LAYER 2 ATTACKS & MITIGATION TECHNIQUES

Yusuf Bhaiji
Cisco Systems

Agenda

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

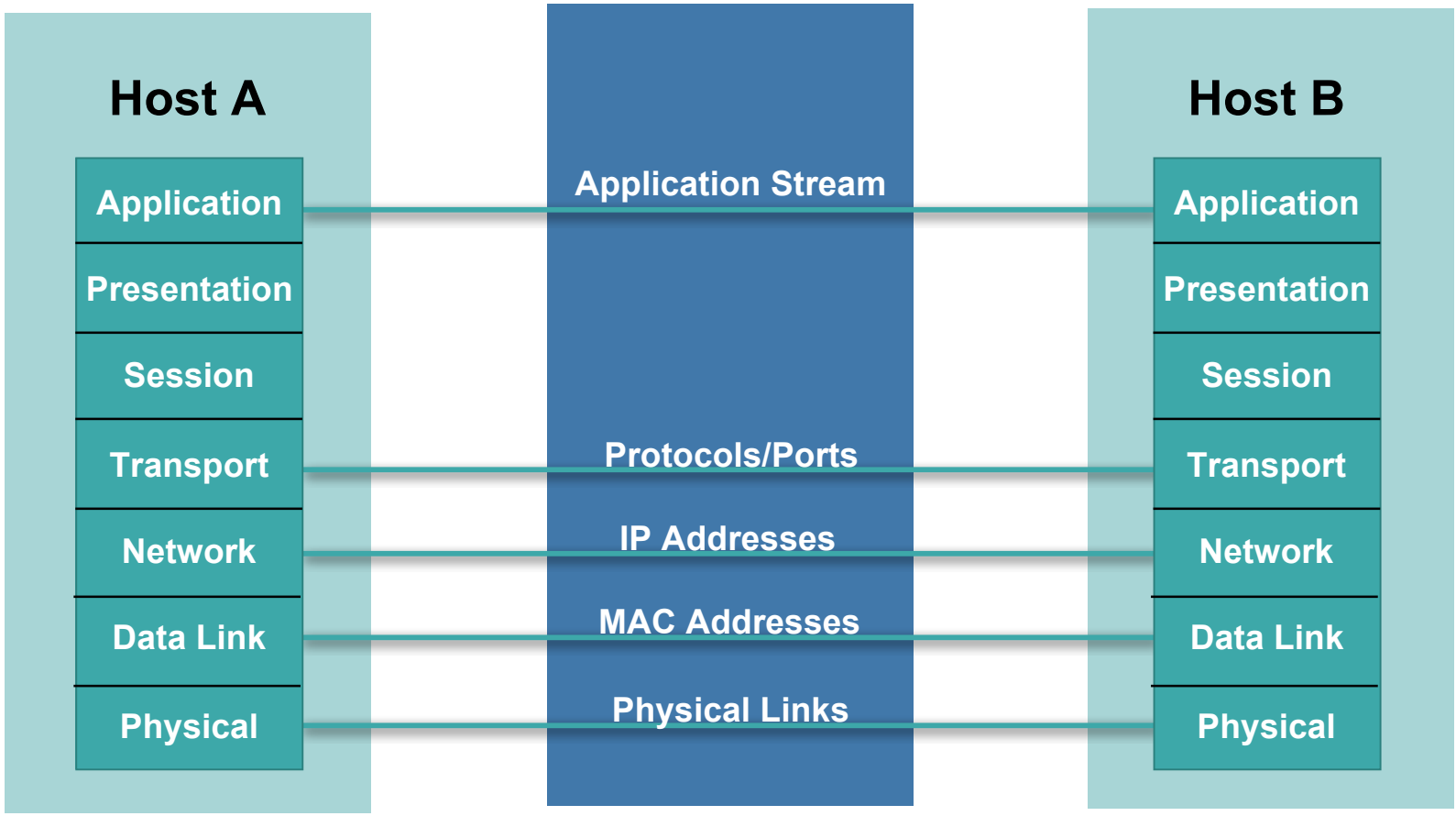
Caveats

- 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
- All testing was done on Cisco Ethernet Switches
  - 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

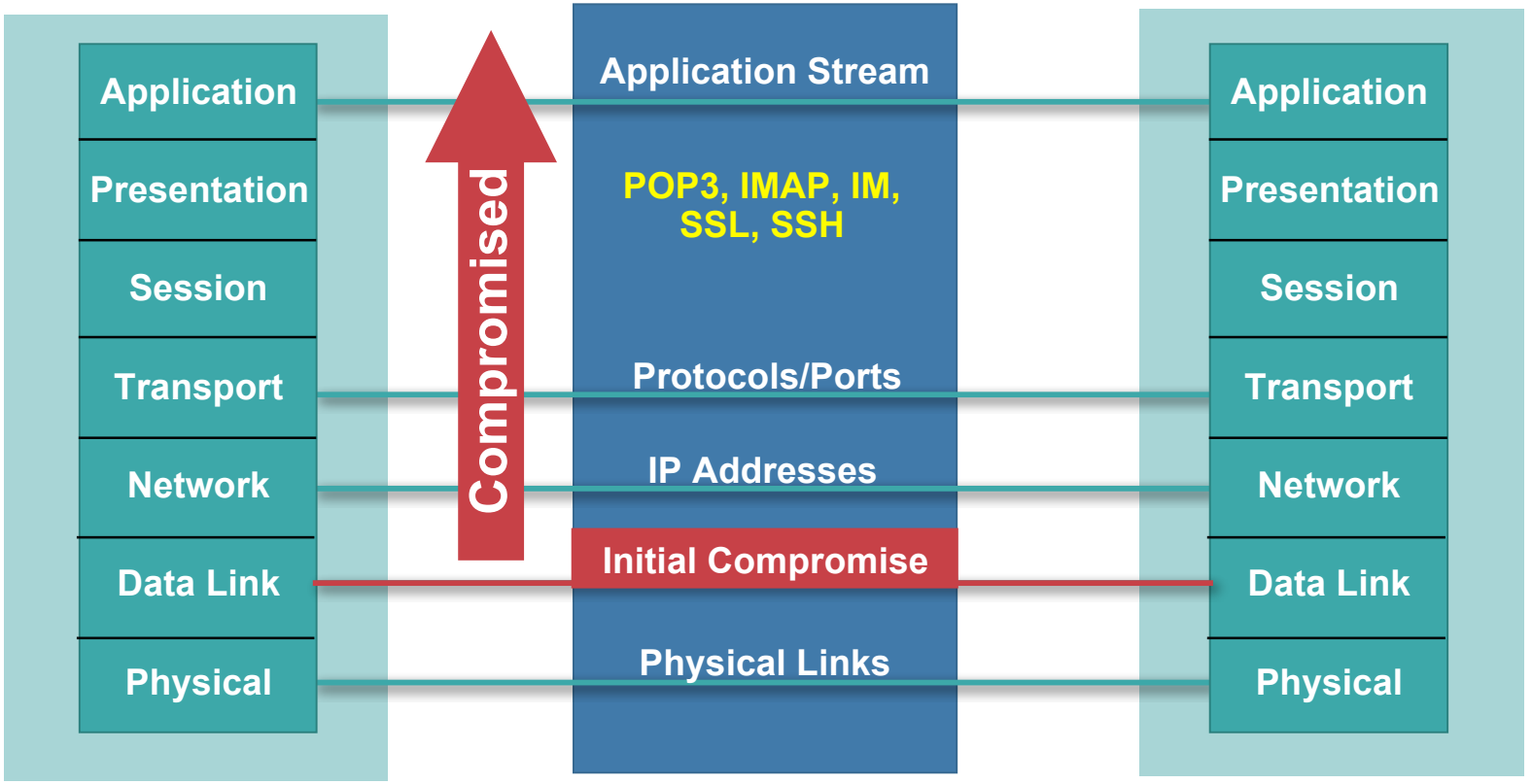
Why Worry About Layer 2 Security?

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

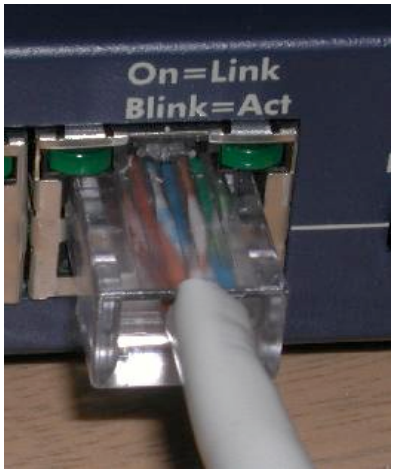


NetOPS/SecOPS, Whose Problem Is It?

Questions:	Most NetOPS	Most SecOPS
• What is your stance on L2 security issues?	• There are L2 security issues?	• I handle security issues at L3 and above
• Do you use VLANs often?	• I use VLANs all the time	• I have no idea if we are using VLANs
• Do you ever put different security levels on the same switch using VLANs?	• Routing in and out of the same switch is OK by me! That's what VLANs are for	• Why would I care what the network guy does with the switch?
• What is the process for allocating addresses for segments?	• The security guy asks me for a new segment, I create a VLAN and assign him an address space	• I ask NetOPs for a segment, they give me ports and addresses

FBI/CSI Risk Assessment*

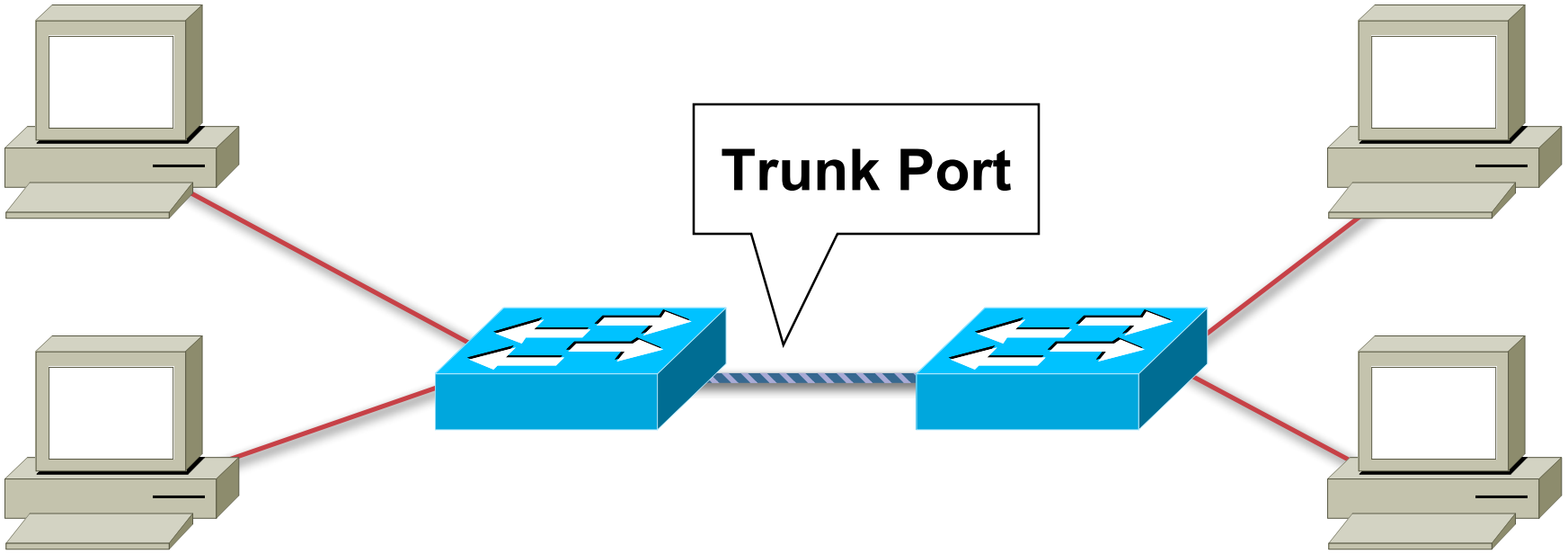
- 99% of all enterprises network ports are OPEN
- Usually any laptop can plug into the network and gain access to the network
- Of companies surveyed total loss was over 141 million
- An average of 11.4 million per incident
- Insider attack by disgruntled employees was listed as likely source by 59%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



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

ATTACKS AND COUNTERMEASURES: VLAN HOPPING ATTACKS

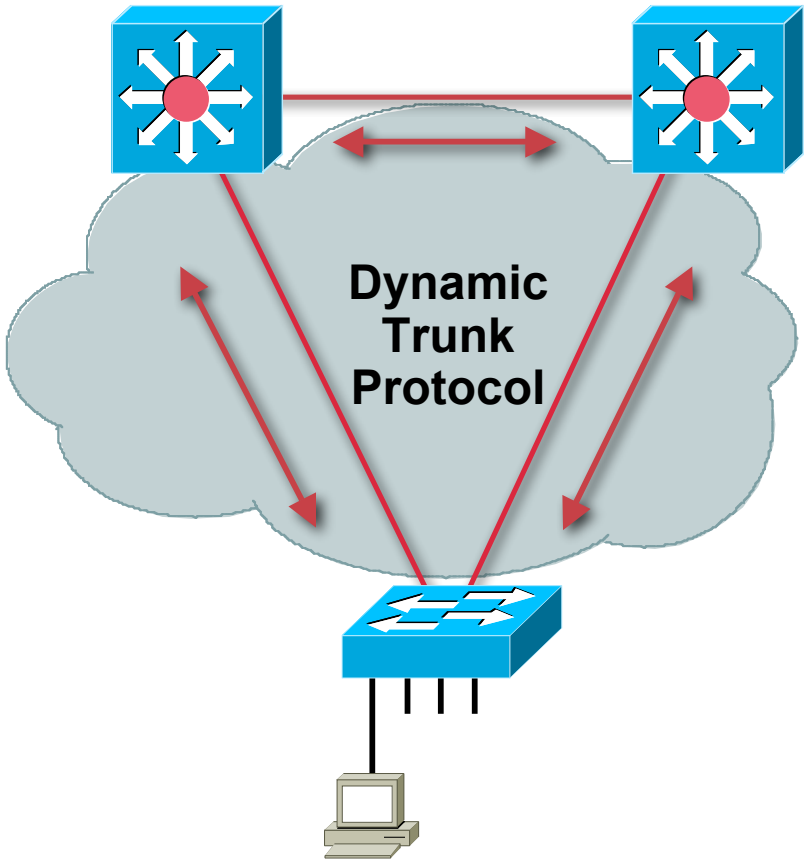
Basic Trunk Port Defined



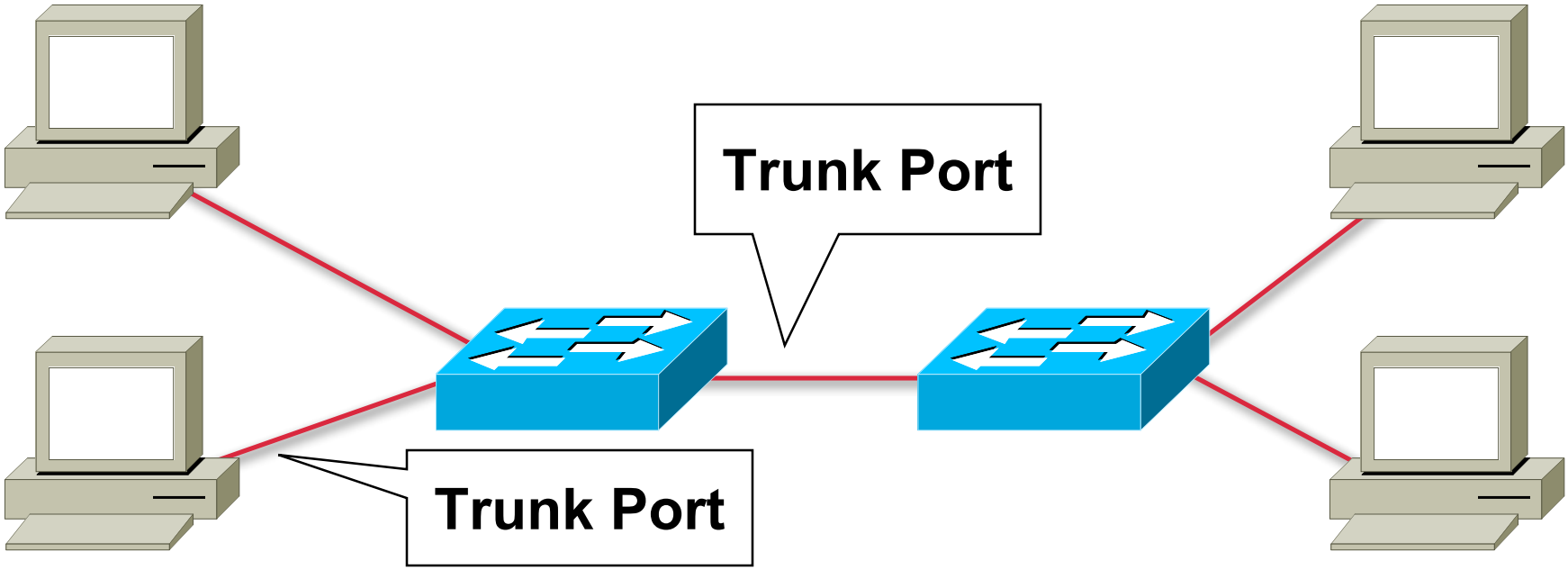
- Trunk ports have access to all VLANS by default
- Used to route traffic for multiple VLANS across the same physical link (generally between switches or phones)
- Encapsulation can be 802.1q or ISL

Dynamic Trunk Protocol (DTP)

- **What is DTP?**
  - **Automates 802.1x/ISL Trunk configuration**
  - **Operates between switches (Cisco IP phone is a switch)**
  - **Does not operate on routers**
  - **Support varies, check your device**
- **DTP synchronizes the trunking mode on end links**
- **DTP state on 802.1q/ISL trunking port can be set to "Auto", "On", "Off", "Desirable", or "Non-Negotiate"**

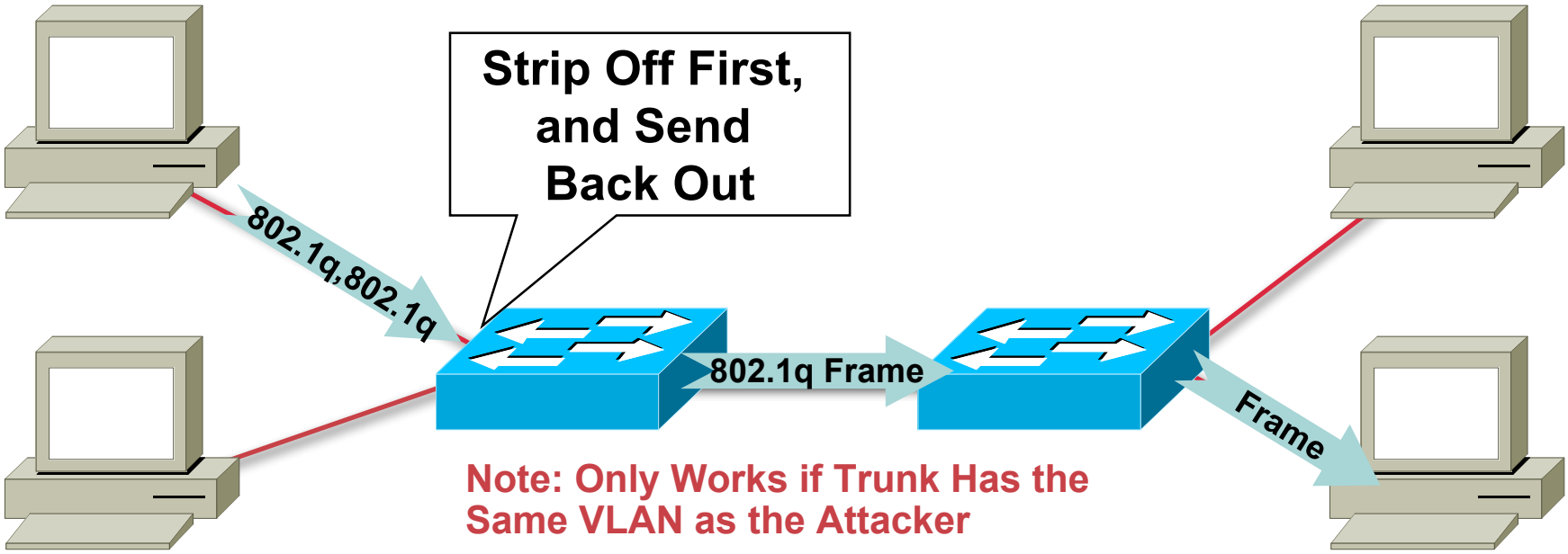


Basic VLAN Hopping Attack



- An end station can spoof as a switch with ISL or 802.1q
- The station is then a member of all VLANs
- Requires a trunking configuration of the Native VLAN to be VLAN 1

Double 802.1q Encapsulation VLAN Hopping Attack



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

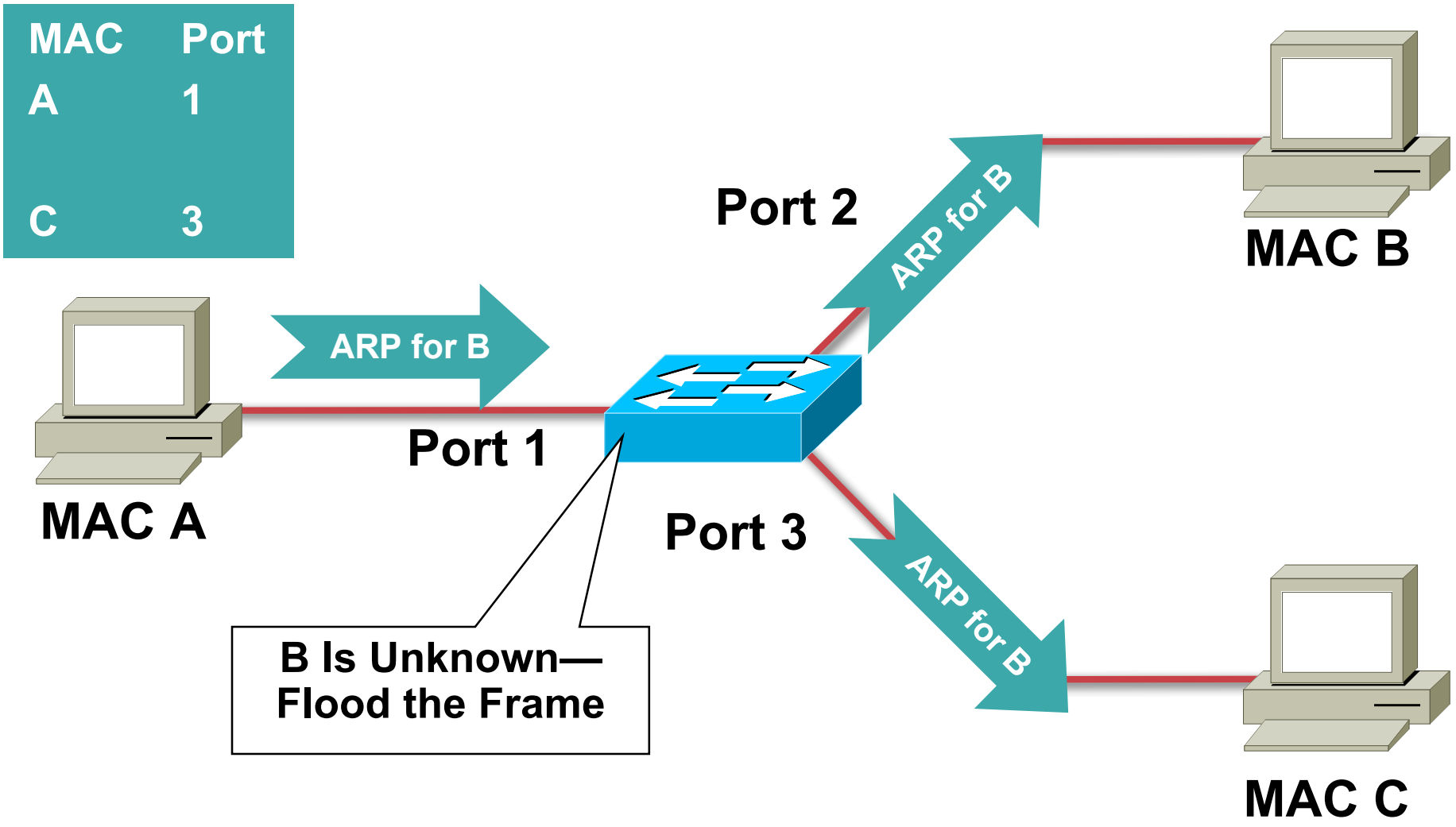
0000.0cXX.XXXX

All F's = Broadcast

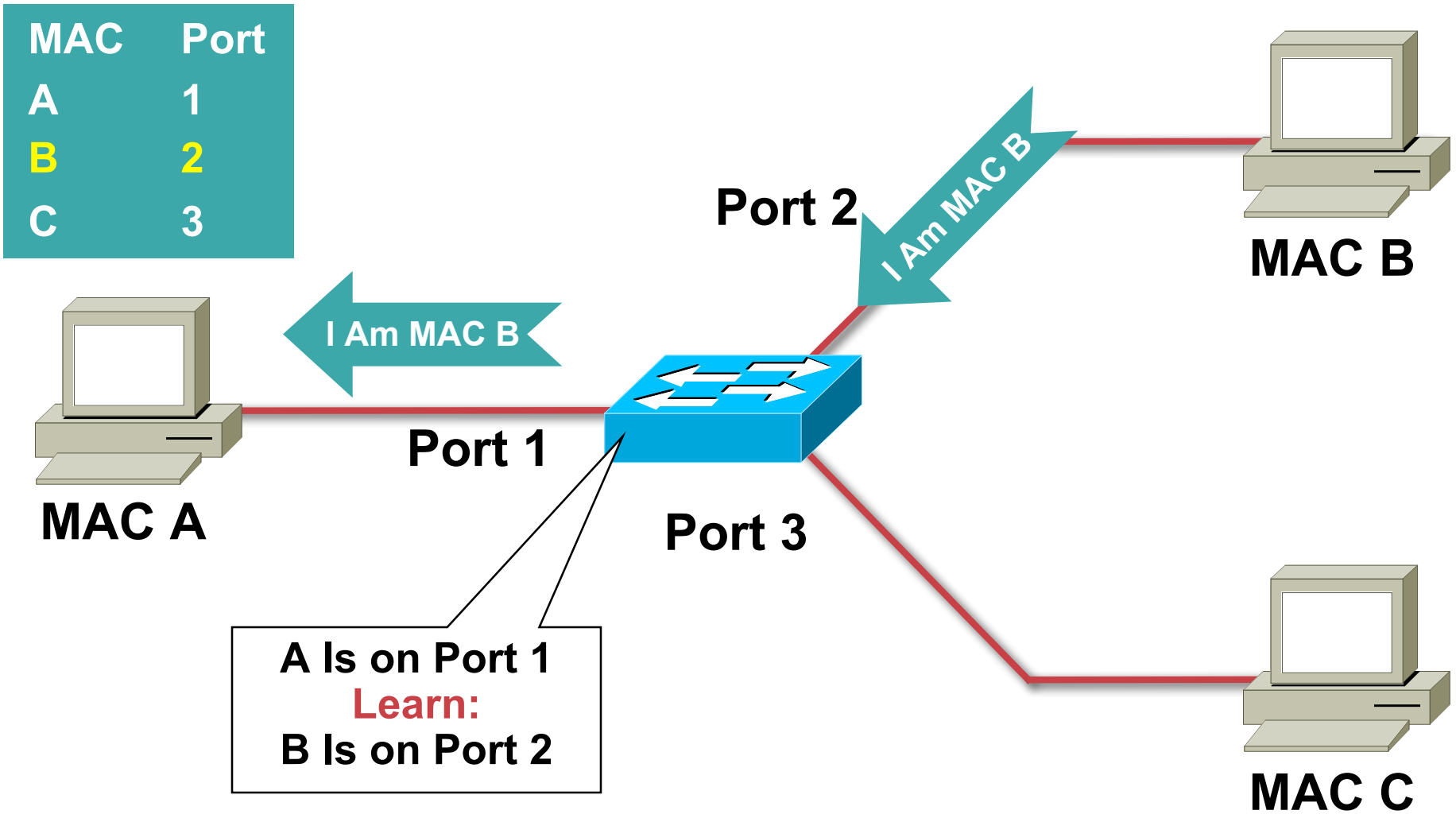
FFFF.FFFF.FFFF

- **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**

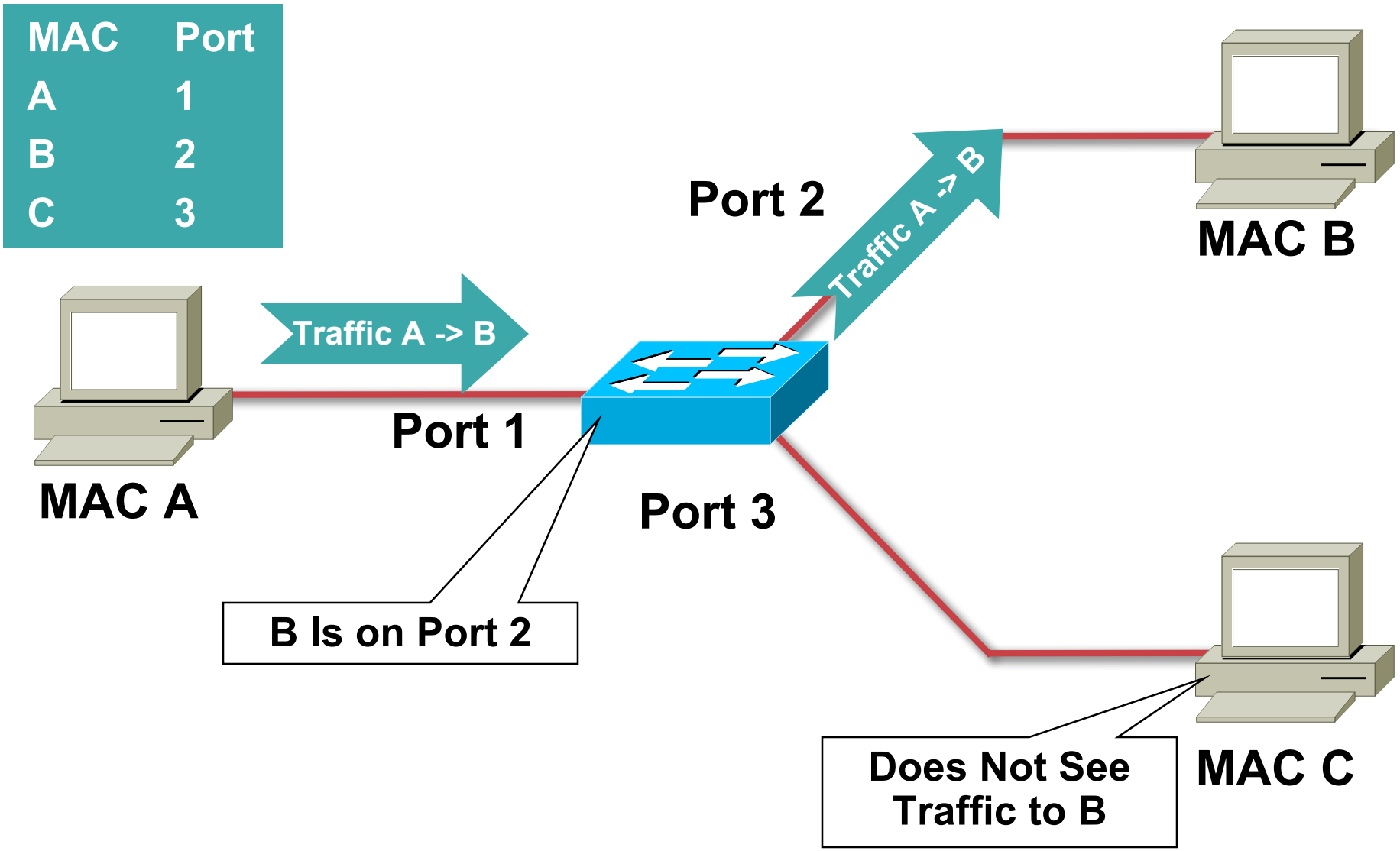
Normal CAM Behavior 1/3



Normal CAM Behavior 2/3



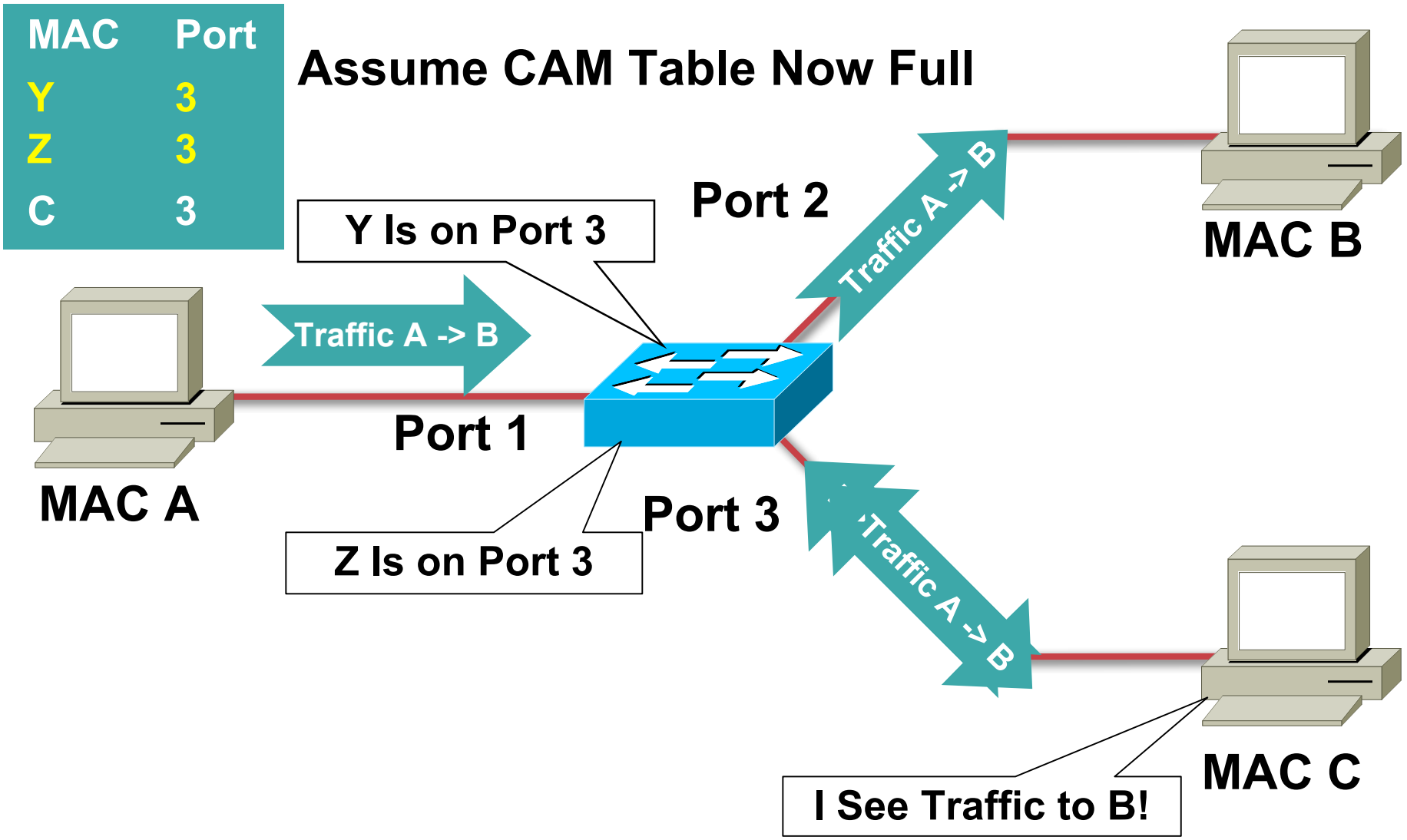
Normal CAM Behavior 3/3



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 Flooding Switches with macof


```
macof –i eth1
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
```

- **Macof sends random source MAC and IP addresses**
- **Much more aggressive if you run the command**

  “macof -i eth1 2> /dev/null”

  macof (part of dsniff)—http://monkey.org/~dugsong/dsniff/

CAM Table Sizes

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

  3xxx—16,000

  4xxx—32,000

  6xxx—128,000

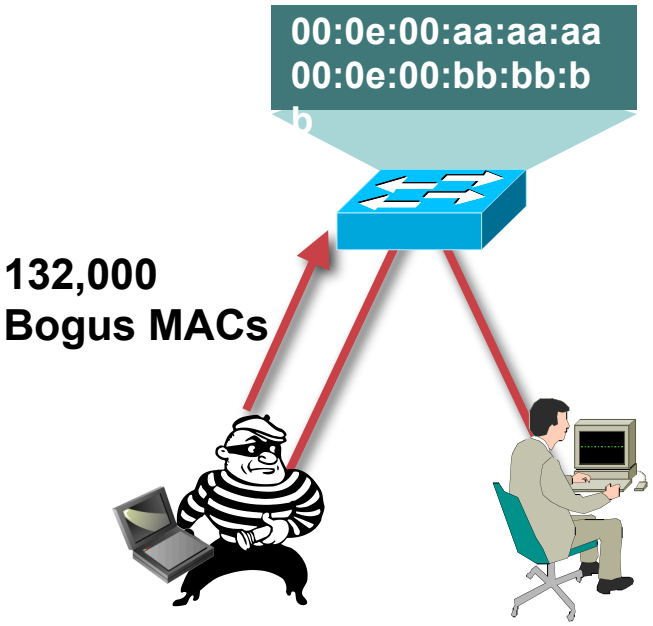
CAM Table FULL!

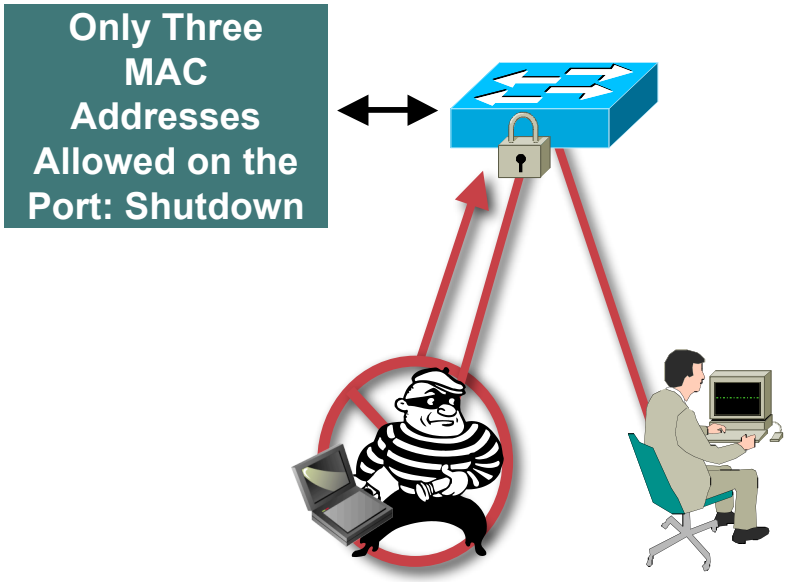
- Once the CAM table on the switch is full, traffic without a CAM entry is flooded out every port on that VLAN
- This will turn a VLAN on a switch basically into a hub
- This attack will also fill the CAM tables of adjacent switches

```
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

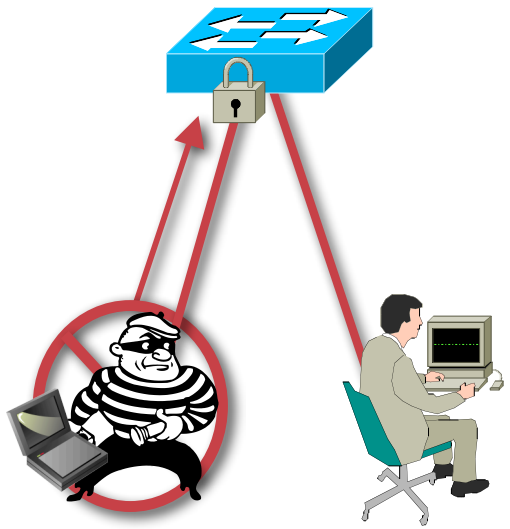




Solution:

- **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)

Port Security: What to Expect

Notice: When Using the Restrict Feature of Port Security, if the Switch Is Under Attack, You Will See a Performance Hit on the CPU

- The performance hit seen with multiple attacks happening at one time is up to 99% CPU utilization
- Because the process is a low priority, on all switches packets were not dropped
- Telnet and management were still available
- Voice MOS scores under attack were very good, as long as QoS was configured

MOS—Mean Opinion Score—
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci786677,00.html

Building the Layers

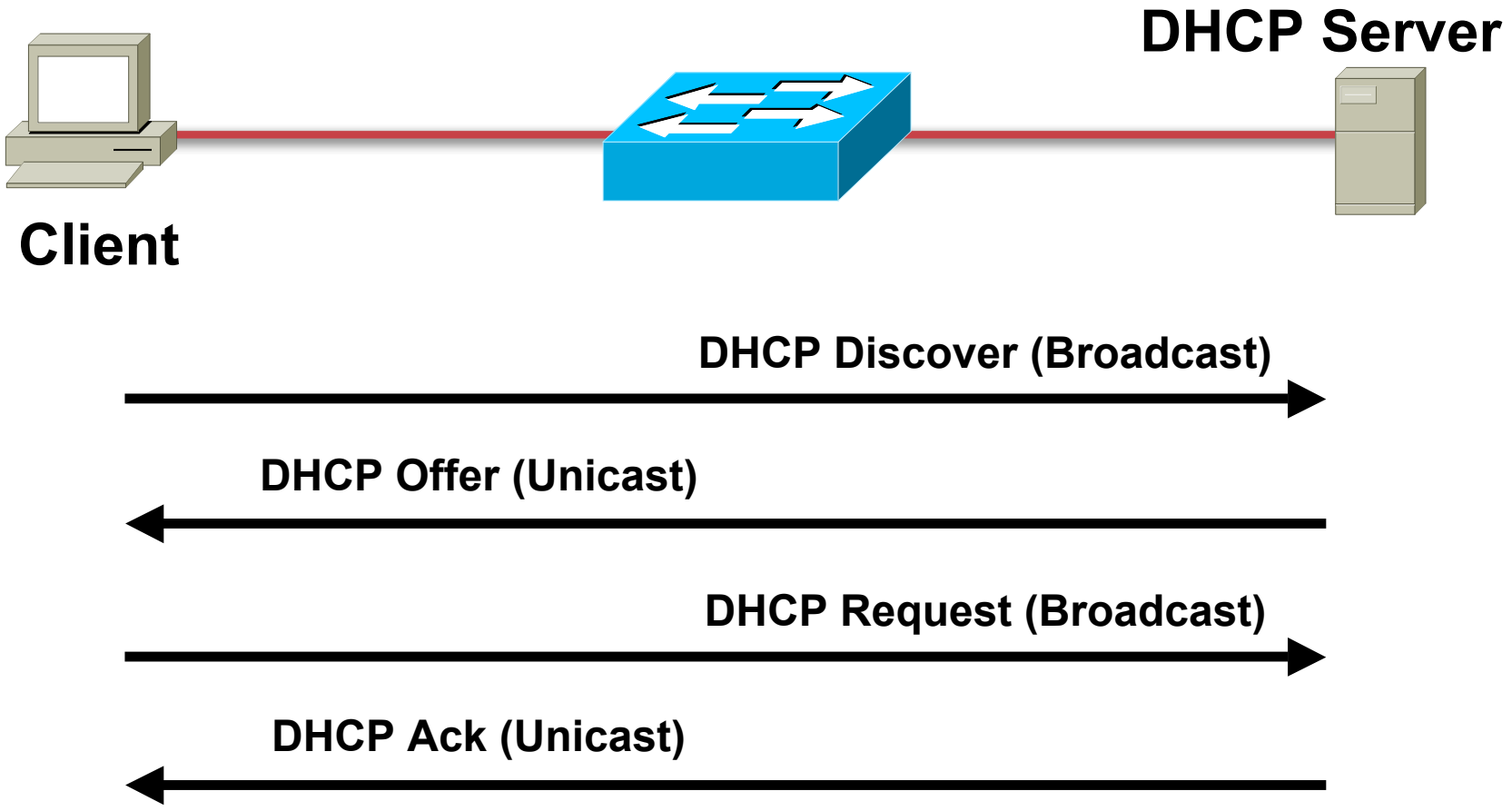
- **Port Security prevents CAM attacks and DHCP starvation attacks**

ATTACKS AND COUNTERMEASURES: DHCP ATTACKS

DHCP Function: High Level

- Server dynamically assigns IP address on demand
- Administrator creates pools of addresses available for assignment
- Address is assigned with lease time
- DHCP delivers other configuration information in options

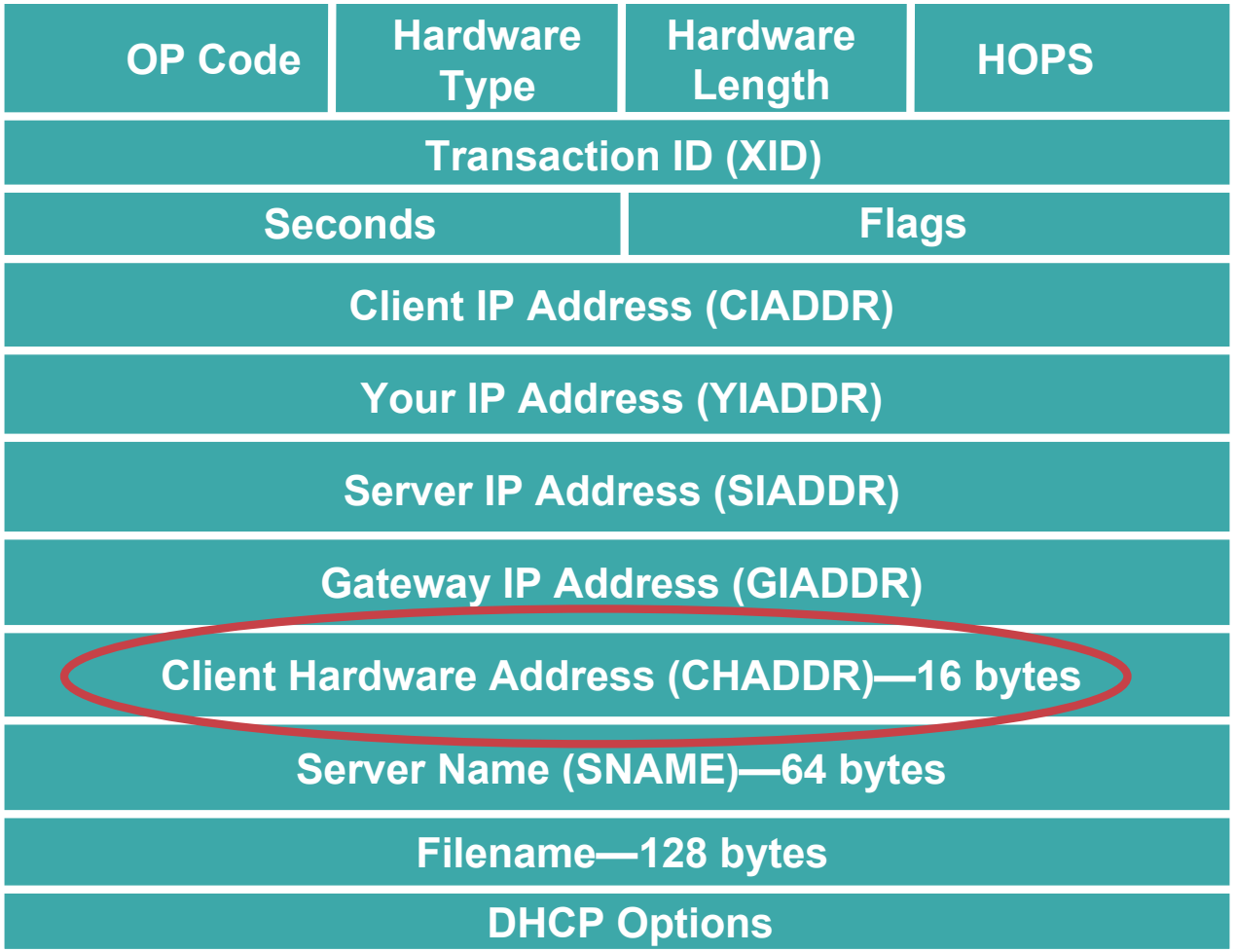
DHCP Function: Lower Level



- DHCP defined by RFC 2131

DHCP Function: Lower Level

IPv4 DHCP Packet Format

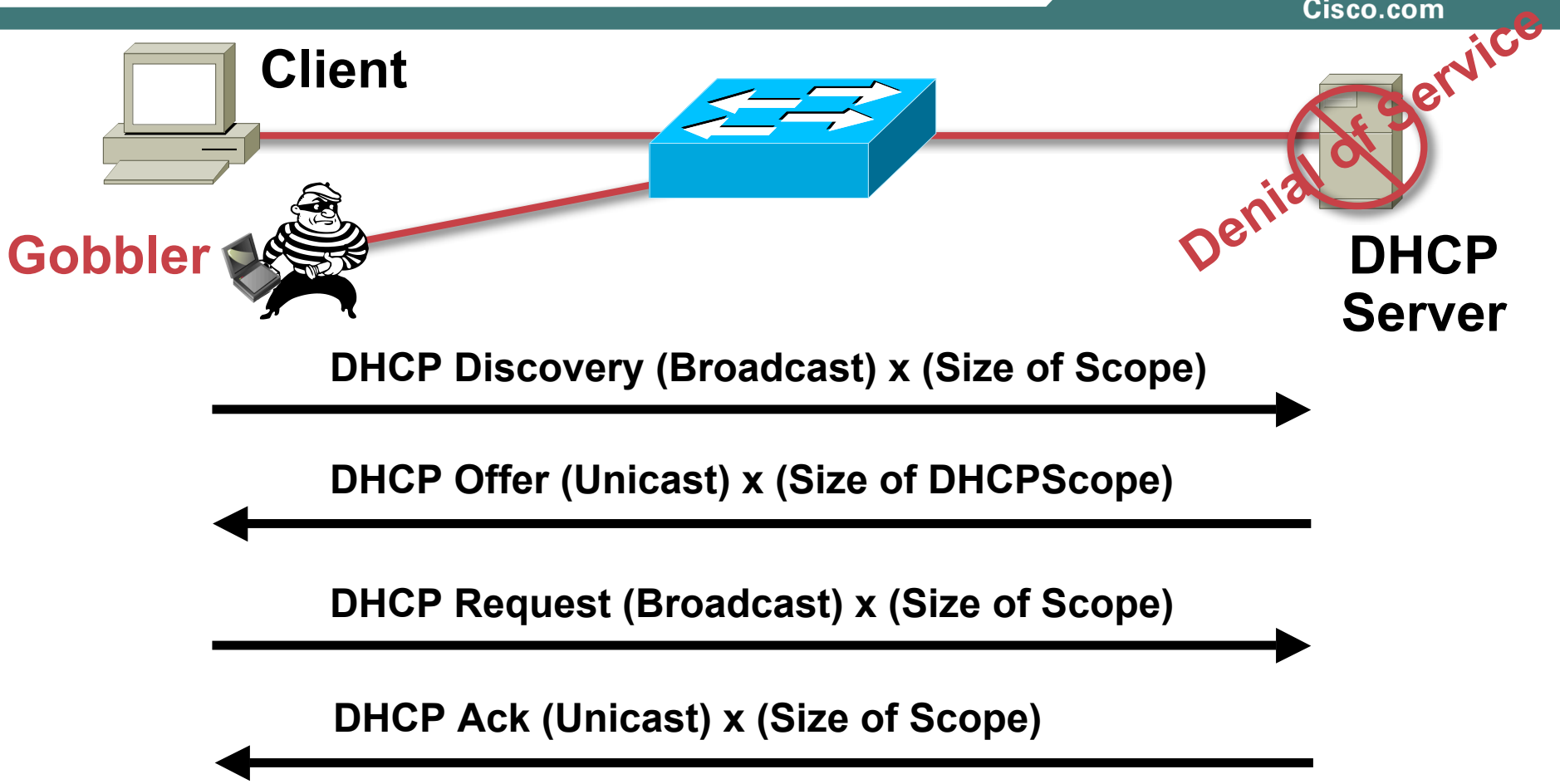


DHCP Function: Lower Level

DHCP Request/Reply Types

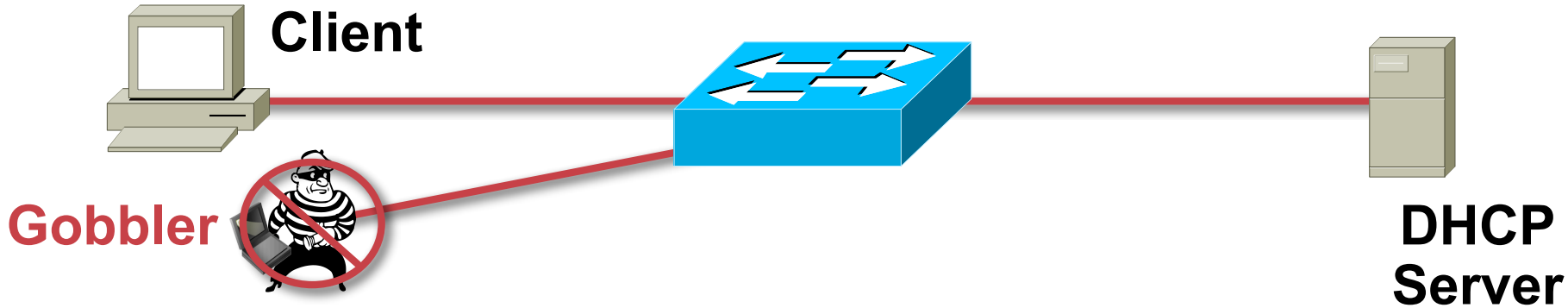
Message	Use
DHCPDISCOVER	Client broadcast to locate available servers
DHCPOFFER	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPREQUEST	Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address
DHCPACK	Server to client with configuration parameters, including committed network address
DHCPNAK	Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired
DHCPDECLINE	Client to server indicating network address is already in use
DHCPRELEASE	Client to server relinquishing network address and canceling remaining lease
DHCPINFORM	Client to server, asking only for local configuration parameters; client already has externally configured network address.

DHCP Attack Types
DHCP Starvation Attack



- Gobbler looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope
- This is a Denial of Service DoS attack using DHCP leases

Countermeasures for DHCP Attacks
DHCP Starvation Attack = Port Security



- Gobbler uses a new MAC address to request a new DHCP lease
- Restrict the number of MAC addresses on an port
- Will not be able to lease more IP address then MAC addresses allowed on the port
- In the example the attacker would get one IP address from the DHCP server

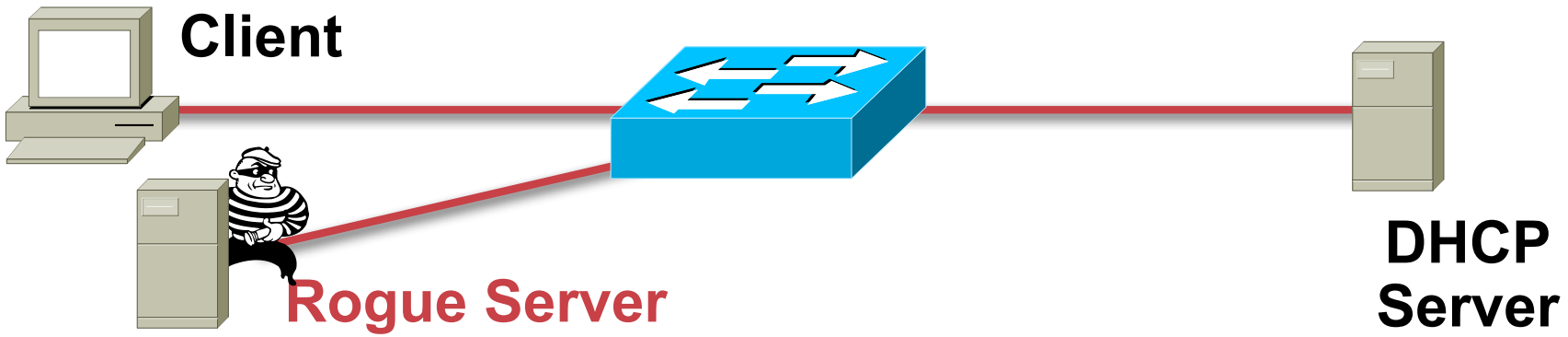
CatOS

```
set port security 5/1 enable
set port security 5/1 port max 1
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 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

DHCP Attack Types
Rogue DHCP Server Attack



DHCP Discovery (Broadcast)

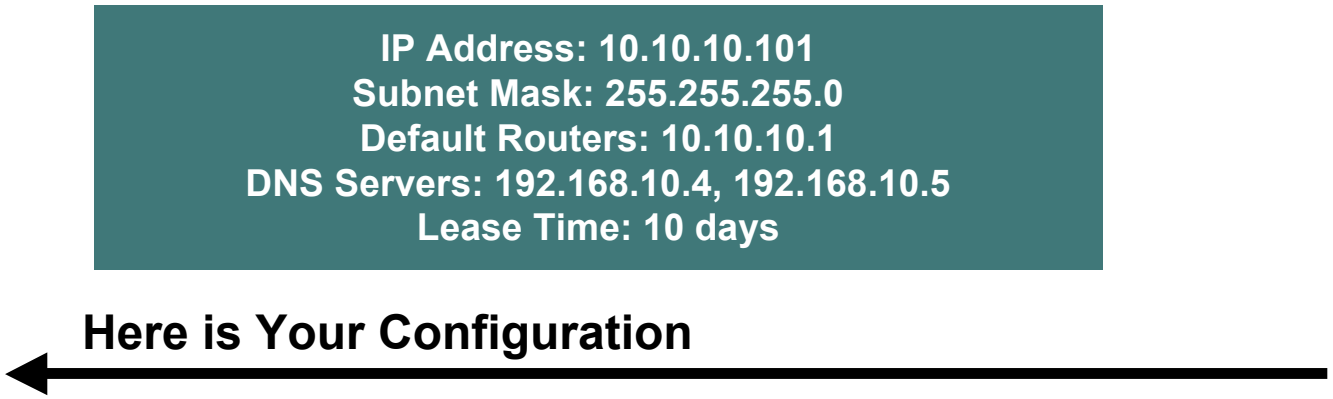
DHCP Offer (Unicast) from Rogue Server

DHCP Request (Broadcast)

DHCP Ack (Unicast) from Rogue Server

DHCP Attack Types
Rogue DHCP Server Attack

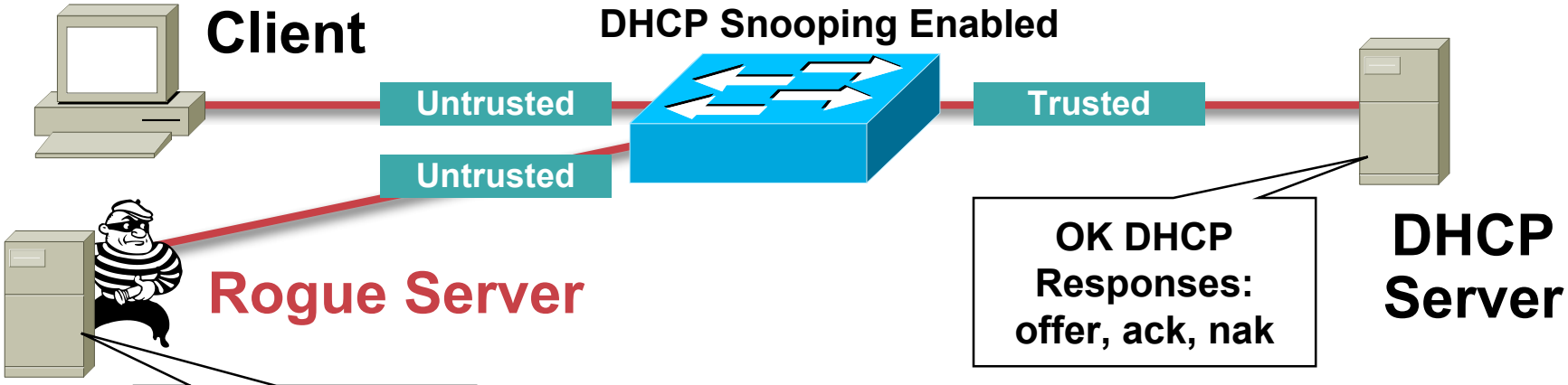
- What can the attacker do if he is the DHCP server?



- What do you see as a potential problem with incorrect information?
  - Wrong Default Gateway—Attacker is the gateway
  - Wrong DNS server—Attacker is DNS server
  - Wrong IP Address—Attacker does DOS with incorrect IP

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

Cisco.com



IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping

DHCP Snooping Untrusted Client

Interface Commands
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)

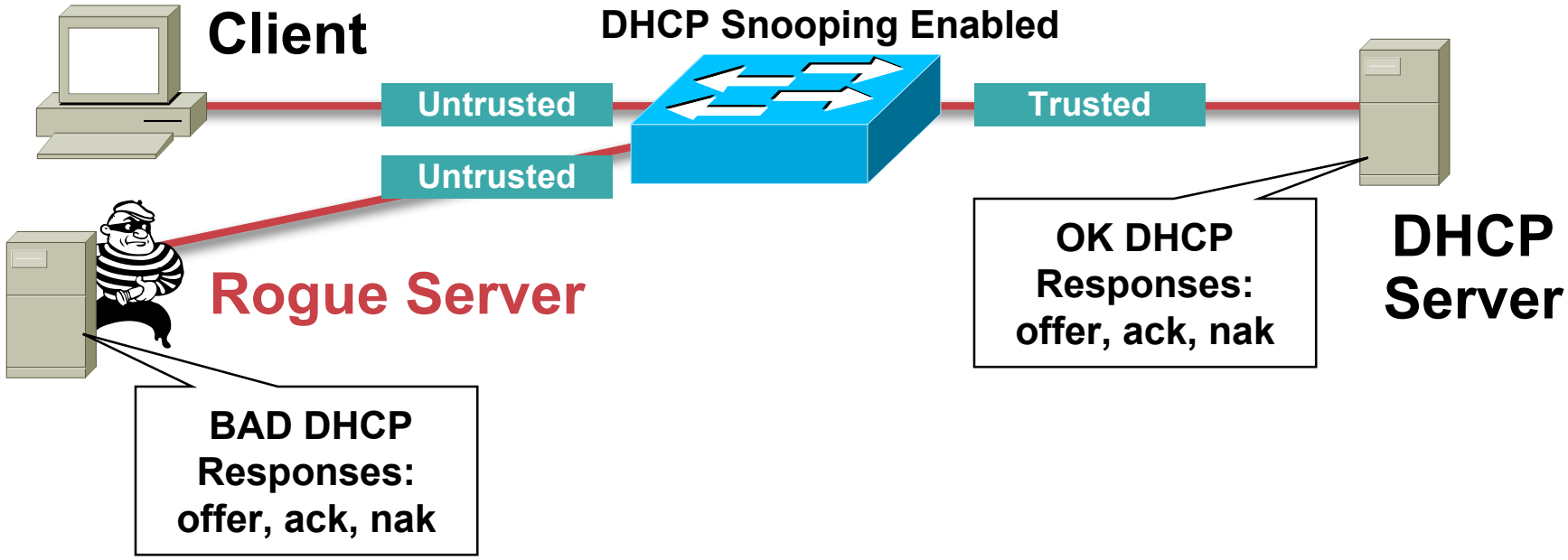
DHCP Snooping Trusted Server or Uplink

Interface Commands
ip dhcp snooping trust

- **By default all ports in the VLAN are untrusted**

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

Cisco.com



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
```

- Table is built by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires

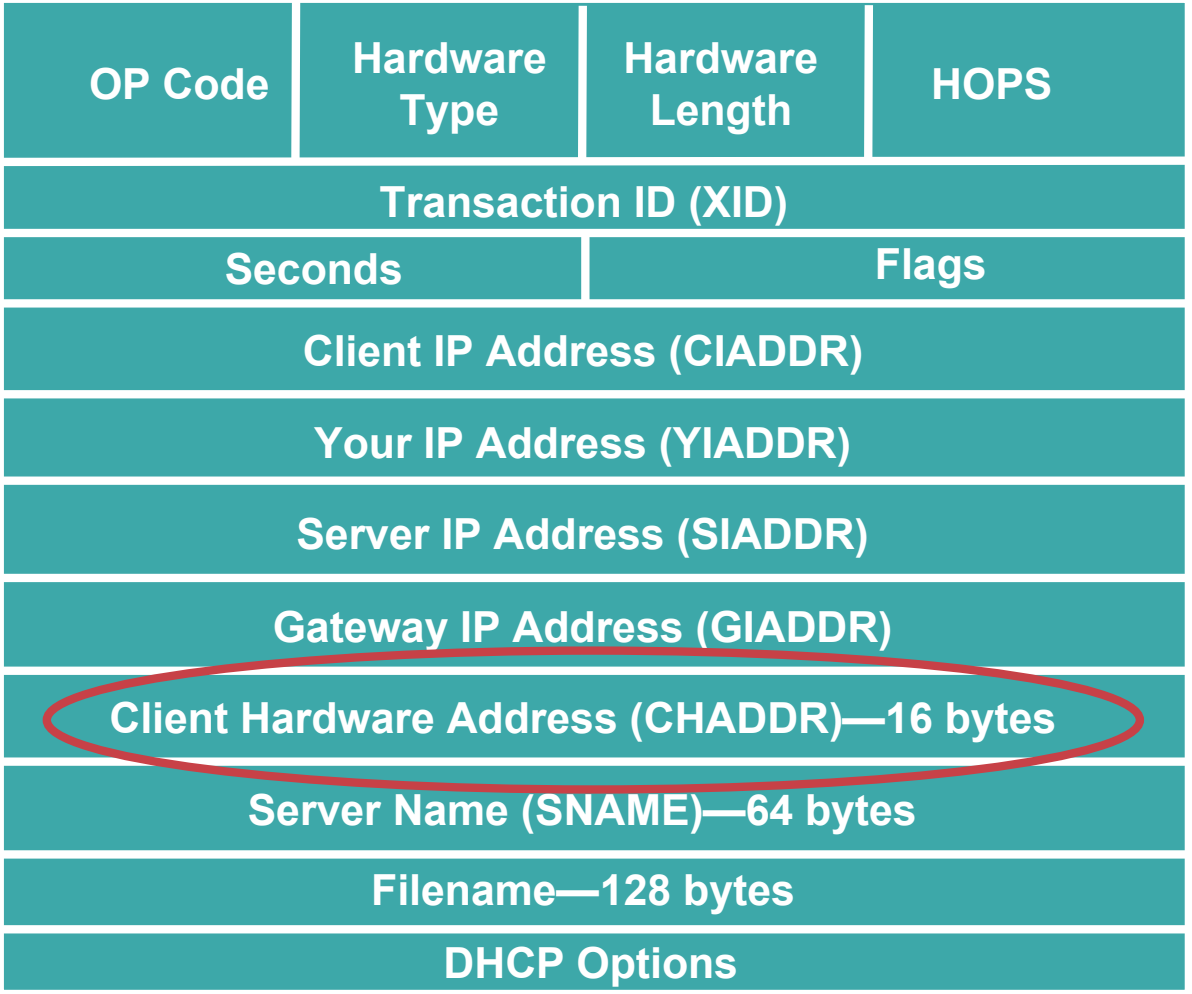
Advanced Configuration DHCP Snooping

- **Not all operating system (Linux) re DHCP on link down**
- **In the event of switch failure, the DHCP Snooping Binding Table can be written to bootflash, ftp, rcp, slot0, and tftp**
- **This will be critical in the next section**

```
ip dhcp snooping database tftp://172.26.168.10/tftpboot/tulledge/ngcs-4500-1-dhcpdb
ip dhcp snooping database write-delay 60
```

Advanced Configuration DHCP Snooping

- Gobbler uses a unique MAC for each DHCP request and Port Security prevents Gobbler
- What if the attack used the same interface MAC address, but changed the Client Hardware Address in the request?
- Port Security would not work for that attack
- The switches now check the CHADDR field of the request to make sure it matches the hardware MAC in the DHCP Snooping Binding table
- If there is not a match, the request is dropped at the interface



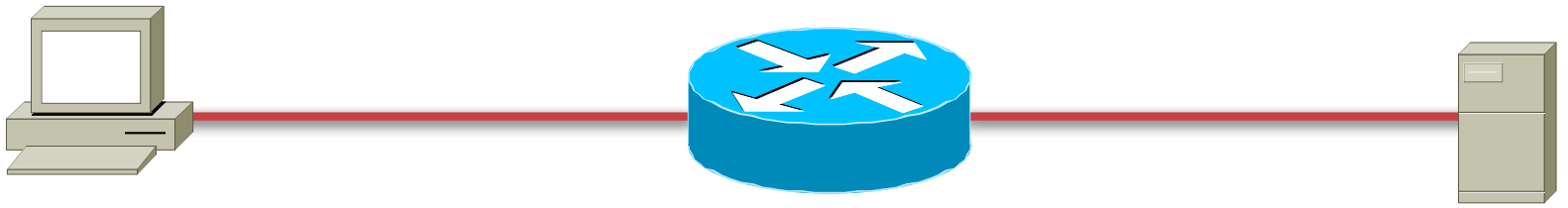
Note: Some Switches Have This on by Default, and Others Don't Please Check the Documentation for Settings

DHCP Rogue Server

- **If there are switches in the network that will not support DHCP Snooping, you can configure VLAN ACL's to block UDP Port 68**

```
set security acl ip ROGUE-DHCP permit udp host 192.0.2.1 any eq 68
set security acl ip ROGUE-DHCP deny udp any any eq 68
set security acl ip ROGUE-DHCP permit ip any any
set security acl ip ROGUE-DHCP permit udp host 10.1.1.99 any eq 68
```

- **Will not prevent the CHADDR DHCP Starvation attack**



Router

192.0.2.1

DHCP Server

10.1.1.99

Summary of DHCP Attacks

- DHCP Starvation attacks can be mitigated by Port Security
- Rogue DHCP servers can be mitigated by DHCP Snooping features
- When configured with DHCP Snooping, all ports in the VLAN will be “Untrusted” for DHCP replies
- Check default settings to see if the CHADDR field is being checked during the DHCP request
- Unsupported switches can run ACLs for partial attack mitigation (can not check the CHADDR field)

DHCP Snooping Capacity

- All DHCP Snooping Binding tables have limits
- All entries stay in the binding table until the lease runs out
- If you have a mobile work environment, reduce the lease time to make sure the binding entries will be removed

```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------- ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     19315       dhcp-snooping  4     FastEthernet3/18
```

Building the Layers

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

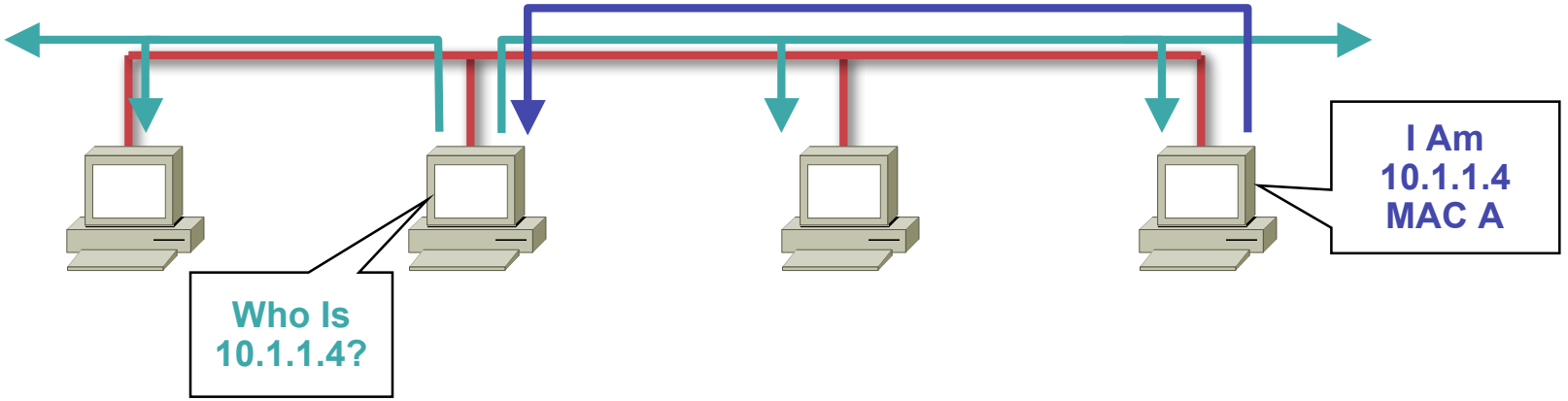
ATTACKS AND COUNTERMEASURES: ARP ATTACKS

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**

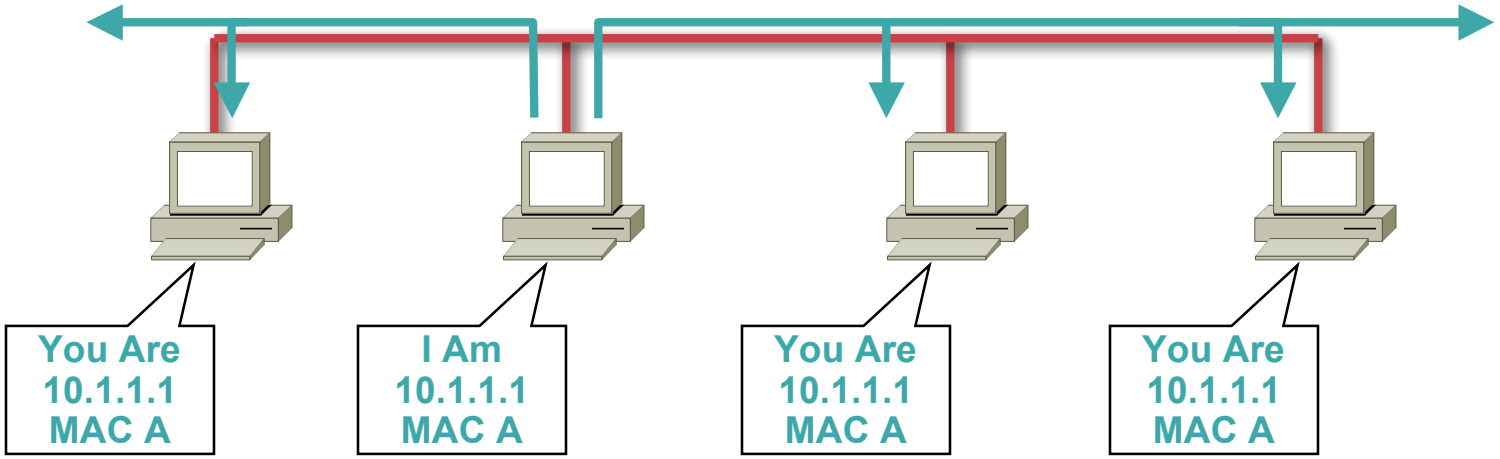
  This ARP request is broadcast using protocol 0806

- **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

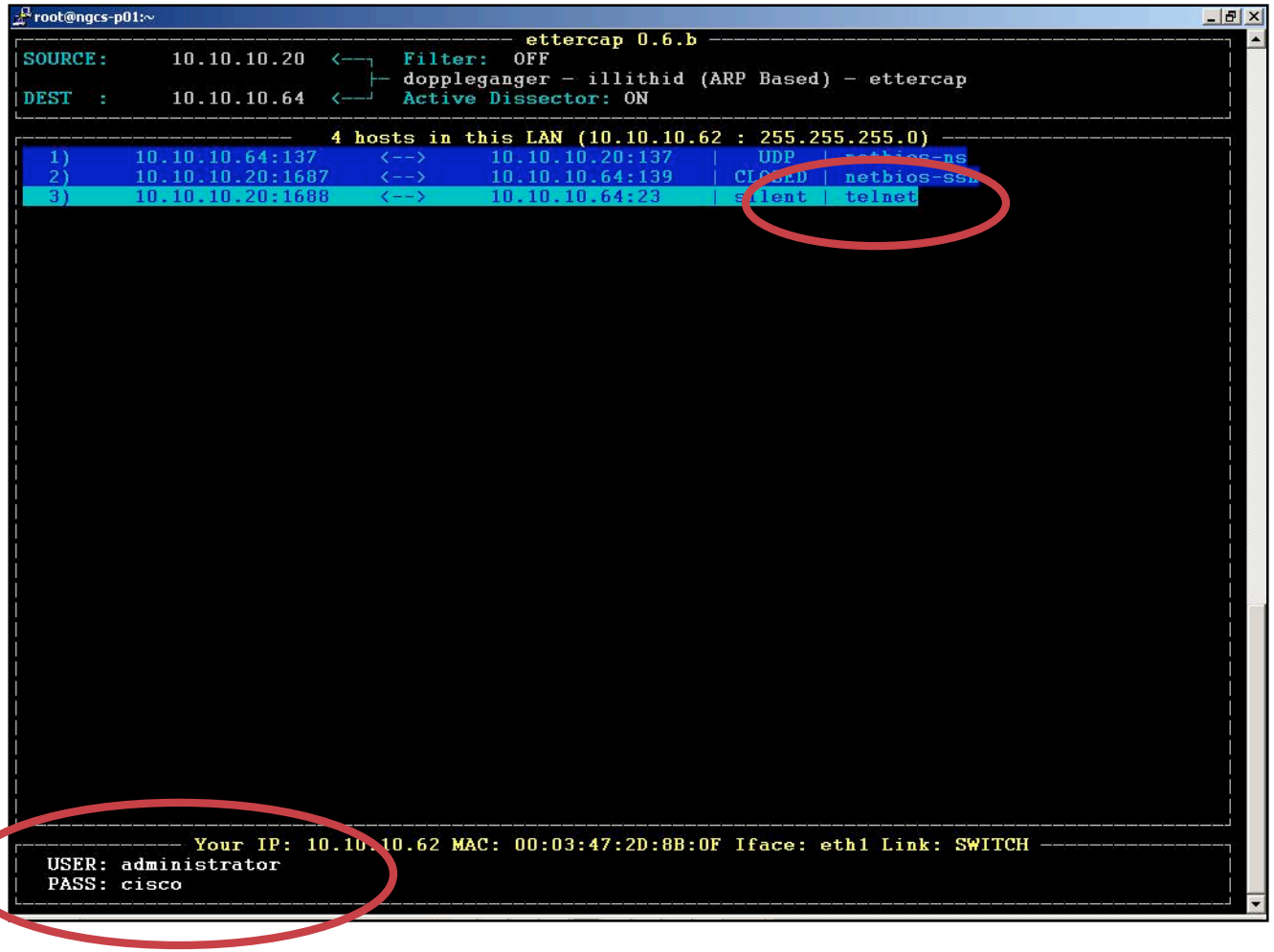


ARP Attack Tools

- 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

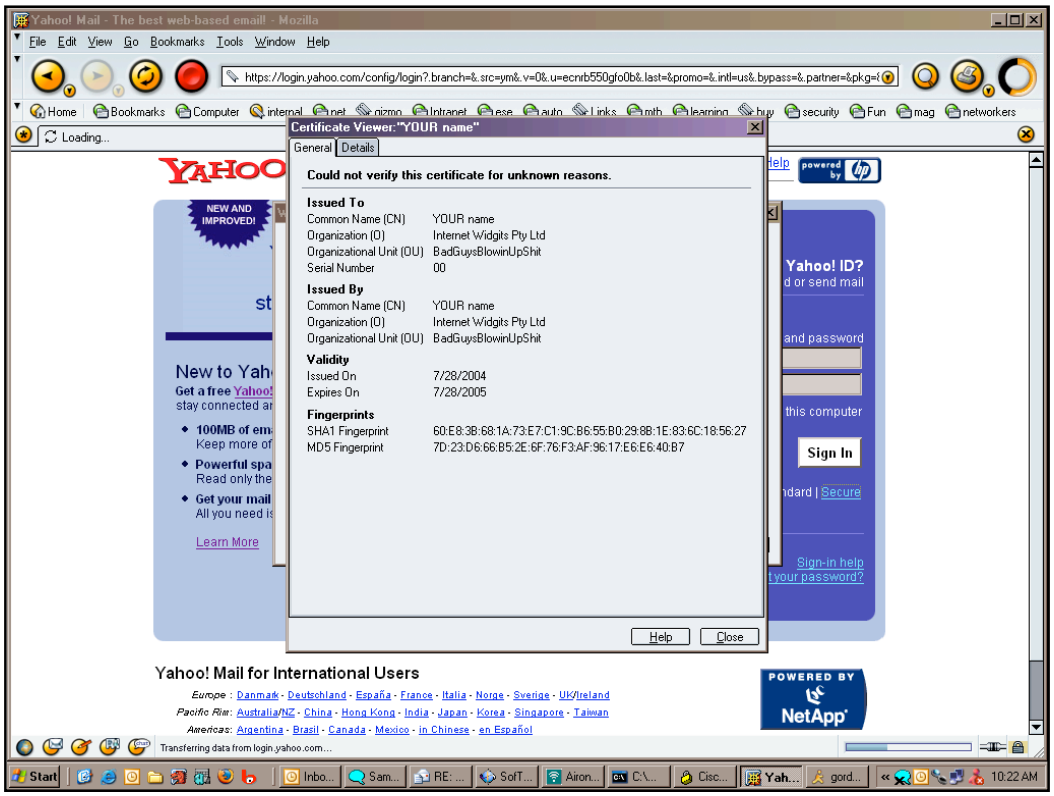
ARP Attack Tools

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



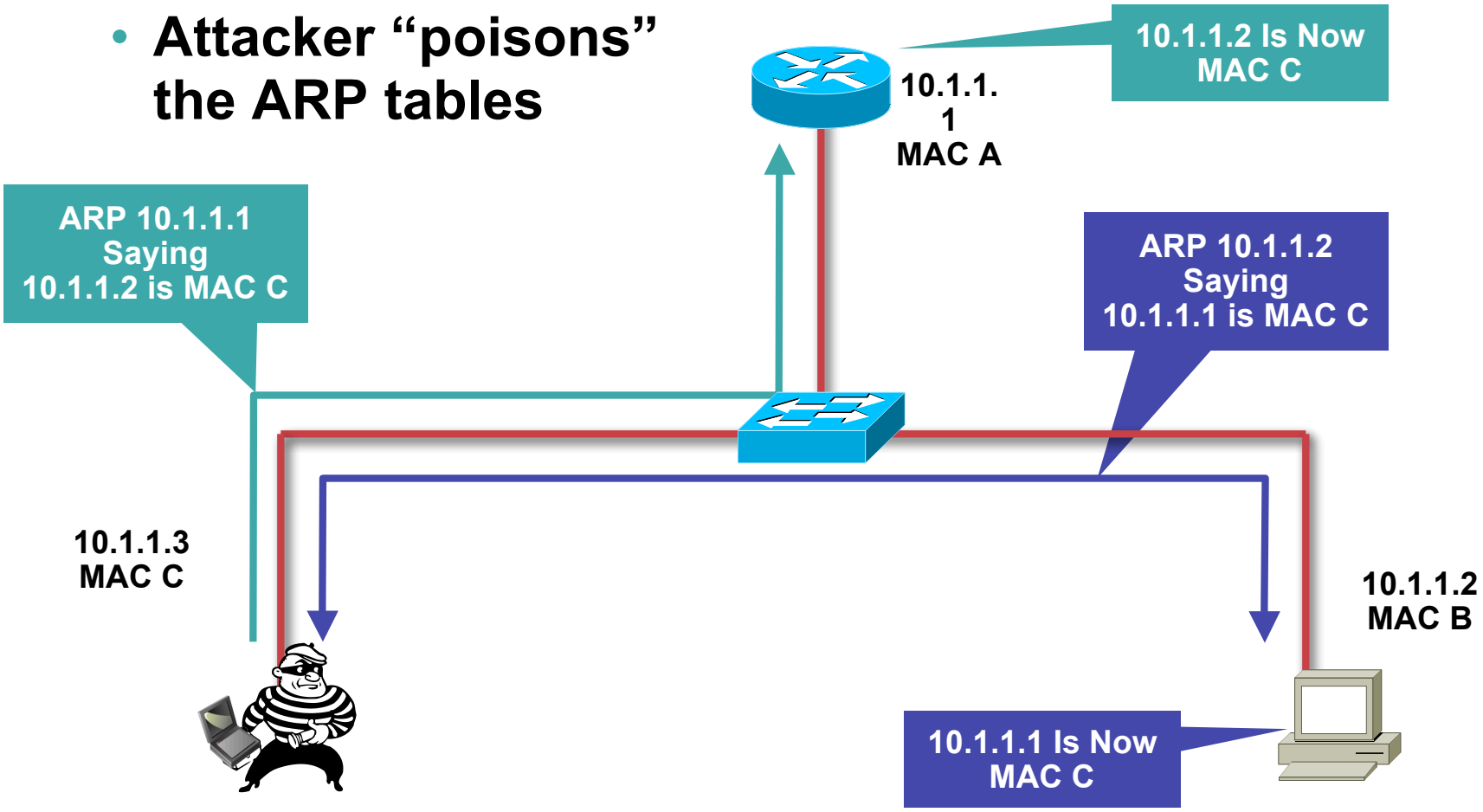
ARP Attack Tools: SSH/SSL

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



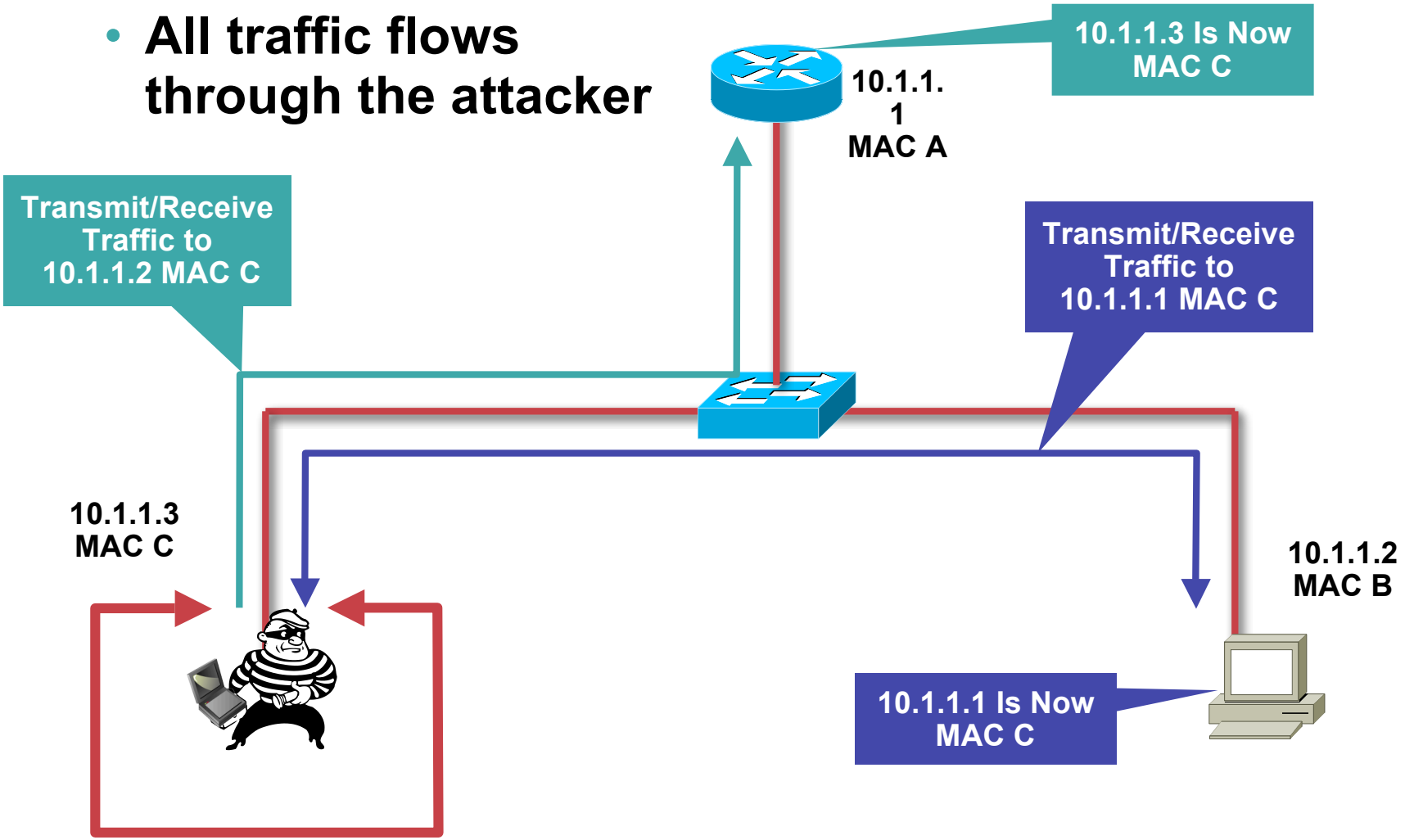
ARP Attack in Action

- Attacker "poisons" the ARP tables



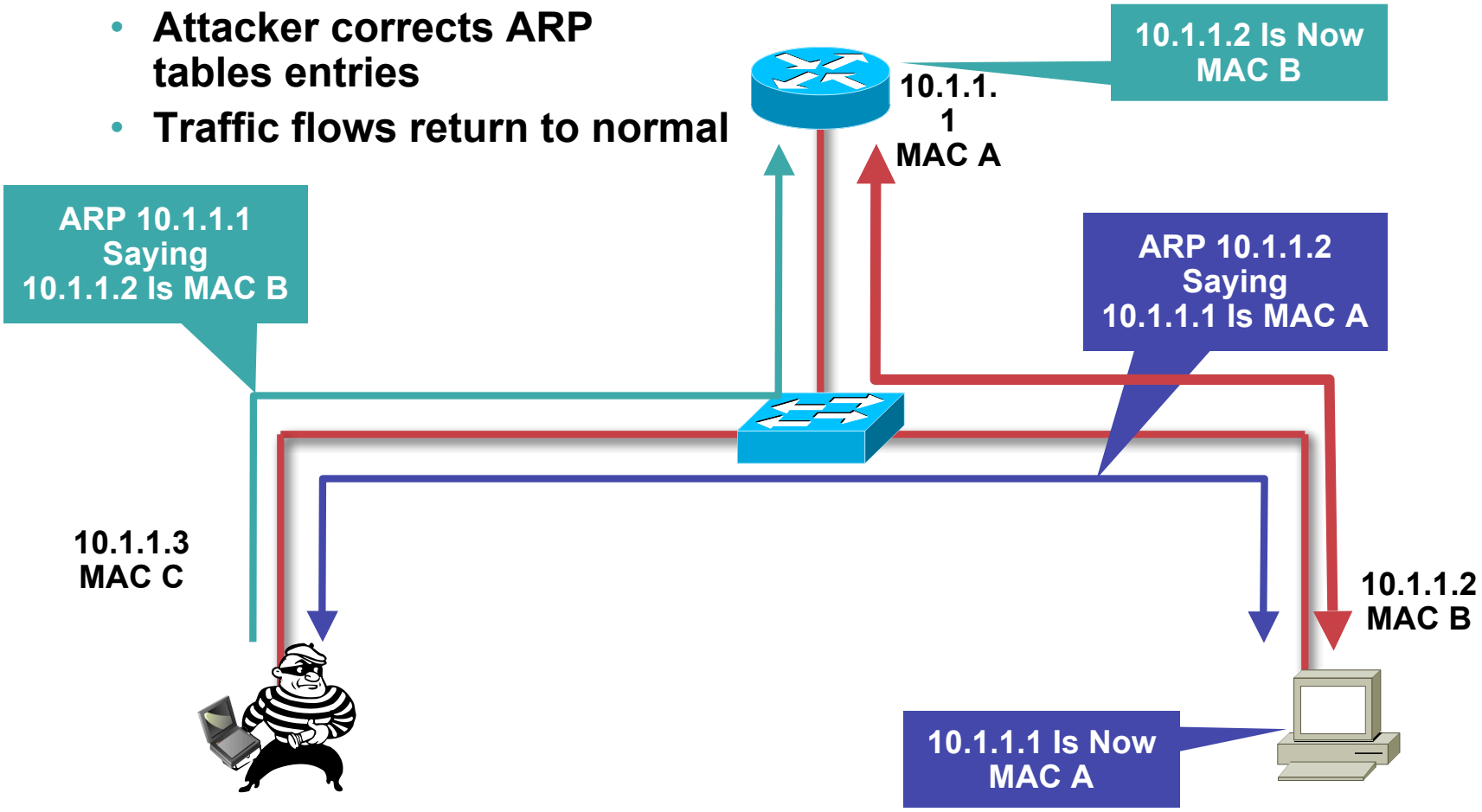
ARP Attack in Action

- All traffic flows through the attacker

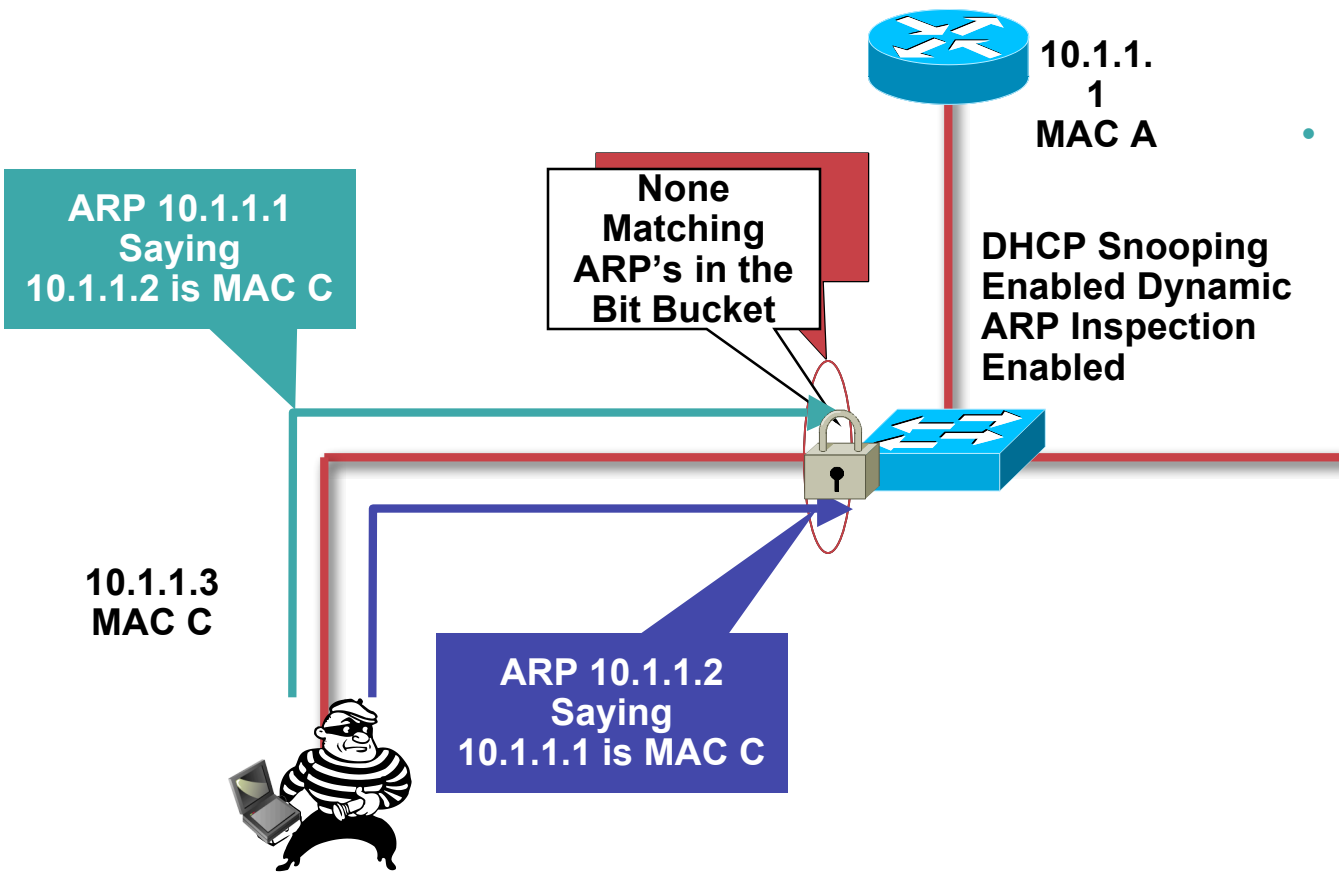


ARP Attack Clean Up

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



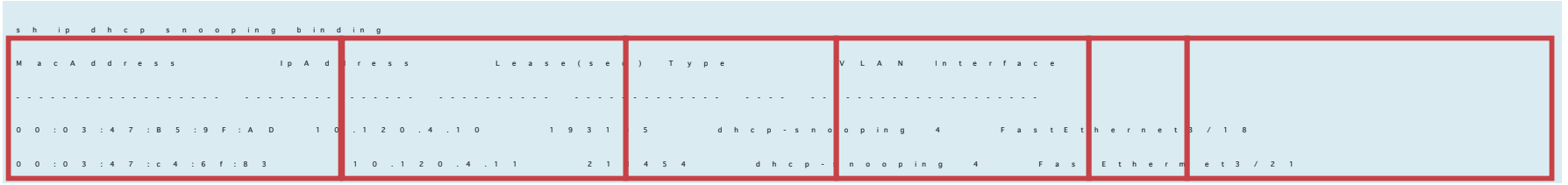
Countermeasures to ARP Attacks: Dynamic ARP Inspection



- 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     1931        dhcp-snooping  4     FastEthernet3/18
00:03:47:c4:6f:83   10.120.4.11     2145        dhcp-snooping  4     FastEthernet3/21
```

- **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

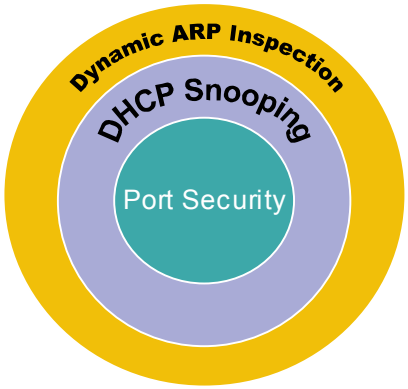
Summary of ARP Attacks

- 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



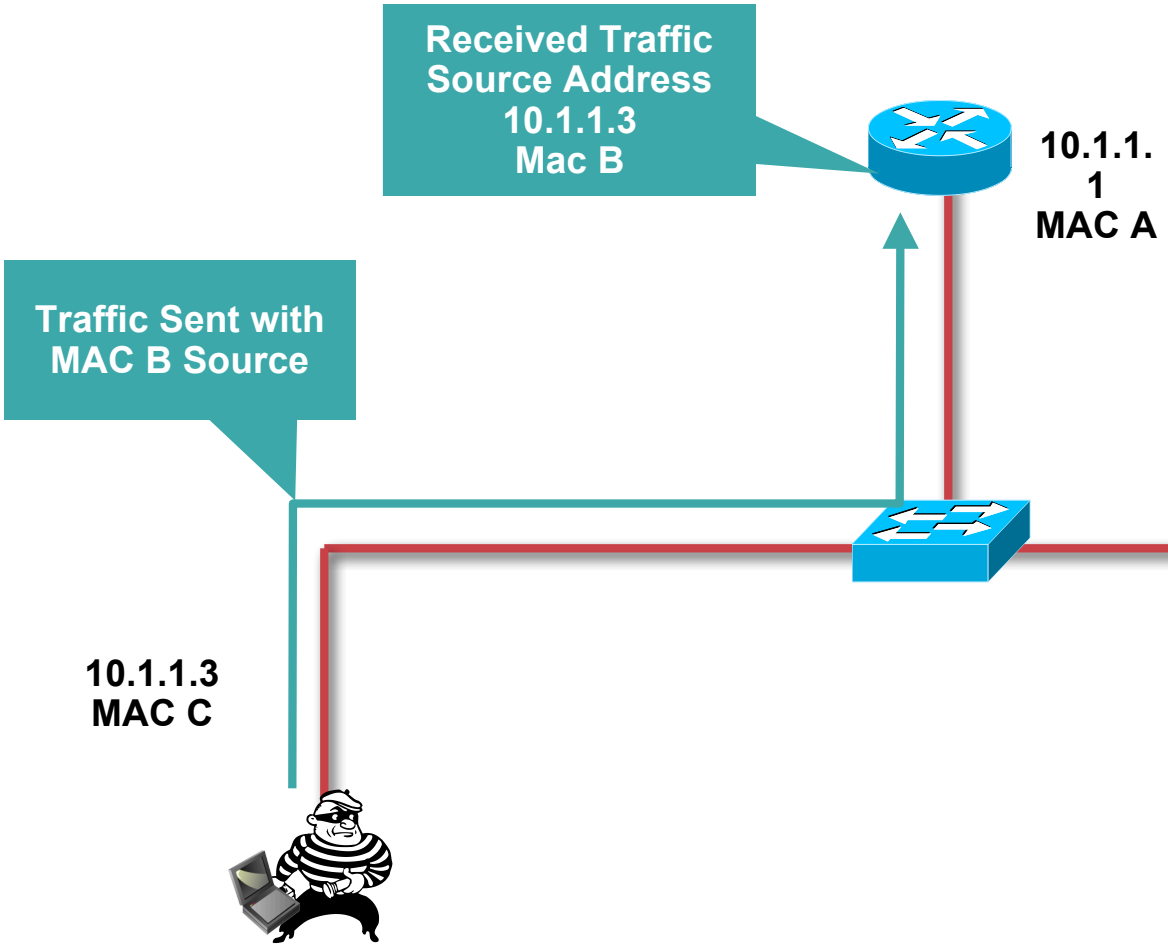
- **Port security prevents CAM attacks and DHCP Starvation attacks**
- **DHCP snooping prevents rogue DHCP server attacks**
- **Dynamic ARP inspection prevents current ARP attacks**

ATTACKS AND COUNTERMEASURES: SPOOFING ATTACKS

Spoofing Attacks

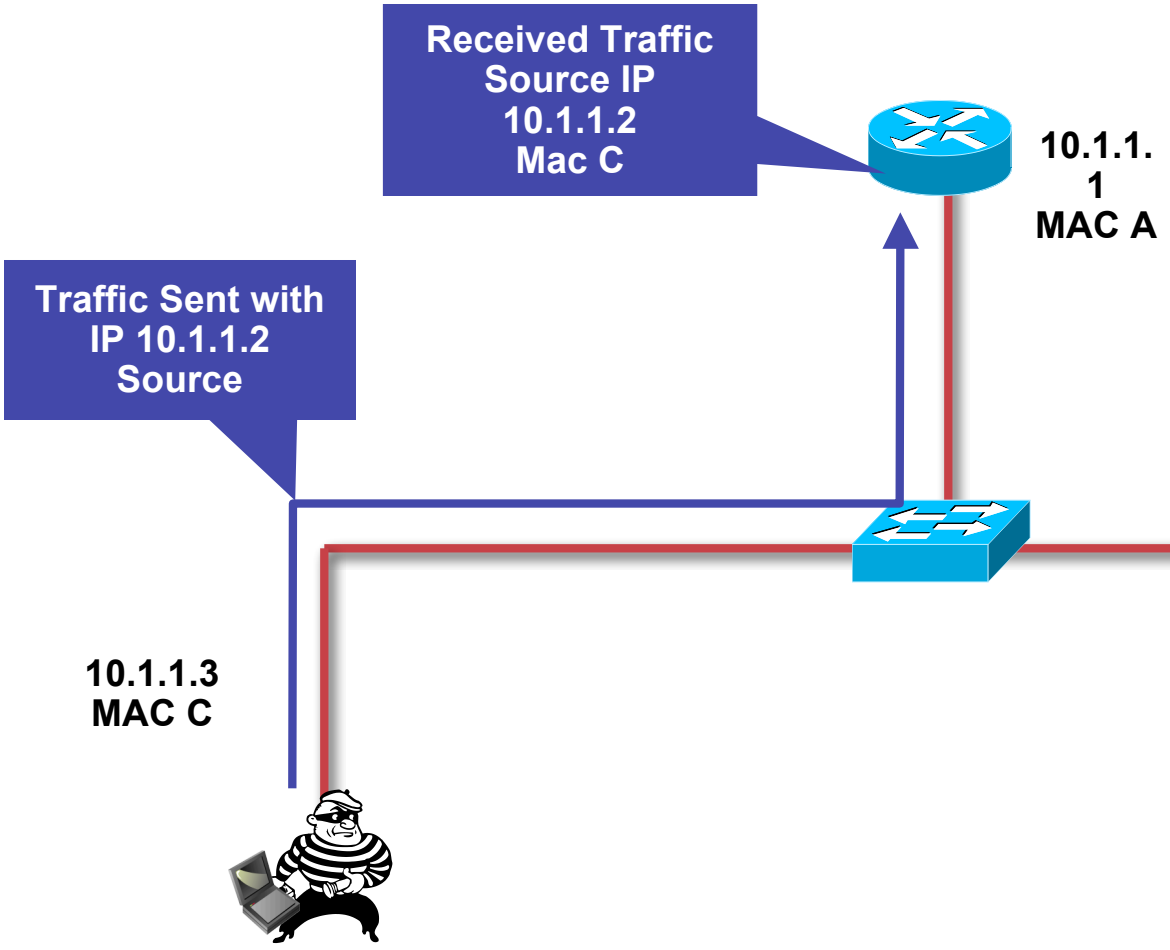
- **MAC spoofing**
  - **If MACs are used for network access an attacker can gain access to the network**
  - **Also can be used to take over someone's identity already on the network**
- **IP spoofing**
  - **Ping of death**
  - **ICMP unreachable storm**
  - **SYN flood**
  - **Trusted IP addresses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

Spoofing Attack: MAC



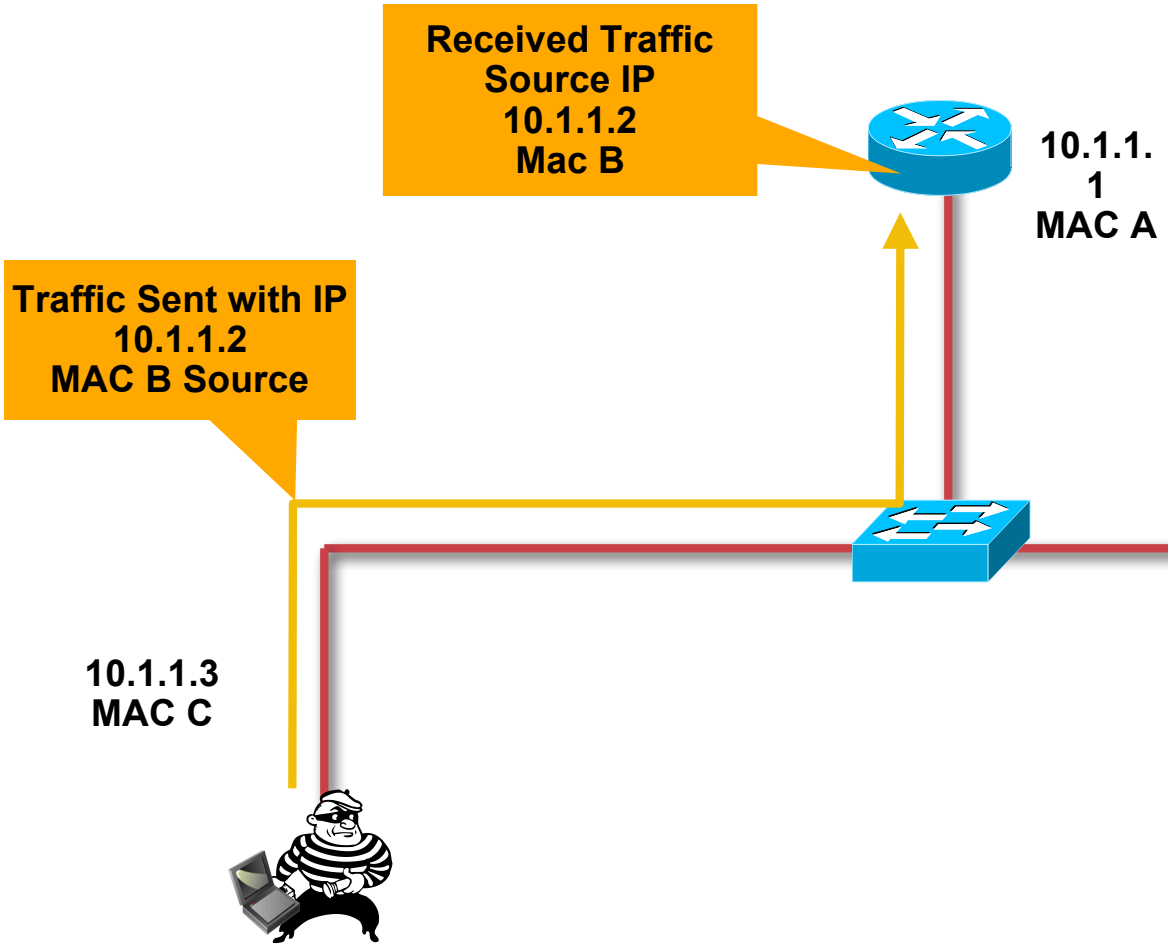
- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

Spoofing Attack: IP



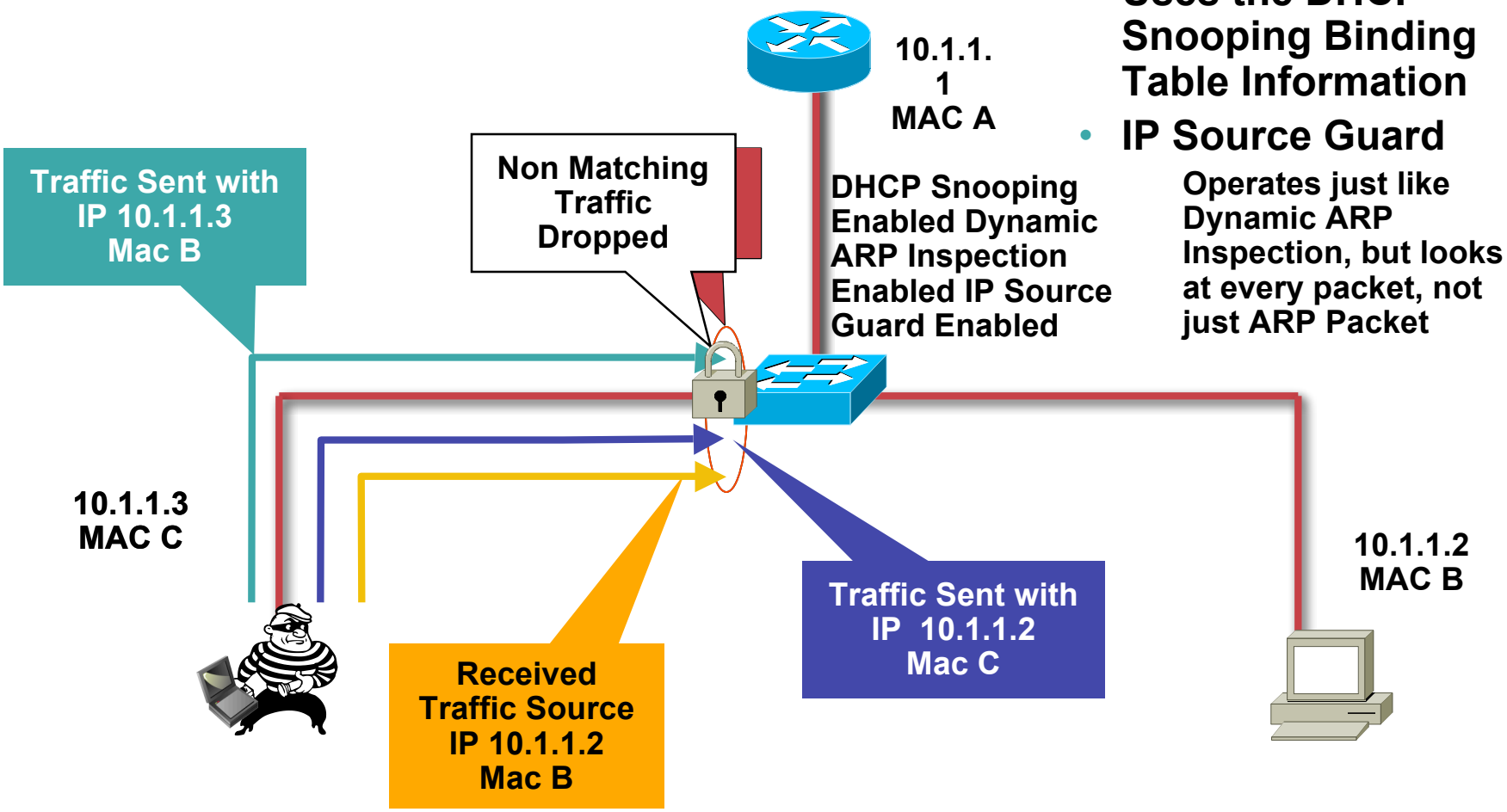
- Attacker sends packets with the incorrect source IP Address
- Whatever device the packet is sent to will never reply to the attacker

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

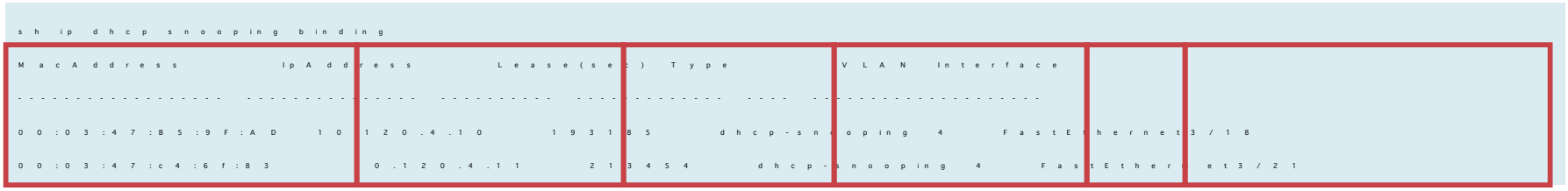


- Uses the DHCP Snooping Binding Table Information
- IP Source Guard
  - Operates just like Dynamic ARP Inspection, but looks at every packet, not just ARP Packet

Countermeasures to Spoofing Attacks: IP Source Guard

Cisco.com

- Uses the information from the DHCP Snooping Binding table



- 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

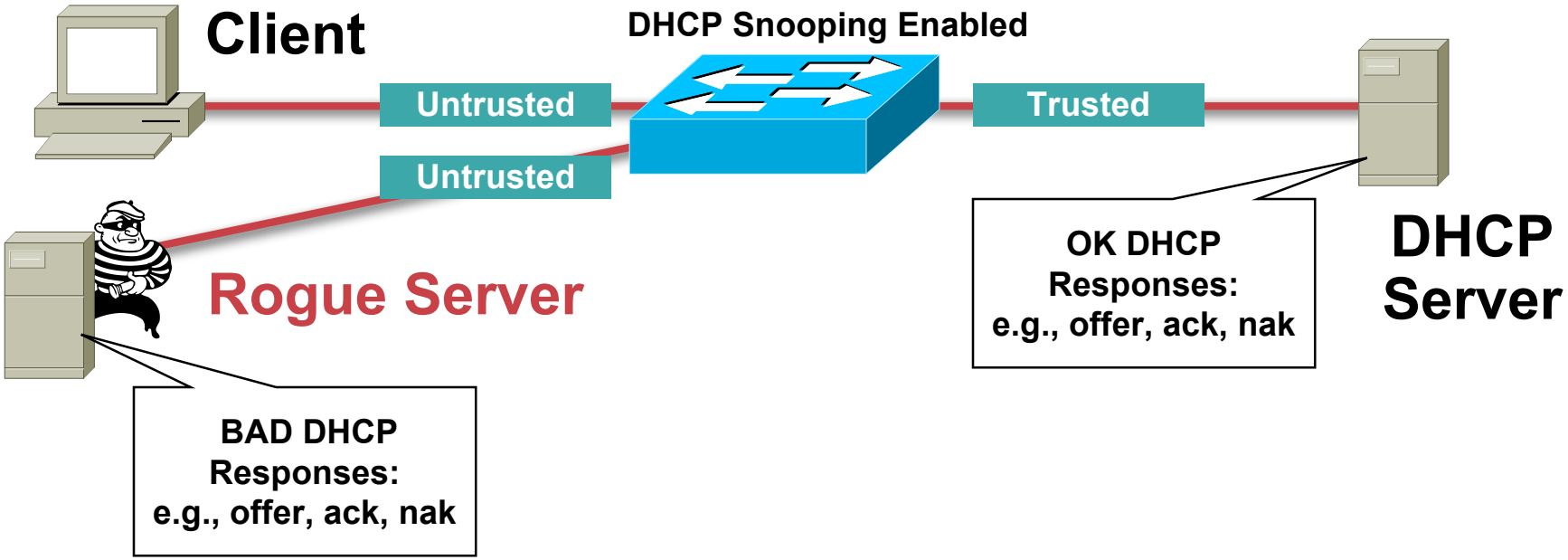
Building the Layers

- 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

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping

Cisco.com

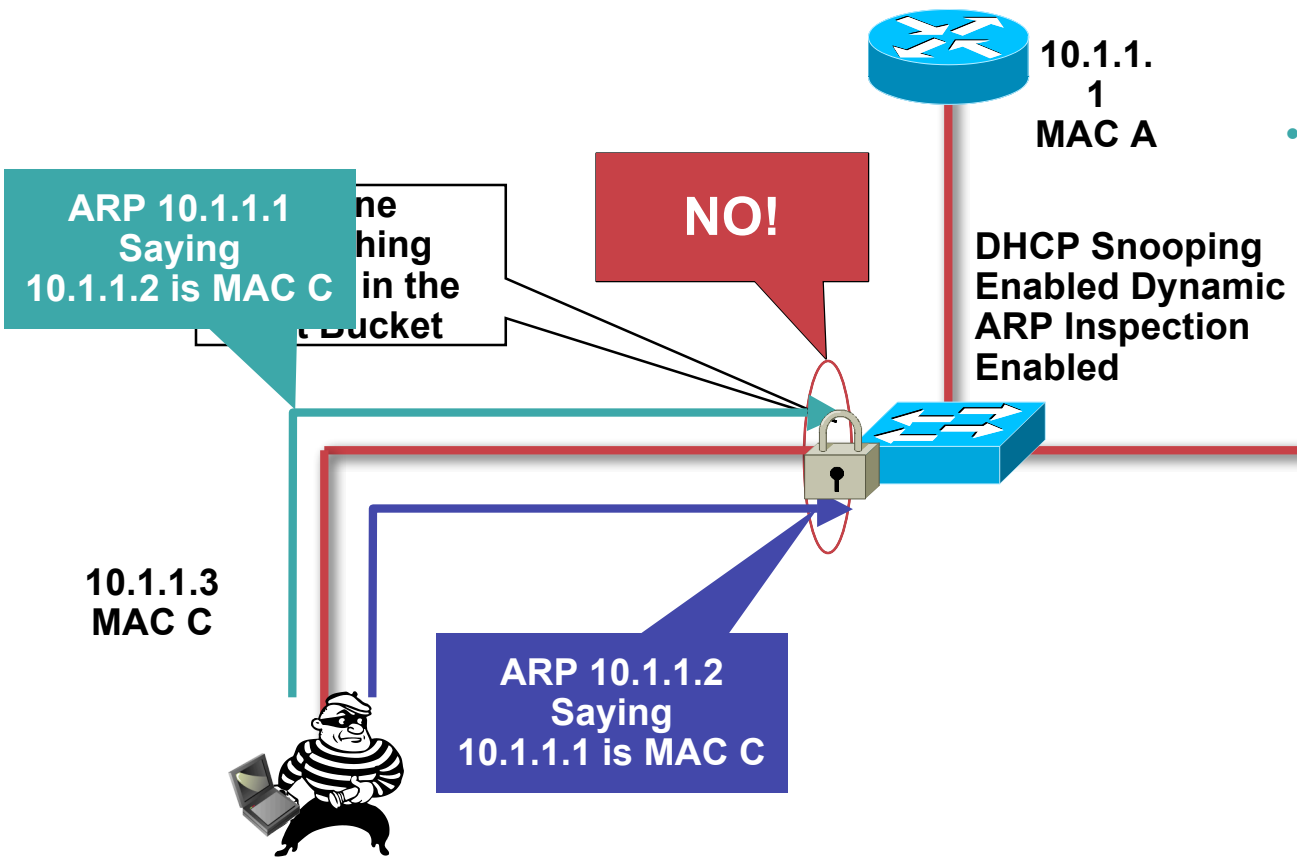


DHCP Snooping Binding Table

```
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
```

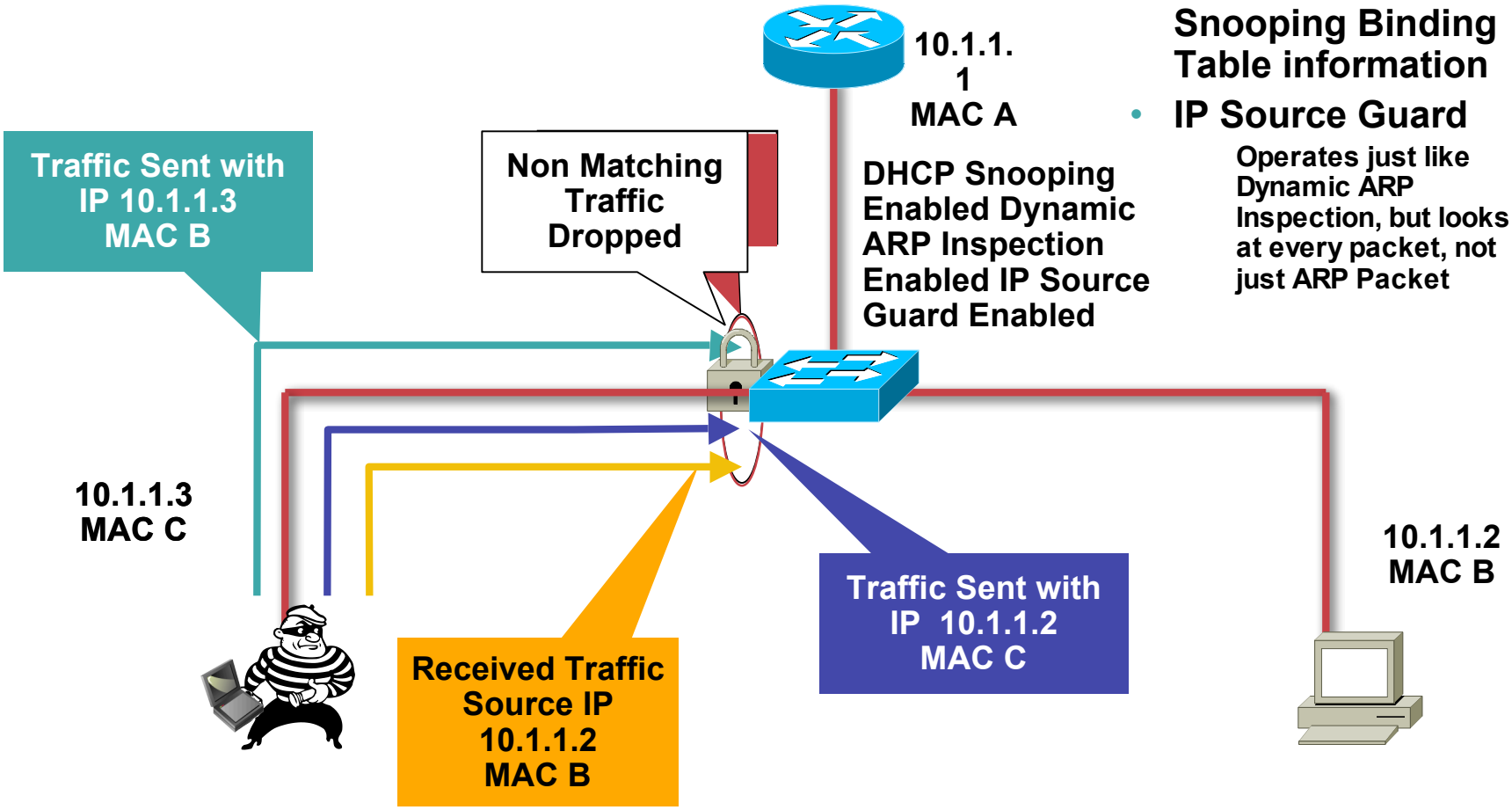
- Table is build by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires

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 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

Matrix for Security Features 1 of 3

Feature/ Platform	6500/ Catalyst OS	6500/Cisco IOS	4500/ Catalyst OS	4500/Cisco IOS
Dynamic Port Security	7.6(1)	12.1(13)E	5.1(1)	12.1(13)EW
DHCP Snooping	8.3(1)	12.2(18)SXE*	N/A	12.1(12c)EW **
DAI	8.3(1)	12.2(18)SXE*	N/A	12.1(19)EW **
IP Source Guard	8.3(1)*	Q1CY '06* 12.2(18)SXD2	N/A	12.1(19)EW **

* Requires Sup720—Support for Sup32 DHCP Snooping and DAI Q3CY05
** For the Catalyst 4500/IOS-Based Platforms, This Requires Sup2+, Sup3, Sup4, Sup 5. These Sups Are Supported on the Catalyst 4006, 4503, 4506, and 4507R Chassis
NOTE: There Are No Plans to Support These Features for any Catalyst 4000/4500 Platform Running Catos, or Any 2900 Platform

Matrix for Security Features 2 of 3

Feature/ Platform	3750/3560 EMI	3550 EMI	2970 EI	2950 EI	2950 SI
Dynamic Port Security	12.1(25)SE	12.2(25)SEA	12.1(11)AX	12.0(5.2)WC1	12.0(5.2)WC1
DHCP Snooping	12.1(25)SE	12.2(25)SEA	12.1(19)EA1	12.1(19)EA1	N/A
DAI	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A
IP Source Guard	12.2(25)SE	12.2(25)SEA	N/A	N/A	N/A

NOTE: Old names of the IOS for the 3000 series switches
IOS Feature Finder—http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Matrix for Security Features 3 of 3

Feature/ Platform	3750/3560 Advance IP	3550 Advanced IP	3750/3560 IP Base	3550 IP Base
Dynamic Port Security	12.1(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA
DHCP Snooping	12.1(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA
DAI	12.2(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA
IP Source Guard	12.2(25)SE	12.2(25)SEA	12.1(25)SE	12.2(25)SEA

NOTE: Name change of the IOS on the 3000 series switches
IOS Feature Finder—http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

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

Layer 2 Security Best Practices 1 of 2

Cisco.com

- 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 (unless you are Cisco VoIP)
- 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 (ARP Inspection, IDS, etc.)

Layer 2 Security Best Practices 2 of 2

Cisco.com

- Enable STP attack mitigation (BPDU Guard, Root Guard)
- Decide what to do about DHCP attacks (DHCP Snooping, VACLs)
- Use MD5 authentication for VTP
- Use CDP only where necessary
- Disable all unused ports and put them in an unused VLAN

All of the Preceding Features Are Dependent on Your Own Security Policy

Lessons Learned

- Carefully consider any time you must count on VLANs to operate in a security role
  - If properly configured, our testing did not discover a method of VLAN Hopping using Cisco switches
  - Pay close attention to the configuration
  - Understand the organizational implications
- 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