Deploying Security in Carrier Ethernet Access Networks

BRKBBA-2004

Georgina Schaefer

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don't forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a 'No Smoking' venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Session Objectives

- There are no major pre-requisites for this session beyond a basic understanding of Layer 2 protocols, IP and Security
- After completing this session you should be able to:
  - Understand the major threats at Layer 2
  - Understand the features that Cisco supports to counter these threats
  - Understand some of the capabilities of widely available attack tools
  - Know the best practices to lock down your infrastructure

Agenda

- Carrier Ethernet Security Landscape
- Layer 2 Attack Landscape
  - Subscriber Threats
  - Switch Threats
  - Infrastructure Threats
- Summary

Carrier Ethernet Security Landscape

Carrier Ethernet Challenges

- Network Convergence
  - Access networks that leverage Ethernet
  - Legacy Services (TDM, FR, ATM…)
  - Broadband and 3-Play
- Network Availability
  - Expectation of similar availability to SDH/SONET for some services
- New Services
  - New franchises with traditionally high SLA expectations – IPTV, VOD, Telephony…
- Traditional circuit-based access networks did not suffer from the unique security threats faced by Ethernet access networks
- Malicious attacks are becoming more sophisticated – a high-speed network is a very desirable target!

Ethernet Access Security Challenges

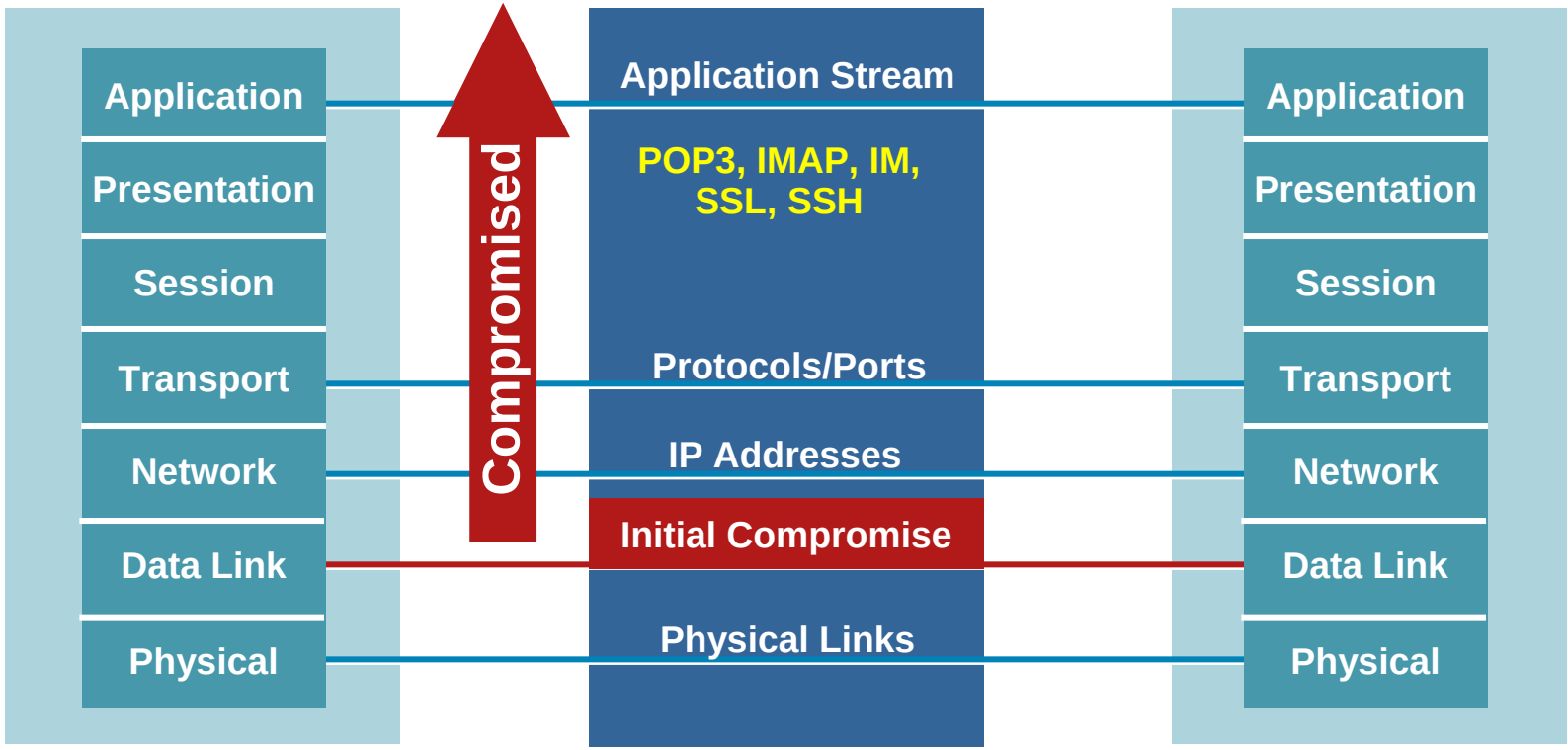
- Service providers must ensure customer isolation on a common “shared” infrastructure
- Most security attacks originate from within the customer's network - not from outside

  The prevalence of botnets results in thousands of remote-controlled hosts capable of Layer 2 and Layer 3 attacks

  First line of attack is to target own subnet
- Publicly available hacker software can enable users to exploit standard Ethernet switch mechanisms without any expert knowledge
- Often the Service Provider’s Carrier Ethernet Access (e.g. ETTH) equipment is located at the Customer Premise in unsecured locations

Layer 2 Security Issues Affect Higher Layers

- OSI Was Built to Allow Different Layers to Work Without the Knowledge of Each Other
- If one layer is hacked, communications are compromised without the other layers being aware of the problem



Potential Security Threats

- Security attacks generally fall into one of the following categories:

  Intrusion: The attacker attempts to gain unauthorized access to network resources, including traffic from other customers

  Common Examples:

  Rogue DHCP server

  IP & MAC address spoofing

  ARP spoofing (Man-in-the-Middle) Attack

  Denial of Service (DoS): The attacker attempts to disrupt normal network and service operations

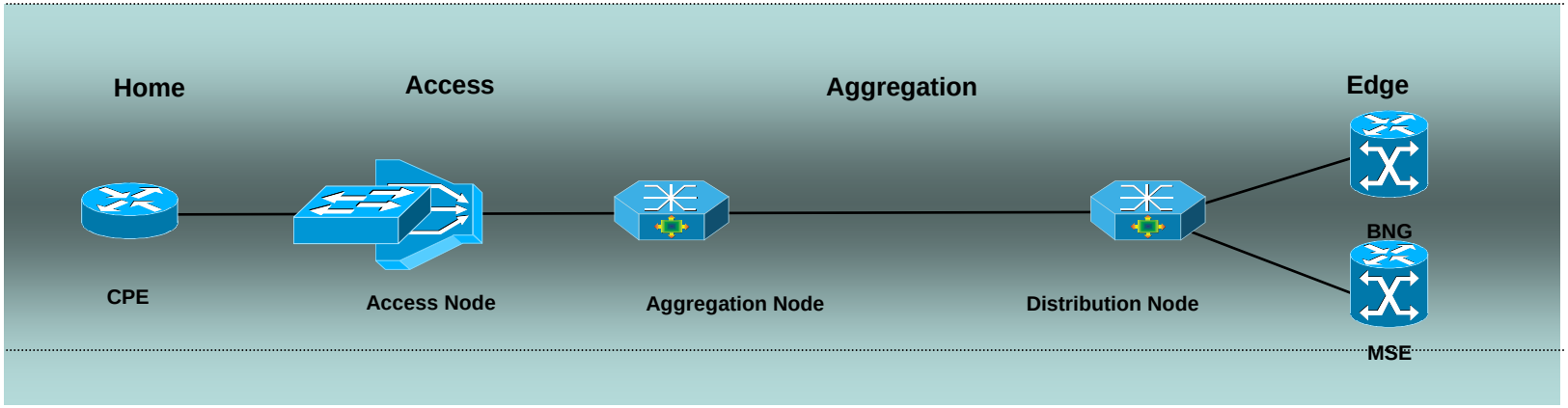
  Common Examples:

  MAC attacks (CAM table overflow)

  Broadcast storms

  L2 PDU storm (STP, LACP, PAgP, etc..)

Carrier Ethernet Security: A Trust Model



- CPE – Not trusted, but should be utilised for trust

  The CPE Provides invaluable security opportunities

  Outbound service control, connection admission, QoS policy enforcement

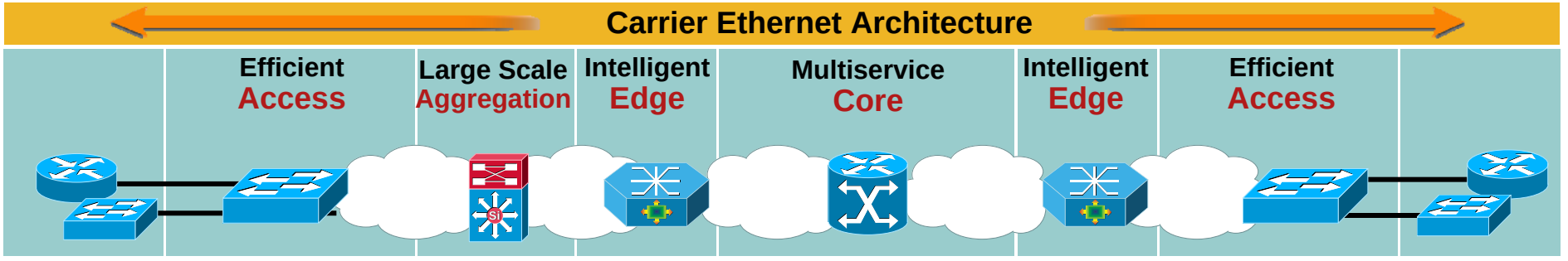
- DSLAM/Switch – Trusted
- Aggregation and Distribution Nodes – Trusted

  Aggregation and Distribution Nodes should have a set of features that "duplicate" the efforts on the CPE for common security mechanisms, but at a higher scale.

  They should also provide strict separation between services including resource partitioning

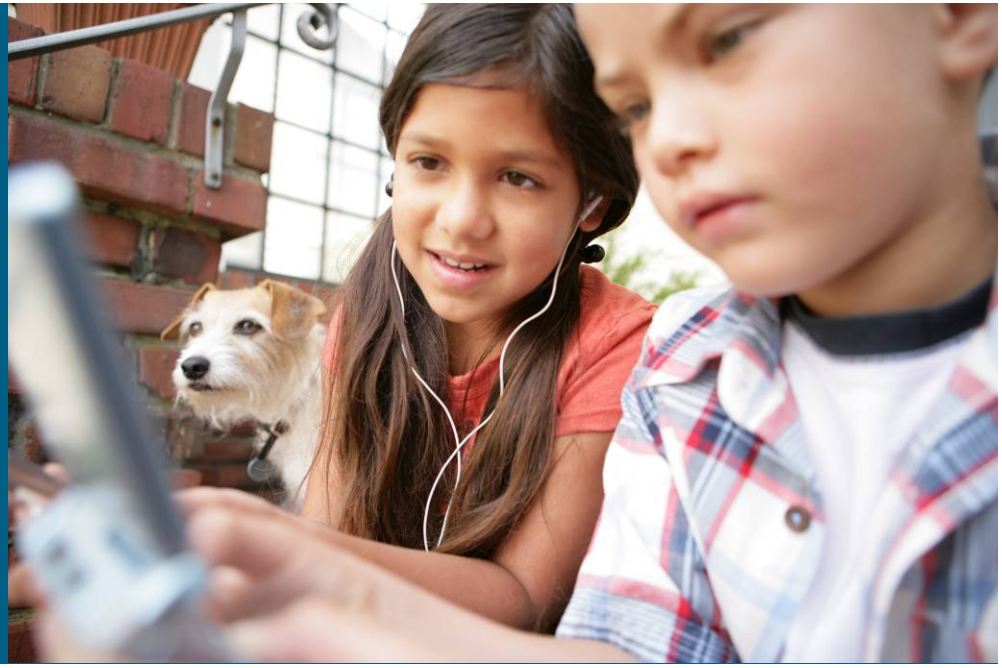
Where do we apply security mechanisms?

In Carrier Ethernet Deployments, the Carrier Ethernet Access (U-PE) device is often responsible to provide Key Security Features as a first line of defense:



Access	Aggregation	Edge	Core
Admission control, Security Policy Enforcement, Classification, Policing and Marking, Queuing and scheduling	Traffic aggregation, VPLS, H-VPLS, Congestion management, L2 wholesale handoff, Service insertion	MPLS, L2TPv3, VPWS, VPLS, L3VPN, Internet Access, Service Gateway, Value Added Services (Security, Voice,…)	Fast Packet Forwarding (IP/MPLS), Sophisticated Traffic Engineering and Congestion management

Layer 2 Attack Landscape

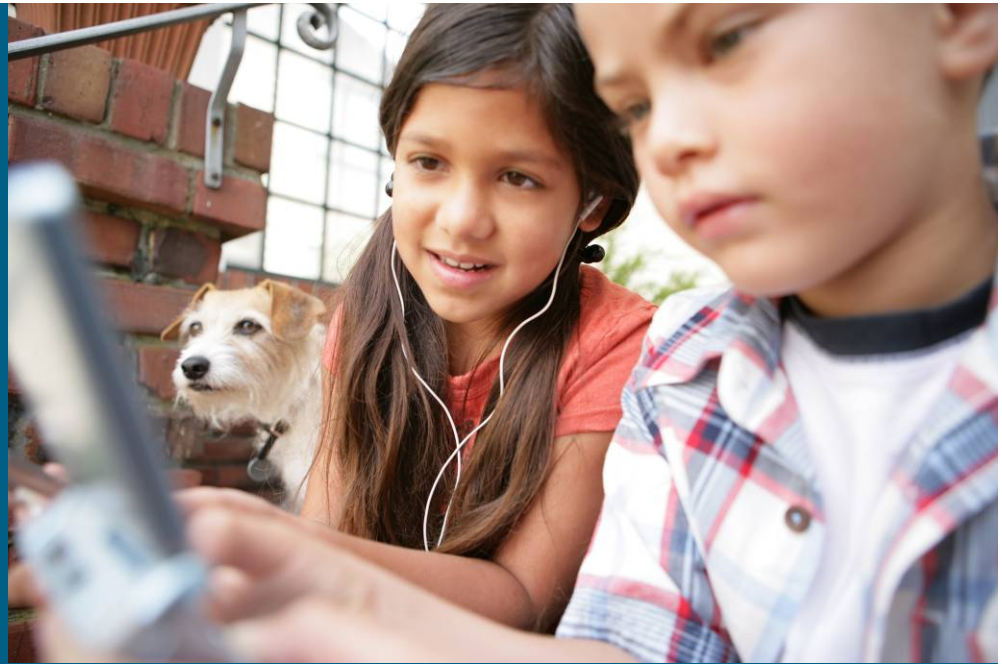


Ethernet Access Security Threats

- Attack targets can be divided into three main categories:

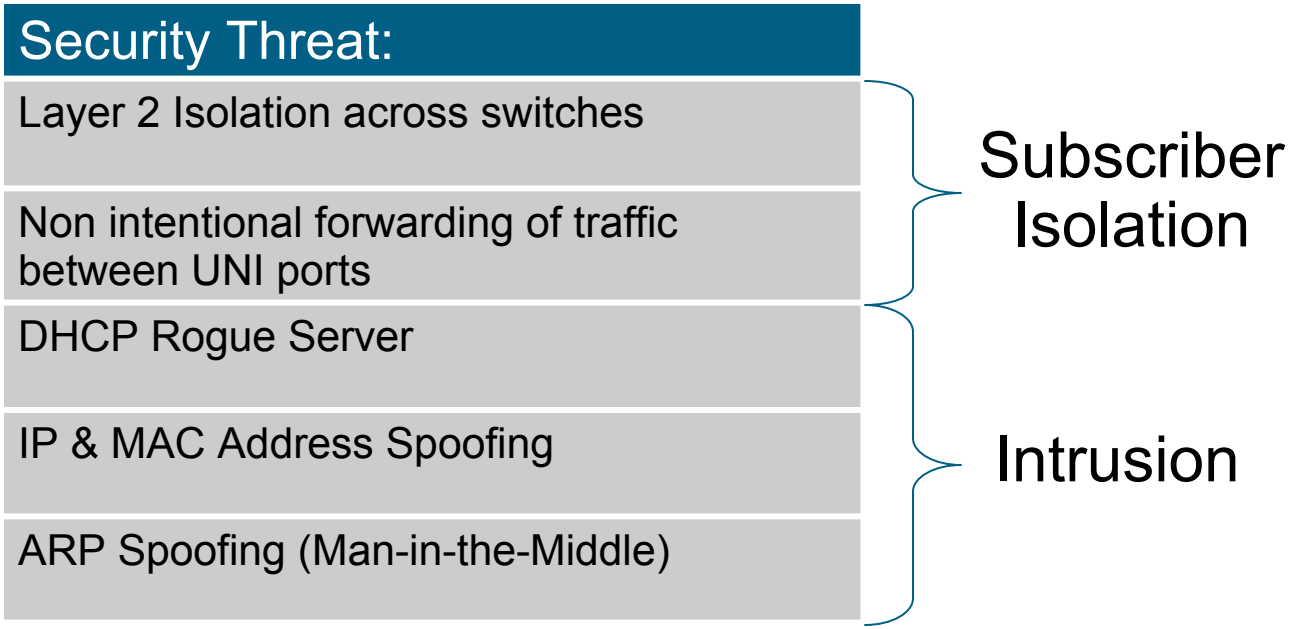
Subscribers	Switches	Infrastructure
Layer 2 service isolation across switches	L2 Control Protocol Attack (STP, CDP, VTP, etc…)	Man-in-the-Middle attacks on critical management traffic
Non intentional forwarding of traffic between UNI ports	MAC Flooding / Overflow	Unauthenticated access to the switch configuration file
DHCP Rogue Server	MAC Flooding / Overflow	Unconfigured Ports providing network access
IP & MAC Address Spoofing	Unicast, multicast, or broadcast storms	Unauthorized network access, junk traffic
ARP Spoofing (Man-in-the-Middle)	Infected users flooding the network / Malicious users attacking the Priority traffic queue	Unauthenticated network access by client devices

Layer 2 Attack Landscape
Subscriber Threats

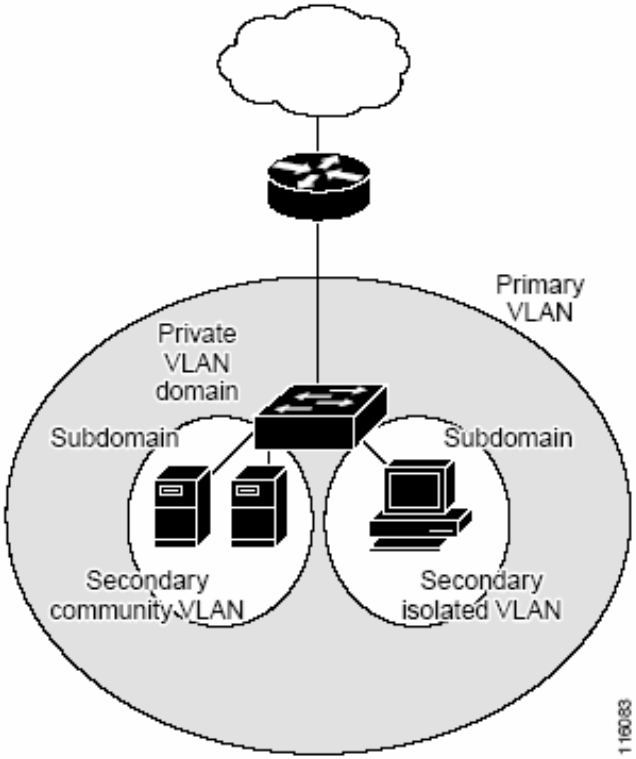


Subscriber Security

- One of the biggest concerns in using a shared Ethernet Access device for multiple customers is how to prevent one customer from affecting another customer



Subscriber Security
Private VLAN



What It Does:

- Private VLANs provide Layer 2 isolation between ports within a common segment
- Two types of subscriber VLANs:
  - Isolated VLANs - Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level. There is no exchange of unicast, broadcast, or multicast traffic with any other switch port that is also an isolated port
  - Community VLANs - Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level

Benefit:

- Offers Layer 2 service separation across switches

Subscriber Security
UNI Default No Local Switching

Configuration example:

```
(config)vlan 10
(config-vlan) uni-vlan isolated
(config-vlan) vlan 20
(config-vlan) uni-vlan community
```

Show command: show vlan uni-vlan <type>

```
Switch#sh vlan uni-vlan type

Vlan Type
---- -----------------
10   UNI isolated
20   UNI community
```

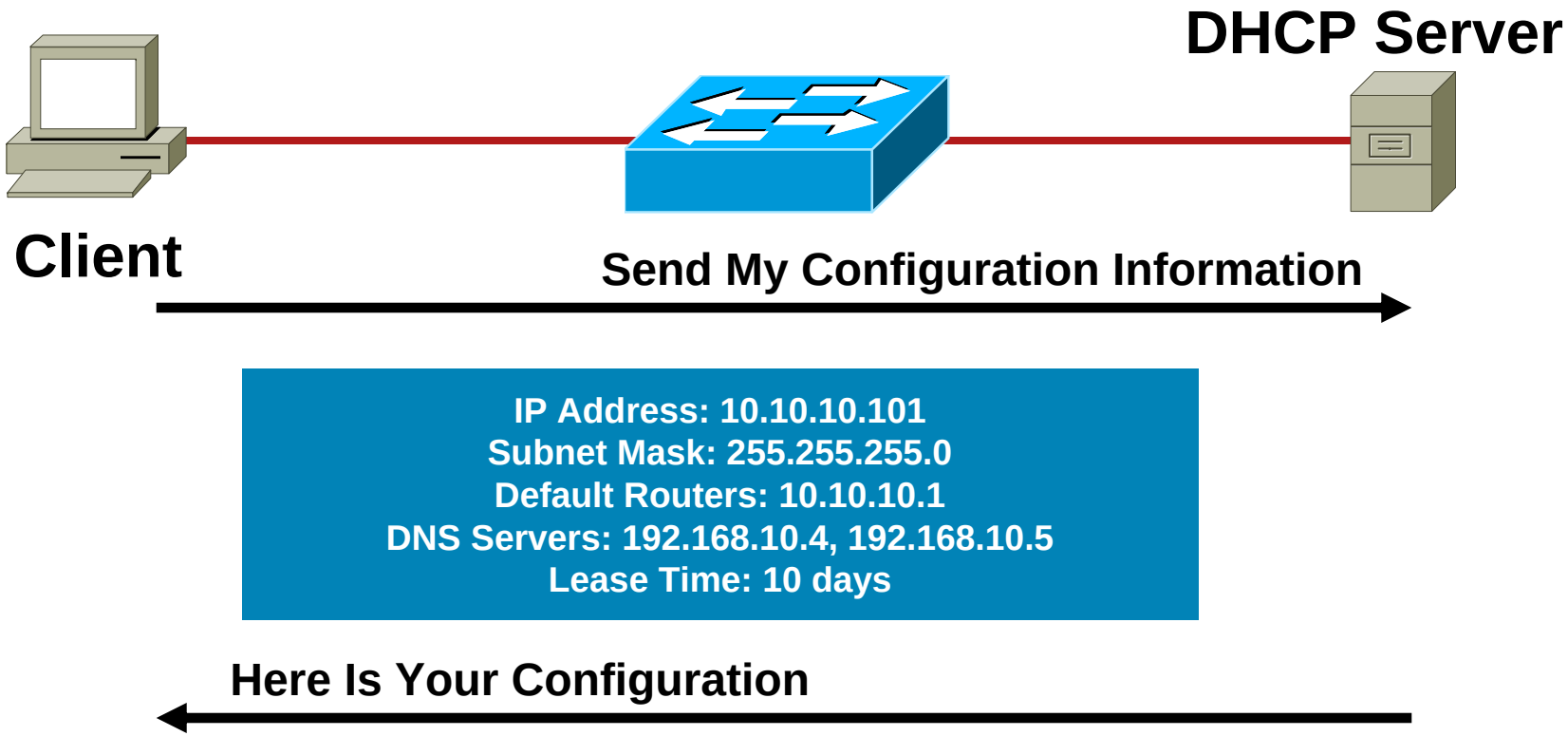
What It Does:

- Traffic is not switched between UNI ports (even if in the same VLAN) unless specifically permitted
- UNI port default behavior

Benefit:

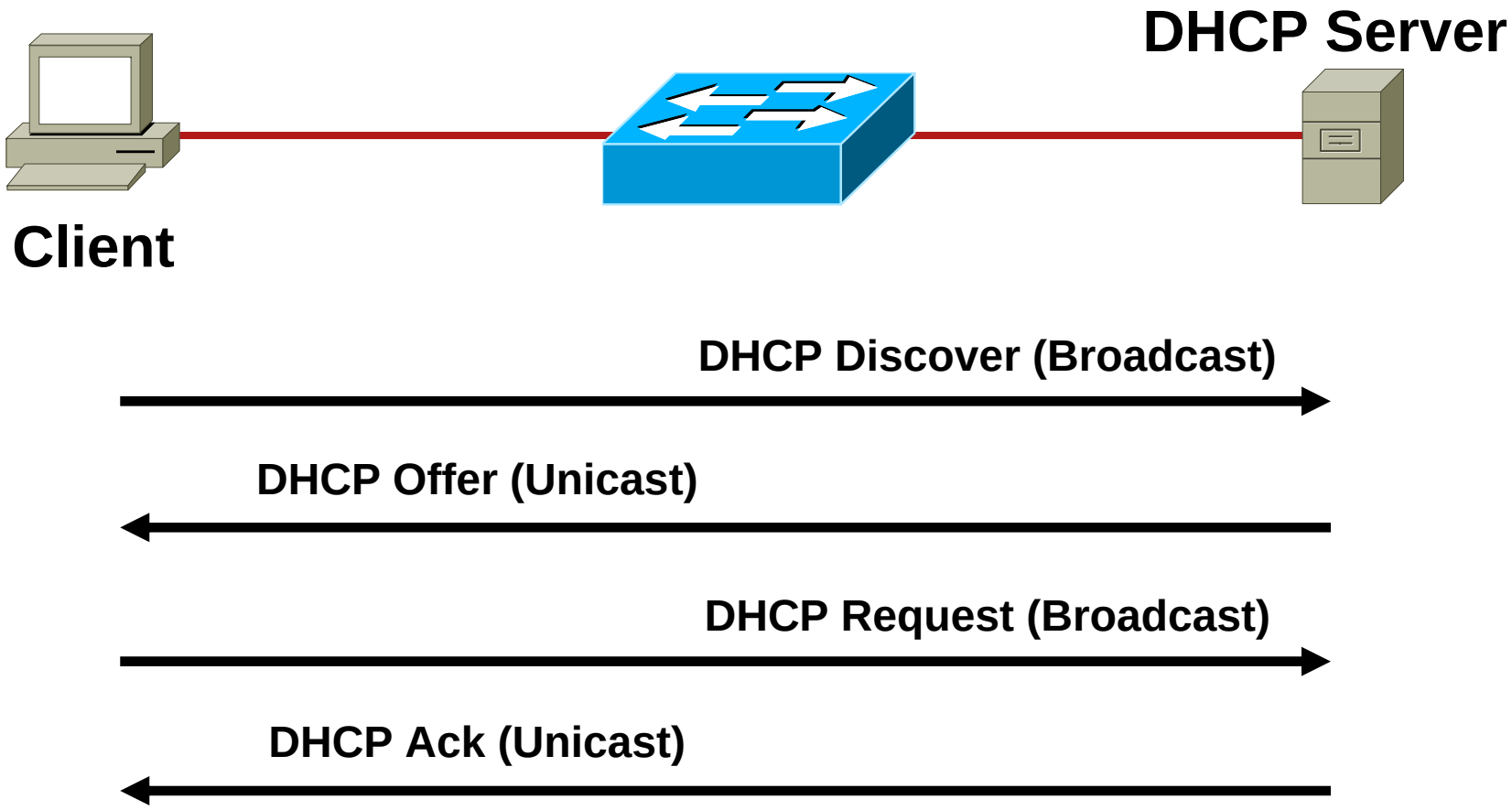
- Provides subscriber isolation, with circuit-like behavior

Subscriber Security
DHCP Rogue Server



- 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

Subscriber Security
DHCP – High Level Overview



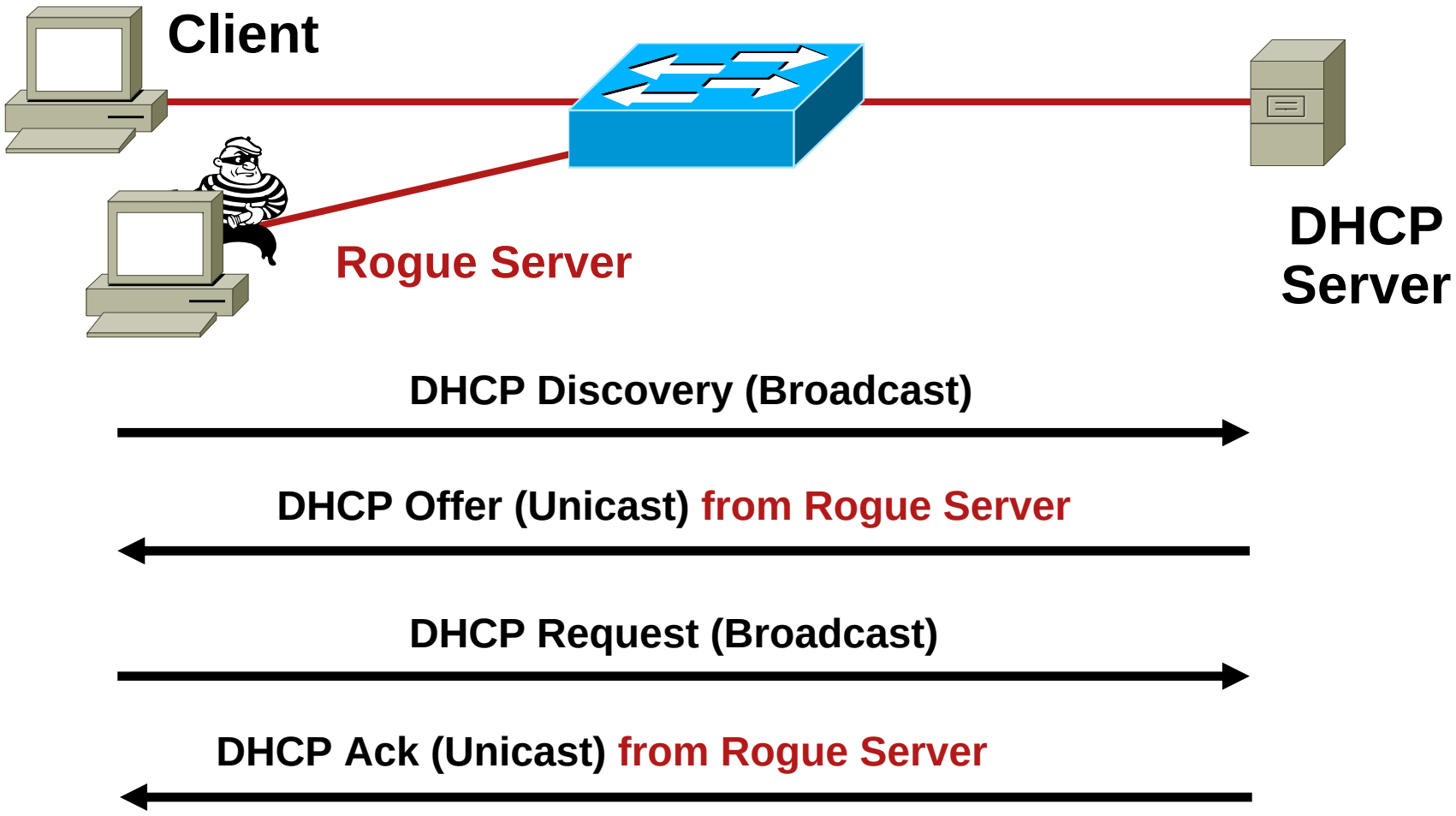
- DHCP defined by RFC 2131

Subscriber Security
DHCP – Low Level

DHCP Request/Reply Types

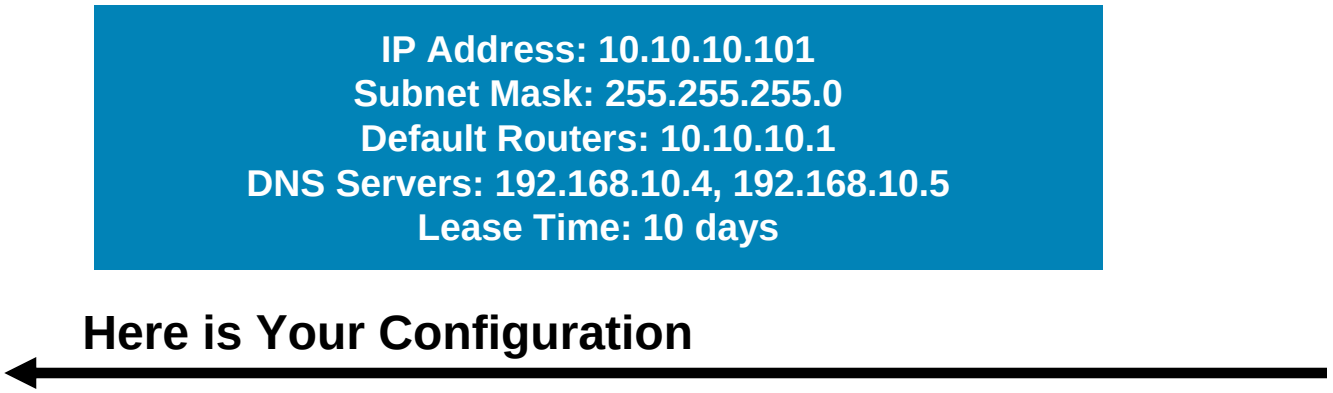
Message	Use
DHCPDISCOVER	Client Broadcast to Locate Available Servers
DHCPOFFER	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPREQUEST	Client Message to Servers Either (A) Requesting Offered Parameters from One Server and Implicitly Declining Offers from All Others, (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

Rogue DHCP Server Attack



Rogue DHCP Server Attack

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



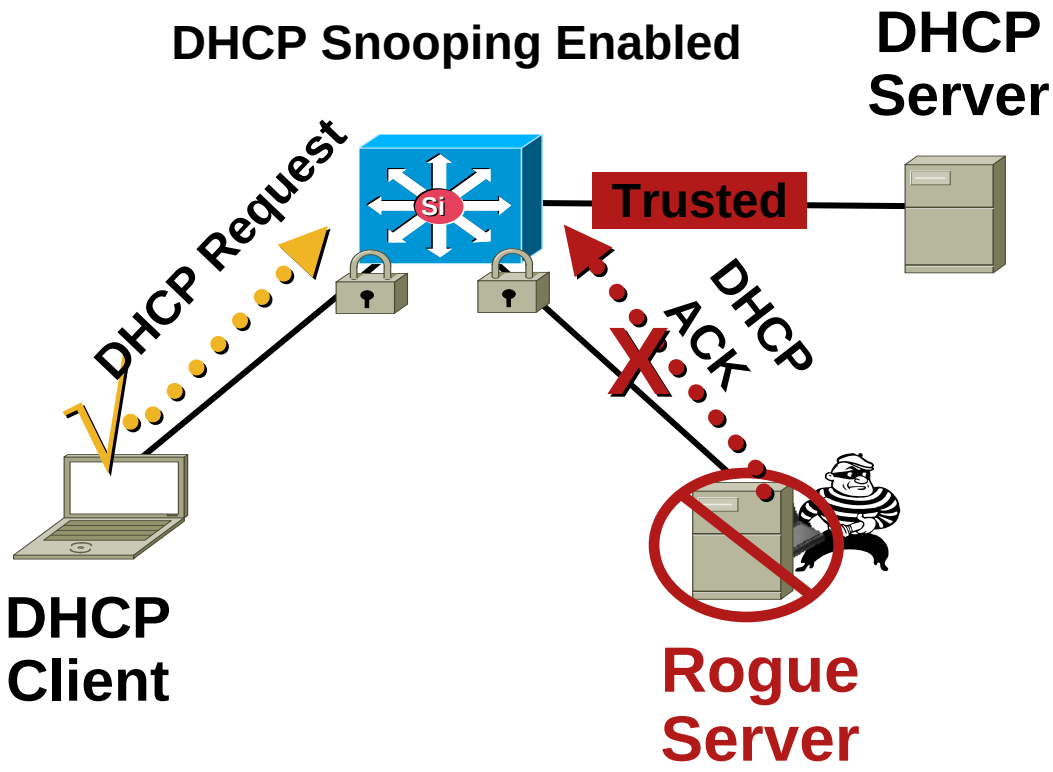
- What is the threat associated with incorrect information?

  Wrong Default Gateway - Attacker is the gateway

  Wrong DNS server - Attacker is DNS server -> DNS poisoning

  Wrong IP Address - Attacker performs attacks with spoofed IP

Countermeasure – DHCP Rogue Server DHCP Snooping



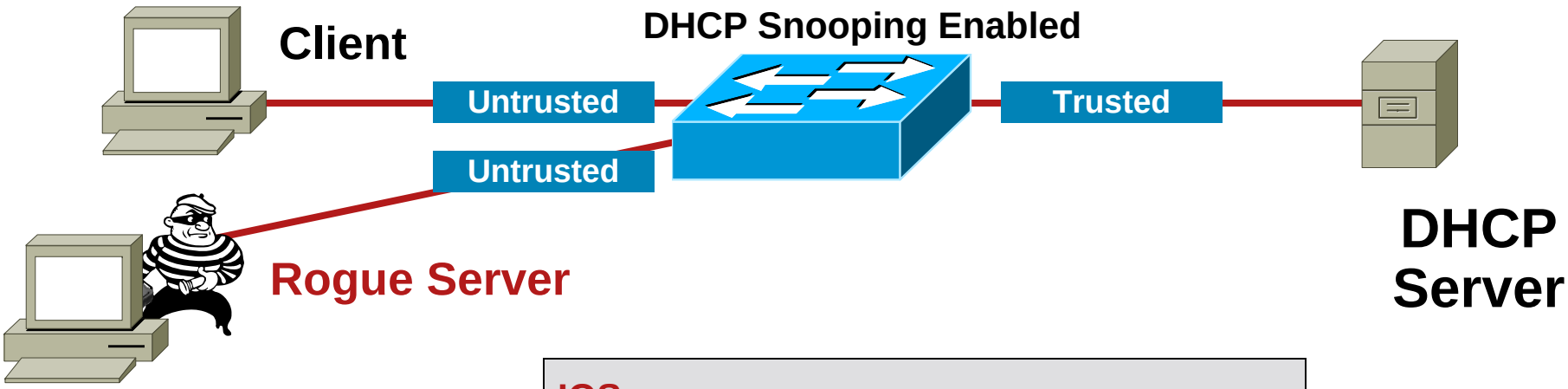
What It Does:

- Switch forwards only DHCP requests from untrusted access ports, drops all other types of DHCP traffic
- Allows only designated DHCP ports or uplink ports trusted to relay DHCP Messages
- Builds a DHCP binding table containing client IP address, client MAC address, port, VLAN

Benefit:

- Eliminates rogue devices from behaving as the DHCP server

Countermeasure – DHCP Rogue 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
```

DHCP Snooping Trusted Server

Interface Commands

```
ip dhcp snooping trust
```

- By default all ports in the VLAN are untrusted

Countermeasure – DHCP Rogue 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
```

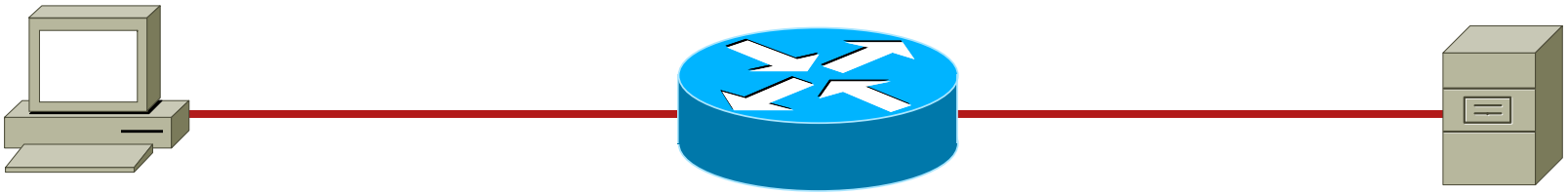
- Table is built by “Snooping” the DHCP reply to the client
- Entries stay in table until DHCP lease time expires
- In the event of switch failure, the DHCP snooping binding table can be written to bootflash, ftp, rcp, slot0, and tftp

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

Countermeasure – DHCP Rogue Server VLAN ACLs

- If there are switches in the network that will not support DHCP snooping, you can configure VLAN ACL's to allow UDP Port 68 only on trusted links

```
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
```



Router 192.0.2.1

DHCP Server 10.1.1.99

Subscriber Security 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 – theft of service

- IP spoofing

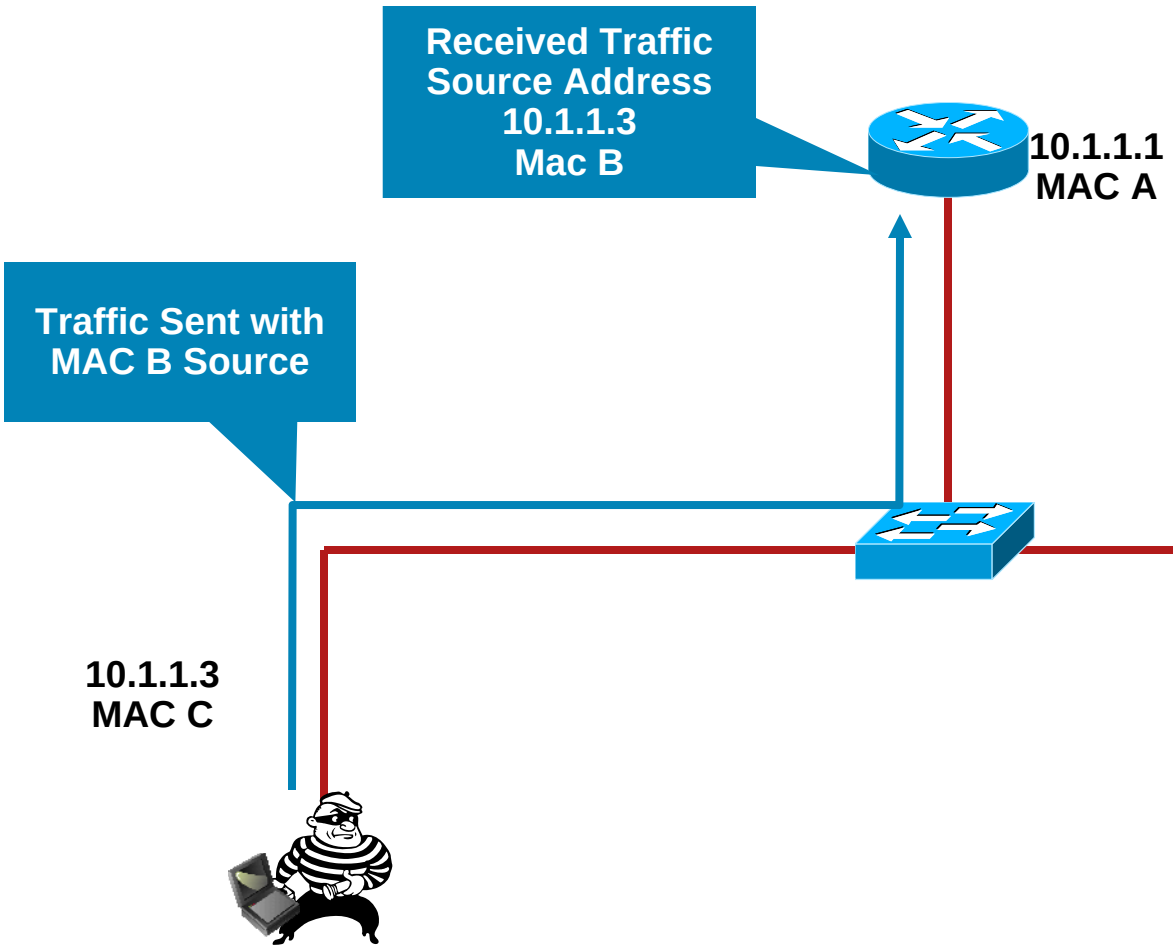
  Ping of death

  ICMP unreachable storm

  SYN flood

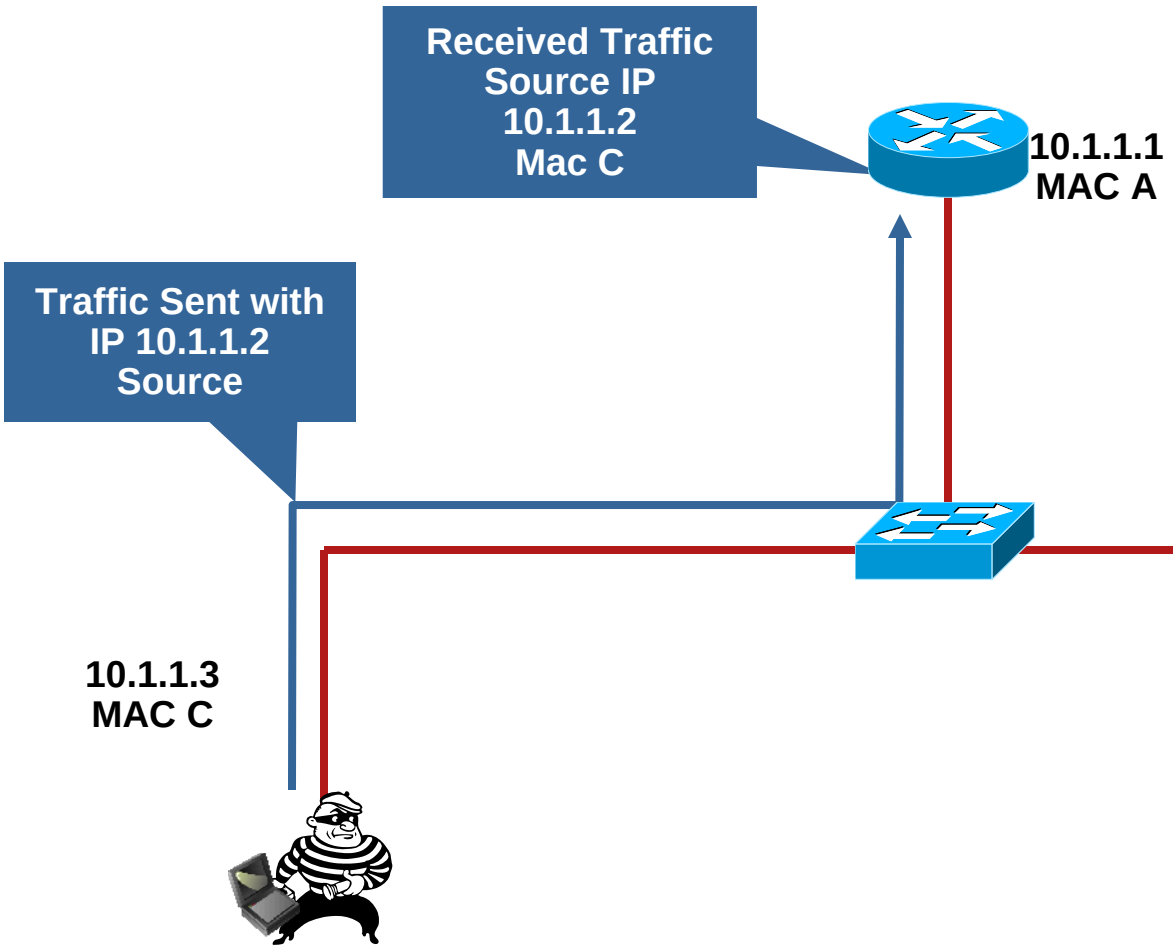
  Trusted IP addresses can be spoofed

Spoofing Attack: MAC



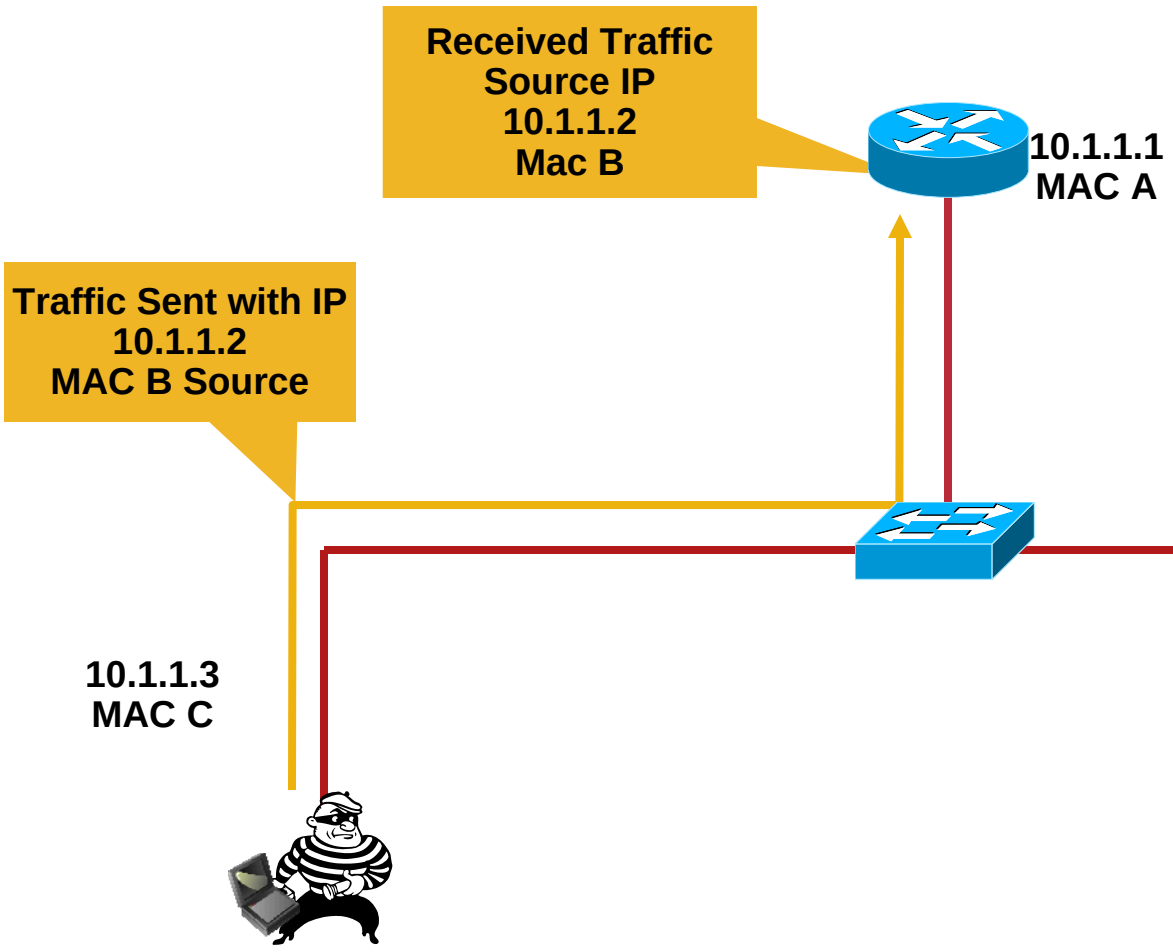
- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

Spoofing Attack: IP



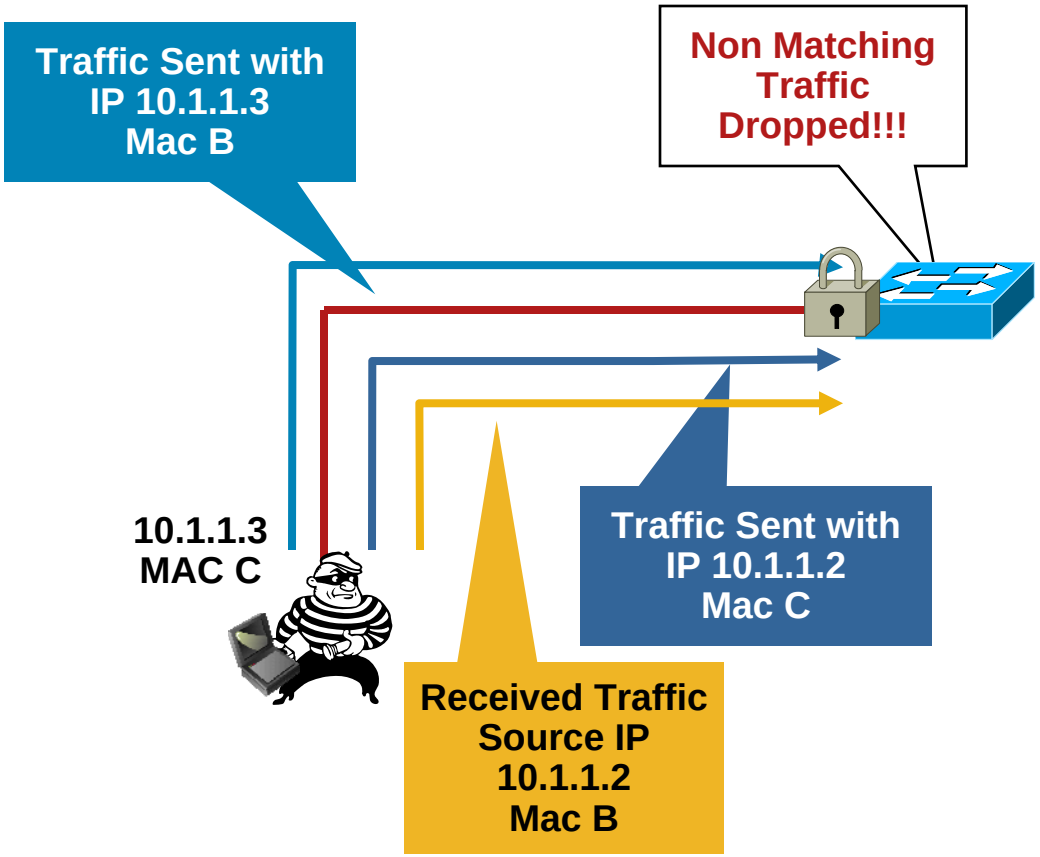
- Attacker sends packets with the incorrect source IP Address
- Whatever device the packet is sent to will never reply to the attacker

Spoofing Attack: IP/MAC



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

Countermeasure to Spoofing Attacks: IP Source Guard



- Binds client IP address, client MAC address, port, VLAN number

What It Does:

- Uses the DHCP snooping binding table information
- If a subscriber is assigned an IP address via DHCP, the switch can enforce that assignment by blocking any packets sent from the client's port claiming to be from a different IP addresses
- This is accomplished by enabling DHCP snooping and IP source guard

Benefit:

- Prevents a subscriber (or malicious user) from using an IP Address or MAC Address not assigned to them

Using IP Source Guard

- DHCP Snooping must be configured first so the binding table is built
- IP Source Guard is configured by port
- 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

  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
```

Configuring IP Source Guard in IOS

IP/MAC Checking Only (Opt 82)

Global Commands

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

Interface Commands

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

IP Checking Only (no Opt 82)

Global Commands

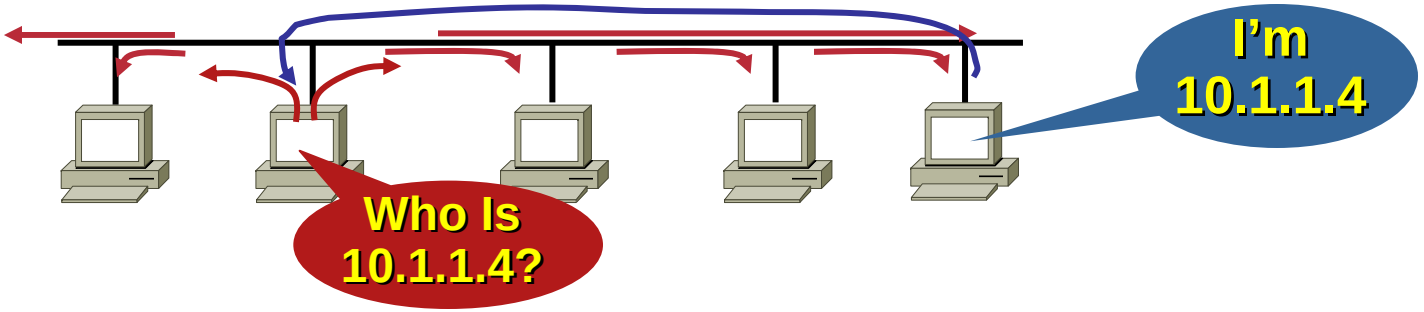
```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

Interface Commands

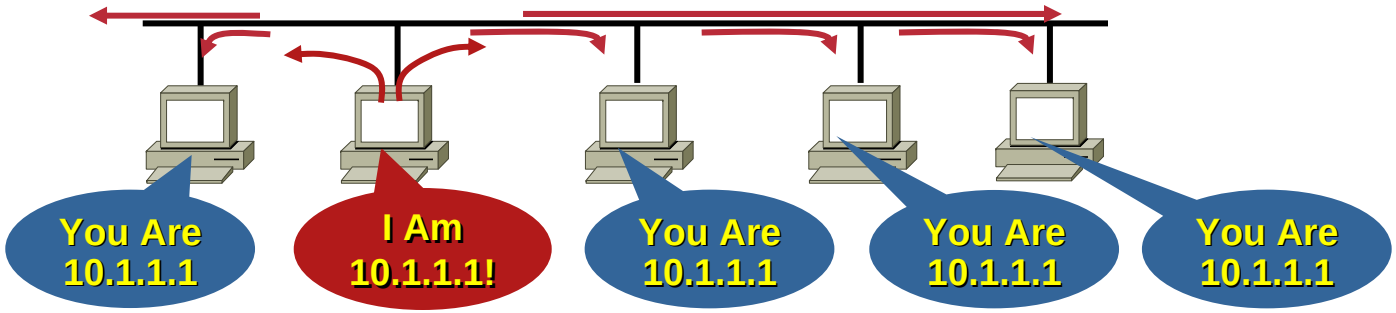
```
ip verify source vlan dhcp-snooping
```

Subscriber Security
ARP Spoofing

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

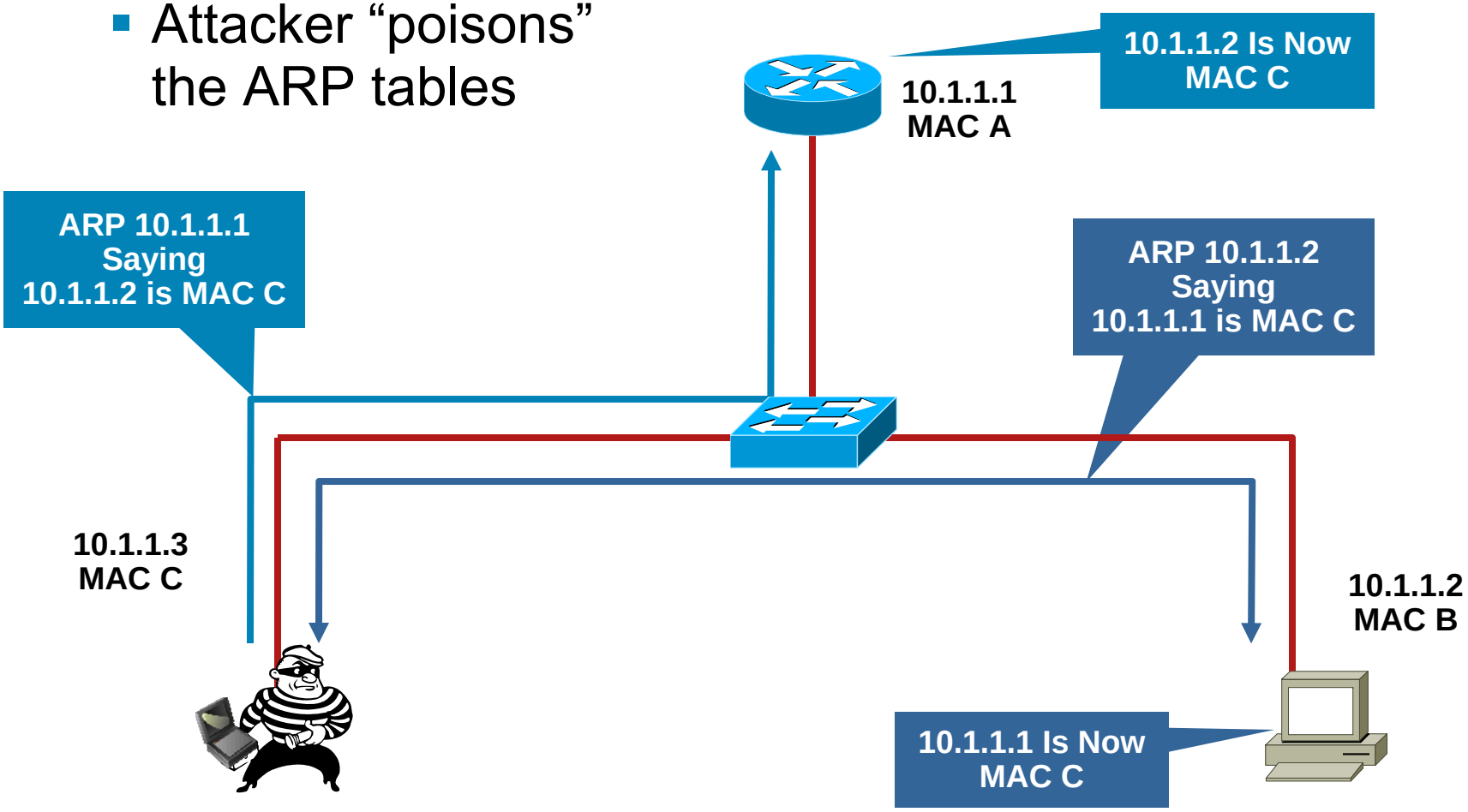


- According to the ARP RFC, a client is allowed to send an unsolicited ARP reply; this is called a gratuitous ARP; other hosts on the same subnet can store this information in their ARP tables



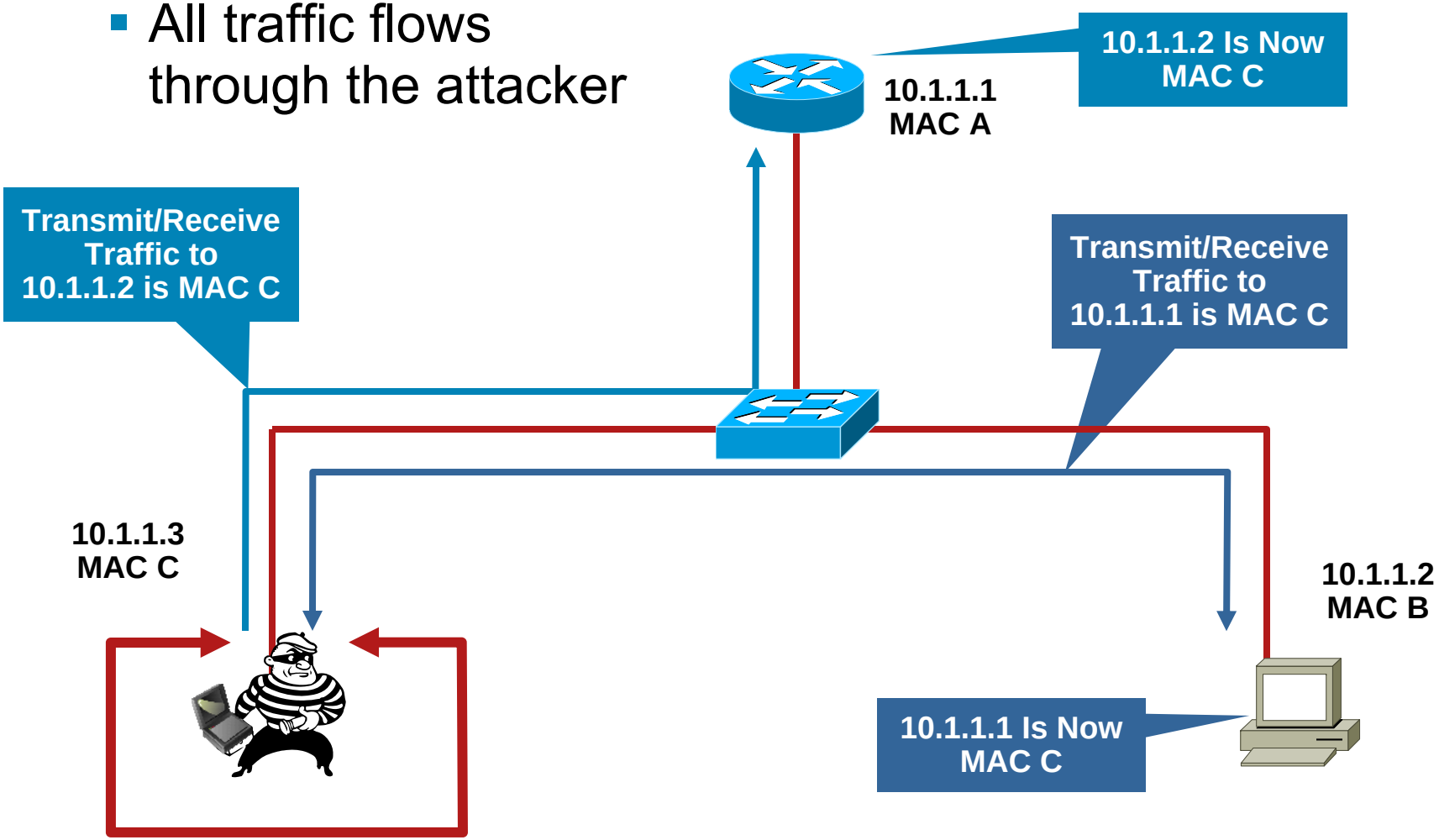
ARP Attack in Action

- Attacker “poisons” the ARP tables



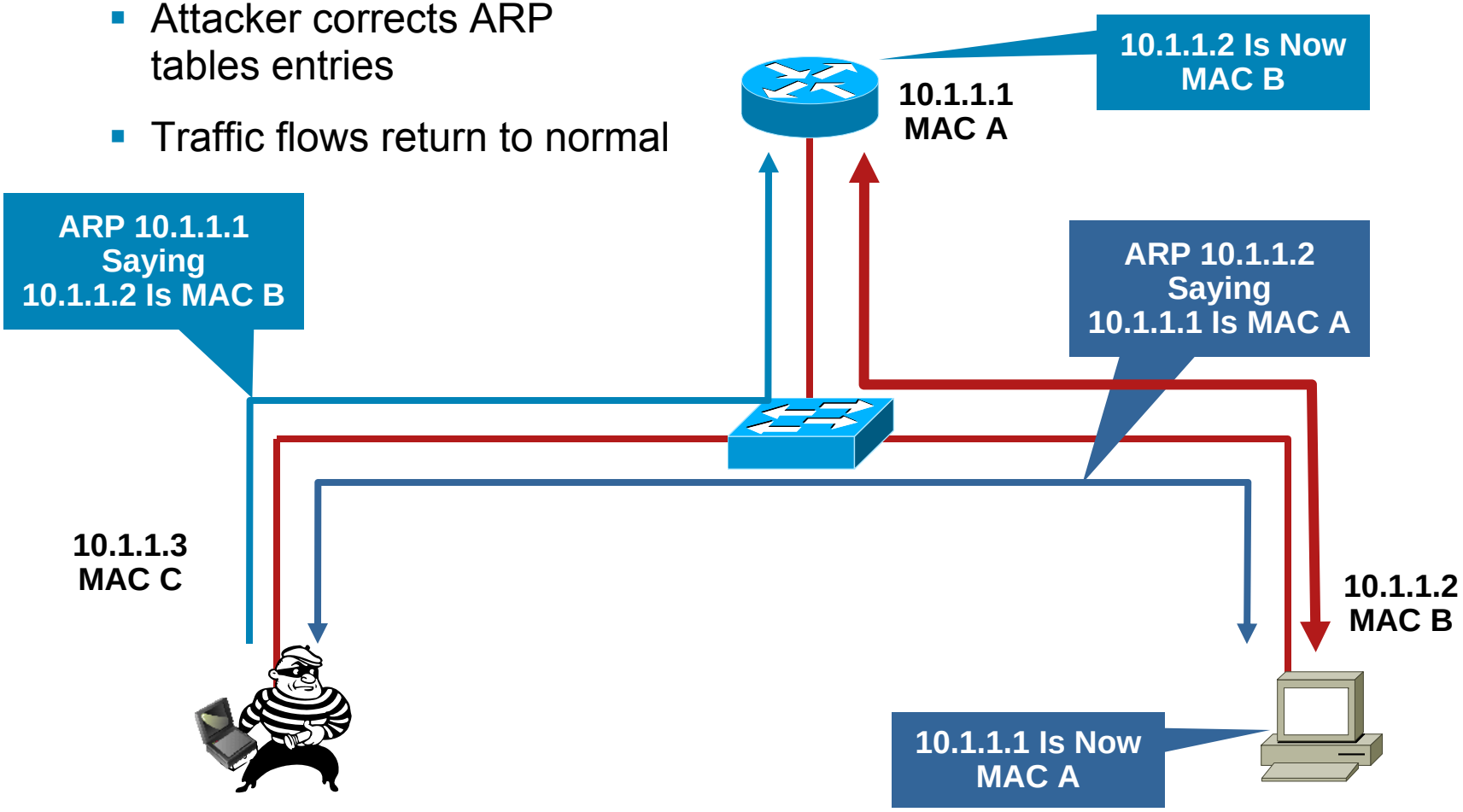
ARP Attack in Action

- All traffic flows through the attacker



ARP Attack Clean Up

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



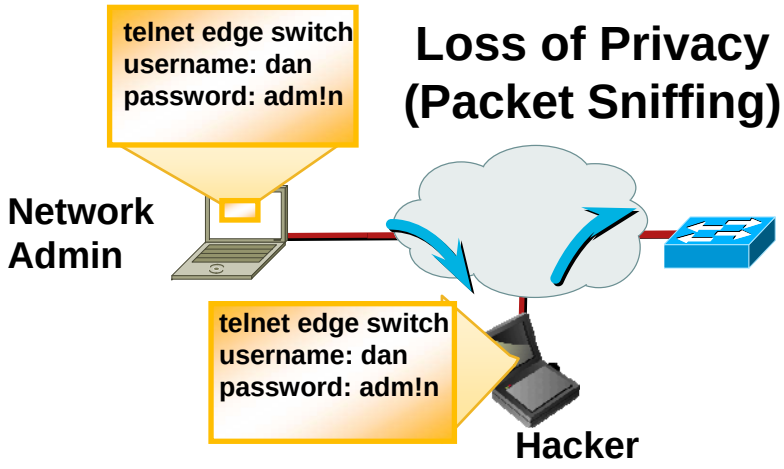
ARP Attack Tools

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

Dsniff www.monkey.org/~dugsong/dsniff
Ettercap http://ettercap.sourceforge.net/
Cain&Abel http://www.oxid.it
Yersinia http://www.yersinia.net

- 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.

Subscriber Security
Telnet Session Attack (Man-in-the-Middle)

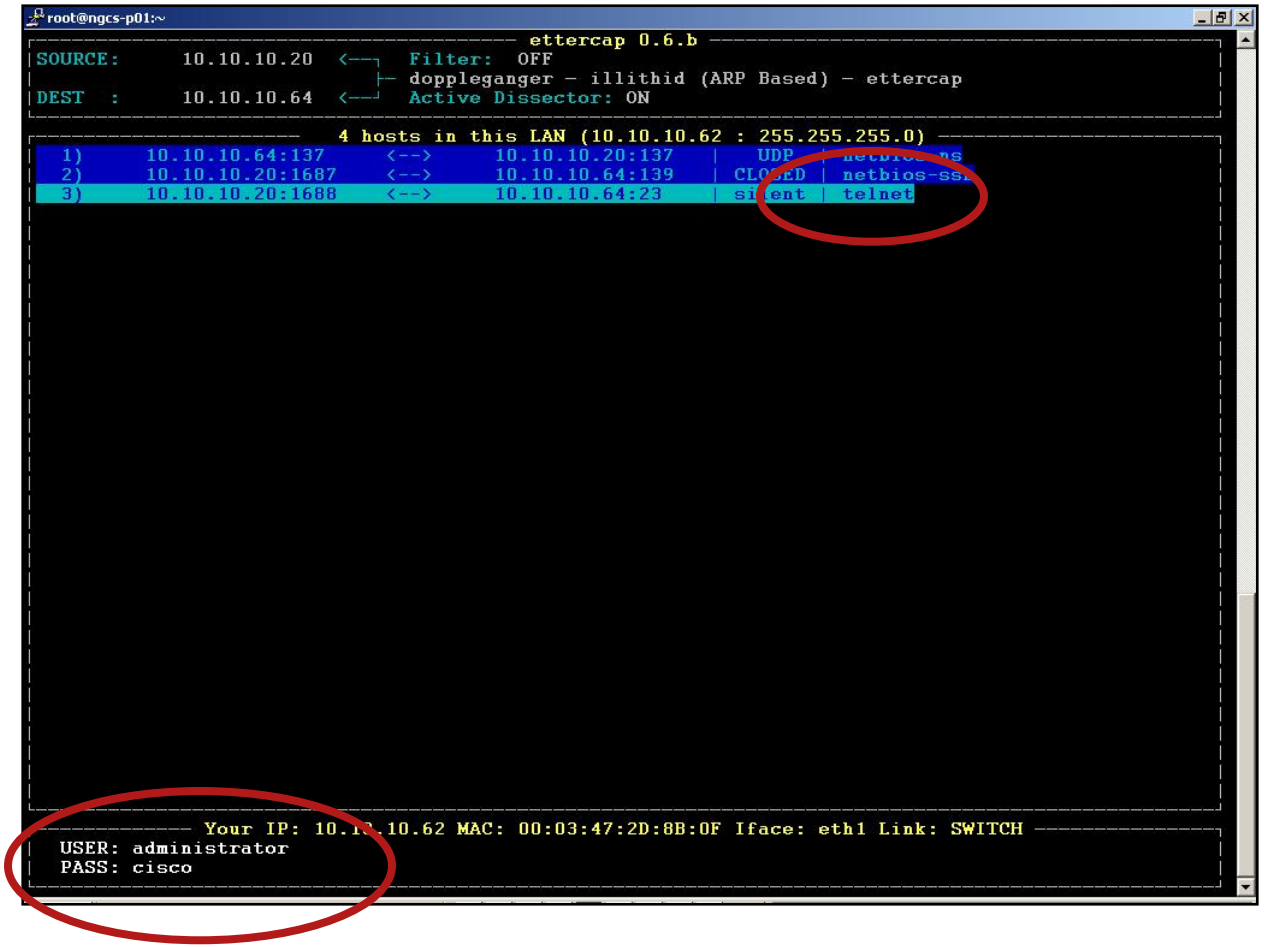


Problem:

- A malicious user can intercept administrative information ("Man-in-the-Middle" attack) in order to hack into or attack a network switch
- Can intercept Administrative Passwords and Network Configuration Information

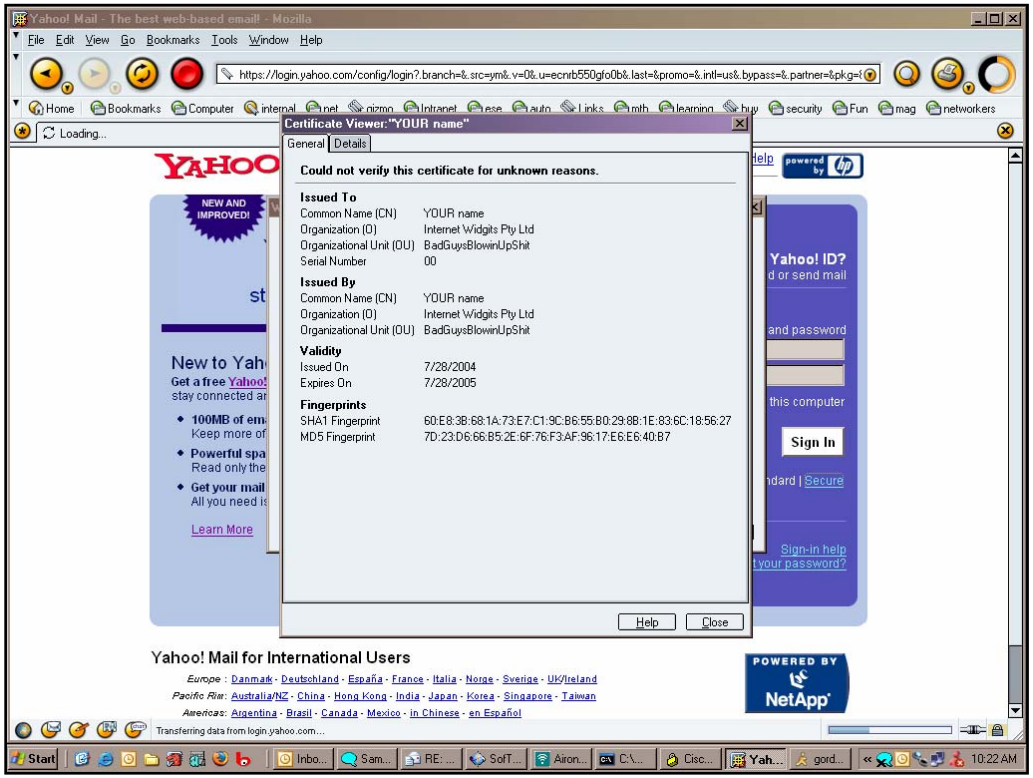
ARP Attack Tools:Telnet

- Ettercap in action
- Runs in Window, Linux, Mac
- Decodes passwords on the fly
- This example, telnet username/ password is captured

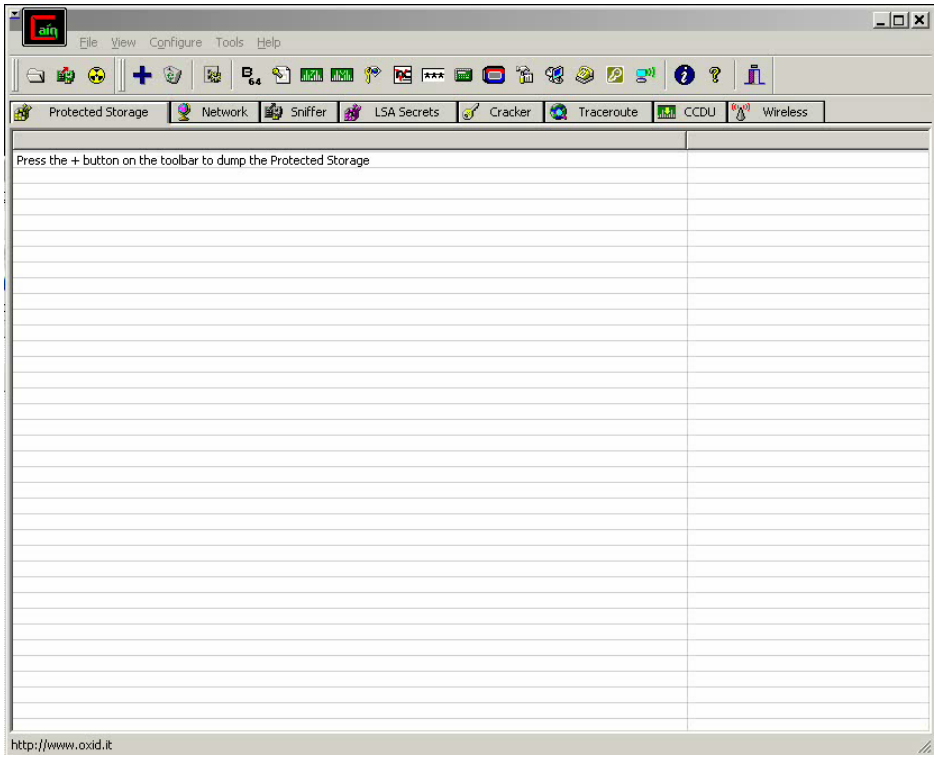


ARP Attack Tools: SSH/SSL

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



Cain Demo



Could Private VLANs help?

- Private VLANs prevent Host-to-Host ARP spoofing attacks

  Unicast ARP Replies cannot be sent between hosts

- DOES NOT stop Host-to-Default Gateway attacks (neither do IP ACLs or IP Proxy ARP)

- ARP entries learned on Layer 3 private VLAN interfaces are sticky ARP entries. For security reasons, ARP entries NEVER age out.

  Connecting new equipment with the same IP address generates a message and the ARP entry is not created

  Requires manual intervention

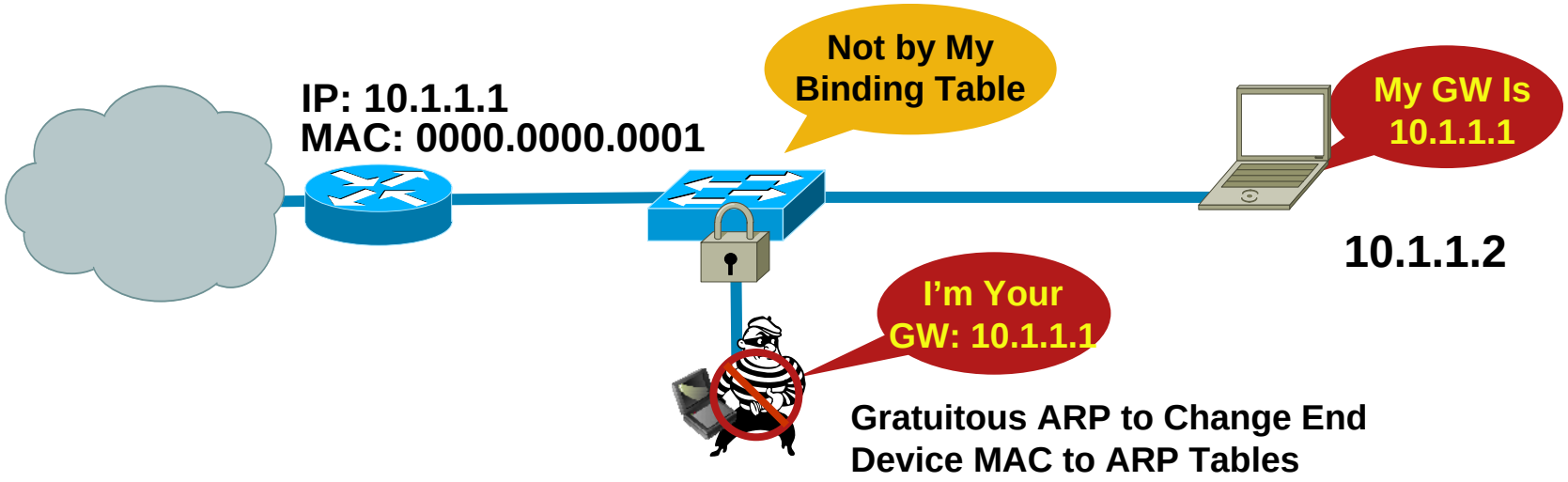
Countermeasure to ARP Attacks: Dynamic ARP Inspection

What It Does:

- Inspects only ARP packets - discards ARP packets with invalid IP-to-MAC address bindings
- Uses the DHCP binding table that was dynamically populated by DHCP Snooping

Benefit:

Effectively stops “man-in-the-middle” attacks and “ARP Spoofing”



Using Dynamic ARP Inspection

- DHCP Snooping must first be configured so the binding table is built
- Wait until all devices have new leases before turning on Dynamic ARP Inspection
- Entries stay in table until the lease runs out
- Dynamic ARP Inspection is configured by VLAN
- You can trust an interface like DHCP Snooping
- Need to rate-limit ARP packets, otherwise Dynamic ARP Inspection turns into a DoS target!

Configuring Dynamic ARP Inspection

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)
```

Dynamic ARP Inspection with 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
```

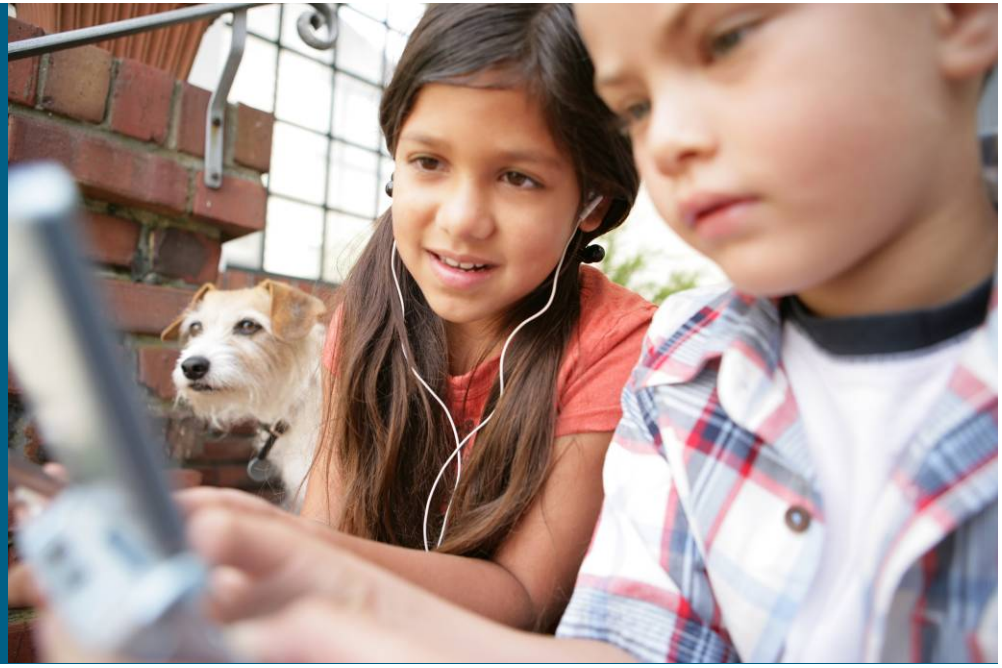
- Show static and dynamic entries in the DHCP snooping binding table is different

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

Subscriber Security Summary

Security Threat:	Solution
Layer 2 Isolation across switches	Private VLANs
Non intentional forwarding of traffic between UNI ports	UNI Default No Local Switching
DHCP Rogue Server	DHCP Snooping
IP & MAC Address Spoofing	Source Guard + DHCP Snooping
ARP Spoofing (Man-in-the-Middle)	Dynamic ARP Inspection + DHCP Snooping

Layer 2 Attack Landscape
Switch Threats



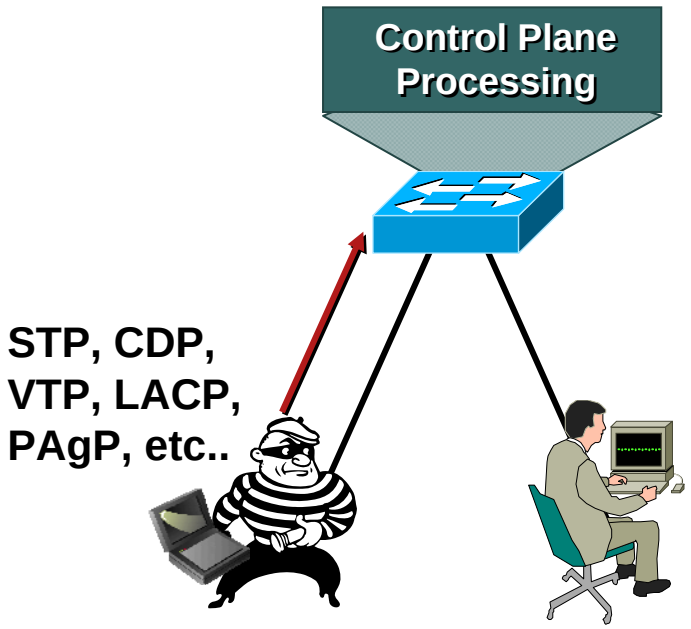
Switch Security

- Security Threats often target the infrastructure itself in order to slow down or halt operation of the device under attack
- Denial-of-Service attacks and flooding attacks are most common

Security Concern:
L2 Control Protocol Attack (STP, LACP, PAgP, CDP, VTP, etc…)
MAC Flooding / Overflow
DHCP Resource Starvation
Unicast, multicast, or broadcast storms
Infected users flooding the network / Malicious users attacking the Priority traffic queue

Denial of Service

Switch Security
Layer 2 PDU Storm Attack



Problem:

- The attacker sends a large amount of Layer 2 Protocol Data Units (PDUs)
- Targets the Layer 2 control plane of the network element
- The performance and operation of the network element can be compromised
- Note: The handling of the Layer 2 protocols will vary by service type (i.e. EPL vs EVPL/E-LAN)…will discuss details later in the session

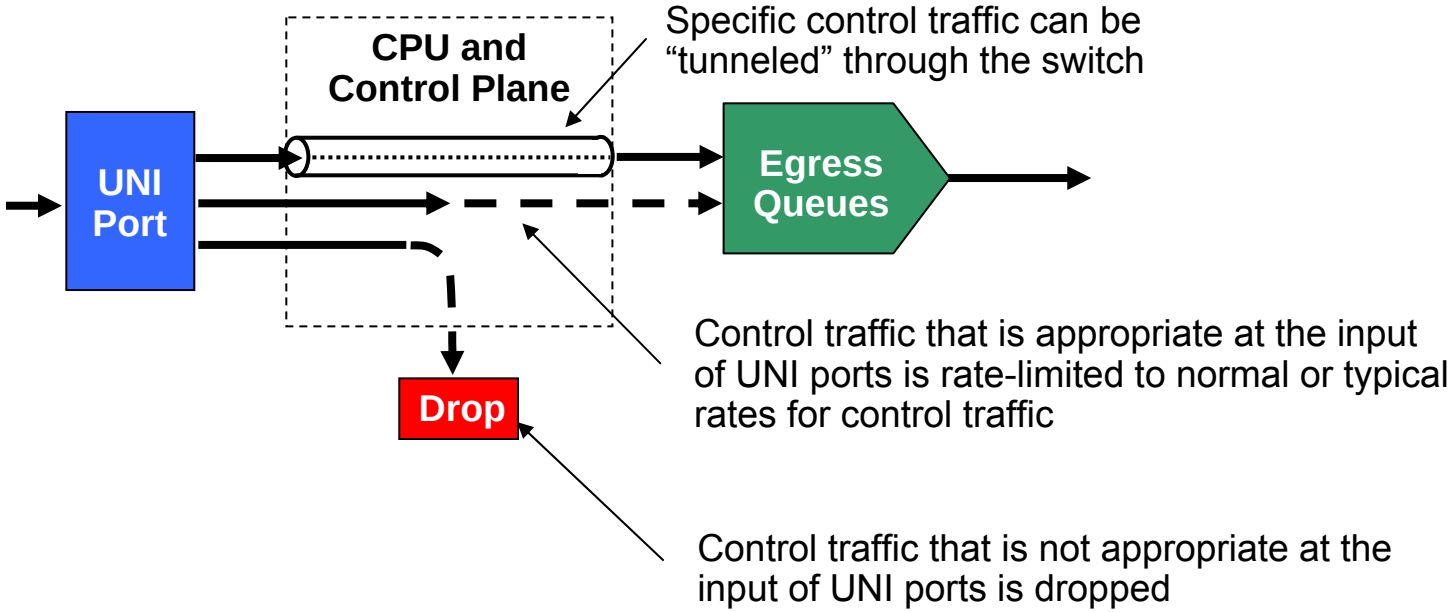
Switch Security
Control Plane Security

What It Does:

- **By default**, control protocols such as STP, VTP, CDP, DTP, PAgP and LACP are dropped at the UNI.
- Under certain other conditions, traffic may be tunneled and/or rate limited

Benefit:

- Provides protection from accidental or malicious L2 PDU DoS attacks which could overload the CPU and degrade system performance and throughput



Switch Security
Control Plane Security

Actions When Protocol is Received on UNI

Protocol	Default Configuration	When Feature is Enabled on UNI Port	L2PT Enabled
STP	Dropped	N/A	Rate Limited
RSVD_STP	Dropped	N/A	N/A
PVST+	Dropped	N/A	Rate Limited
LACP	Dropped	N/A	Rate Limited
PAgP	Dropped	N/A	Rate Limited
802.1X	Dropped	Rate Limited	N/A
CDP	Dropped	N/A	Rate Limited
DTP	Dropped	N/A	N/A
UDLD	Dropped	Rate Limited	Rate Limited
VTP	Dropped	N/A	Rate Limited
CISCO_L2	Dropped	N/A	Rate Limited
KEEPALIVE	Rate Limited	N/A	N/A
SWITCH_MAC	Dropped	N/A	N/A
SWITCH_ROUTER_MAC	Dropped	N/A	N/A
SWITCH_IGMP	Rate Limited	Forwarded	N/A
SWITCH_ L2PT	Dropped	Rate Limited	Rate Limited

Switch Security
Control Plane Security

Display the default policer assignment for interface fa0/1:

switch#**show platform policer cpu interface fa0/1**

Policers assigned for CPU protection

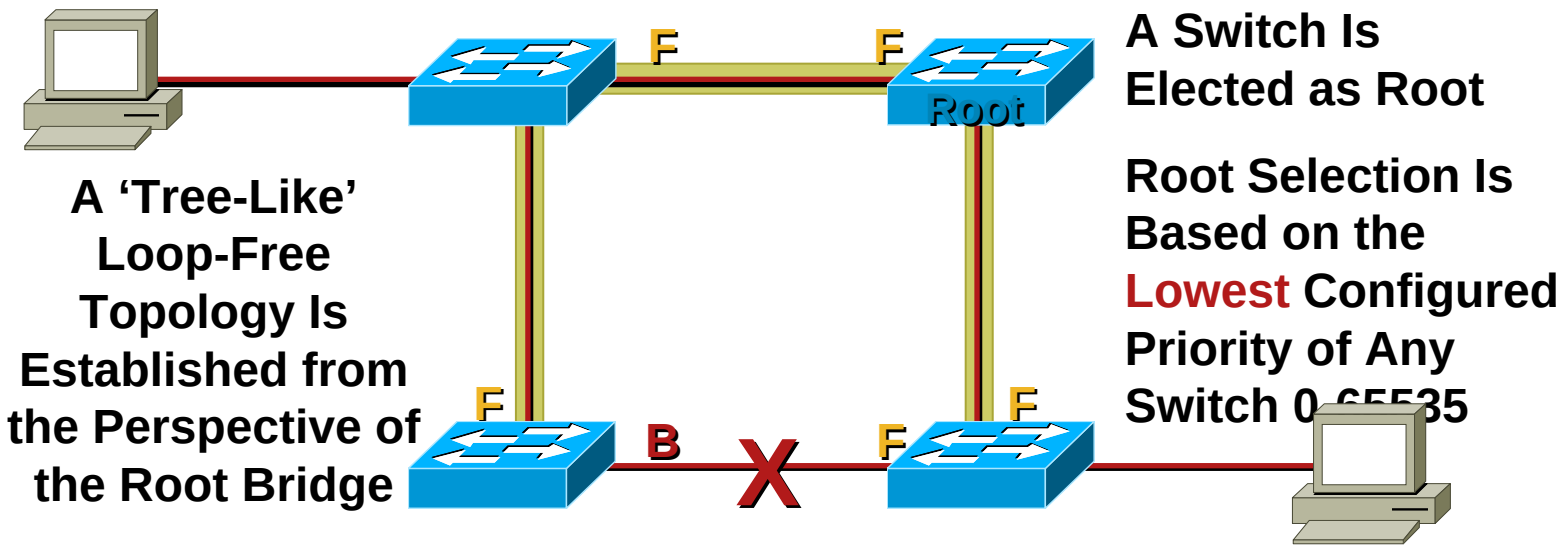
```
================================================
 Feature                        Policer      Physical
                                Index        Policer
================================================
  Fa0/1
  STP                             1            26
  LACP                            2            26
  8021X                           3            26
  RSVD_STP                        4            26
  PVST_PLUS                       5            26
  CDP                             6            26
  DTP                             7            26
  UDLD                            8            26
  PAGP                            9            26
  VTP                            10            26
  CISCO_L2                       11            26
  KEEPALIVE                      12             0
  SWITCH_MAC                     13            26
  SWITCH_ROUTER_MAC              14            26
  SWITCH_IGMP                    15             0
  SWITCH_L2PT                    16            26
```

“26” is the Default “Drop All Policer”

“0” is the Default “Rate-Limiting Policer” for Interface FA 0/1

Spanning Tree Attacks

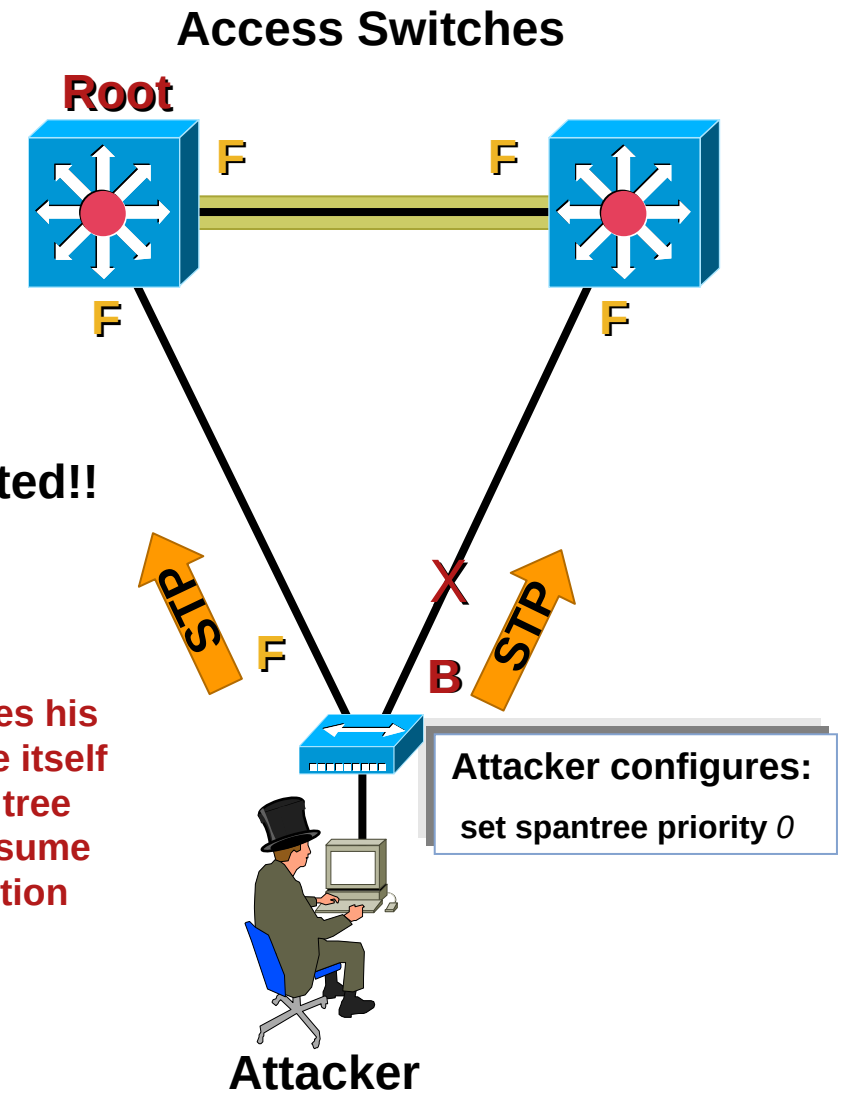
STP maintains loop-free topologies in a Redundant Layer 2 Infrastructure – *Applicable to dual-homed L2 CPE where the SP supports interaction with customer STP*



- 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 a storm!

Spanning Tree Attack Example 1/2

- Send BPDU messages to become root bridge



Spanning Tree Attack Example 2/2

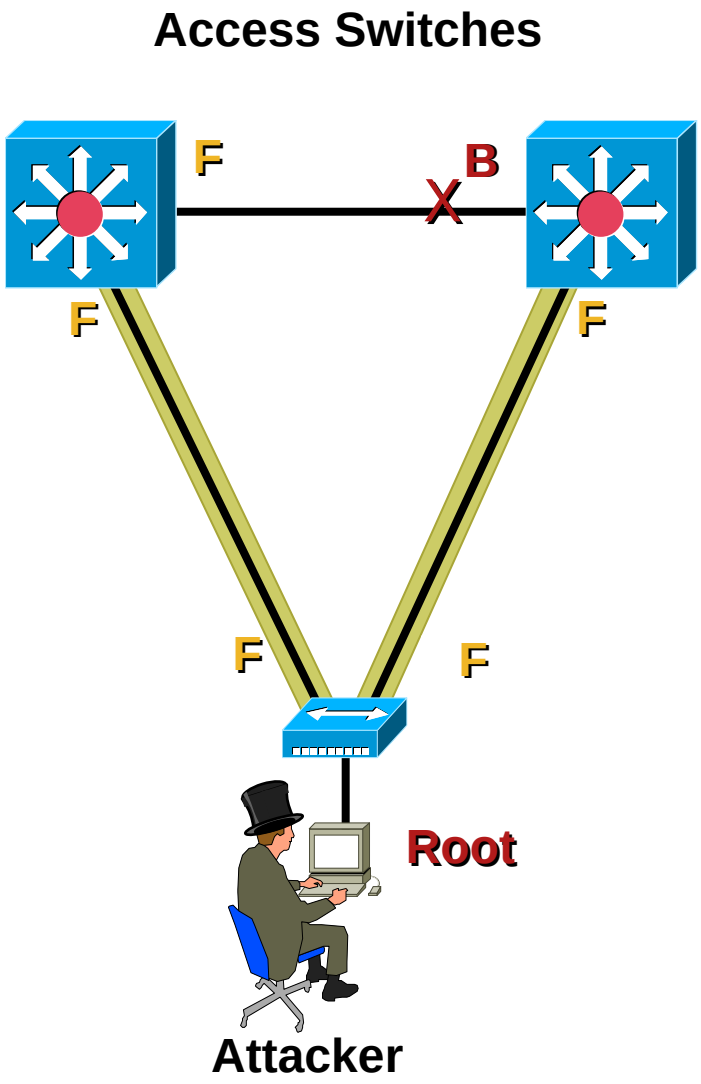
- The attacker then sees frames he shouldn't

  MITM, DoS, etc. all possible

- 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
- The most likely DoS attack is to continually remove and introduce STP devices with zero bridge priority – causing continual STP recalculation and interrupting forwarding

  Standard 802.1d STP takes 30-45 seconds to deal with a failure or root bridge change (nice DoS)

  PortFast and UplinkFast can greatly improve this



STP Attack Mitigation

- Don't disable STP, introducing a loop would become another attack

- BPDU Guard
  - Disables ports using portfast upon detection of a BPDU message on the port
  - Globally enabled on all ports running portfast

Configure globally:

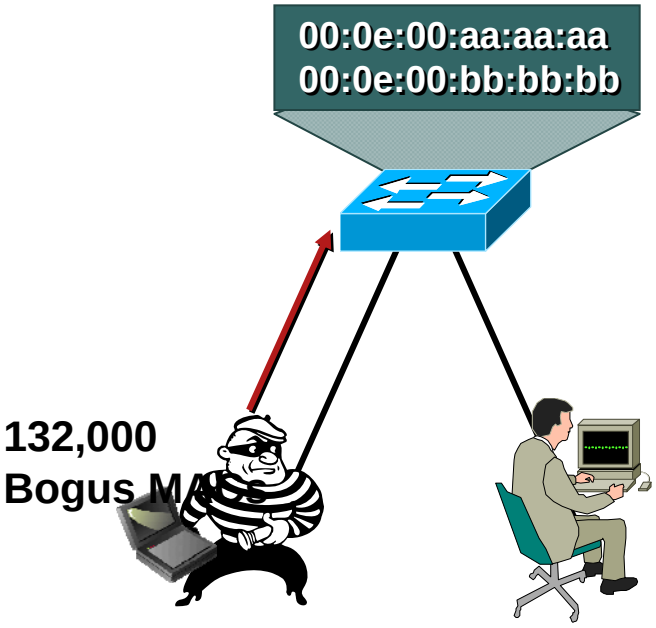
```
spanning-tree portfast bpduguard default
```

- Root Guard
  - Configured on access interfaces on a per-port basis
  - Disables ports who would become the root bridge due to their BPDU advertisement

Per customer port:

```
spanning-tree guard root
```

Switch Security
MAC Flooding Attack

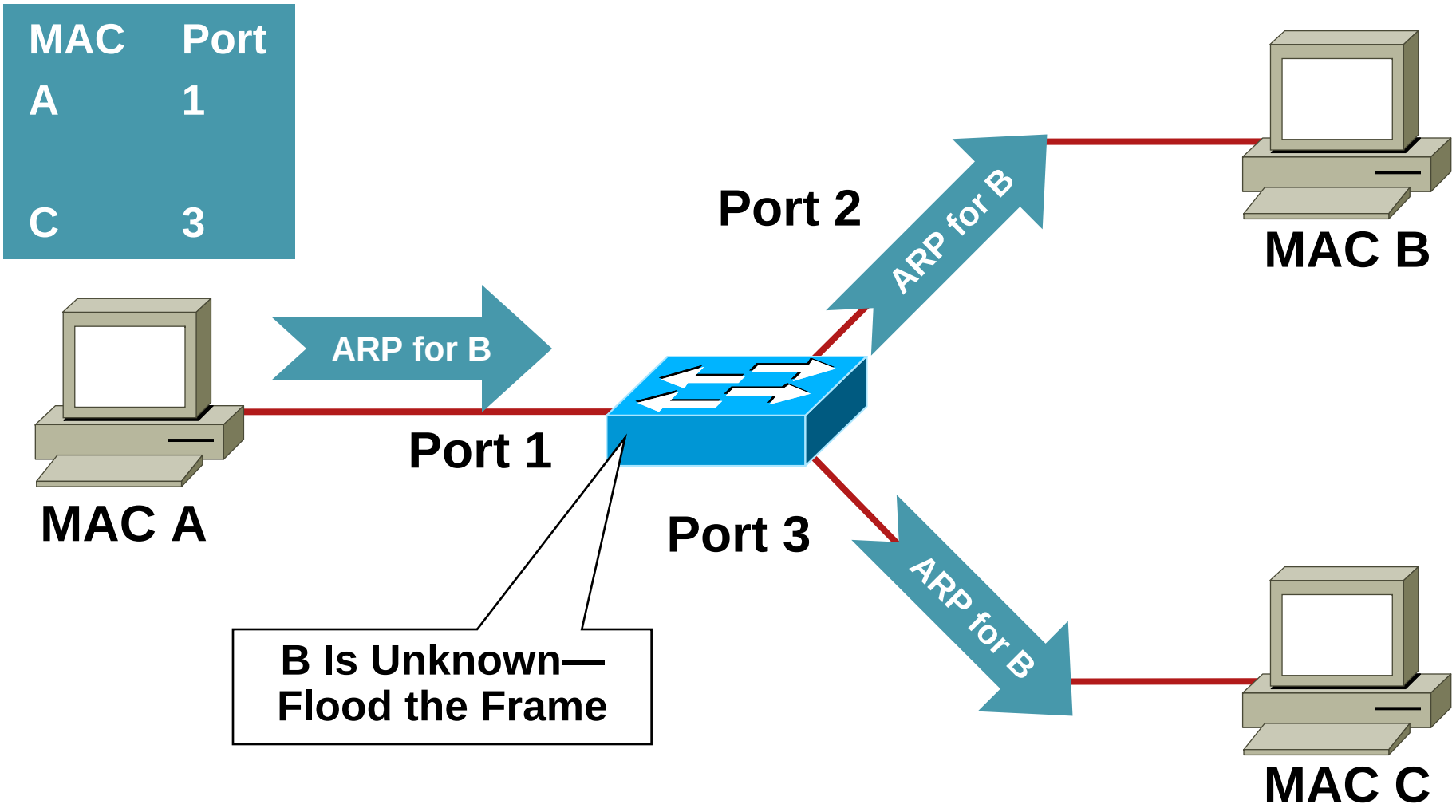


Problem:

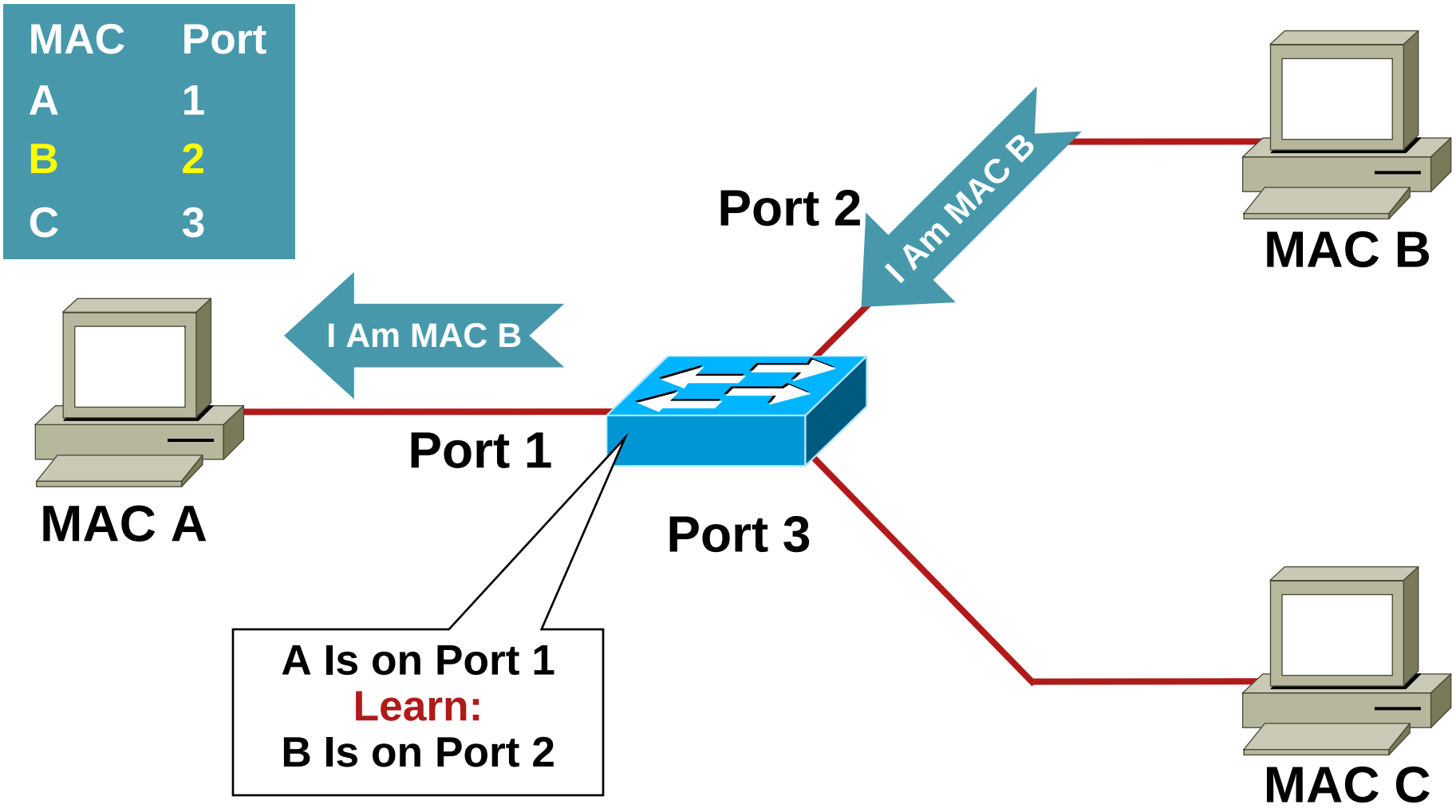
- "Script Kiddie" Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus MACs; Turning the VLAN into a "Hub" and Eliminating Privacy

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

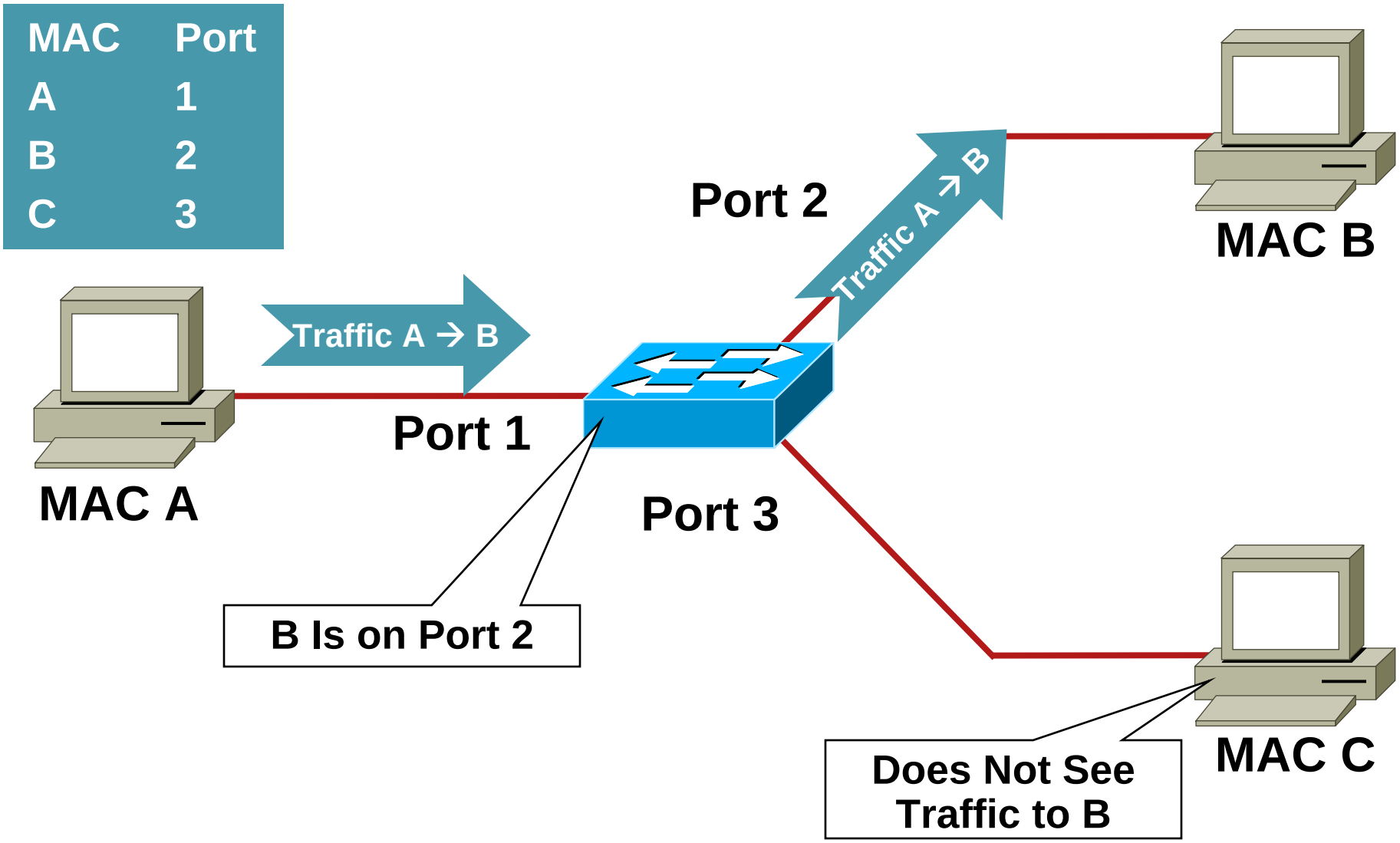
Normal CAM Behavior 1/3



Normal CAM Behavior 2/3



Normal CAM Behavior 3/3



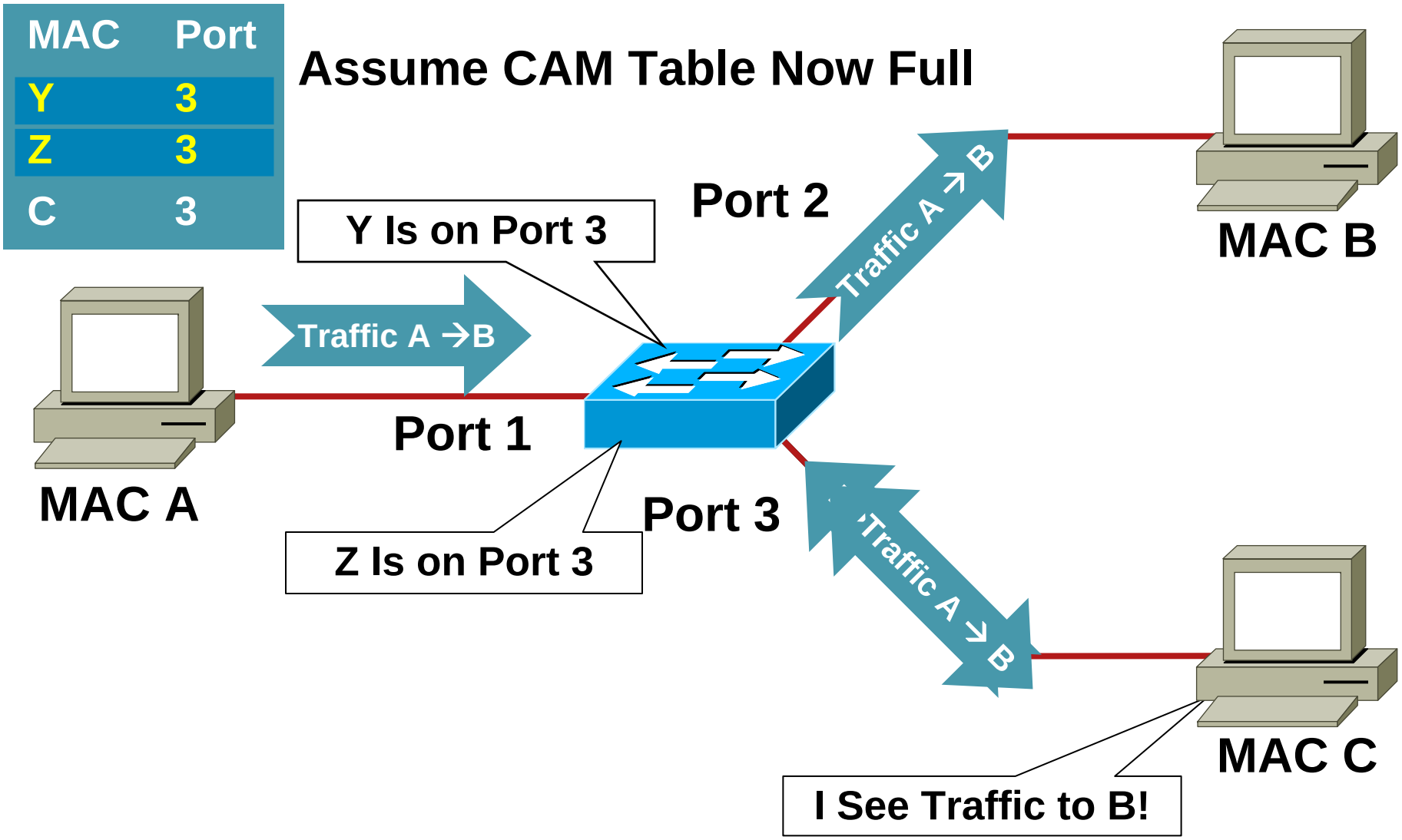
CAM Overflow 1/2

- Macof tool since 1999
- Macof sends random source MAC and IP addresses

  macof (part of dsniff) - http://monkey.org/~dugsong/dsniff/
- Attack successful by exploiting the size limit on CAM tables. 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
- Yersinia—Flavor of the month attack tool

CAM Overflow 2/2



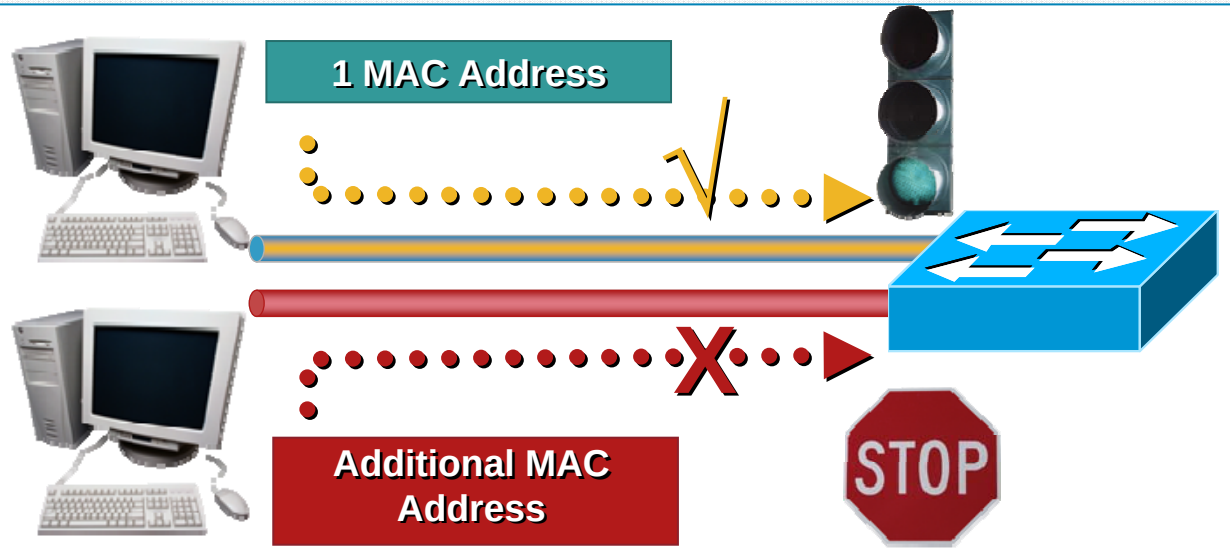
Countermeasure for MAC Flooding Port Security

What It Does:

- Limits the number of MAC addresses on an interface and ensures only approved MAC addresses are able to access the interface

Benefit:

- Protection against malicious MAC Flooding attacks
- Ensures only approved users can log on to the network (secure MAC entries)
- The service provider can use this feature to limit the number of MAC addresses per subscriber UNI (can be included as part of the SLA)



Using Port Security

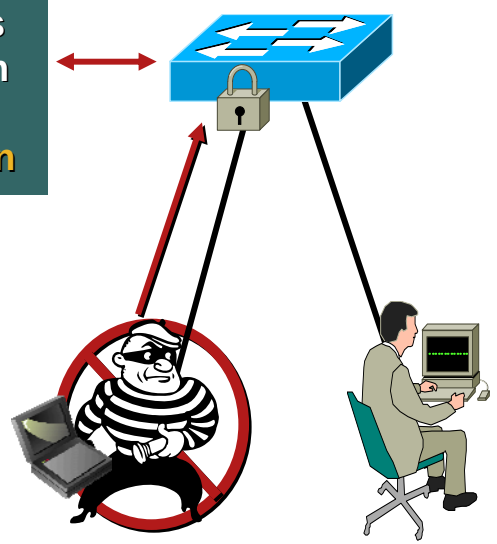
- In the past you would have to type in the only MAC you were going to allow on that port
- You can now put a limit to how many MAC address a port will learn
- You can also put timers in to state how long the MAC address will be bound to that switch port
- You might still want to do static MAC entries on ports that there should be no movement of devices, as in server farms
- Feature called “Sticky Port Security”, settings will survive reboot (not on all switches)

Configuring Port Security

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
```

Only 3 MAC Addresses Allowed on the Port: Take Action



Security Violation Mode Actions:

Violation Mode	Traffic is forwarded[1]	Sends SNMP trap	Sends syslog message	Displays error message[2]	Violation counter increments	Shuts down port
protect	No	No	No	No	No	No
restrict	No	Yes	Yes	No	Yes	No
shutdown	No	Yes	Yes	No	Yes	Yes

Countermeasure for MAC Flooding Configurable Per VLAN MAC Learning

What It Does:

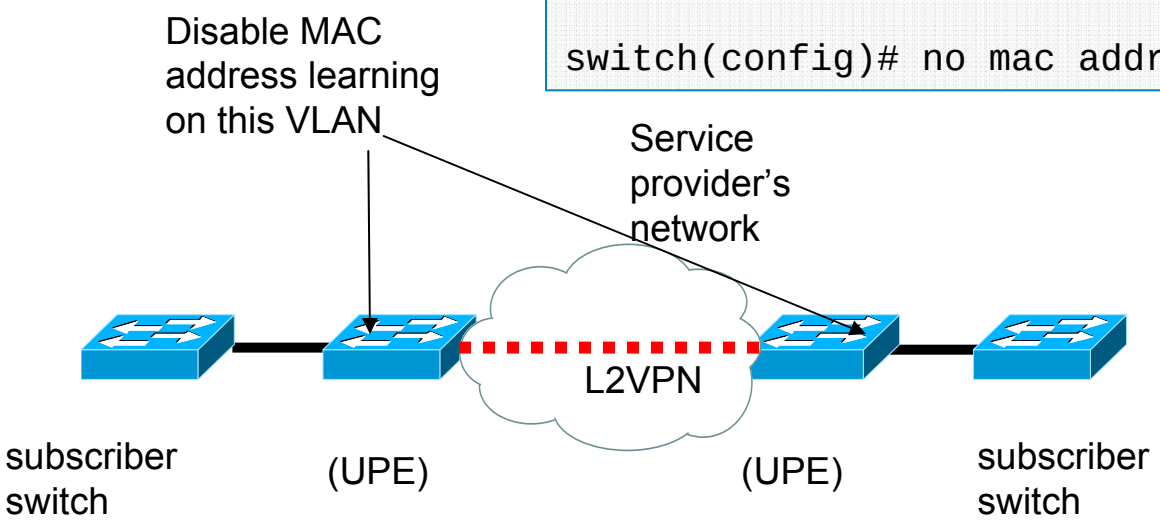
- Provides a configurable mechanism to control how MAC addresses are learned on a per VLAN basis

Benefit:

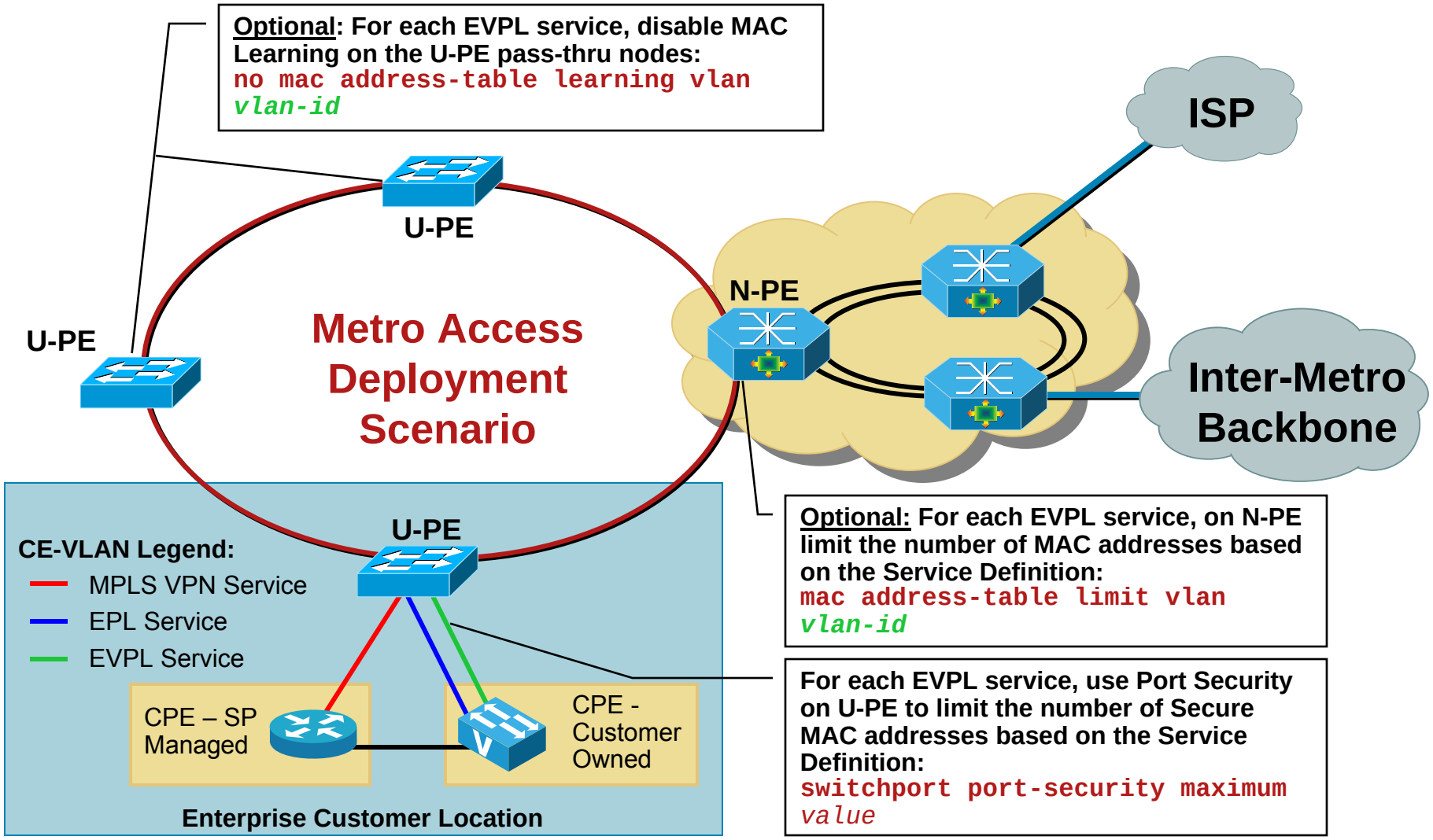
- VLANs with only two ports can have MAC learning disabled, avoiding unnecessary depletion of the CAM table space
- Protection against malicious MAC flooding attacks on that VLAN

To Disable MAC learning for VLAN 10:

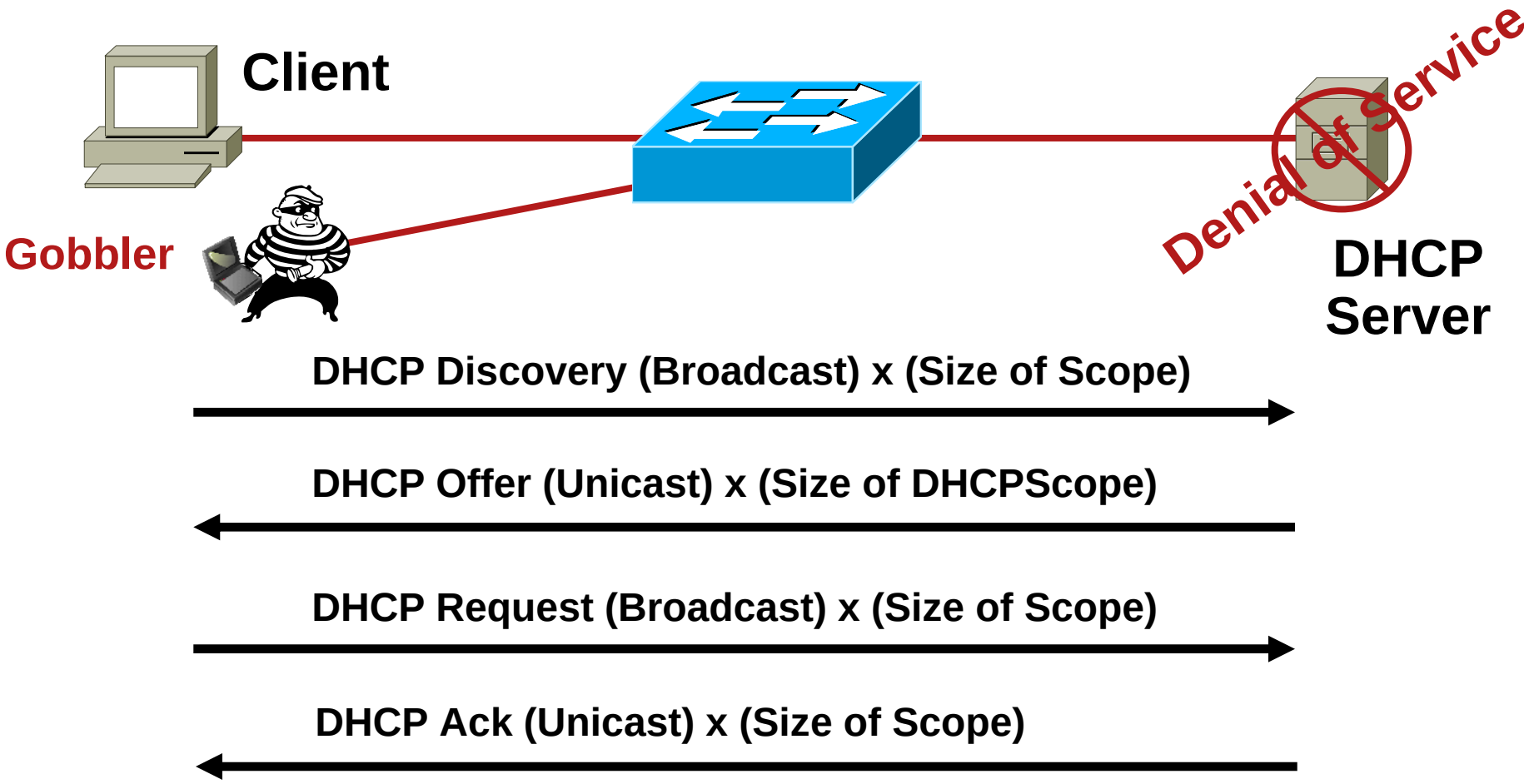
```
switch(config)# no mac address-table learning vlan 10
```



Port Security + Configurable Per VLAN MAC Learning

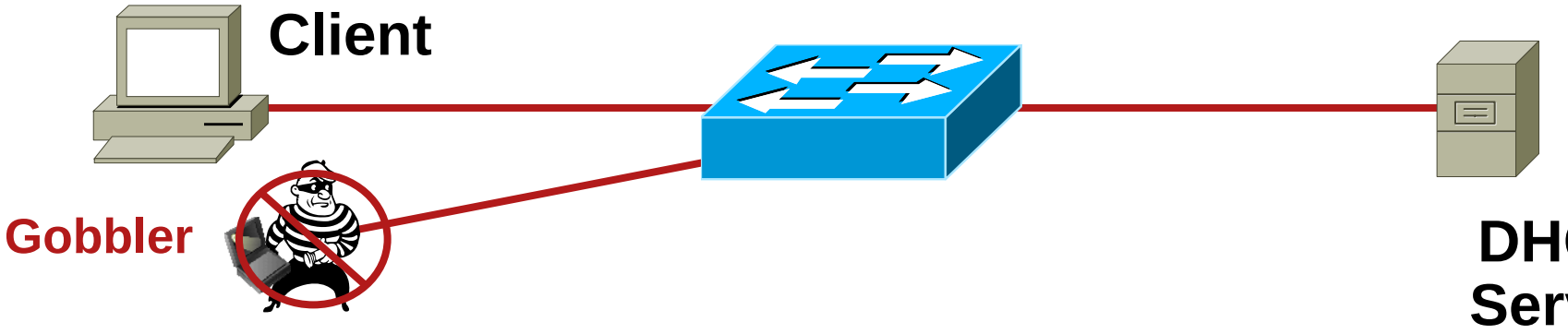


Switch Security
DHCP Starvation Attack



- 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

Countermeasures for DHCP Starvation Port Security



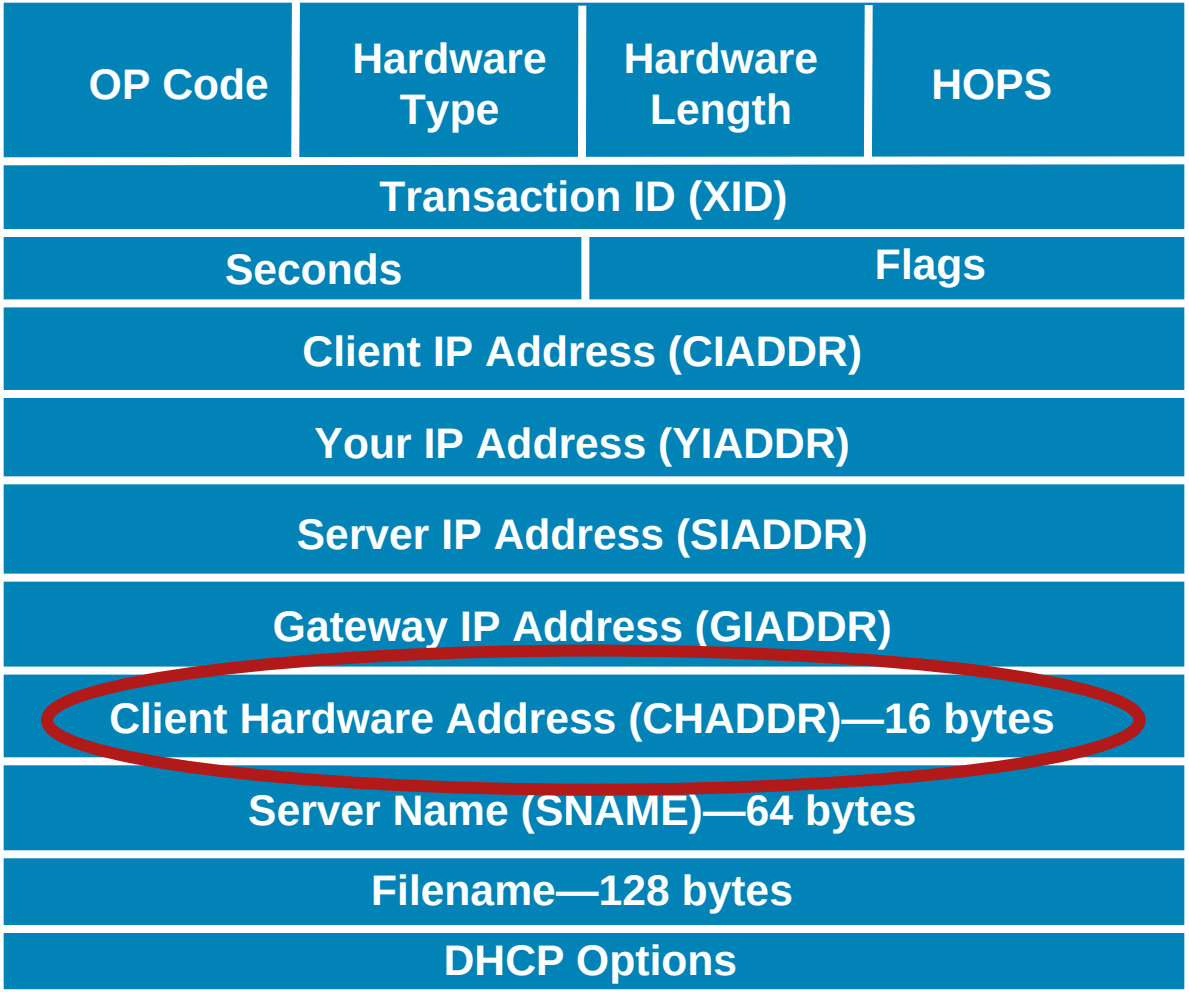
- Gobbler uses a new MAC address to request a new DHCP lease
- Restrict the number of MAC addresses on an port
- Will not be able to lease more IP address then MAC addresses allowed on the port
- In the example the attacker would get one IP address from the DHCP server

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
```

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



What else should I rate-limit?

- ARP

  No valid reason for high levels of ARP traffic – is often an indicator of infected hosts

  Can be used to DoS a switch running Dynamic ARP Inspection, which processes every ARP packet

- DHCP

  Rate-limiting provides additional protection against DHCP Resource Starvation attacks

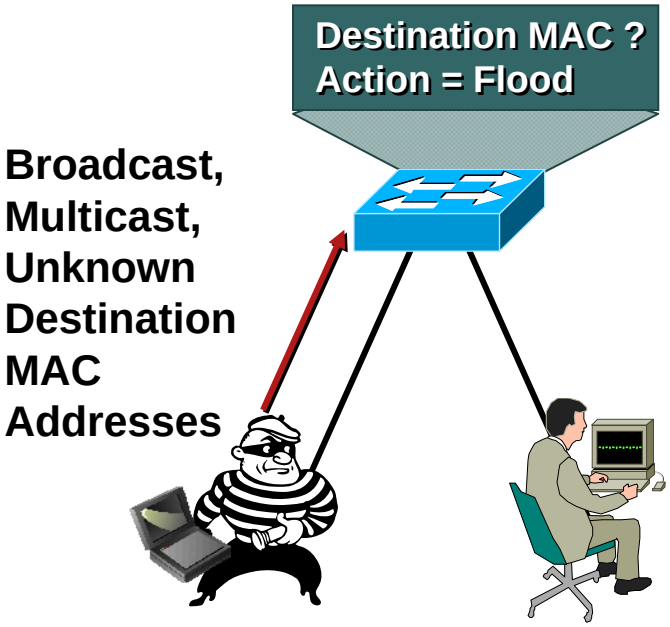
  Many DHCP packets can be used to DoS a switch running DHCP Snooping

- IGMP

  Can DoS a router with IGMP Joins, which installs a lot of (*,G) state in the router

  Can transmit multicast traffic which triggers a router to send PIM Register messages to the Rendezvous Point (RP) -> DoSs the RP

Switch Security
Broadcast Storm Attack



Problem:

- The attacker sends a large amount of traffic with broadcast, multicast or unknown destination MAC addresses to a network element
- This action exploits the fact that an Ethernet switch's behavior is to flood these type of frames
- A large amount of this traffic may diminish system resources (e.g., memory, CPU utilization, etc.) along the transmission path
- Bandwidth may also be affected by the excessive traffic replication.

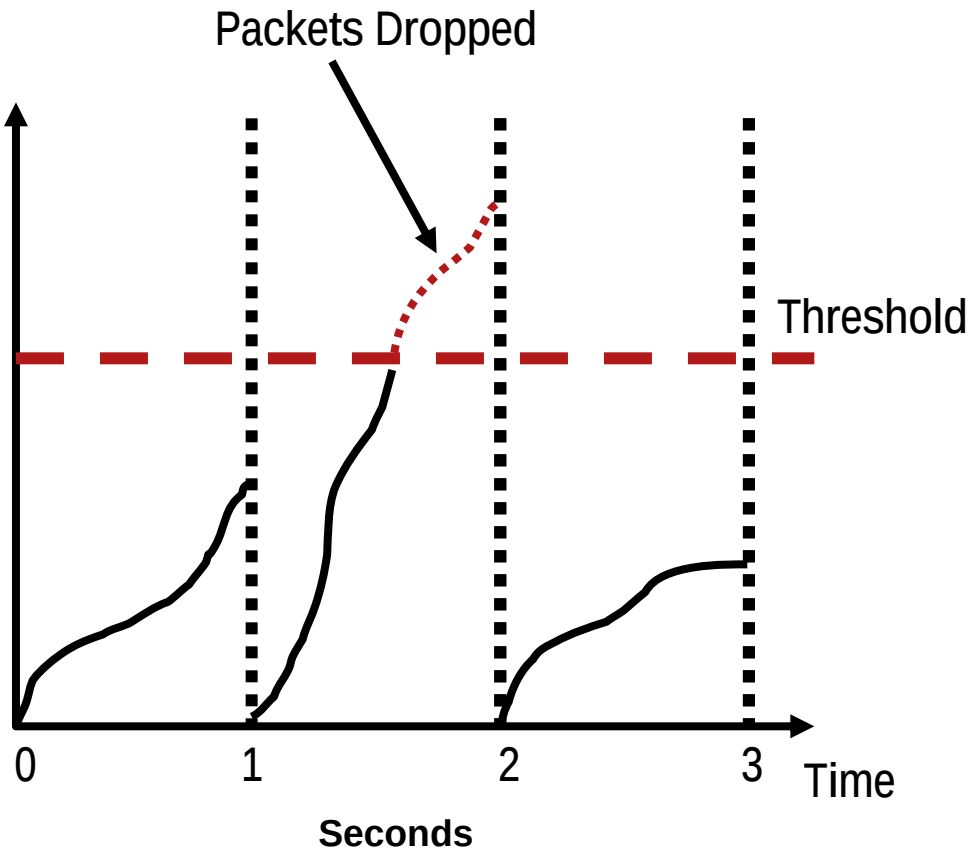
Countermeasure against Storm Attacks Storm Control

What It Does:

- Limits the volume of broadcast, multicast and/or unicast traffic
- Ports can be disabled or can send traps if configuration limits are exceeded
- Also sometimes known as Broadcast suppression

Benefit:

- Protects the network from intentional and unintentional flood attacks
- Limits the combined rate of broadcast and multicast traffic to normal peak loads



Configuring Storm Control

- Rate limiting/control of broadcast frames

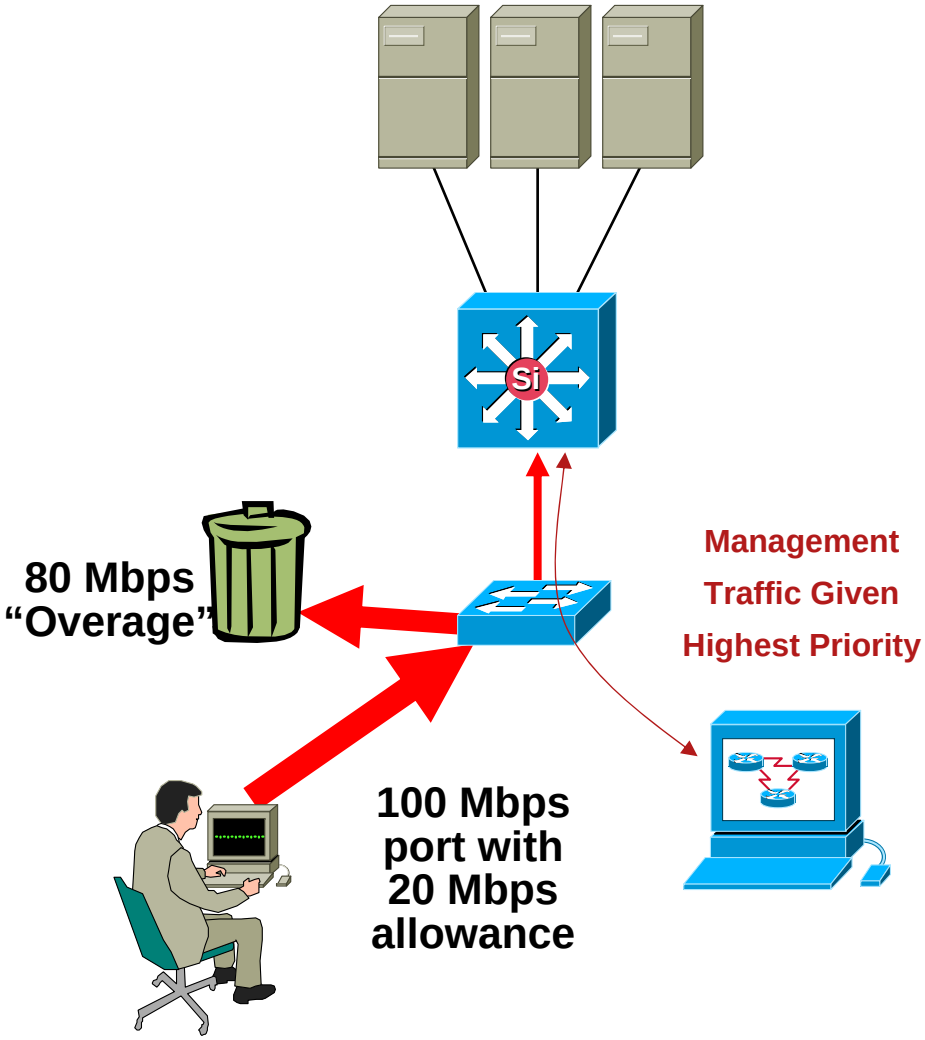
  Broadcast Suppression/Storm Control monitors broadcasts within a one-second storm control interval. Once the threshold is reached, filters out subsequent broadcast packets until the end of the traffic storm control interval

- Some switches support port shut-down and trap generation

IOS
Interface Commands

```
storm-control multicast level 70
storm-control broadcast level 50
storm-control unicast level 80
```

Switch Security
Data Plane Storms - Rate Limiting



What It Does:

- Rate limiters can limit traffic per VLAN, port or user to mitigate the impact of packet-blasting worms and limit amount of traffic a user can send onto the network
- Can rate limit using either traffic policing or shaping functions

Benefit:

- Prevents a malicious user from flooding the network with traffic, affecting other users and the management of the network itself

Switch Security
Data Plane Storms - Priority Policing

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth 500000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface
  gigabitethernet0/1
Switch(config-if)# service-policy
  output policy1
Switch(config-if)# exit
```

What It Does:

- A strict priority queue can consume all available bandwidth and starve all other queues
- Priority policing limits the amount of traffic that can be scheduled by the priority queue

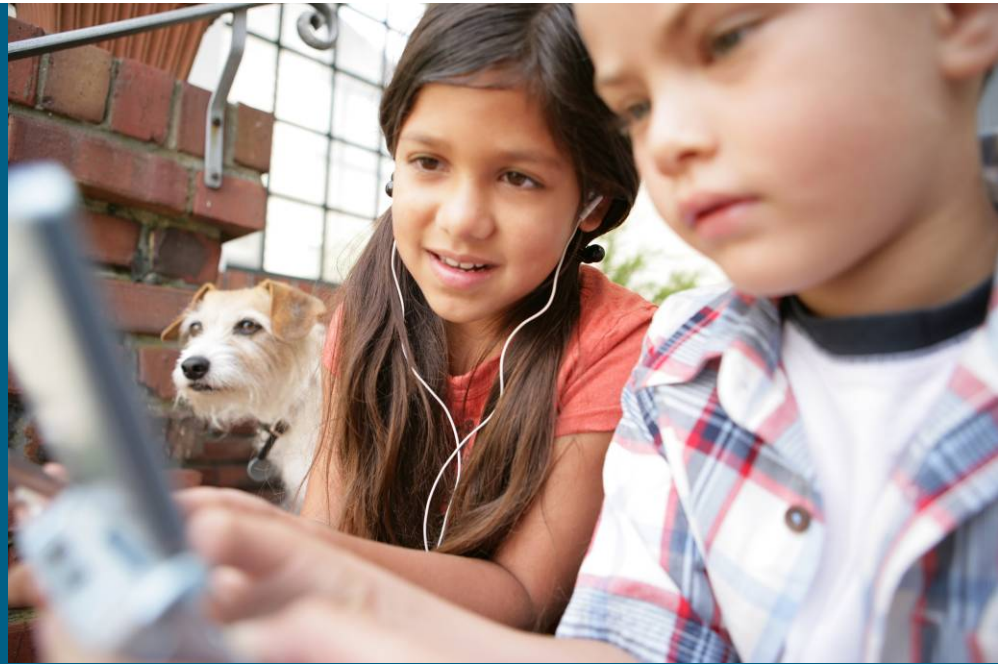
Benefit:

- Prevents a malicious user from flooding the network traffic marked as priority, starving other classes
- Allows the Service Provider to "trust" the customer QoS markings (DSCP, IPP, CoS) without being concerned with complete starvation of lower class queues

Switch Security

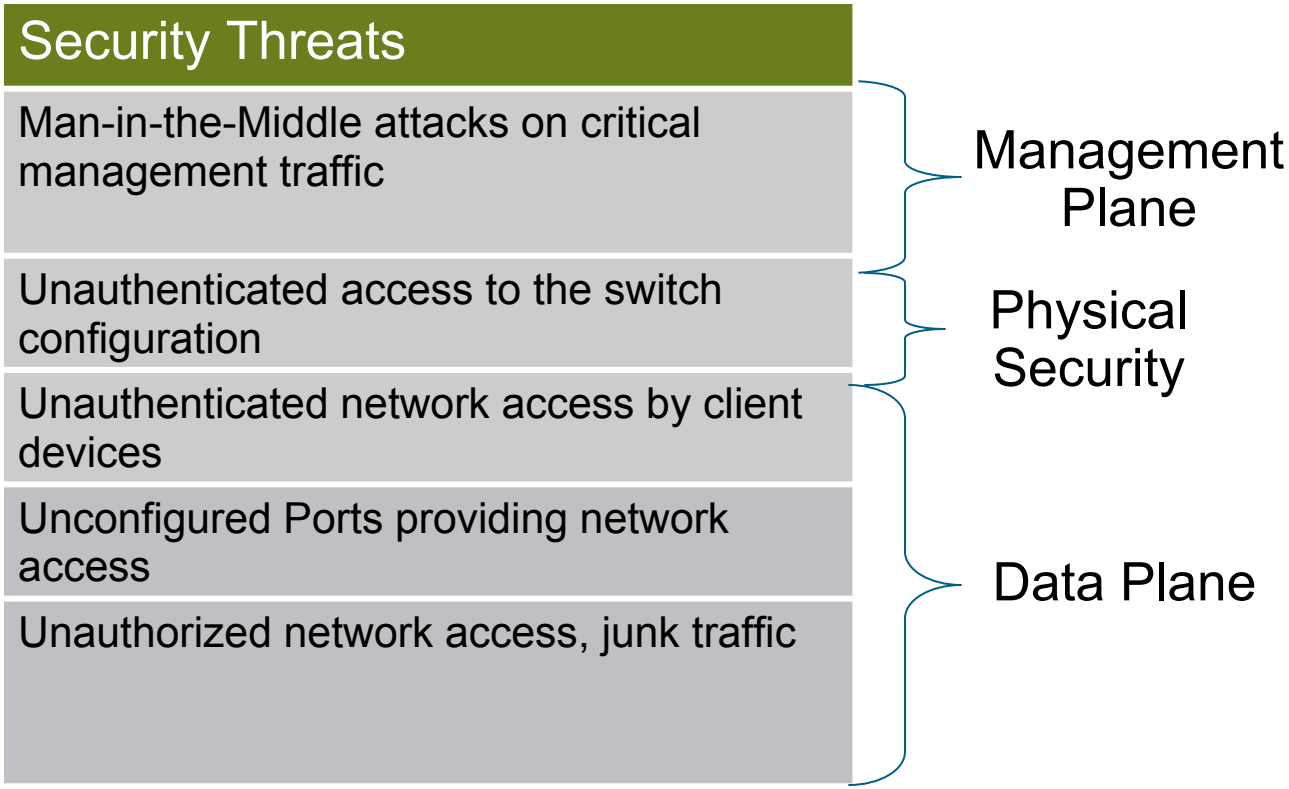
Security Concern:	Solution
L2 Control Protocol Attack (STP, LACP, PAgP, CDP, VTP, etc…)	Control Plane Policing
MAC Flooding / Overflow	Port Security & Configurable Per VLAN MAC Learning
DHCP Resource Starvation	Port Security + DHCP Snooping
Unicast, multicast, or broadcast storms	Storm Control
Infected users flooding the network / Malicious users attacking the Priority traffic queue	Rate-limiting, Priority policing

Layer 2 Attack Landscape Infrastructure Threats



Infrastructure Security

- Infrastructure attacks exploit insecure data, control and management planes as well as weak physical security
- It is essential to ensure that only valid traffic is allowed through the switch through filtering and blocking. This must be done at the edge of the SP network e.g. Metro Access switches



Infrastructure Security Management Plane

- 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 (SNMP, TFTP, Telnet, etc.)
- Consider secure variants of these protocols where available (SNMPv3, SCP, SSH, etc.). Where impossible, consider Out- of-Band (OOB) management
- When OOB management is not possible:

  Put the management VLAN into a dedicated VLAN

  Limit access to the management protocols using the "set ip permit" lists on the management protocols

- Use secure Remote-Access practices
- Verify all configuration changes

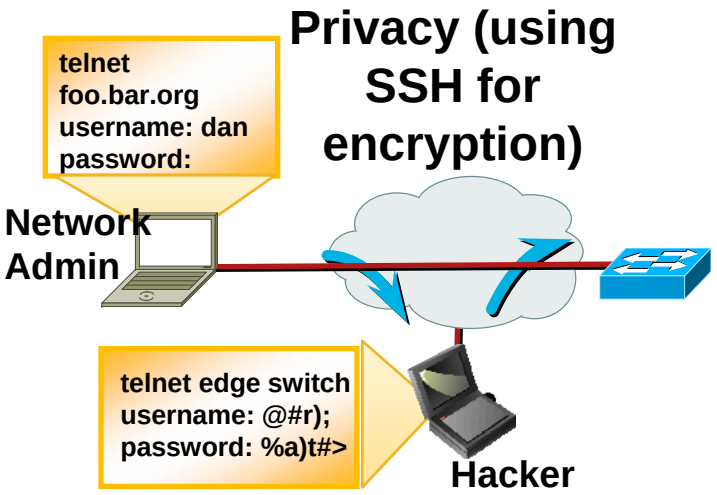
SNMP

- SNMP Community
  - No default public RO/private RW
  - Standard password guidelines
  - Different communities on each access device
- SNMP ACL
- SNMP View/Privilege
- SNMP v3

```
snmp-server community k4llekula RO 2
snmp-server community 87gf6v3c RW 3
```

```
access-list 2 permit 195.20.1.160 0.0.0.31
access-list 3 permit 195.21.1.160 0.0.0.31
```

Secure Shell (SSH)



What It Does:

- SSH is a protocol that can provide a secure connections to a remote device for management
- Data is sent through an encrypted tunnel (DES or 3DES) to secure transmission and integrity of data.
- Authenticates users and ensures secure file transfer and copying
- To use this feature, you must install the cryptographic (encrypted) software image on your switch

Benefit:

- Both sides of tunnel are authenticated so that man-in-the-middle attacks are prevented and critical management information is not compromised
- Provides improved security as compared to Telnet sessions by providing strong encryption when a device is authenticated
- Protects passwords and configuration information

Remote Access Protection

A. Protect Telnet access using login and enable passwords
B. Use SSH if possible
C. Secure the vty ports used for Telnet access with an ACL
D. Implement password management and use Enable Secret
E. Register users with separate user IDs on each router
F. Authenticate and account for remote users TACACS+/RADIUS
G. Authenticate devices directly attached to access switches
H. Use “motd” to detail legal impact of breaking into the system

Verification of Configurations

- Use AAA per-command authorization and accounting

  Limits inadvertent mistakes as well!

- Store configuration history and changes. Log who has made a configuration change, and when
- Implement a procedure for the parsing and verification of configurations. A centralized server should verify the consistency of the configurations.
- Use Rancid to collect all core and distribution configurations every 15 minutes, all access configurations every 24 hours

  http://www.shrubbery.net/rancid/

- Cisco Configuration Assurance Solution (CAS) automatically performs regular, systematic audits of the production network to diagnose device mis-configurations, configuration policy violations etc.

Switch Security
Physical/Environmental Security

- With live deployments there have been several occurrences of physical “break in” to get access to the console port
- By default switches allow a user with physical access to interrupt the boot process while the switch is powering up and enter a new password
- Solution is “password recovery disable”

What It Does:

- The system administrator can disable some of the functionality of password recovery by allowing an end user to reset a password only by agreeing to return to the default configuration
- In this case, the switch will erase the configuration file if forced into the password recovery process

Benefit:

- Prevents malicious users from accessing critical information contained in the configuration file by using the password recovery process

Infrastructure Security
IEEE 802.1x Authentication

What It Does:

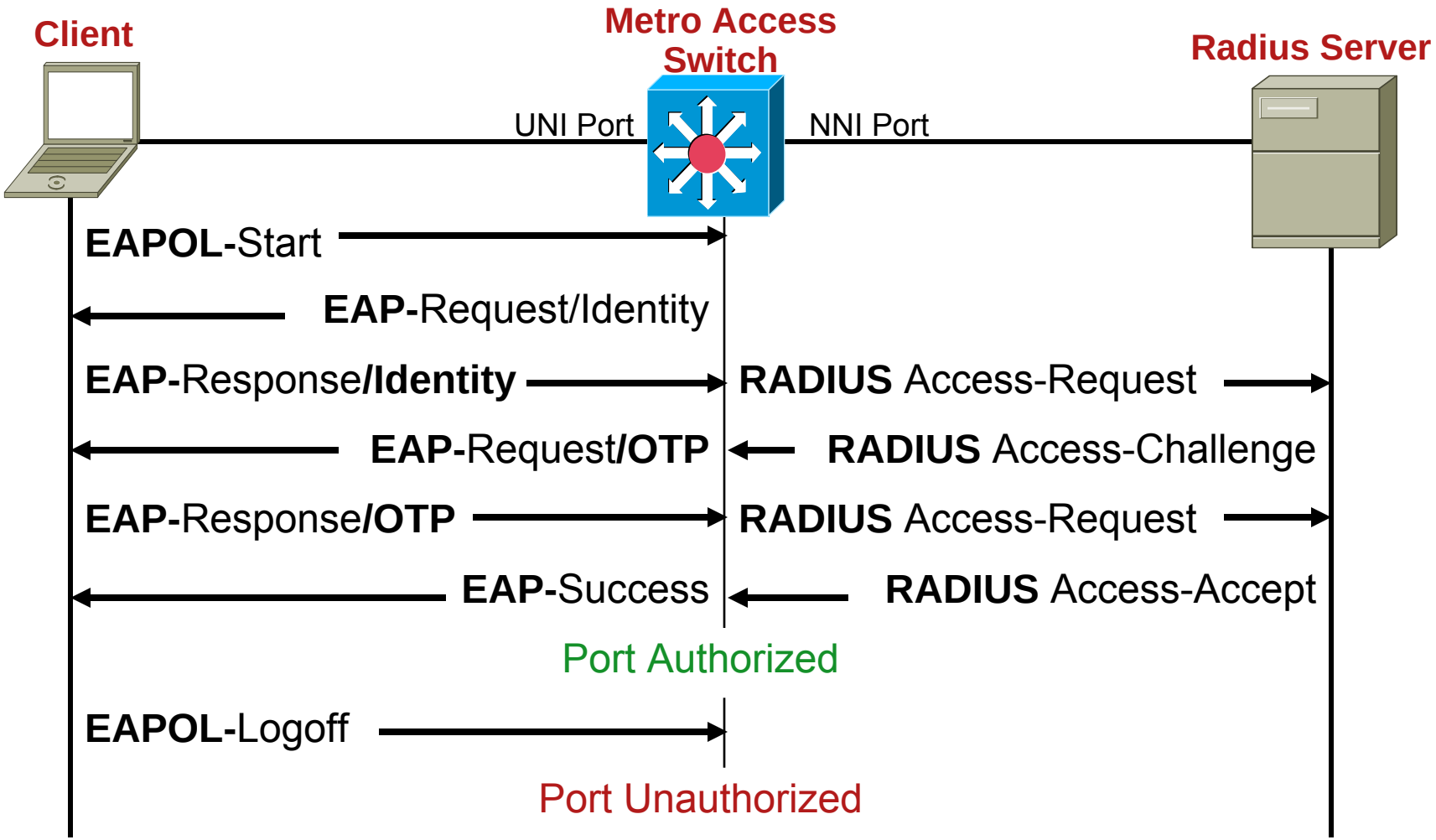
- Client-server-based access control and authentication protocol
- The Metro Access switch controls the physical access to the network based on the authentication status of the customer client device
- The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client

Benefit:

- Prevents unauthorized users from connecting to the network through a UNI port unless they are properly authenticated
- The RADIUS server database maintains "username-to-VLAN mappings", assigning the VLAN based on the username of the client connected to the Metro access switch port. You can use this feature to assign network access (VLAN) for client devices.

IEEE 802.1x
How it works

802.1x message exchange required for Port Authorization:



802.1x Authentication

- Combined with “no service password recovery” a physically hacked access switch (U-PE) cannot authenticate with the aggregation switch

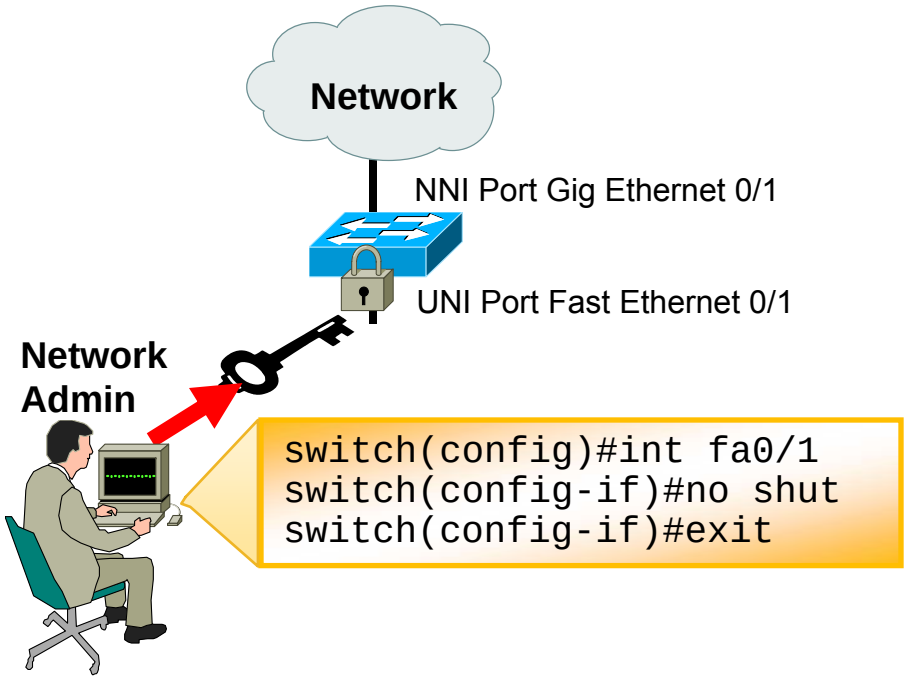
  Authentication info is erased when the box is reset

- Requires 802.1x “Supplicant” (client) on access switches

  On 802.1q trunks

- Requires 802.1x Authenticator on 802.1q trunks on aggregation devices

Infrastructure Security
UNI Default Port Down



What It Does:

- Unlike ports on traditional Enterprise LAN switching products, the UNI ports are Shut Down by default
- NNI ports are enabled (no shut) by default to allow for remote connectivity by the Network Admin

Benefit:

- Prevents unauthorized access to network services while a switch is being installed and initially configured
- Default behavior for UNI / NNI port types

Infrastructure Security
Access Control Lists (ACLs)

What It Does:

- ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs
- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP)
- Ethernet (MAC) ACLs are used to filter non-IP traffic.
- Port, VLAN and Router ACLs are supported

Benefit:

- Restrict network use by certain users or devices
- Administrators can selectively apply extended ACLs based on the time of day and week for added flexibility and/or automation

Infrastructure Security
Access Control Lists (ACLs)

- **Port ACLs** - Control traffic entering a Layer 2 interface (inbound)
- **Router ACLs** - Control routed traffic between VLANs, applied to Layer 3 interfaces (inbound or outbound).
- **VLAN ACLs** or VLAN maps - Control all packets (forwarded and routed).
  - VLAN maps can be used to filter traffic between devices in the same VLAN
  - Control based on Layer 3 addresses for IPv4
  - Unsupported protocols are controlled through MAC addresses using Ethernet ACEs.

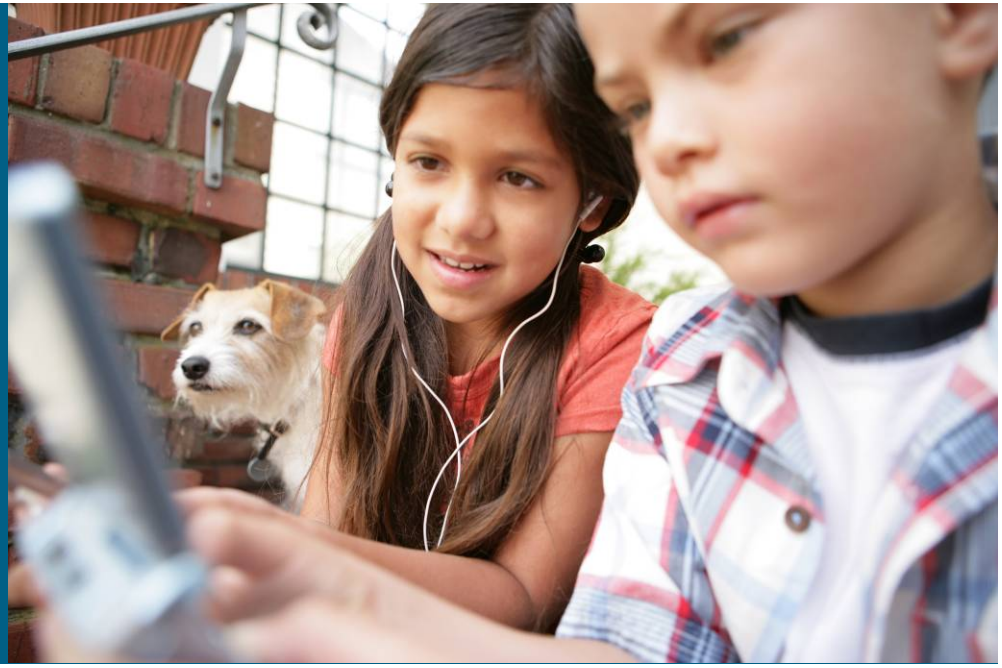
```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any

Switch# show access-lists
Standard IP access list 2
10 deny 171.69.198.102
20 permit any
```

Infrastructure Security Summary

Security Threats	
Man-in-the-Middle attacks on critical management traffic	Out-of-Band Management, SNMPv3, SSH, per-command AAA
Unauthenticated access to the switch configuration	Password recovery disable
Unauthenticated network access by client devices	802.1x
Unconfigured Ports providing network access	UNI Default Port Down
Unauthorized network access, junk traffic	Access Lists

Summary



Layer 2 Security Best Practices

- Isolate users from each other
- Lockdown unused ports
- Use information gleaned from DHCP to protect against spoofing attacks
- Authenticate attached client devices and limit the number of MAC addresses per port
- Protect switch infrastructure by limiting traffic that consumes CPU resource
- Manage switches as securely as possible (SSH, OOB, SNMPv3, etc.)

Summary

- This presentation discussed the primary threats and security solutions for Layer 2 access networks
- With default settings, Layer 2 protocols and switches are vulnerable to multiple attacks
- Cisco has an extensive range of solutions to address known intrusion and denial-of-service attacks exploiting Layer 2 protocols
- These solutions should be complemented with other infrastructure “lockdown” techniques, discussed in SEC-2013 “Network Core Infrastructure Protection: Best Practices”
- These solutions should ideally be complemented with mechanisms to counter infected hosts through detection and remediation mechanisms, discuss in SEC-2016 “Network-based Solutions for Broadband Security”

Useful information

Related Sessions

- SEC-2015 Detecting Router Abuse
- SEC-2016 Network-based Solutions for Broadband
- BBA-3002 Aggregation Networks for Residential and Business Services

Meet the Experts
IP NGN Architectures and Technologies

- Oliver Boehmer
  Network Consulting Engineer

- Moustafa Kattan
  Consulting Systems Engineer

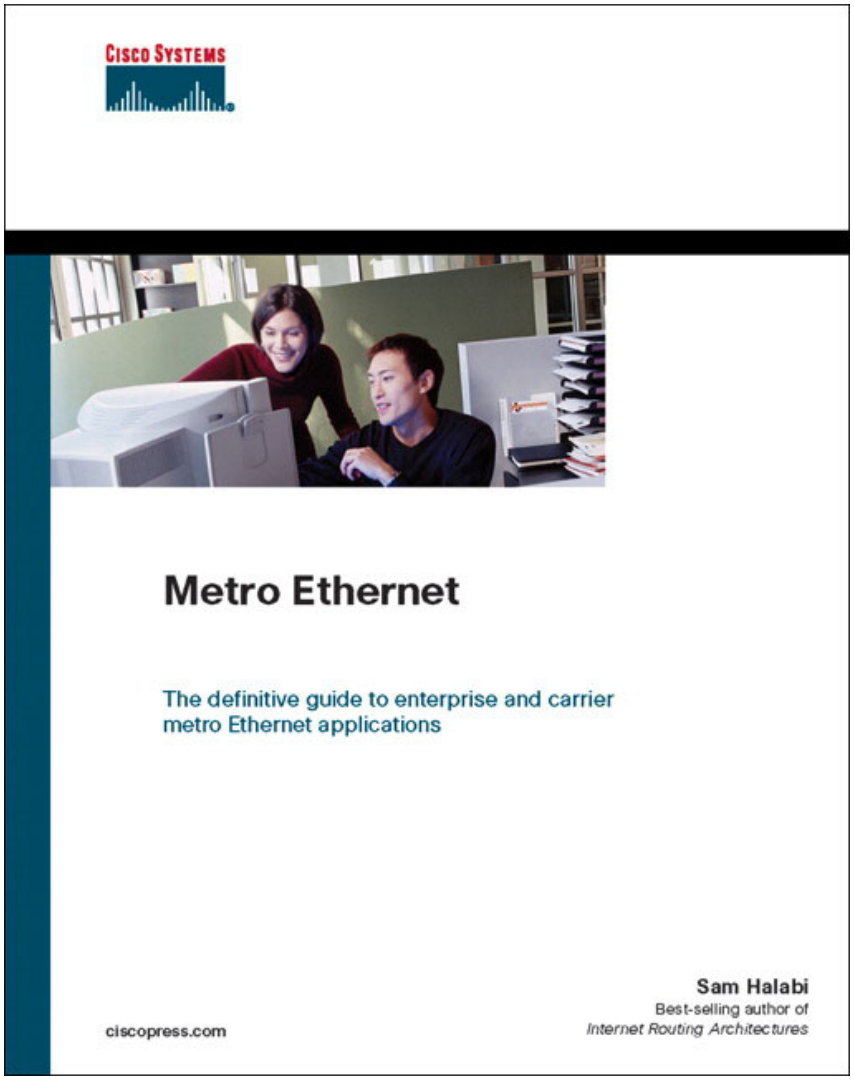
- Yves Hertoghs
  Distinguished System Engineer

- Ed Draiss
  Product Manager

Recommended Reading

BRKBBA -2004

- Metro Ethernet



Available in the Cisco Company Store

Q and A