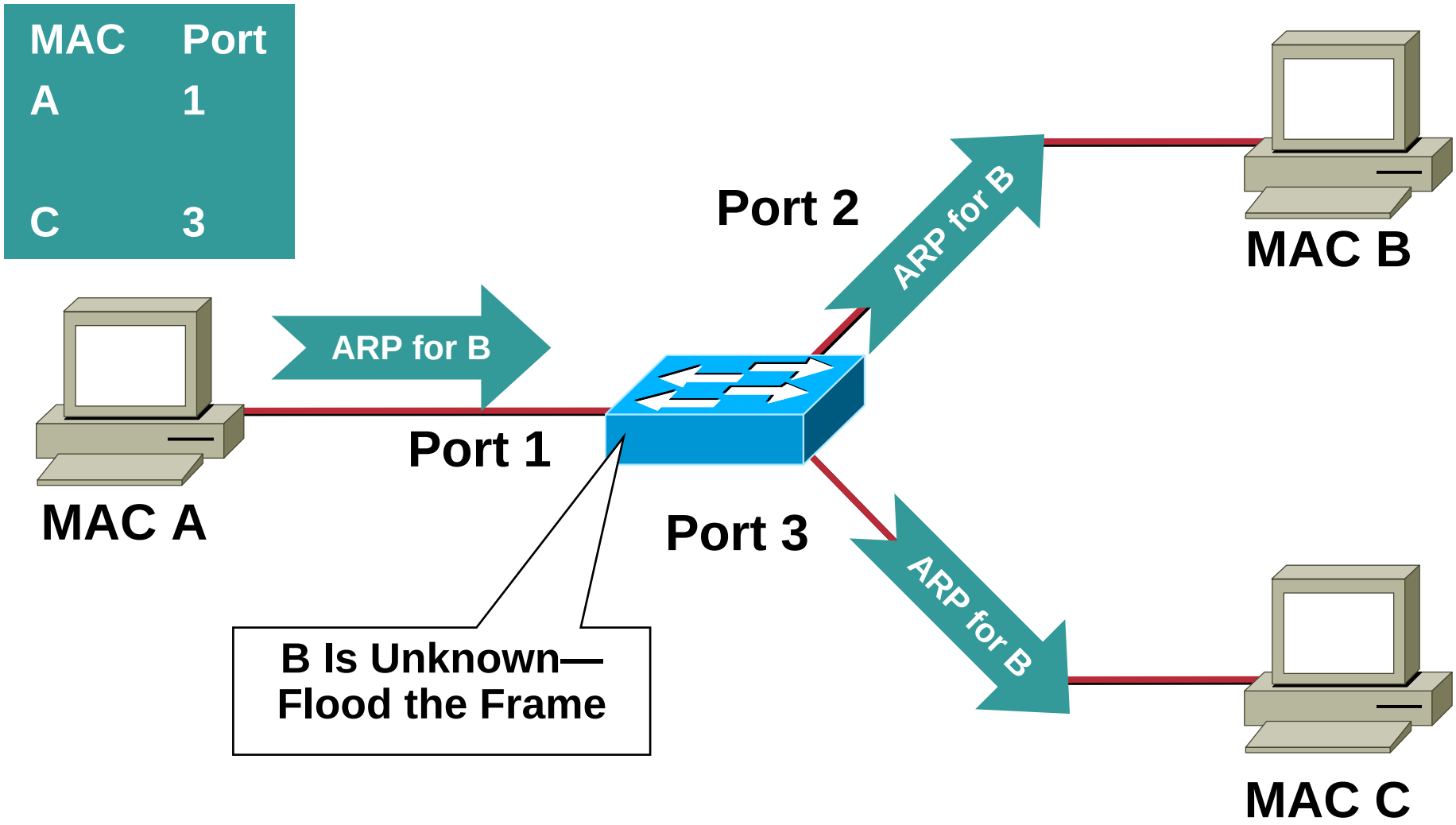
0000.0cXX.XXXX

All F's = Broadcast

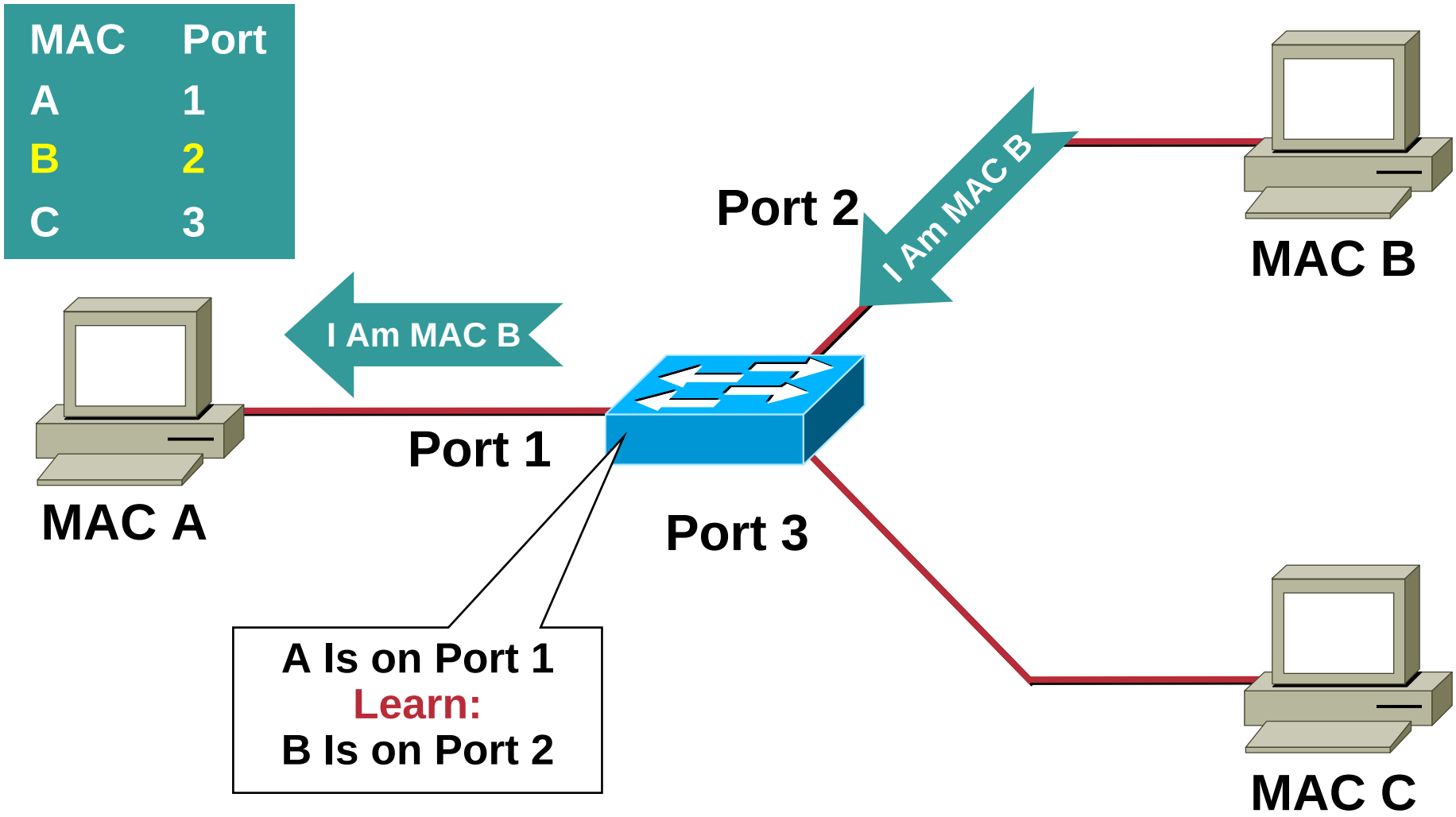
FFFF.FFFF.FFFF

- **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**

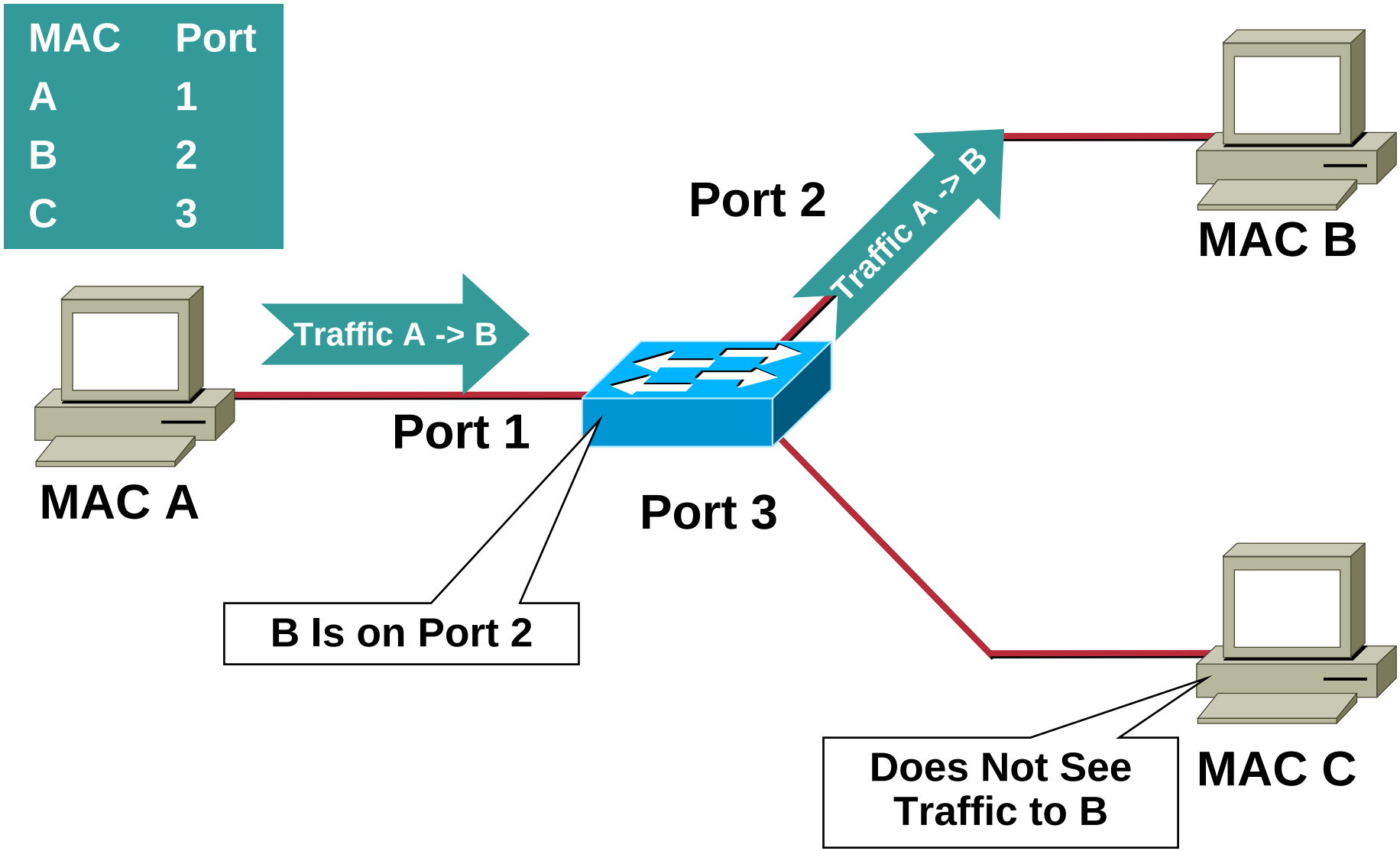
Normal CAM Behavior 1/3



Normal CAM Behavior 2/3



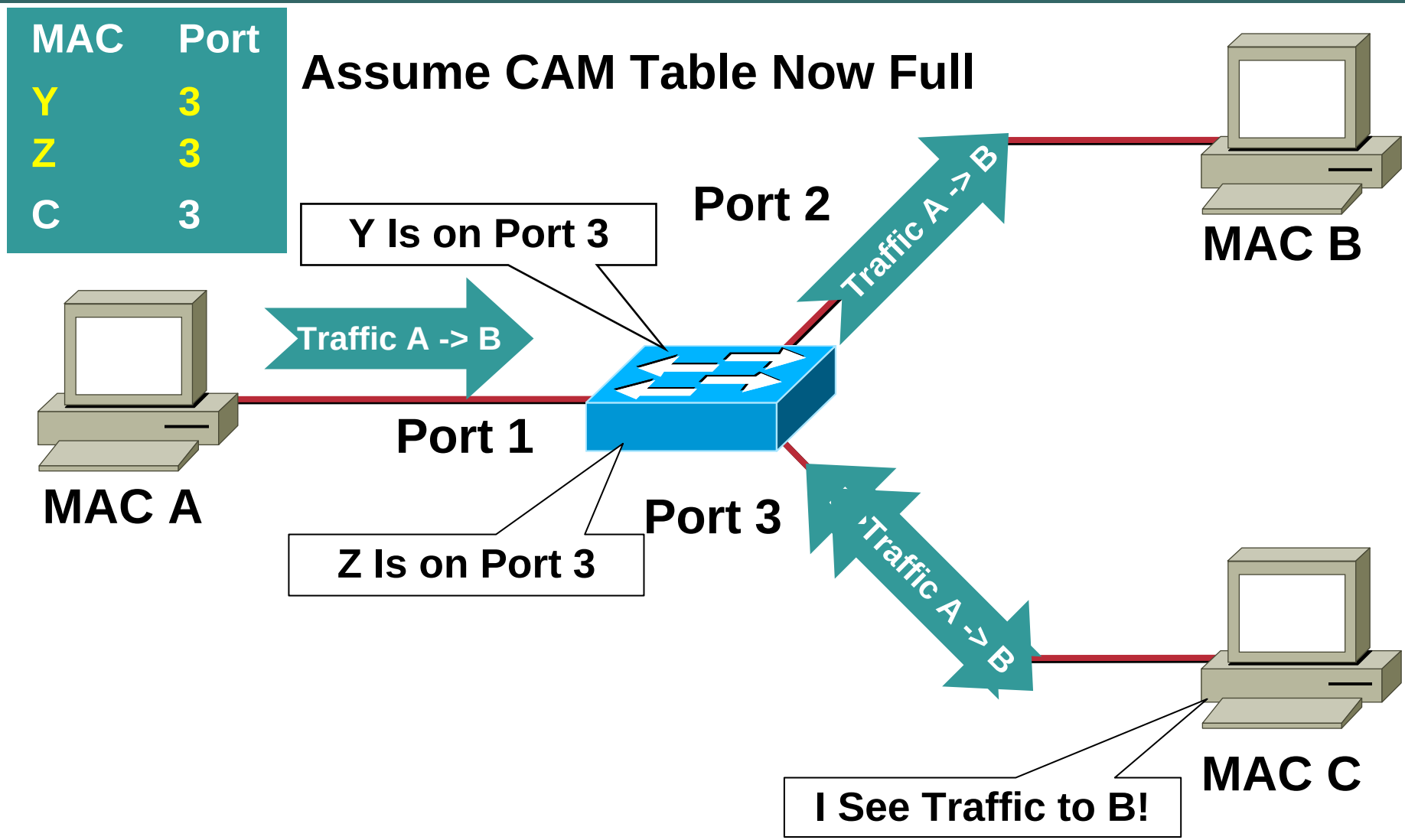
Normal CAM Behavior 3/3



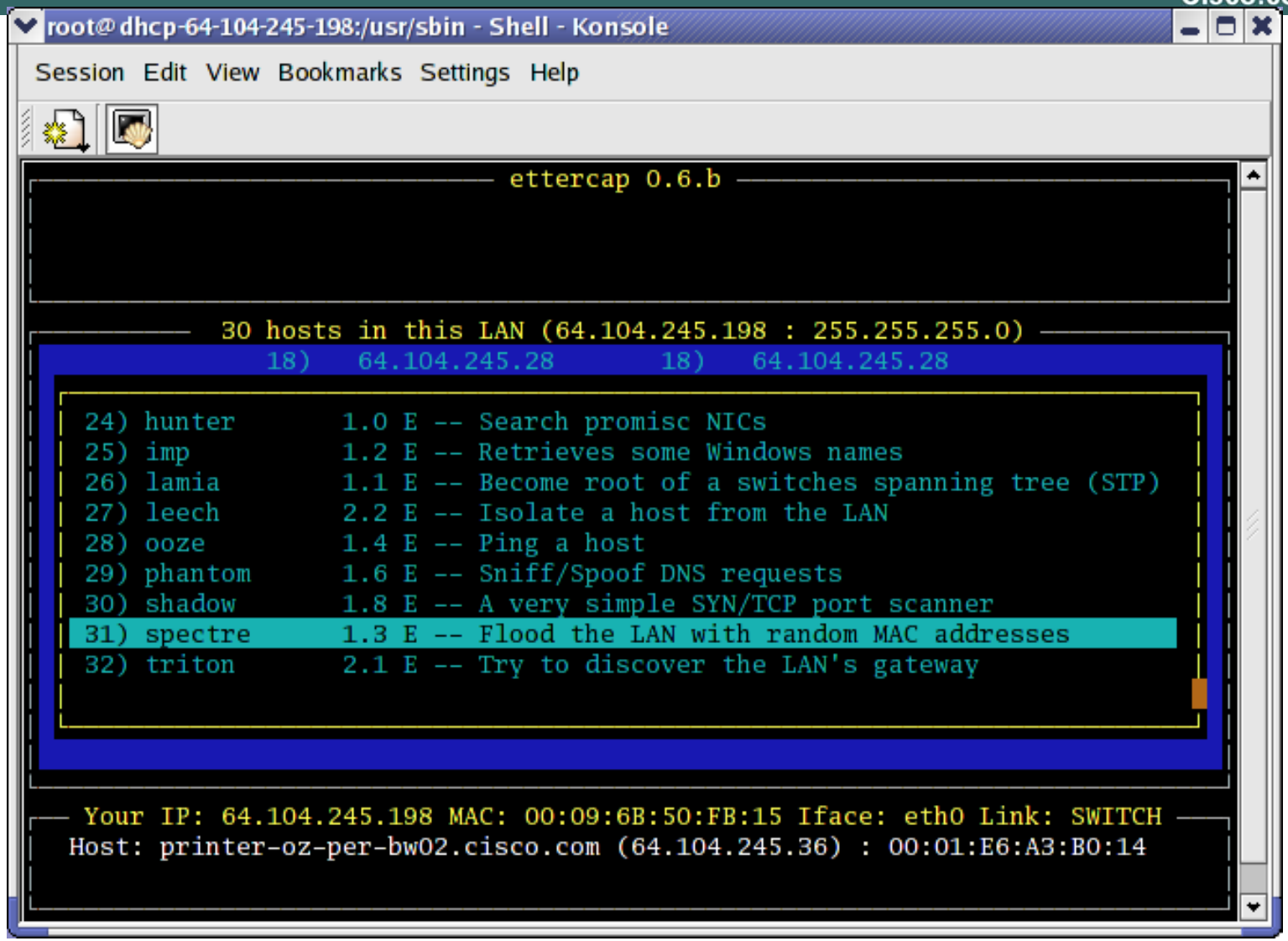
CAM Overflow 1/3

- **macof tool since 1999**
  - **About 100 lines of perl**
  - **Included in “dsniff”**
- **Attack successful by exploiting the size limit on CAM tables**

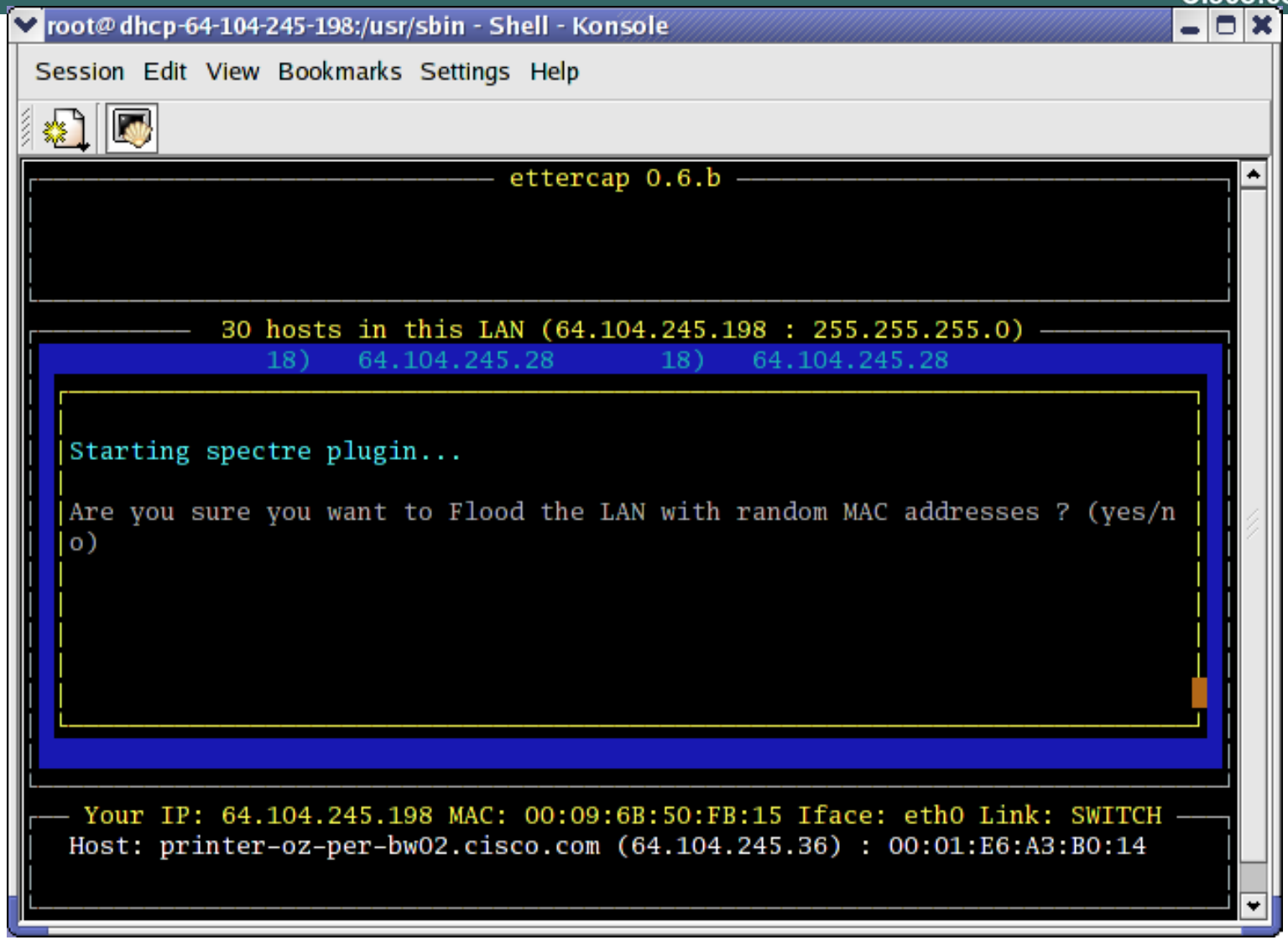
CAM Overflow 2/3



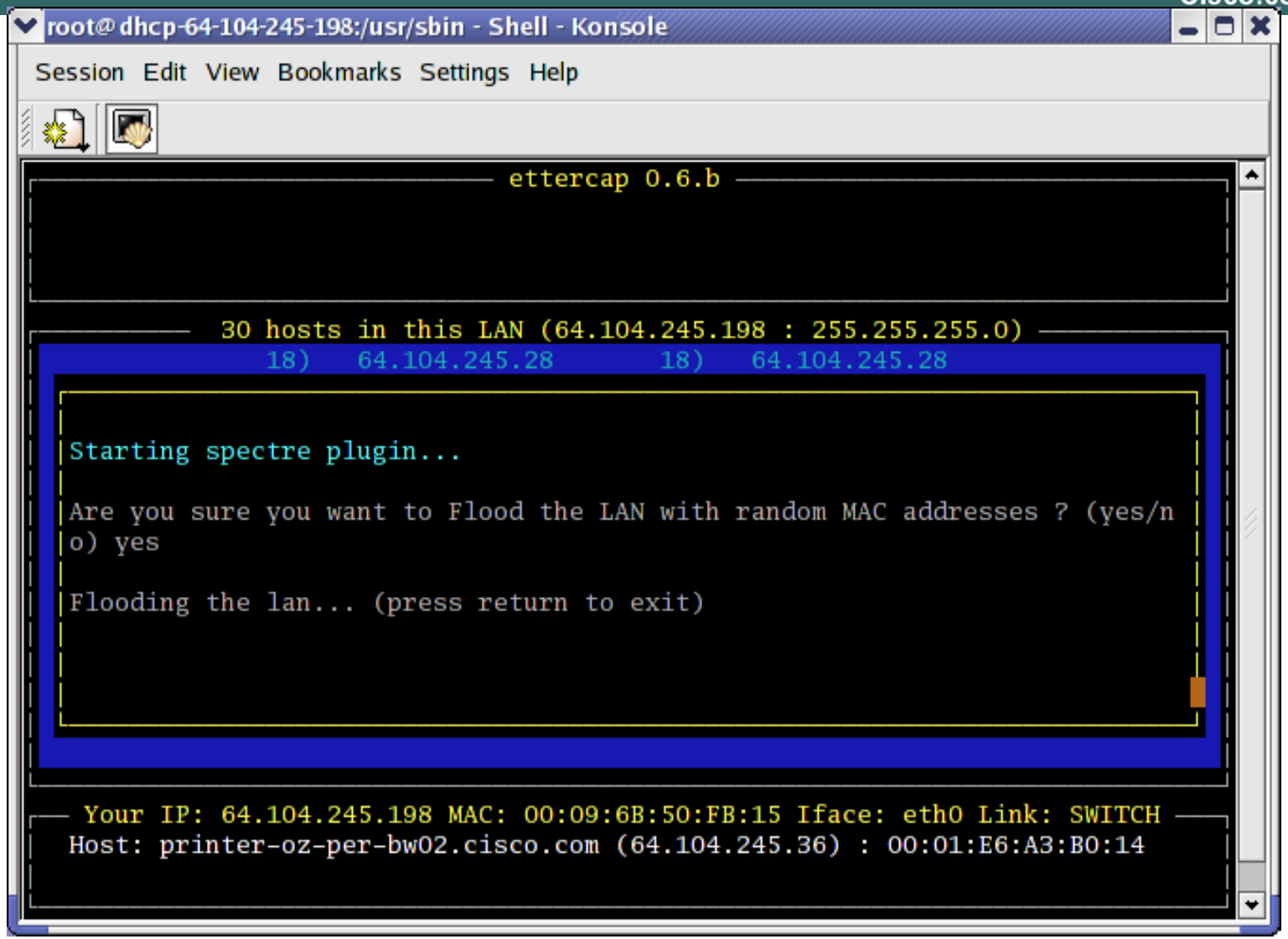
MAC/CAM Attacks
Flooding the MAC Table?



MAC/CAM Attacks
Flooding the MAC Table?



MAC/CAM Attacks
Flooding the MAC Table?



MAC/CAM Attacks
MACOF Attack Tool?

MACOF is one of a number of tools available with "DSNIFF"

Dynamically generates MAC addresses to fill the Switch CAM table…

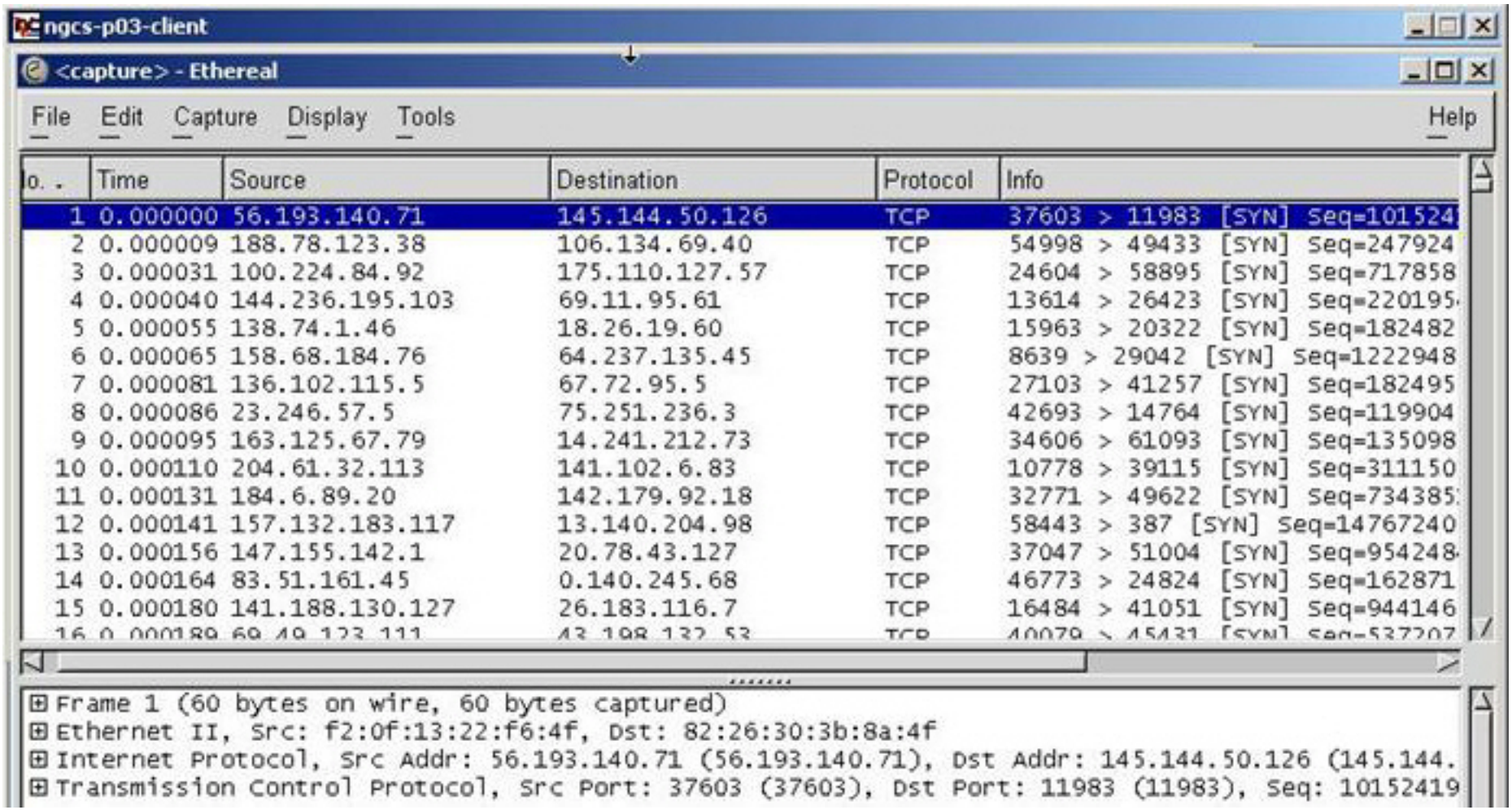
Three main development platforms
Red Hat Linux, Solaris and Open BSD
(Also on Win2K/XP, FreeBSD, Debian, AIX, and HPUX)

http://www.monkey.org/~dugsong/dsniff

```
[root@macattack]# macof –i eth0
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

MAC/CAM Attacks
MACOF Attack seen from Ethereal?

Using ETHEREAL to trace the progress of the MACOF attack…



CAM Table Sizes

- **Each switch has a limit on CAM tables**
- **Size by basic switch**

  3xxx—16,000

  4xxx—32,000

  6xxx—128,000

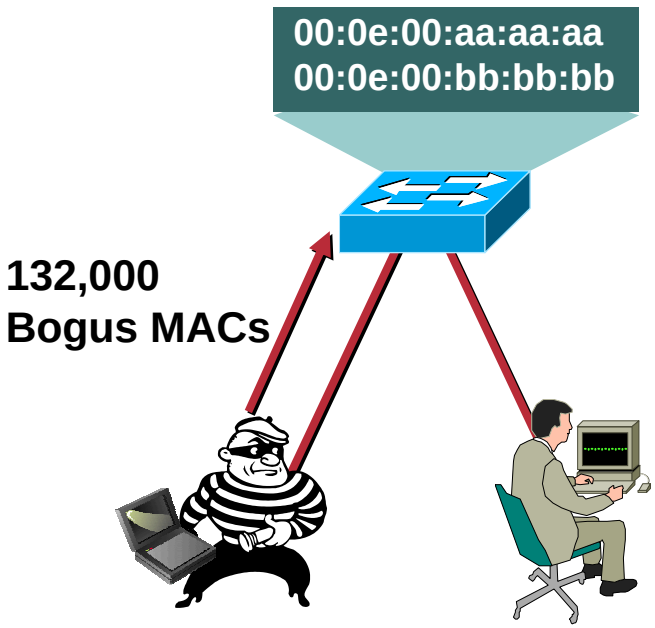
CAM Table FULL!

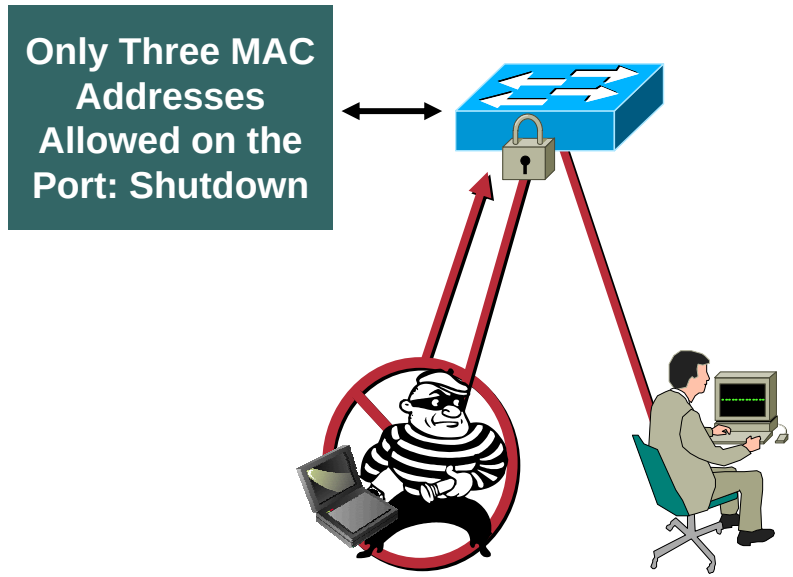
- **Once you have flooded the CAM table, packets from any new session will be forwarded out all switch ports (default switch behavior), allowing a malicious user to run a packet sniffer to capture users traffic…**
- **This will turn a VLAN on a switch basically into a hub**
- **This attack will also fill the CAM tables of adjacent switches**

```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

Countermeasures for MAC Attacks

Port Security Limits the Amount of MAC's on an Interface

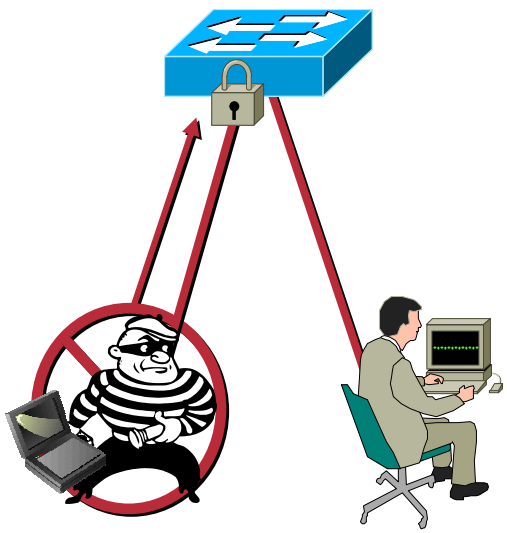




Solution:

- **Port security limits MAC flooding attack and locks down port and sends an SNMP trap**

Port Security: Example Config



CatOS

```
set port security 5/1 enable
set port security 5/1 port max 3
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```

IOS®

```
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

- Three MAC addresses encompass the phone, the switch in the phone, and the PC
- “Restrict” rather than “error disable” to allow only three, and log more than three
- Aging time of two and aging type inactivity to allow for phone CDP of one minute

If Violation Error-Disable, the Following Log Message Will Be Produced: 4w6d: %PM-4-ERR_DISABLE: Psecure-Violation Error Detected on Gi3/2, Putting Gi3/2 in Err-Disable State

Port Security

Not All Port Security Created Equal

- In the past you would have to type in the ONLY MAC you were going to allow on that port
- You can now put a limit to how many MAC address a port will learn
- You can also put timers in to state how long the MAC address will be bound to that switch port
- You might still want to do static MAC entries on ports that there should be no movement of devices, as in server farms
- If you are going to be running Cisco IPT, you will need a minimum of three MAC addresses on each port if you are running voice VLANs
- New feature called "Sticky Port Security", settings will survive reboot (not on all switches)

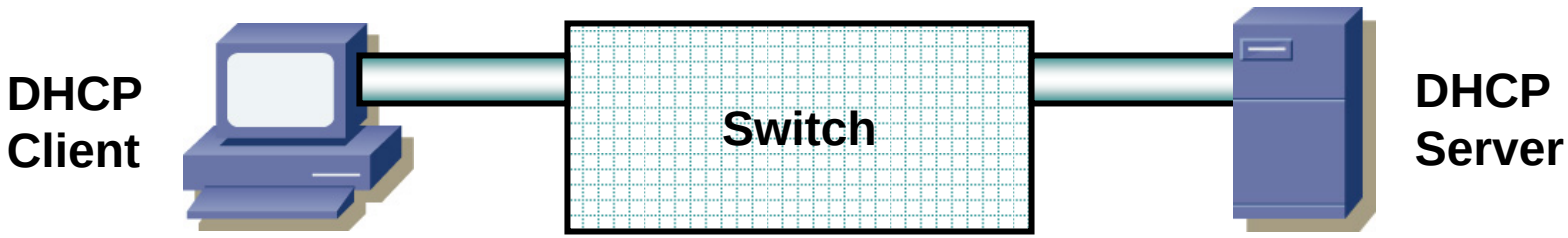
Building the Layers

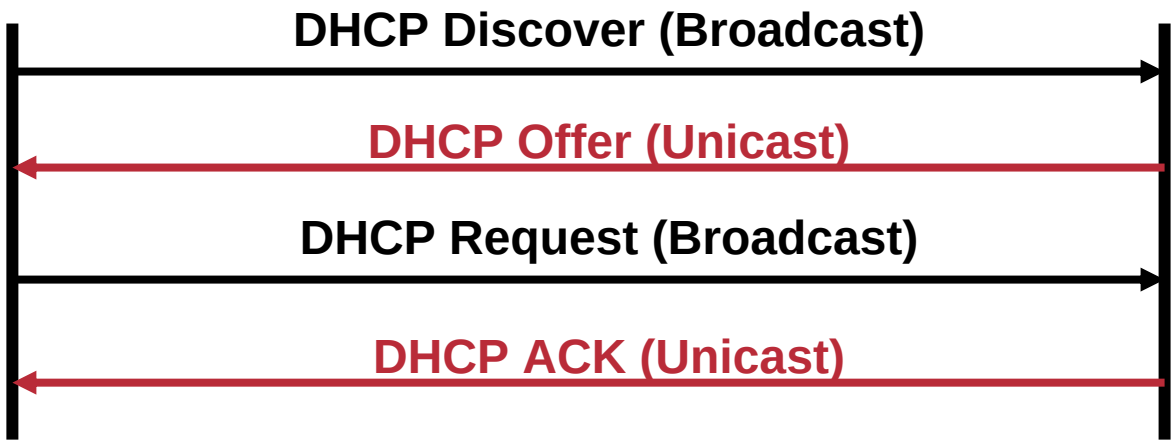
- **Port Security prevents CAM attacks and DHCP starvation attacks**

ATTACKS AND COUNTERMEASURES: DHCP ATTACKS

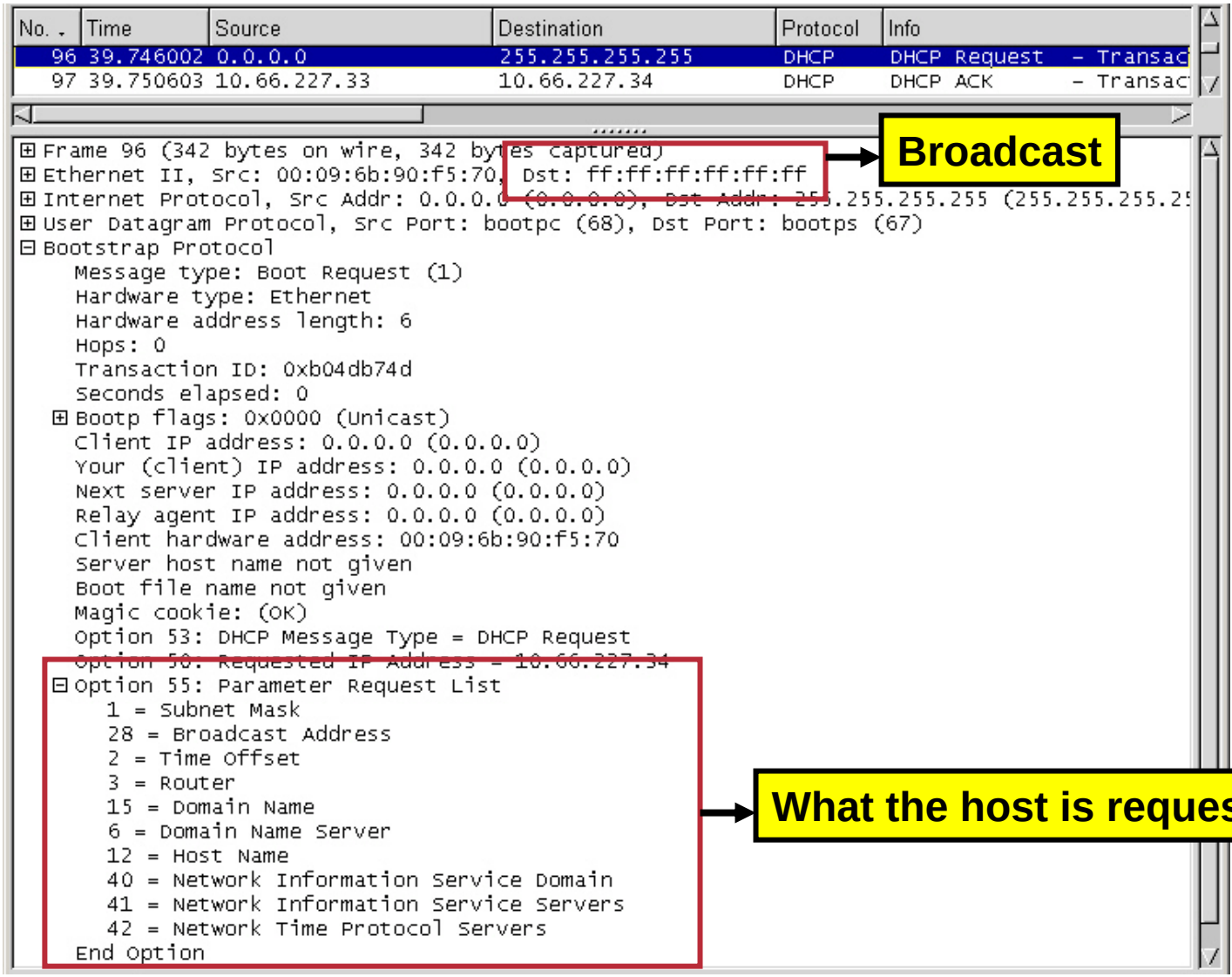
DHCP Refresher

Dynamic Host Configuration Protocol is designed to serve IP addresses to requesting hosts from a pool of addresses setup by an administrator…

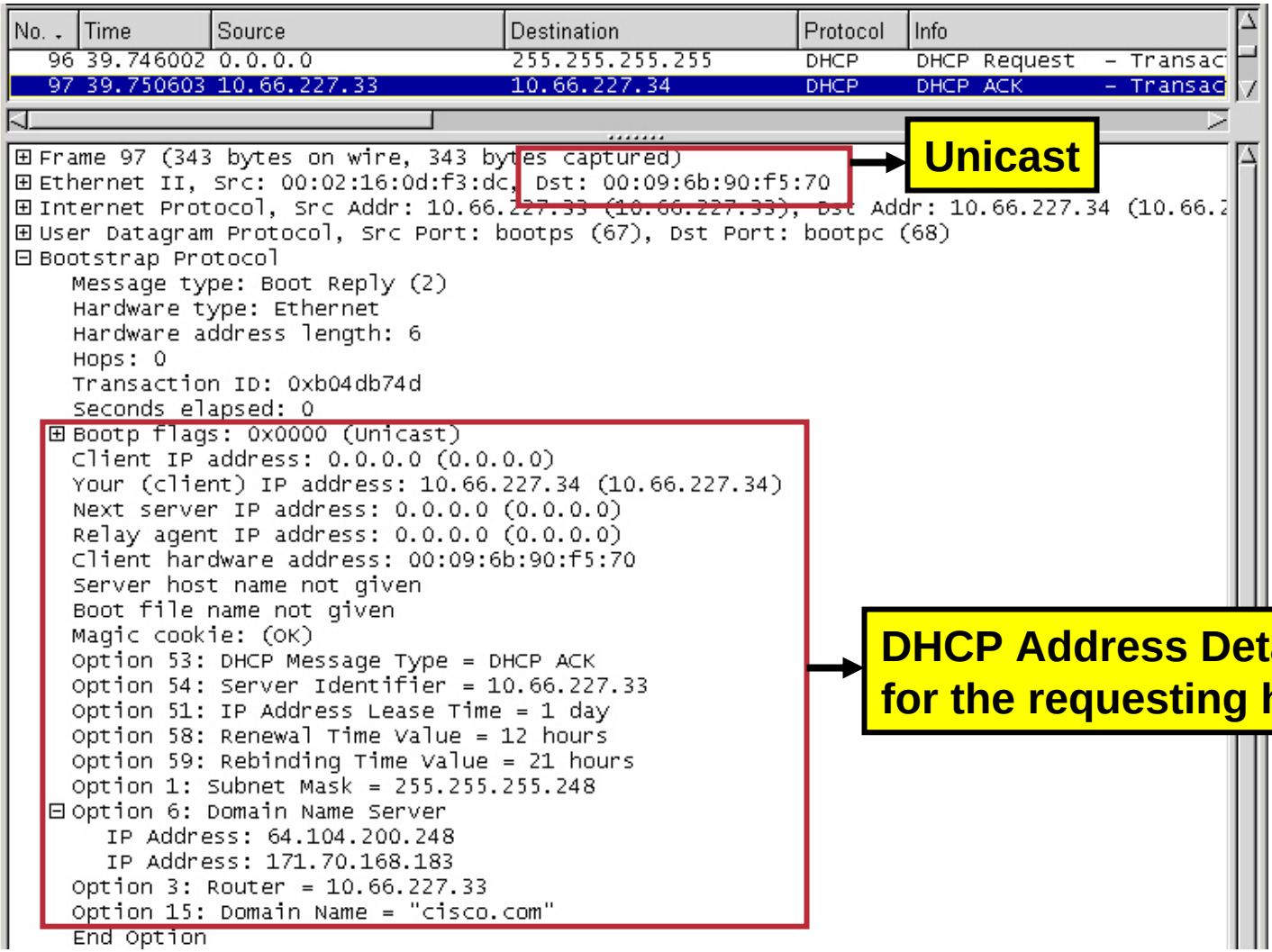




DHCP Request

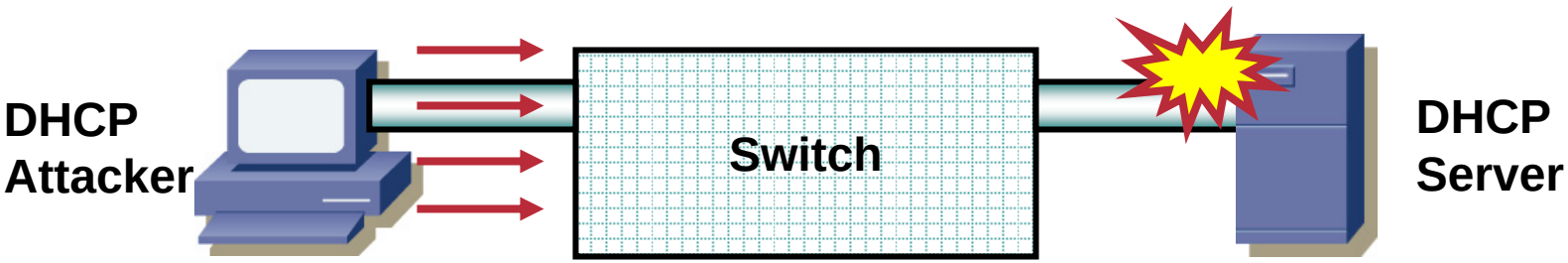


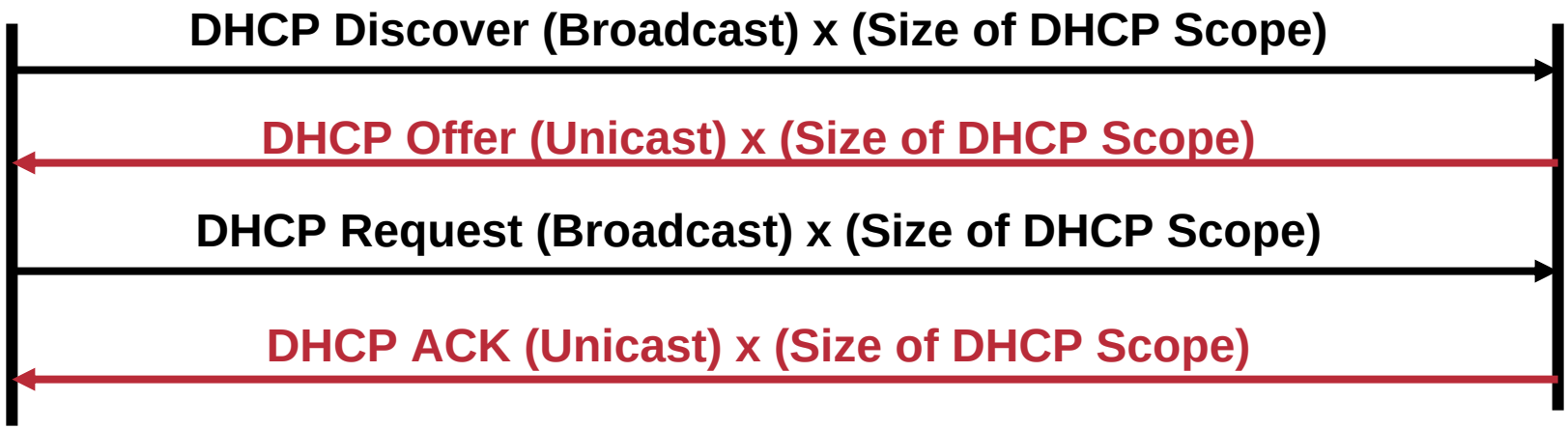
DHCP ACK (the reply)



DHCP Starvation Attack

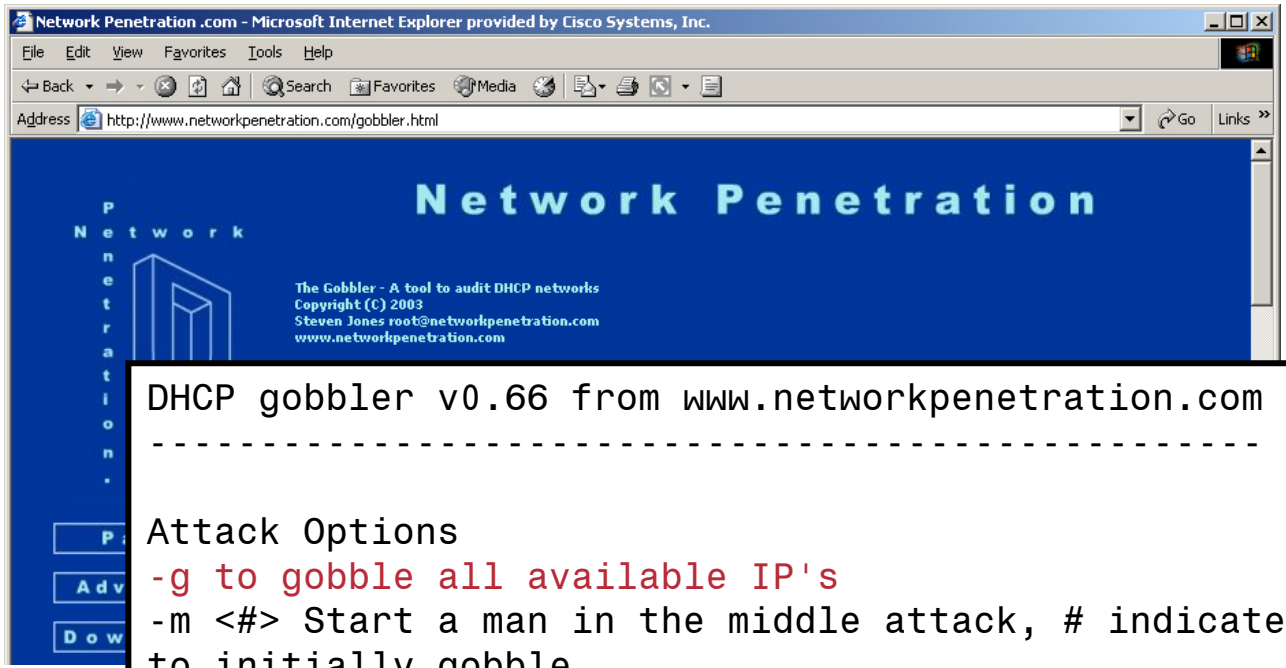
Denial of Service (DoS) attack that can be used to grab ALL the addresses from the DHCP server – Now all other hosts requesting DHCP address will be denied from accessing network due to no available addresses…





DHCP Attack Tools

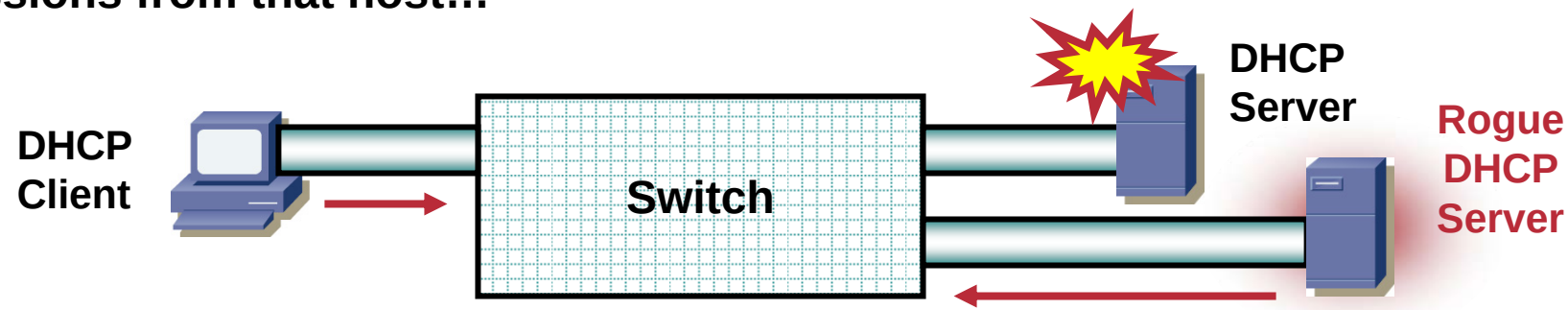
Denial of Service (DoS) attack that can be used to grab ALL the addresses from the DHCP server so that no other host can get onto the network…

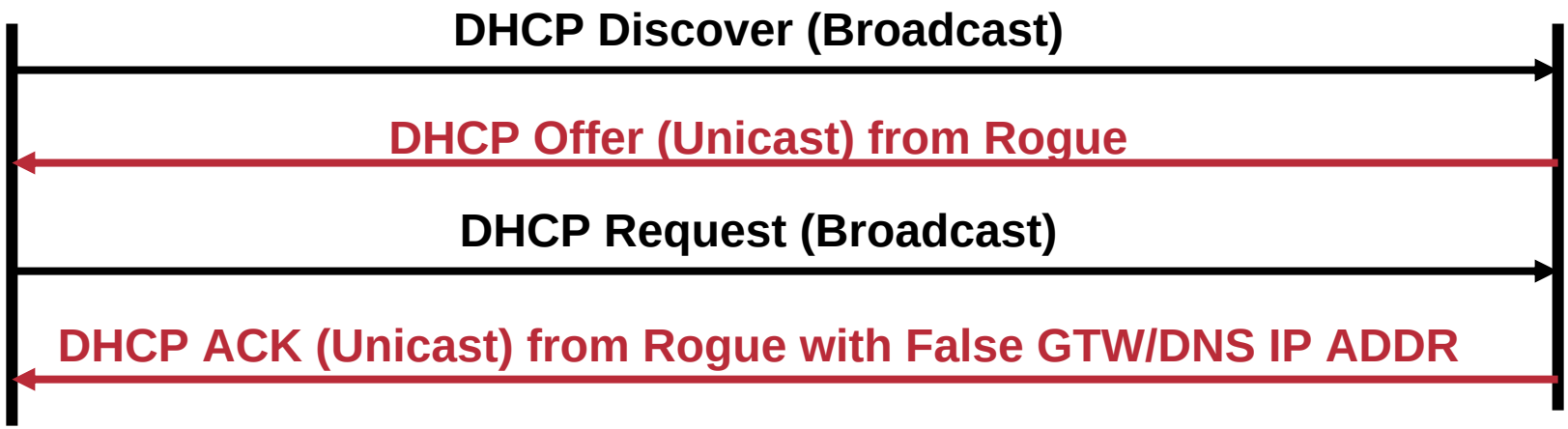



```
DHCP gobbler v0.66 from www.networkpenetration.com
--------------------------------------------------

Attack Options
-g to gobble all available IP's
-m <#> Start a man in the middle attack, # indicates number of connections
to initially gobble

Man in the middle attack options
-D <IP Address> IP address of spoofed DNS server
-G <IP Address> IP address of spoofed default gateway
-A <IP Address> IP address of fake DHCP server (can be spoofed)
```

DHCP Rogue Server Attack

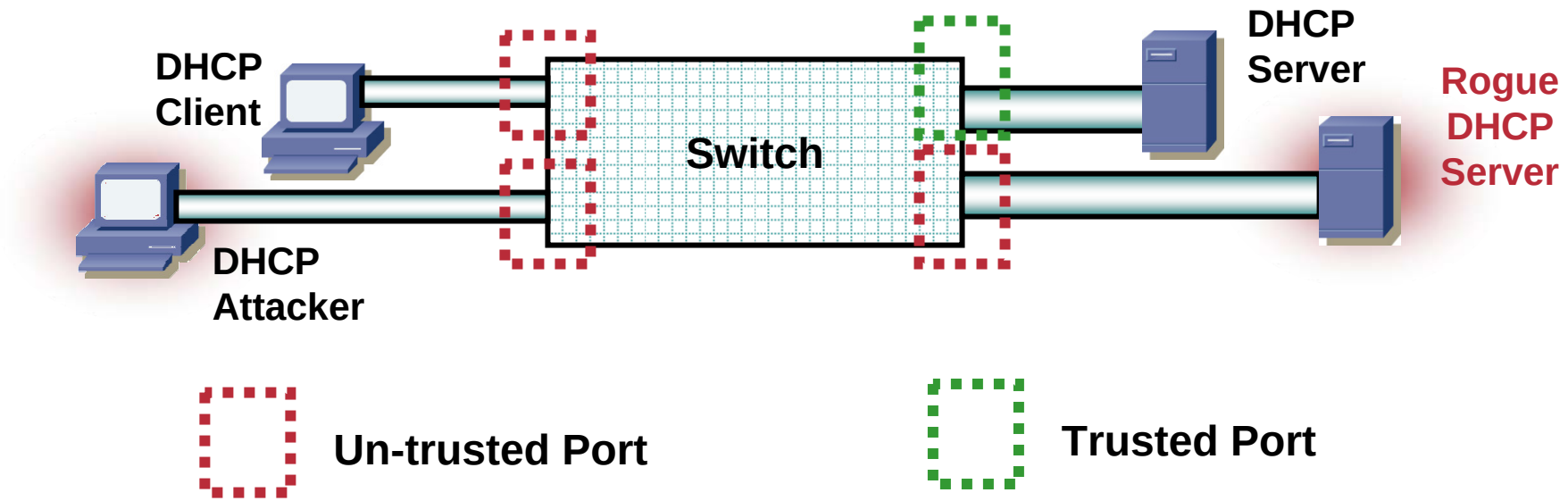
The Rogue DHCP Server can issue DHCP Requests pointing to false DNS or Gateway (maybe use its own IP for this) – allowing it to snoop on sessions from that host…





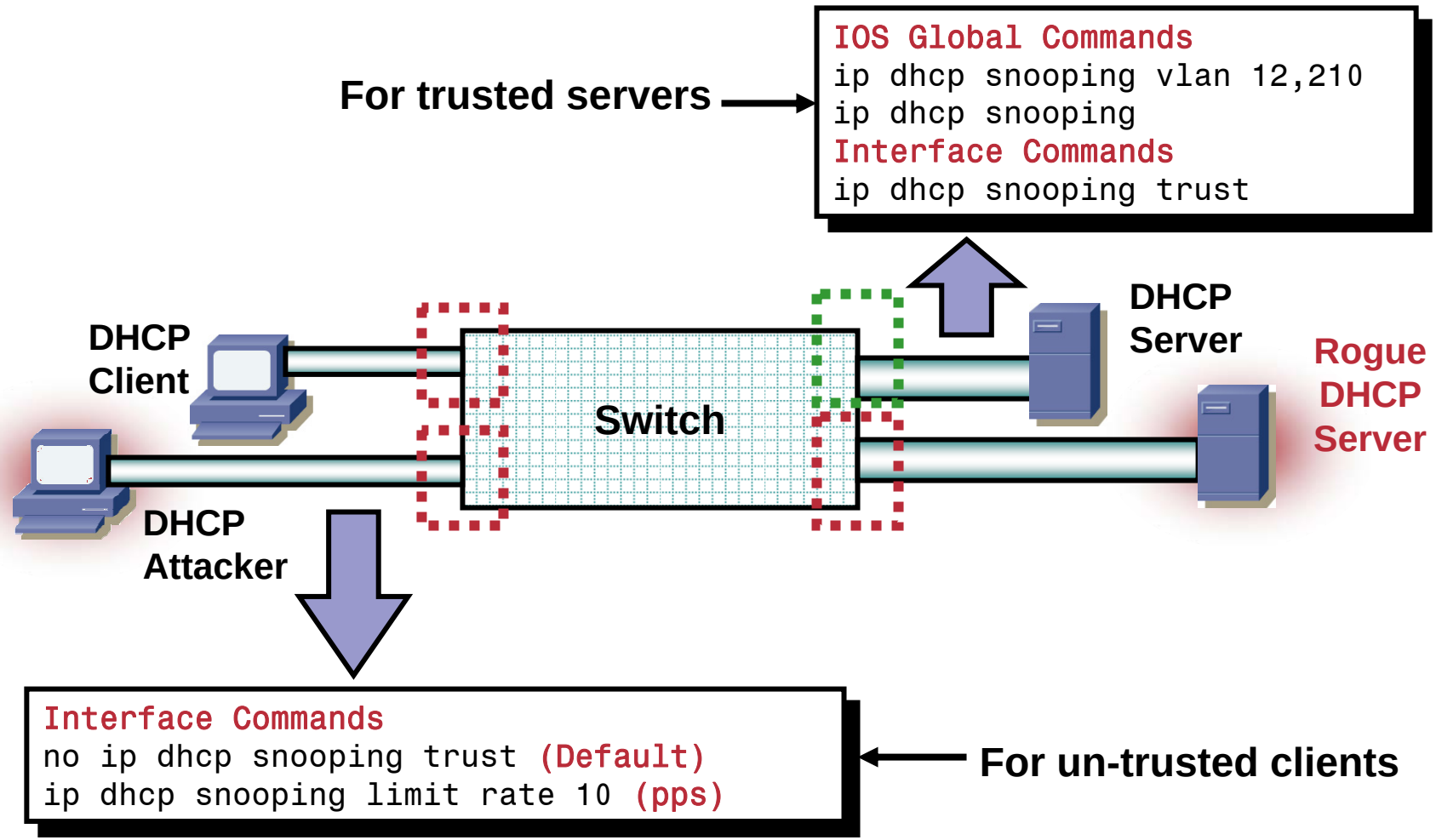
Mitigating DHCP Attacks

The new DHCP Snooping Feature prevents MITM attacks and DoS attacks on the DHCP server

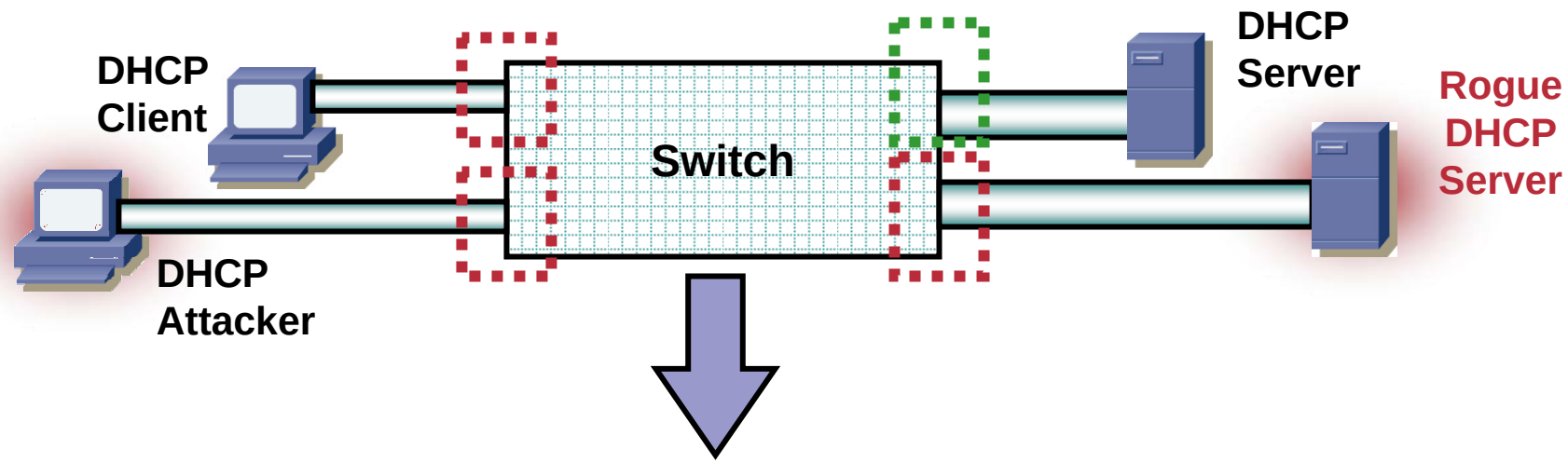


When DHCP Packets originate from an UNTRUSTED port – only Client Requests are forwarded – all other DHCP packets are dropped (DHCP Offer, DHCP ACK, NACK or other DHCP server orientated packets…

Mitigating DHCP Attacks



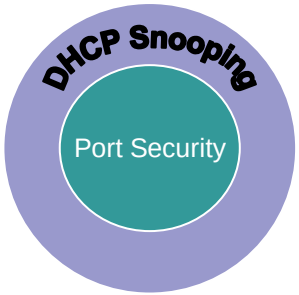
DHCP Binding Table




```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:00:09:f3:2a:19   10.66.227.33     138225      dhcp-snooping  12    GigabitEthernet4/12
```

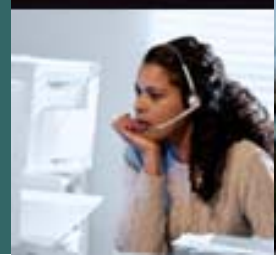
This binding table is the same one used for other security features like IP Source Guard and Dynamic ARP Inspection

Building the Layers



- **Port Security prevents CAM Attacks and DHCP Starvation attacks**
- **DHCP Snooping prevents Rogue DHCP Server attacks**

ATTACKS AND COUNTERMEASURES: ARP ATTACKS

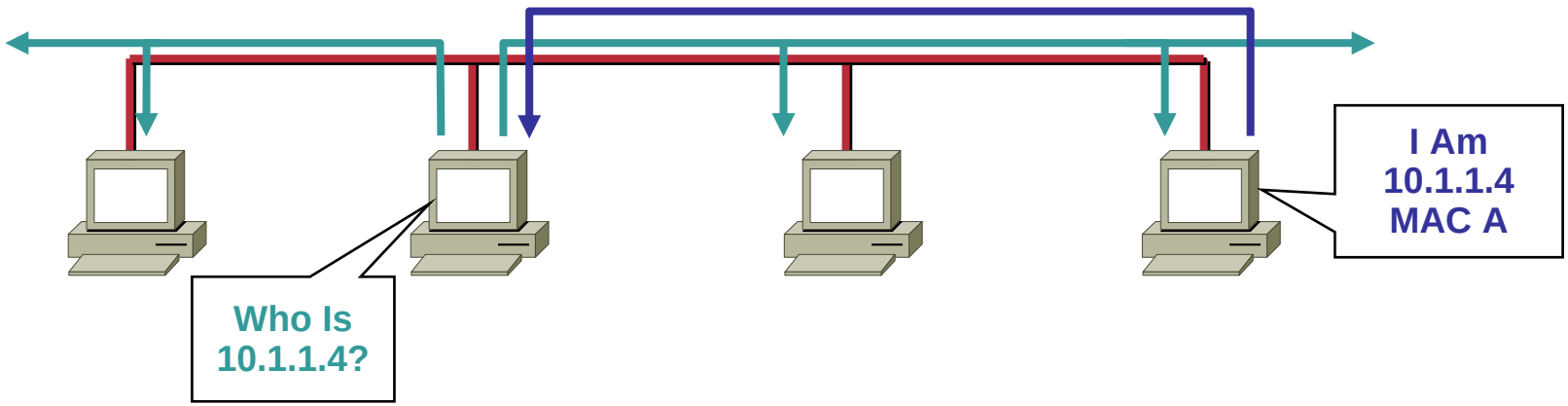


ARP Function Review

- **Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address**

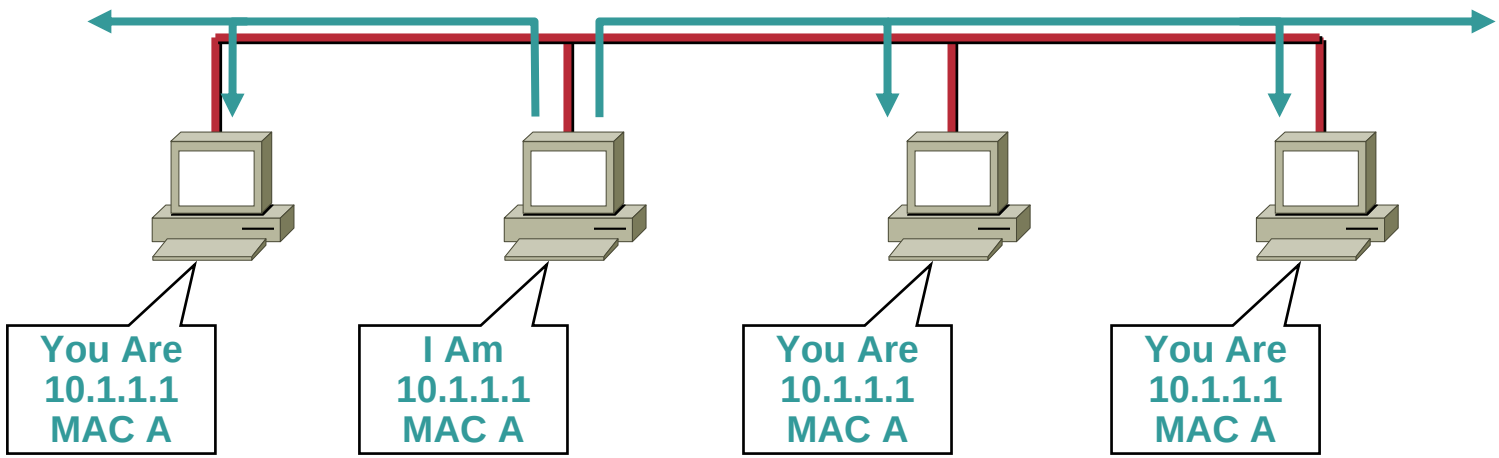
  This ARP request is broadcast using protocol 0806

- **All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply**



ARP Function Review

- According to the ARP RFC, a client is allowed to send an unsolicited ARP reply; this is called a gratuitous ARP; other hosts on the same subnet can store this information in their ARP tables
- Anyone can claim to be the owner of any IP/MAC address they like
- ARP attacks use this to redirect traffic

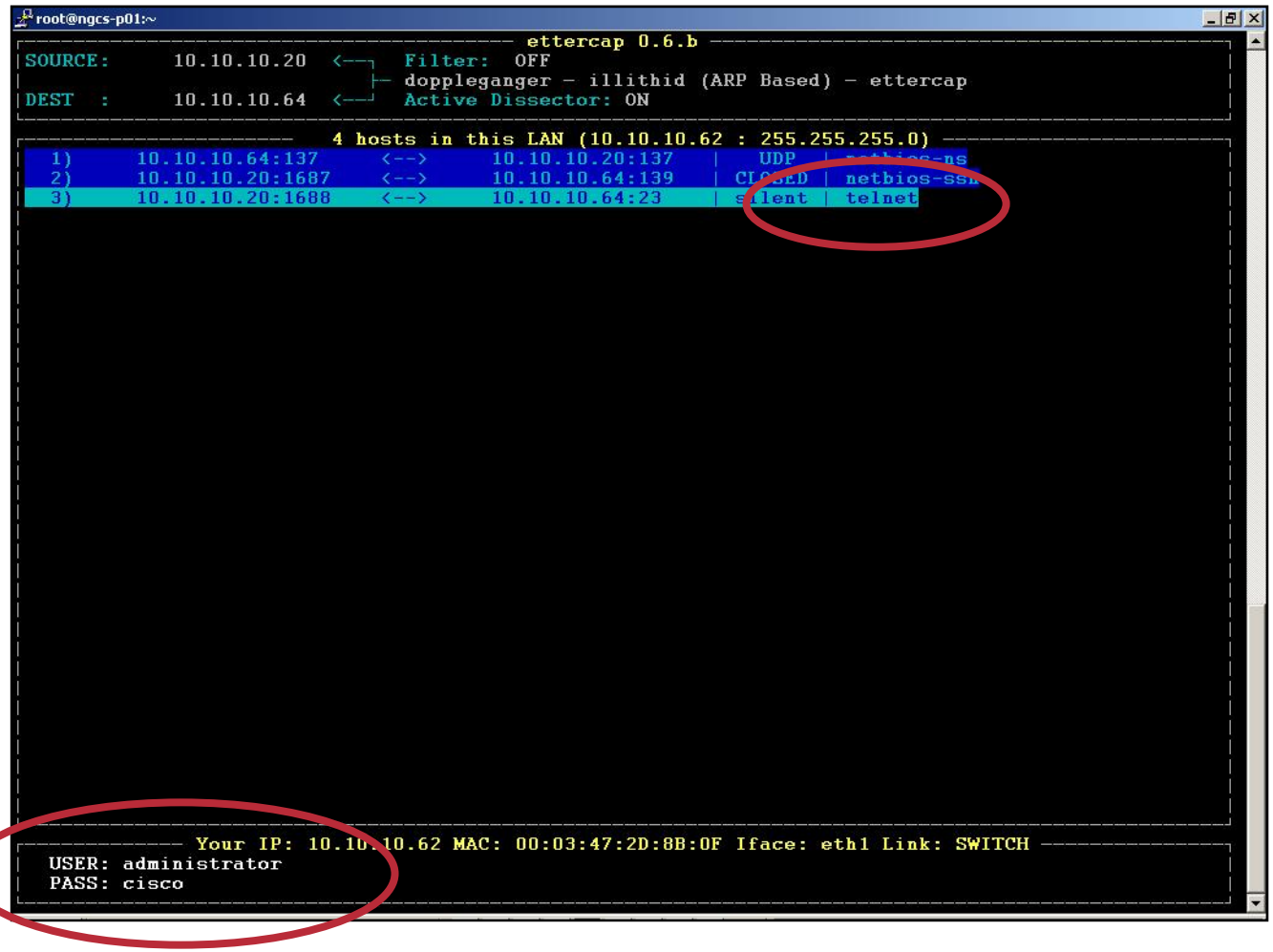


ARP Attack Tools

- **Two major tools on the Net for ARP man-in-the-middle attacks**
  - **dsniff—http://monkey.org/~dugsong/dsniff/**
  - **ettercap—http://ettercap.sourceforge.net/index.php**
  - **Both "tools" function similar to each other**
- **ettercap is the second generation of ARP attack tools**
  - **ettercap has a nice GUI, and is almost point and click**
  - **Interesting features of ettercap**
  - **Packet Insertion, many to many ARP attack**
- **Both capture the traffic/passwords of applications (over 30)**
  - **FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL**

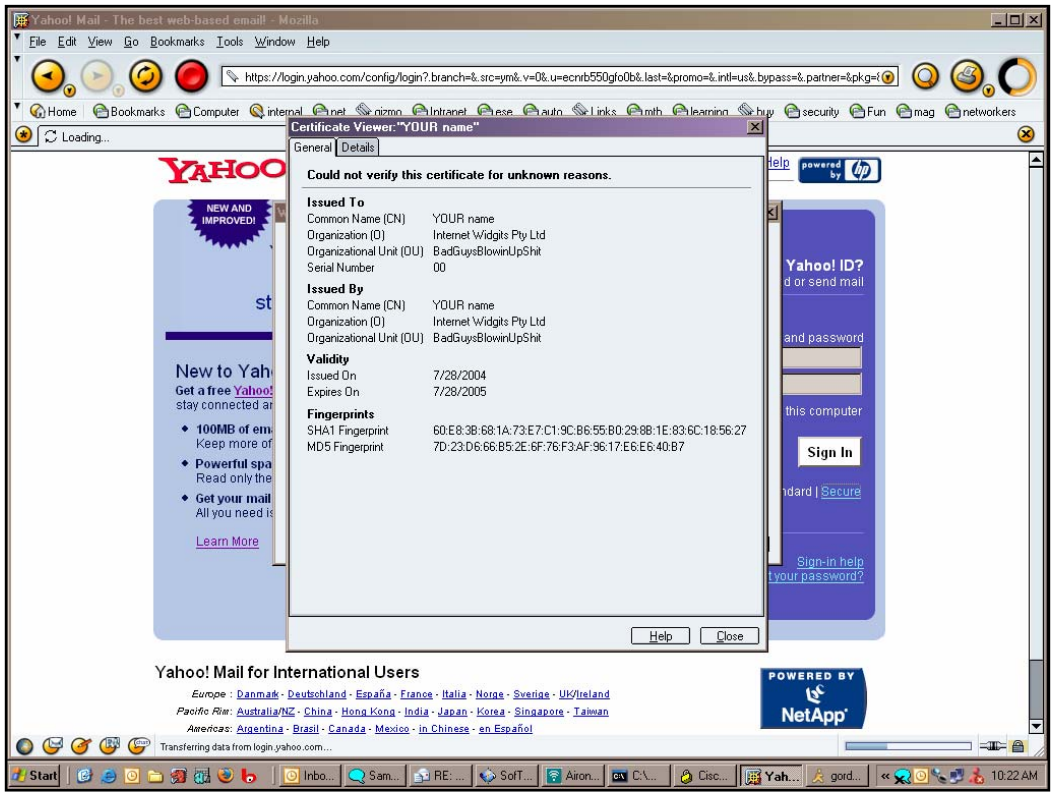
ARP Attack Tools

- Ettercap in action
- As you can see runs in Window, Linux, Mac
- Decodes passwords on the fly
- This example, telnet username/ password is captured



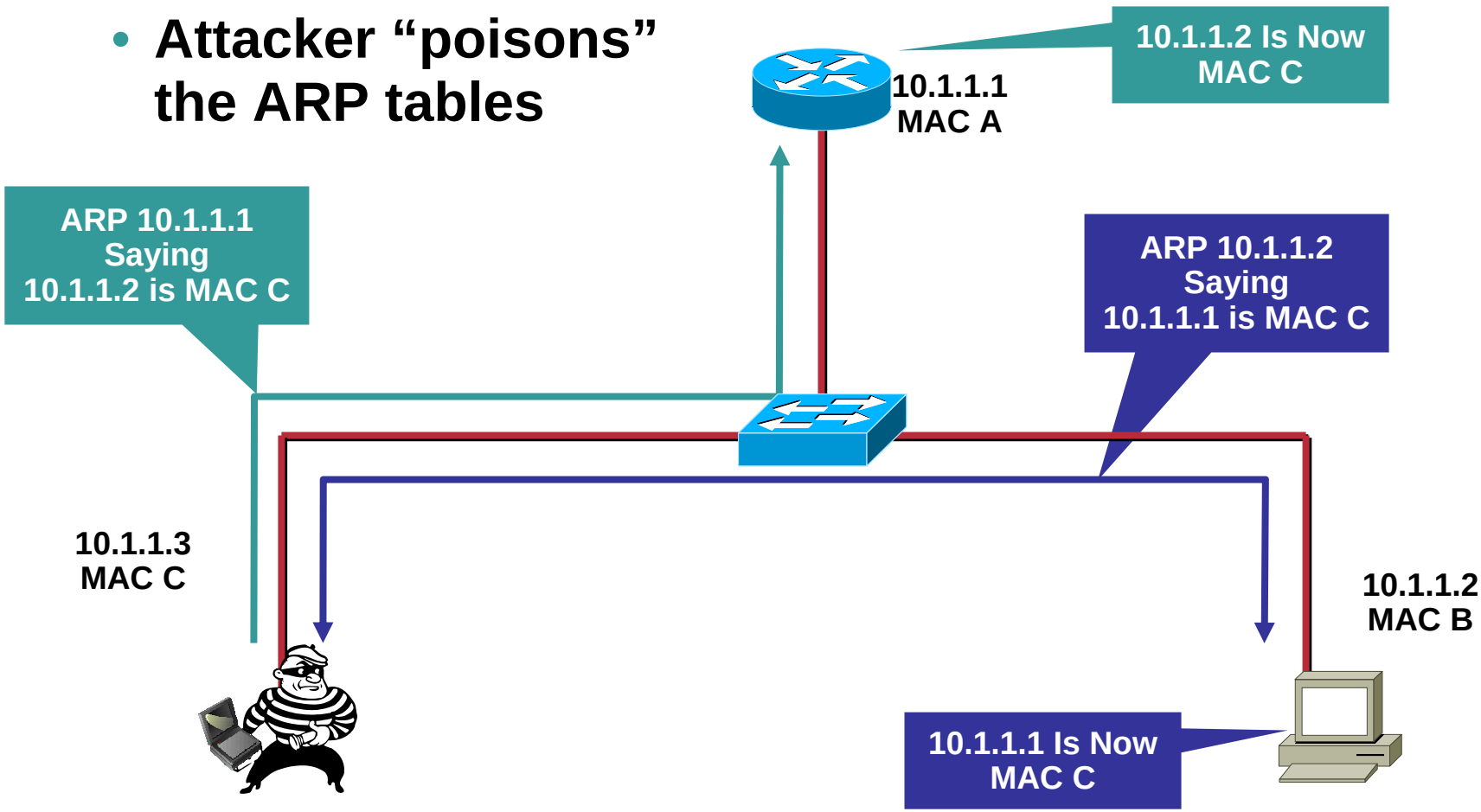
ARP Attack Tools: SSH/SSL

- **Using these tools SSL/SSH sessions can be intercepted and bogus certificate credentials can be presented**
- **Once you have accepted the certificate, all SSL/SSH traffic for all SSL/SSH sites can flow through the attacker**



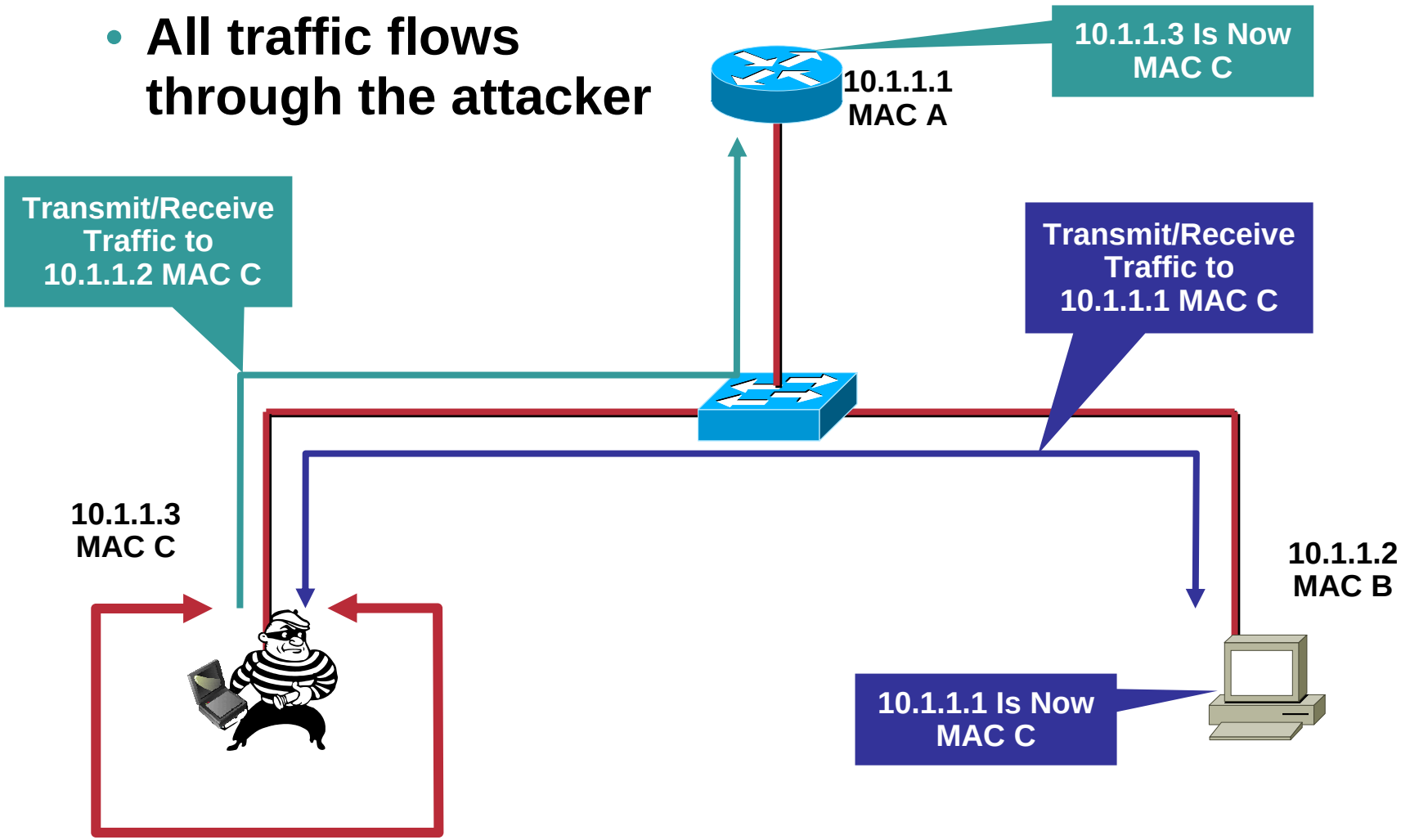
ARP Attack in Action

- Attacker "poisons" the ARP tables



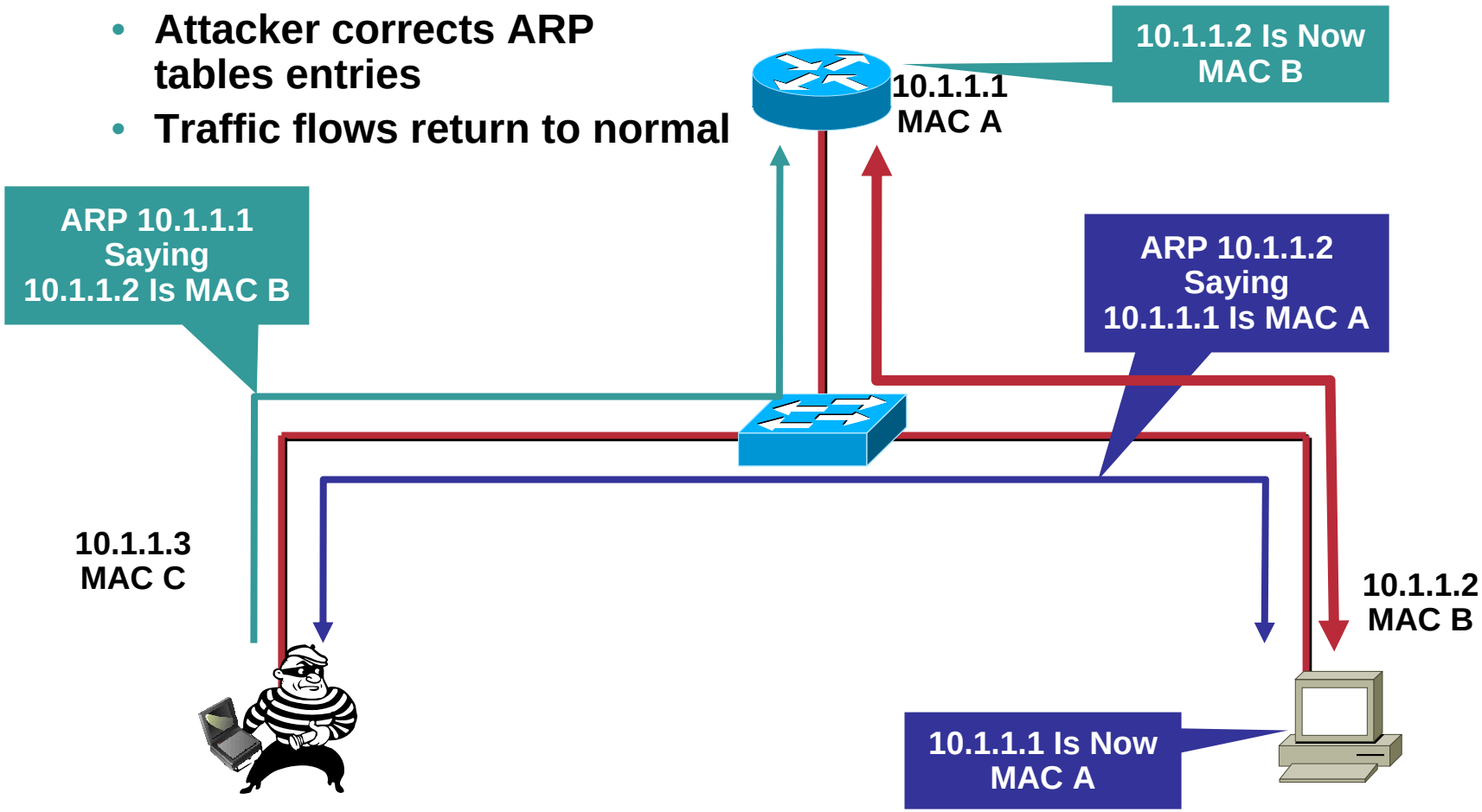
ARP Attack in Action

- All traffic flows through the attacker

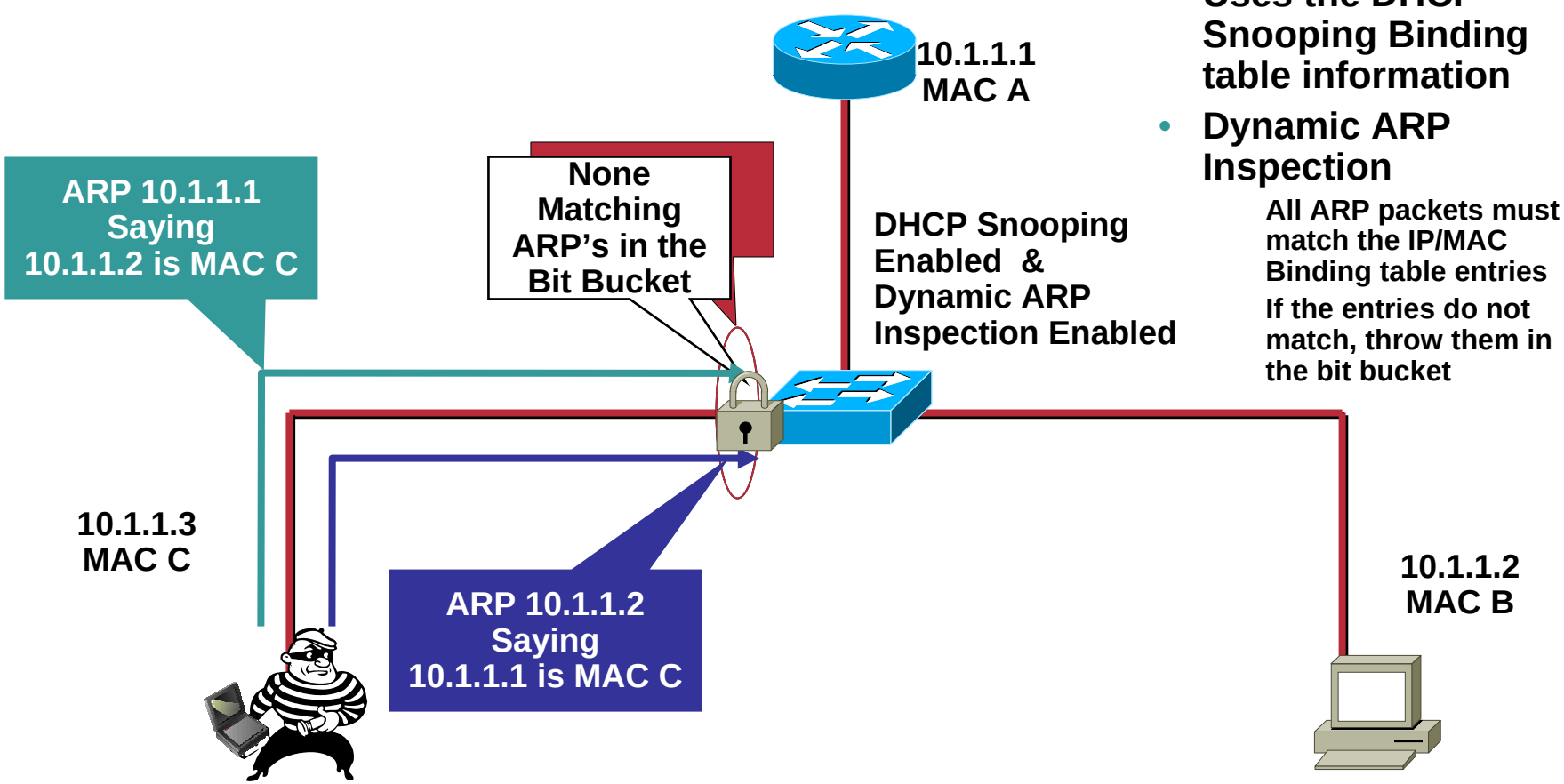


ARP Attack Clean Up

- Attacker corrects ARP tables entries
- Traffic flows return to normal



Countermeasures to ARP Attacks: Dynamic ARP Inspection



- Uses the DHCP Snooping Binding table information
- Dynamic ARP Inspection
  - All ARP packets must match the IP/MAC Binding table entries
  - If the entries do not match, throw them in the bit bucket

Countermeasures to ARP Attacks: Dynamic ARP Inspection

- **Uses the information from the DHCP Snooping Binding table**

```
sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:03:47:B5:9F:AD	10.120.4.10	193185	dhcp-snooping	4	FastEthernet3/18
00:03:47:c4:6f:83	10.120.4.11	213454	dhcp-snooping	4	FastEthermet3/21

- **Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, it not, traffic is blocked**

Countermeasures to ARP Attacks: Dynamic ARP Inspection

Configuration of Dynamic ARP Inspection (DAI)

- DHCP Snooping had to be configured so the binding table it built
- DAI is configured by VLAN
- You can trust an interface like DHCP Snooping
- Be careful with rate limiting—varies between platforms
- Suggested for voice is to set the rate limit above the default if you feel dial tone is important

Countermeasures to ARP Attacks: Dynamic ARP Inspection

Dynamic ARP Inspection Commands

IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
ip arp inspection vlan 4,104
ip arp inspection log-buffer entries 1024
ip arp inspection log-buffer logs 1024 interval 10
Interface Commands
ip dhcp snooping trust
ip arp inspection trust

IOS
Interface Commands
no ip arp inspection trust
(default)
ip arp inspection limit rate 15
(pps)

Countermeasures to ARP Attacks: Dynamic ARP Inspection

Error Messages in Show Log

```
sh log:
4w6d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 296 milliseconds on Gi3/2.
4w6d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/2, putting Gi3/2 in err-disable state
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.2/12:19:27 UTC Wed Apr 19 2000])
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.3/12:19:27 UTC Wed Apr 19 2000])
```

Non DHCP Devices

- **Can use Static bindings in the DHCP Snooping Binding table**

IOS
Global Commands
ip source binding 0000.0000.0001 vlan 4 10.0.10.200 interface fastethernet 3/1

- **Show static and dynamic entries in the DHCP Snooping Binding table is different**

IOS
Show Commands
show ip source binding

Binding Table Info

- No entry in the binding table—no traffic!
- Wait until all devices have new leases before turning on Dynamic ARP Inspection
- Entrees stay in table until the lease runs out
- All switches have a binding size limit
  - 3000 switches—1,000 entrees
  - 4000 switches—2,000 entrees (6000 for the SupV-10GE)
  - 6000 switches—16,000 entrees

Summary of ARP Attacks

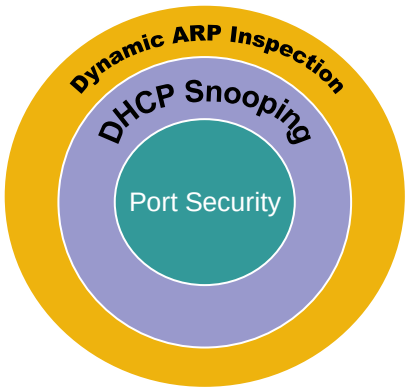
- Dynamic ARP Inspection prevents ARP attacks by intercepting all ARP requests and responses
- DHCP Snooping must be configured first, otherwise there is no binding table for dynamic ARP Inspection to use
- The DHCP Snooping table is built from the DHCP request, but you can put in static entries

  If you have a device that does not DHCP, but you would like to turn on Dynamic ARP Inspection, you would need a static entry in the table

More ARP Attack Information

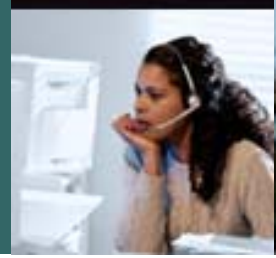
- Some IDS systems will watch for an unusually high amount of ARP traffic
- ARPWatch is freely available tool to track IP/MAC address pairings
  - Caution—you will need an ARPWatch server on every VLAN
  - Hard to manage and scale
  - You can still do static ARP for critical routers and hosts (administrative pain)

Building the Layers



- **Port security prevents CAM attacks and DHCP Starvation attacks**
- **DHCP snooping prevents rogue DHCP server attacks**
- **Dynamic ARP inspection prevents current ARP attacks**

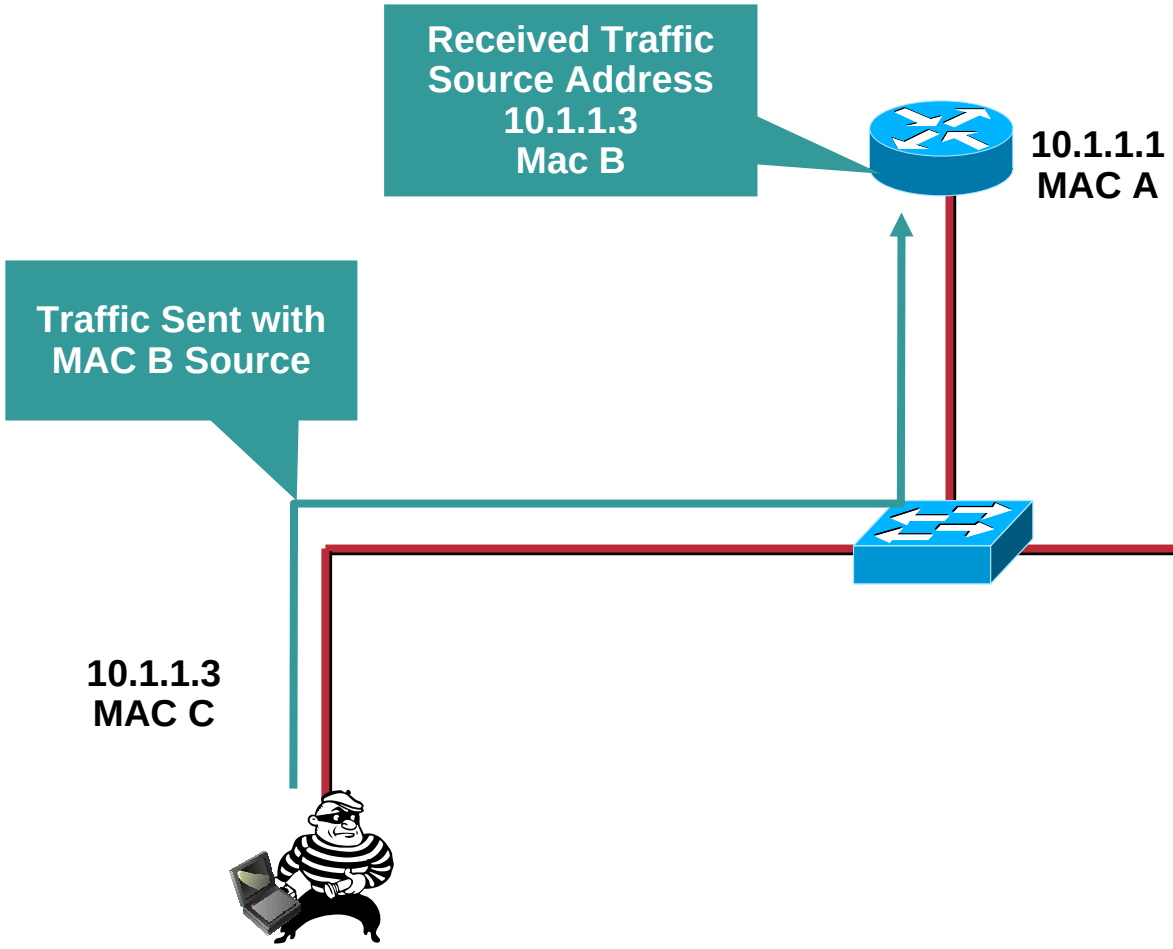
ATTACKS AND COUNTERMEASURES: SPOOFING ATTACKS



Spoofing Attacks

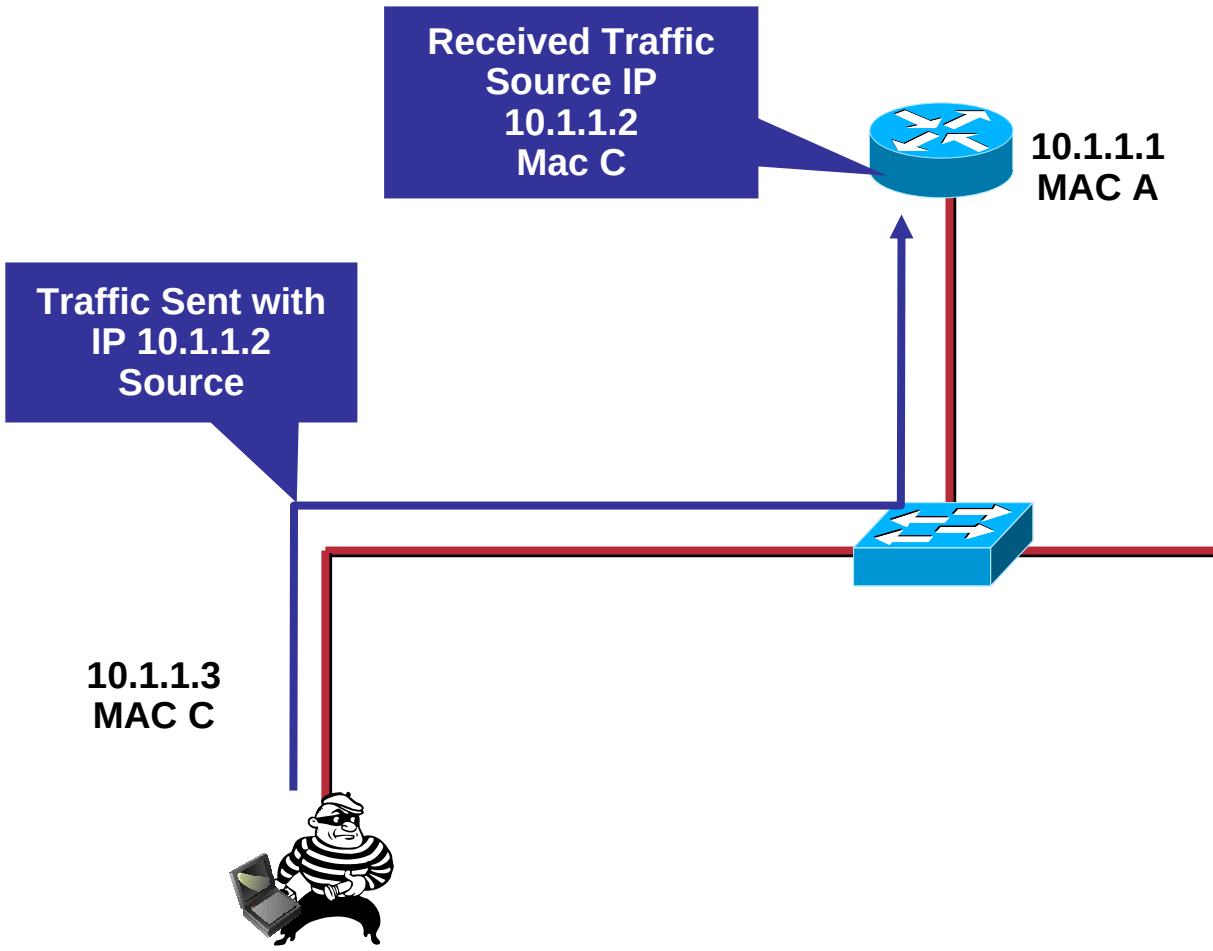
- **MAC spoofing**
  - **If MACs are used for network access an attacker can gain access to the network**
  - **Also can be used to take over someone's identity already on the network**
- **IP spoofing**
  - **Ping of death**
  - **ICMP unreachable storm**
  - **SYN flood**
  - **Trusted IP addresses can be spoofed**

Spoofing Attack: MAC



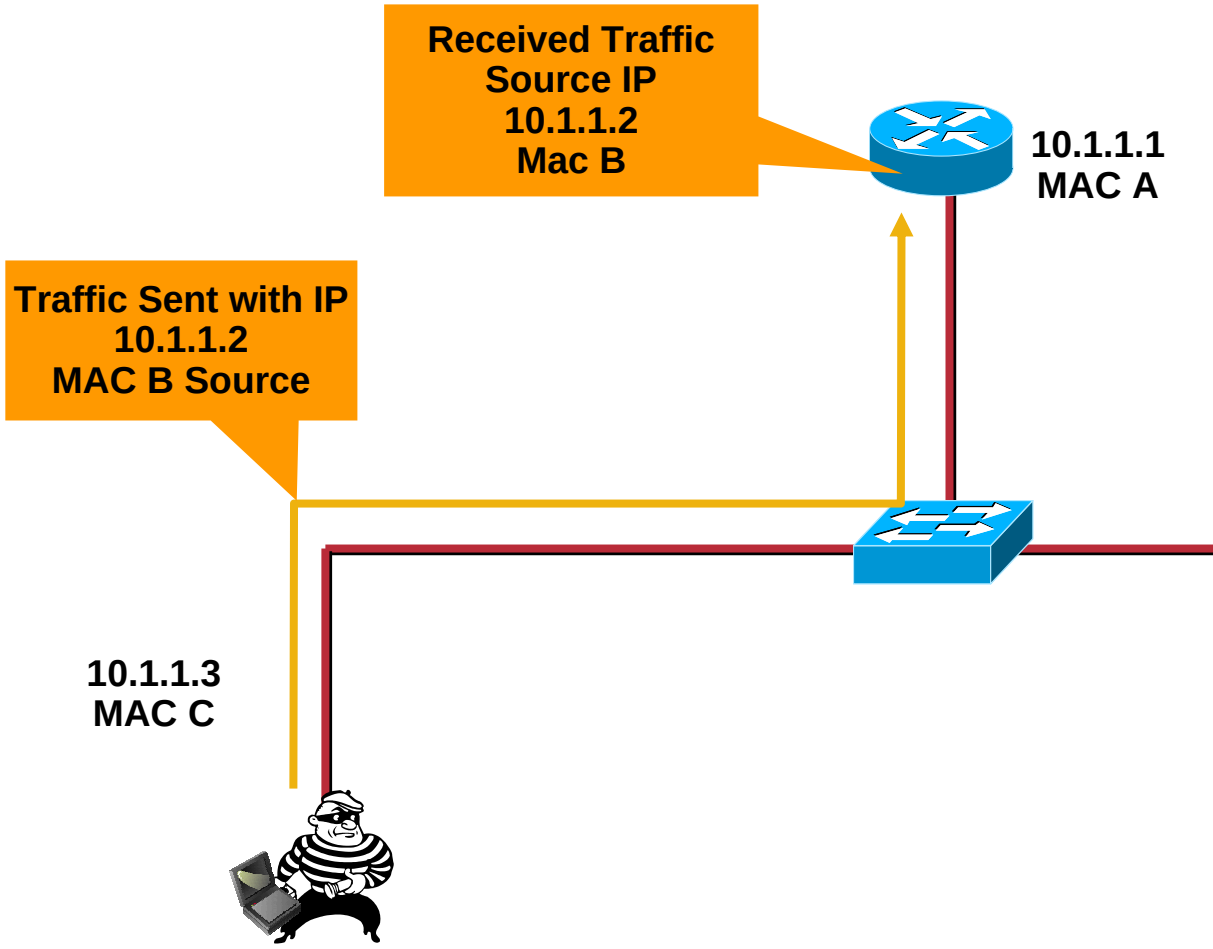
- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

Spoofing Attack: IP



- Attacker sends packets with the incorrect source IP Address
- Whatever device the packet is sent to will never reply to the attacker

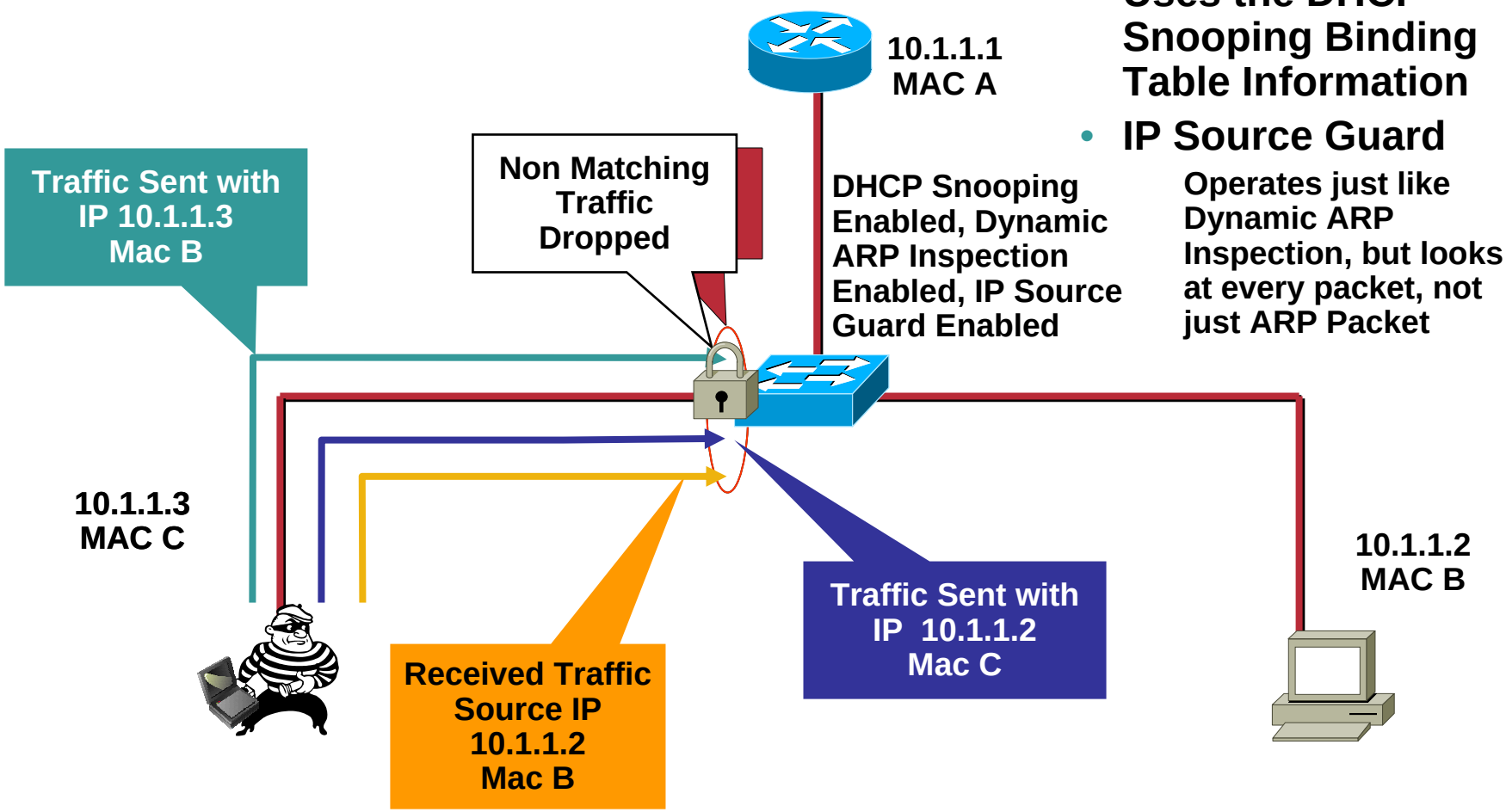
Spoofing Attack: IP/MAC



- Attacker sends packets with the incorrect source IP and MAC address
- Now looks like a device that is already on the network

Countermeasures to Spoofing Attacks: IP Source Guard

- Uses the DHCP Snooping Binding Table Information
- IP Source Guard
  - Operates just like Dynamic ARP Inspection, but looks at every packet, not just ARP Packet



Countermeasures to Spoofing Attacks: IP Source Guard

- **Uses the information from the DHCP Snooping Binding table**

```
sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10      193185      dhcp-snooping  4     FastEthernet3/18
00:03:47:c4:6f:83   10.120.4.11      213454      dhcp-snooping  4     FastEthermet3/21
```

- **Looks at the MacAddress and IpAddress fields to see if the traffic from the interface is in the binding table, it not, traffic is blocked**

Countermeasures to Spoofing Attacks: IP Source Guard

Configuration of IP Source Guard

- DHCP Snooping had to be configured so the binding table it built
- IP Source Guard is configured by port
- IP Source Guard with MAC does not learn the MAC from the device connected to the switch, it learns it from the DHCP Offer
- MAC and IP checking can be turned on separately or together

  For IP—

  Will work with the information in the binding table

  For MAC—

  Must have an Option 82 enabled DHCP server (Microsoft does not support option 82)

  Have to Change all router configuration to support Option 82

  All Layer 3 devices between the DHCP request and the DHCP server will need to be configured to trust the Option 82 DHCP Request—ip dhcp relay information trust

Note: There are at least two DHCP servers that support Option 82 Field Cisco Network Registrar® and Avaya

Countermeasures to Spoofing Attacks: IP Source Guard

IP Source Guard

IP Source Guard Configuration IP/MAC Checking Only (Opt 82)

IOS
Global Commands
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping
port-security

IP Source Guard Configuration IP Checking Only (no Opt 82)

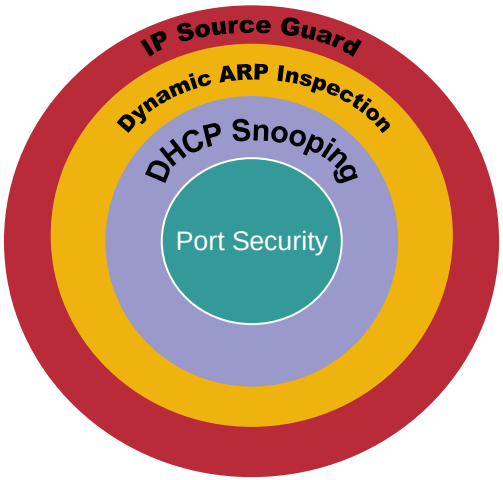
IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping

IP Source Guard vs. DAI

While IP Source Guard and Dynamic ARP Inspection offer similar functions, they are different in the way they operate and facilitate protection …

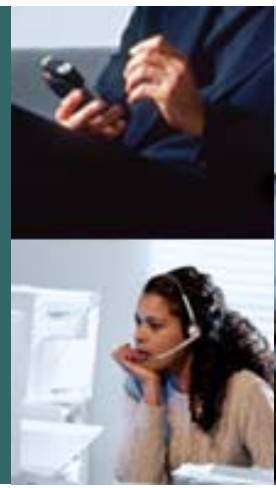
Dynamic ARP Inspection	IP Source Guard
- DHCP Snooping creates IP to MAC bindings - DAI Intercepts all ARP requests - Intercepted ARP is validated against IP to MAC binding - Does not switch ARP packets with invalid source address - Used primarily to prevent MITM attacks	- Initially all traffic blocked - Snoops DHCP Address - Creates IP to MAC binding - Installs per port VACL to deny traffic other than snooped source - Protects against IP and MAC spoofing - Will not prevent a MITM attack
Dynamic ARP Inspection	IP Source Guard

Building the Layers

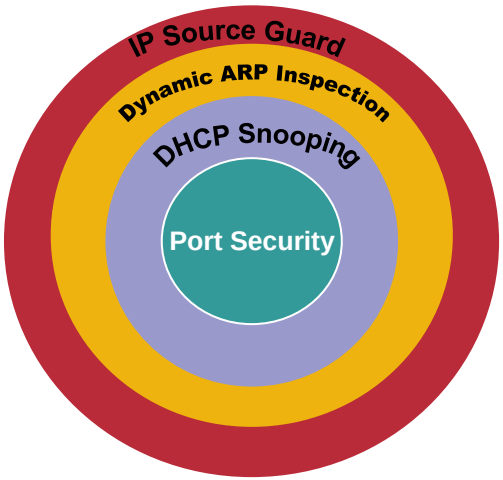


- **Port security prevents CAM attacks and DHCP Starvation attacks**
- **DHCP Snooping prevents Rogue DHCP Server attacks**
- **Dynamic ARP Inspection prevents current ARP attacks**
- **IP source guard prevents IP/MAC Spoofing**

SUMMARY



Building the Layers



- Port Security prevents CAM attacks
- DHCP Snooping prevents Rogue DHCP Server attacks
- Dynamic ARP Inspection prevents current ARP attacks
- IP Source Guard prevents IP/MAC Spoofing

Best Practices for L2 Security

Cisco.com

1. Always use a dedicated VLAN ID for Trunk Ports
2. Disable unused ports and put them in an unused VLAN
3. Use Secure Transmission when managing Switches (SSH, OOB, Permit Lists)
4. Deploy Port Security
5. Set all host ports to Non Trunking (unless you are Cisco VoIP)
6. ALWAYS use a dedicated VLAN for Trunk Ports
7. Avoid using VLAN 1
8. Have a plan for ARP Security issues and implement it! (ARP Inspection, IDS, etc.)
9. Use SNMP V3 to secure SNMP transmission
10. Use STP Attack mitigation – Root Guard and BPDU Guard
11. Use CDP only where necessary
12. Use MD5 Authentication for VTP
13. Plan & implement DHCP Attack mitigation (DHCP Snooping, VACLs)
14. Use Private VLAN's to better secure guest VLAN's
15. Use and implement 802.1x (IBNS) to protect entry into your network
16. Consider using VACL's to limit access to key network resources…