Network Security

CS6823
Layer 2 Security

Phillip Mak
pmak@nyu.edu

The material within was originally presented at Cisco Networkers Live Conference 2008-2009. Modified since.

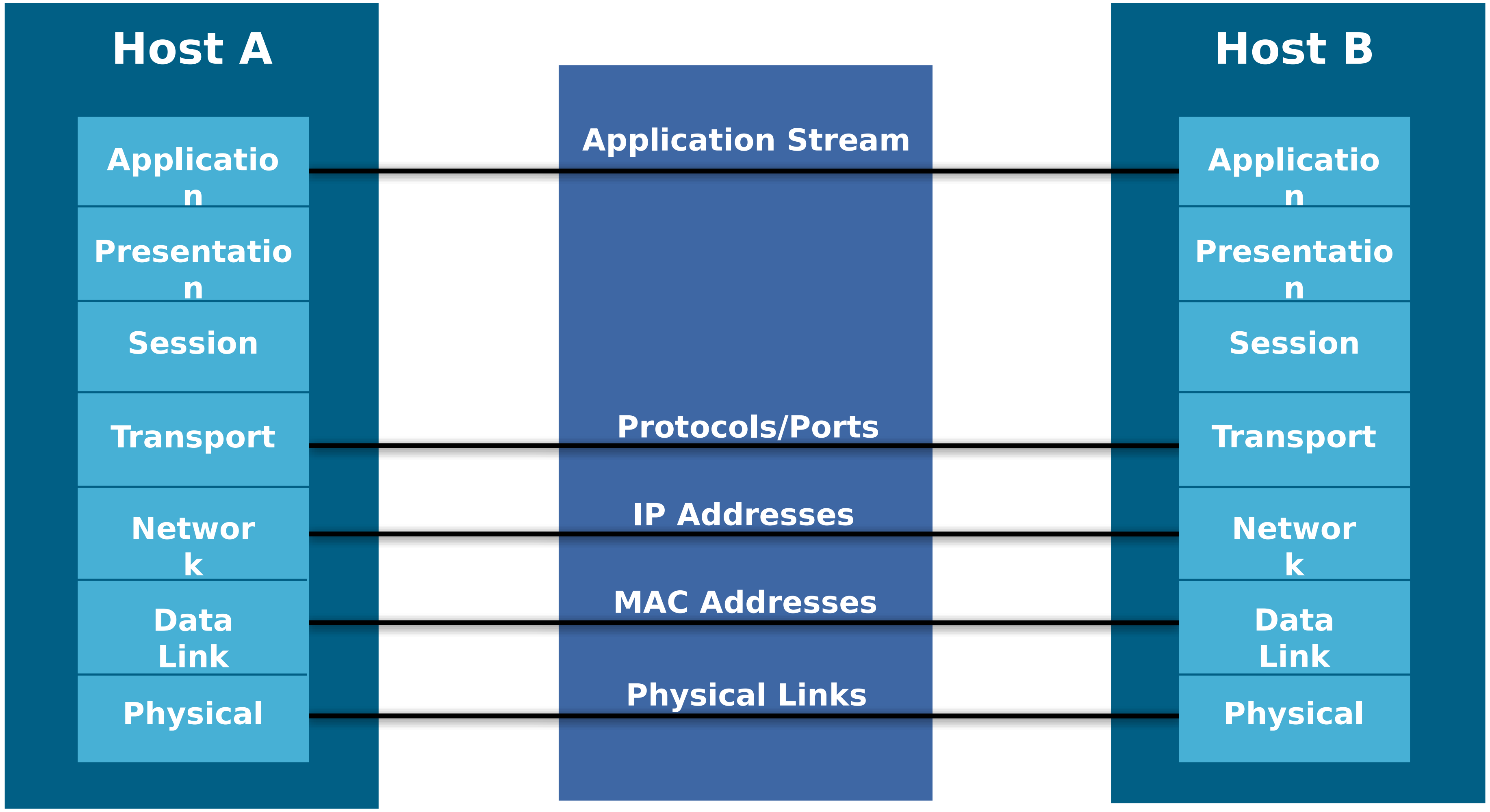
Objectives

- Be able to explain and describe the major types Layer 2 security issues
- Topics
  - CAM Table Overflow Attack
  - VLAN Hopping Attacks
    - Basic VLAN Hopping
    - Double Tagging
  - DHCP Attacks
    - DHCP Address Starvation
    - Rogue DHCP Server
  - ARP
  - Layer 2 and 3 Spoofing
  - Spanning Tree Protocol

Layer 2 Switch Security

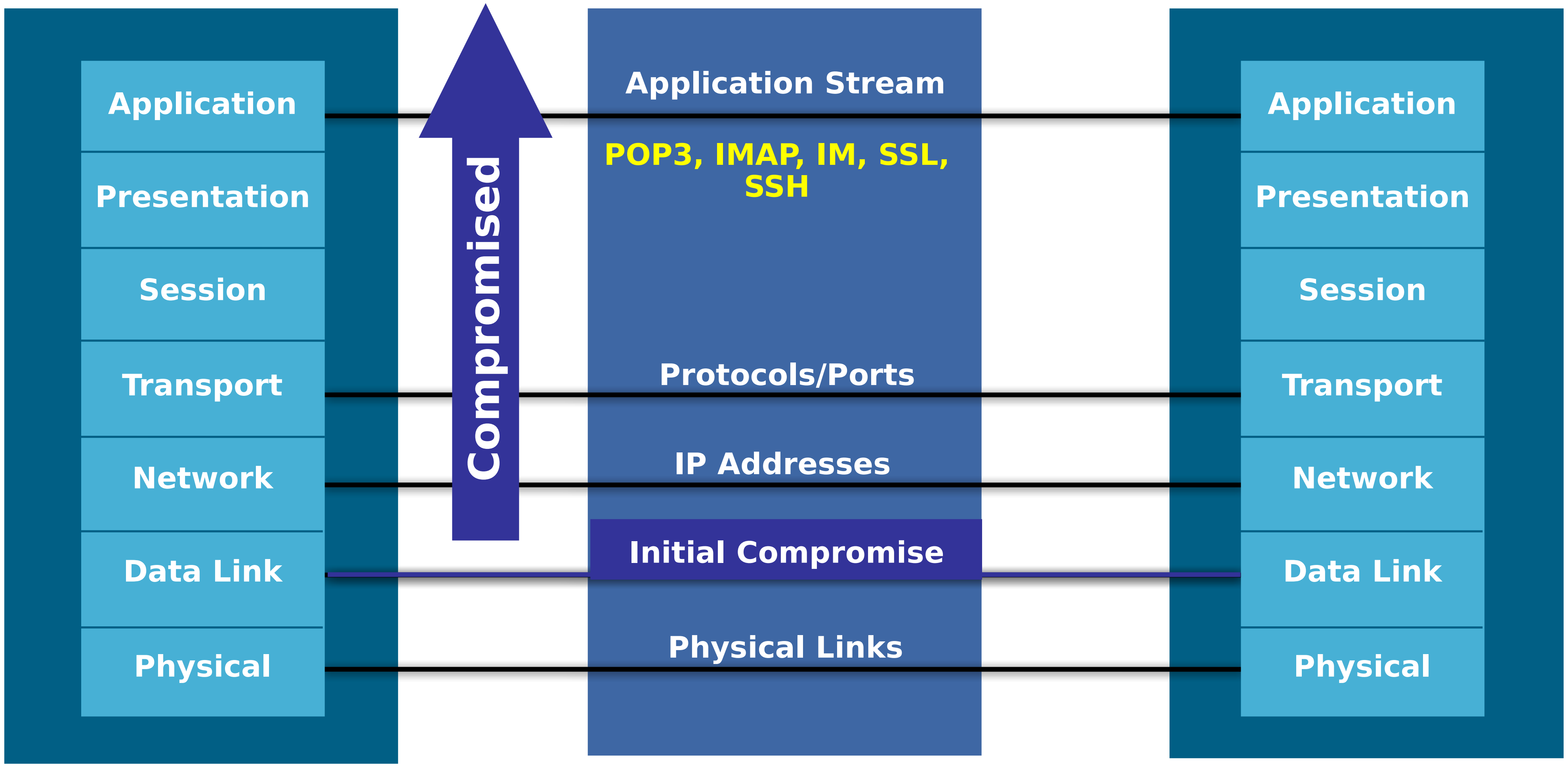
Why Worry About Layer 2 Security?

- OSI was built to allow different layers to work without the knowledge of each other



Lower Levels Affect Higher Levels

- This means if one layer is hacked, communications are compromised without the other layers being aware
- Security is only as strong as the weakest link
- Layer 2 can be VERY weak



MAC Attacks

MAC Address CAM Table

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

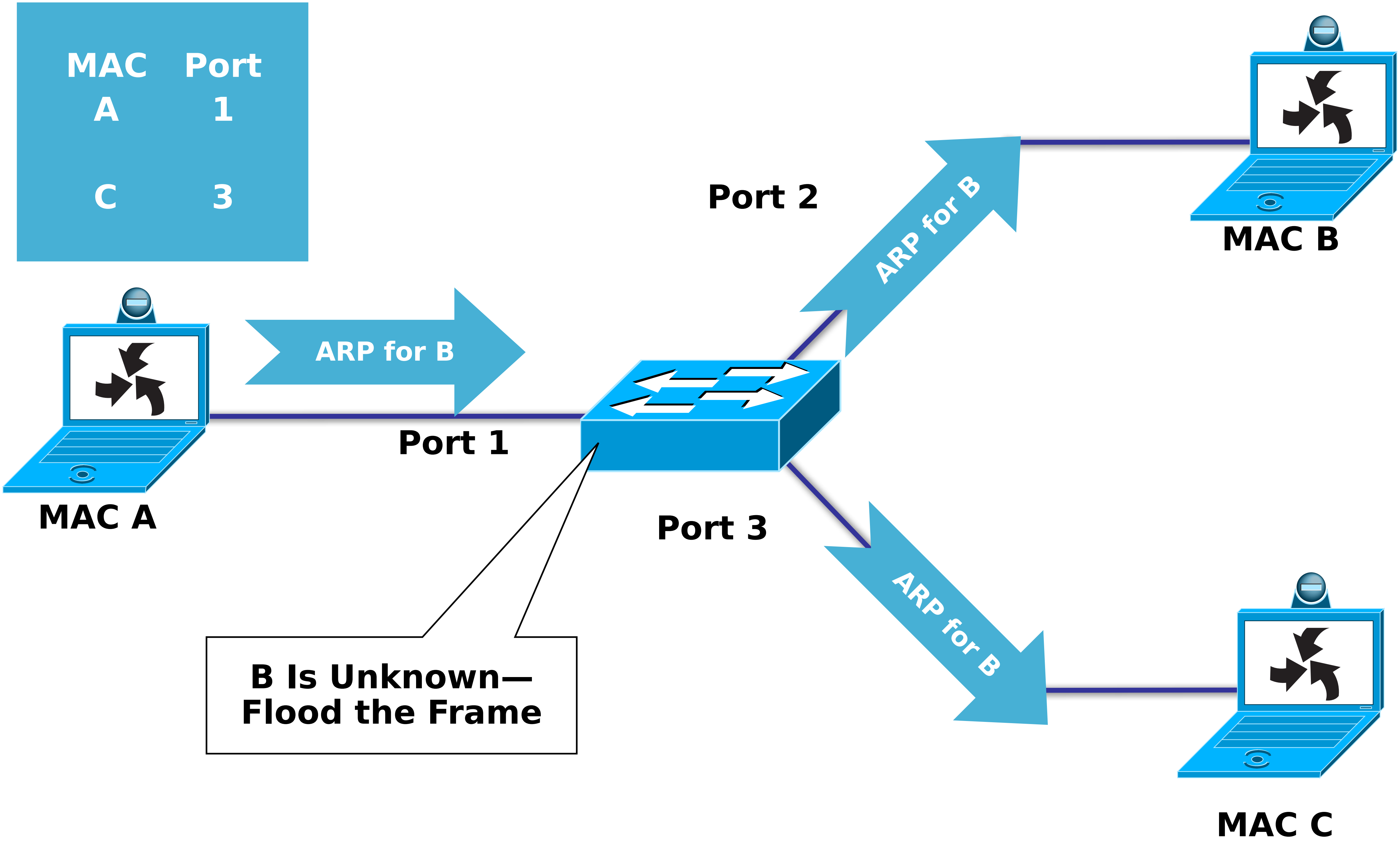
0000.0cXX.XXXX

All Fs = Broadcast

FFFF.FFFF.FFFF

- CAM table stands for Content Addressable Memory
- The CAM table stores the mapping of MAC addresses to the physical interface, and associated VLAN parameters. the .
- All CAM tables have a fixed size

Normal CAM Behavior 1/3

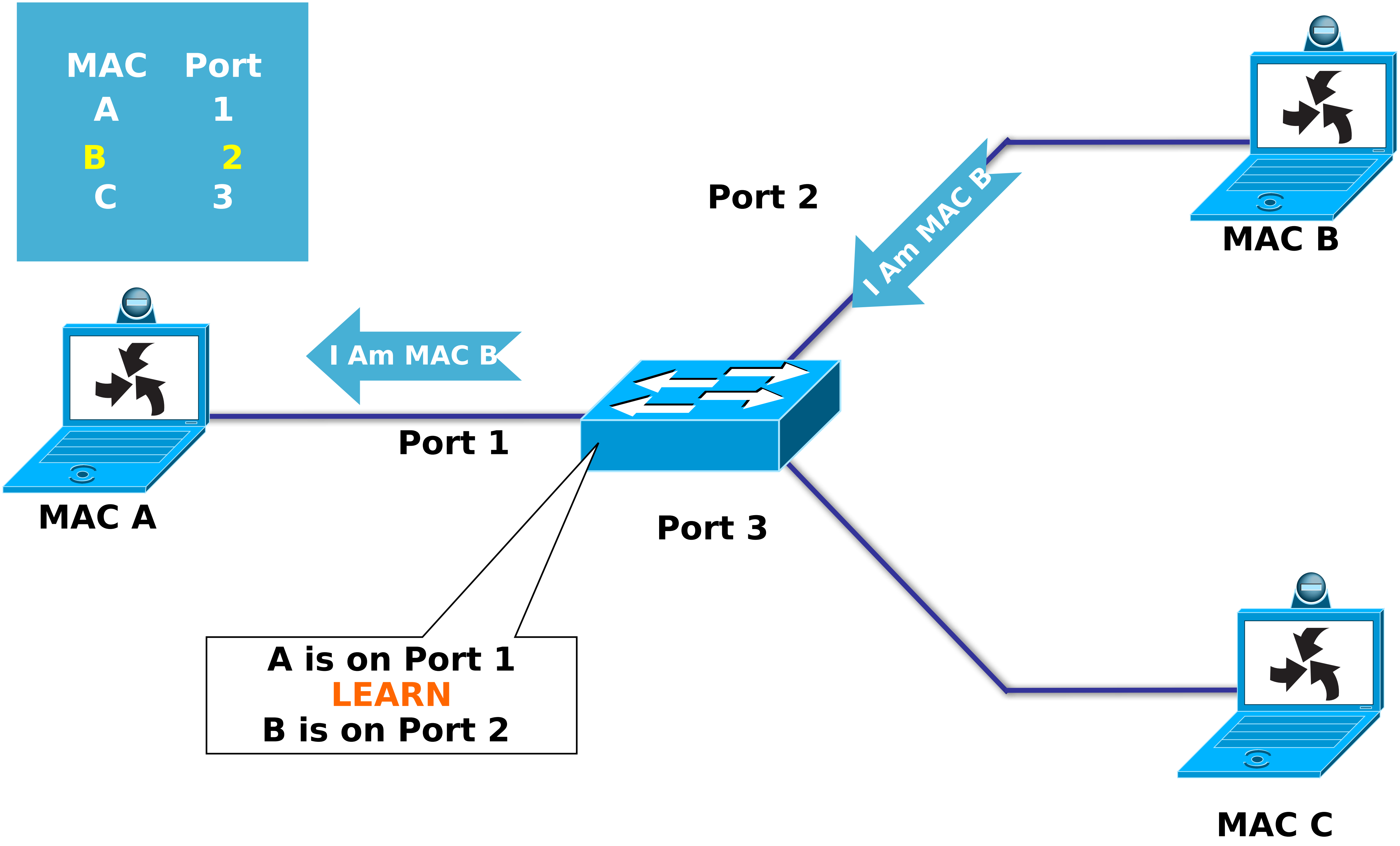


MAC	Port
A	1
C	3

B Is Unknown—
Flood the Frame

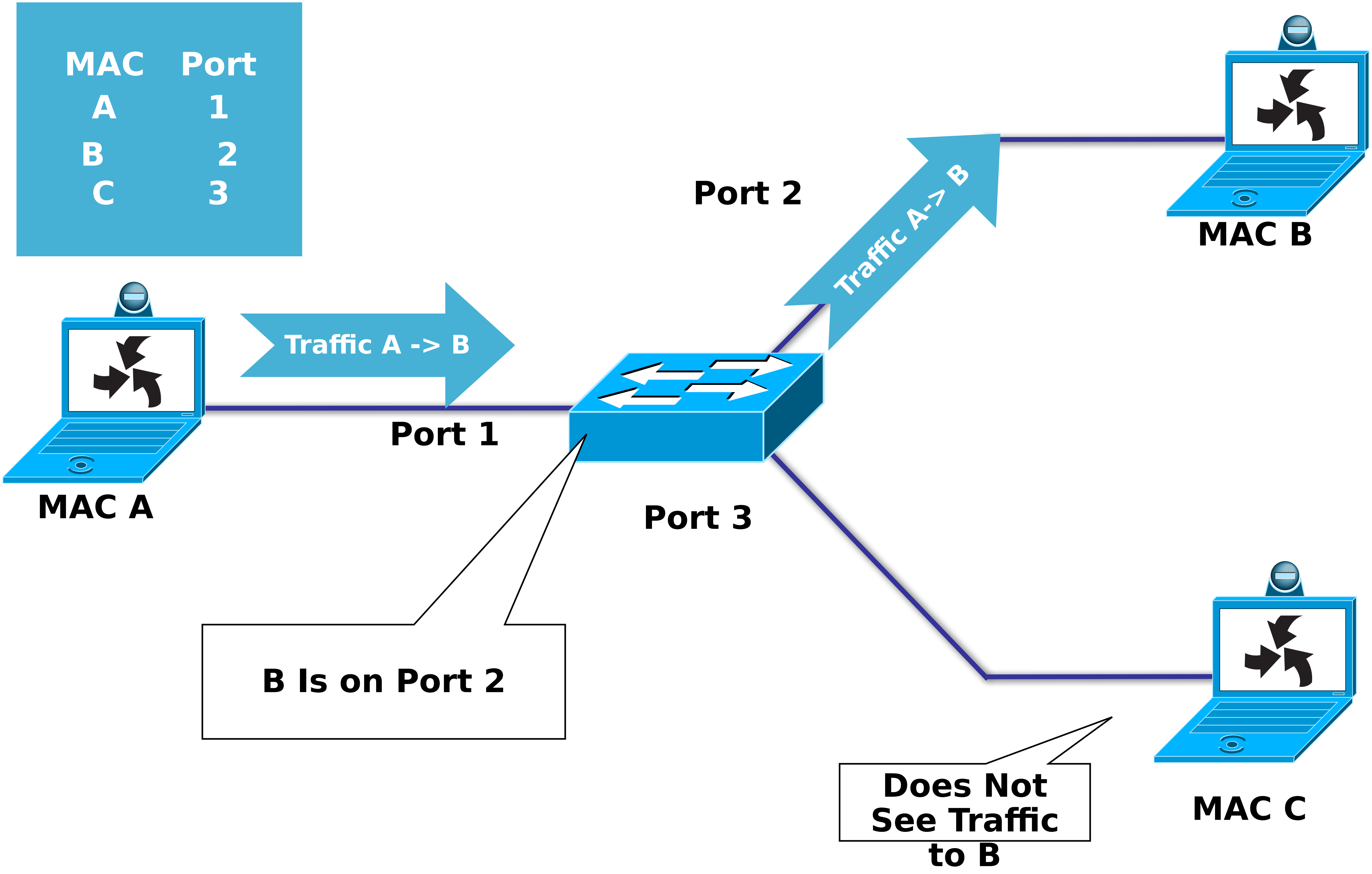
Normal CAM Behavior 2/3

MAC	Port
A	1
B	2
C	3



A is on Port 1
LEARN
B is on Port 2

Normal CAM Behavior 3/3

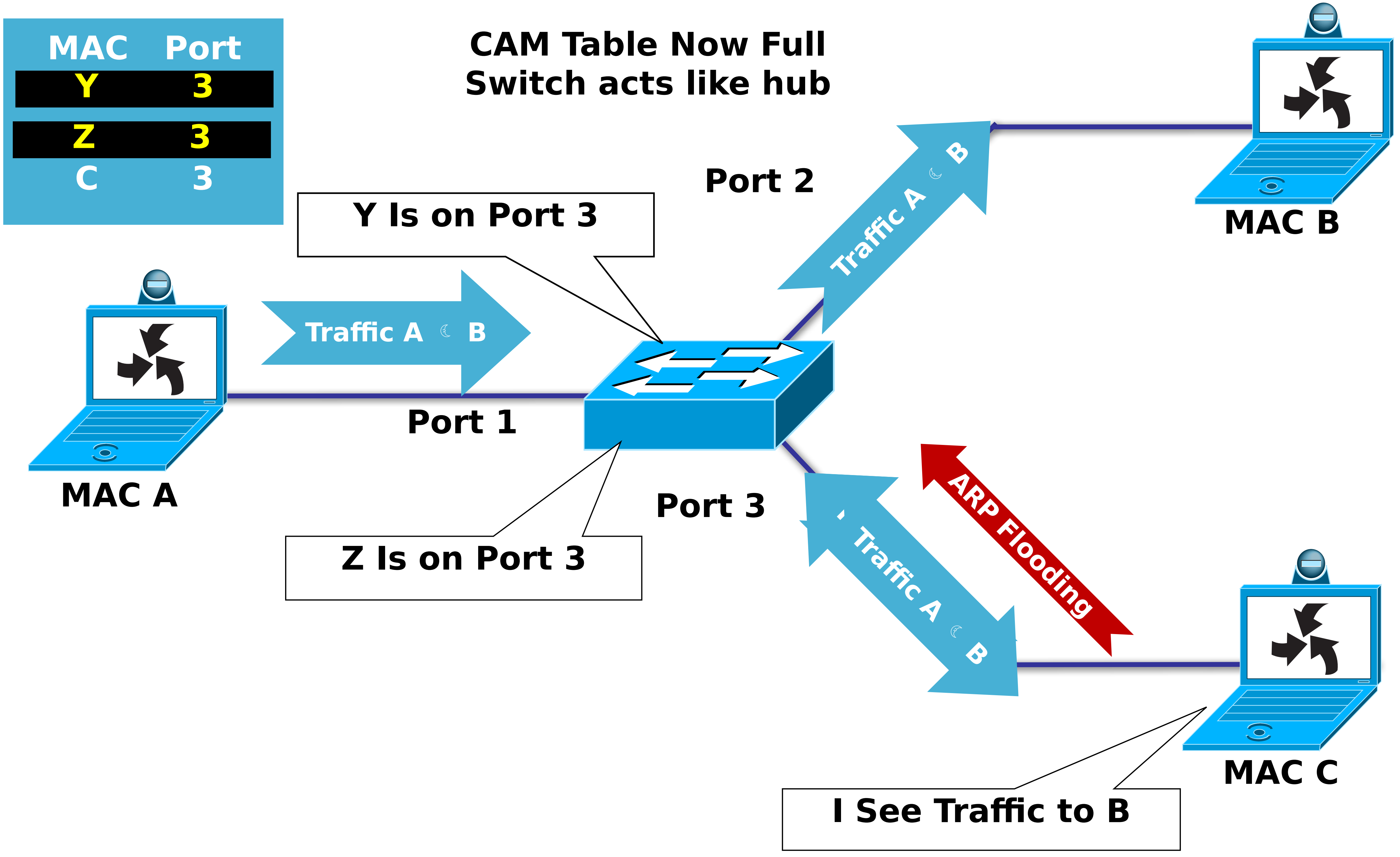


MAC	Port
A	1
B	2
C	3

B Is on Port 2

Does Not See Traffic to B

CAM Overflow Attack



MAC	Port
Y	3
Z	3
C	3

CAM Table Now Full
Switch acts like hub

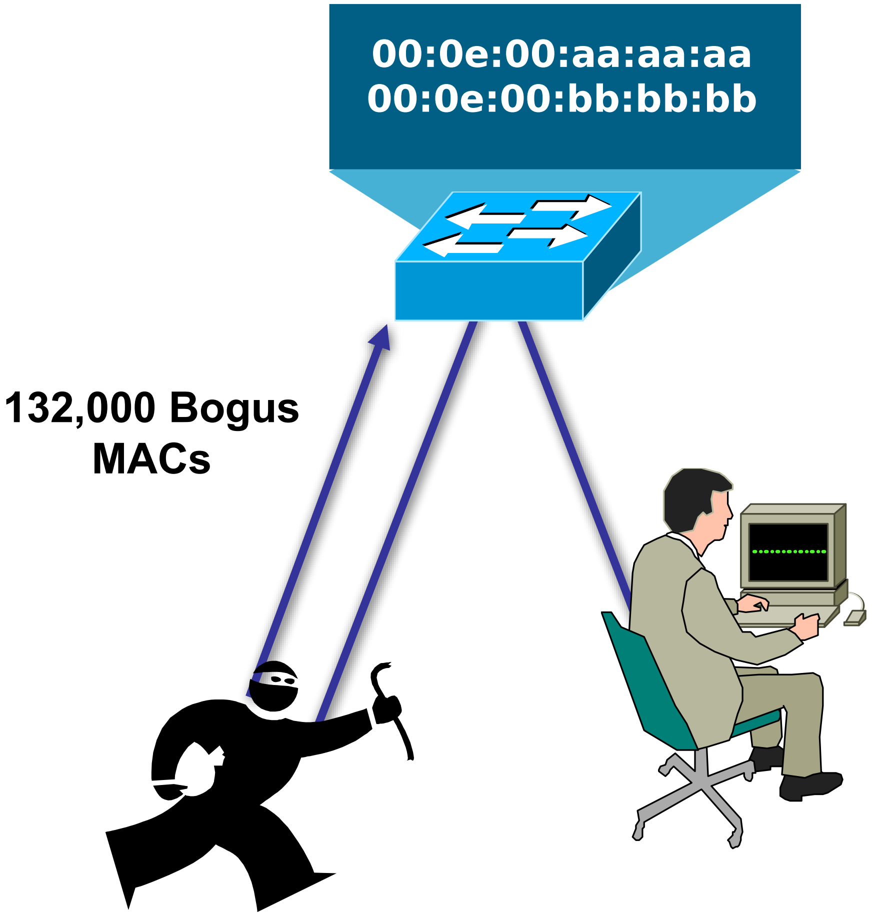
Y Is on Port 3

Z Is on Port 3

I See Traffic to B

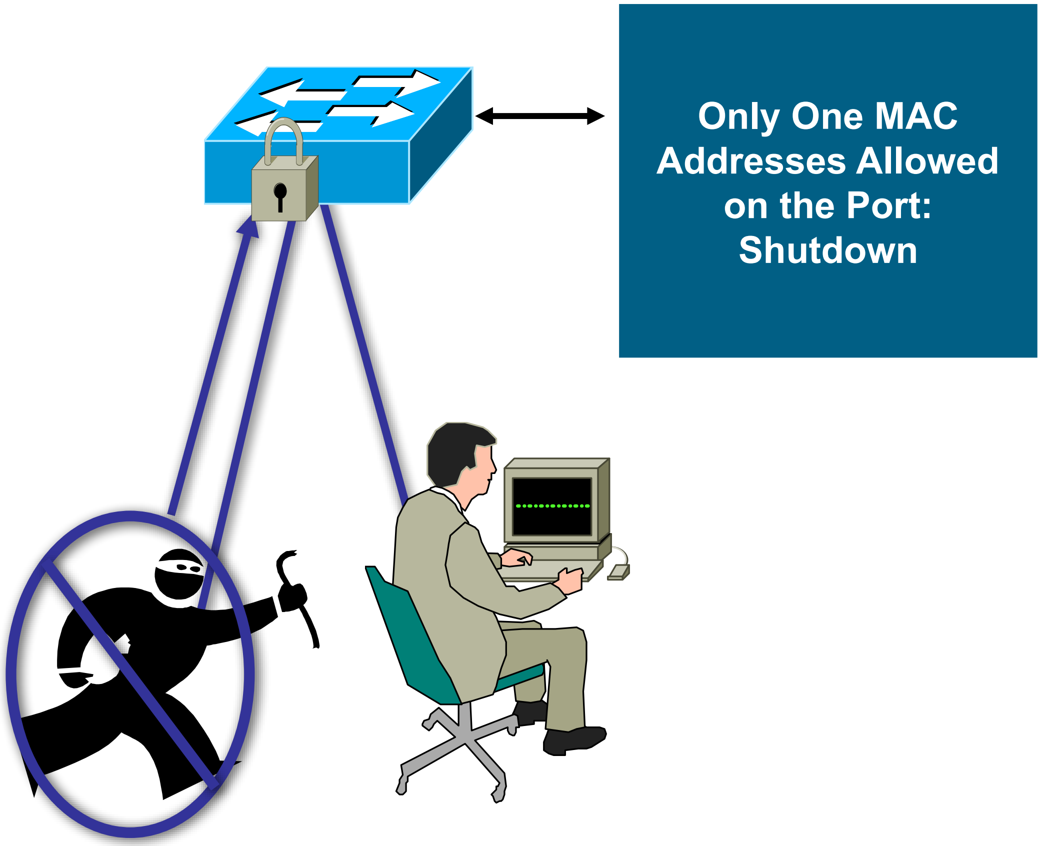
Countermeasures for MAC Attacks: Port Security

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
- May need to allow multiple MAC address on a port, say, for IP Phones

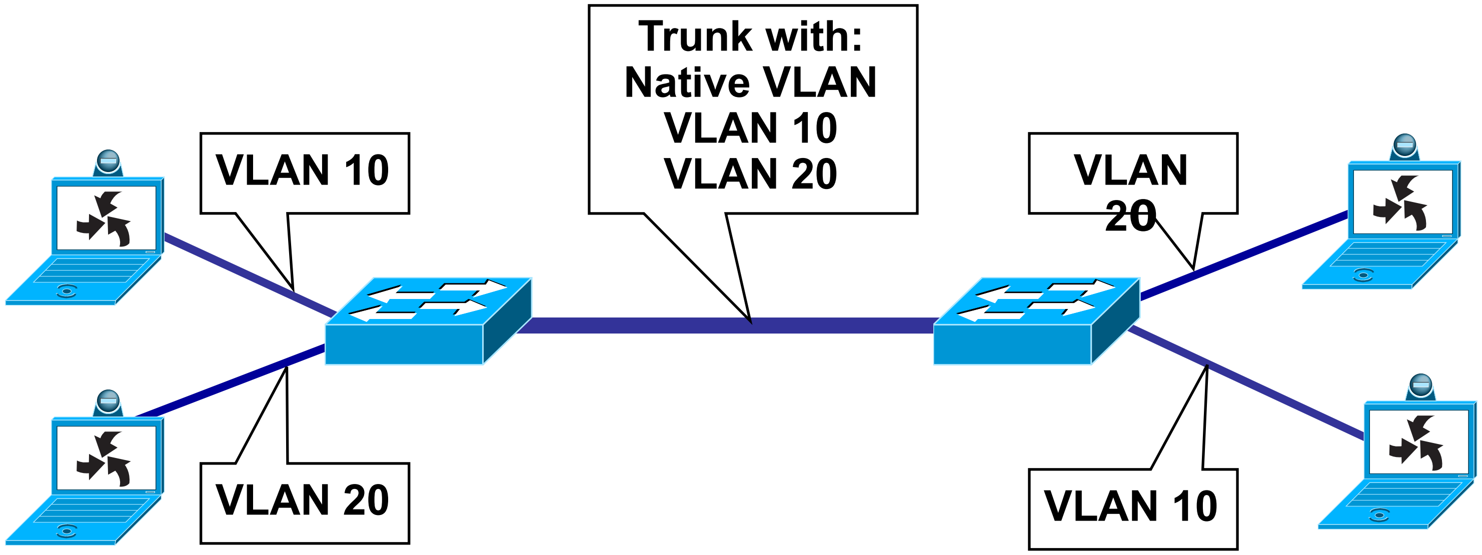


Port Security

- 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 on how many MAC addresses a port will learn
- You can also put timers in to state how long the MAC address will be bound to that switch port
  - “CAM Aging” – typical aging time is 5 minutes
- You might still want to do static MAC entries on ports that there should be no movement of devices, such as in server farms

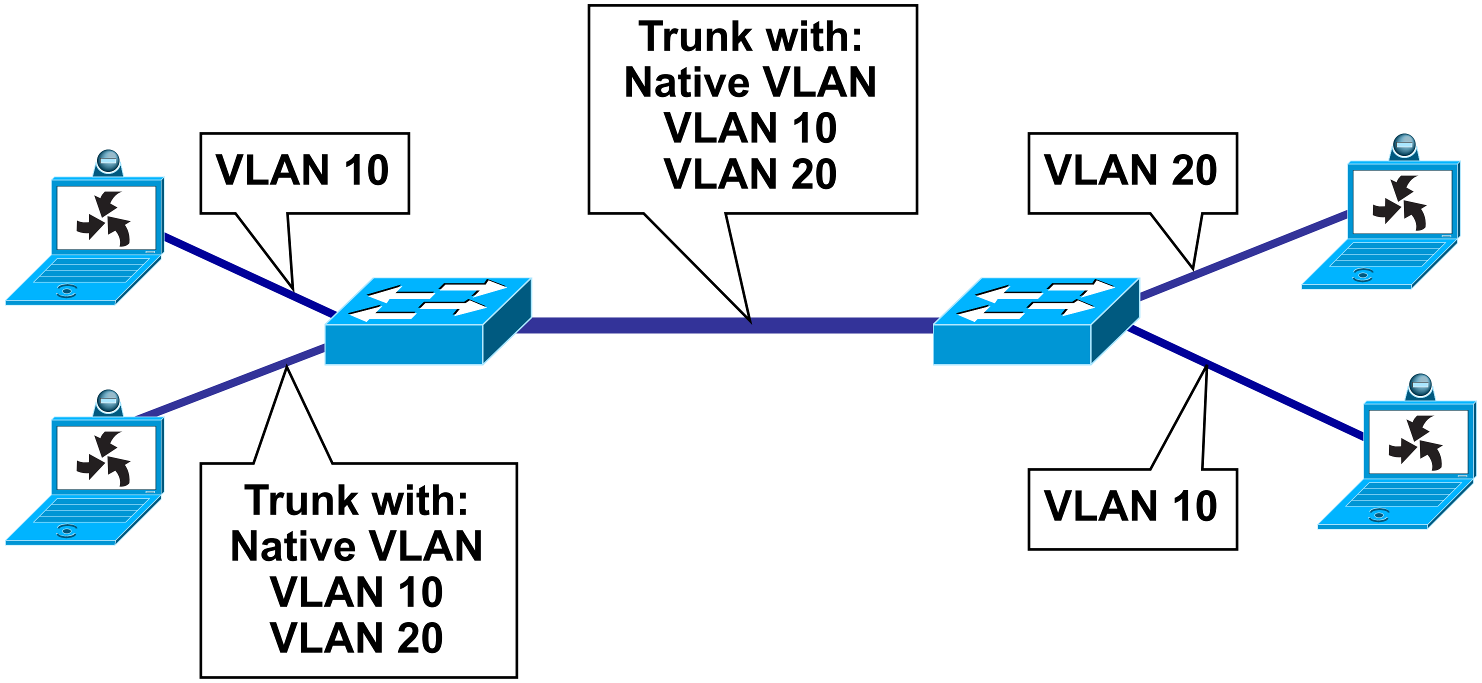
VLAN Hopping Attacks

Basic Trunk Port Defined



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

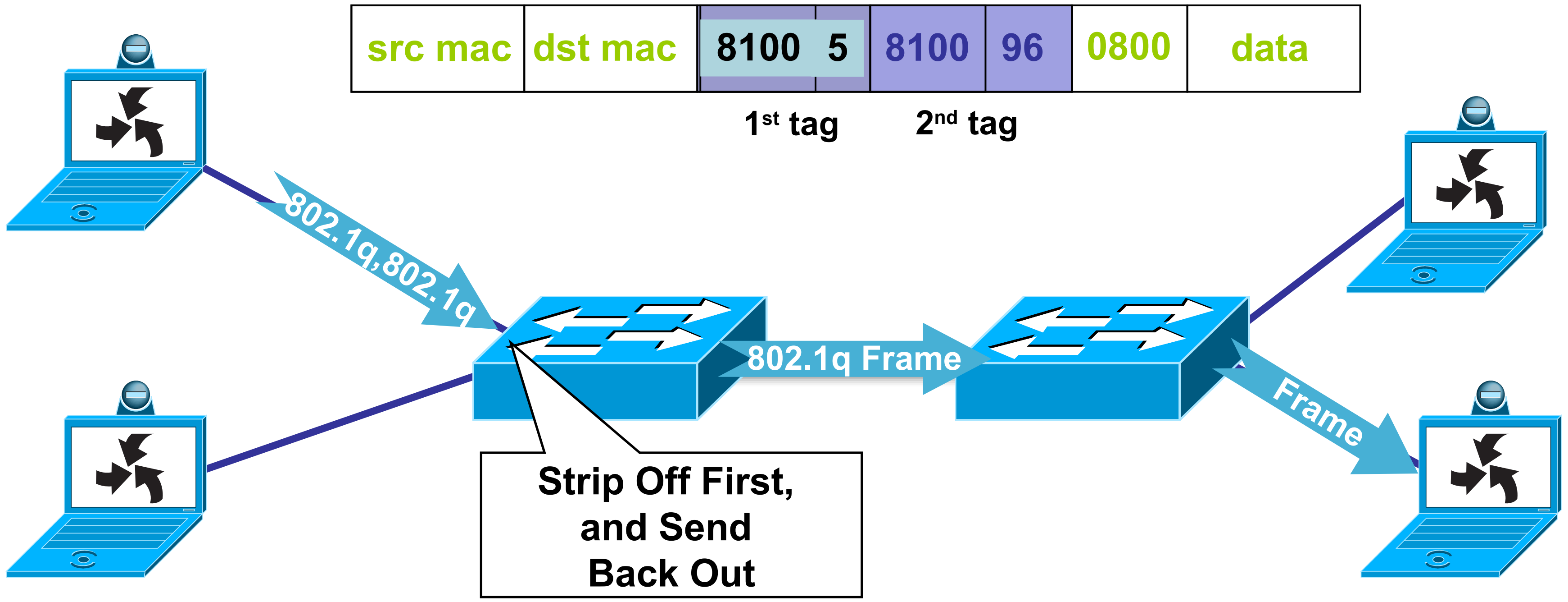
Basic VLAN Hopping Attack: Switch Spoofing



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

- Mitigations
  - Disable auto-trunking on user facing ports (DTP off)
  - Do not use VLAN 1 for user traffic as management traffic requires VLAN 1
  - Explicitly configure trunking on infrastructure ports

Double 802.1q Encapsulation VLAN Hopping Attack



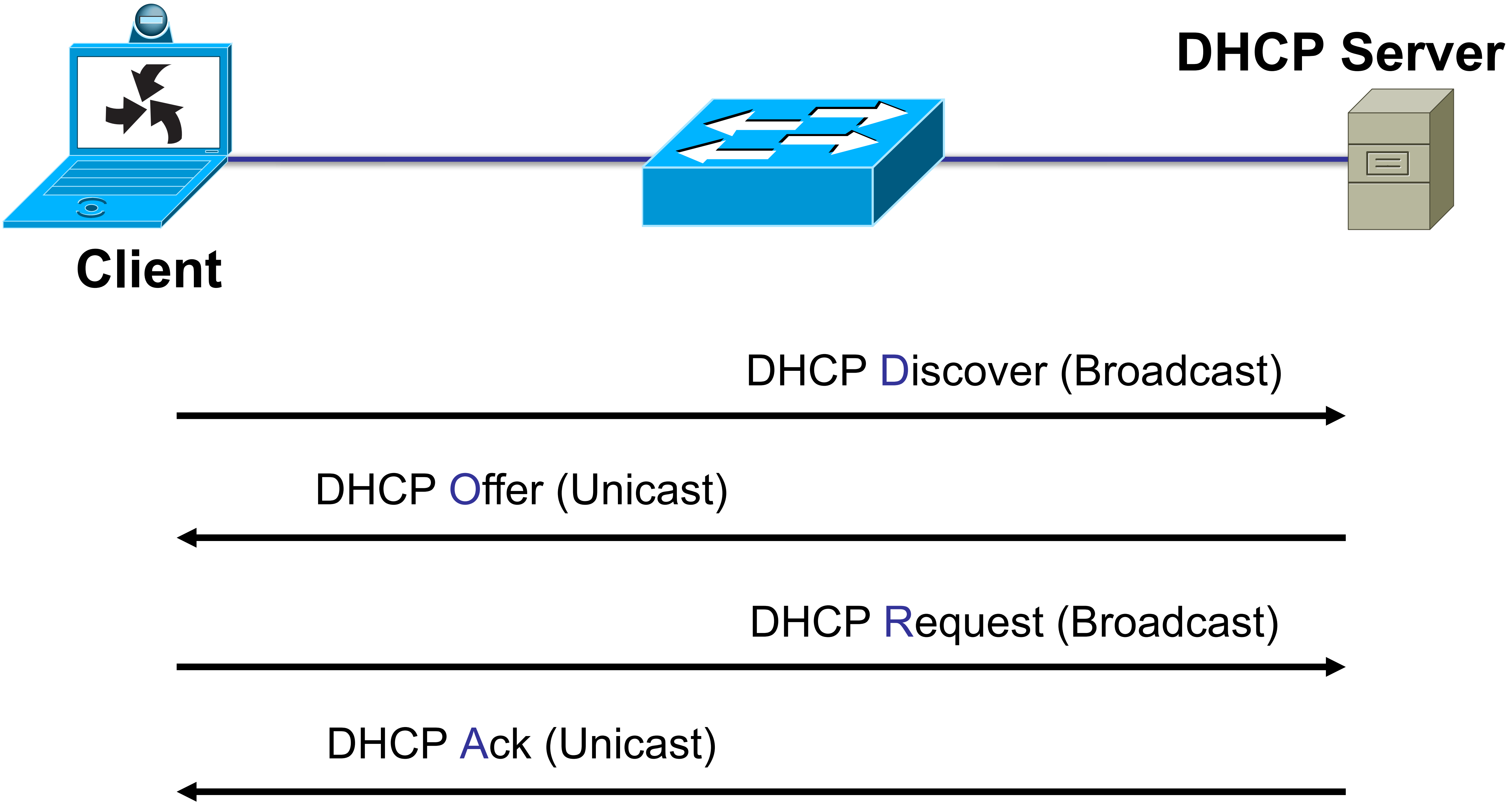
- Attacker needs to be a part of the native VLAN
- Send 802.1q double encapsulated frames
- Switch performs only one level of decapsulation
- Unidirectional traffic only
- Works even if trunk ports are set to off

Mitigations

- Explicitly set the VLAN IDs used on a trunk port
- Do not use VLAN 1 for user traffic as management traffic requires VLAN 1
- Require all VLANs to be tagged on trunks

DHCP Attacks

DHCP Function



DHCP Server

Client

DHCP Discover (Broadcast)

DHCP Offer (Unicast)

DHCP Request (Broadcast)

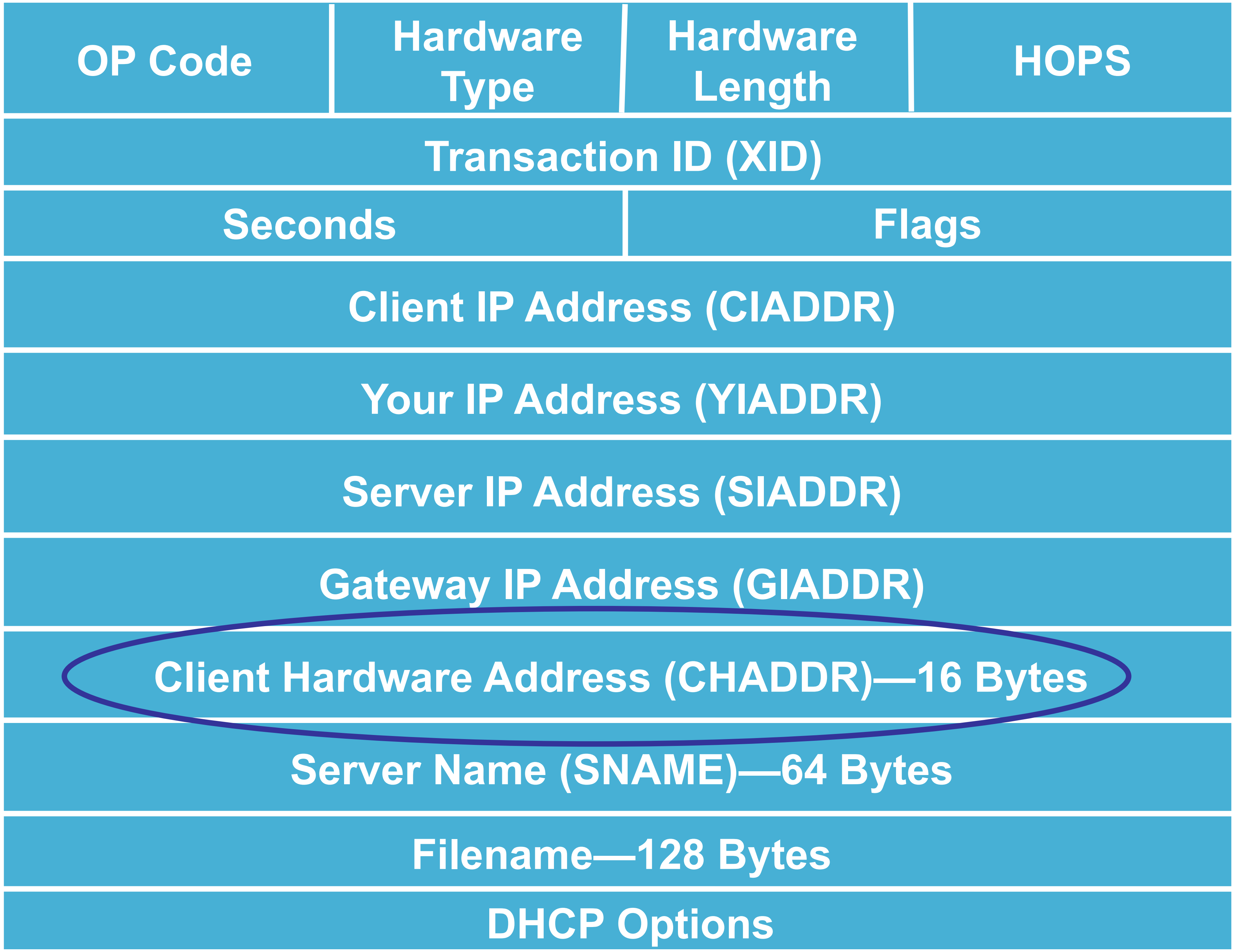
DHCP Ack (Unicast)

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

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

DHCP Function: Lower Level

IPv4 DHCP Packet Format



OP Code | Hardware Type | Hardware Length | HOPS

Transaction ID (XID)

Seconds | Flags

Client IP Address (CIADDR)

Your IP Address (YIADDR)

Server IP Address (SIADDR)

Gateway IP Address (GIADDR)

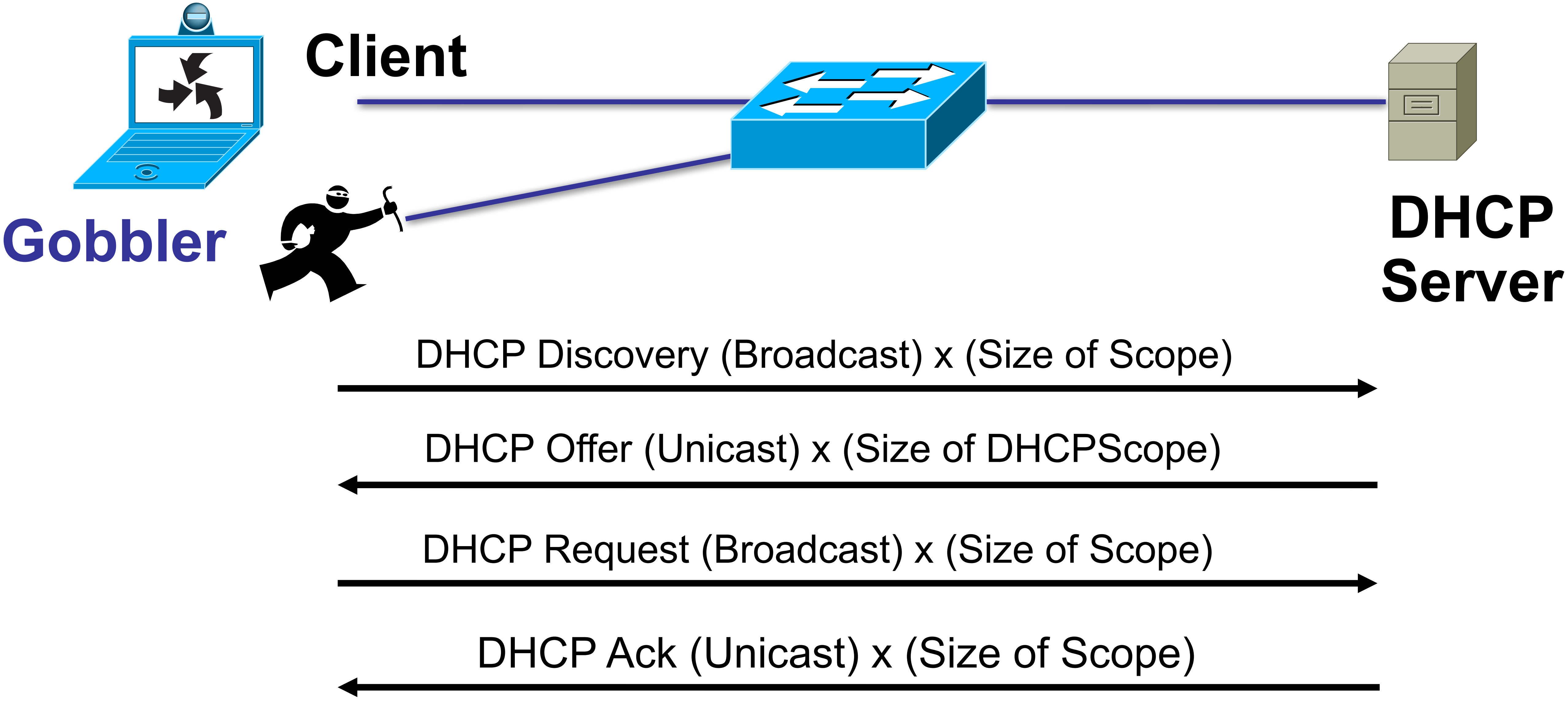
Client Hardware Address (CHADDR)—16 Bytes

Server Name (SNAME)—64 Bytes

Filename—128 Bytes

DHCP Options

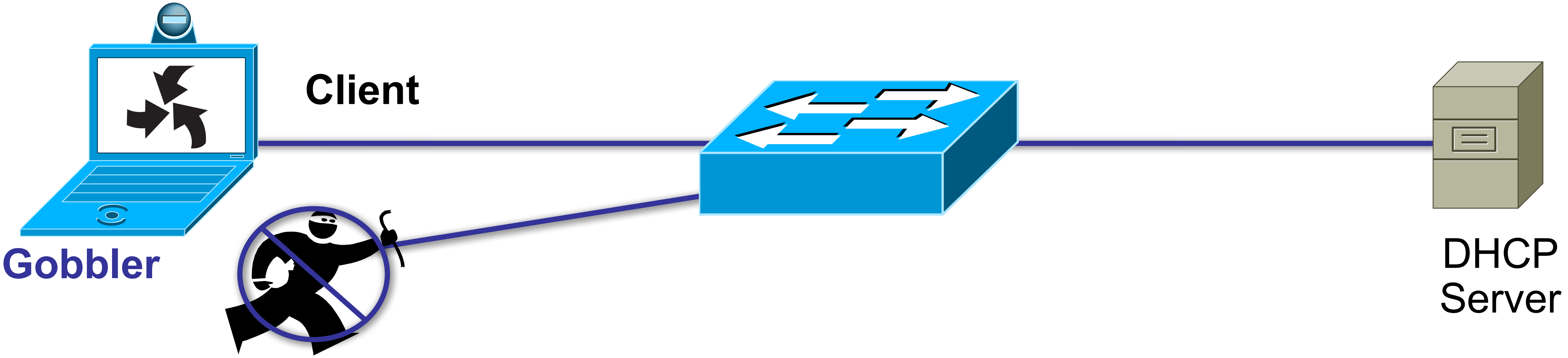
DHCP Attack Types - DHCP Starvation Attack


Client
Gobbler
DHCP Server
DHCP Discovery (Broadcast) x (Size of Scope)
DHCP Offer (Unicast) x (Size of DHCPScope)
DHCP Request (Broadcast) x (Size of Scope)
DHCP Ack (Unicast) x (Size of Scope)

- Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope
- This is a Denial of Service DoS attack using DHCP leases
- There are types of Starvation attacks: using the Discovery Messages, or using the Request messages

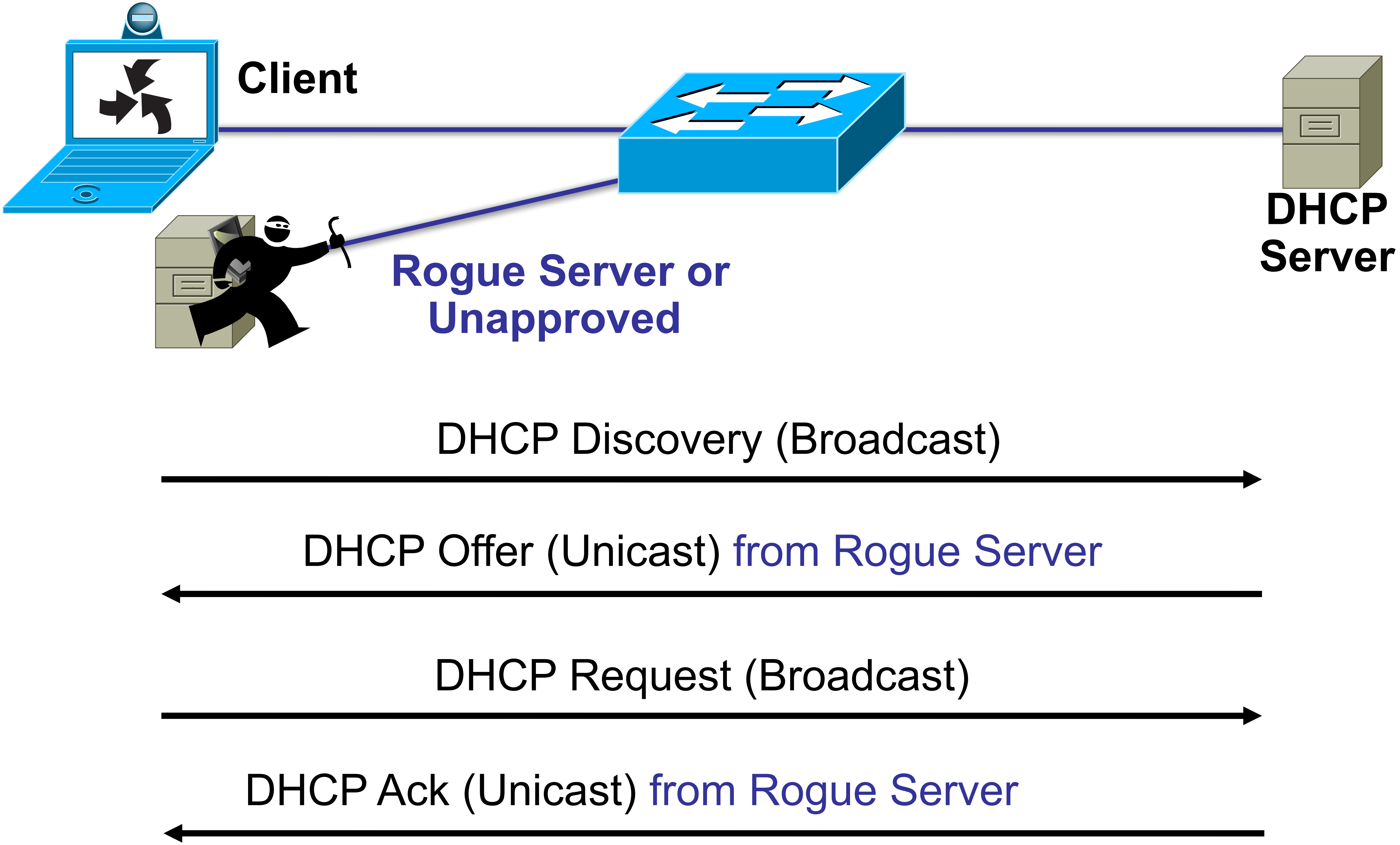
Countermeasures for DHCP Attacks

DHCP Starvation Attack = Port Security



- Gobbler uses a new MAC address to request a new DHCP lease
- Port security - 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

DHCP Attack Types - Rogue DHCP Server Attack



Client

DHCP Server

Rogue Server or Unapproved

DHCP Discovery (Broadcast) →

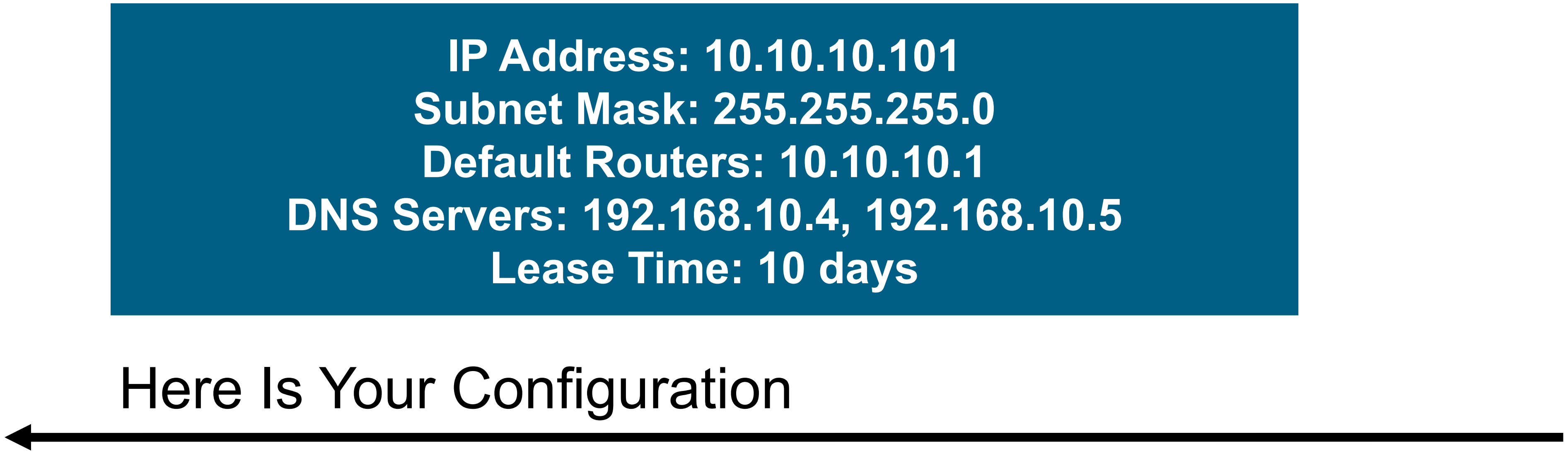
← DHCP Offer (Unicast) from Rogue Server

DHCP Request (Broadcast) →

← DHCP Ack (Unicast) from Rogue Server

DHCP Attack Types -Rogue DHCP Server Attack

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

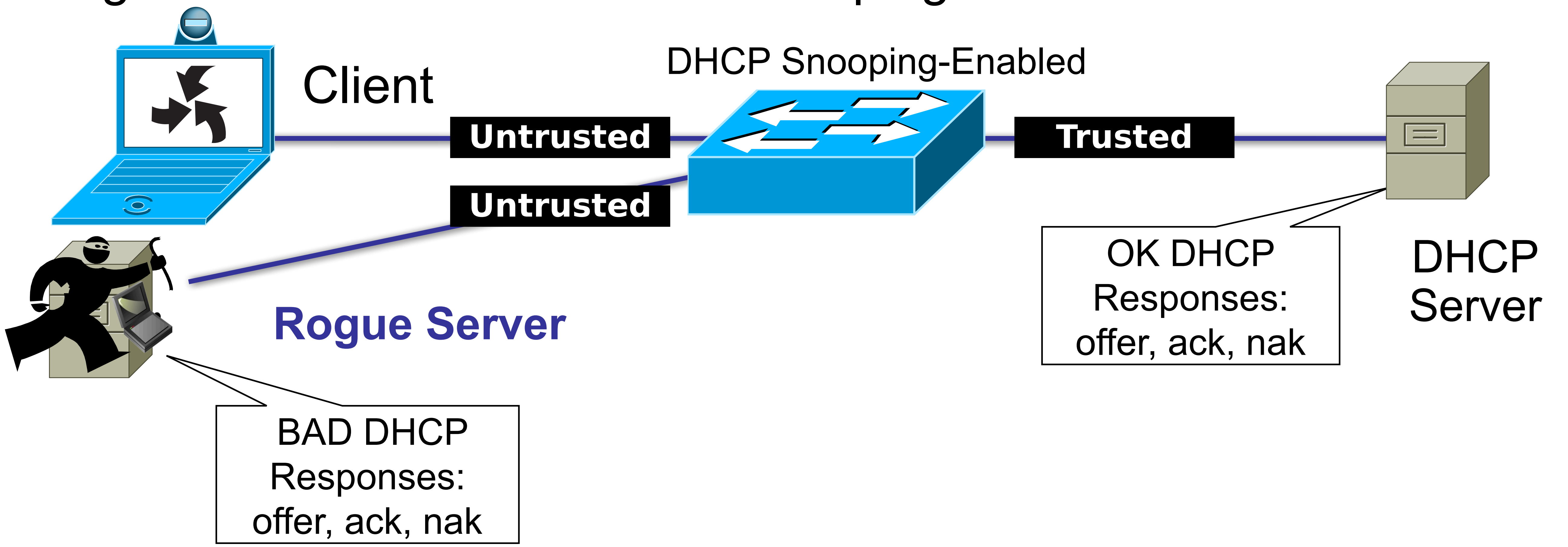


IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease Time: 10 days

Here Is Your Configuration

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

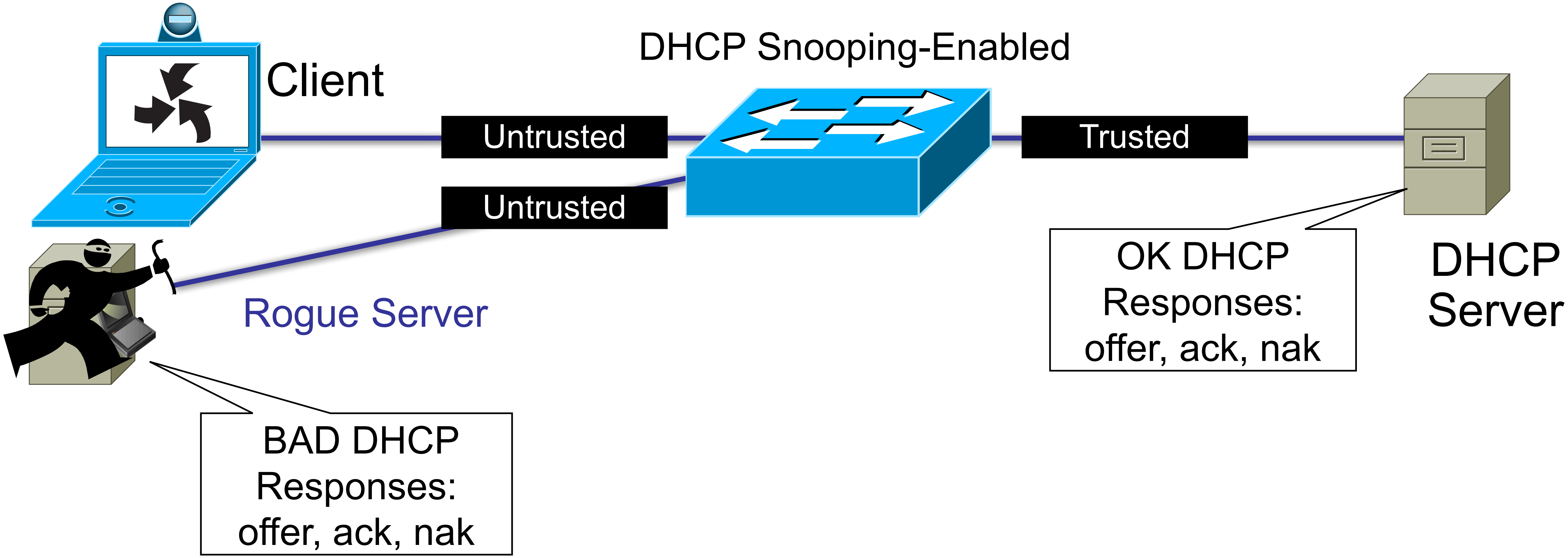
Countermeasures for DHCP Attacks
Rogue DHCP Server = DHCP Snooping



- Enable "DHCP Snooping" feature on switch
  - Set interface on the DHCP server to be trusted
  - Disable trust on other interfaces
  - Limit the rate of DHCP request from client

- DHCP Snooping is supported on most higher-end routers/switches

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

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

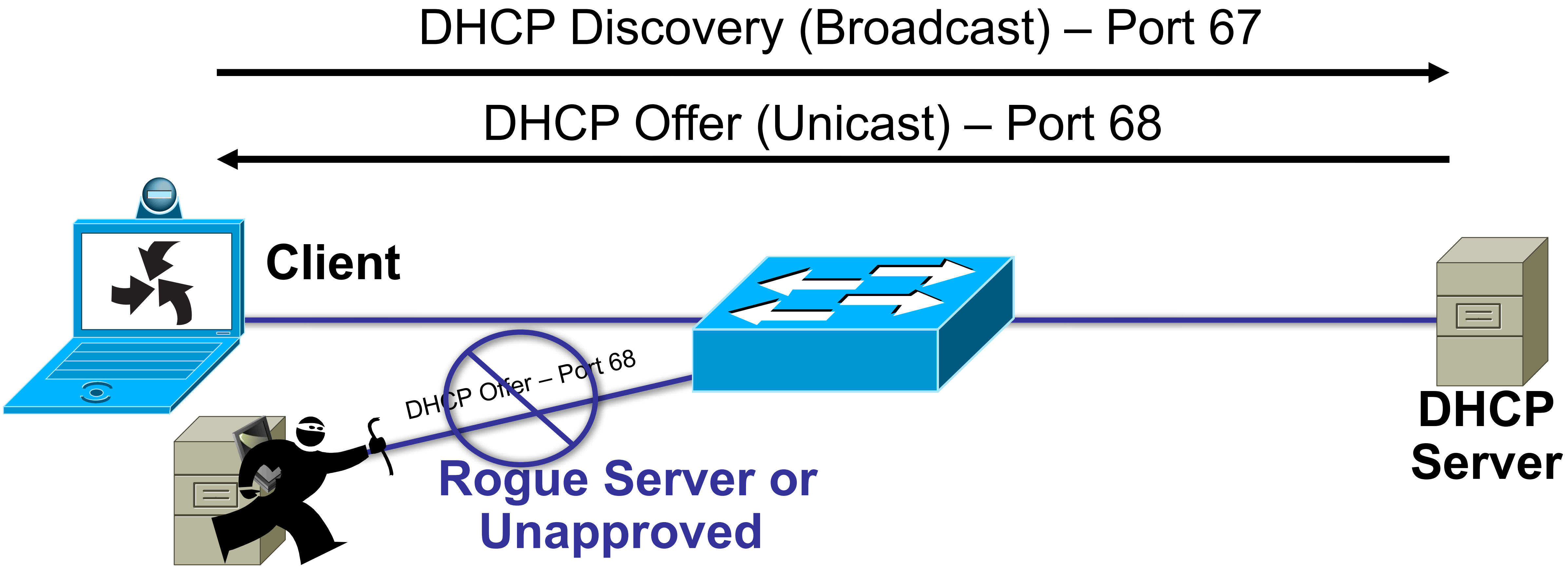
<table>
<tr><td>OP Code</td><td>Hardware Type</td><td>Hardware Length</td><td>HOPS</td></tr>
<tr><td colspan="4">Transaction ID (XID)</td></tr>
<tr><td colspan="2">Seconds</td><td colspan="2">Flags</td></tr>
<tr><td colspan="4">Client IP Address (CIADDR)</td></tr>
<tr><td colspan="4">Your IP Address (YIADDR)</td></tr>
<tr><td colspan="4">Server IP Address (SIADDR)</td></tr>
<tr><td colspan="4">Gateway IP Address (GIADDR)</td></tr>
<tr><td colspan="4">Client Hardware Address (CHADDR)—16 Bytes</td></tr>
<tr><td colspan="4">Server Name (SNAME)—64 Bytes</td></tr>
<tr><td colspan="4">Filename—128 Bytes</td></tr>
<tr><td colspan="4">DHCP Options</td></tr>
</table>

Note: Some switches have this on by default, and other's don't;

please check the documentation for settings

DHCP Rogue Server

- If there are switches in the network that will not support DHCP snooping, you can configure VLAN ACLs to block UDP port 68


DHCP Discovery (Broadcast) – Port 67
DHCP Offer (Unicast) – Port 68
Client
DHCP Offer – Port 68
Rogue Server or Unapproved
DHCP Server

- Will not prevent the CHADDR DHCP starvation attack

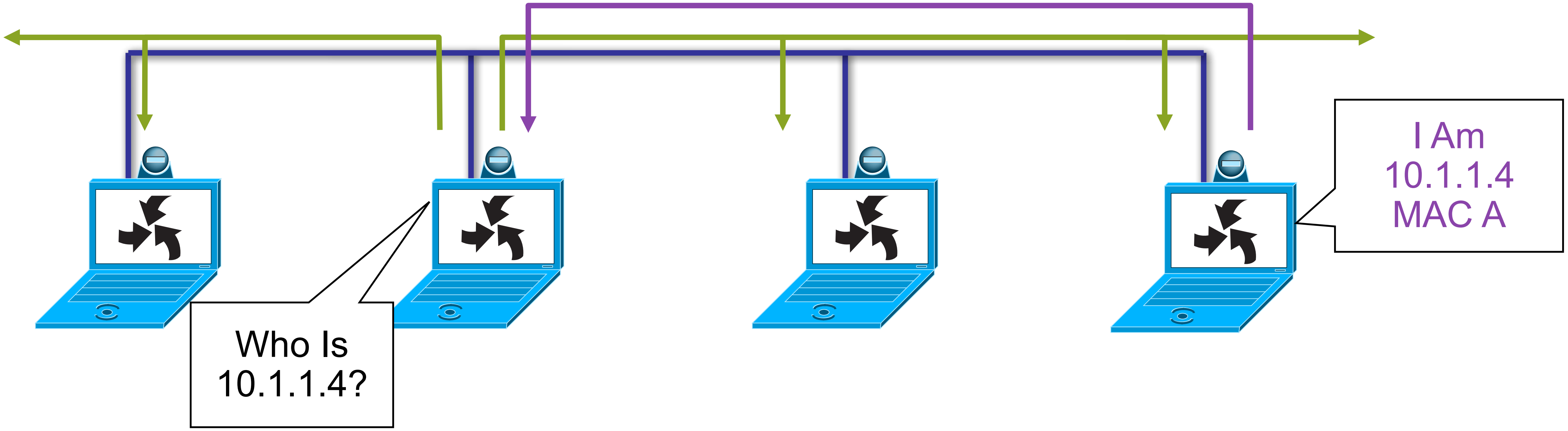
Summary of DHCP Attacks

- 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)

ARP Attacks

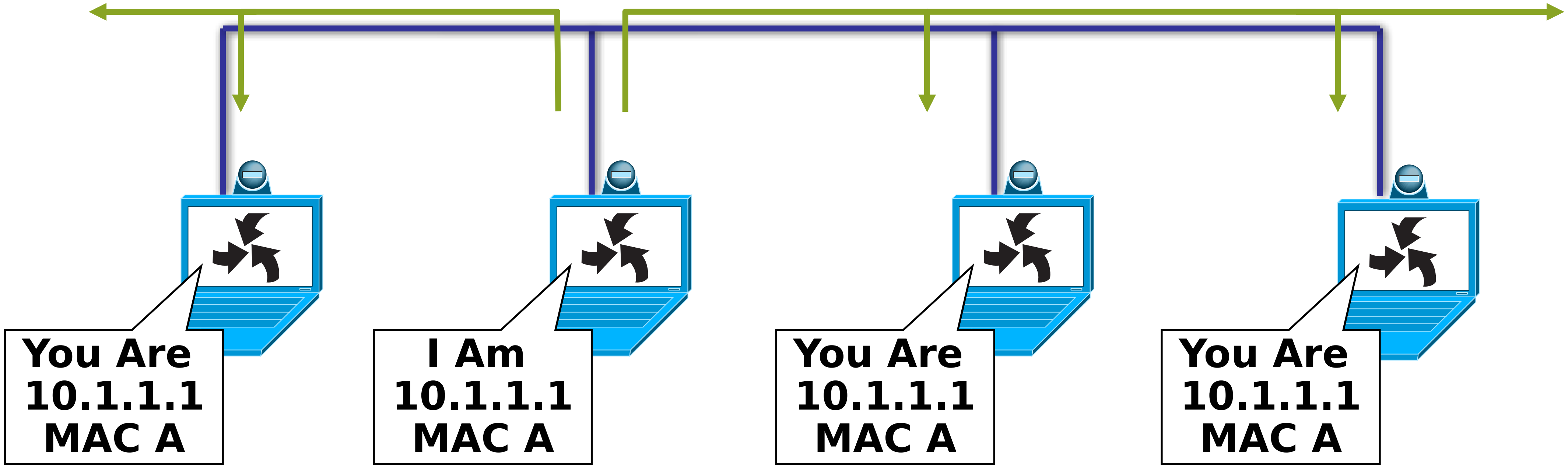
ARP Function Review

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



ARP Function Review

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



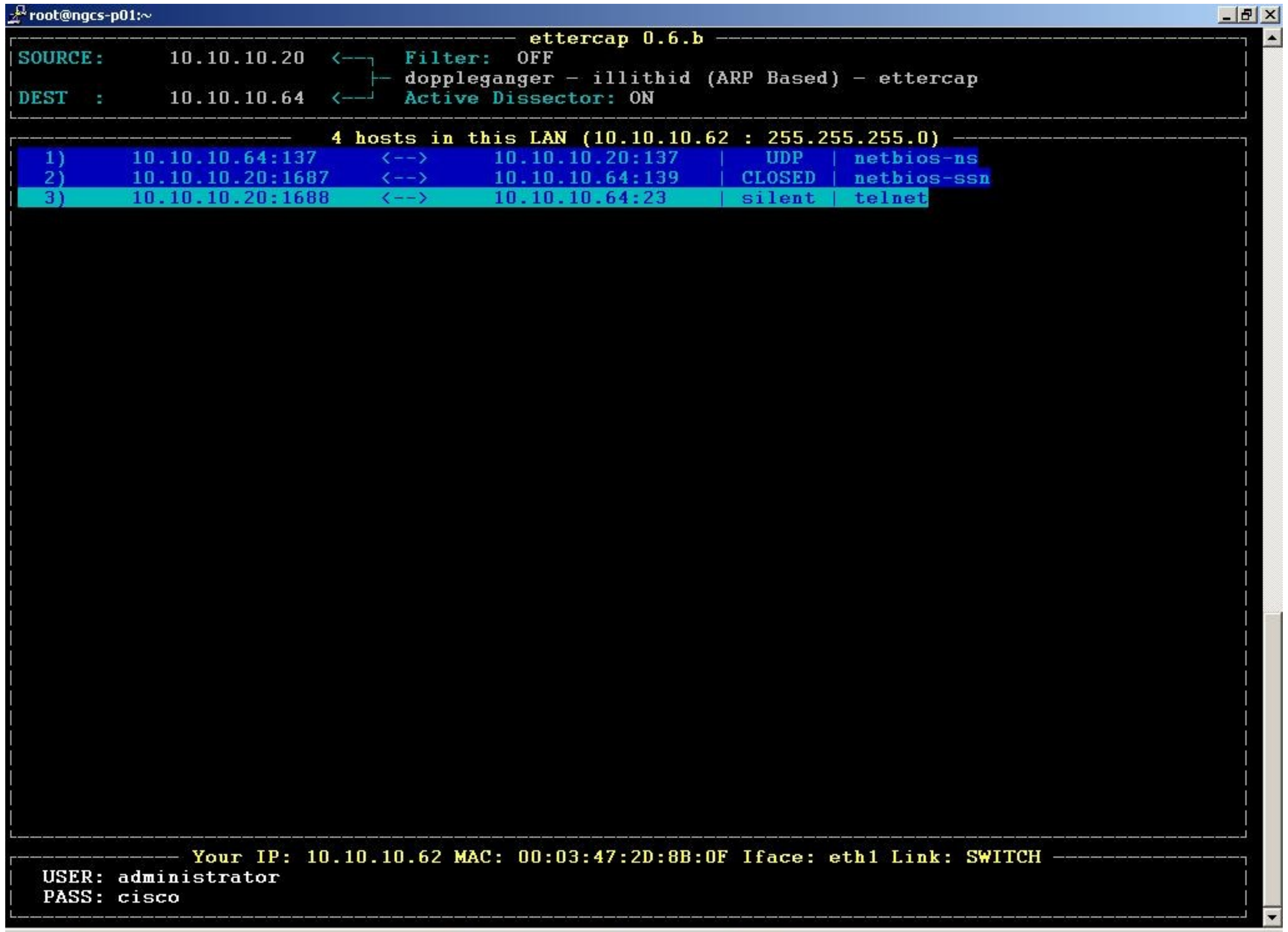
ARP Request/Reply Example

“Who has [B IP]? Tell [A IP]”
Ethernet Header
Dst MAC: (ff:ff:ff:ff:ff:ff)
Src MAC: [A’s MAC]
ARP Header
Type: Request
Sender MAC: [A’s MAC]
Sender IP: [A’s IP]
Target MAC: ff:ff:ff:ff:ff:ff
Target IP: [B’s IP]

“[B’s IP] is at [B’s MAC]”
Ethernet Header
Dst MAC: [A’s MAC] If gratuitous: ff:ff:ff:ff:ff:ff
Src MAC: [B’s MAC]
ARP Header
Type: Reply
Sender MAC: [B’s MAC]
Sender IP: [B’s IP]
Target MAC: [A’s MAC] If gratuitious: ff:ff:ff:ff:ff:ff
Target IP: [A’s IP]

ARP Attack Tools

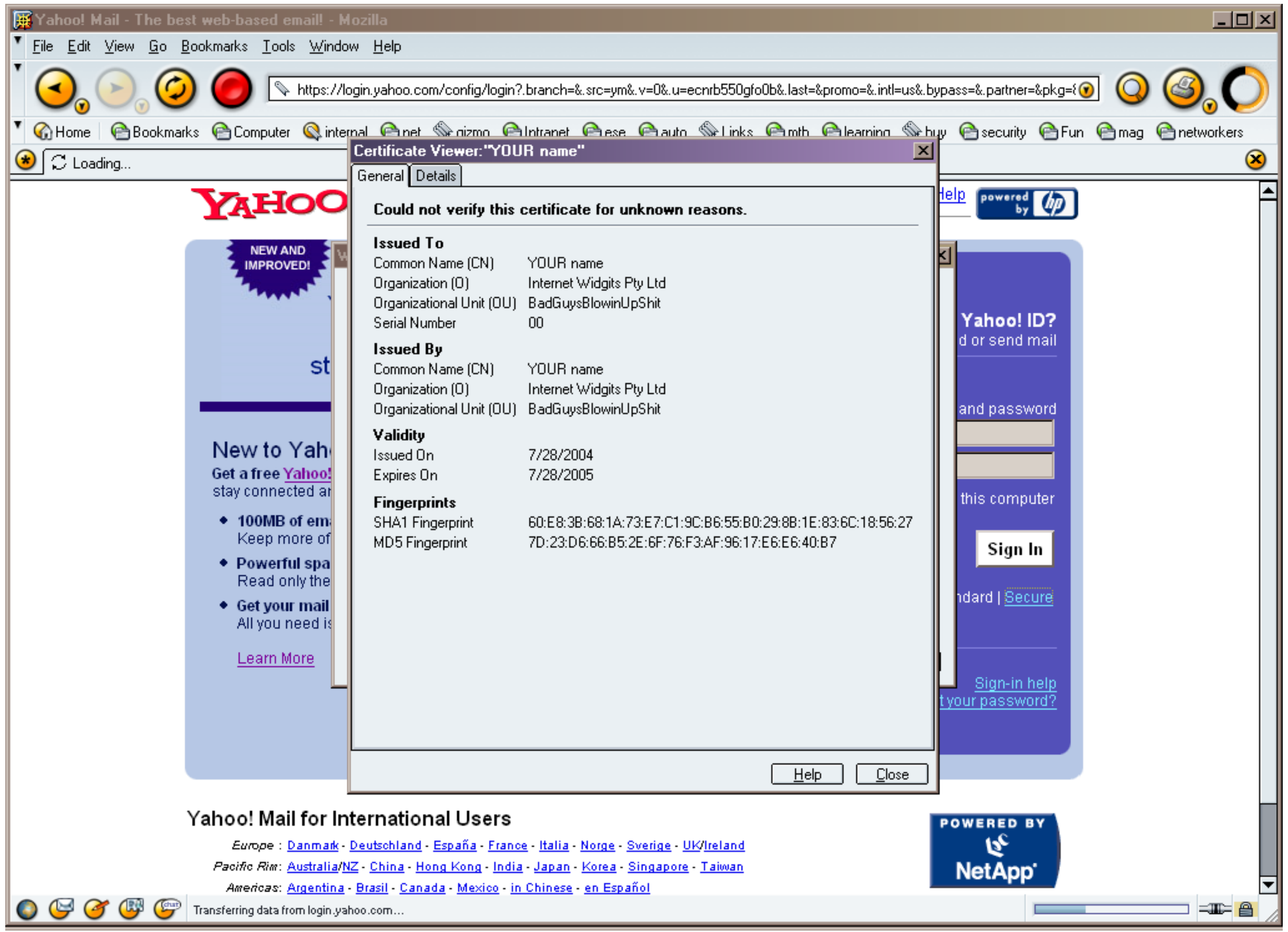
- Many tools on the net for ARP man-in-the-middle attacks
  - Dsniff, Cain & Abel, ettercap, Yersinia, etc.
- ettercap: http://ettercap.sourceforge.net/index.php
  - Decodes passwords on the fly
- Most have a very nice GUI, and is almost point and click
- Packet insertion, many to many ARP attack
- All of them capture the traffic/passwords of common applications
- SSL/SSH sessions can be intercepted and bogus certificate credentials can be presented to perform MITM attack



root@ngcs-p01:~

```
--------------------------------------- ettercap 0.6.b ----------------------------------------
|SOURCE:      10.10.10.20  <--┐  Filter:  OFF                                                 |
|                             ├─ doppleganger - illithid (ARP Based) - ettercap                 |
|DEST  :      10.10.10.64  <--┘  Active Dissector: ON                                          |
-----------------------------------------------------------------------------------------------
---------------------- 4 hosts in this LAN (10.10.10.62 : 255.255.255.0) ----------------------
|  1)     10.10.10.64:137    <-->     10.10.10.20:137   |  UDP   | netbios-ns                  |
|  2)     10.10.10.20:1687   <-->     10.10.10.64:139   | CLOSED | netbios-ssn                 |
|  3)     10.10.10.20:1688   <-->     10.10.10.64:23    | silent | telnet                      |

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



Yahoo! Mail - The best web-based email! - Mozilla

https://login.yahoo.com/config/login?.branch=&.src=ym&.v=0&.u=ecnrb550gfo0b&.last=&promo=&.intl=us&.bypass=&.partner=&pkg=

Certificate Viewer:"YOUR name"

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN) YOUR name
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) BadGuysBlowinUpShit
Serial Number 00

Issued By

Common Name (CN) YOUR name
Organization (O) Internet Widgits Pty Ltd
Organizational Unit (OU) BadGuysBlowinUpShit

Validity

Issued On 7/28/2004
Expires On 7/28/2005

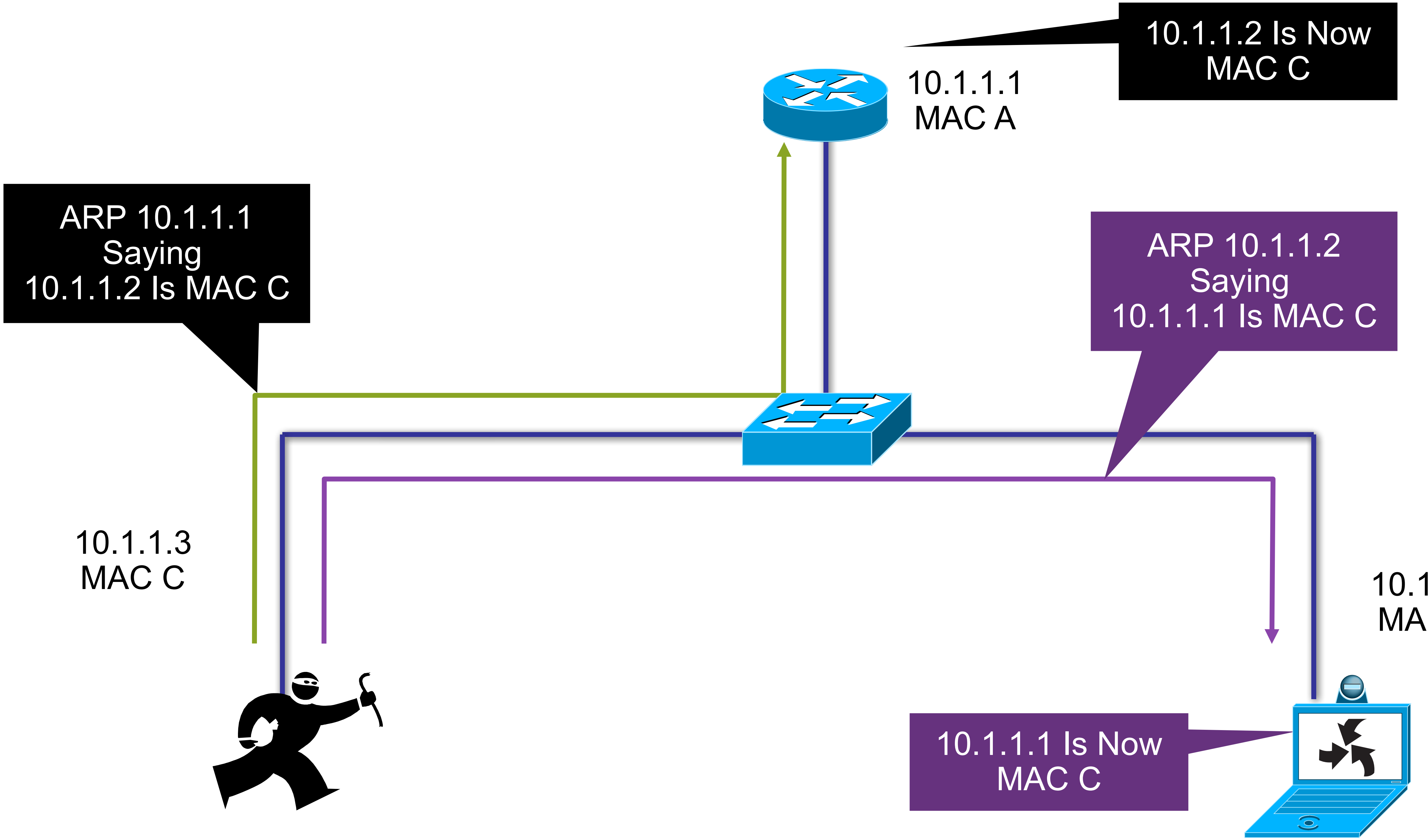
Fingerprints

SHA1 Fingerprint 60:E8:3B:68:1A:73:E7:C1:9C:B6:55:B0:29:8B:1E:83:6C:18:56:27
MD5 Fingerprint 7D:23:D6:66:B5:2E:6F:76:F3:AF:96:17:E6:E6:40:B7

Transferring data from login.yahoo.com...

ARP Attack in Action

- Attacker “poisons” the ARP tables



10.1.1.2 Is Now MAC C

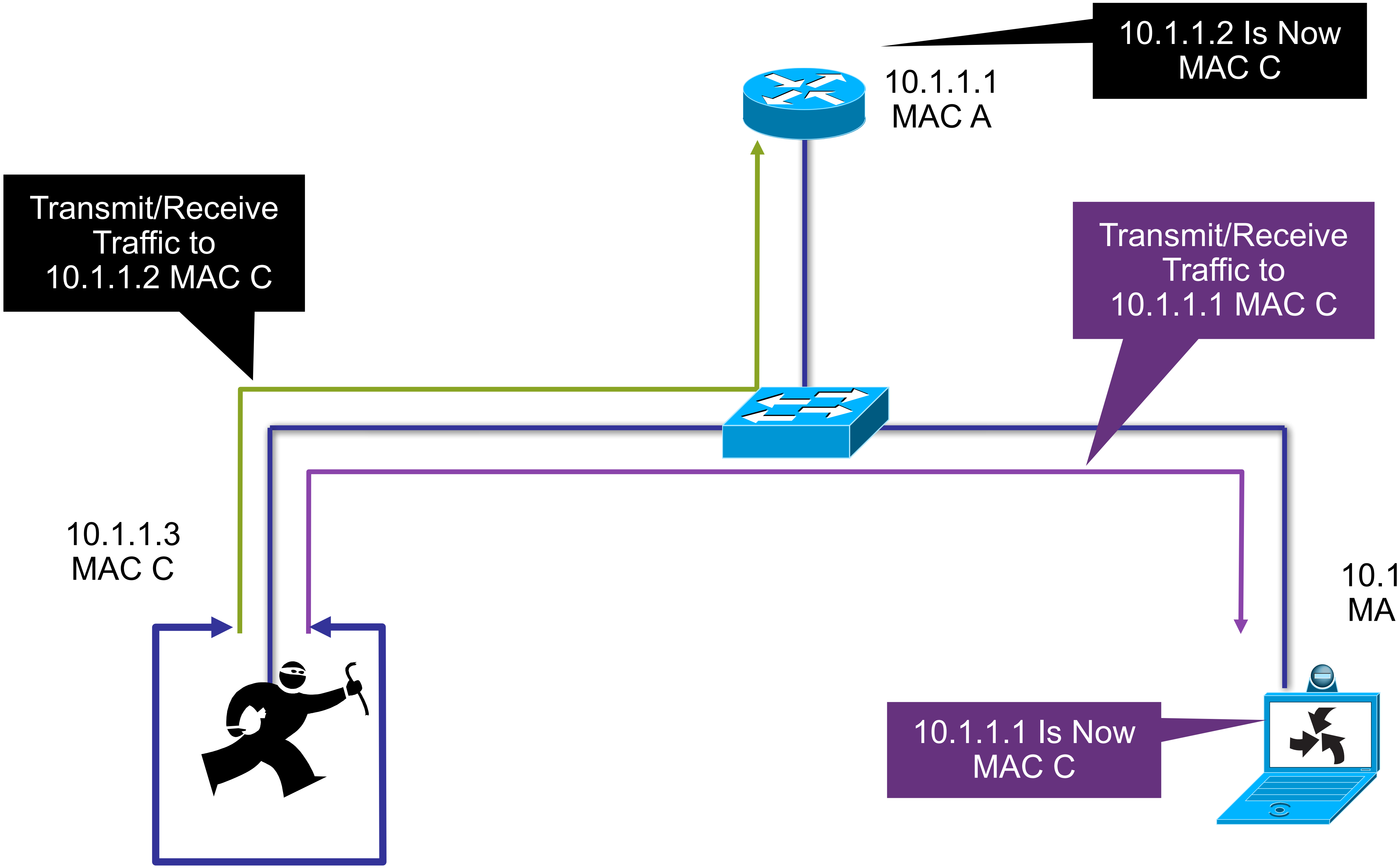
ARP 10.1.1.1 Saying 10.1.1.2 Is MAC C

ARP 10.1.1.2 Saying 10.1.1.1 Is MAC C

10.1.1.1 Is Now MAC C

ARP Attack in Action

- All traffic flows through the attacker



10.1.1.2 Is Now MAC C

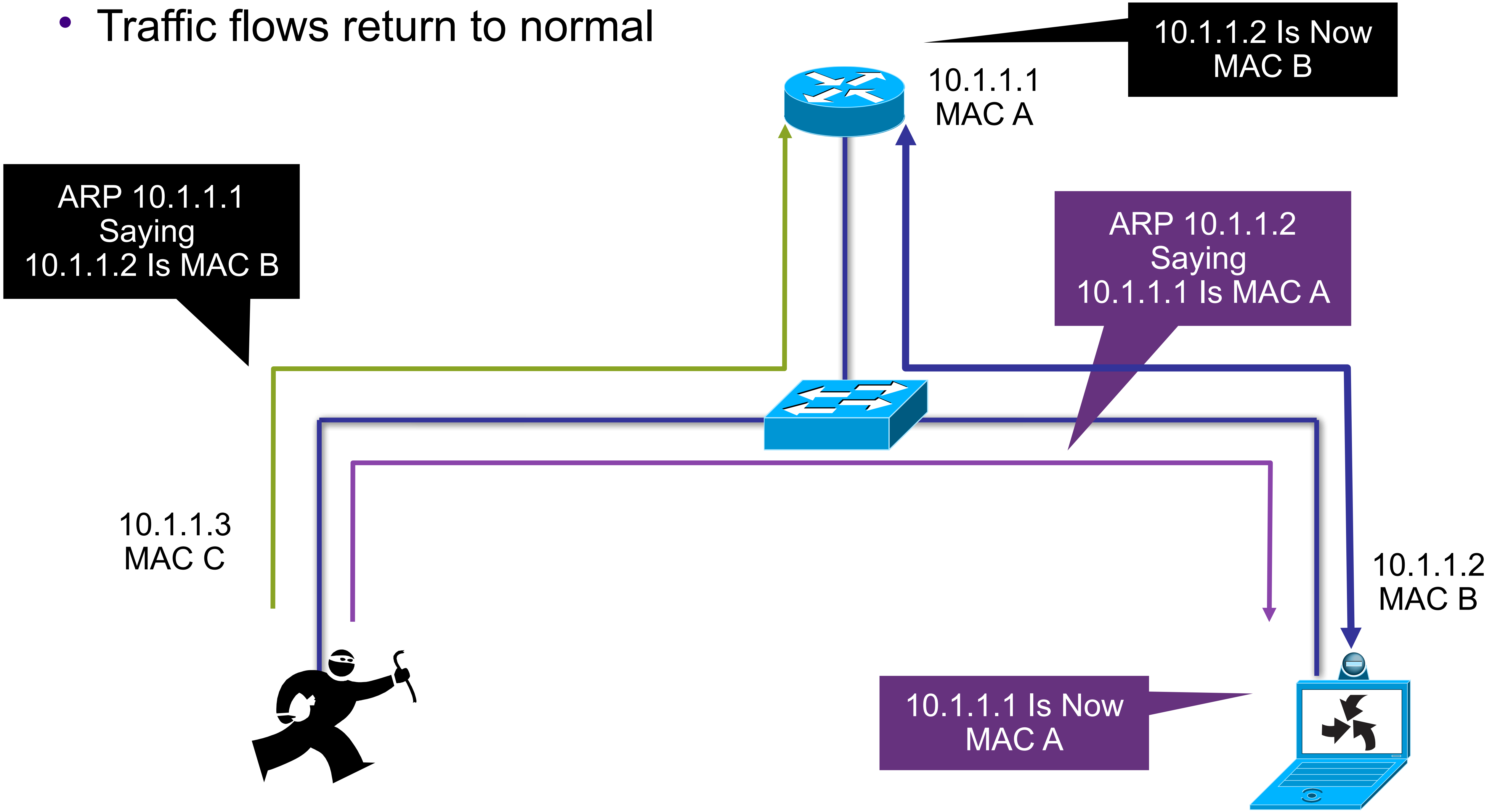
Transmit/Receive Traffic to 10.1.1.2 MAC C

Transmit/Receive Traffic to 10.1.1.1 MAC C

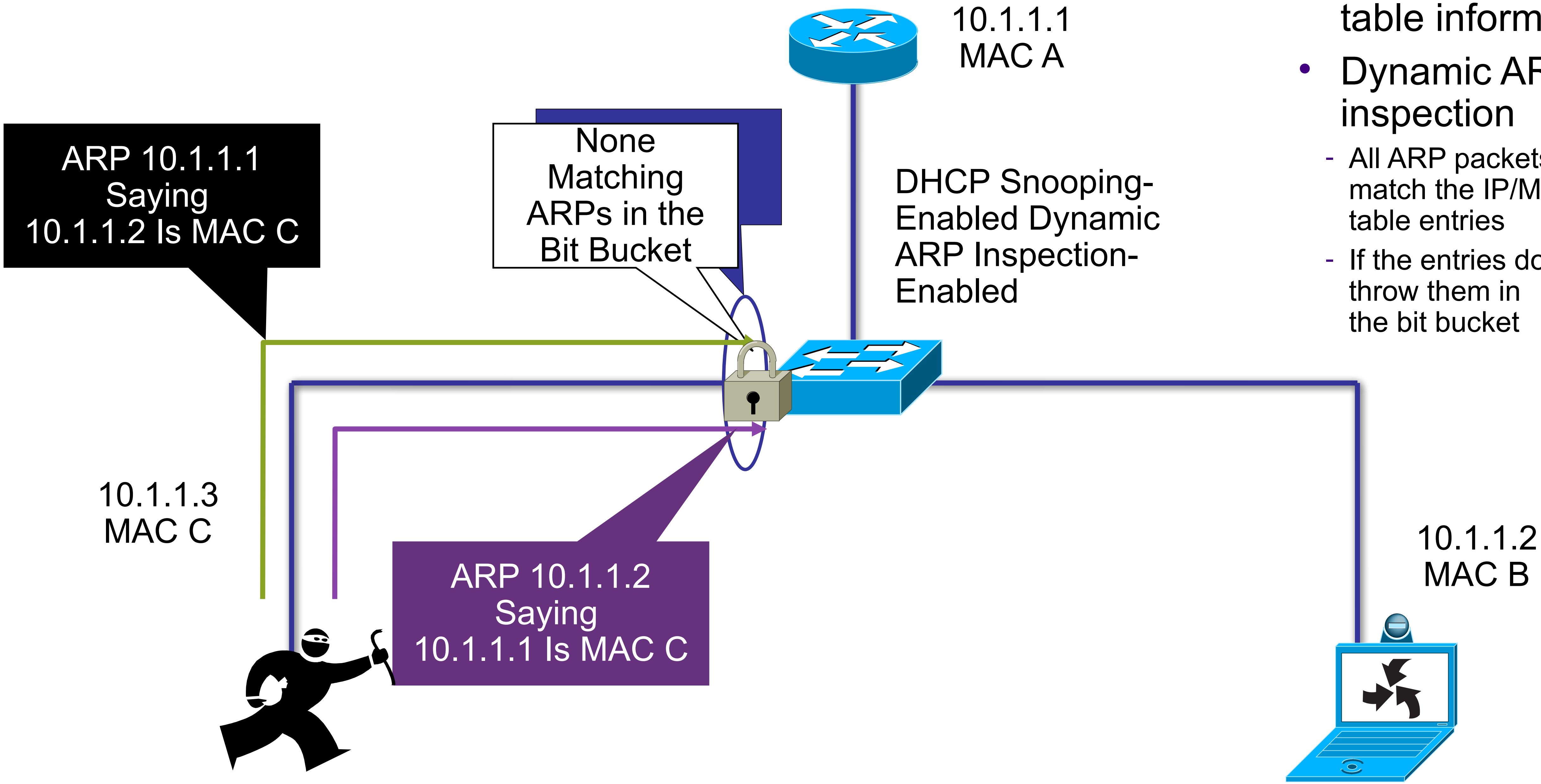
10.1.1.1 Is Now MAC C

ARP Attack Clean Up

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



Countermeasures to ARP Attacks: Dynamic ARP Inspection (DAI)


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

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

Countermeasures to ARP Attacks: Dynamic ARP Inspection

- For Cisco devices, DHCP snooping has to be configured so the binding table is built
- DAI is configured by VLAN
- You can trust an interface like DHCP snooping

```
                              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 MAC address and IP address fields to see if the ARP from the interface is in the binding; if not, traffic is blocked

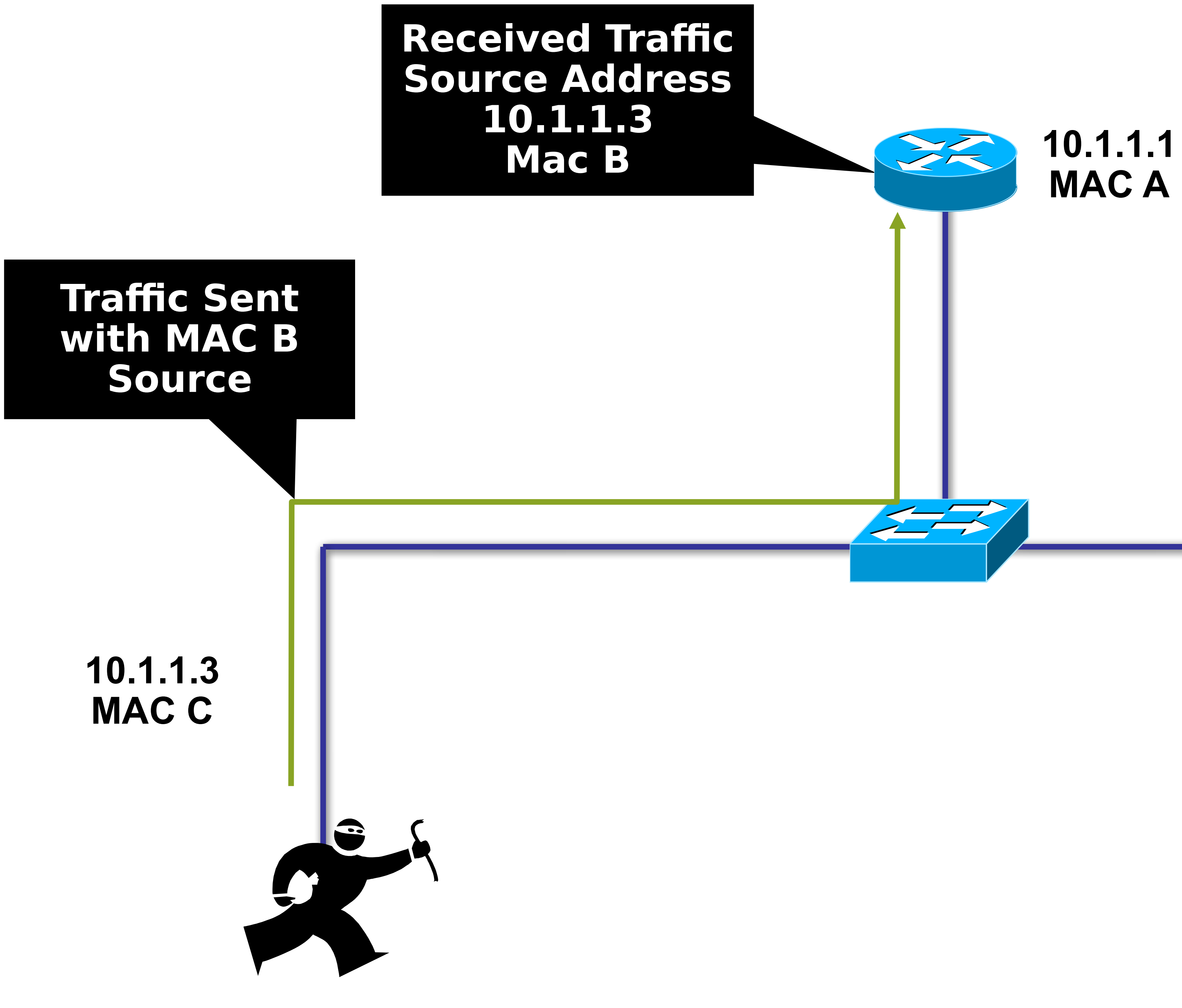
Spoofing Attacks

Spoofing Attacks

- MAC spoofing
  - If MACs are used for network access an attacker can gain access to the network
  - Also can be used to take over someone’s identity already on the network

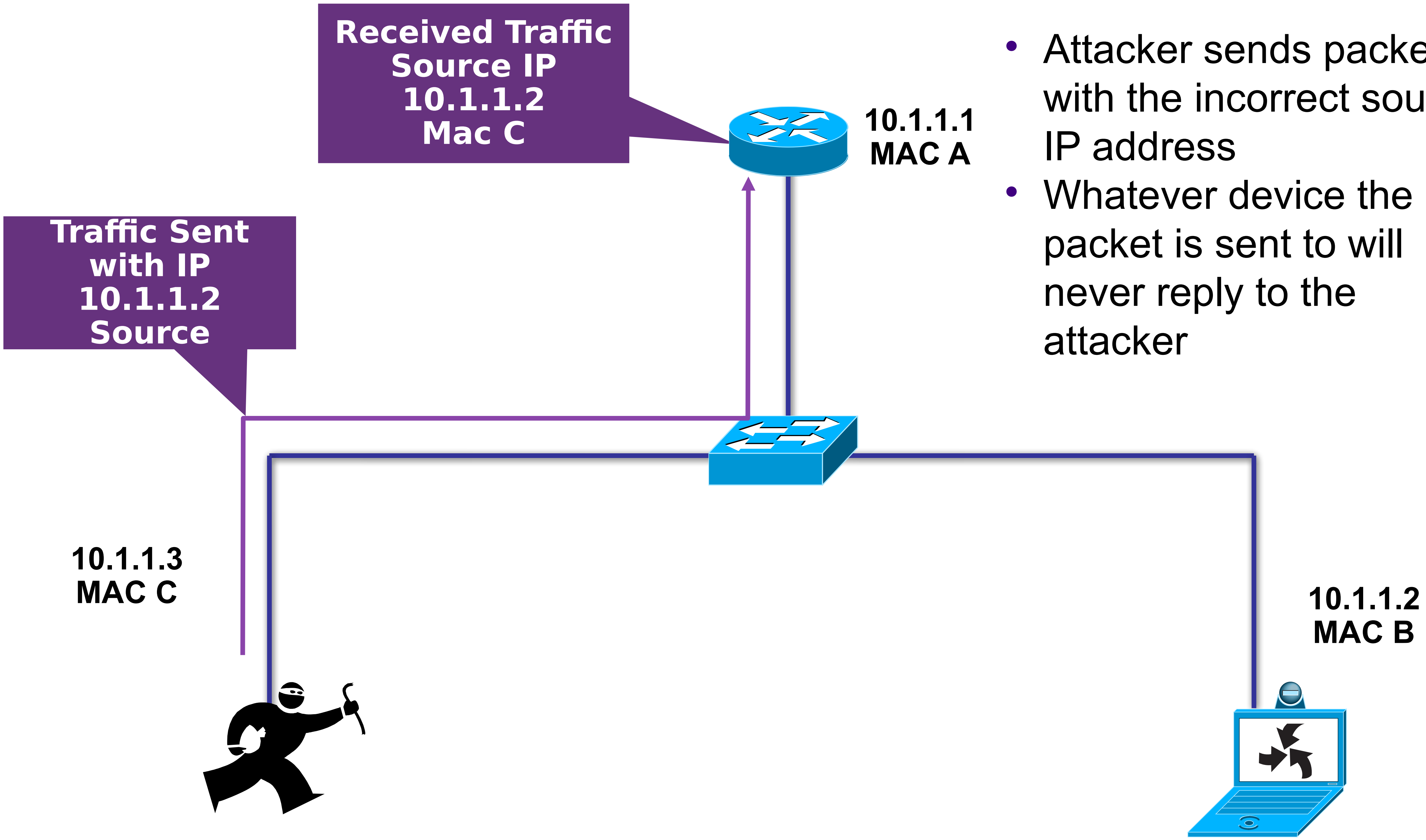
- IP spoofing
  - Ping of death
  - ICMP unreachable storm
  - SYN flood
  - Trusted IP addresses can be spoofed

Spoofing Attack: MAC



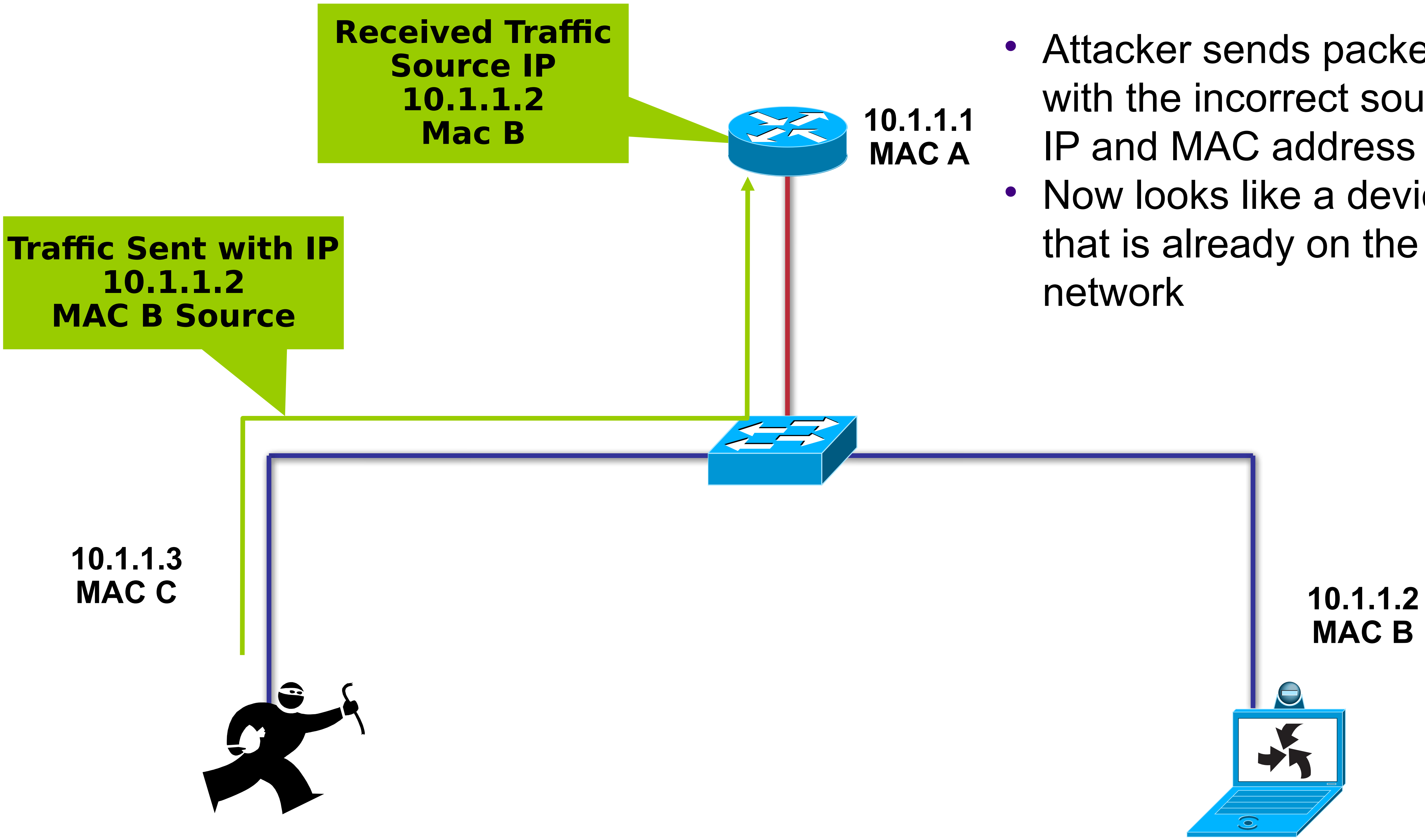
- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like 10.1.1.2

Spoofing Attack: IP


Received Traffic Source IP 10.1.1.2 Mac C
10.1.1.1
MAC A
Traffic Sent with IP 10.1.1.2 Source
10.1.1.3
MAC C
10.1.1.2
MAC B

- 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

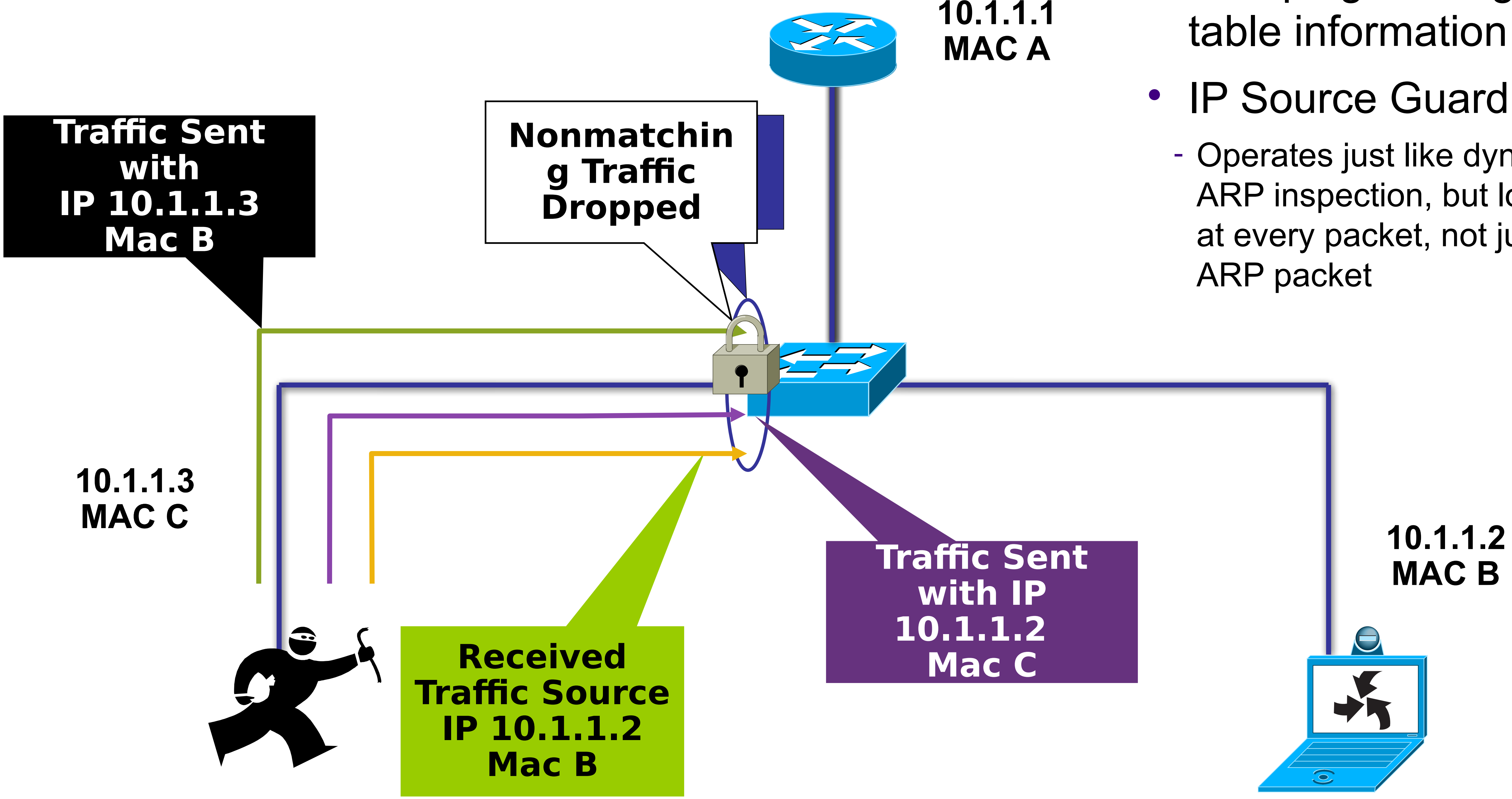


- Attacker sends packets with the incorrect source IP and MAC address
- Now looks like a device that is already on the network

NYU TANDON SCHOOL OF ENGINEERING

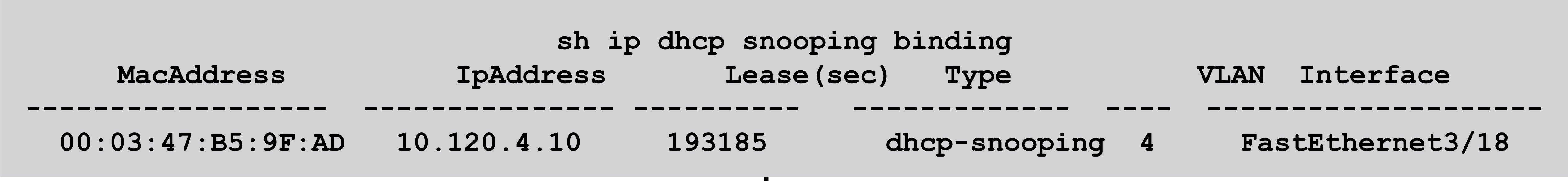
Countermeasures to Spoofing Attacks: IP Source Guard

- Uses the DHCP snooping binding table information
- IP Source Guard
  - Operates just like dynamic ARP inspection, but looks at every packet, not just ARP packet


10.1.1.1
MAC A
Traffic Sent with IP 10.1.1.3 Mac B
Nonmatching Traffic Dropped
10.1.1.3
MAC C
Received Traffic Source IP 10.1.1.2 Mac B
Traffic Sent with IP 10.1.1.2 Mac C
10.1.1.2
MAC B

Countermeasures to Spoofing Attacks: IP Source Guard

- Uses the information from the DHCP snooping binding table



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

if the traffic from the interface is in the binding table, it not, traffic is blocked

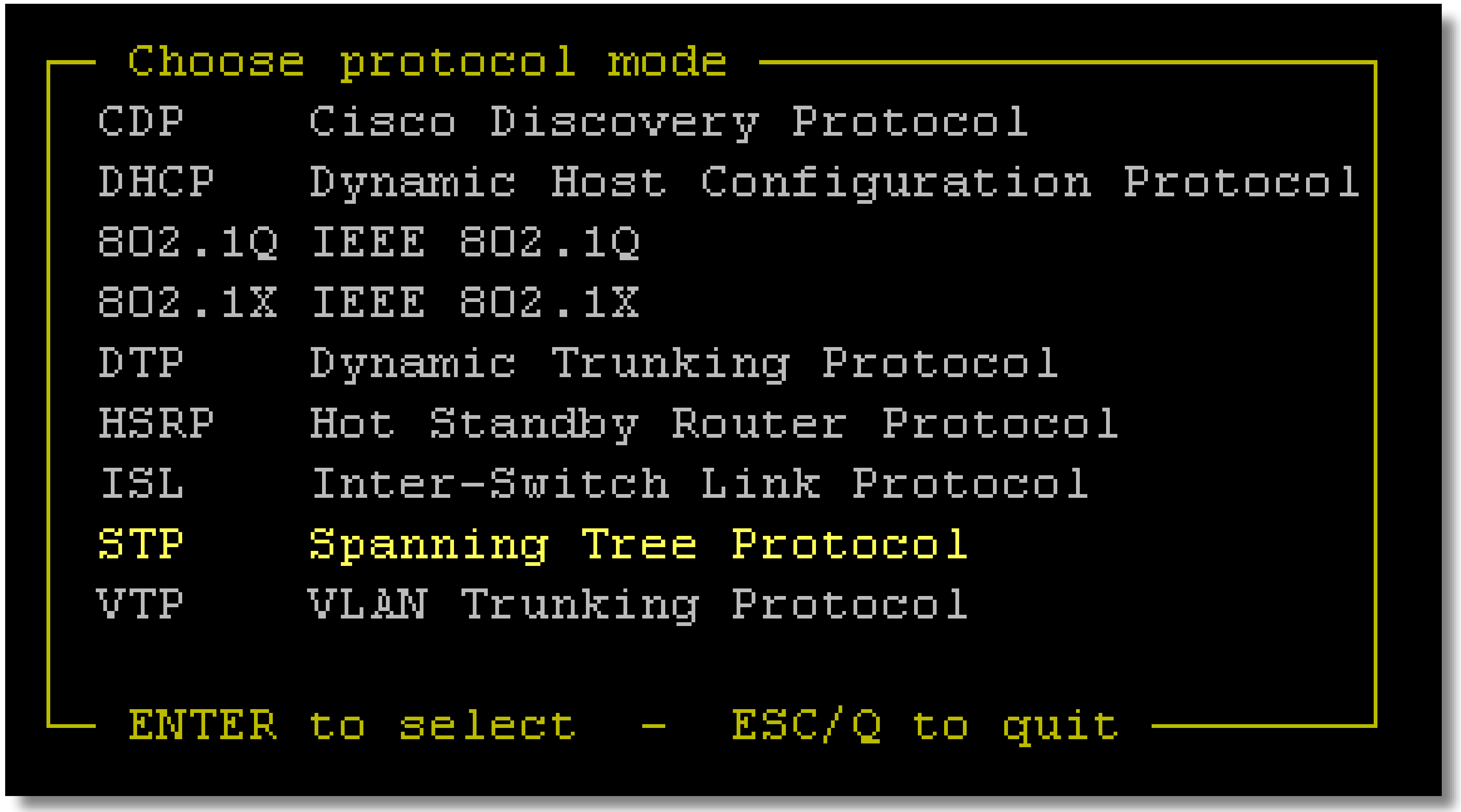
Countermeasures to Spoofing Attacks: IP Source Guard

- DHCP snooping has 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 traffic
- Drawbacks
  - Not supported on all hardware
  - Resource intensive as it inspects all packets

Attacks on other Protocols

Other Protocols?

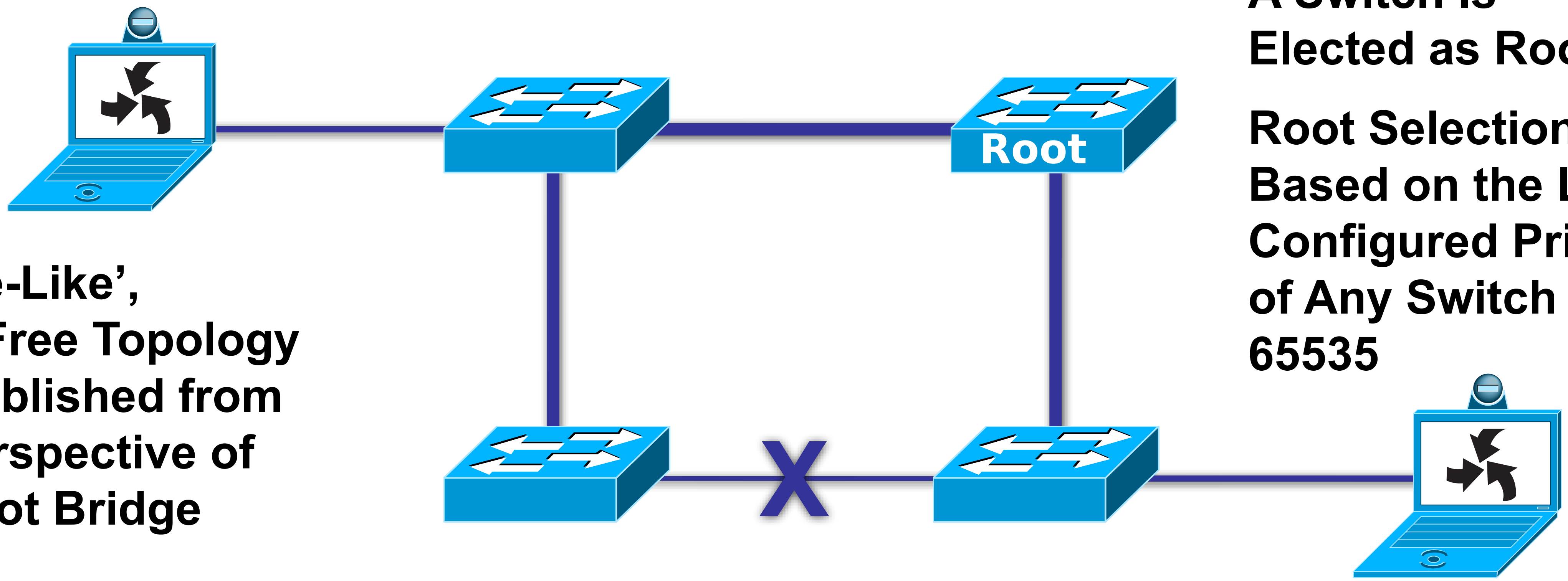
- Yersinia can help you with:
  - CDP
  - DHCP
  - 802.1Q
  - 802.1X
  - DTP
  - HSRP
  - STP
  - ISL
  - VTP



```
┌─ Choose protocol mode ───────────────────────────────┐
│ CDP     Cisco Discovery Protocol                     │
│ DHCP    Dynamic Host Configuration Protocol          │
│ 802.1Q IEEE 802.1Q                                   │
│ 802.1X IEEE 802.1X                                   │
│ DTP     Dynamic Trunking Protocol                    │
│ HSRP    Hot Standby Router Protocol                  │
│ ISL     Inter-Switch Link Protocol                   │
│ STP     Spanning Tree Protocol                       │
│ VTP     VLAN Trunking Protocol                       │
│                                                      │
└─ ENTER to select  -  ESC/Q to quit ──────────────────┘
```

Spanning Tree Basics

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



A Switch Is Elected as Root

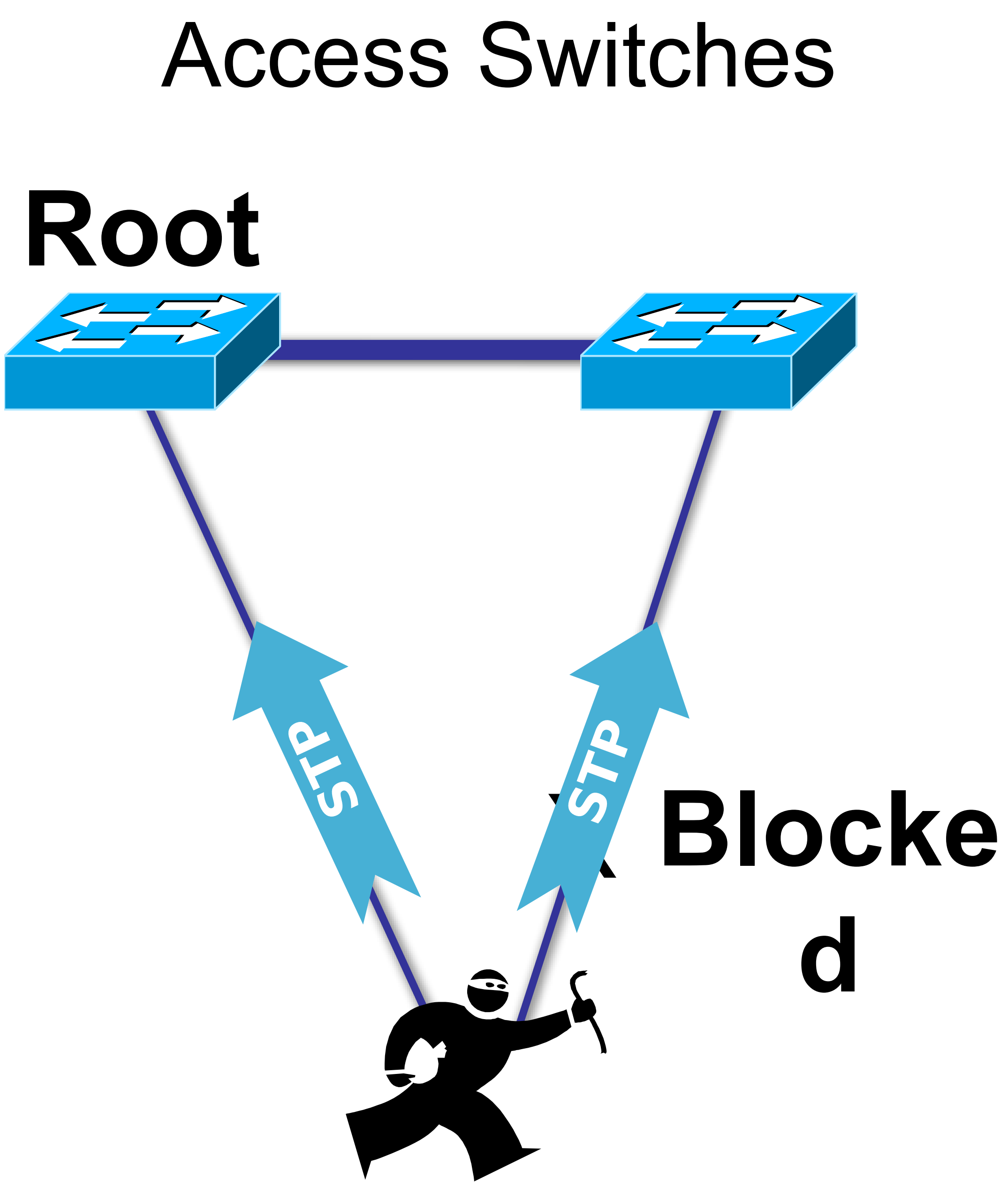
Root Selection Is Based on the Lowest Configured Priority of Any Switch 0–65535

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

Spanning Tree Attack Example

- Send BPDU messages to become root bridge



Access Switches

Root

STP

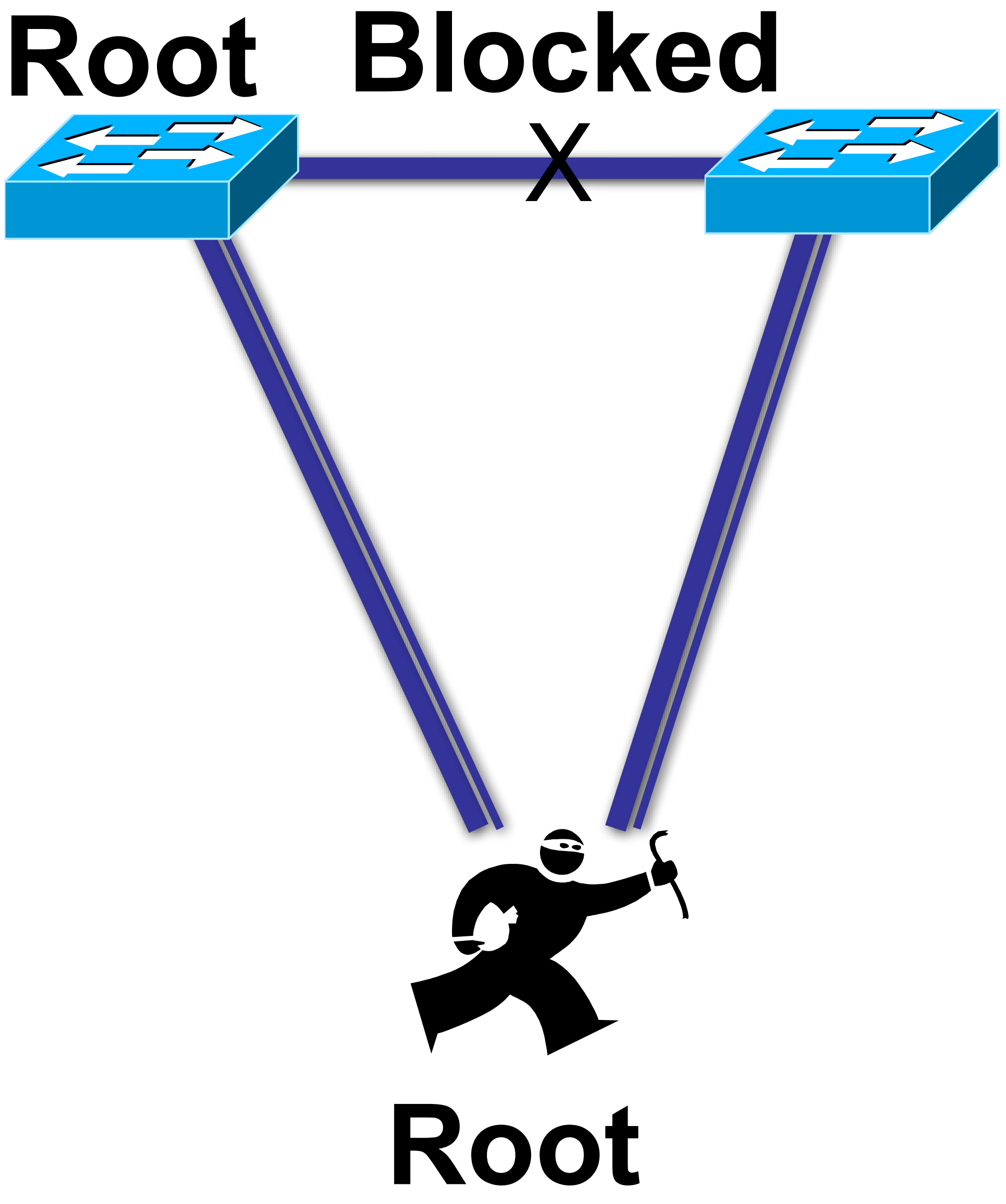
STP

X Blocke d

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)

Access Switches



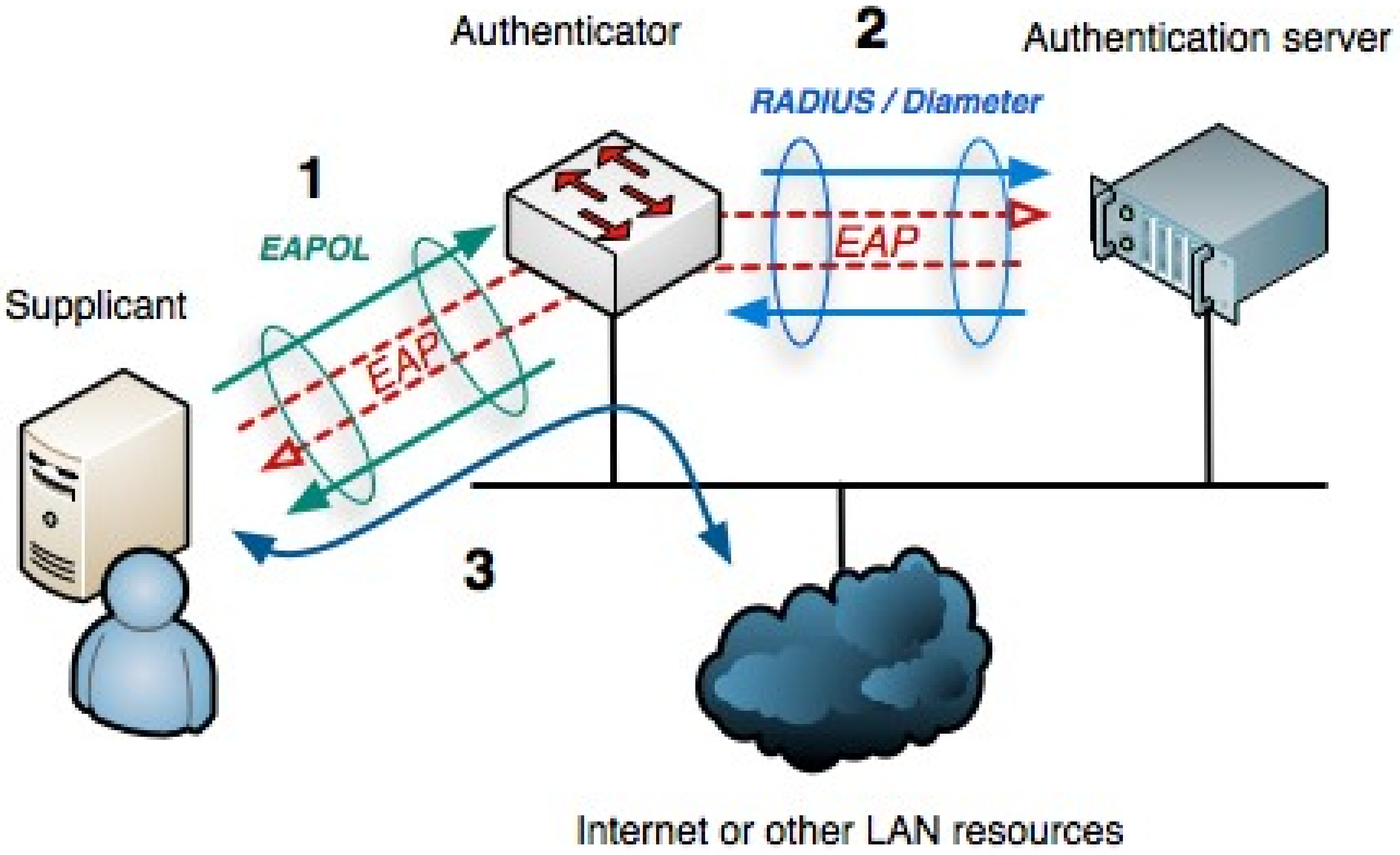
STP Attack Mitigation

- Enable BPDU Guard on access ports
  - BPDU Guard disables the port upon BPDU reception
  - Called “BPDU Protection” in Juniper devices
- Design loop-free topologies where ever possible, so you do not need STP (difficult due to redundancy reasons)
- Disable ports using portfast upon detection of a BPDU message on the port
- Root Guard
  - Limits which devices are allowed to be root
  - Allows a device to participate in STP unless the device attempts to become root bridge due to their BPDU advertisement
  - Configured on a per port basis

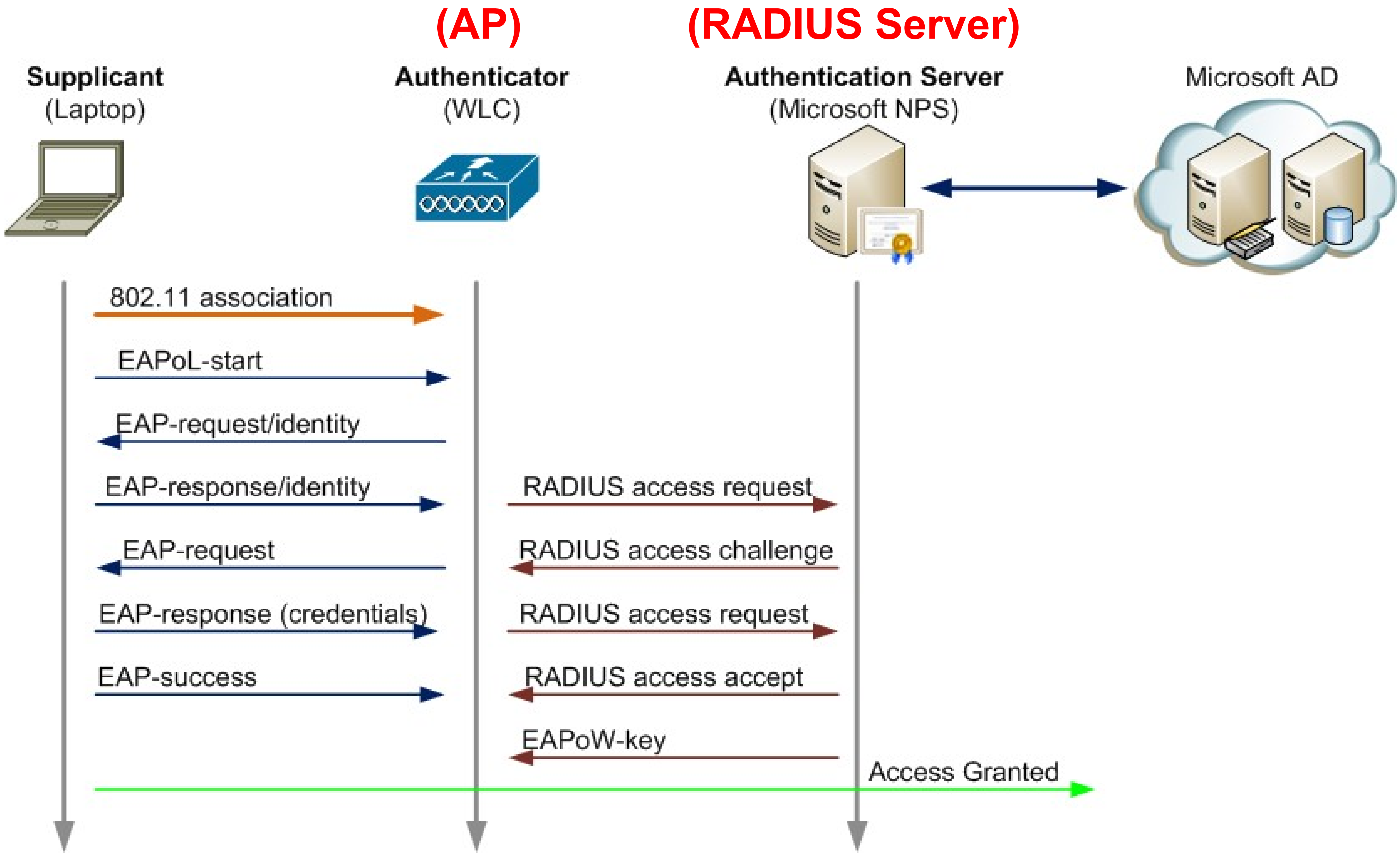
802.1x

802.1x Overview

- IEEE standard for Port-Based Network Access Control
- Started for wireless, but is now a standard in wired enterprise networks
- Authenticate devices before allowing connection to the network



Client Association – 802.1x (Enterprise)



Types of 802.1x Authentication

- MAC authentication
- Extensible Authentication Protocol (EAP)
  - EAP-MD5: password based (insecure)
  - EAP-TLS: certificate based
  - EAP-PEAP: Protected EAP
  - EAP-TTLS: Protects EAP in a TLS Tunnel
  - EAP-FAST: Flexible Authentication via Secure Tunneling (developed by Cisco)
  - Cisco LEAP: Insecure
  - Others
- Captive Portal
  - Used in public wi-fi, allows access to captive portal until credentials are provided