Understanding and Preventing Layer 2 Attacks

BRKSEC-2002

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –MAC Attacks
  - –VLAN Hopping
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –Attacks on other LAN protocols
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.

Associated Sessions

- BRKSEC-2046 Cisco Trusted Security (CTS) and Security Group Tagging
- BRKSEC-2005 Deploying Wired 802.1x

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

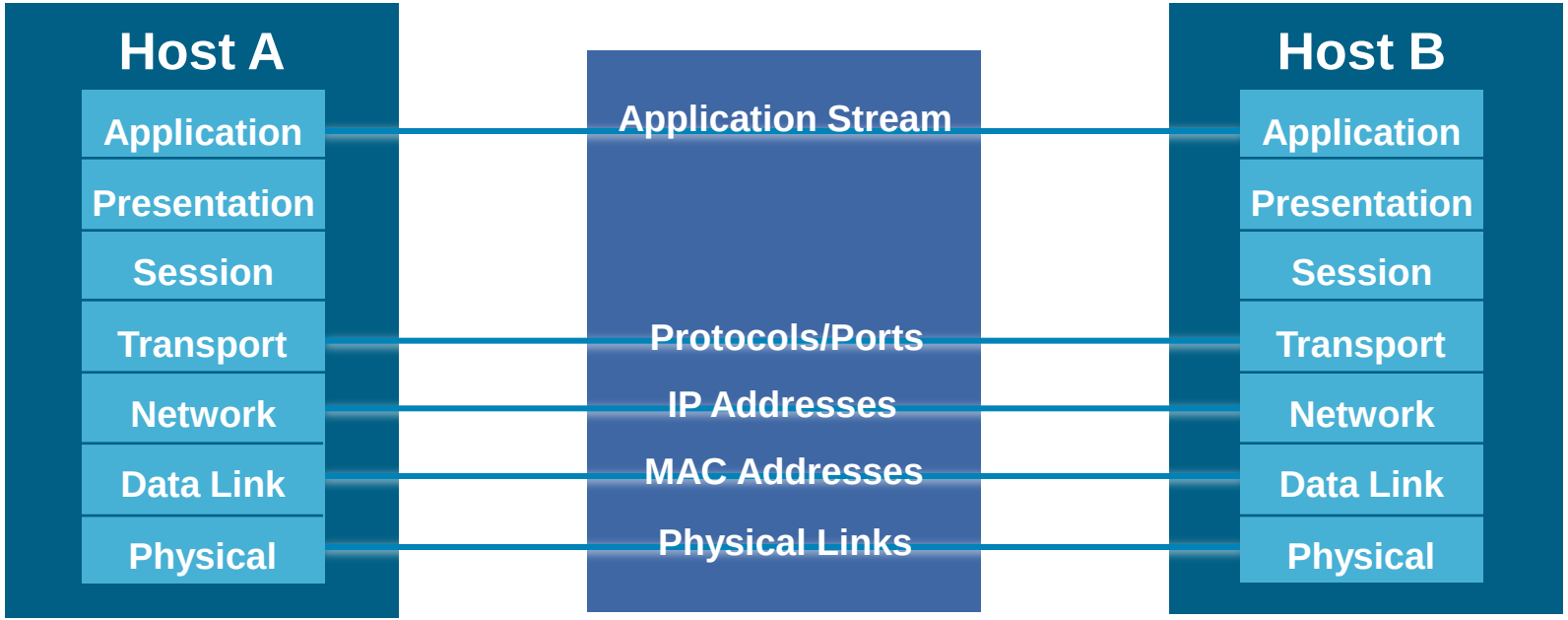
Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Why Worry About Layer 2 Security?

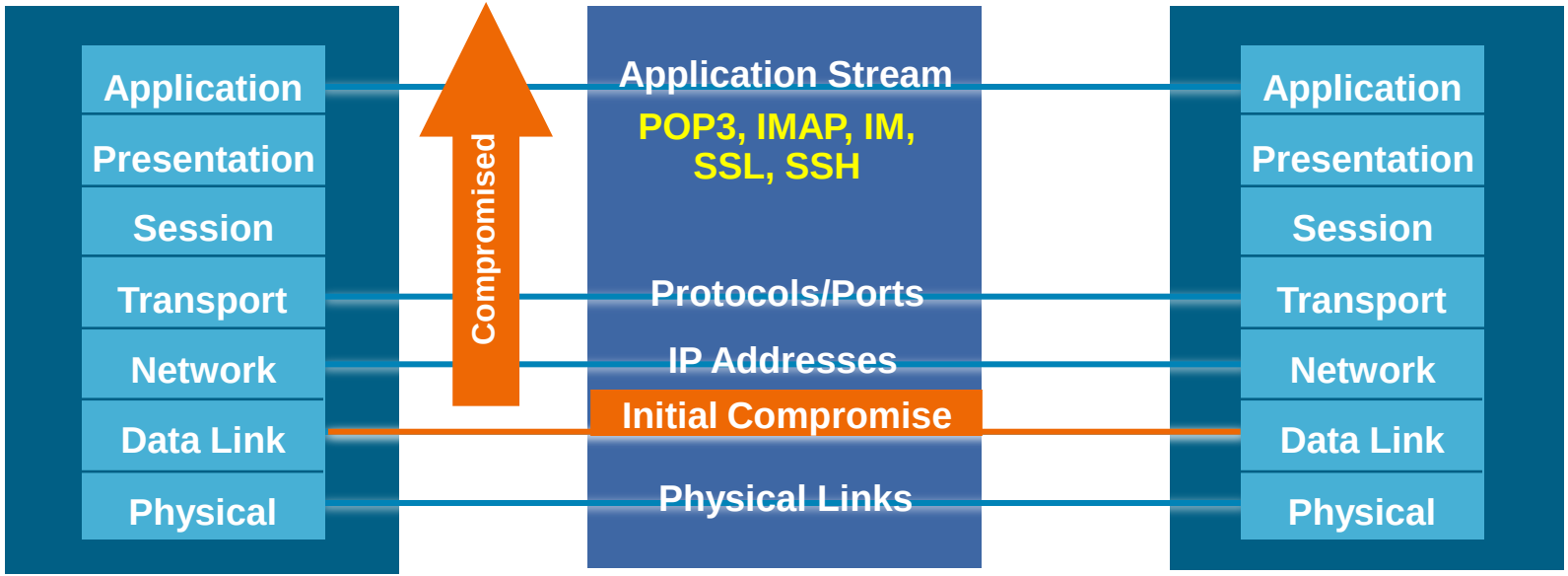
OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –MAC Attacks
  - –VLAN Hopping
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

© 2011 Cisco and/or its affiliates. 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

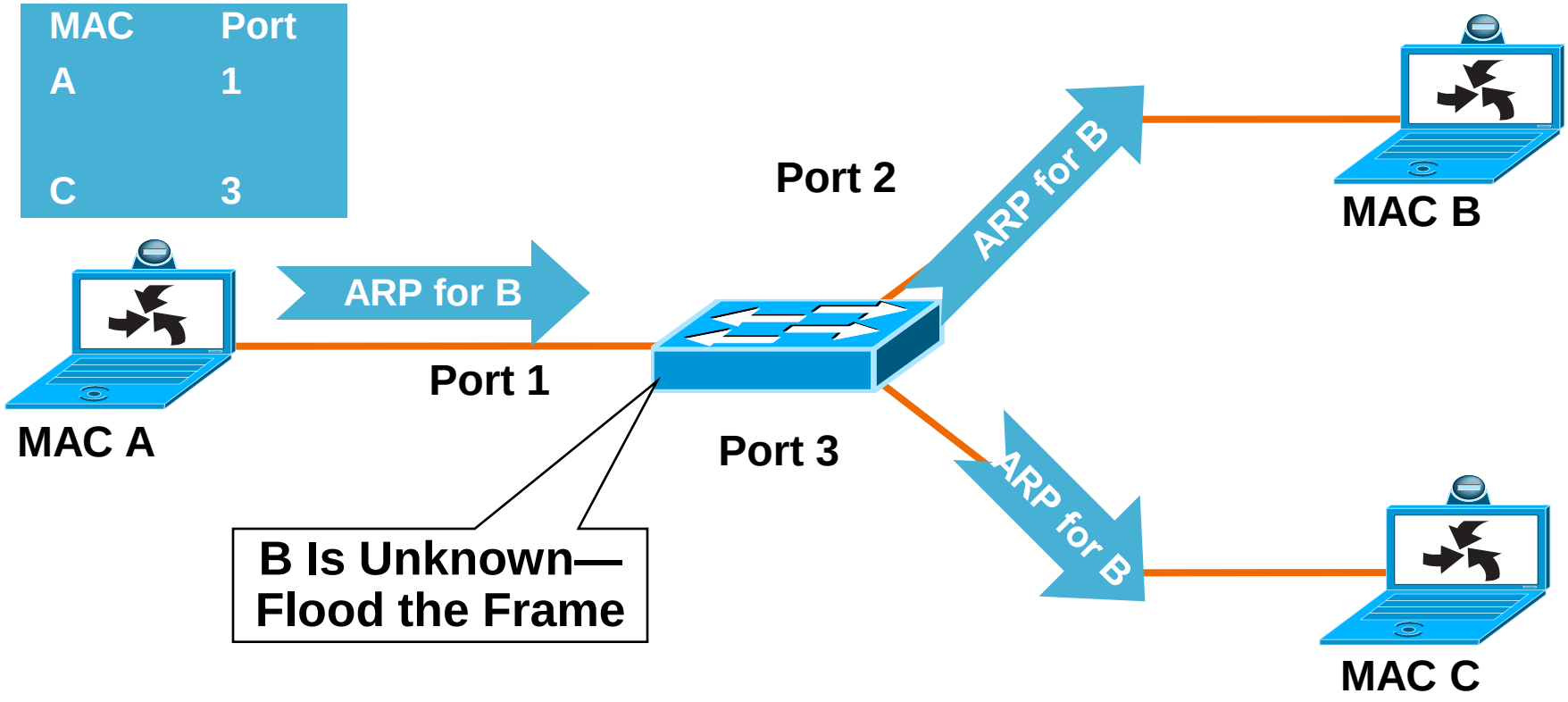
All Fs = Broadcast

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

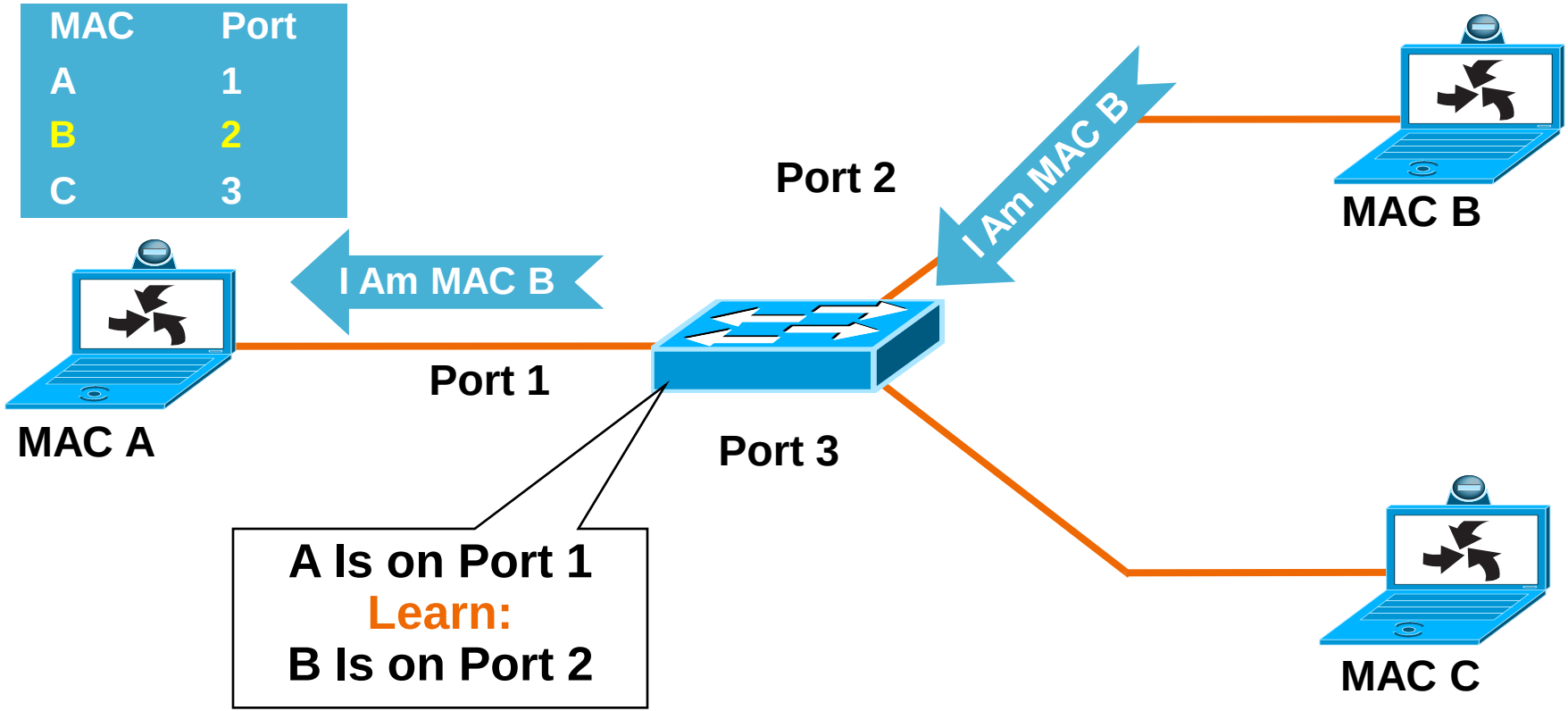
© 2011 Cisco and/or its affiliates. All rights reserved.

Normal CAM Behaviour (1/3)



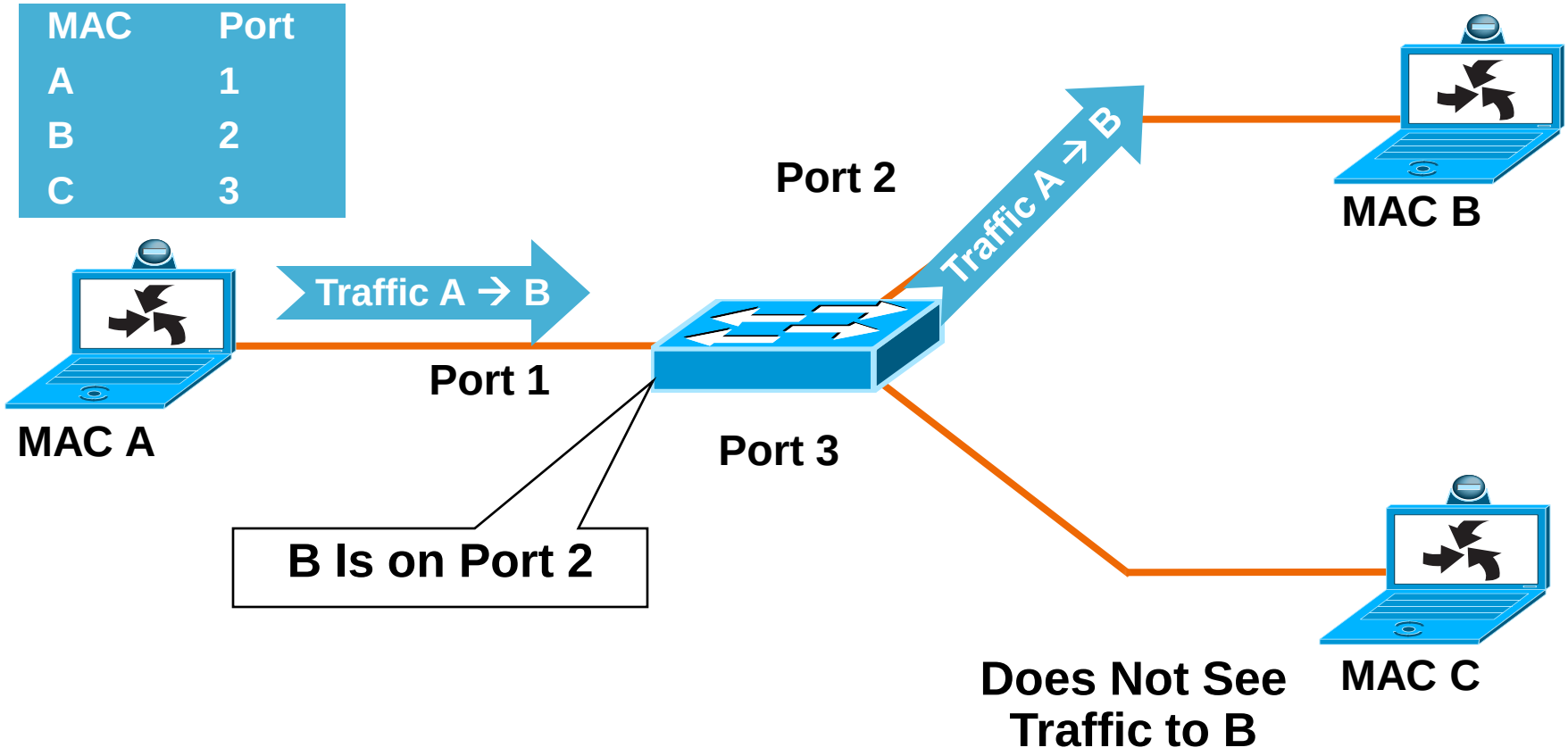
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Normal CAM Behaviour (2/3)



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Normal CAM Behaviour (3/3)



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

CAM Overflow—Tools (1/2)

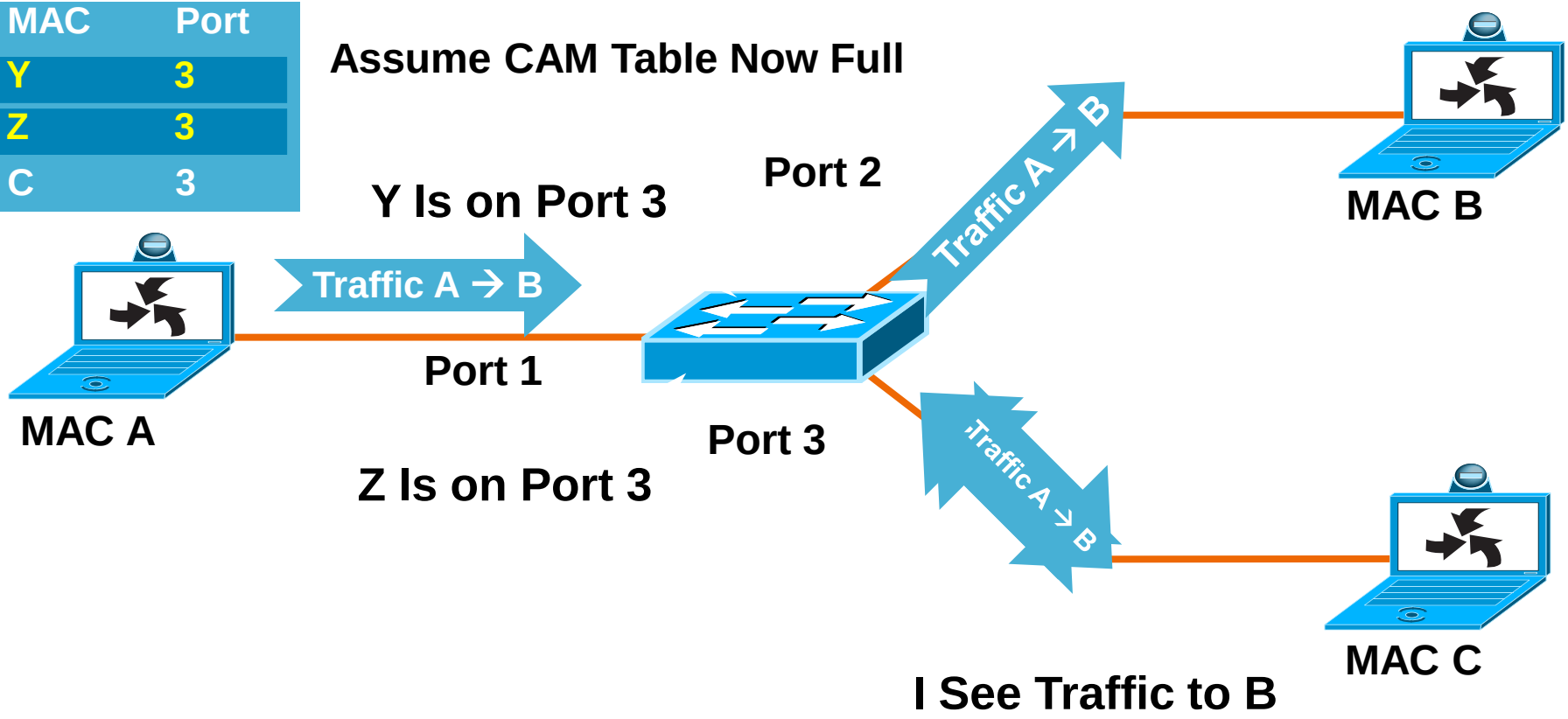
- macof tool since 1999
  - –About 100 lines of perl
  - –Included in “dsniff”
- Attack successful by exploiting the size limit on CAM tables
- Yersinia: Swiss-army knife of L2 attacks

© 2011 Cisco and/or its affiliates. All rights reserved.

CAM Overflow (2/2)

MAC	Port
Y	3
Z	3
C	3

Assume CAM Table Now Full



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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/

© 2011 Cisco and/or its affiliates. All rights reserved.

CAM Table Full

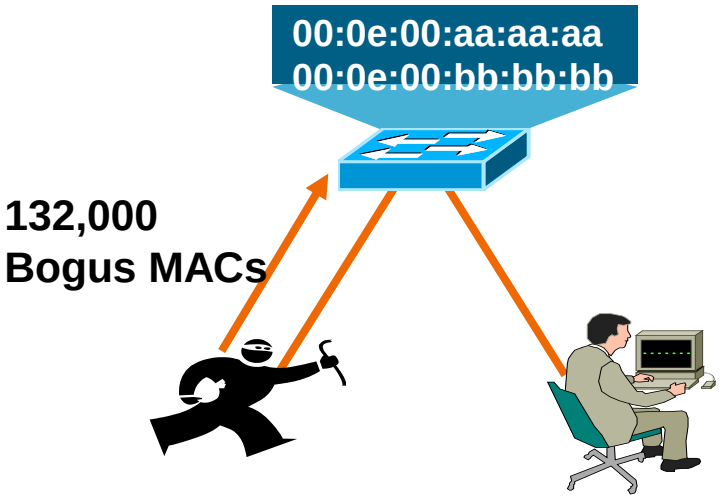
- Once the CAM table on the switch is full, traffic without a CAM entry is flooded out every port on that VLAN
- This will turn a VLAN on a switch basically into a hub
- This attack will also fill the CAM tables of adjacent switches

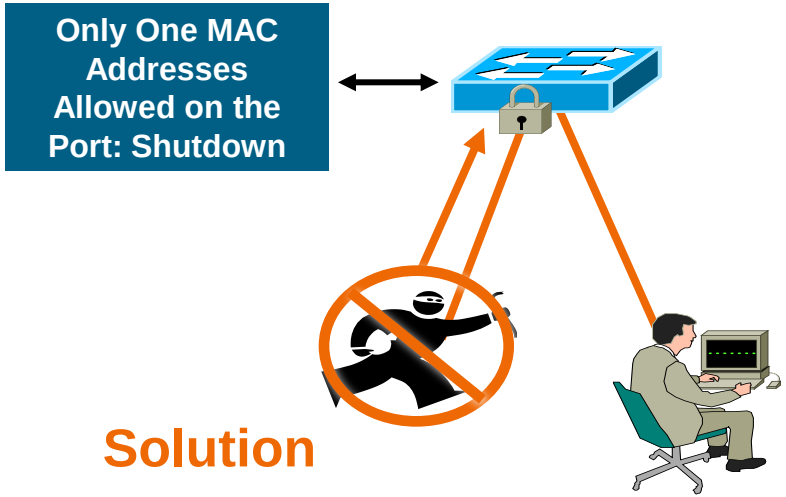
```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```


© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Countermeasures for MAC Attacks

Port Security Limits the Amount of MACs on an Interface





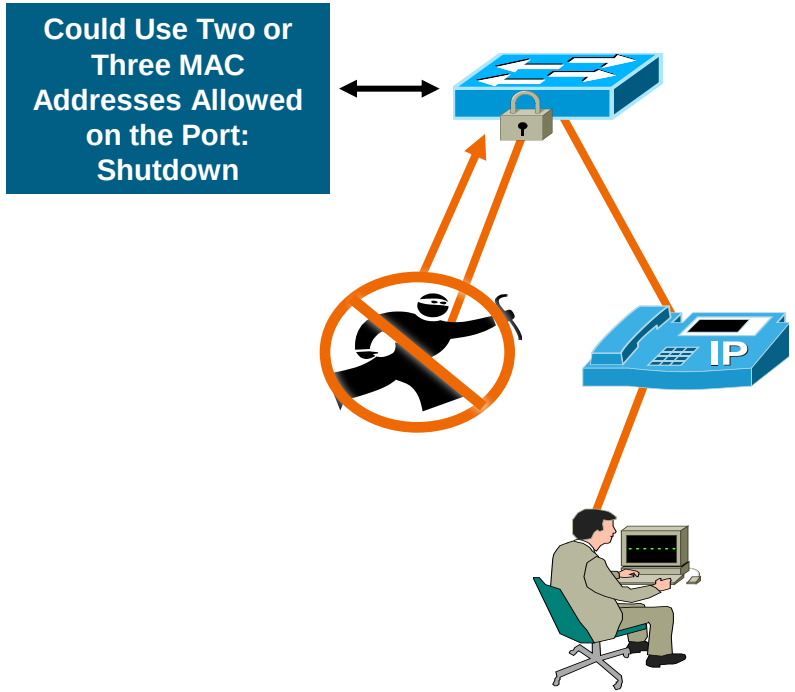
Solution

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

© 2011 Cisco and/or its affiliates. All rights reserved.

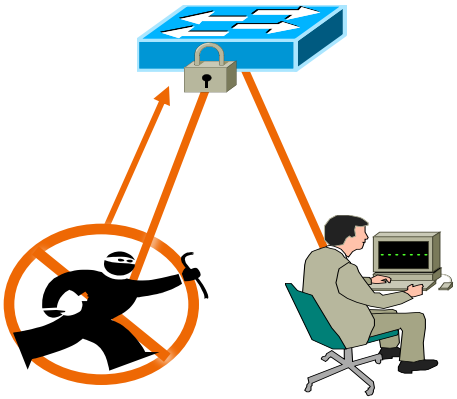
Countermeasures for MAC Attacks with IP Phones

- Phones can use two or three depending on the switch hardware and software
  - –Some switches look at the CDP traffic and some don't, if they don't, they need two, if they do they need three
  - –Some hardware (3550) will always need three
- 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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Port Security: Example Config



```
Cisco Catalyst OS
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
Cisco 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
```

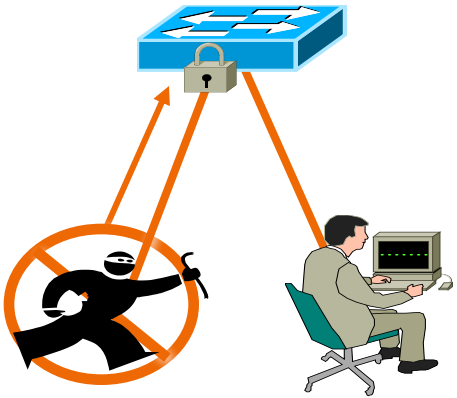
Will Enable Voice to Work Under Attack

- 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 1 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

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public

New Features for Port Security



New Commands

```
Cisco 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

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public

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
- “Sticky Port Security”; settings survive reboot (not on all switches)

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Port Security and LLDP-MED

- Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP)
  - –A standard that works like CDP for media endpoints
  - –Could affect port security deployments
- If the switch does not understand LLDP-MED
  - –You will need to set the port to three; the device (phone) can be in both VLAN—voice and data—and the PC will be in the data VLAN
  - –Or the setting can be two for the data VLAN (one phone and one PC) and one in the voice VLAN for the phone
- If the switch supports LLDP-MED
  - –The LLDP-MED should be treated as CDP and will not be counted on the port so the setting could be two or higher
  - –Early versions of switch Cisco IOS did count the LLDP-MED, so please be careful with the settings

Good link for this is: http://en.wikipedia.org/wiki/LLDP-MED

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 utilisation
- 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 1000s
- Voice MOS scores under attack were very good, as long as QoS was configured
- Designed to protect the switch and limit MAC addresses, has no authentication; look at 802.1X for that
- Minimum settings for phones are two usually, higher numbers should be considered

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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Building the Layers

- Port Security prevents CAM attacks (and *some* DHCP starvation attacks)

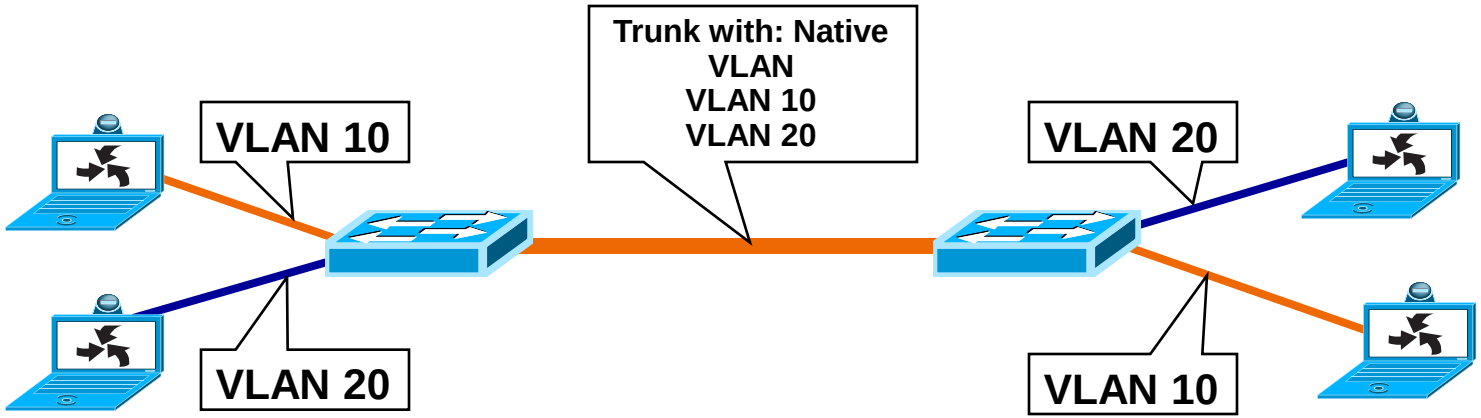
© 2011 Cisco and/or its affiliates. All rights reserved.

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –MAC Attacks
  - –VLAN Hopping
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.

Basic Trunk Port Defined

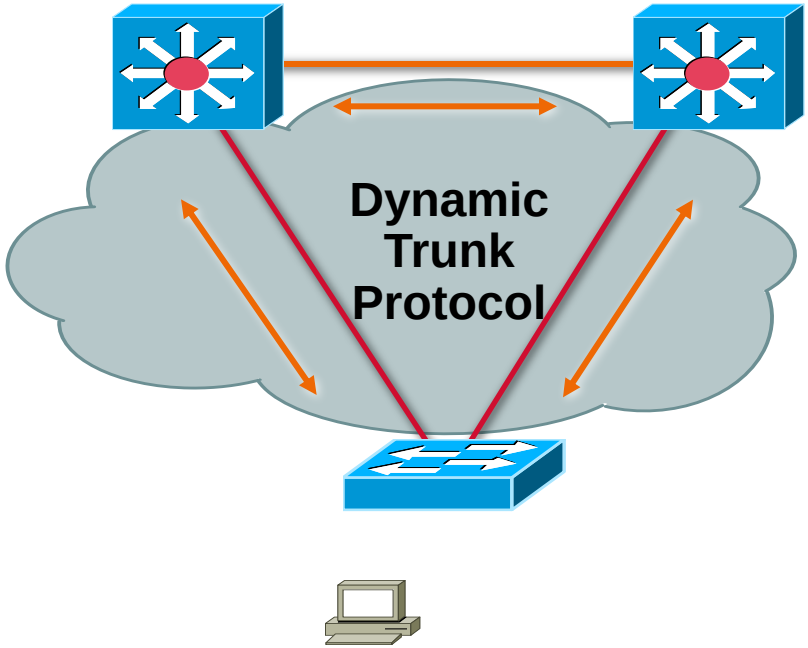


- Trunk ports have access to all VLANs by default
- Used to route traffic for multiple VLANs across the same physical link (generally between switches or phones)
- Encapsulation can be 802.1Q

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

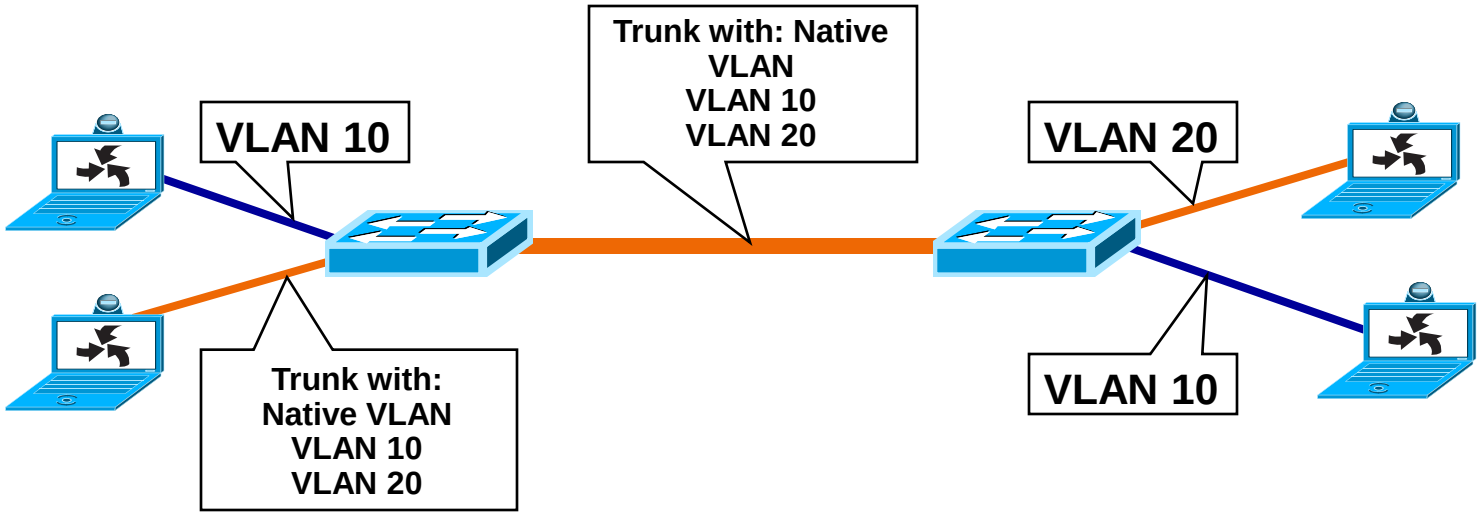
Dynamic Trunk Protocol (DTP)

- What is DTP?
  - –Automates 802.1Q trunk configuration
  - –Operates between switches (Cisco IP phone is a switch)
  - –Does not operate on routers
  - –Support varies, check your device
- DTP synchronises the trunking mode on end links
- DTP state on 802.1Q trunking port can be set to “Auto,” “On,” “Off,” “Desirable,” or “Non-Negotiate”



© 2011 Cisco and/or its affiliates. All rights reserved.

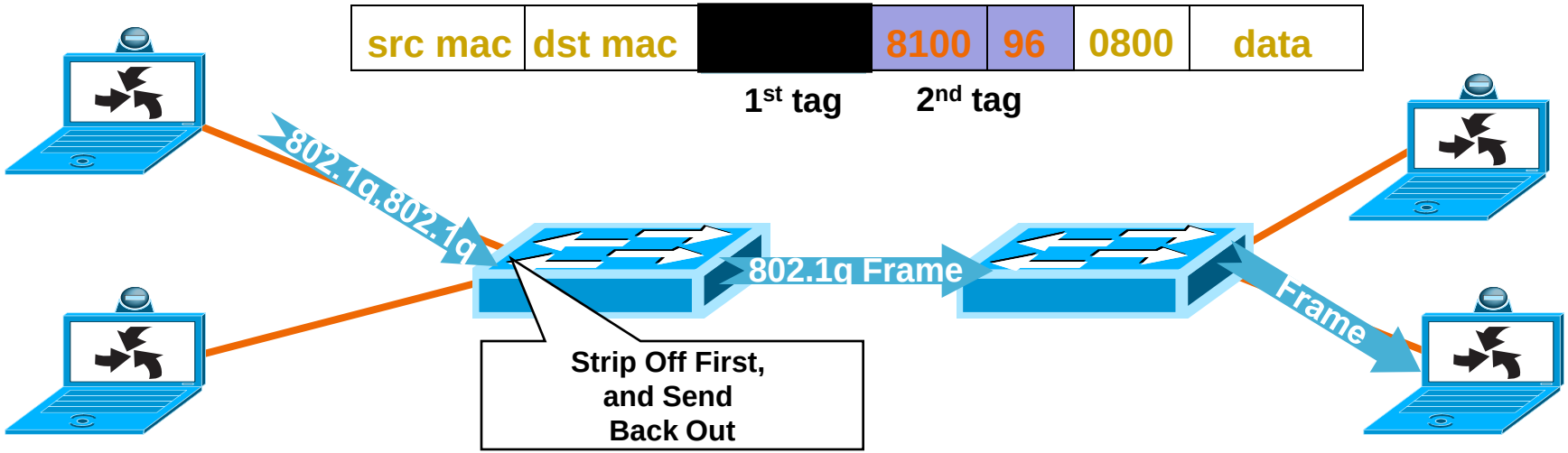
Basic VLAN Hopping Attack



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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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

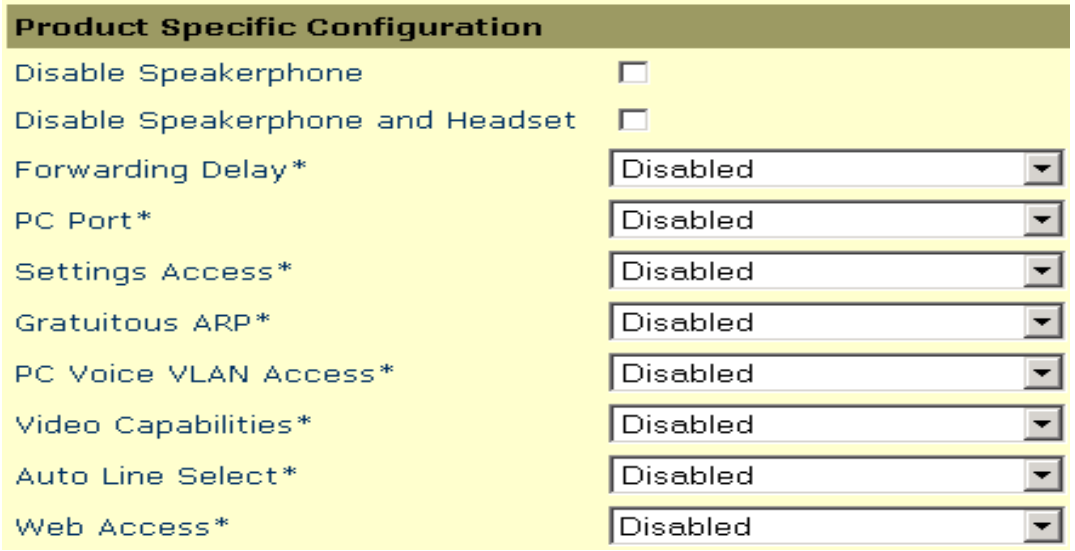
Note: Only works if trunk has the same VLAN as the attacker

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

IP Phones VLAN Security

Configurable Options

- Block voice VLAN from PC port
- Ignore Gratuitous ARPs (GARPs)



These Features Were All Introduced in CCM 3.3(3), Except Signed Config Files and Disable Web Access Which Were Introduced in CCM 4.0

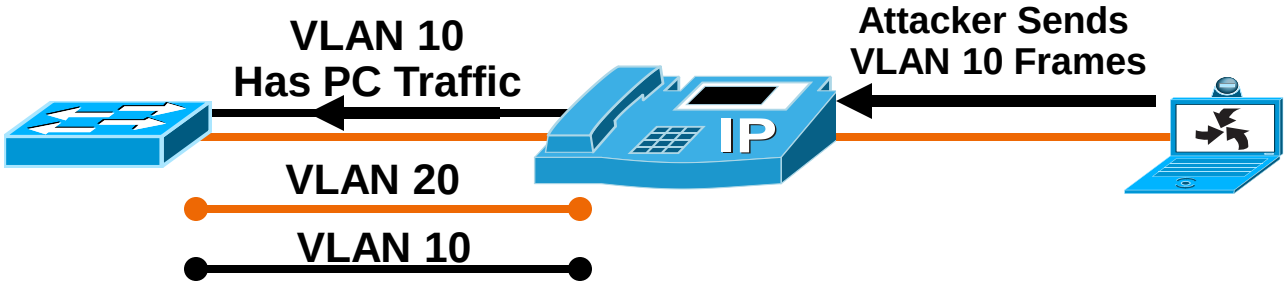
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Voice VLAN Access

- Normal VLAN operation
  - –VLAN 20 is native to the PC and is not tagged
  - –VLAN 10 is the voice VLAN, and is tagged with 10

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

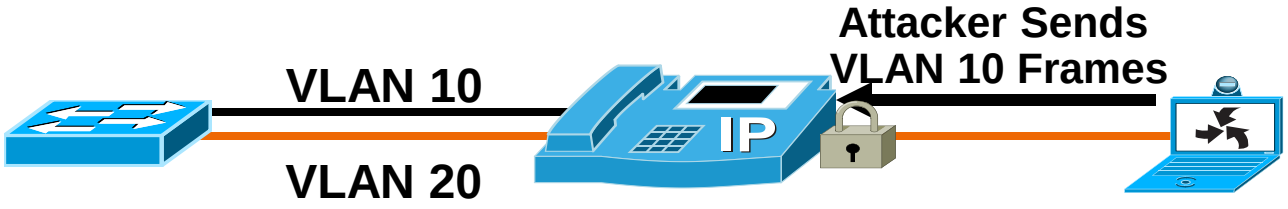
Voice VLAN Access: Attack



- Attacking voice VLAN
  - –Attacker sends 802.1Q tagged frames from the PC to the phone
  - –Traffic from the PC is now in the voice VLAN

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

IP Phone
PC Voice VLAN Access Setting



- Preventing voice VLAN attacks
  - –Enable settings for PC voice VLAN access
  - –Tagged traffic will be stopped at the PC port on the phone
- Differences between phone model implementations
  - –7940, 7960, 7941G, 7961G, and 7971G only block voice VLAN, allowing PC to run 802.1Q on any other VLAN
  - –All phones that run JAVA block all packets containing an 802.1Q header
  - –7912 doesn't block anything

© 2011 Cisco and/or its affiliates. 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

© 2011 Cisco and/or its affiliates. All rights reserved.

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

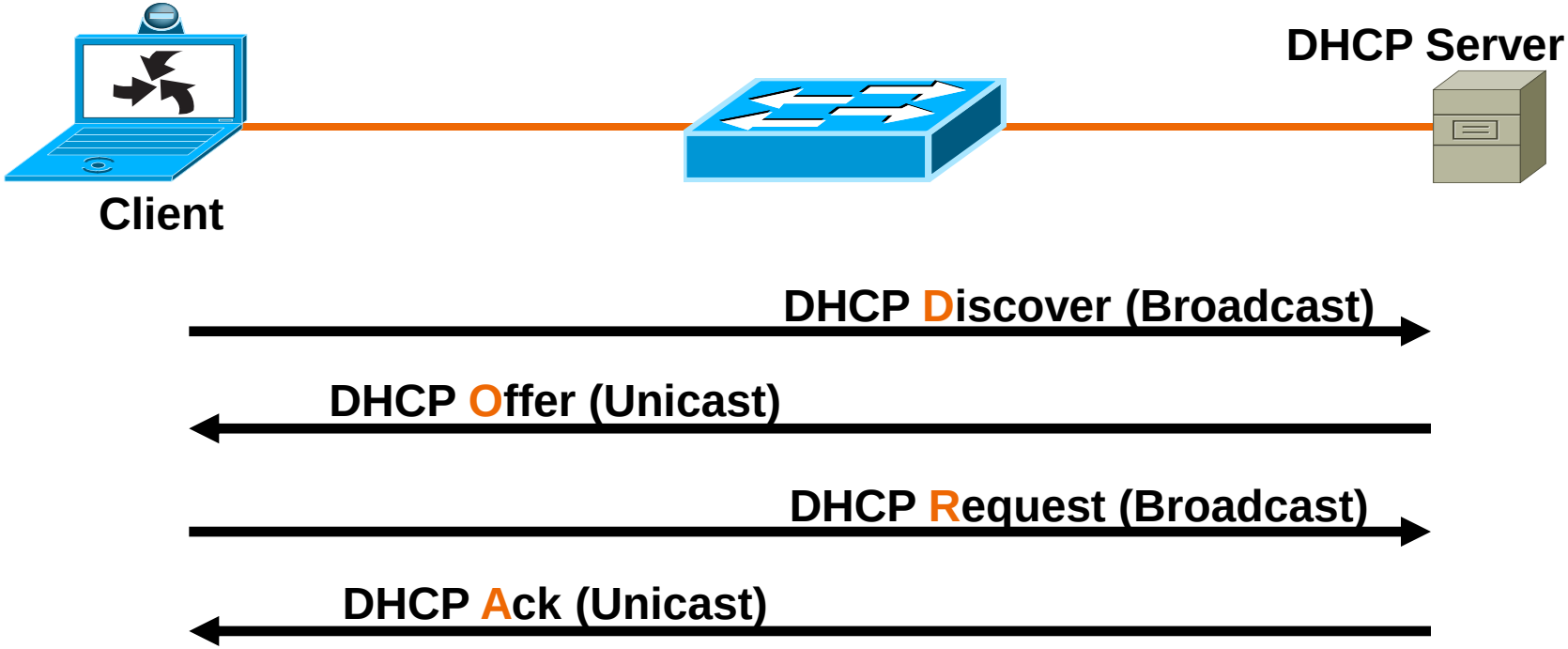
© 2011 Cisco and/or its affiliates. All rights reserved.

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
- Similar functionality in Ipv6 for DHCP

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

DHCP Function: Lower Level



- DHCP defined by RFC 2131

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

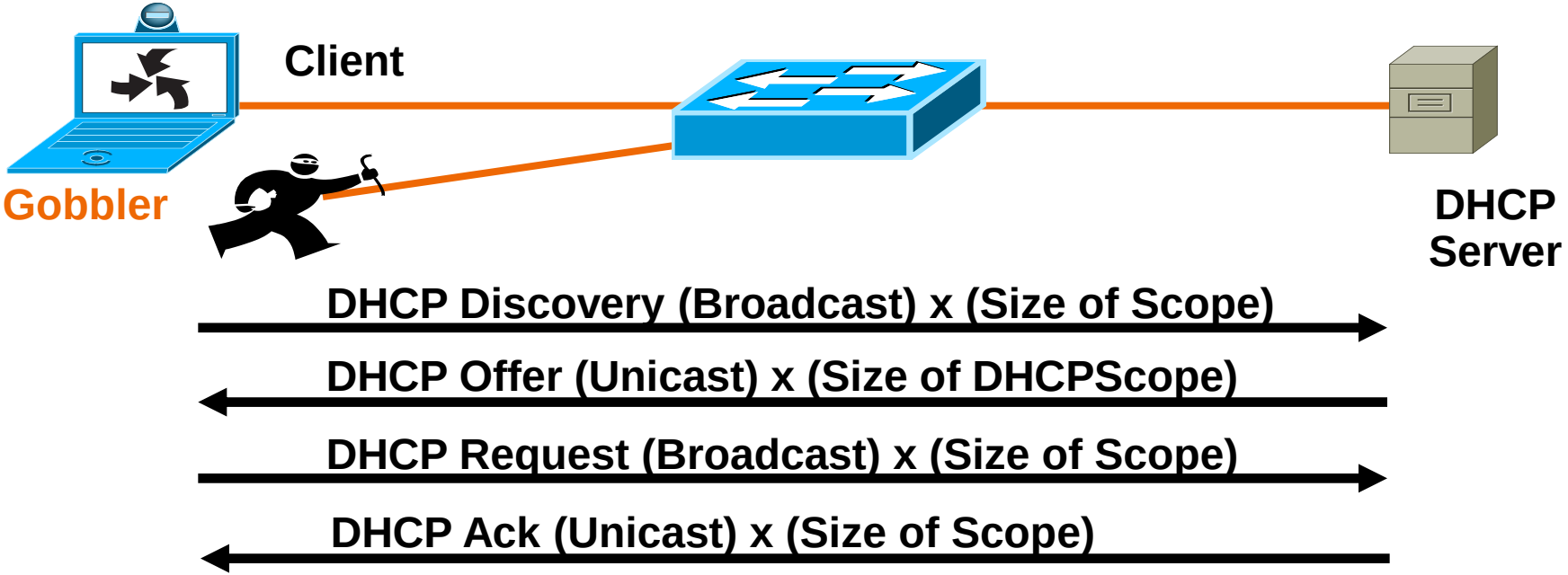
DHCP Function: Lower Level

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.

© 2011 Cisco and/or its affiliates. All rights reserved.

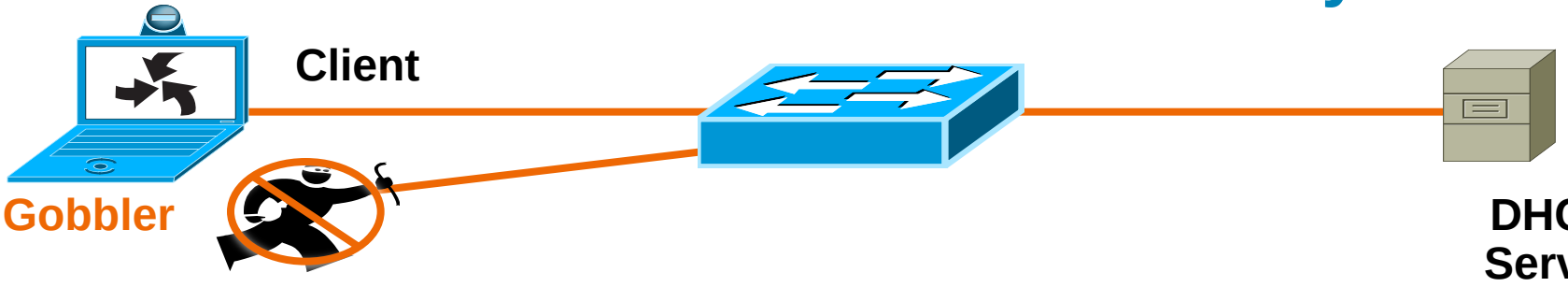
DHCP Attack Types
DHCP Starvation Attack



- 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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Countermeasures for DHCP Attacks
DHCP Starvation Attack = Port Security

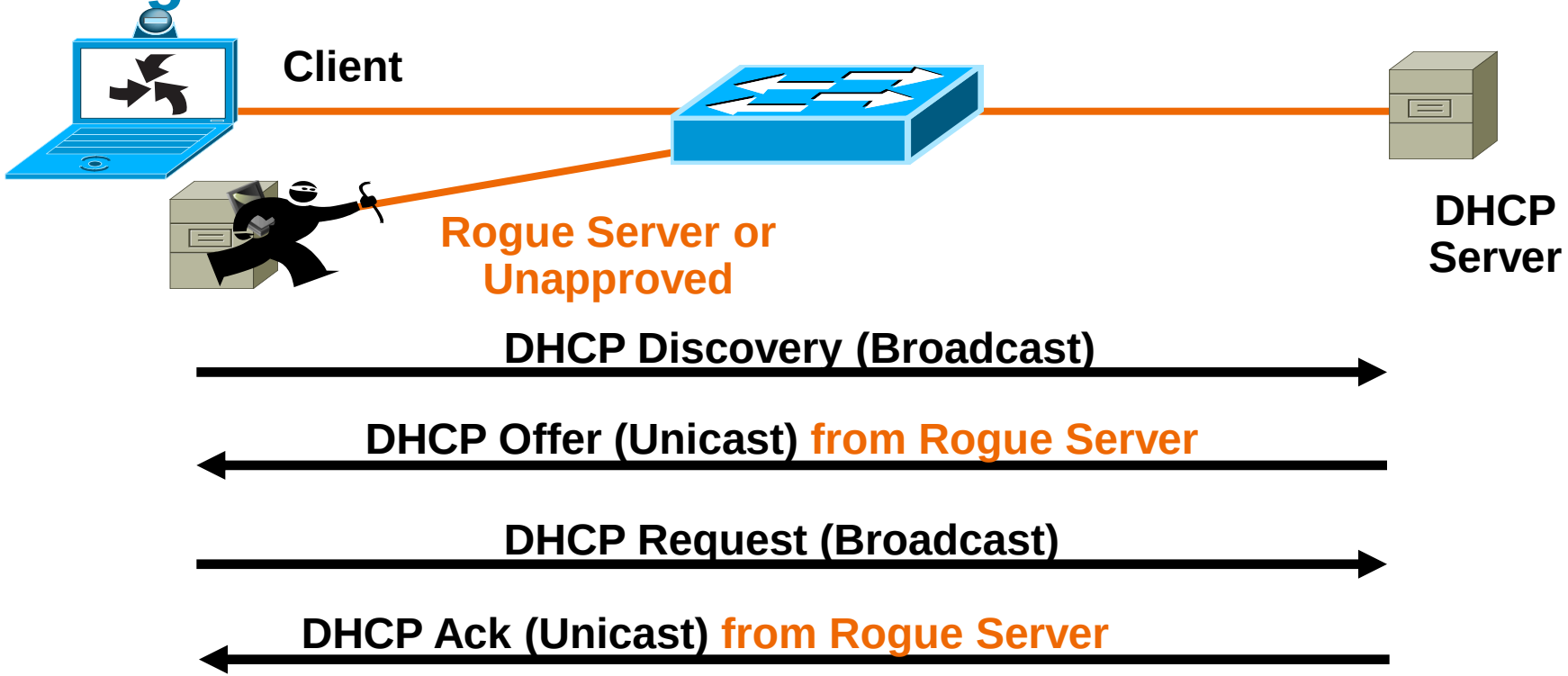


- Gobbler uses a new MAC address to request a new DHCP lease
- Restrict the number of MAC addresses on a port
- Will not be able to lease more IP address then MAC addresses allowed on the port
- In the example the attacker would get one IP address from the DHCP server

```
Cisco Catalyst OS
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
Cisco 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
```


© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

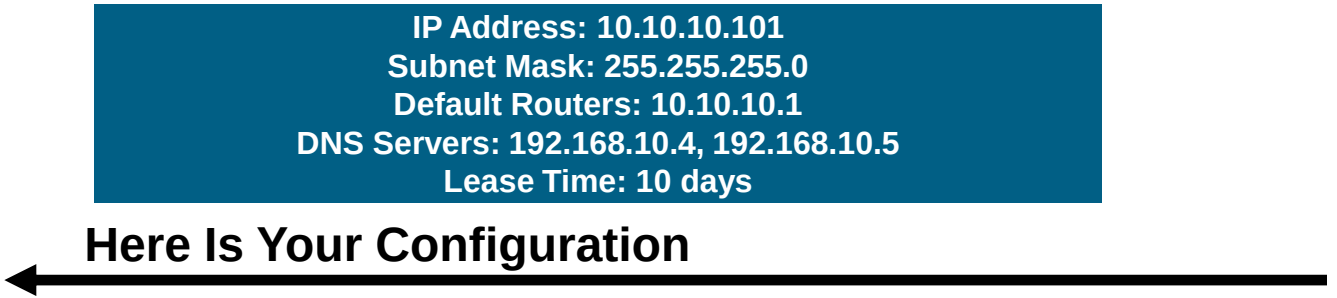
DHCP Attack Types
Rogue DHCP Server Attack



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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?

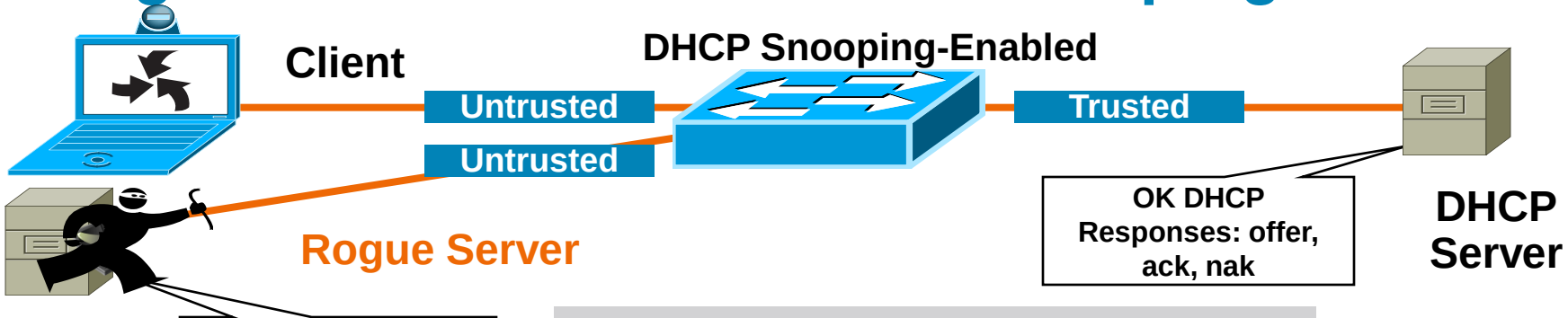
    Wrong default gateway—Attacker is the gateway

    Wrong DNS server—Attacker is DNS server

    Wrong IP address—Attacker does DOS with incorrect IP

© 2011 Cisco and/or its affiliates. All rights reserved.

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping




```
Cisco 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)
```

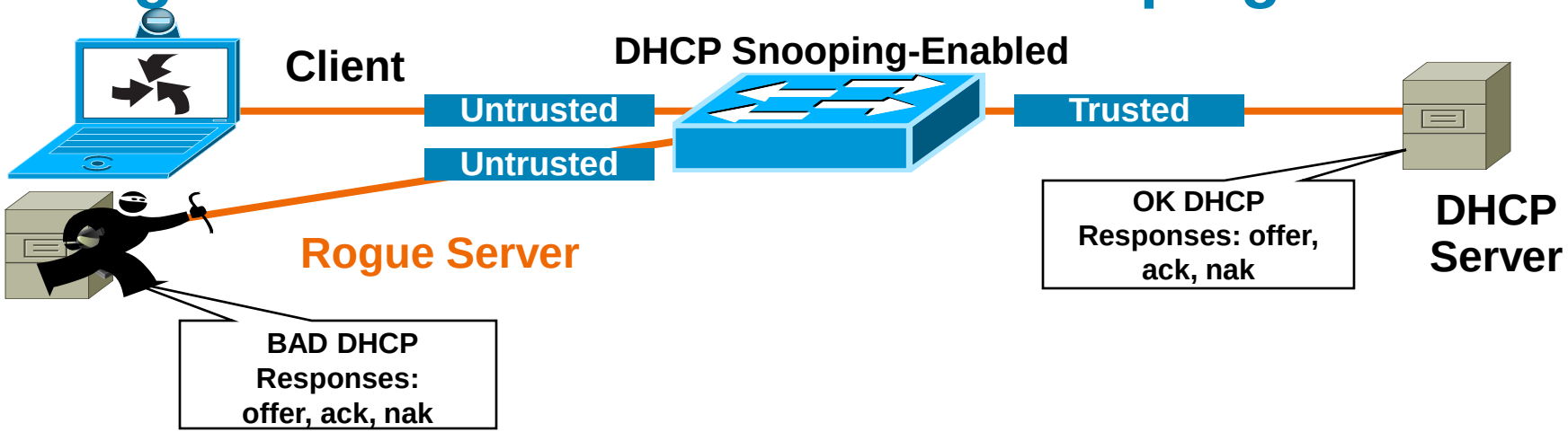
DHCP Snooping Trusted Server or Uplink

```
Interface Commands
ip dhcp snooping trust
```

- By default all ports in the VLAN are untrusted

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping



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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Advanced Configuration DHCP Snooping

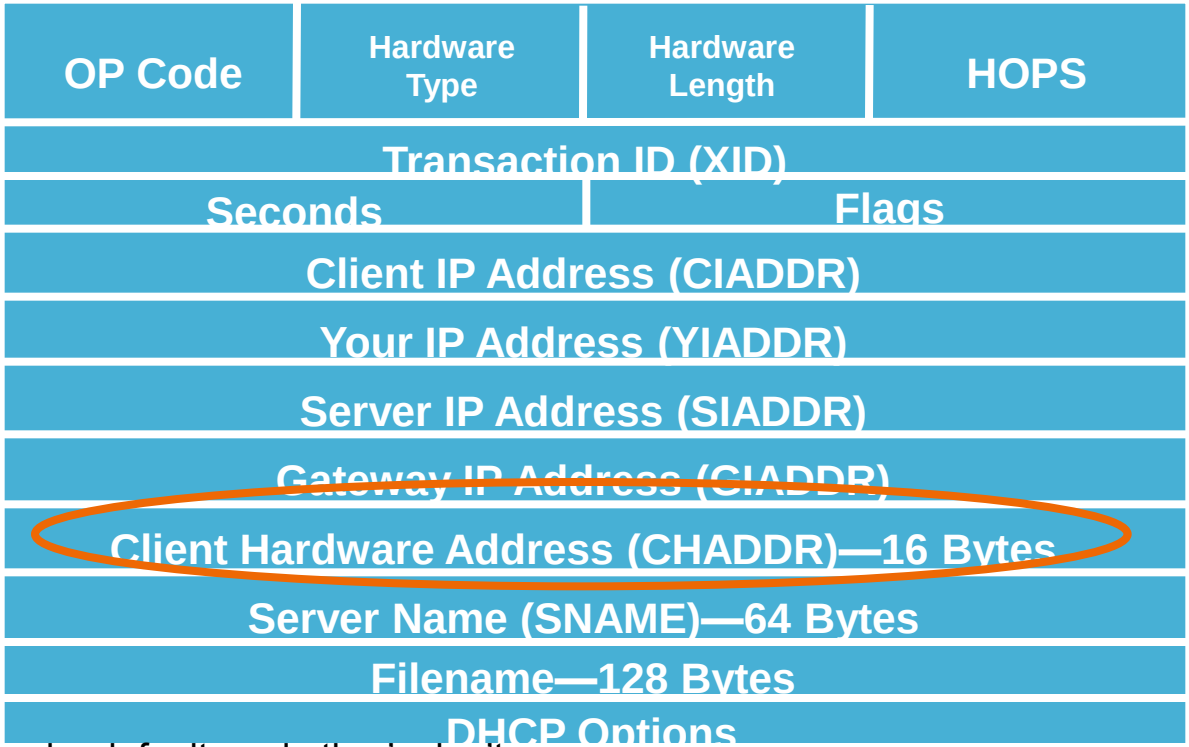
- Not all operating system (Linux) re DHCP on link down
- In the event of switch failure, the DHCP snooping binding table can be written to bootflash, ftp, rcp, slot0, and tftp

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


© 2011 Cisco and/or its affiliates. All rights reserved.

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



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

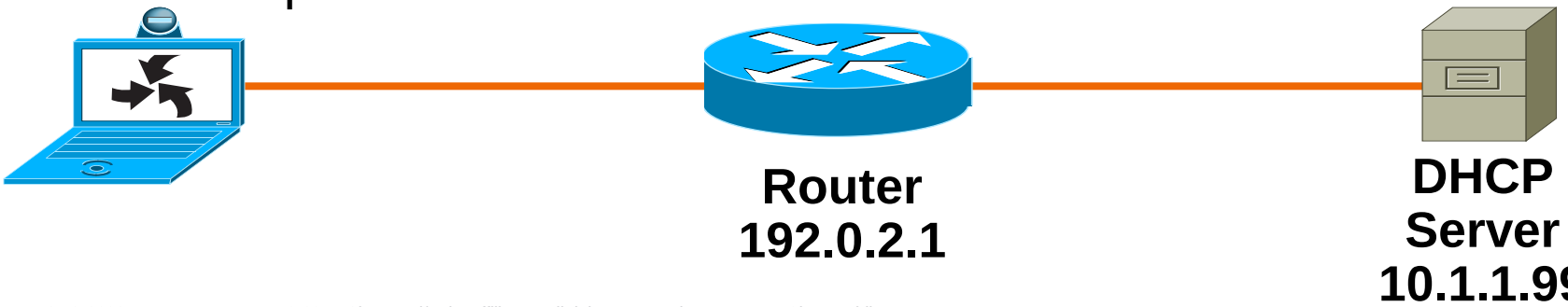
© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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)

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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
```


© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Building the Layers

- Port security prevents CAM attacks and DHCP starvation attacks
- DHCP snooping prevents rogue DHCP server attacks

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

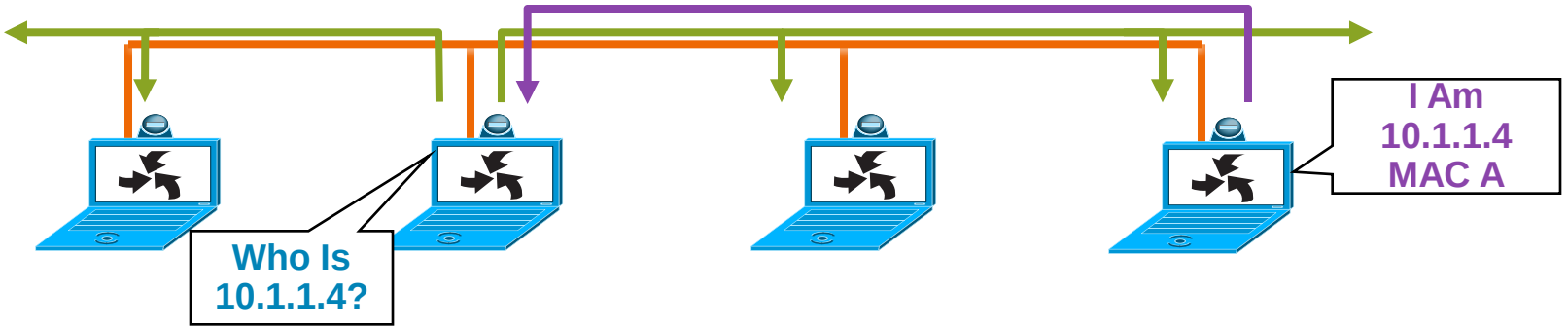
Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.

ARP Function Review

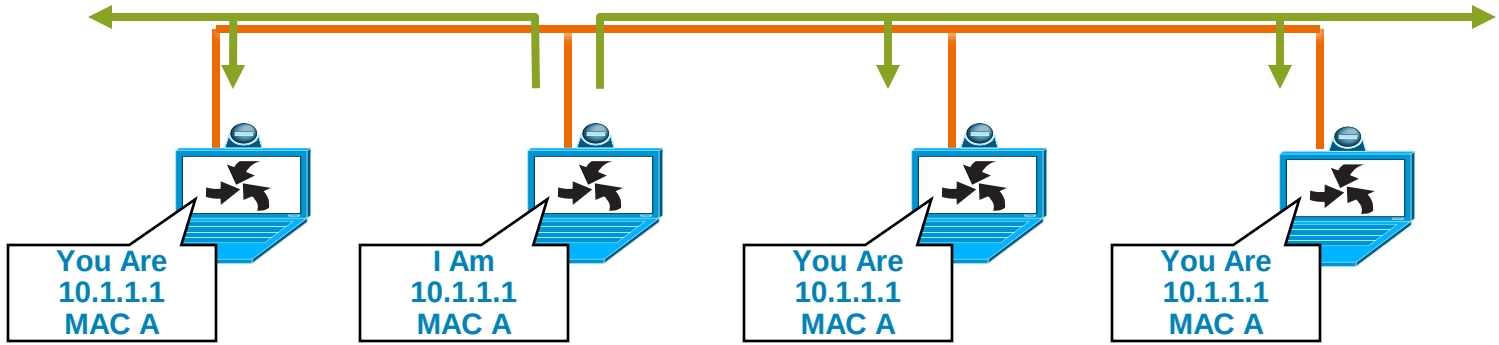
- Before a station can talk to another station it must do an ARP request to map the IP address to the MAC address
  - –This ARP request is broadcast using protocol 0806
- All computers on the subnet will receive and process the ARP request; the station that matches the IP address in the request will send an ARP reply



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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



© 2011 Cisco and/or its affiliates. All rights reserved.

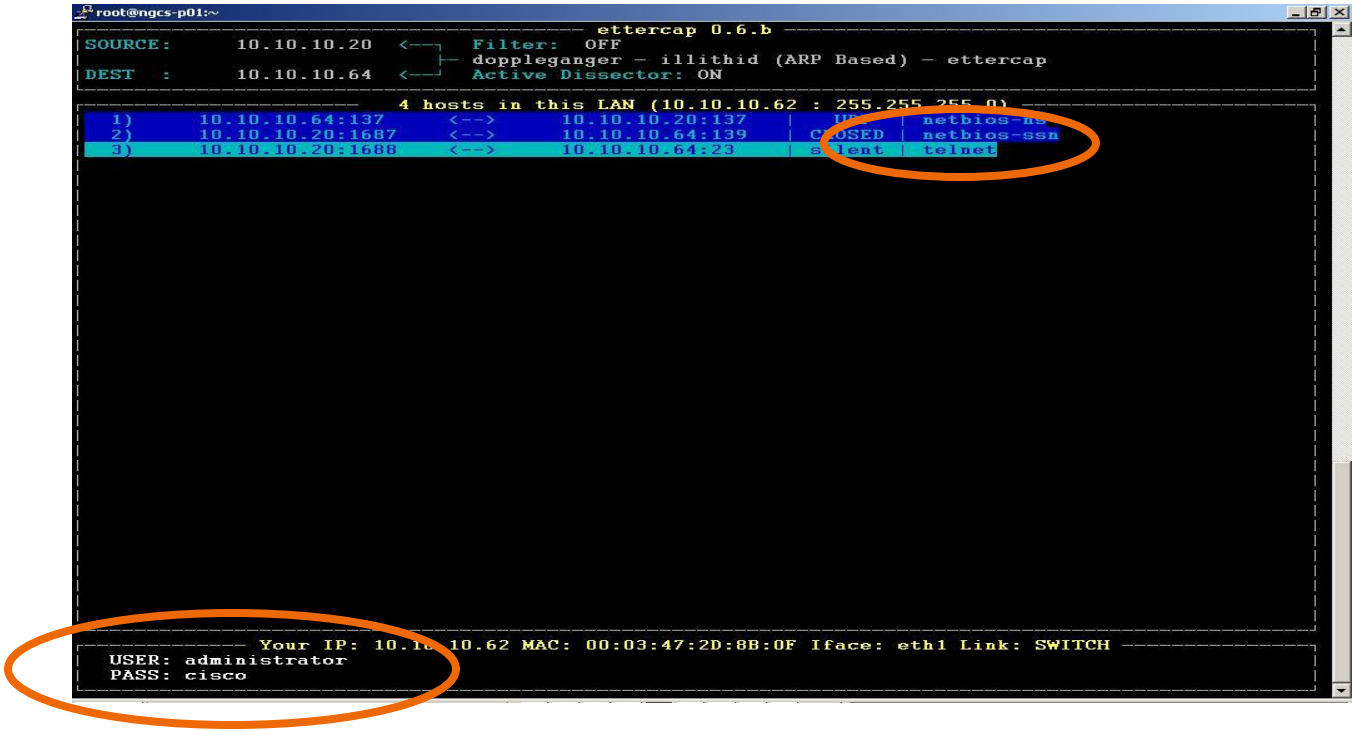
ARP Attack Tools

- 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.

© 2011 Cisco and/or its affiliates. All rights reserved.

ARP Attack Tools

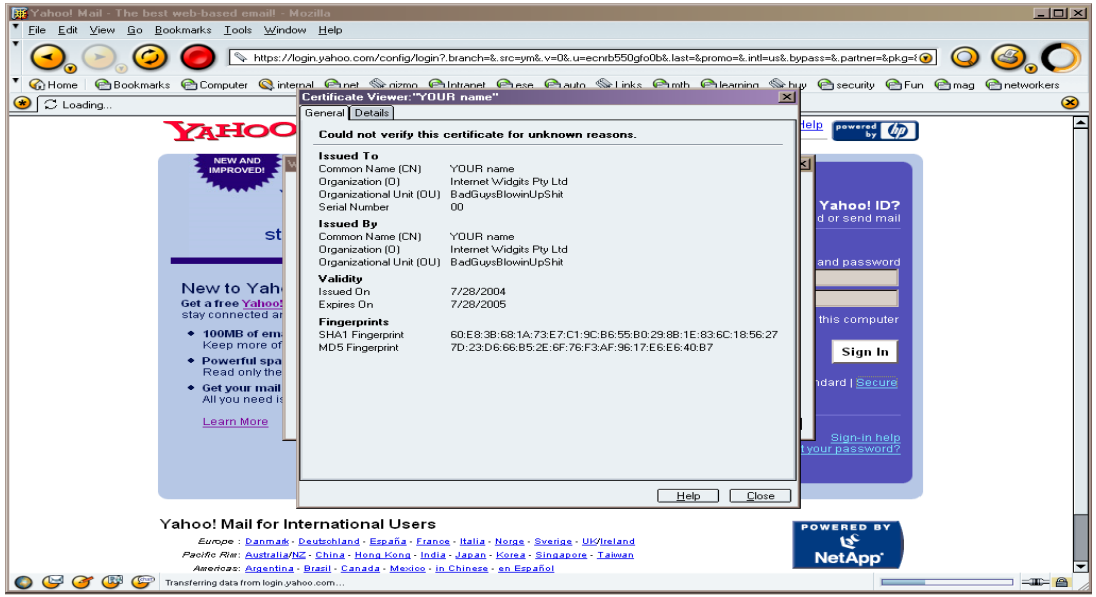
- Ettercap in action
- As you can see runs in Window, Linux, Mac
- Decodes passwords on the fly
- This example, telnet username/ password is captured



© 2011 Cisco and/or its affiliates. All rights reserved.

ARP Attack Tools: SSH/SSL

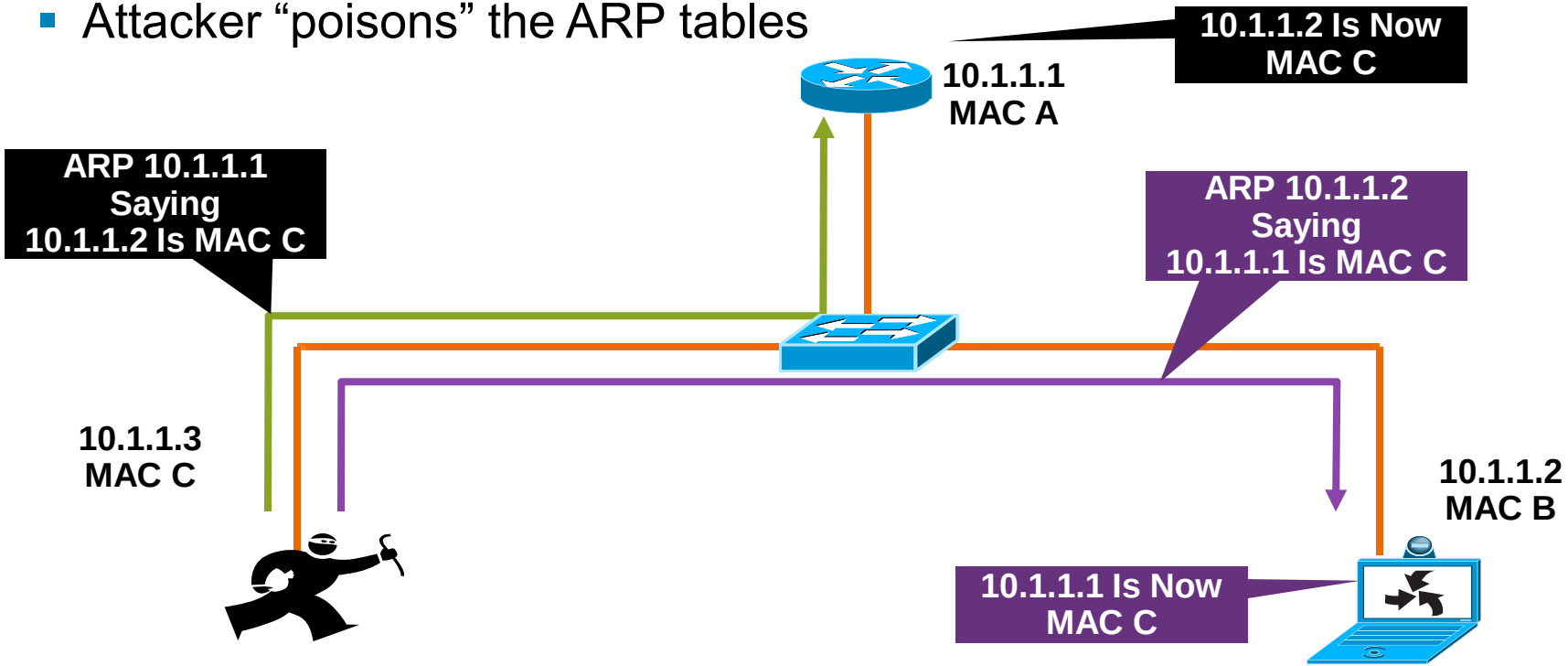
- Using these tools SSL/SSH sessions can be intercepted and bogus certificate credentials can be presented
- Once you have excepted the certificate, all SSL/SSH traffic for all SSL/SSH sites can flow through the attacker



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

ARP Attack in Action

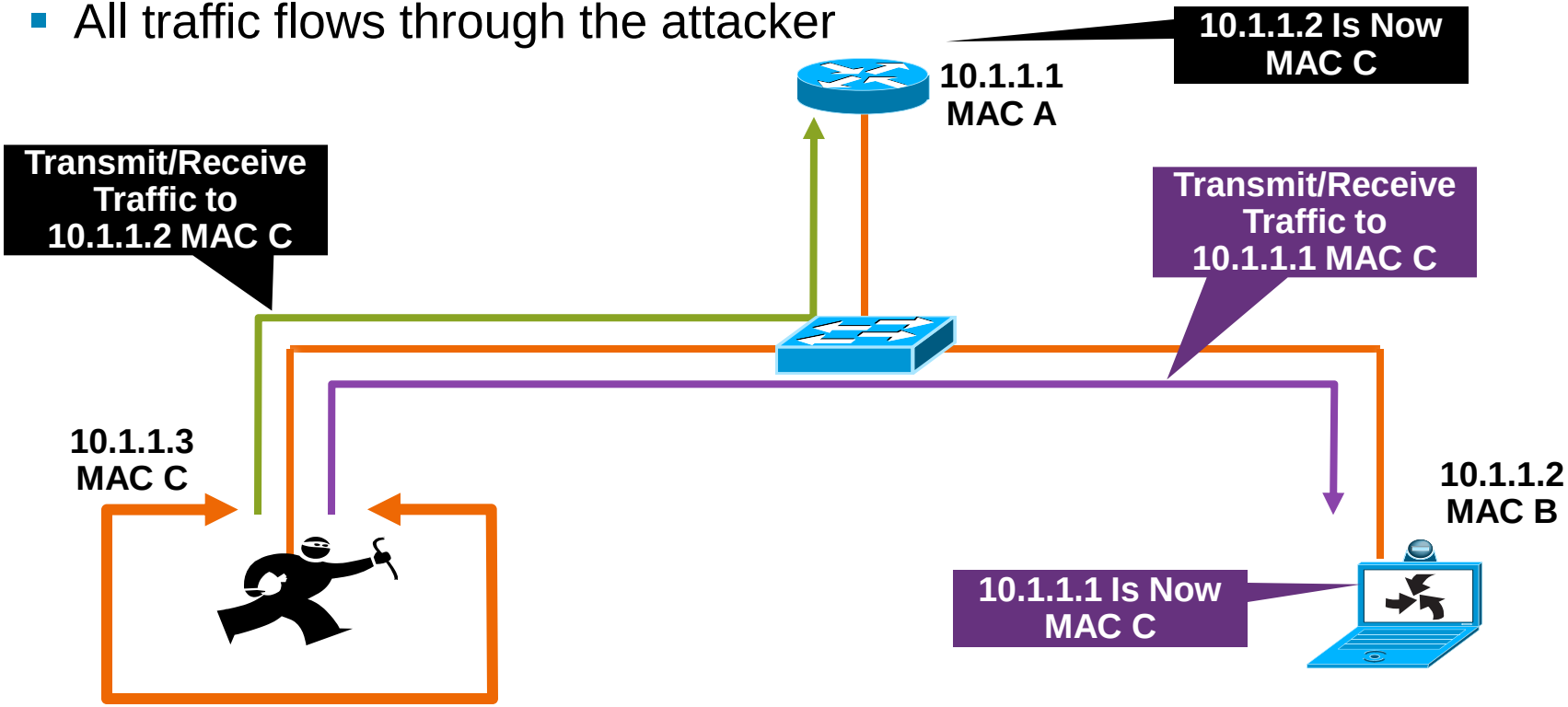
- Attacker “poisons” the ARP tables



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

ARP Attack in Action

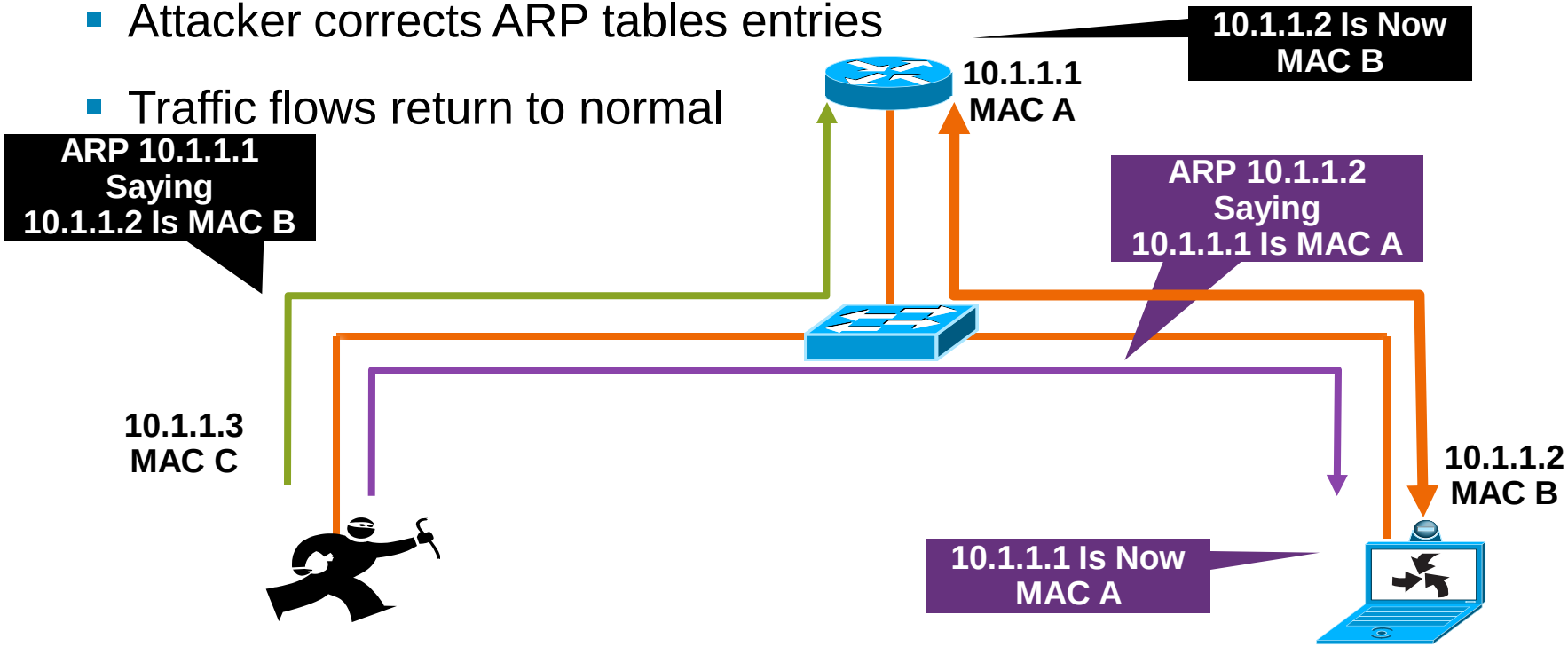
- All traffic flows through the attacker



© 2011 Cisco and/or its affiliates. All rights reserved.

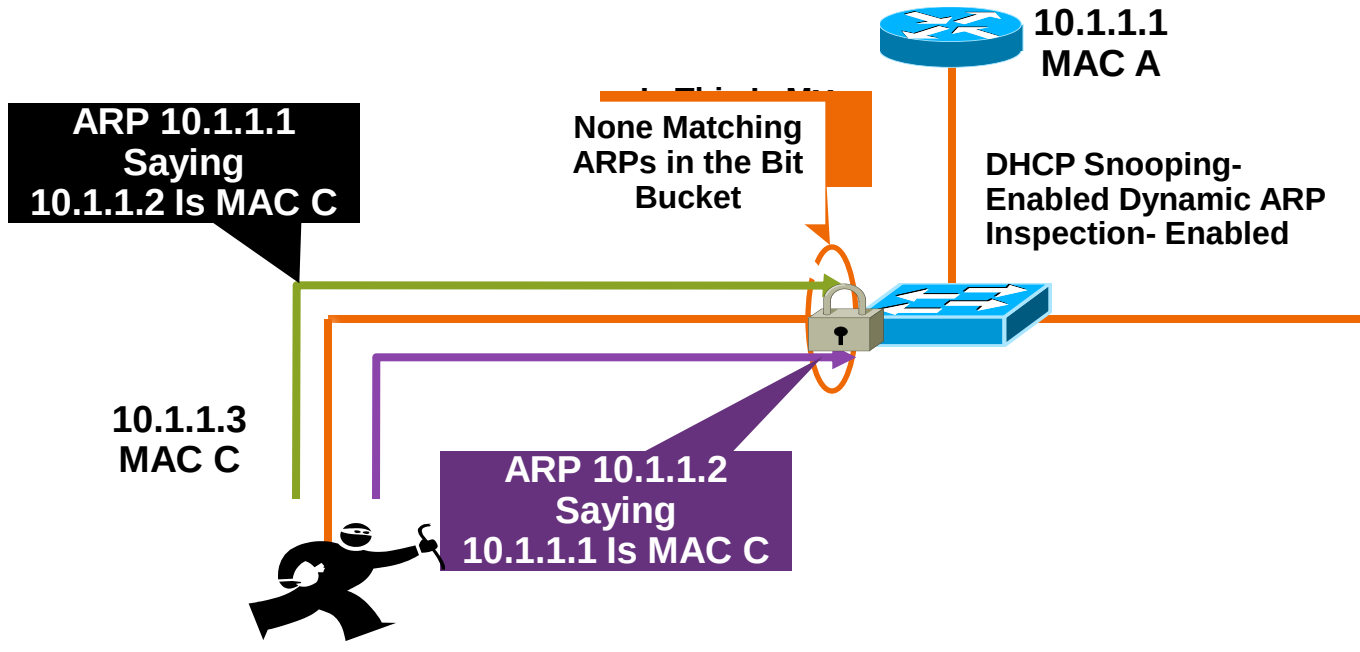
ARP Attack Clean Up

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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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

© 2011 Cisco and/or its affiliates. All rights reserved.

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; if not, traffic is blocked

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Countermeasures to ARP Attacks: Dynamic ARP Inspection

Dynamic ARP Inspection Commands

```
Cisco 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
```

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


© 2011 Cisco and/or its affiliates. All rights reserved.

Additional Checks

- Can check for both destination or source MAC and IP addresses
  - –Destination MAC: Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body
  - –Source MAC: Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body
  - –IP address: Checks the ARP body for invalid and unexpected IP addresses; addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Cisco IOS Commands

```
Cisco IOS
Global Commands
ip arp inspection validate dst-mac

ip arp inspection validate src-mac

ip arp inspection validate ip

Enable all commands
ip arp inspection validate src-mac dst-mac ip
```

- Each check can be enabled independently
  - –Each by themselves, or any combination of the three
- The last command overwrites the earlier command
  - –If you have dst-mac enabled and then enable src-mac, dst-mac is no longer active

© 2011 Cisco and/or its affiliates. All rights reserved.

Countermeasures to ARP Attacks: Dynamic ARP Inspection

Error Messages in Show Log

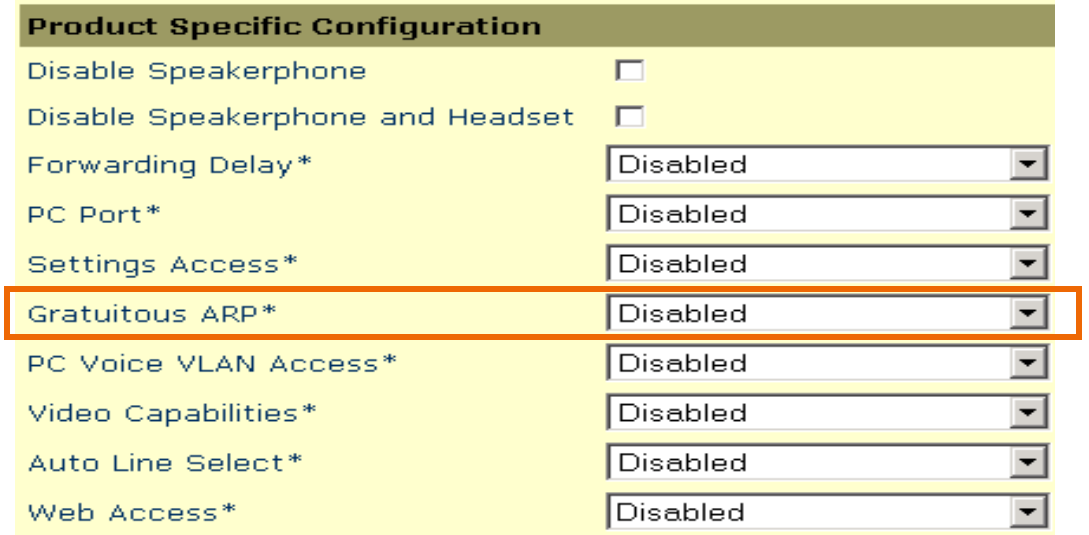
```
sh log:
4w6d: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 296 milliseconds on Gi3/2.
4w6d: %PM-4-ERR_DISABLE: arp-inspection error detected on Gi3/2, putting Gi3/2 in err-disable
state
4w6d: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi3/2, vlan
183.([0003.472d.8b0f/10.10.10.62/0000.0000.0000/10.10.10.2/12:19:27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


© 2011 Cisco and/or its affiliates. All rights reserved.

Phone ARP Features

Configurable Options

- Block voice VLAN from PC port
- Ignore Gratuitous ARPs (GARPs)

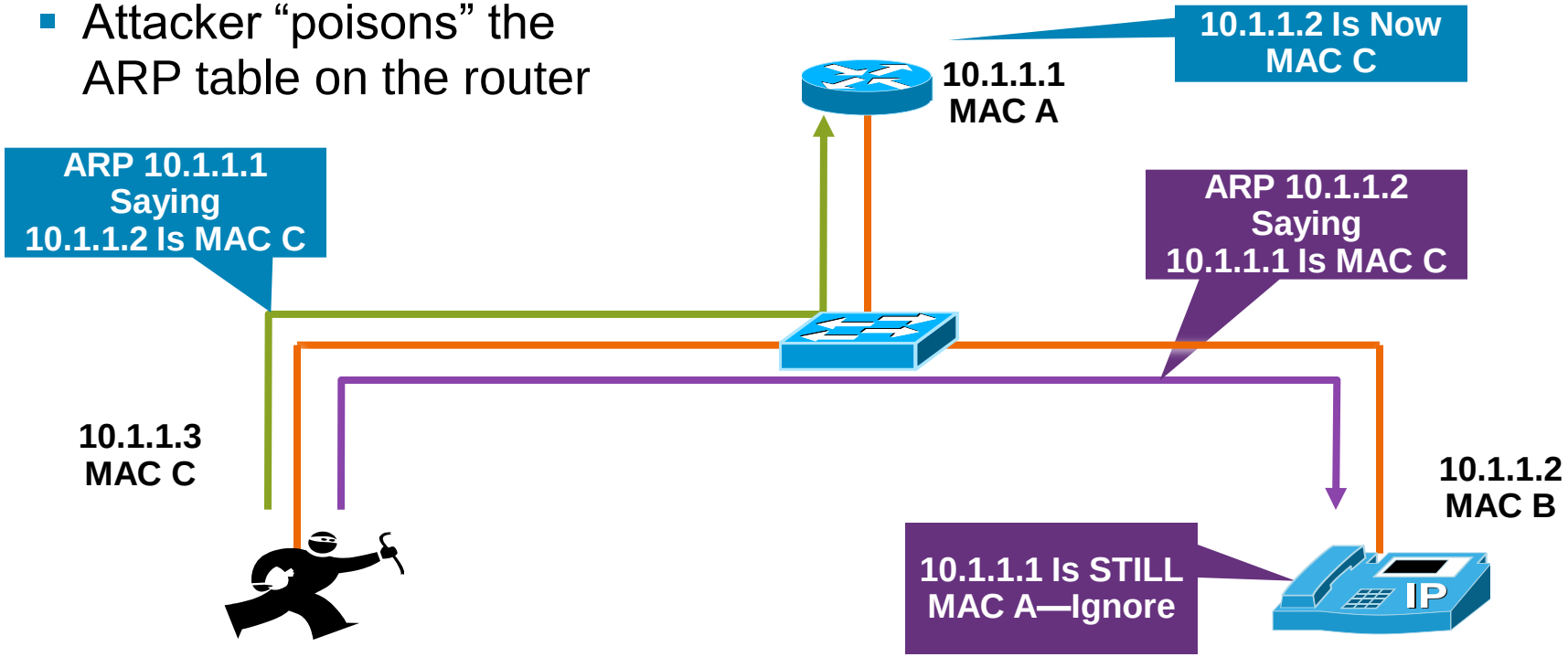


These Features Were All Introduced in CCM 3.3(3), Except Signed Config Files and Disable Web Access Which Were Introduced in CCM 4.0

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Phone ARP Features

- Attacker “poisons” the ARP table on the router

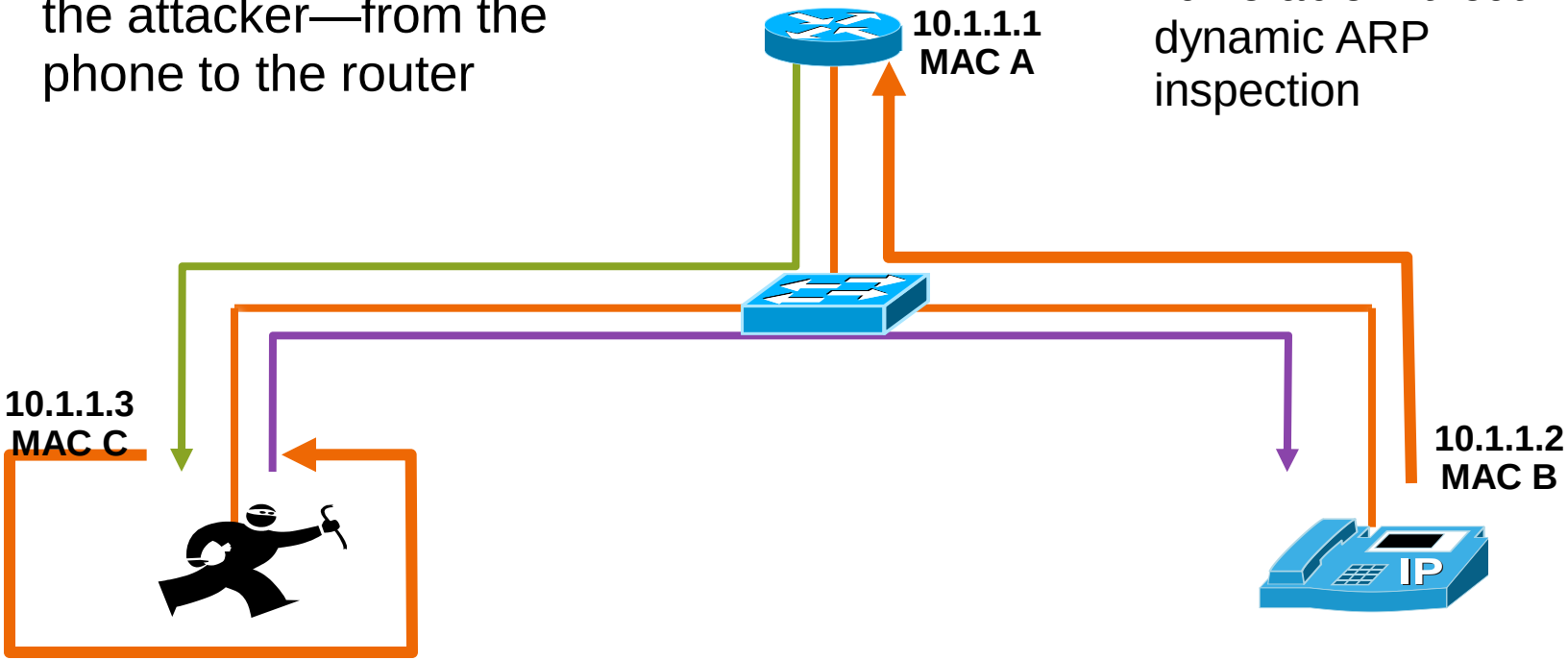


© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Phone ARP Features

- Traffic from the router to the attacker—from the phone to the router

- Traffic from the phone is protected, but the router is still vulnerable without dynamic ARP inspection



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Non-DHCP Devices

- Can use static bindings in the DHCP snooping binding table

```
Cisco 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

```
Cisco IOS
Show Commands
 show ip source binding
```


© 2011 Cisco and/or its affiliates. All rights reserved.

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

© 2011 Cisco and/or its affiliates. All rights reserved.

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

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

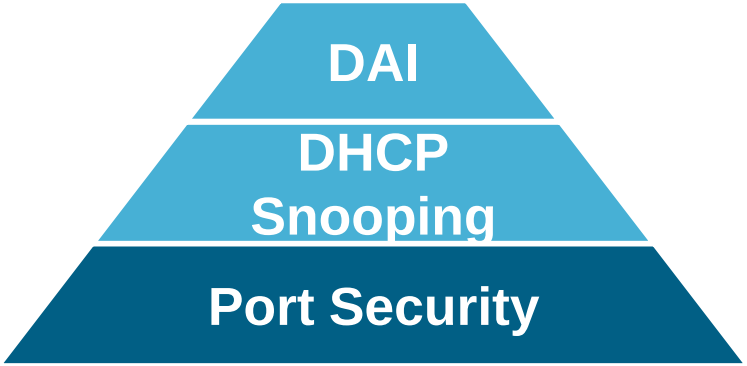
More ARP Attack Information

- 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)

© 2011 Cisco and/or its affiliates. All rights reserved.

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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

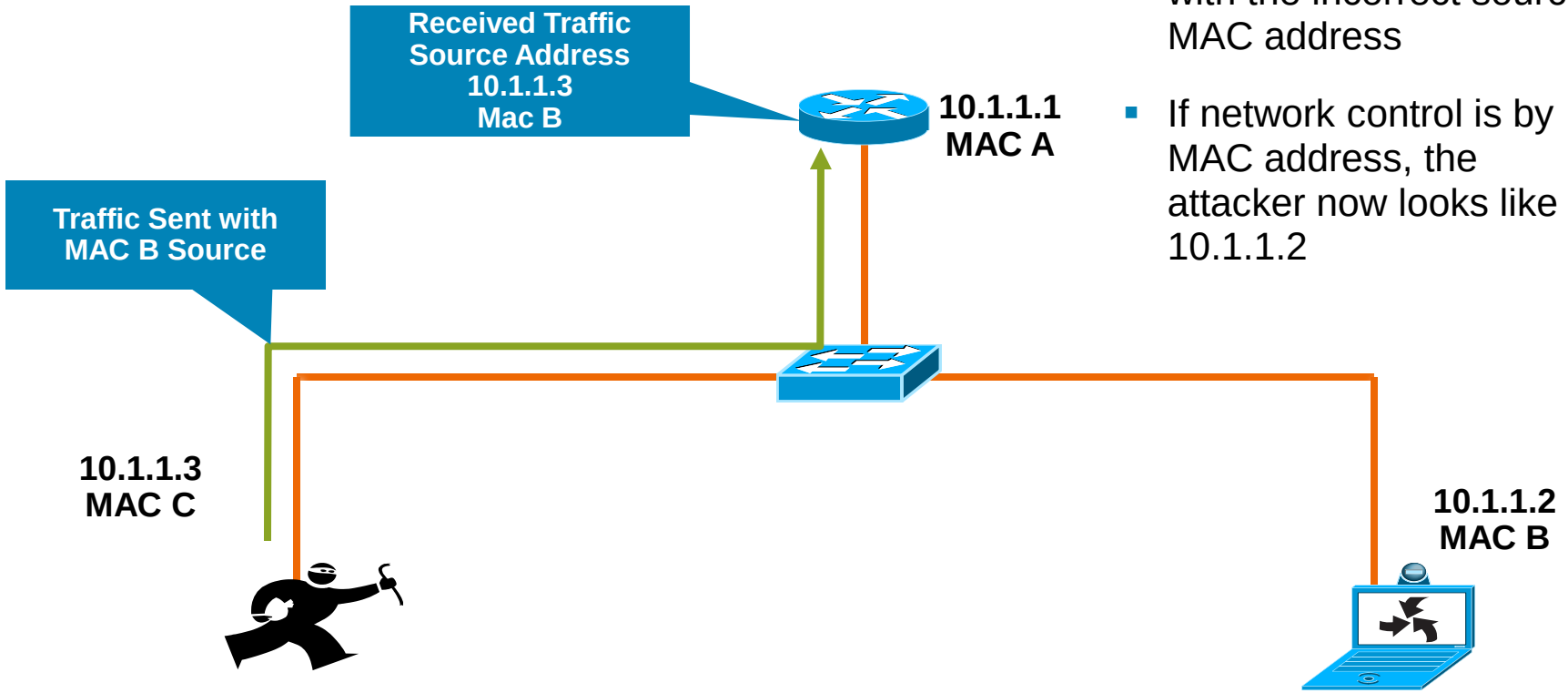
© 2011 Cisco and/or its affiliates. All rights reserved.

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

© 2011 Cisco and/or its affiliates. All rights reserved.

Spoofing Attack: MAC

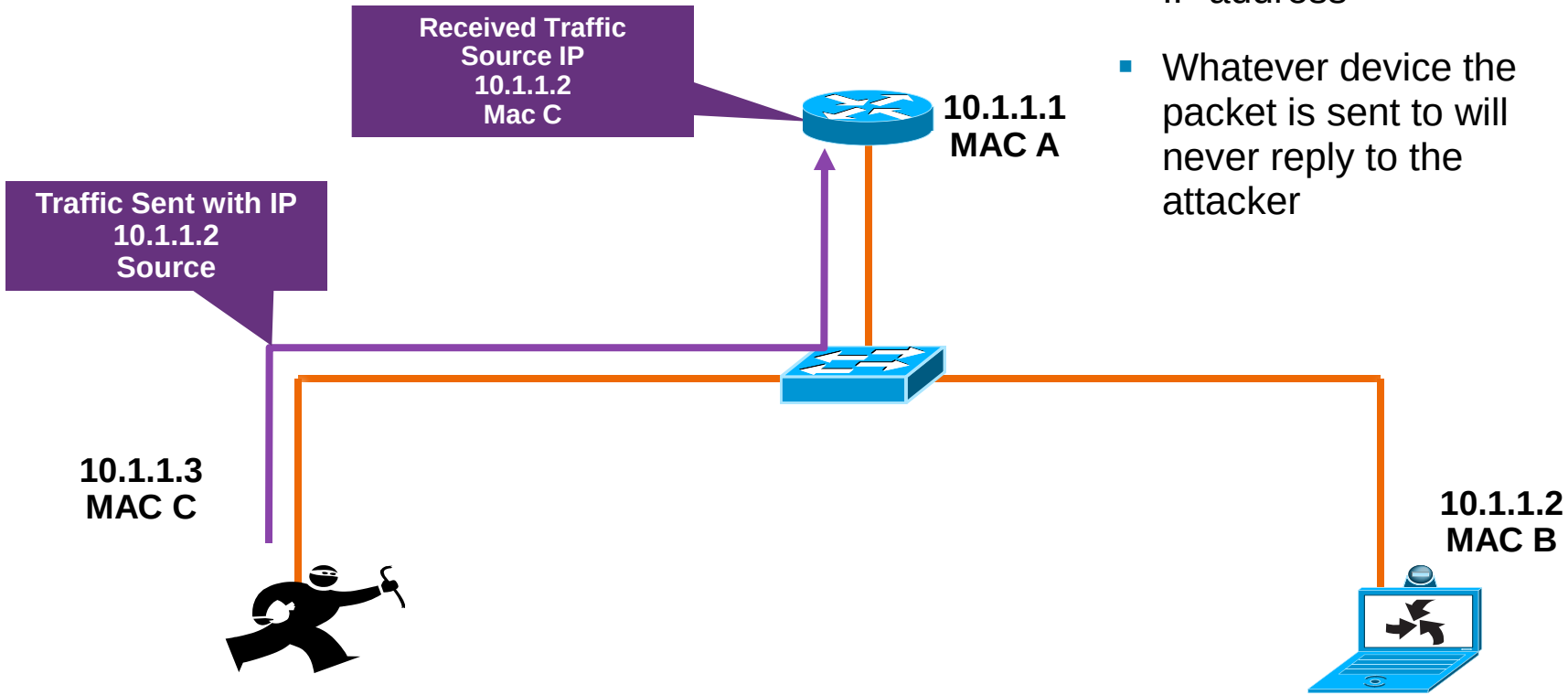


- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Spoofing Attack: IP

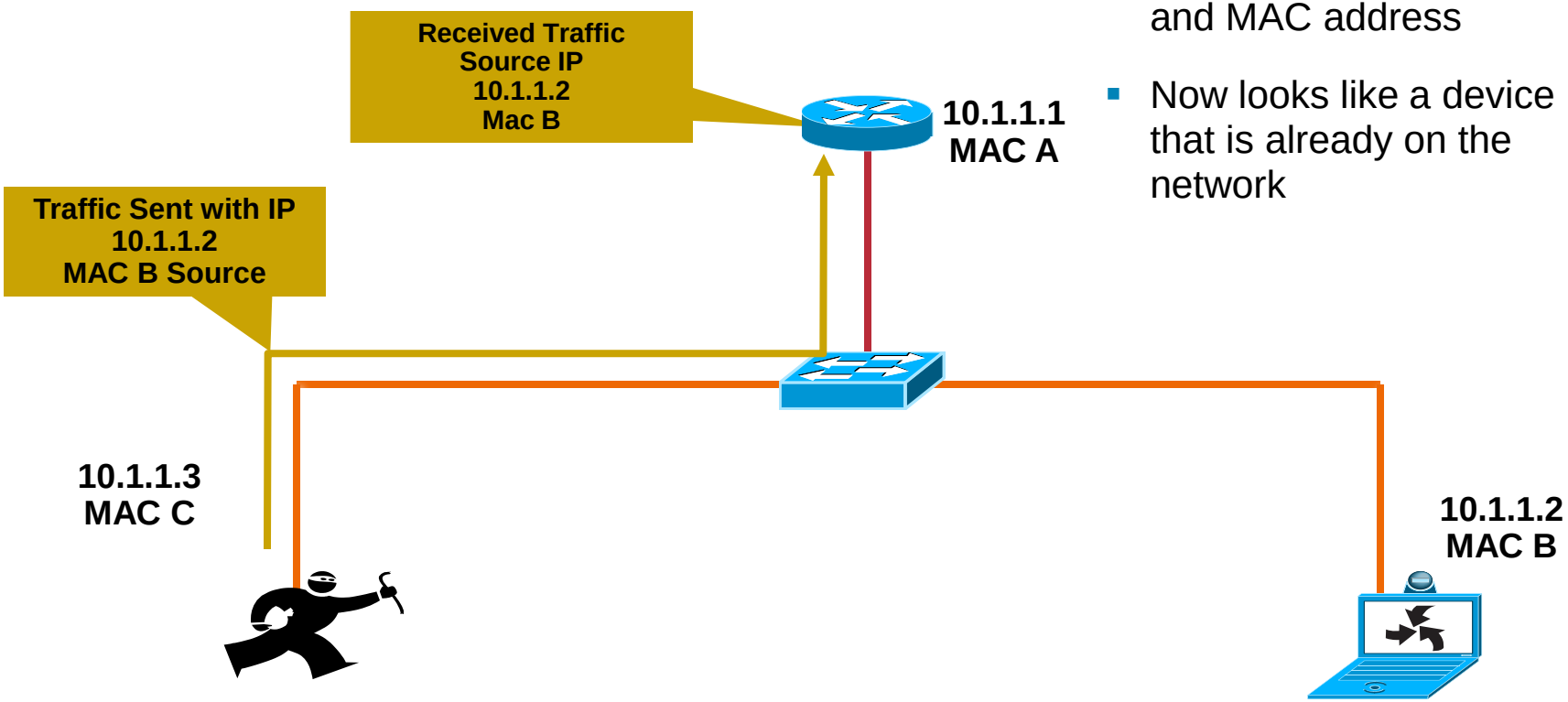
- Attacker sends packets with the incorrect source IP address
- Whatever device the packet is sent to will never reply to the attacker



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Spoofing Attack: IP/MAC

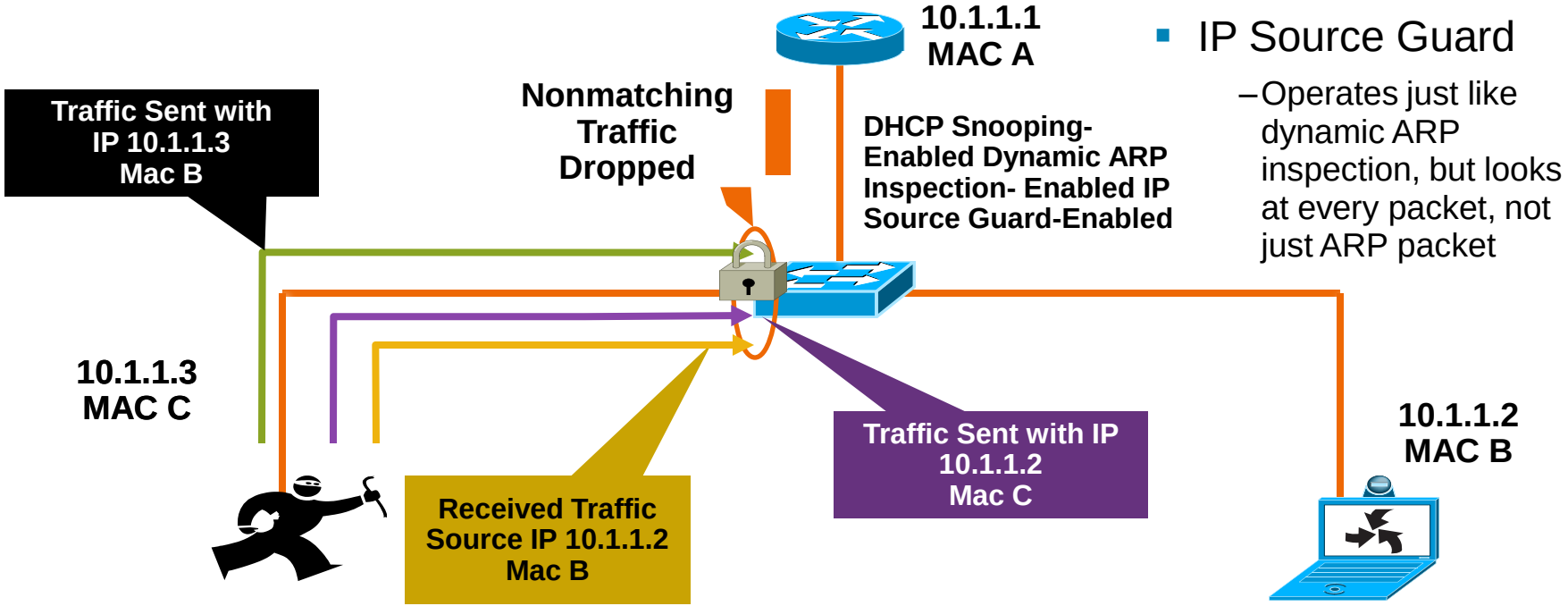
- Attacker sends packets with the incorrect source IP and MAC address
- Now looks like a device that is already on the network



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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

© 2011 Cisco and/or its affiliates. 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 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

© 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public

Clearing 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

© 2011 Cisco and/or its affiliates. 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

```
Cisco 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)

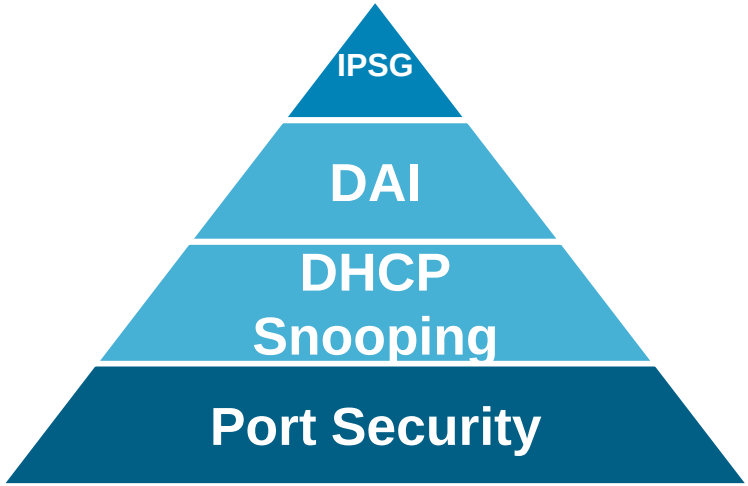
```
Cisco IOS
Global Commands
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping
   port-security
```

Static IP addresses can be learned, but only used for IP Source Guard

© 2011 Cisco and/or its affiliates. All rights reserved.

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



© 2011 Cisco and/or its affiliates. All rights reserved.

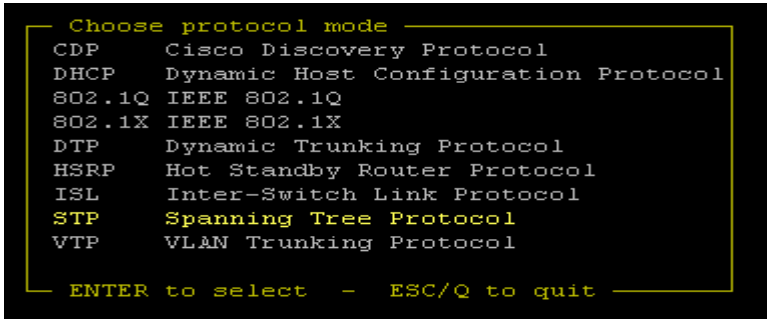
Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –Attacks on other protocols
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.

Other Protocols?

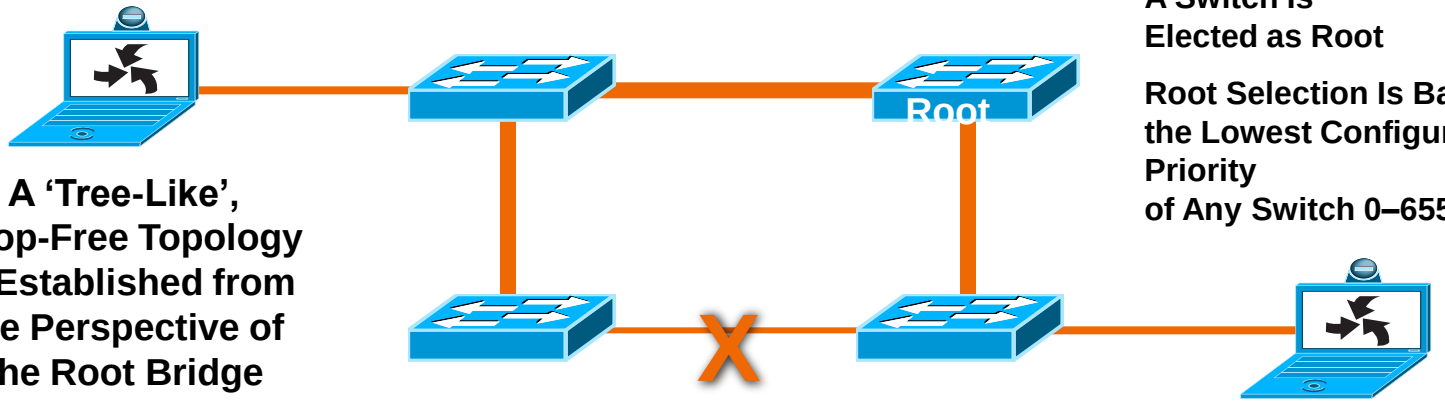
- Yersinia can help you with:
  - –CDP
  - –DHCP
  - –802.1Q
  - –802.1X
  - –DTP
  - –HSRP
  - –STP
  - –VTP



© 2011 Cisco and/or its affiliates. All rights reserved.

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

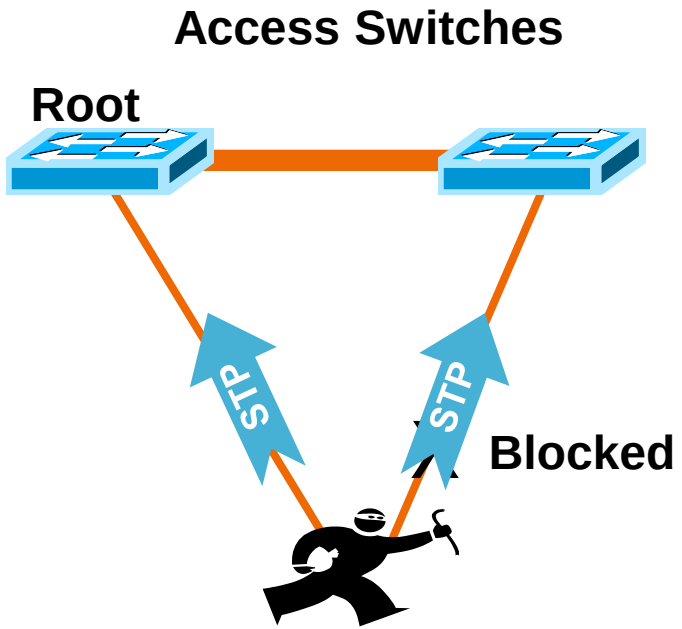
A ‘Tree-Like’, Loop-Free Topology Is Established from the Perspective of the Root Bridge

- 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

© 2011 Cisco and/or its affiliates. All rights reserved.

Spanning Tree Attack Example

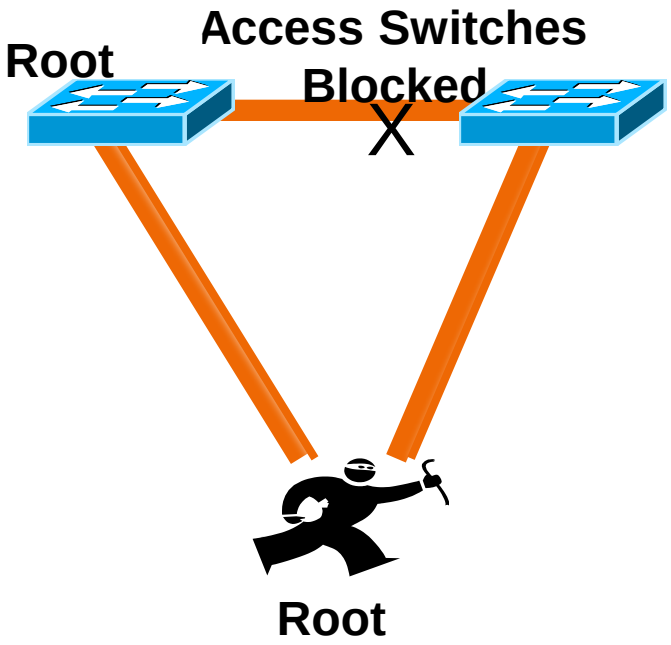
- Send BPDU messages to become root bridge



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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)



© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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 Cisco Catalyst OS 5.4.1 for Cisco Catalyst 2000 Series, Cisco Catalyst 4000 Series, Cisco Catalyst 5000 Series, and Cisco Catalyst 6000 Series; 12.0XE for native Cisco IOS 6000 Series; 12.1(8a)EW for Cisco 4000 Series 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
```


© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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 Cisco Catalyst OS 6.1.1 for Cisco Catalyst 29XX, Cisco Catalyst 4000 Series, Cisco Catalyst 5000 Series, Cisco Catalyst 6000 Series; 12.0(7) XE for native Cisco IOS 6000 Series, 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)
```


© 2011 Cisco and/or its affiliates. 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 nonstandard VLAN where nothing but management traffic resides
  - –Consider physically backhauling 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 Cisco Catalyst 6000 Series with Cisco Catalyst OS 6.1 and Cisco Catalyst 4000 Series/29XXG with Cisco Catalyst OS 6.3; 3550 in 12.1(11)EA1; 2950 in 12.1(12c)EA1; Cisco IOS 6000 Series 12.1(5c)E12; Cisco IOS 4000 Series in 12.1(13)EW

© 2011 Cisco and/or its affiliates. All rights reserved.

Agenda

- Layer 2 Attack Landscape
- Attacks and Countermeasures
  - –VLAN Hopping
  - –MAC Attacks
  - –DHCP Attacks
  - –ARP Attacks
  - –Spoofing Attacks
  - –General Attacks
- Summary

© 2011 Cisco and/or its affiliates. All rights reserved.

The One Thing to Remember

- If you do not have a binding table entry, you will not allow traffic from that port with these features enabled
  - –Dynamic ARP inspection
  - –IP Source Guard
- Users get grumpy when this happens
- Would be wise to test and understand before deployment

© 2011 Cisco and/or its affiliates. All rights reserved.

Matrix for Security Features (1/3)

Feature/Platform	6500/ Cisco Catalyst OS	6500/Cisco IOS	Nexus 7000	4500/Cisco IOS
Dynamic Port Security	7.6(1)	12.1(13)E	4.1	12.1(13)EW
Per VLAN Dynamic Port Security	8.3(1)	12.2(33)SXH	4.1	12.2(31)SGA ***
DHCP Snooping	8.3(1)	12.2(18)SXE*	4.1	12.1(12c)EW ***
DAI	8.3(1)	12.2(18)SXE*	4.1	12.1(19)EW ***
IP Source Guard	8.3(1)**	12.2(18)SXD2	4.1	12.1(19)EW ***

*Works on trunks today, roadmapped for access ports

**Requires Sup720—support for Sup32 DHCP snooping and DAI

***For the Cisco Catalyst 4500-Cisco IOS-based platforms, this requires Sup2+ or above

These Sups are supported on the Cisco Catalyst 4006, 4503, 4506, and 4507R chassis running

© 2011 Cisco and/or its affiliates. All rights reserved.

Matrix for Security Features (2/3)

Feature/Platform	3750/3560 EMI	3550 EMI	2960 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
Per VLAN Dynamic Port Security	12.2(37)SE	NA	12.2(37)SE	NA	NA
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 Cisco IOS for the 3000 Series switches
Cisco IOS feature finder: http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

Matrix for Security Features (3/3)

Feature/Platform	3750/3560 Advanced 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)SEA	12.2(25)SEA
Per VLAN Dynamic Port Security	12.2(37)SE	N/A	12.2(37)SEA	N/A
DHCP Snooping	12.1(25)SE	12.1(25)SEA	12.1(25)SEA	12.1(25)SEA
DAI	12.2(25)SE	12.2(25)SEA	12.2(25)SEA	12.2(25)SEA
IP Source Guard	12.2 (25)SE	12.2(25)SEA	12.1(25)SEA	12.2(25)SEA

Note: Name change of the Cisco IOS on the 3000 Series switches
Cisco IOS feature finder: http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

© 2011 Cisco and/or its affiliates. All rights reserved.
Cisco Public

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 nontrunking (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.)

© 2011 Cisco and/or its affiliates. All rights reserved.

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

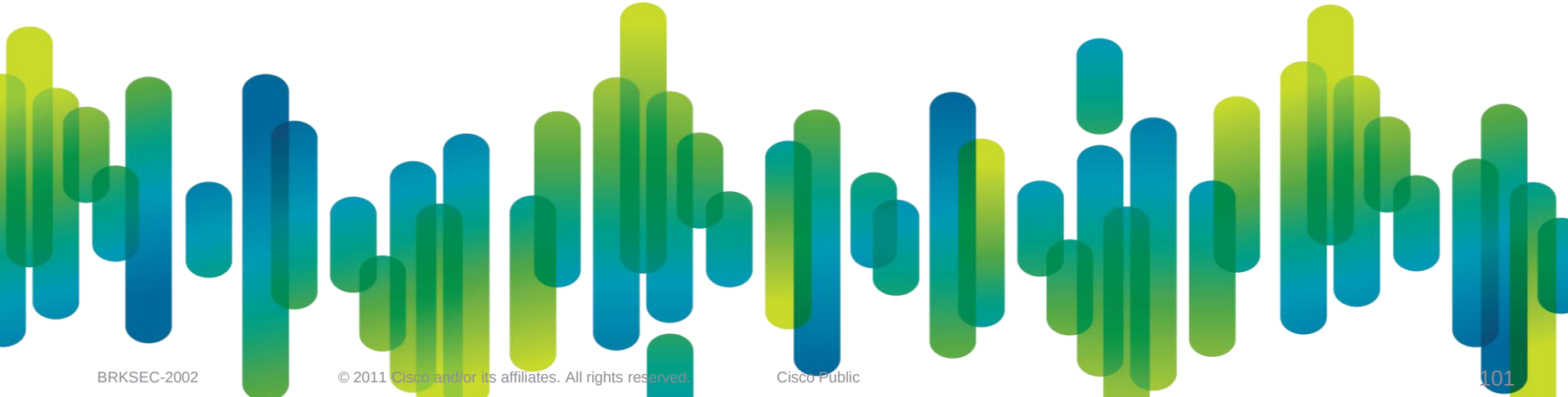
© 2011 Cisco and/or its affiliates. All rights reserved.

Reference Materials

- SAFE Blueprints
  - –http://www.cisco.com/go/safe/
- Cisco Catalyst® 3750
  - –http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm
- Cisco Catalyst 4000
  - –http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/index.htm
- Cisco Catalyst 6500
  - –Cisco Catalyst OS and Cisco IOS®
  - –http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/
- IP Phones
  - –http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm
- Data Centre
  - –http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor3
- All SRNDs (System Network Reference Designs)
  - –http://www.cisco.com/go/srnd/

© 2011 Cisco and/or its affiliates. All rights reserved.

Q & A



© 2011 Cisco and/or its affiliates. All rights reserved.

Complete Your Online Session Evaluation

Complete your session evaluation:

- Directly from your mobile device by visiting www.ciscoliveaustralia.com/mobile and login by entering your badge ID (located on the front of your badge)
- Visit one of the Cisco Live internet stations located throughout the venue
- Open a browser on your own computer to access the Cisco Live onsite portal

© 2011 Cisco and/or its affiliates. All rights reserved.


CISCO