Understanding, Preventing, and Defending Against Layer 2 Attacks

Yusuf Bhaiji

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures
    - VLAN Hopping
    - MAC Attacks
    - DHCP Attacks
    - ARP Attacks
    - Spoofing Attacks
    - General Attacks
- Summary

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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 types of attacks
- 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
- These are IPv4 only attacks today
- There are data center sessions for security, this is access ports for users

© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures

    VLAN Hopping

    MAC Attacks

    DHCP Attacks

    ARP Attacks

    Spoofing Attacks

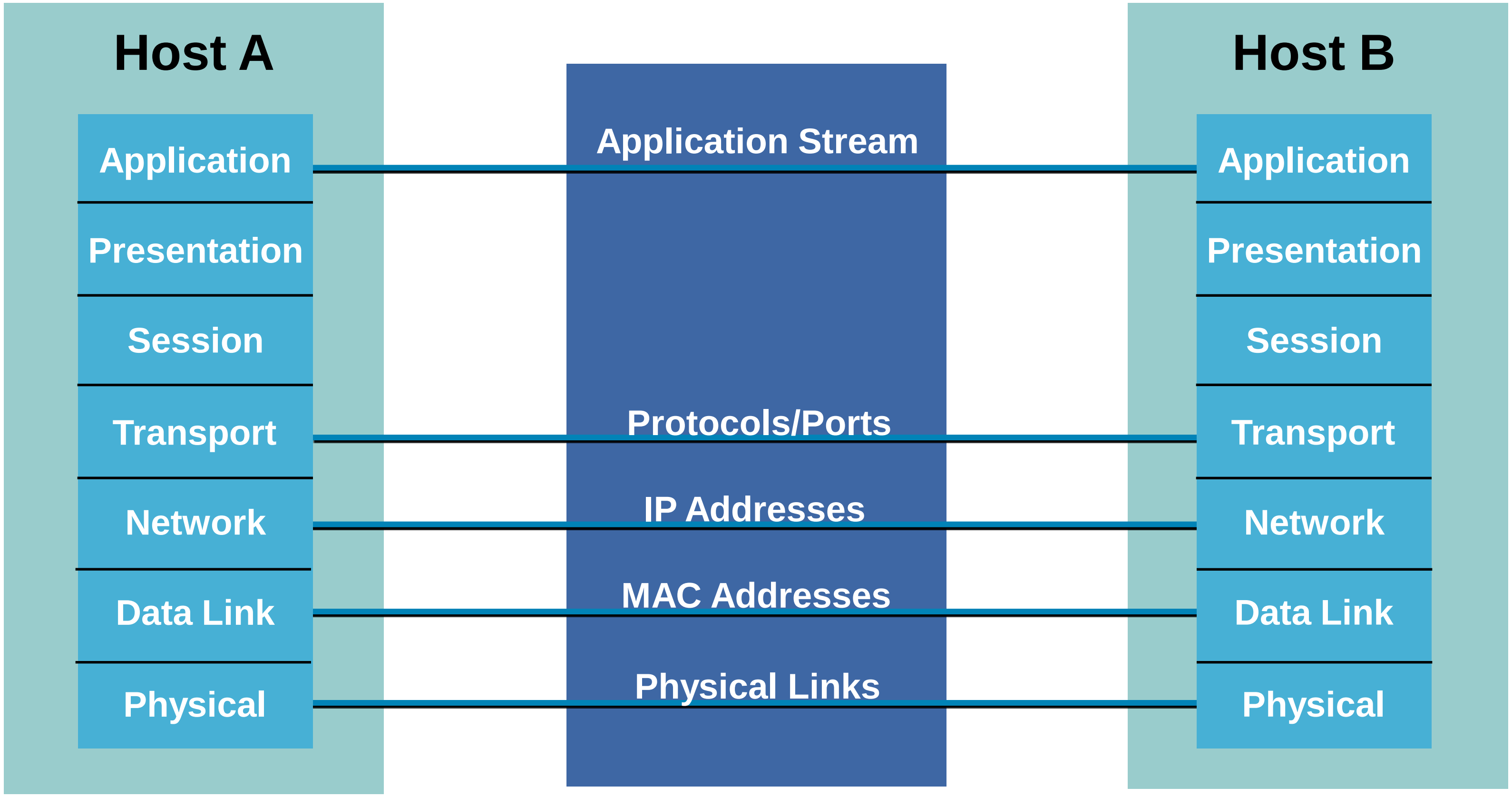
    General Attacks

- Summary

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Why Worry About Layer 2 Security?

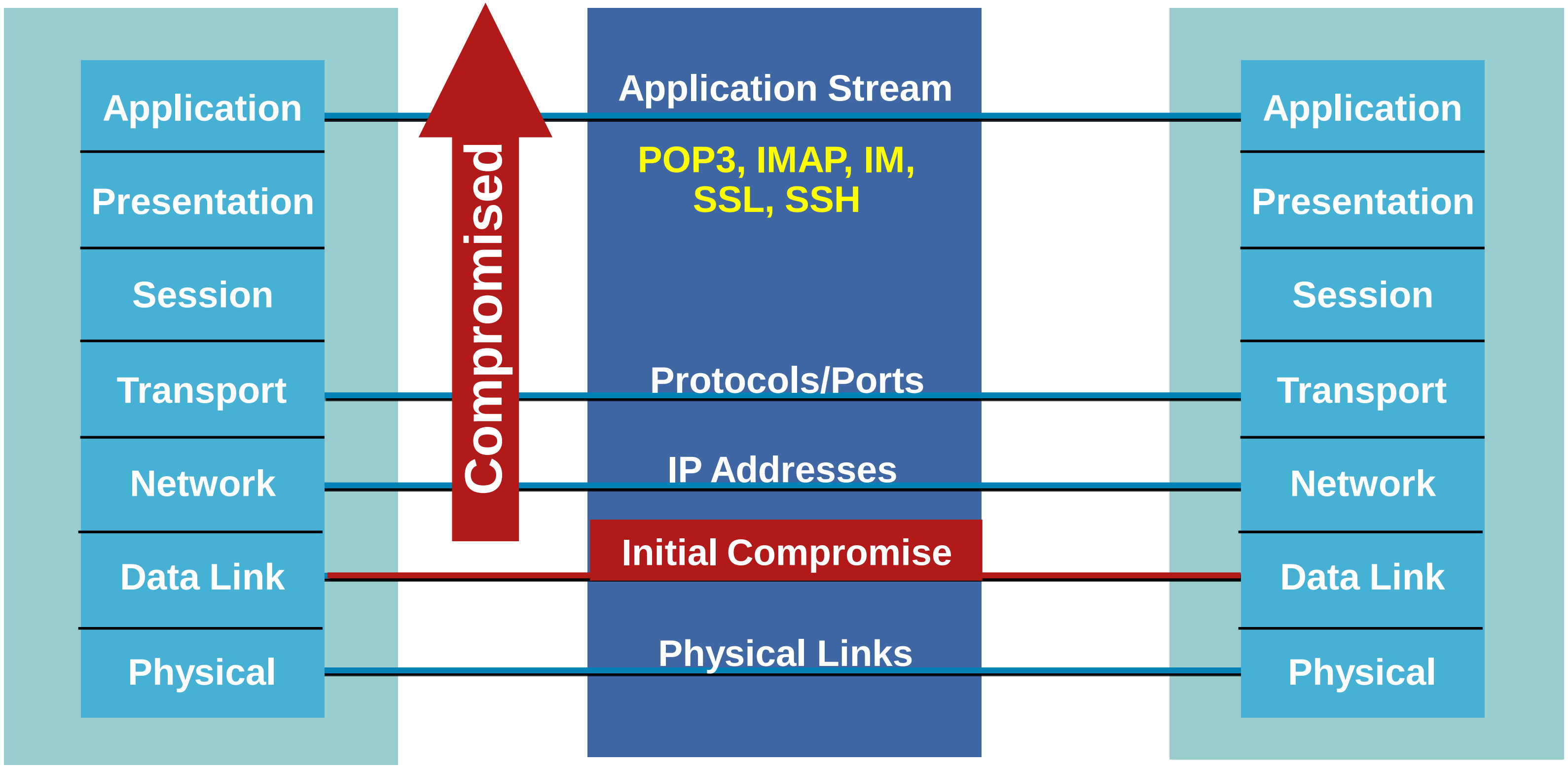
OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other



© 2007 Cisco Systems, Inc. All rights reserved.

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



Who Owns VLANS? NetOPS/SecOPS?

Questions	NetOPS	SecOPS
• Security Policy for VLANs	• We have L2 security issues?	• I handle it at L3 and above
• Do you use VLANS often	• I use them all the time	• I have no idea how often
• Do you use VLANs for security?	• Routing in and out of the same switch are fine, that is why we have a Layer 3 switch	• It is a switch, why would I care?
• What addresses are assigned per VLAN?	• Security Guy asks for a segment, I make a VLAN and give it some addresses	• I ask NetOPS they, they give me Ports and addresses

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures

    VLAN Hopping

    MAC Attacks

    DHCP Attacks

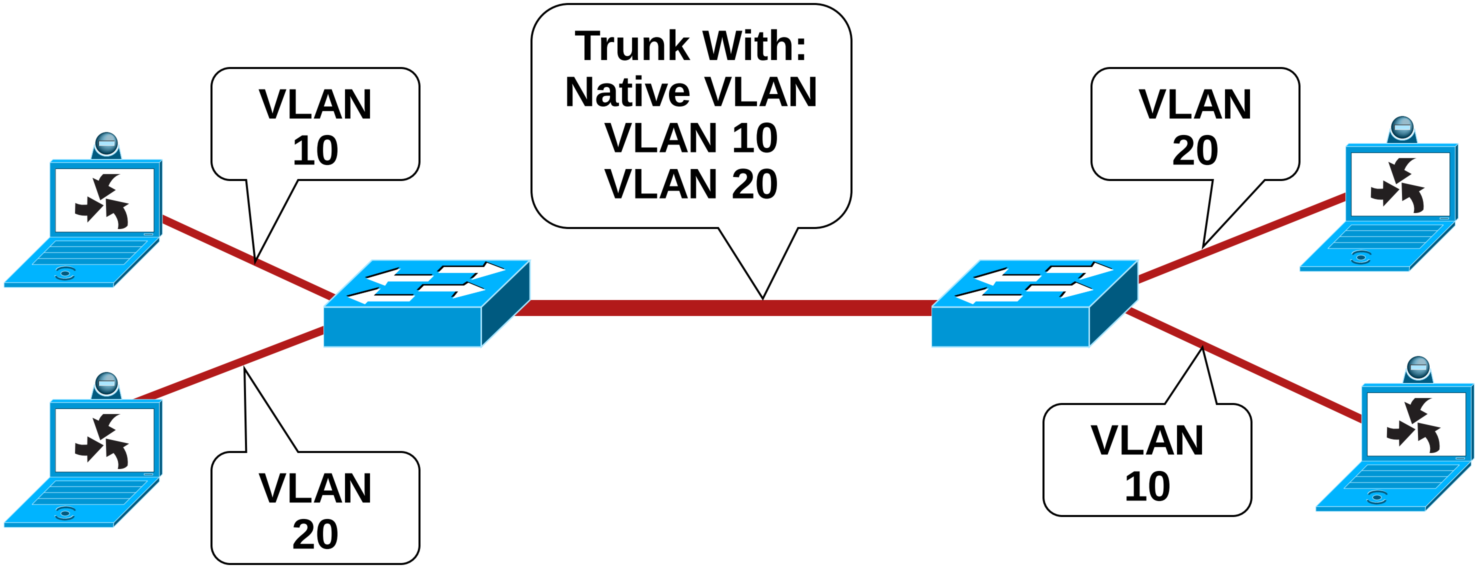
    ARP Attacks

    Spoofing Attacks

    General Attacks

- Summary

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

© 2007 Cisco Systems, Inc. All rights reserved.

Dynamic Trunk Protocol (DTP)

- What is DTP?

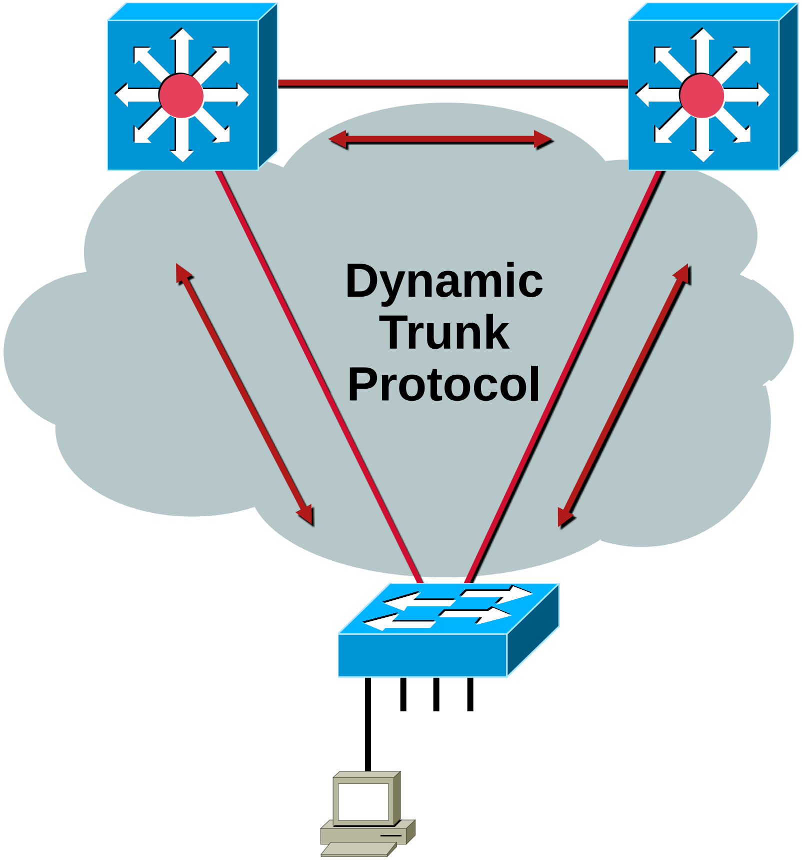
  Automates 802.1x/ISL
  Trunk configuration

  Operates between switches
  (Cisco IP phone is a switch)

  Does not operate on routers

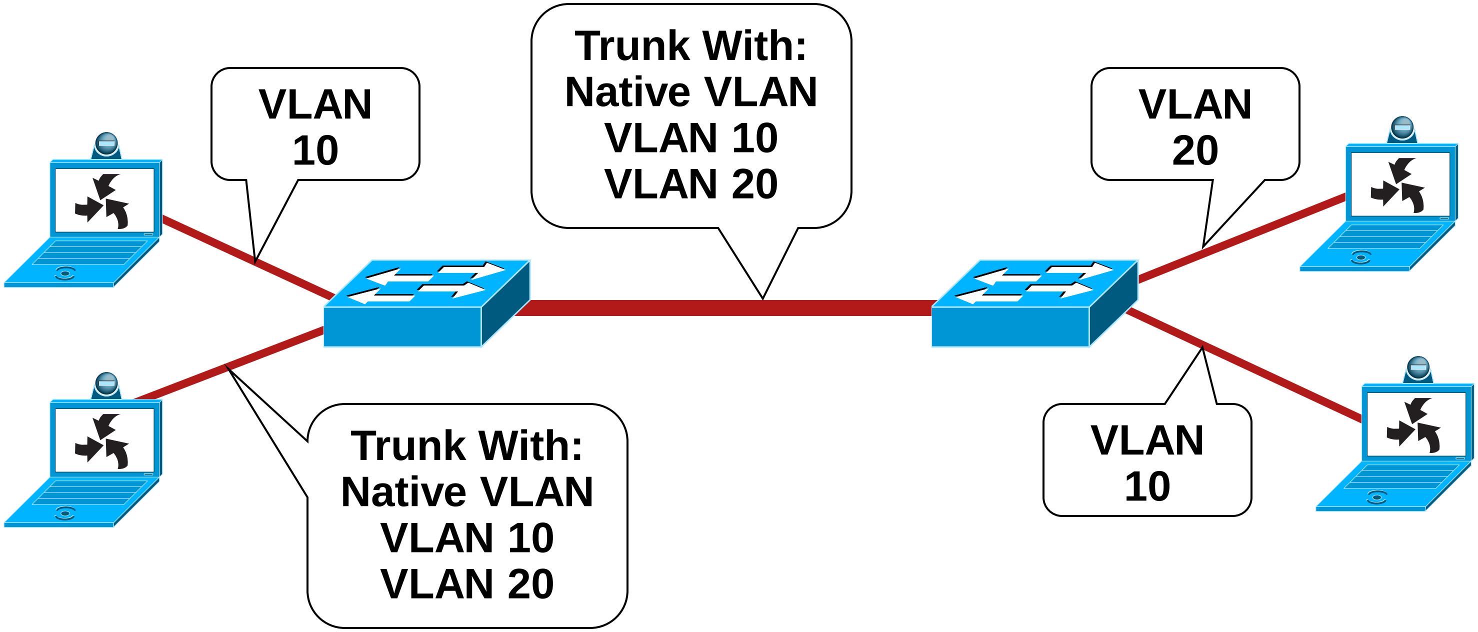
  Support varies, check
  your device

- 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”



© 2007 Cisco Systems, Inc. All rights reserved.

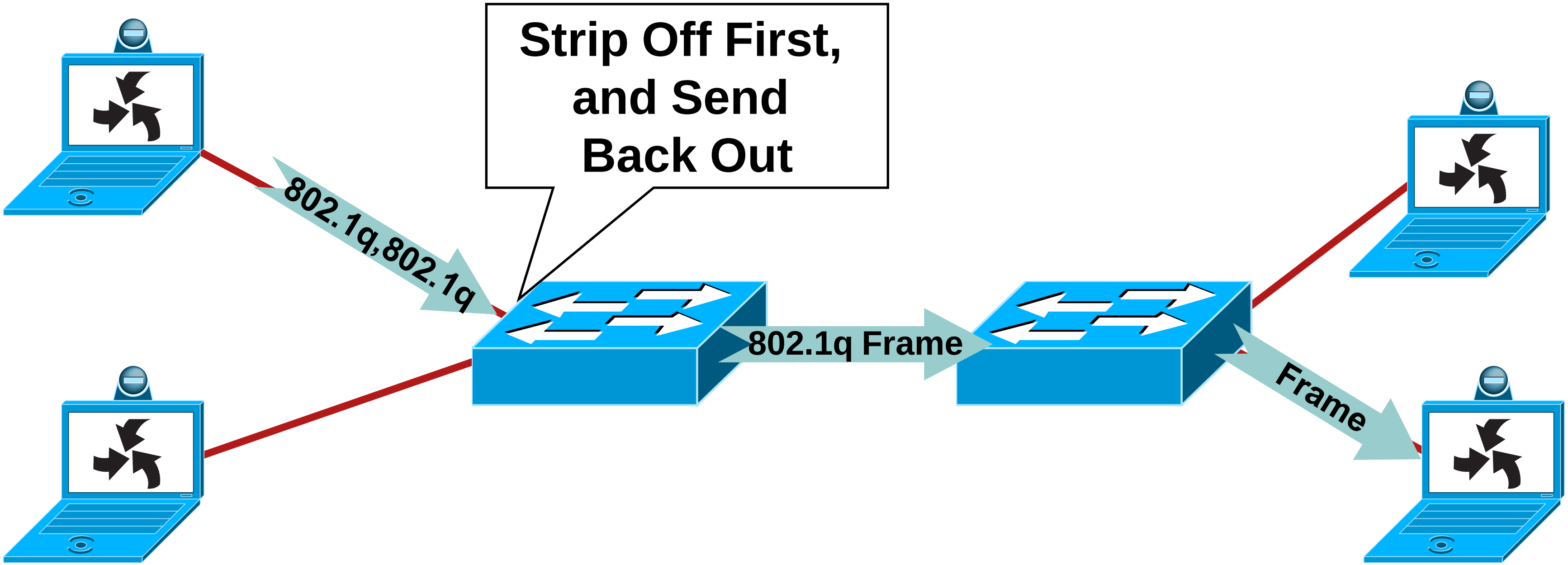
Basic VLAN Hopping Attack


VLAN 10
Trunk With: Native VLAN VLAN 10 VLAN 20
VLAN 20
Trunk With: Native VLAN VLAN 10 VLAN 20
VLAN 10

- 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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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

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

© 2007 Cisco Systems, Inc. All rights reserved.

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
- Use PC Voice VLAN Access on phones that support it
- Use 802.1q tag all on the trunk port

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures
  - VLAN Hopping
  - MAC Attacks
  - DHCP Attacks
  - ARP Attacks
  - Spoofing Attacks
  - General Attacks
- Summary

© 2007 Cisco Systems, Inc. All rights reserved.

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 Fs = Broadcast

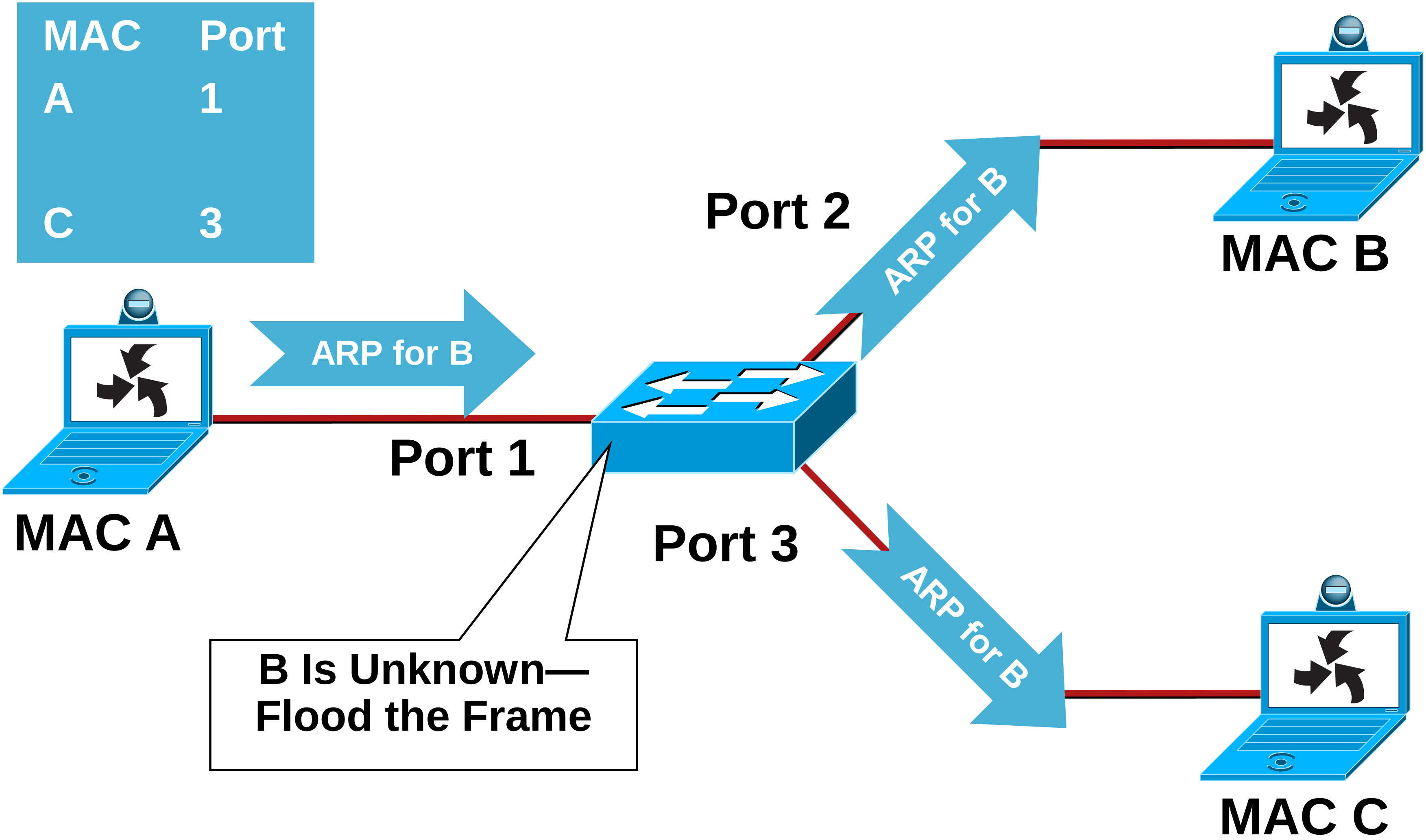
FFFF.FFFF.FFFF

- 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
- All CAM tables have a fixed size

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Normal CAM Behavior (1/3)

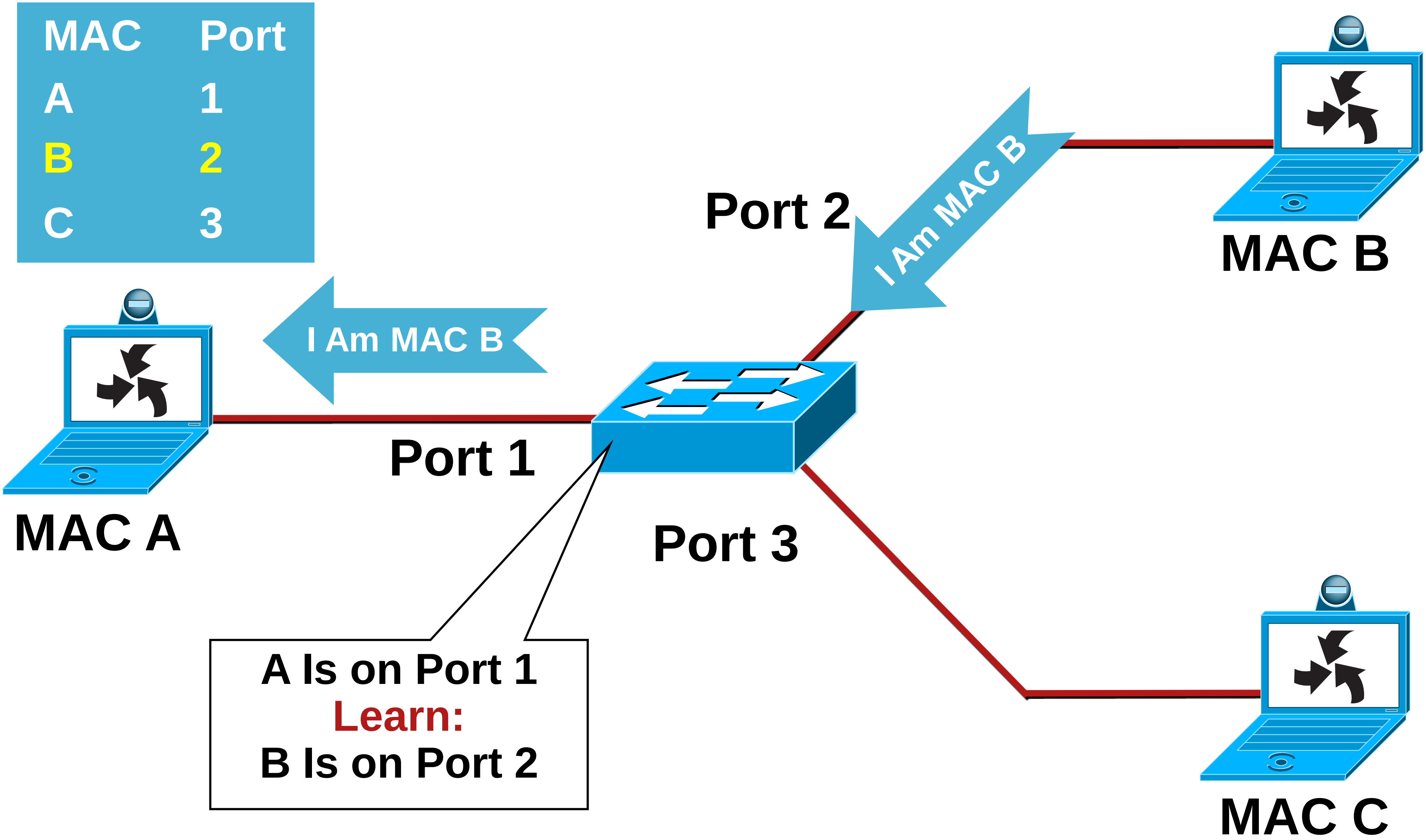
MAC	Port
A	1
C	3



B Is Unknown—
Flood the Frame

© 2007 Cisco Systems, Inc. All rights reserved.

Normal CAM Behavior (2/3)



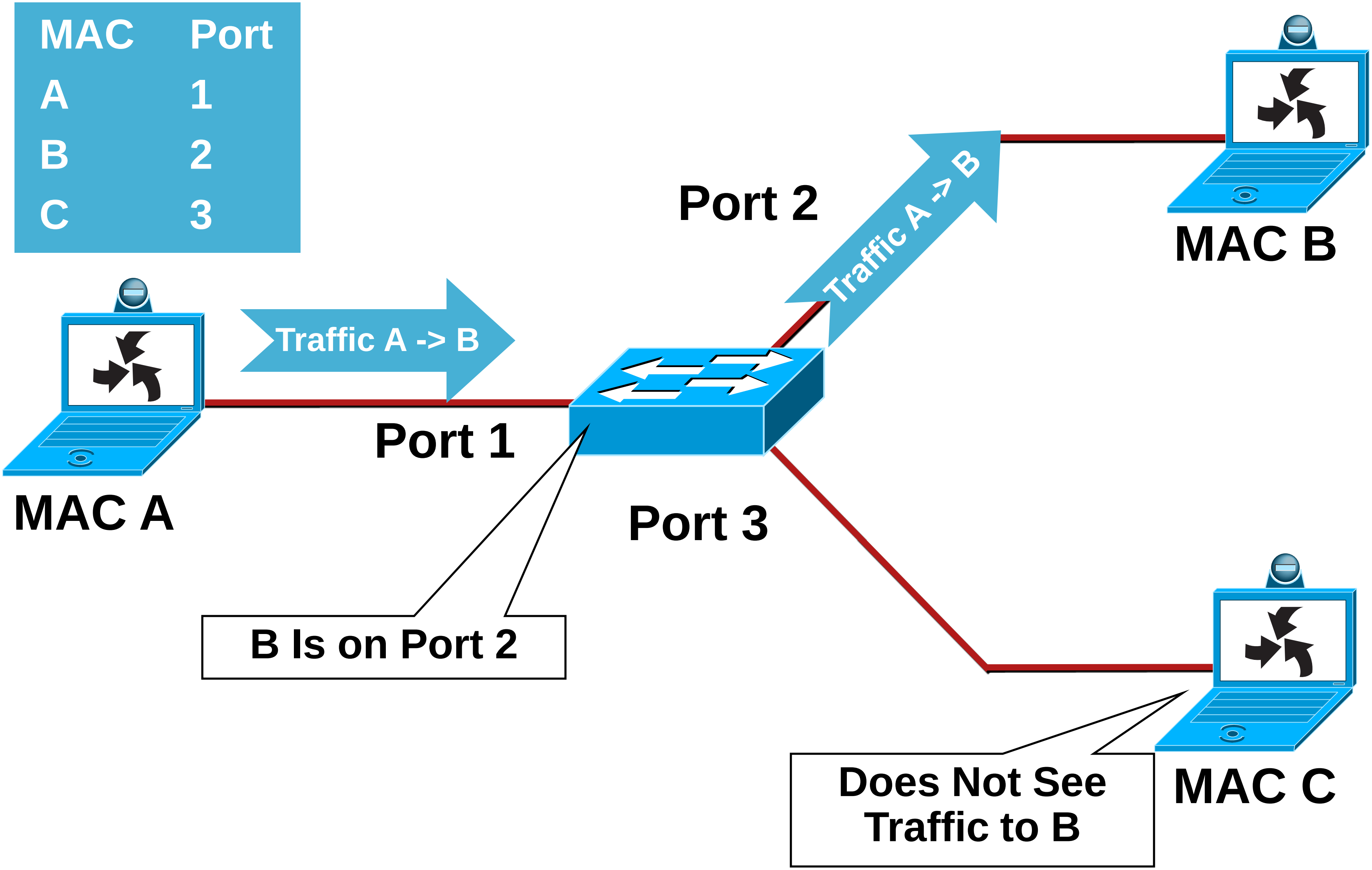
MAC	Port
A	1
B	2
C	3

A Is on Port 1
Learn:
B Is on Port 2

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Normal CAM Behavior (3/3)

MAC	Port
A	1
B	2
C	3



B Is on Port 2

Does Not See Traffic to B

© 2007 Cisco Systems, Inc. All rights reserved.

CAM Overflow (1/2)

- macof tool since 1999

  About 100 lines of perl

  Included in “dsniff”

- Attack successful by exploiting the size limit on CAM tables

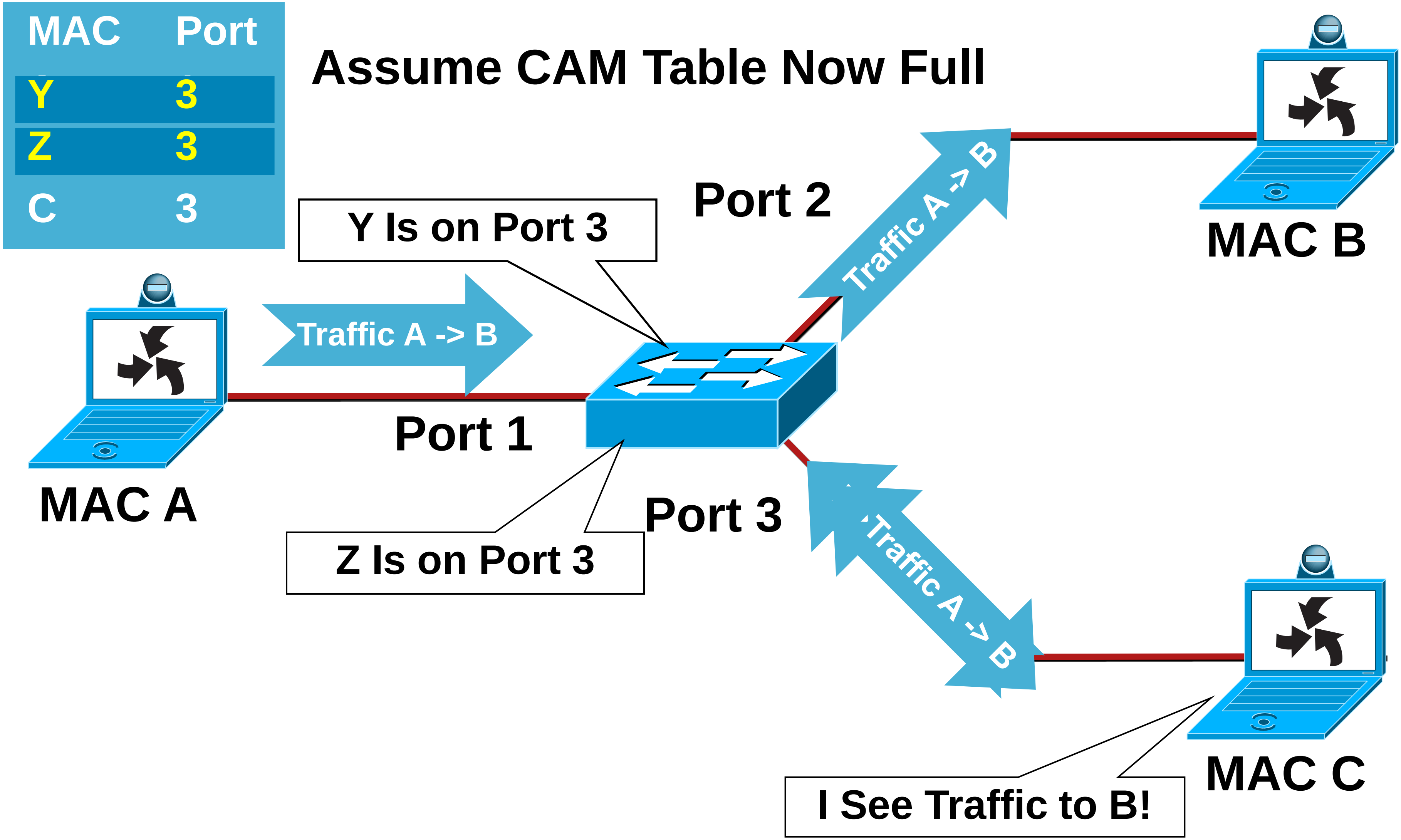
- Yersinia—flavor of the month attack tool

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

CAM Overflow (2/2)

MAC	Port
Y	3
Z	3
C	3

Assume CAM Table Now Full



© 2007 Cisco Systems, Inc. All rights reserved.

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/

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

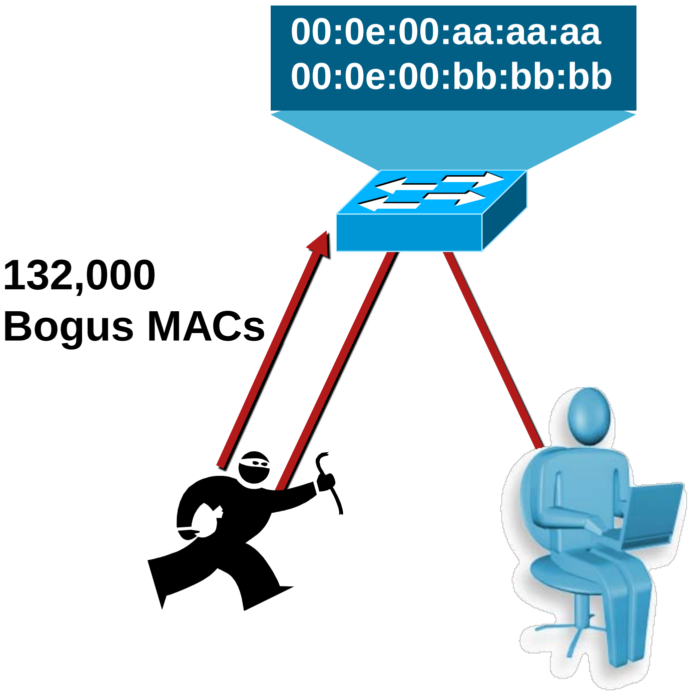
CAM Table Full

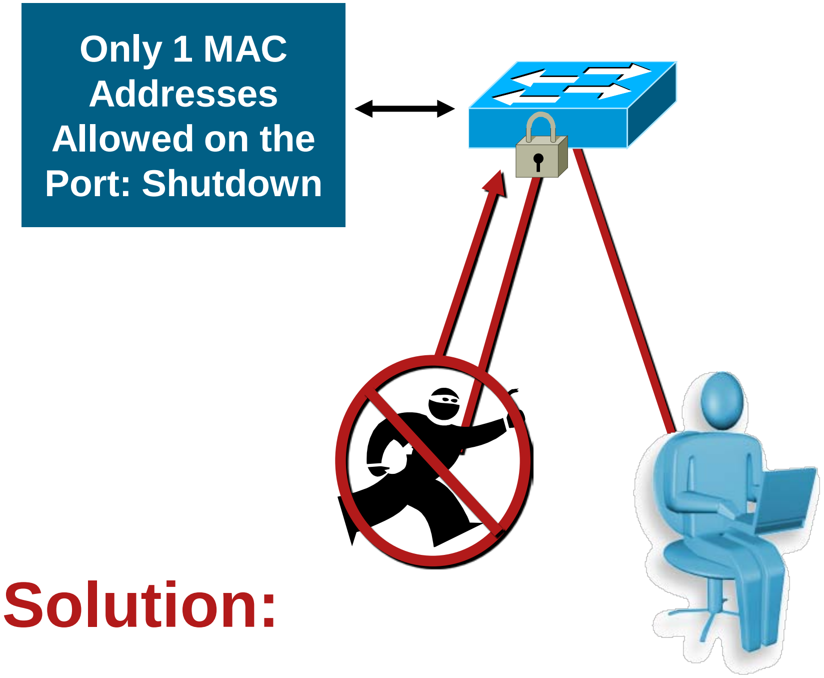
- Once the CAM table on the switch is full, traffic without a CAM entry is flooded out every port on that VLAN
- This will turn a VLAN on a switch basically into a hub
- This attack will also fill the CAM tables of adjacent switches

```
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 MACs on an Interface





Solution:

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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

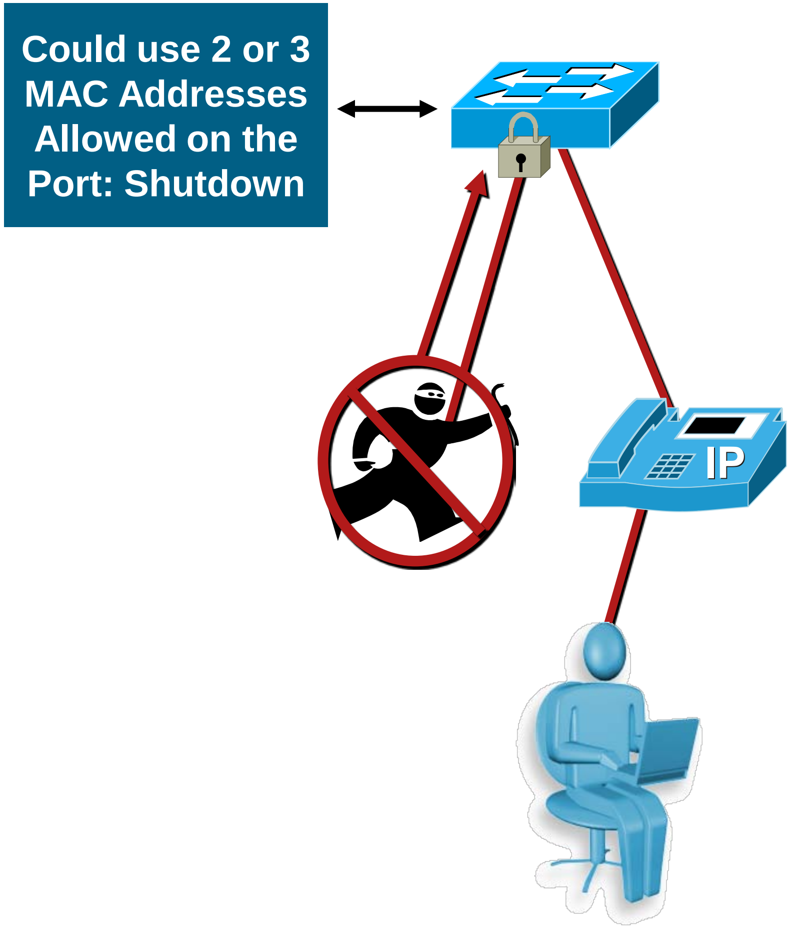
Countermeasures for MAC Attacks with IP Phones

- Phones can use 2 or 3 depending on the switch hardware and software

  Some switches look at the CDP traffic and some don't, if they don't, they need 2, if they do they need 3

  Some hardware (3550) will always need 3

- Default config is disable port, might want to restrict for VoIP
- This feature is to protect that switch, you can make the number anything you like as long as you don't overrun the CAM table



Could use 2 or 3 MAC Addresses Allowed on the Port: Shutdown

© 2007 Cisco Systems, Inc. All rights reserved.

Port Security: Example Config

Will Enable Voice to Work Under Attack

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
```

- Number is not to control access, it is to protect the switch from attack
- Depending on security policy, disabling the port might be preferred, even with VoIP
- 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

New Features for Port Security

New Commands

IOS®

```
switchport port-security
switchport port-security maximum 1 vlan voice
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
snmp-server enable traps port-security trap-rate 5
```

- Per port per VLAN max MAC addresses
- Restrict now will let you know something has happened—you will get an SNMP trap

  Everyone asked so Cisco did it

© 2007 Cisco Systems, Inc. All rights reserved.

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
- CHANGE XXX 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
- Would want to limit the SNMP message, don’t want 1000’s
- Voice MOS scores under attack were very good,
  as long as QoS was configured

MOS—Mean Opinion Score—http://en.wikipedia.org/wiki/Mean_Opinion_Score

© 2007 Cisco Systems, Inc. All rights reserved.

Building the Layers

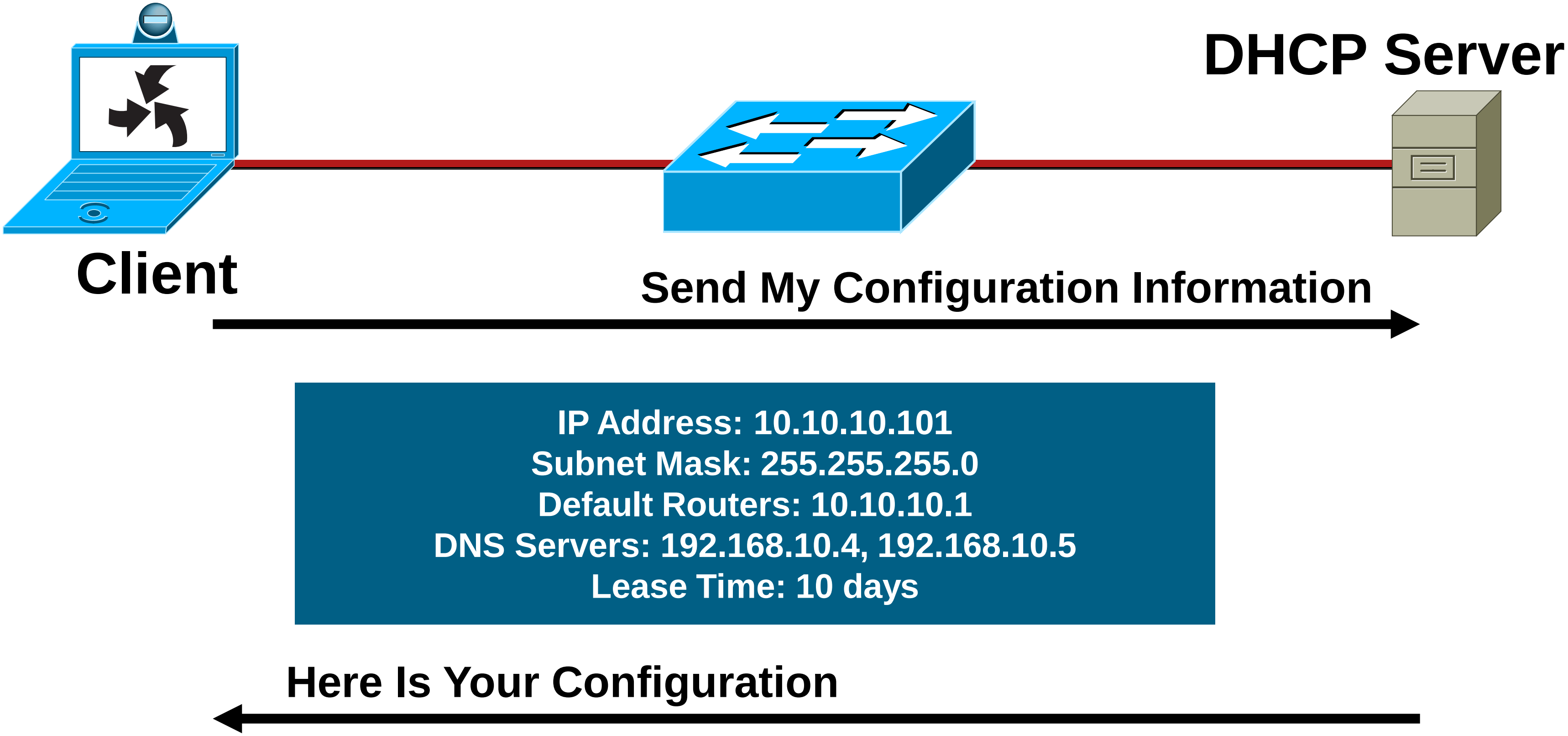
- Port Security prevents CAM attacks and DHCP starvation attacks

Port Security

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures
  - VLAN Hopping
  - MAC Attacks
  - DHCP Attacks
  - ARP Attacks
  - Spoofing Attacks
  - General Attacks
- Summary

DHCP Function: High Level



DHCP Server

Client

Send My Configuration Information

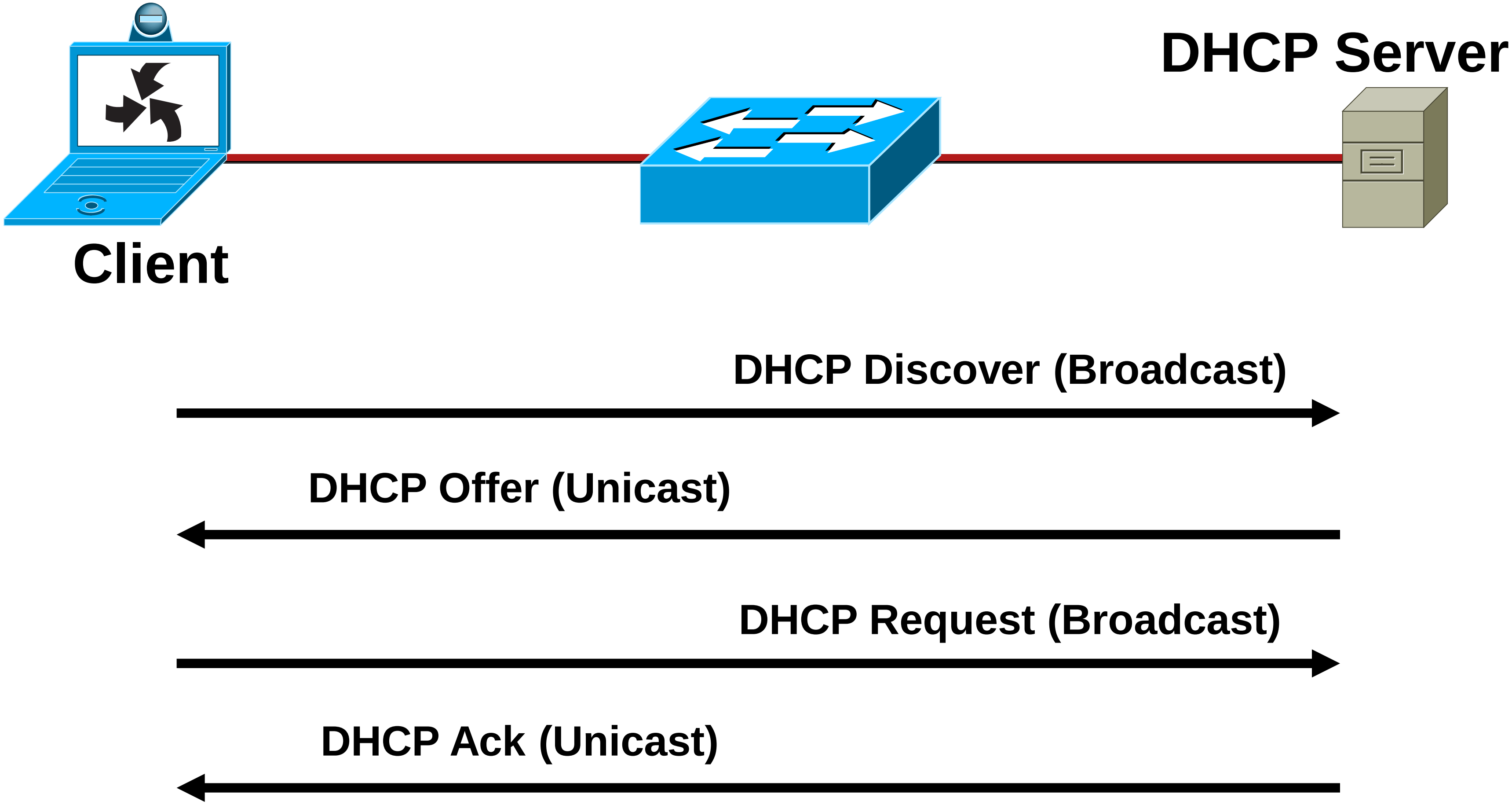
IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease Time: 10 days

Here Is Your Configuration

- 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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

DHCP Function: Lower Level



DHCP Server

Client

DHCP Discover (Broadcast)

DHCP Offer (Unicast)

DHCP Request (Broadcast)

DHCP Ack (Unicast)

- DHCP defined by RFC 2131

DHCP Function: Lower Level

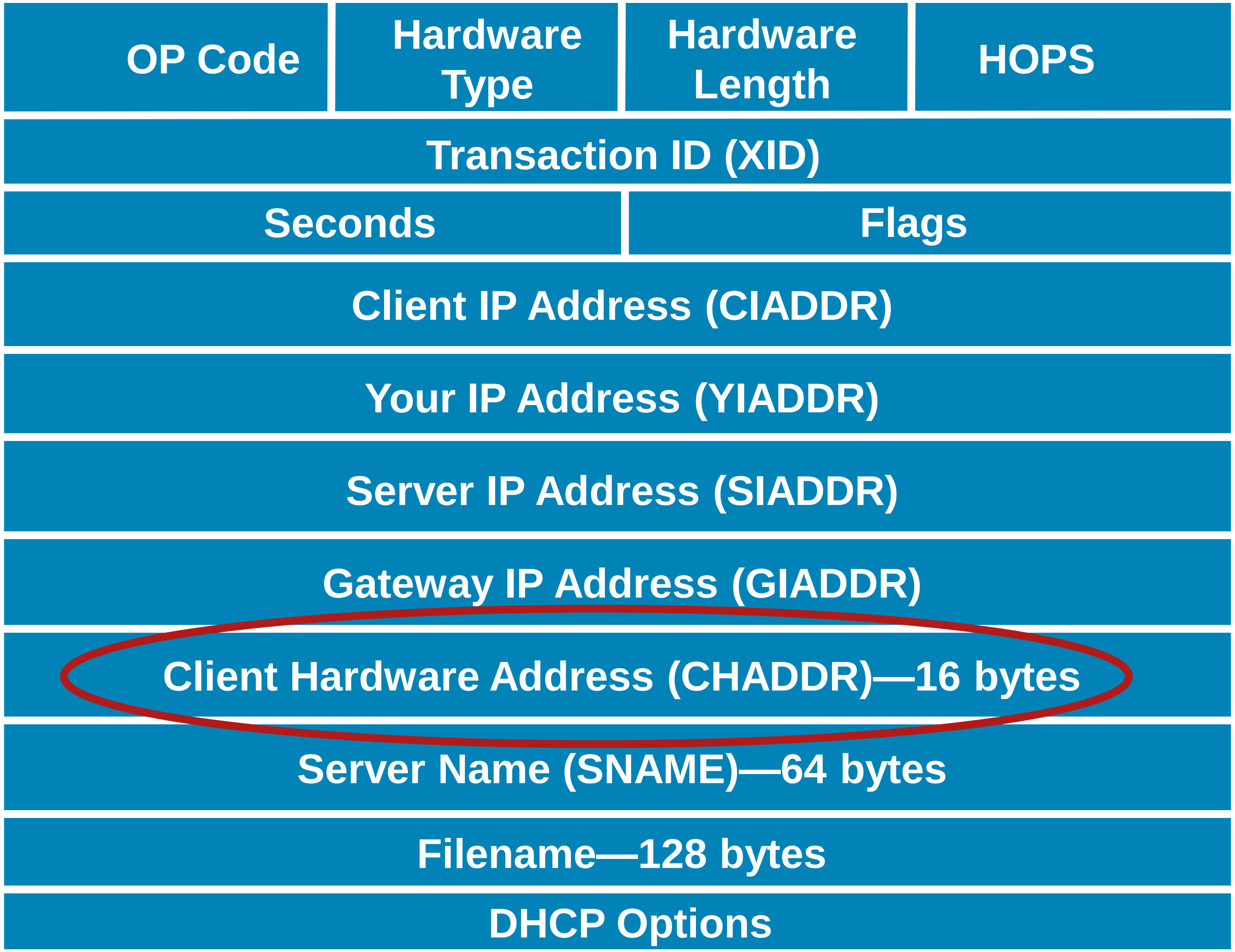
DHCP Request/Reply Types

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.

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

DHCP Function: Lower Level

IPv4 DHCP Packet Format



OP Code | Hardware Type | Hardware Length | HOPS

Transaction ID (XID)

Seconds | Flags

Client IP Address (CIADDR)

Your IP Address (YIADDR)

Server IP Address (SIADDR)

Gateway IP Address (GIADDR)

Client Hardware Address (CHADDR)—16 bytes

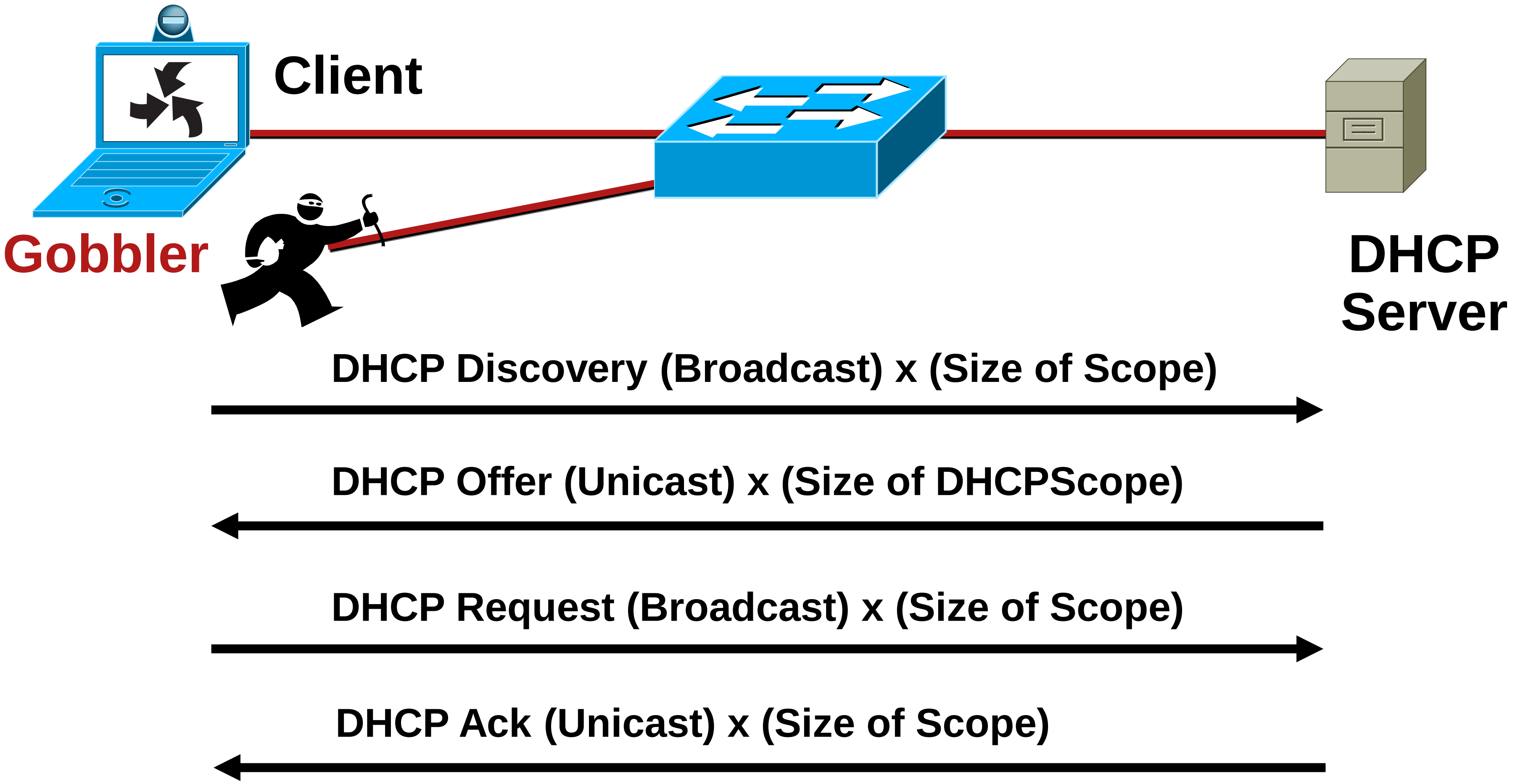
Server Name (SNAME)—64 bytes

Filename—128 bytes

DHCP Options

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

DHCP Attack Types
DHCP Starvation Attack



Client

Gobbler

DHCP Server

DHCP Discovery (Broadcast) x (Size of Scope)

DHCP Offer (Unicast) x (Size of DHCPScope)

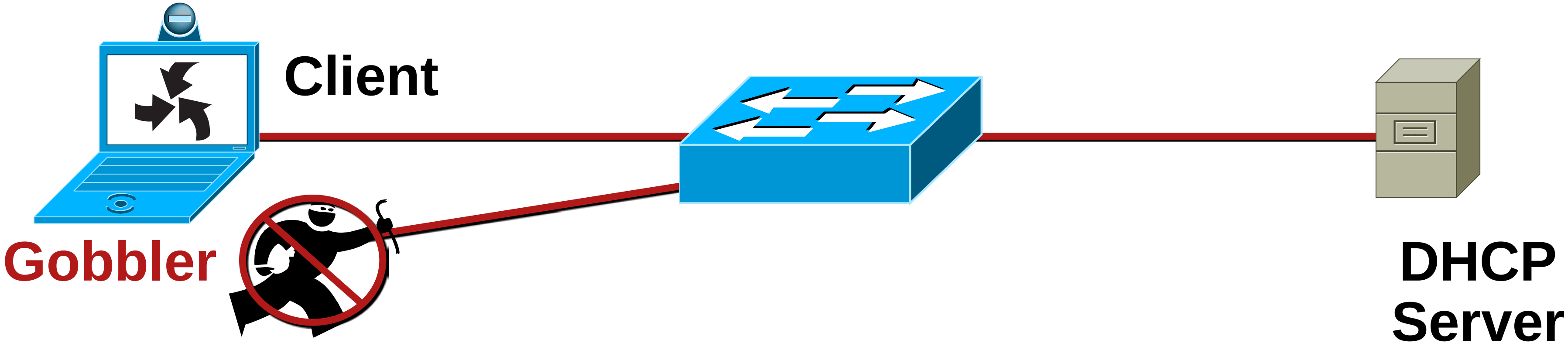
DHCP Request (Broadcast) x (Size of Scope)

DHCP Ack (Unicast) x (Size of Scope)

- Gobbler/DHCPx 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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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

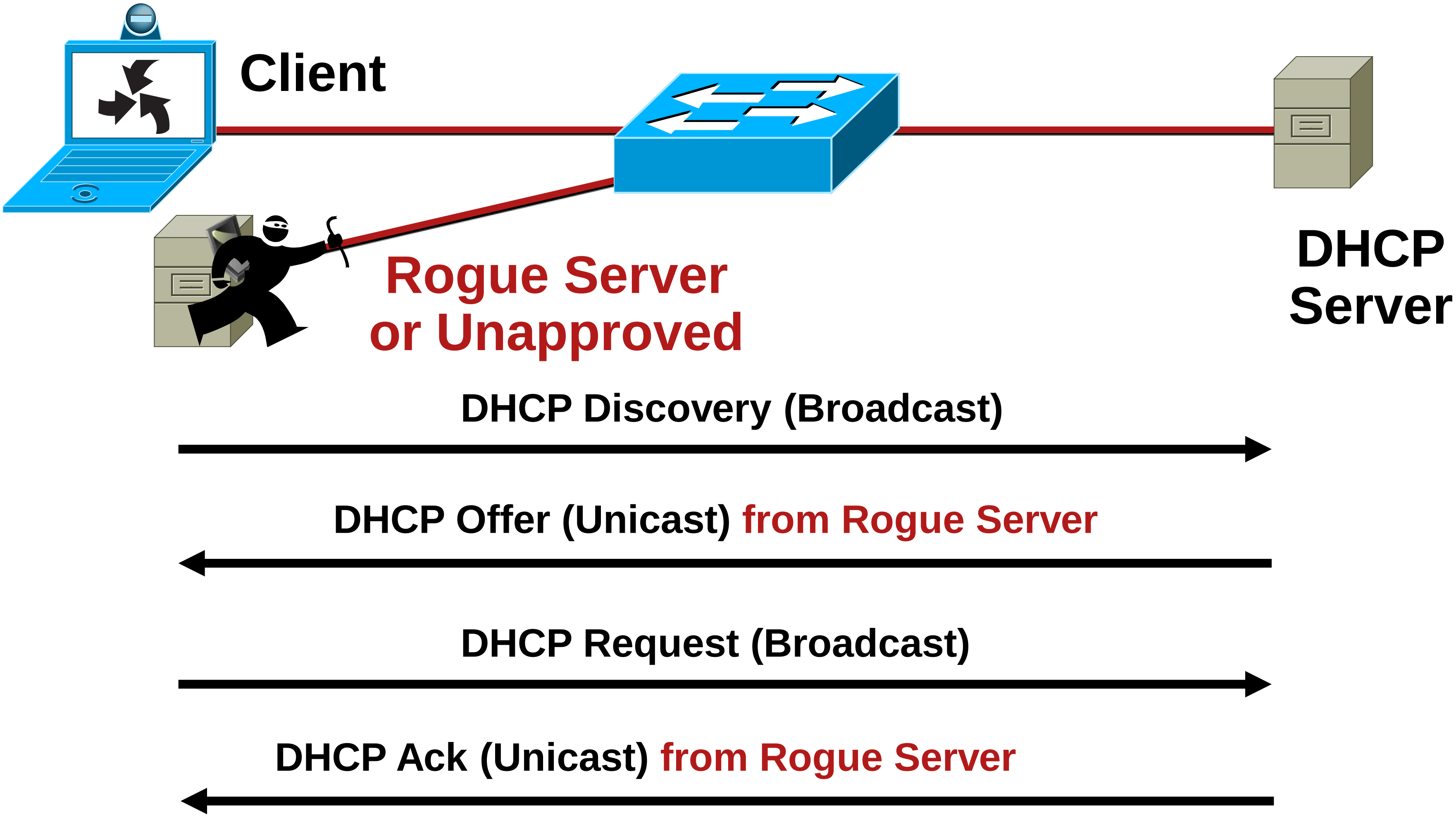
```
set port security 5/1 enable
set port security 5/1 port max 1
set port security 5/1 violation restrict
set port security 5/1 age 2
set port security 5/1 timer-type inactivity
```

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
```

© 2007 Cisco Systems, Inc. All rights reserved.

DHCP Attack Types
Rogue DHCP Server Attack



Client

Rogue Server or Unapproved

DHCP Server

DHCP Discovery (Broadcast)

DHCP Offer (Unicast) from Rogue Server

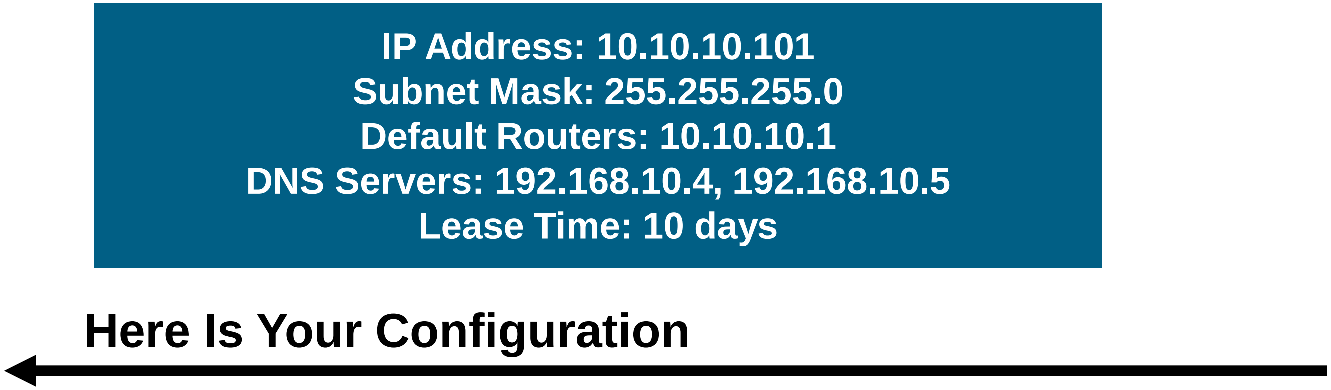
DHCP Request (Broadcast)

DHCP Ack (Unicast) from Rogue Server

© 2007 Cisco Systems, Inc. All rights reserved.

DHCP Attack Types
Rogue DHCP Server Attack

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



IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease Time: 10 days

Here Is Your Configuration

- What do you see as a potential problem with incorrect information?

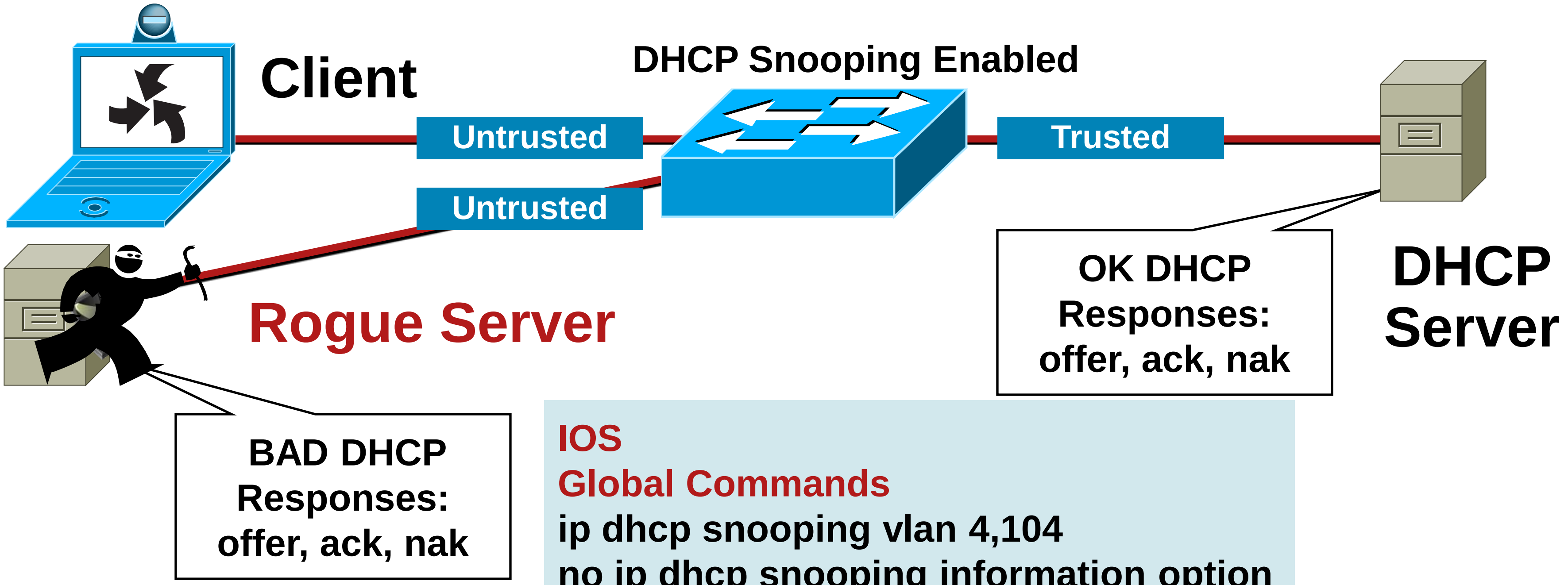
  Wrong Default Gateway—Attacker is the gateway

  Wrong DNS server—Attacker is DNS server

  Wrong IP Address—Attacker does DOS with incorrect IP

© 2007 Cisco Systems, Inc. All rights reserved.

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping



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

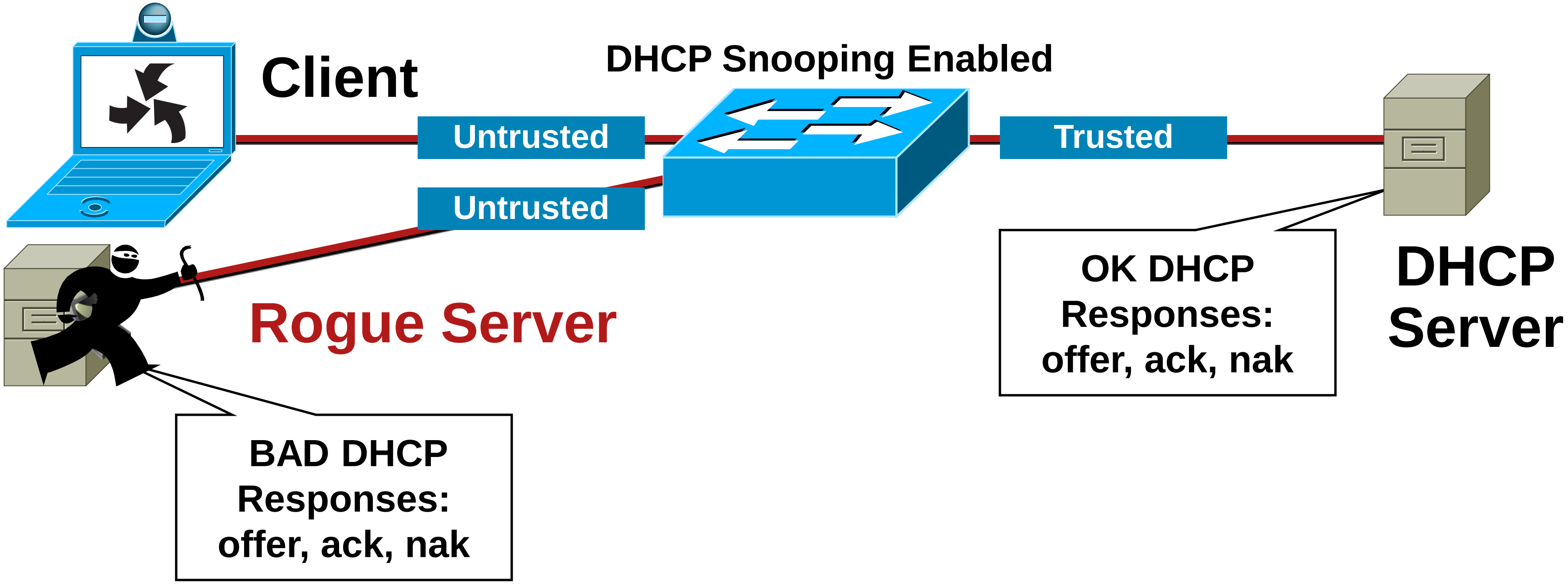
Interface Commands

```
ip dhcp snooping trust
```

- By default all ports in the VLAN are untrusted

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Countermeasures for DHCP Attacks Rogue DHCP Server = DHCP Snooping



OK DHCP Responses: offer, ack, nak

BAD DHCP Responses: offer, ack, nak

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

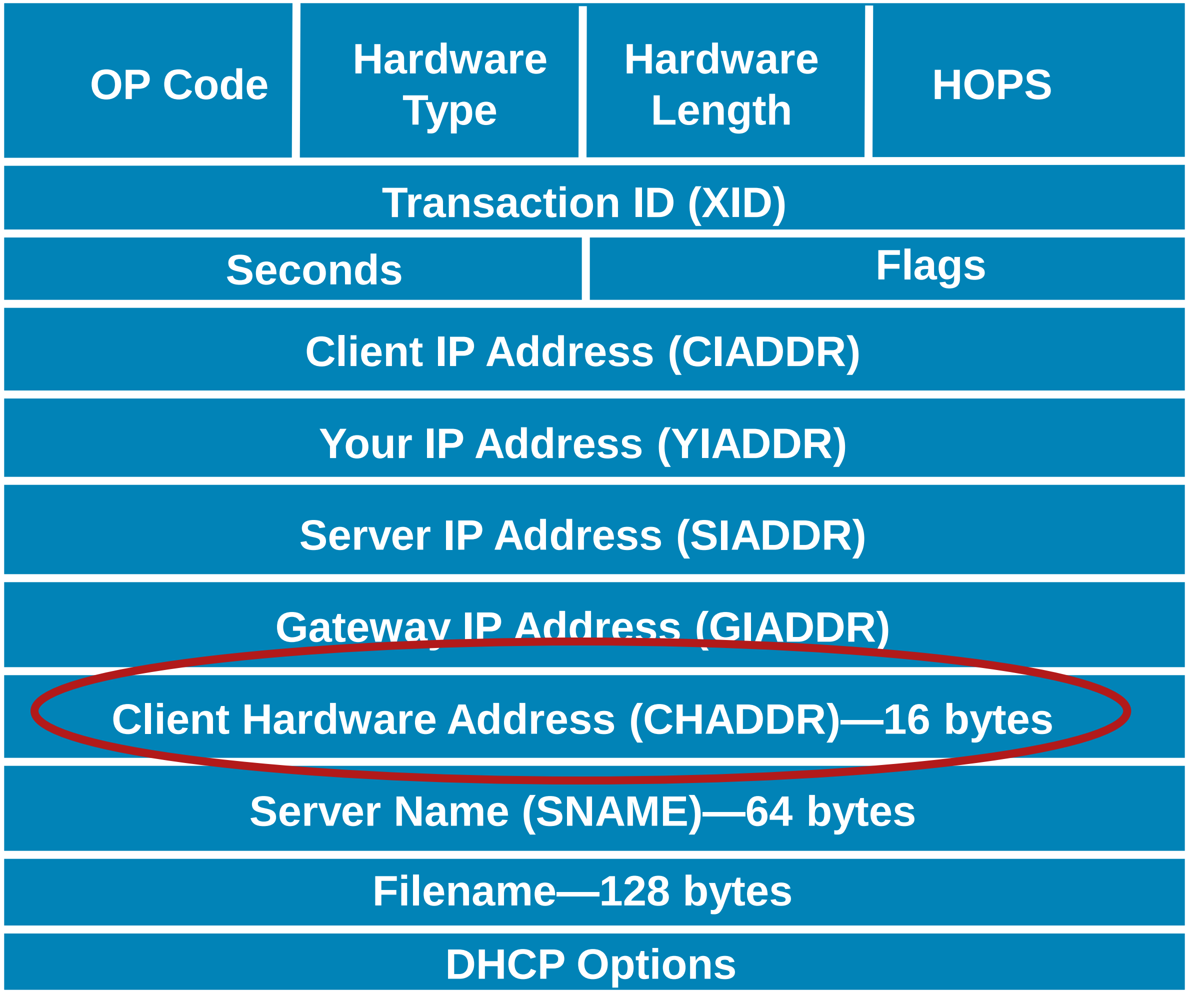
Advanced Configuration DHCP Snooping

- 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 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


OP Code
Hardware Type
Hardware Length
HOPS
Transaction ID (XID)
Seconds
Flags
Client IP Address (CIADDR)
Your IP Address (YIADDR)
Server IP Address (SIADDR)
Gateway IP Address (GIADDR)
Client Hardware Address (CHADDR)—16 bytes
Server Name (SNAME)—64 bytes
Filename—128 bytes
DHCP Options

Note: some switches have this on by default, and others don't; please check the documentation for settings

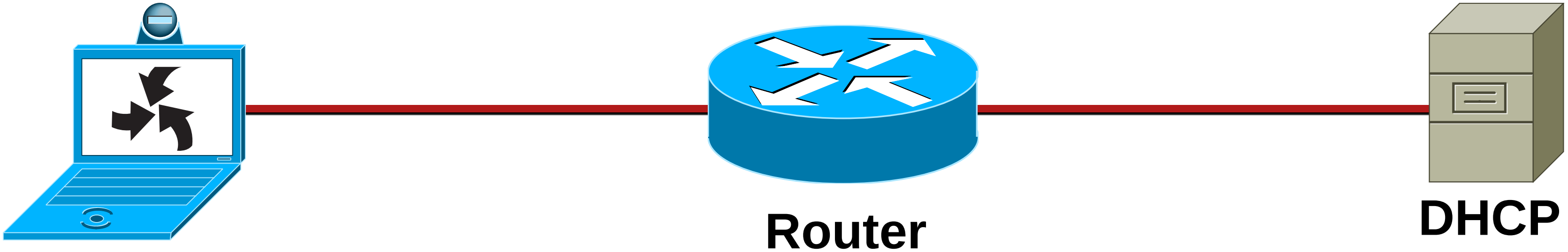
© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

DHCP Rogue Server

- If there are switches in the network that will not support DHCP Snooping, you can configure VLAN ACLs 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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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)

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

DHCP Snooping Capacity

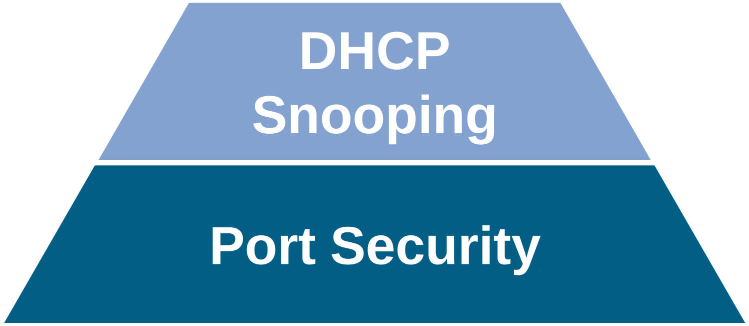
- All DHCP Snooping Binding tables have limits
- All entries stay in the binding table until the lease runs out
- If you have a mobile work environment, reduce the lease time to make sure the binding entries will be removed

```
sh ip dhcp snooping binding
MacAddress            IpAddress        Lease(sec)  Type            VLAN   Interface
------------------    ---------------  ----------  -------------   ----   --------------------
00:03:47:B5:9F:AD     10.120.4.10      193185      dhcp-snooping   4      FastEthernet3/18
```

© 2007 Cisco Systems, Inc. All rights reserved.

Building the Layers

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



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter measures

  VLAN Hopping

  MAC Attacks

  DHCP Attacks

  ARP Attacks

  Spoofing Attacks

  General Attacks

- Summary

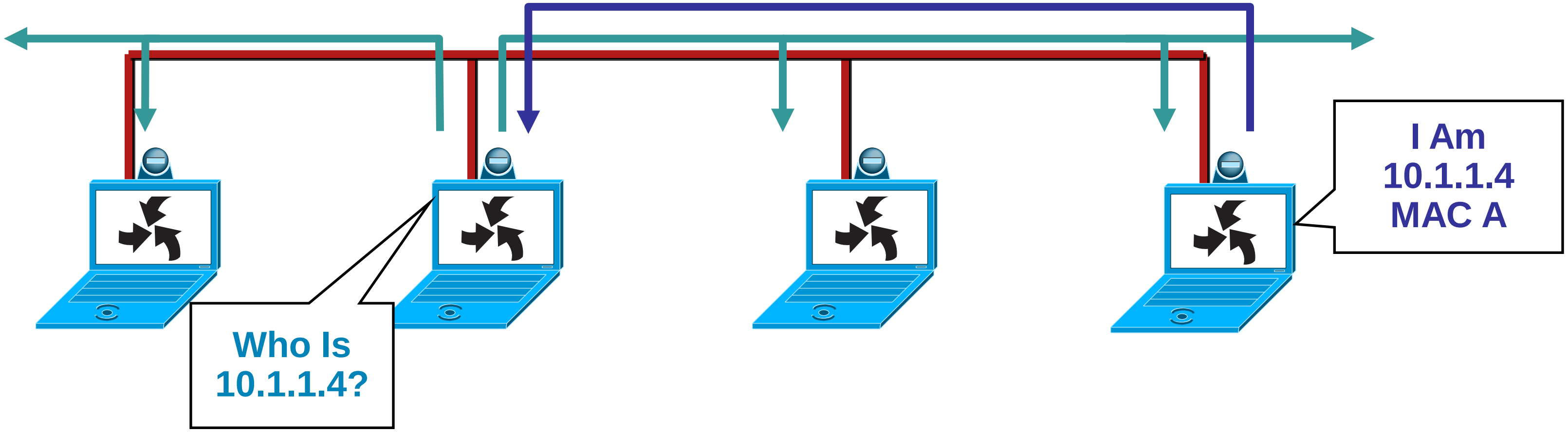
© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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

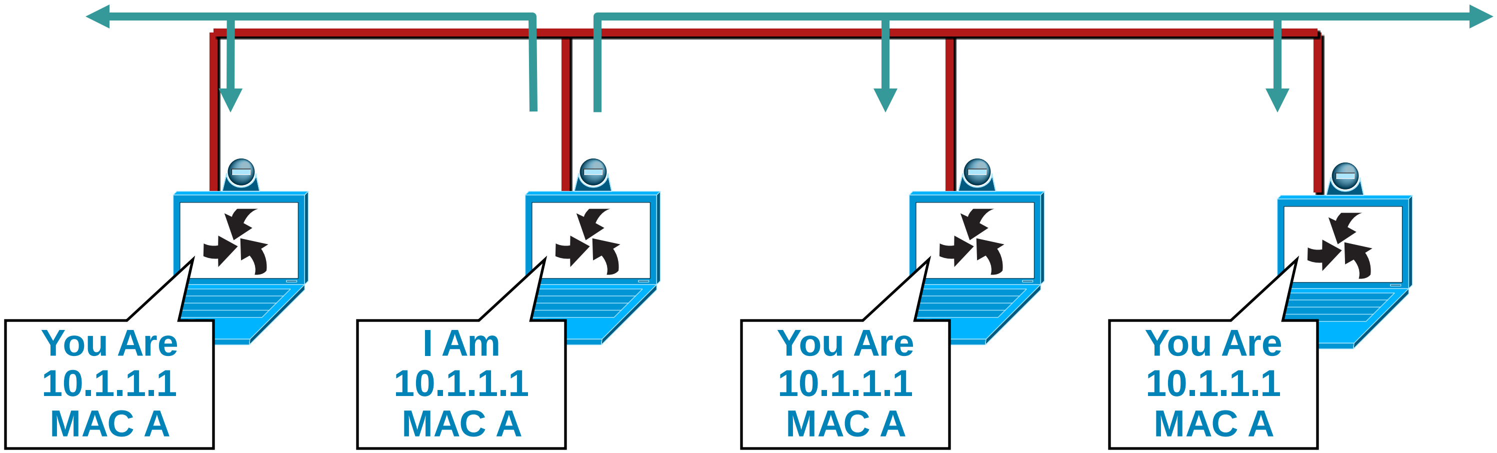
- All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply



© 2007 Cisco Systems, Inc. All rights reserved.

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



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

ARP Attack Tools

- Many tools on the Net for ARP man-in-the-middle attacks

  Dsniff, Cain & Abel, ettercap, Yersinia, etc...

- ettercap—http://ettercap.sourceforge.net/index.php

  Some are second or third generation of ARP attack tools

  Most have a very nice GUI, and is almost point and click

  Packet Insertion, many to many ARP attack

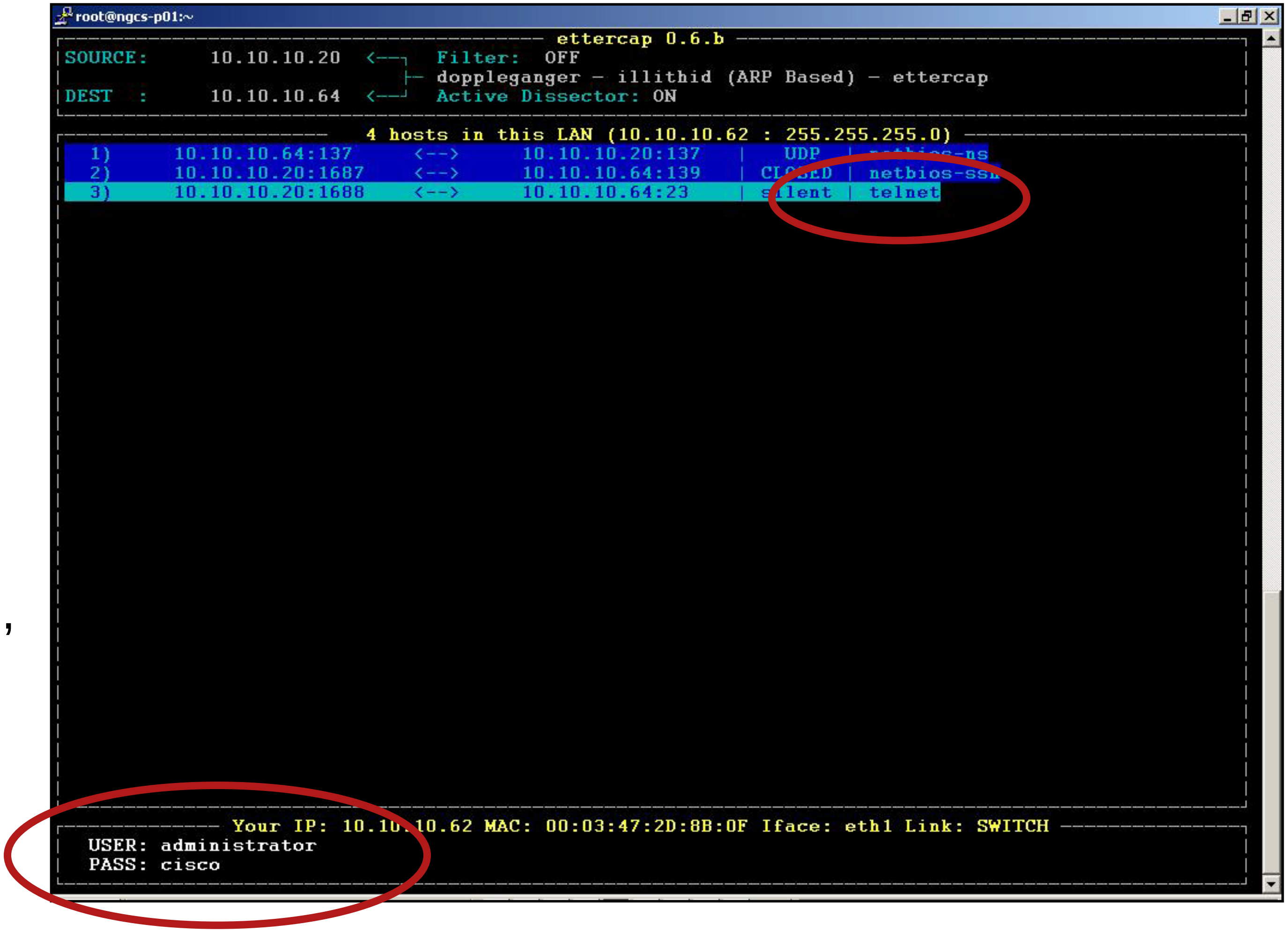
- All of them capture the traffic/passwords of applications

  FTP, Telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, RIP, OSPF, PPTP, MS-CHAP, SOCKS, X11, IRC, ICQ, AIM, SMB, Microsoft SQL, etc…

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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



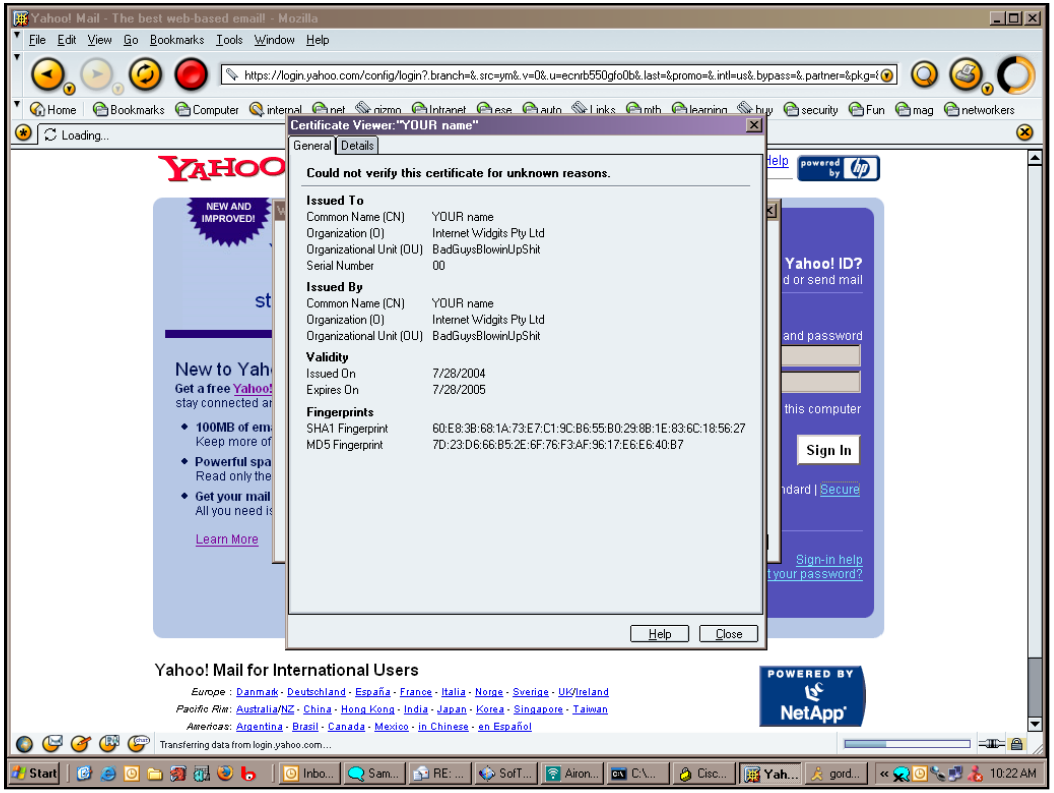
```
---------------------------------- ettercap 0.6.b ---------------------------------
|SOURCE:      10.10.10.20  <--┐  Filter:  OFF
|                             ├- doppleganger - illithid (ARP Based) - ettercap
|DEST   :     10.10.10.64  <--┘  Active Dissector: ON
-----------------------------------------------------------------------------------

--------------------- 4 hosts in this LAN (10.10.10.62 : 255.255.255.0) ----------
|  1)    10.10.10.64:137     <-->    10.10.10.20:137    |  UDP    | netbios-ns
|  2)    10.10.10.20:1687    <-->    10.10.10.64:139    | CLOSED  | netbios-ssn
|  3)    10.10.10.20:1688    <-->    10.10.10.64:23     | silent  | telnet

------------ Your IP: 10.10.10.62 MAC: 00:03:47:2D:8B:0F Iface: eth1 Link: SWITCH --
   USER: administrator
   PASS: cisco
```

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


Yahoo! Mail - The best web-based email! - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://login.yahoo.com/config/login?.branch=&.src=ym&.v=0&.u=ecnrb550gfo0b&.last=&promo=&.intl=us&.bypass=&.partner=&pkg=
Loading...
Transferring data from login.yahoo.com...
Yahoo! Mail for International Users
Sign In
Help
Close

Certificate Viewer:"YOUR name"

General | Details

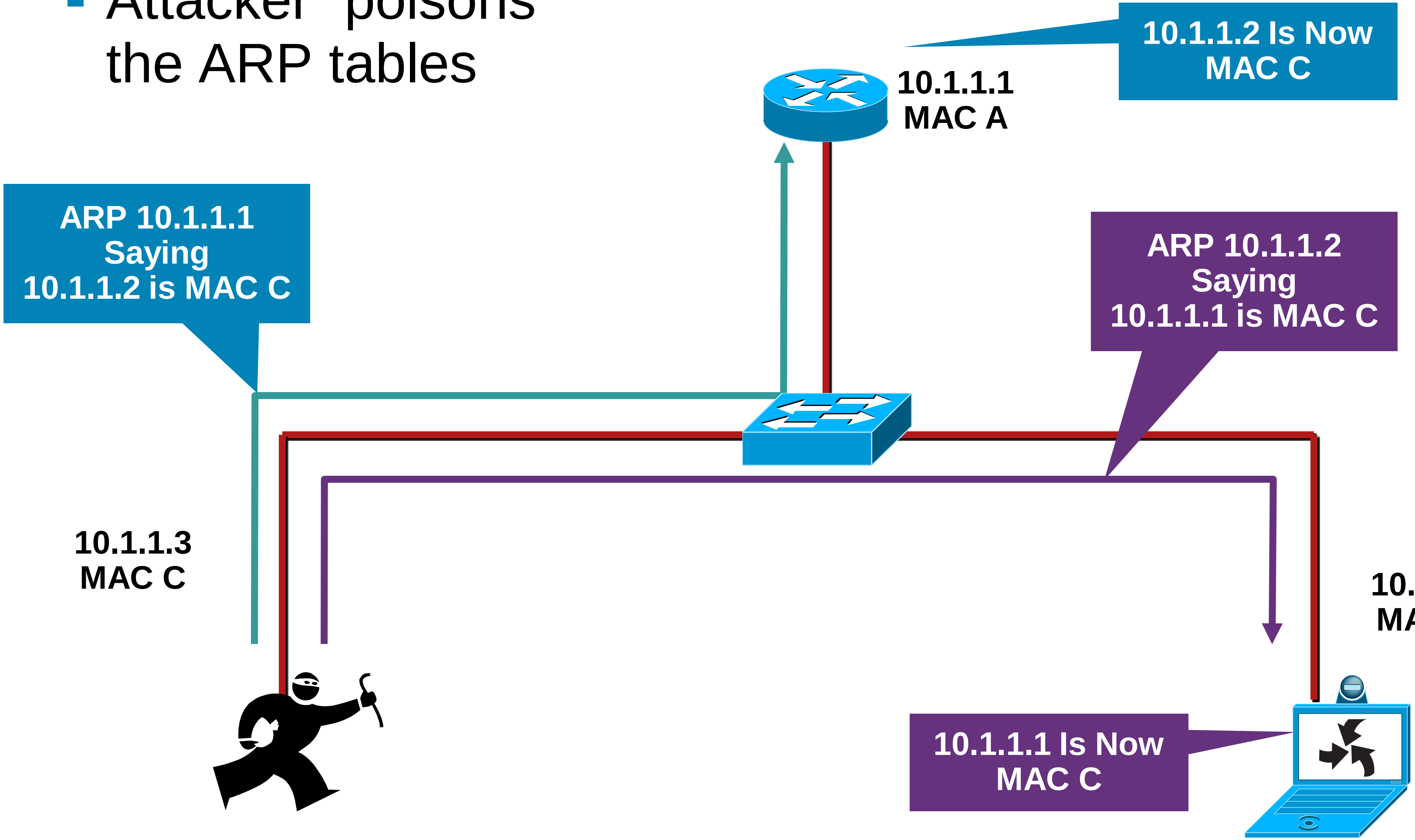
Could not verify this certificate for unknown reasons.

```
Issued To
Common Name (CN)           YOUR name
Organization (O)           Internet Widgits Pty Ltd
Organizational Unit (OU)   BadGuysBlowinUpShit
Serial Number              00
Issued By
Common Name (CN)           YOUR name
Organization (O)           Internet Widgits Pty Ltd
Organizational Unit (OU)   BadGuysBlowinUpShit
Validity
Issued On                  7/28/2004
Expires On                 7/28/2005
Fingerprints
SHA1 Fingerprint           60:E8:3B:68:1A:73:E7:C1:9C:B6:55:B0:29:8B:1E:83:6C:18:56:27
MD5 Fingerprint            7D:23:D6:66:B5:2E:6F:76:F3:AF:96:17:E6:E6:40:B7
```

© 2007 Cisco Systems, Inc. All rights reserved.

ARP Attack in Action

- Attacker “poisons” the ARP tables



10.1.1.2 Is Now MAC C

10.1.1.1
MAC A

ARP 10.1.1.1 Saying 10.1.1.2 is MAC C

ARP 10.1.1.2 Saying 10.1.1.1 is MAC C

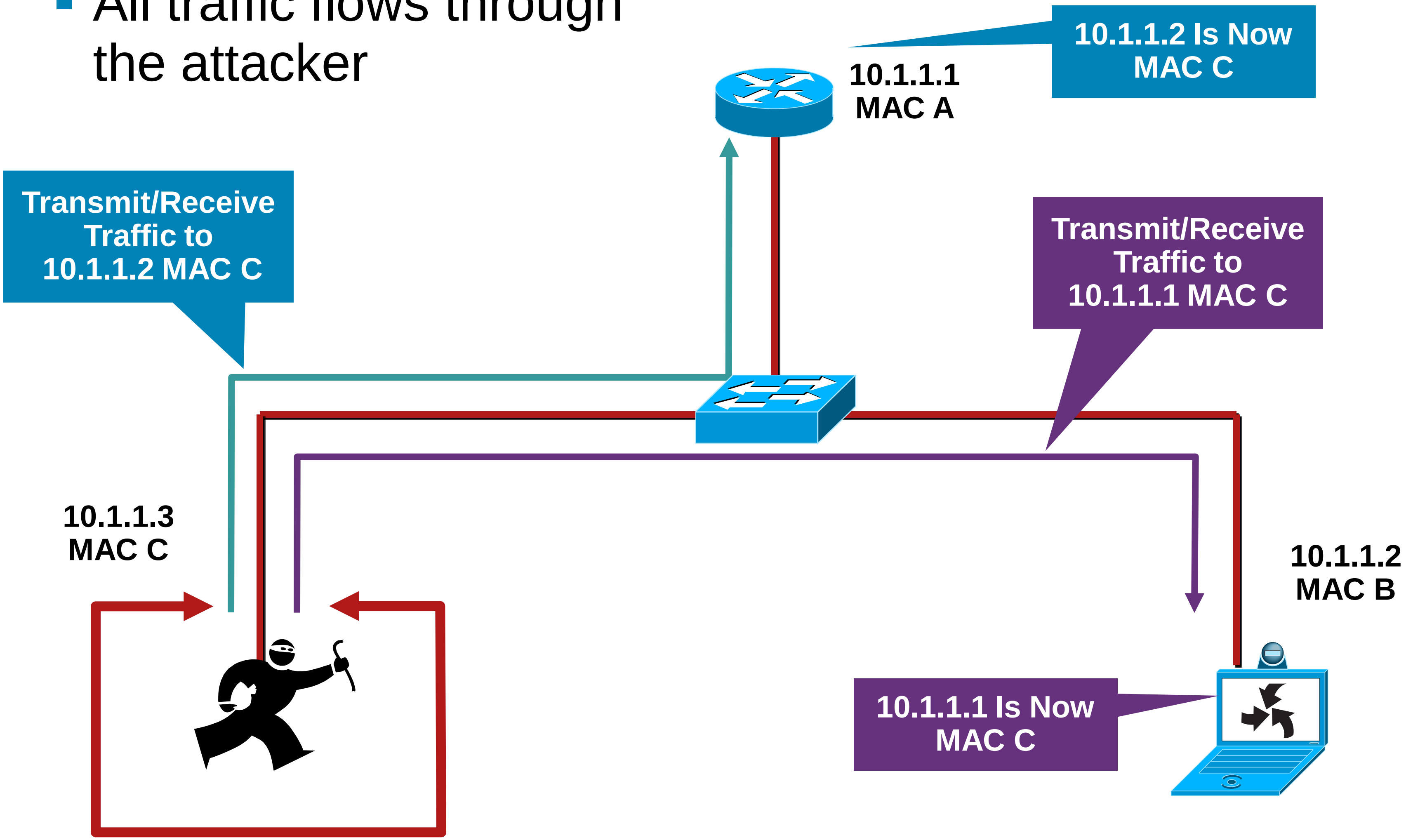
10.1.1.3
MAC C

10.1.1.2
MAC B

10.1.1.1 Is Now MAC C

ARP Attack in Action

- All traffic flows through the attacker

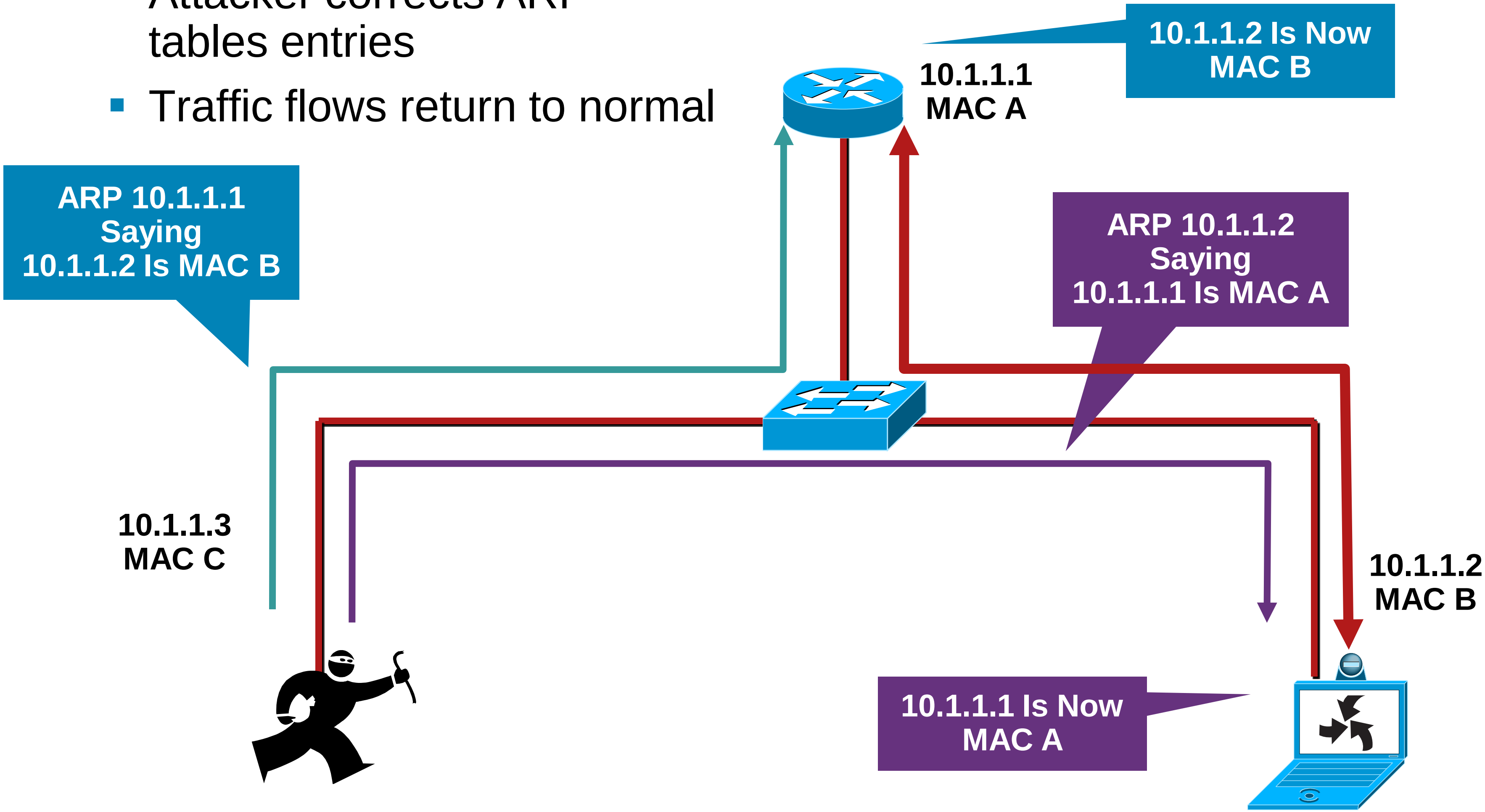


10.1.1.2 Is Now MAC C
10.1.1.1
MAC A
Transmit/Receive Traffic to 10.1.1.2 MAC C
Transmit/Receive Traffic to 10.1.1.1 MAC C
10.1.1.3
MAC C
10.1.1.2
MAC B
10.1.1.1 Is Now MAC C

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

ARP Attack Clean Up

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



ARP 10.1.1.1 Saying 10.1.1.2 Is MAC B

10.1.1.1 MAC A

10.1.1.2 Is Now MAC B

ARP 10.1.1.2 Saying 10.1.1.1 Is MAC A

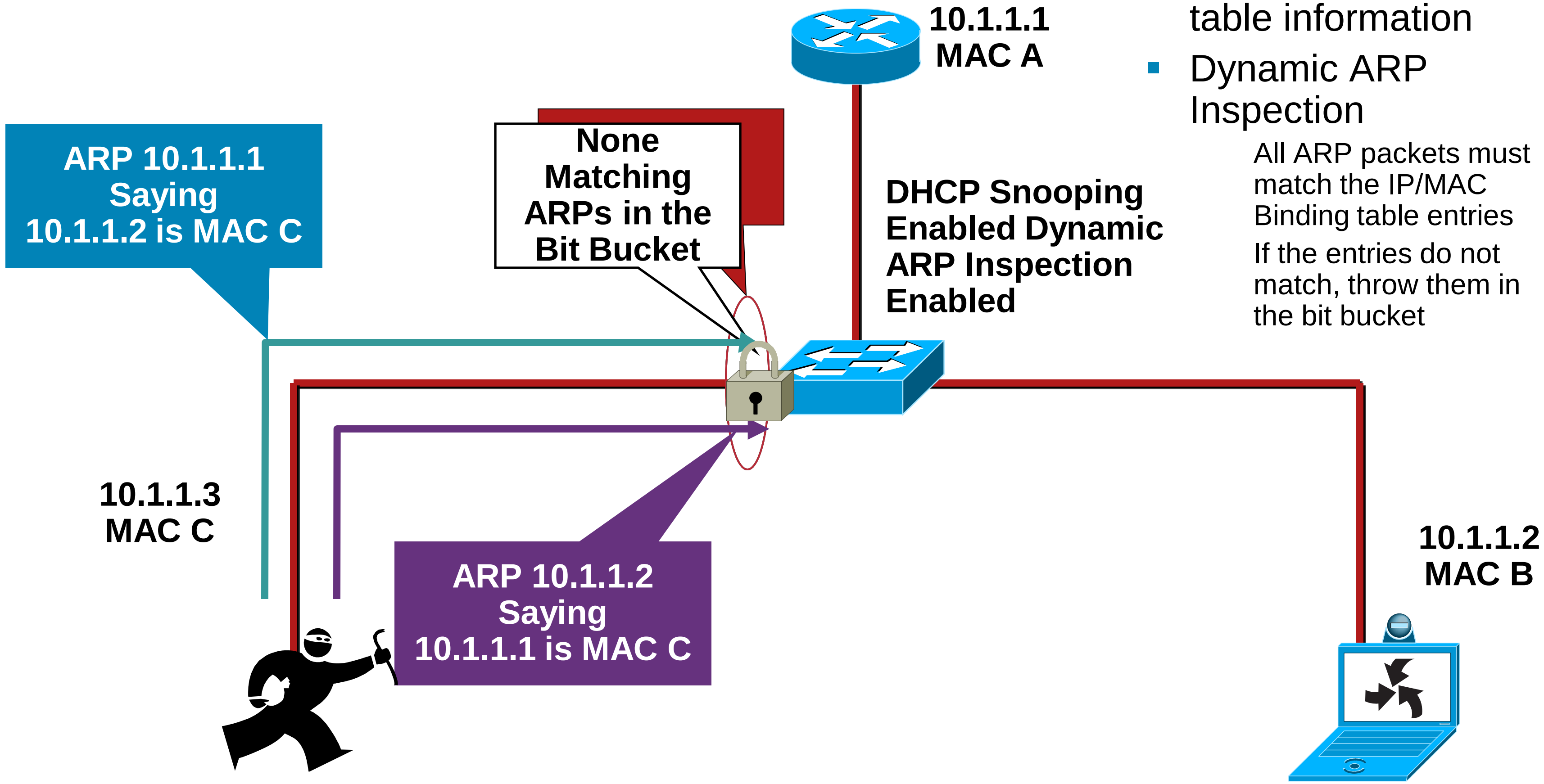
10.1.1.3 MAC C

10.1.1.2 MAC B

10.1.1.1 Is Now MAC A

© 2007 Cisco Systems, Inc. All rights reserved.

Countermeasures to ARP Attacks: Dynamic ARP Inspection


10.1.1.1
MAC A
ARP 10.1.1.1 Saying 10.1.1.2 is MAC C
None Matching ARPs in the Bit Bucket
DHCP Snooping Enabled Dynamic ARP Inspection Enabled
10.1.1.3
MAC C
ARP 10.1.1.2 Saying 10.1.1.1 is MAC C
10.1.1.2
MAC B

- 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
```

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

© 2007 Cisco Systems, Inc. All rights reserved.

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

© 2007 Cisco Systems, Inc. All rights reserved.

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)
```

© 2007 Cisco Systems, Inc. All rights reserved.

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])
```

© 2007 Cisco Systems, Inc. All rights reserved.

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
```

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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—2500 entrees

    4000 switches—4000 entrees (6000 for the SupV-10GE)

    6000 switches—16,000 entrees

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

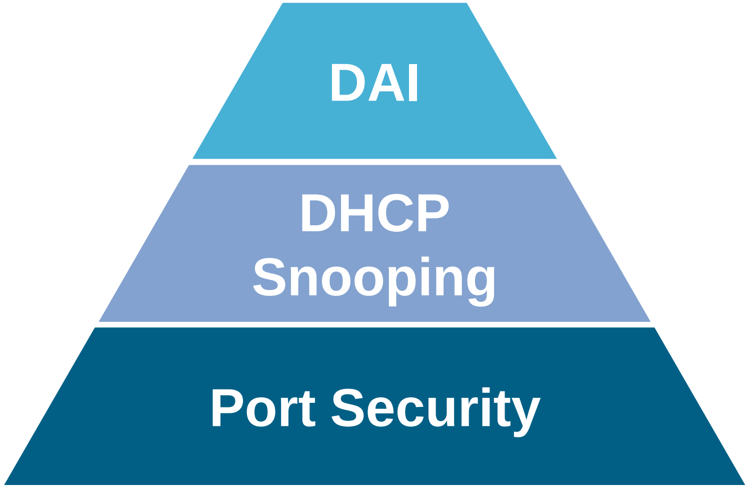
More ARP Attack Information

- 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)

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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



© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures

  VLAN Hopping

  MAC Attacks

  DHCP Attacks

  ARP Attacks

  Spoofing Attacks

  General Attacks
- Summary

© 2007 Cisco Systems, Inc. All rights reserved.

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

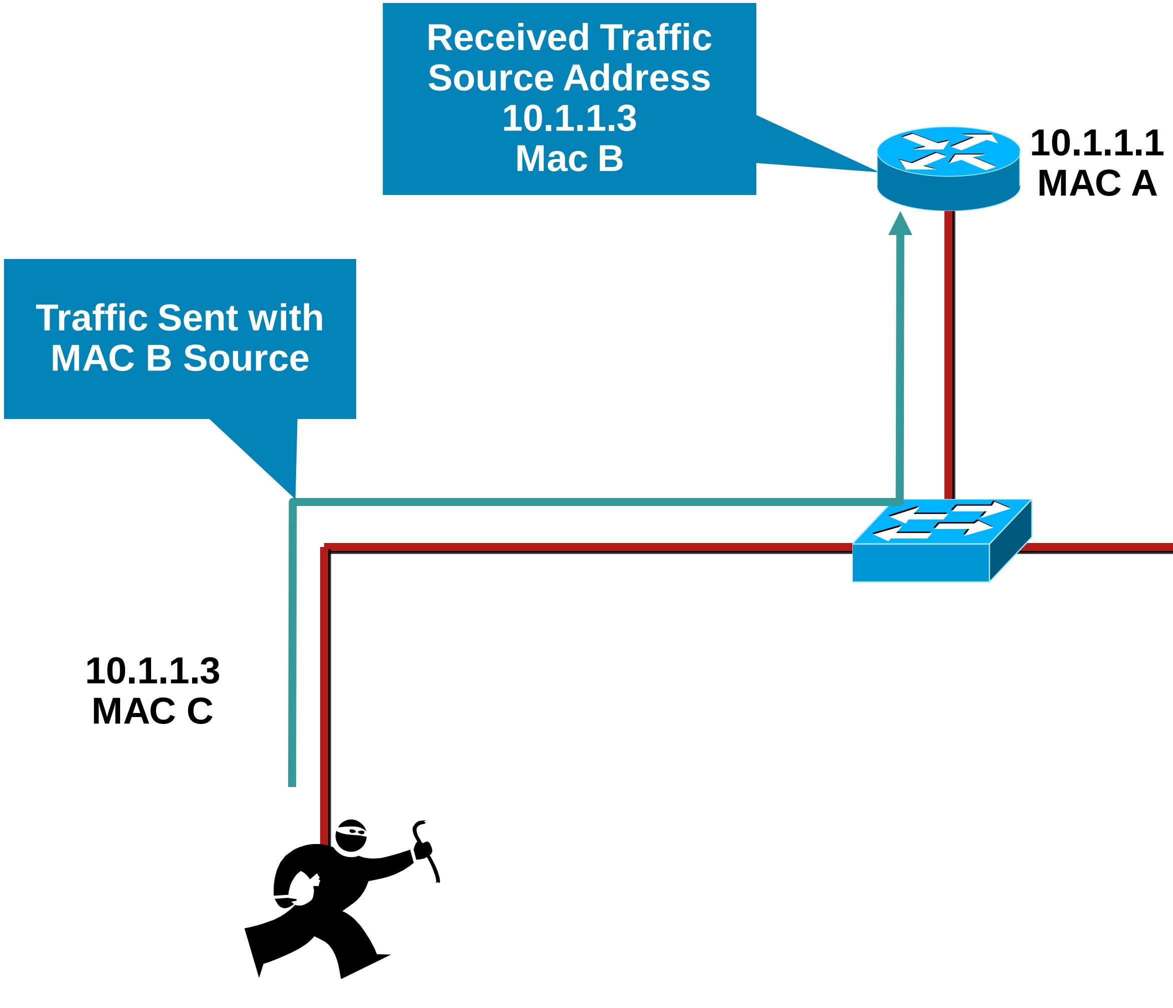
  ICMP unreachable storm

  SYN flood

  Trusted IP addresses can be spoofed

© 2007 Cisco Systems, Inc. All rights reserved.

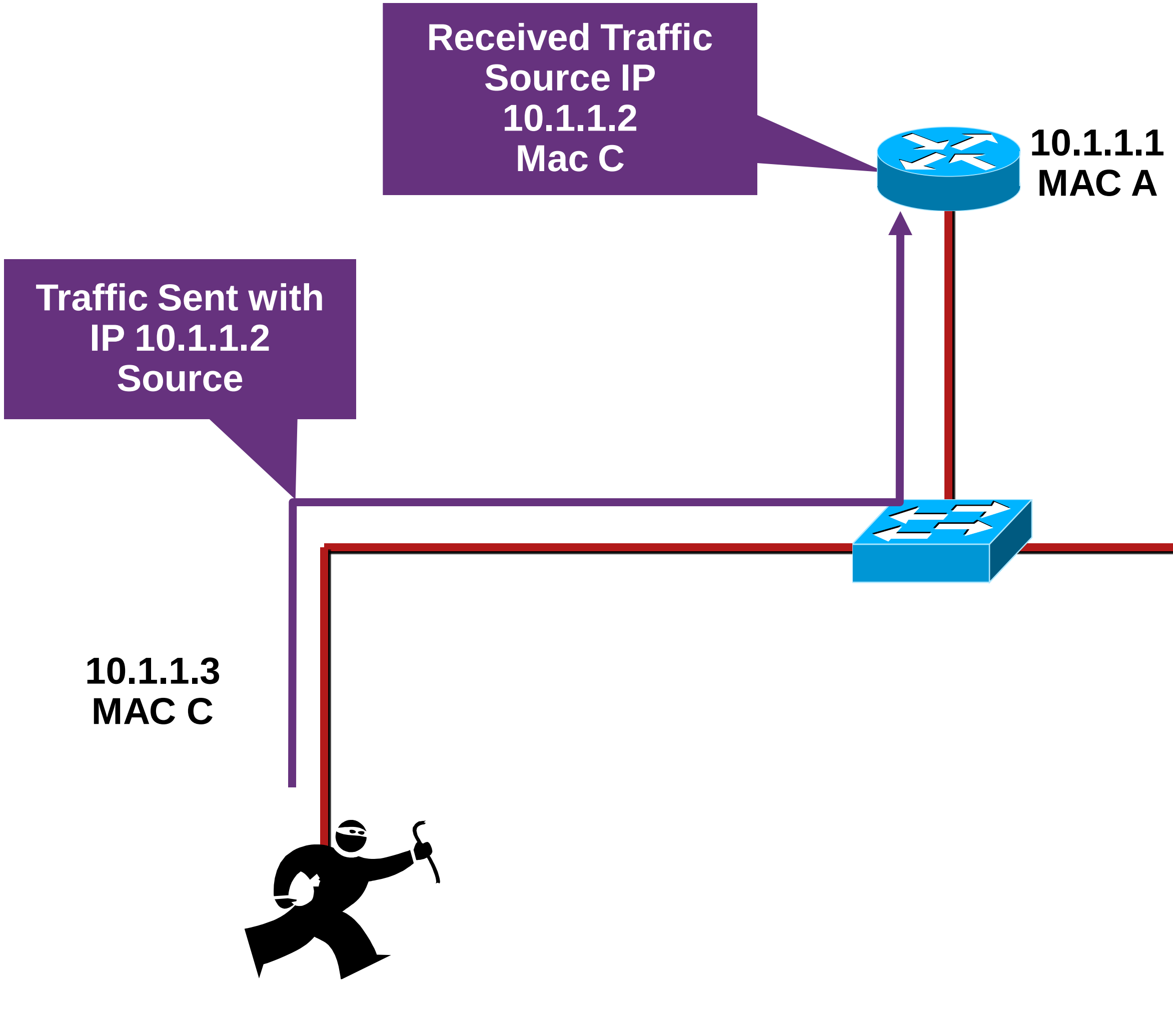
Spoofing Attack: MAC



- 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

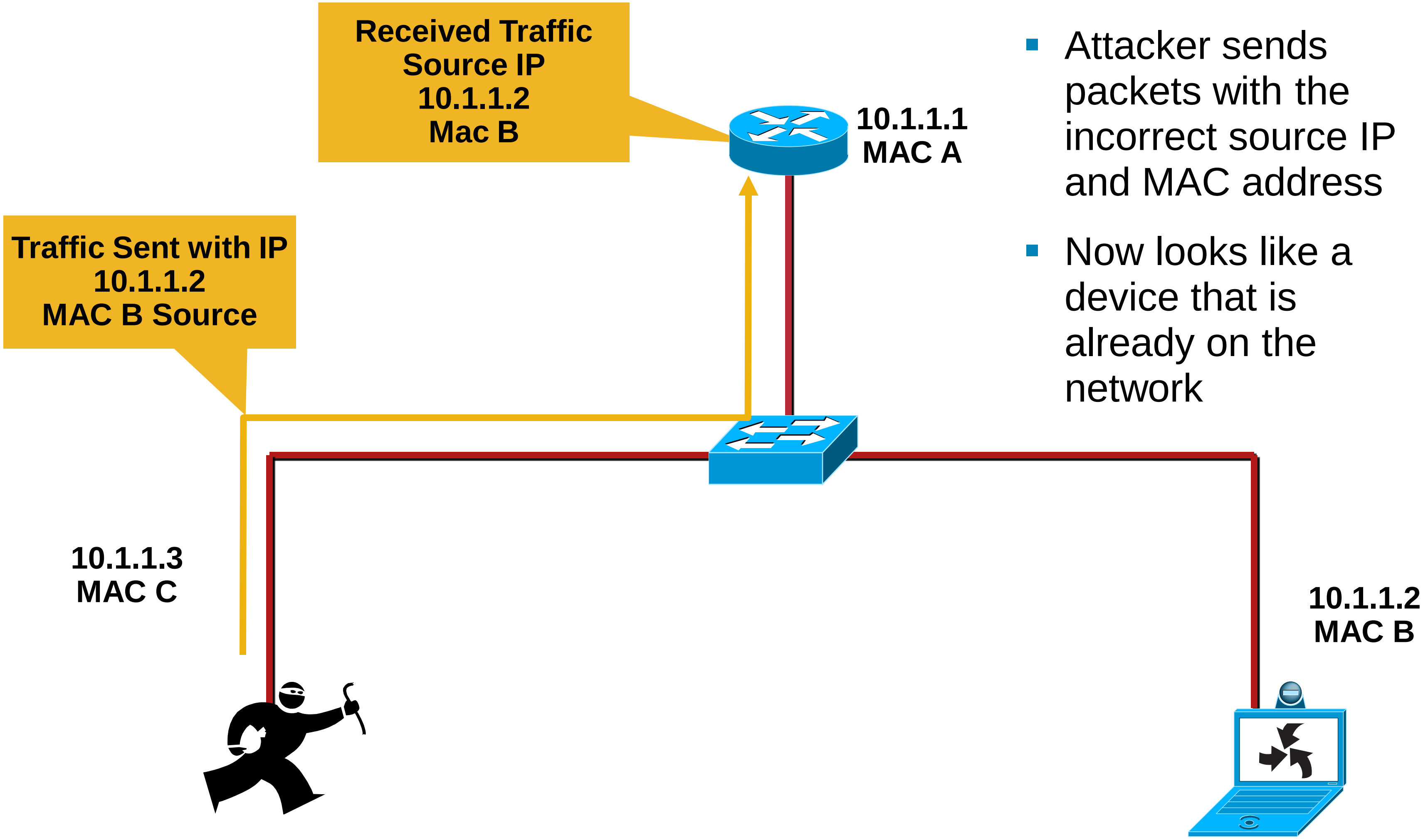
© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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



Received Traffic
Source IP
10.1.1.2
Mac B

Traffic Sent with IP
10.1.1.2
MAC B Source

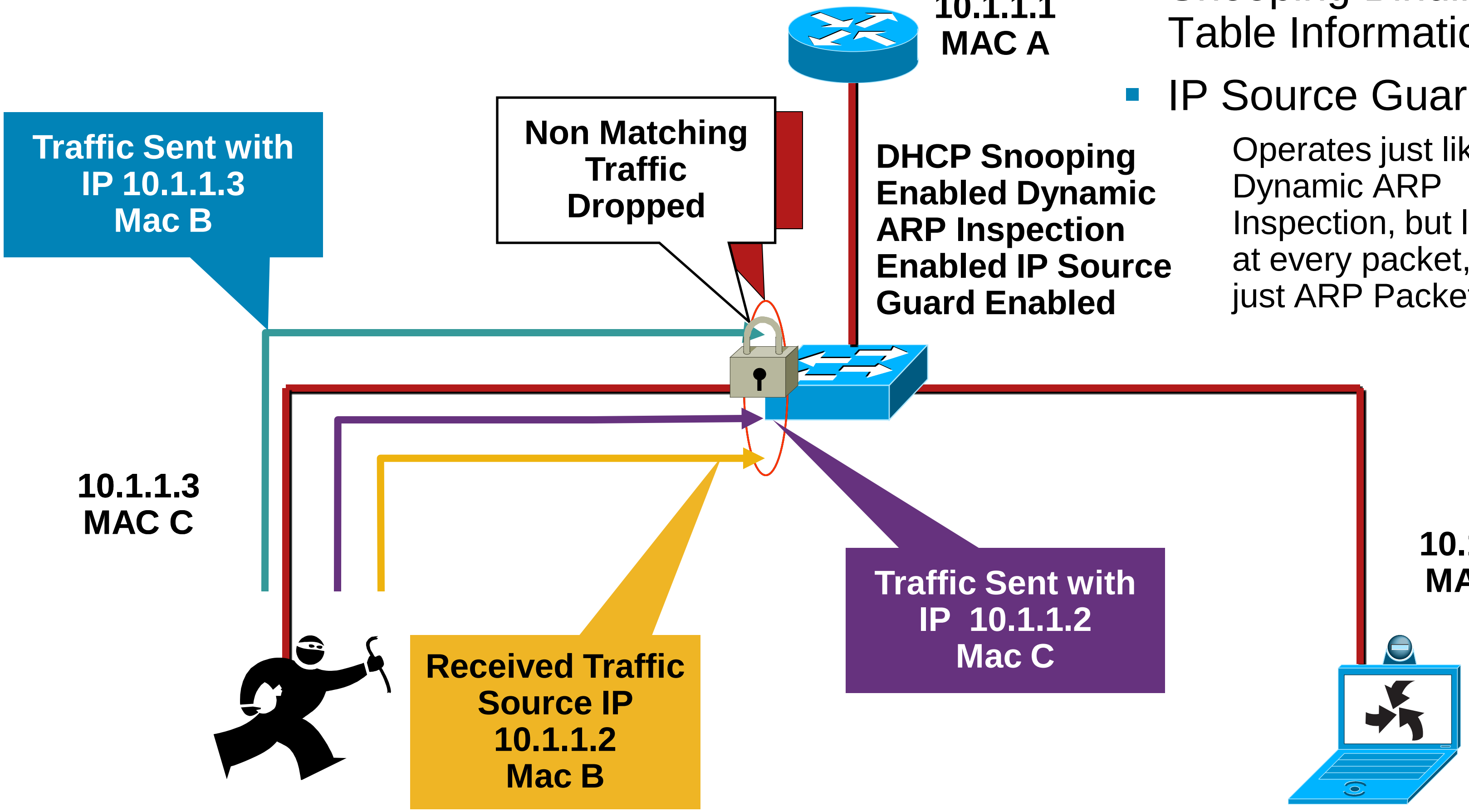
- Attacker sends packets with the incorrect source IP and MAC address
- Now looks like a device that is already on the network

© 2007 Cisco Systems, Inc. All rights reserved.

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


10.1.1.1
MAC A
Non Matching Traffic Dropped
Traffic Sent with IP 10.1.1.3 Mac B
DHCP Snooping Enabled Dynamic ARP Inspection Enabled IP Source Guard Enabled
10.1.1.3
MAC C
Traffic Sent with IP 10.1.1.2 Mac C
10.1.1.2
MAC B
Received Traffic Source IP 10.1.1.2 Mac B

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
```

- 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

© 2007 Cisco Systems, Inc. All rights reserved.

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
- There are very few DHCP servers that support Option 82 (*relay information option*) for DHCP
- If you do not have an Option 82 enabled DHCP you most likely will not get an IP address on the client

Note: There Are at Least Two DHCP Servers That Support Option 82 Field Cisco Network Registrar® and Avaya

Clear Up Source Guard

- 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

- Most enterprises do not need to check the MAC address with IPSG

  There are no known, good attacks that can use this information in an enterprise network

© 2007 Cisco Systems, Inc. All rights reserved.

Countermeasures to Spoofing Attacks: IP Source Guard

IP Source Guard

IP Source Guard Configuration
IP Checking Only (no Opt 82)
What most Enterprises Will Run

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 Configuration
IP/MAC Checking Only (Opt 82)

IOS

Global Commands

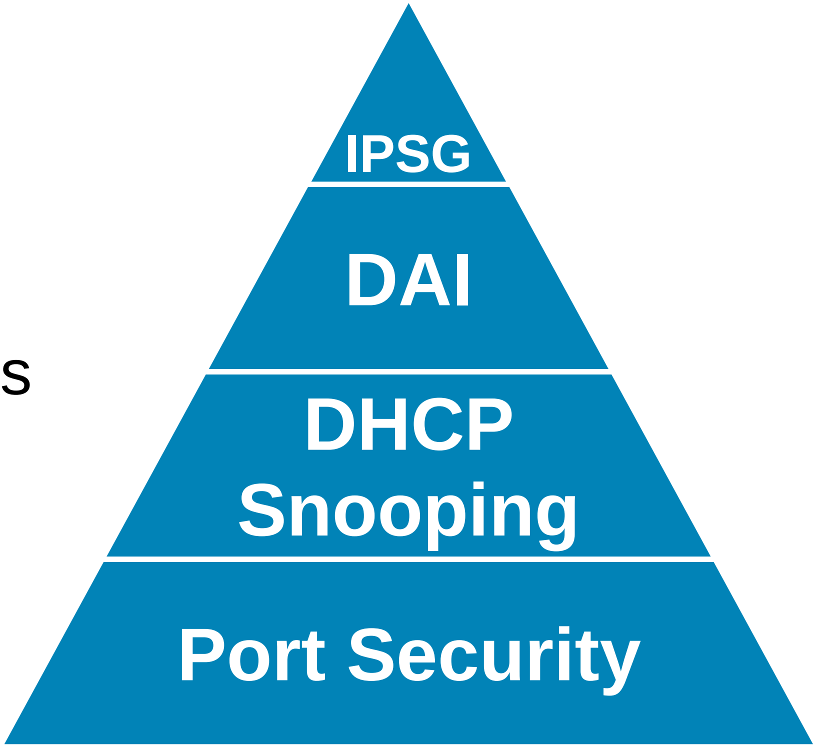
```
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
```

Interface Commands

```
ip verify source vlan dhcp-snooping
   port-security
```

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



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures

  VLAN Hopping

  MAC Attacks

  DHCP Attacks

  ARP Attacks

  Spoofing Attacks

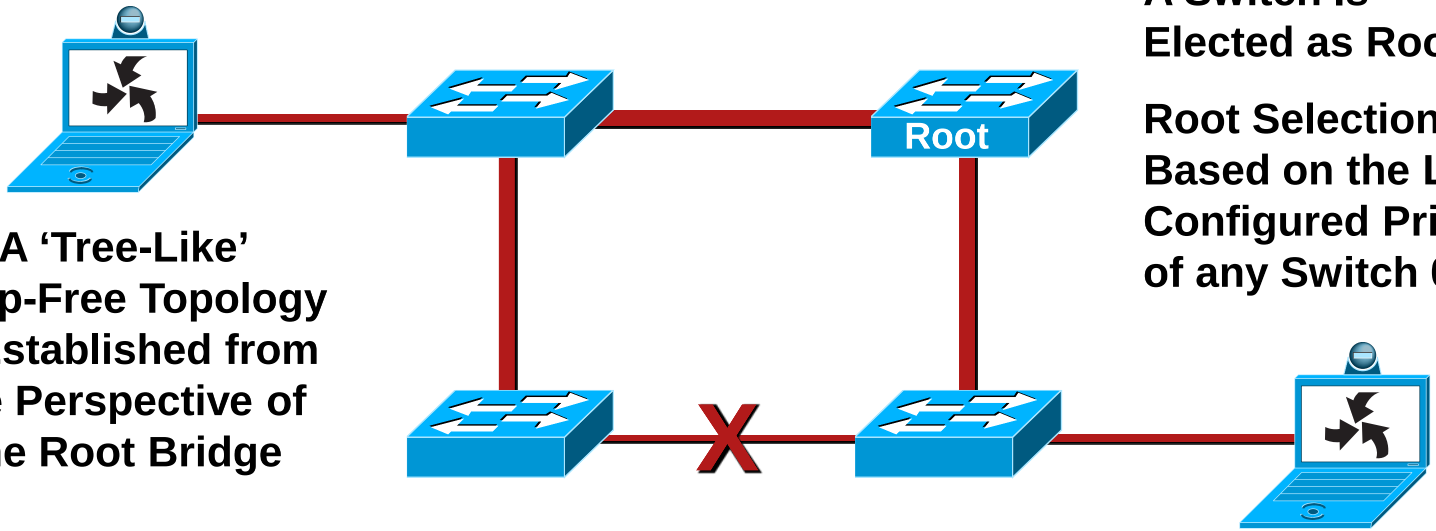
  General Attacks

- Summary

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Spanning Tree Basics

- STP Purpose: to maintain loop-free topologies in a redundant Layer 2 infrastructure



A Switch Is Elected as Root

Root Selection Is Based on the Lowest Configured Priority of any Switch 0–65535

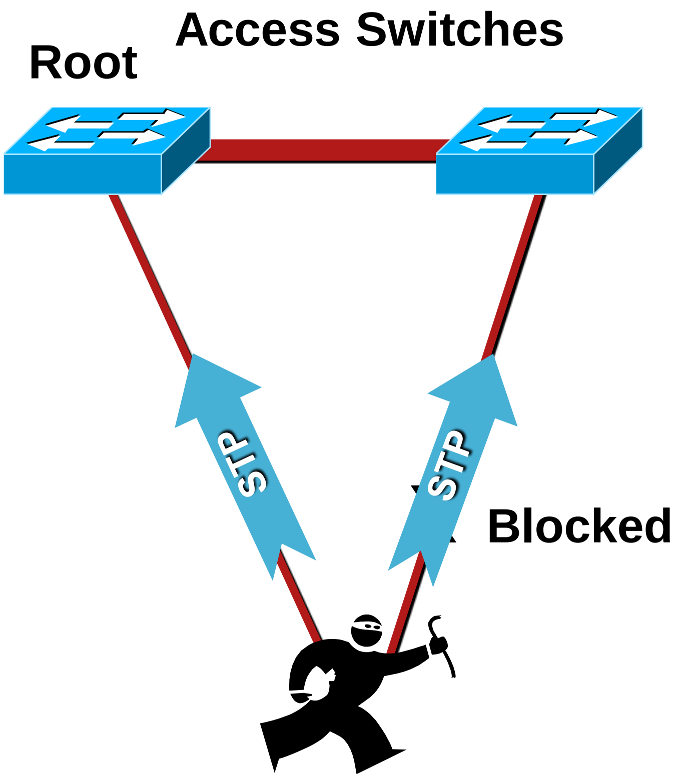
A 'Tree-Like' Loop-Free Topology Is Established from the Perspective of the Root Bridge

- STP is very simple; messages are sent using Bridge Protocol Data Units (BPDUs); basic messages include: configuration, topology change notification/acknowledgment (TCN/TCA); most have no "payload"
- Avoiding loops ensures broadcast traffic does not become storms

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

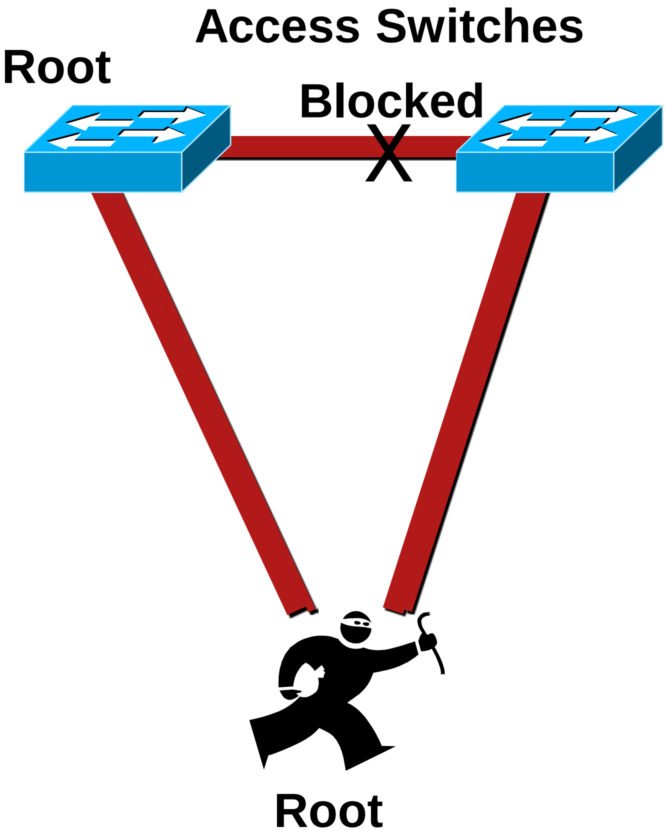
Spanning Tree Attack Example

- Send BPDU messages to become root bridge



Spanning Tree Attack Example

- Send BPDU messages to become root bridge
  - The attacker then sees frames he shouldn't
    - MITM, DoS, etc. all possible
    - Any attack is very sensitive to the original topology, trunking, PVST, etc.
    - Although STP takes link speed into consideration, it is always done from the perspective of the root bridge. Taking a Gb backbone to half-duplex 10 Mb was verified
    - Requires attacker is dual homed to two different switches (with a hub, it can be done with just one interface on the attacking host)



© 2007 Cisco Systems, Inc. All rights reserved.

STP Attack Mitigation

- Try to design loop-free topologies where ever possible, so you do not need STP
- Don’t disable STP, introducing a loop would become another attack
- BPDU Guard
- Should be run on all user facing ports and infrastructure facing ports

  Disables ports using portfast upon detection of a BPDU message on the port

  Globally enabled on all ports running portfast

  Available in Catalyst OS 5.4.1 for Cat 2K, 4K, 5K, and 6K; 12.0XE for native Cisco IOS 6K; 12.1(8a)EW for 4K IOS; 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
```

© 2007 Cisco Systems, Inc. All rights reserved.

STP Attack Mitigation

- Root Guard

  Disables ports who would become the root bridge due to their BPDU advertisement

  Configured on a per port basis

  Available in Catalyst OS 6.1.1 for Catalyst 29XX, 4K, 5K, and 6K; 12.0(7) XE for native Cisco IOS 6K, 12.1(8a)EW for 4K Cisco IOS; 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)
```

Cisco Discovery Protocol (CDP)

- **Not** normally an attack
- Runs at Layer 2 and allows Cisco devices to chat with one another
- Can be used to learn sensitive information about the CDP sender (IP address, software version, router model …)
- CDP is in the clear and unauthenticated
- Consider disabling CDP, or being very selective in its use in security sensitive environments
- Used by Cisco IPT for Network Management
- Note: there was a reason Cisco developed CDP, some Cisco apps make use of it!

```
CatOS> (enable) set cdp disable <mod>/<port> | all
IOS(config)#no cdp run
IOS(config-if)#no cdp enable
```

© 2007 Cisco Systems, Inc. All rights reserved.

CDP Attacks

- Besides the information gathering benefit CDP offers an attacker, there was a vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets
- If you need to run CDP, be sure to use Cisco IOS code with minimum version numbers: 12.2(3.6)B, 12.2(4.1)S, 12.2(3.6)PB, 12.2(3.6)T, 12.1(10.1), 12.2(3.6) or CatOS code 6.3, 5.5, or 7.1 and later
- Problem was due to improper memory allocation for the CDP process (basically there was no upper limit)
- For more information:

    http://www.cisco.com/warp/public/707/cdp_issue.shtml

    http://www.kb.cert.org/vuls/id/139491

© 2007 Cisco Systems, Inc. All rights reserved.

Switch Management

- Management can be your weakest link

  All the great mitigation techniques we talked about aren’t worth much if the attacker telnets into your switch and disables them

- Most of the network management protocols we know and love are insecure (syslog, SNMP, TFTP, Telnet, FTP, etc.)
- Consider secure variants of these protocols as they become available (SSH, SCP, SSL, OTP etc.), where impossible, consider out of band (OOB) management

  Put the management VLAN into a dedicated non-standard VLAN where nothing but management traffic resides

  Consider physically back-hauling this interface to your management network

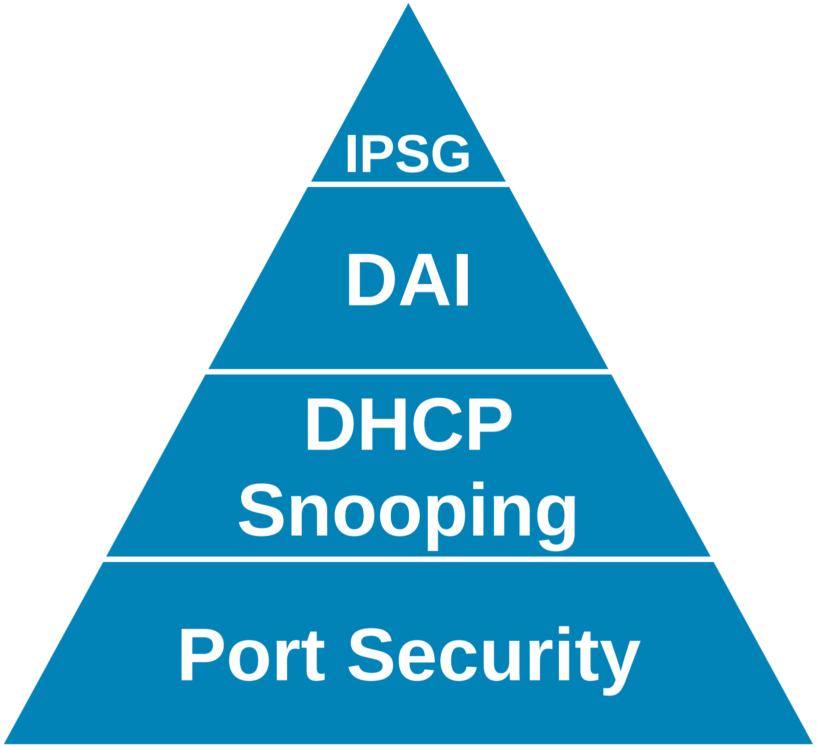
- When OOB management is not possible, at least limit access to the management protocols using the “set ip permit” lists on the management protocols
- SSH is available on Catalyst 6K with Catalyst OS 6.1 and Catalyst 4K/29XXG with Catalyst OS 6.3; 3550 in 12.1(11)EA1; 2950 in 12.1(12c)EA1; Cisco IOS 6K 12.1(5c)E12; IOS 4K in 12.1(13)EW

Agenda

- Layer 2 Attack Landscape
- Attacks and Counter Measures
  - VLAN Hopping
  - MAC Attacks
  - DHCP Attacks
  - ARP Attacks
  - Spoofing Attacks
  - General Attacks
- Summary

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



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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
  (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.)

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Layer 2 Security Best Practices (2/2)

- 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—with phones it is useful
- Disable all unused ports and put them in an unused VLAN

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

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Q and A

© 2007 Cisco Systems, Inc. All rights reserved.