GenCyber Networking

ARP Poisoning

Refresher on ARP

- We are talking layer 2 of the OSI (data link)
- Most switches operate at layer 2, and perform as much networking as possible on layer 2
  - It’s quicker to do it this way rather than sending it via layer 3 (IP address) to a router, etc.
- The MAC address is how machines on a subnet communicate
  - When you ping an IP, if it is on the same subnet as your machine, the IP address gets translated back into a MAC address

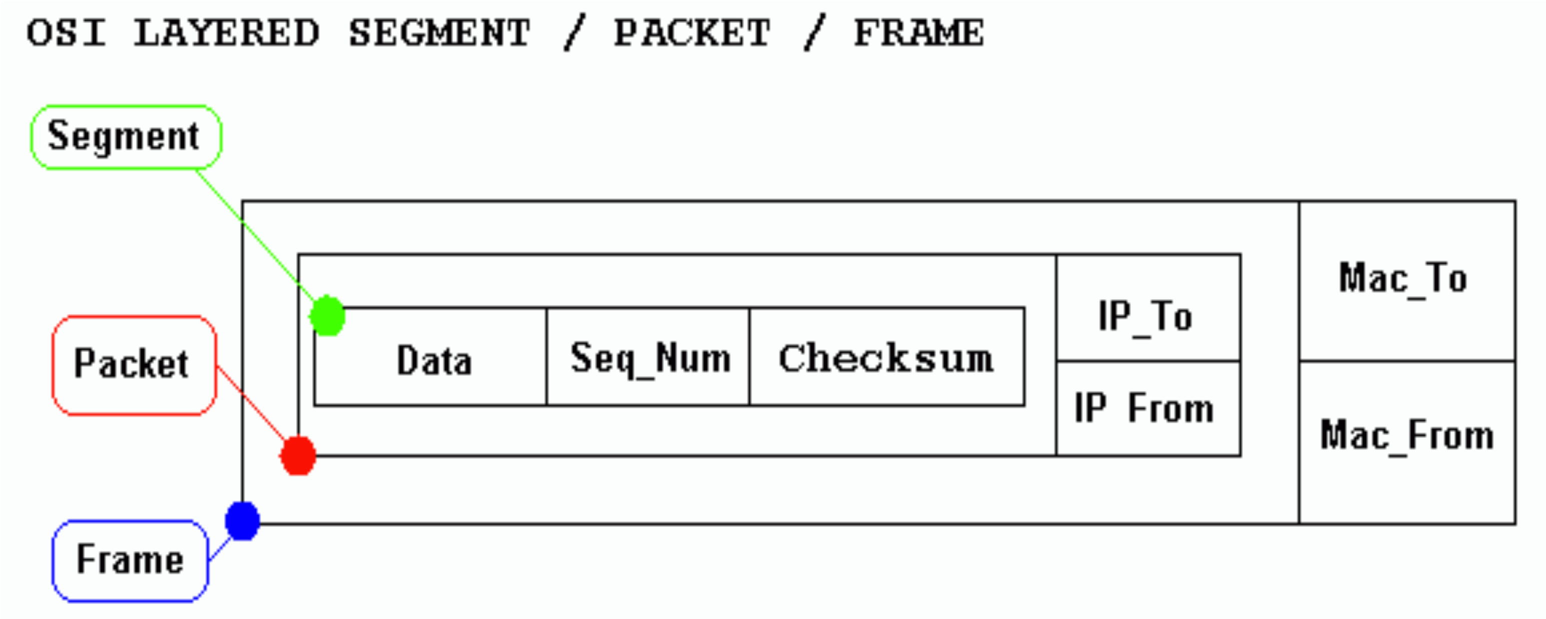
Refresher on ARP

- IP to MAC translations are stored in the MAC table of your system
- Switches also keep track of what IP/MAC addresses are on which physical ports connected to the switch:

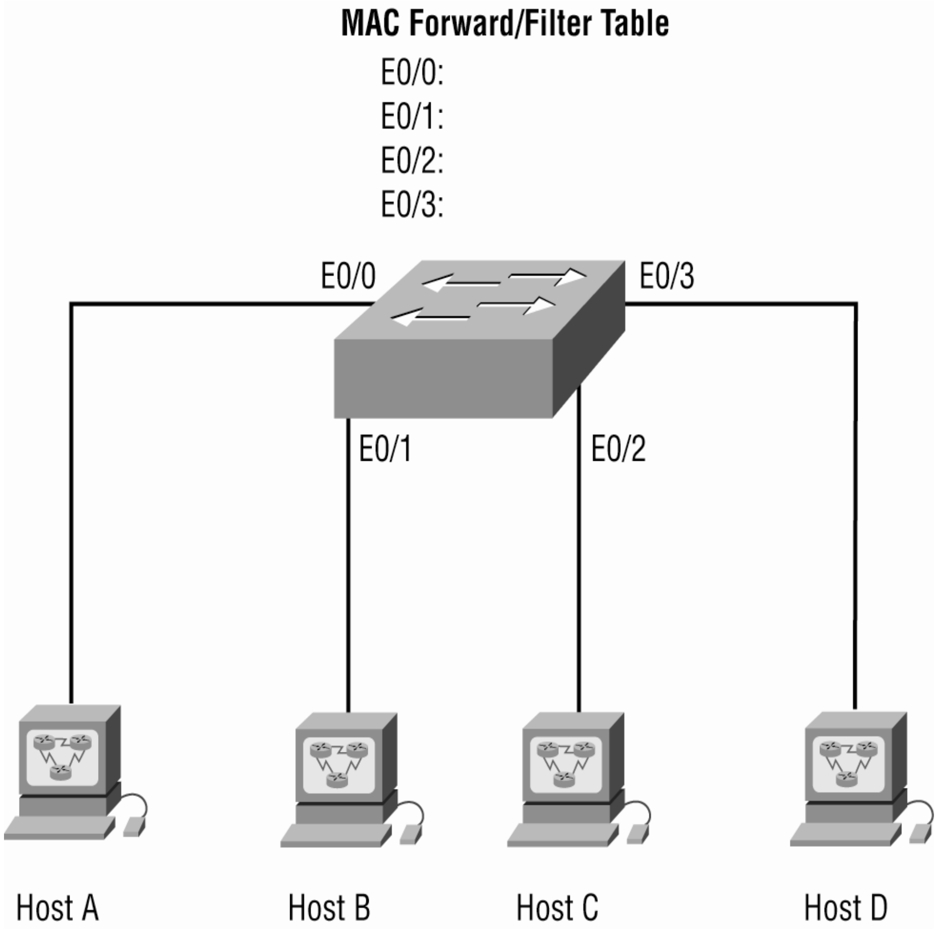
Address Learning

- MAC forward/filter table is empty on boot
- When device transmits and interface receives a frame, switch puts frames source address in MAC table
- Floods the network with the frame except on source port
- If device answers, switch will place that MAC in the database as well (point-to-point)

Layer 2 Frames



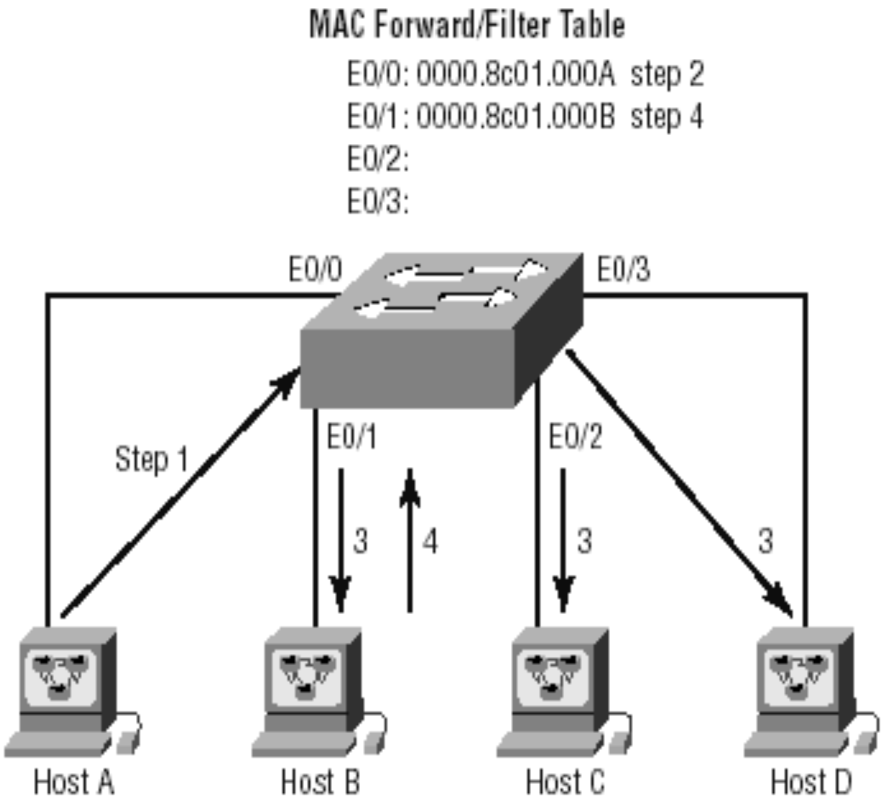
Empty MAC Table



MAC Forward/Filter Table

E0/0:
E0/1:
E0/2:
E0/3:

How Switches Learn Hosts' Locations



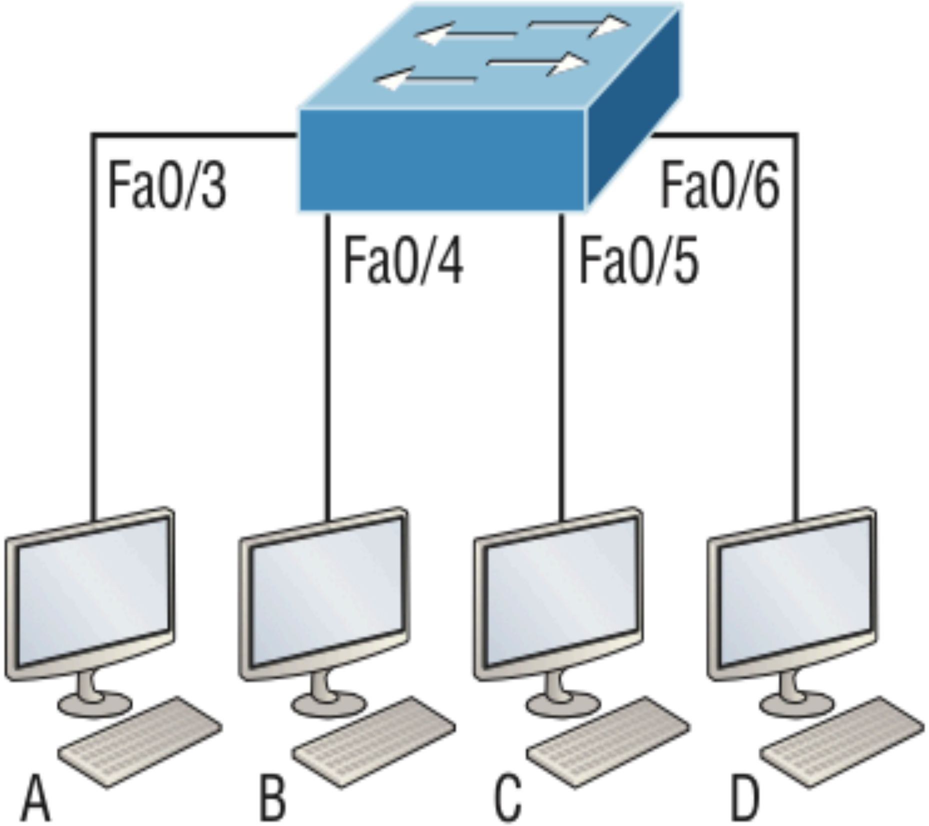
MAC Forward/Filter Table

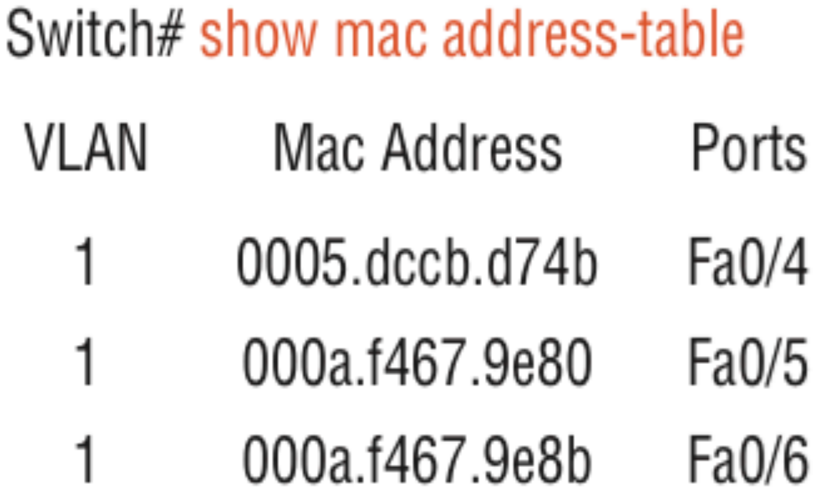
E0/0: 0000.8c01.000A step 2
E0/1: 0000.8c01.000B step 4
E0/2:
E0/3:

Forward/Filter Decisions

- When a frame arrives at a switch interface, destination address is compared to database
  - If found, frame is forwarded only to the destination (frame filtering)
  - If not found, frame is flooded on all interfaces except the source interface
- Broadcast on LAN will flood the frame out all active ports except the source

Forward/Filter Example (A→D)



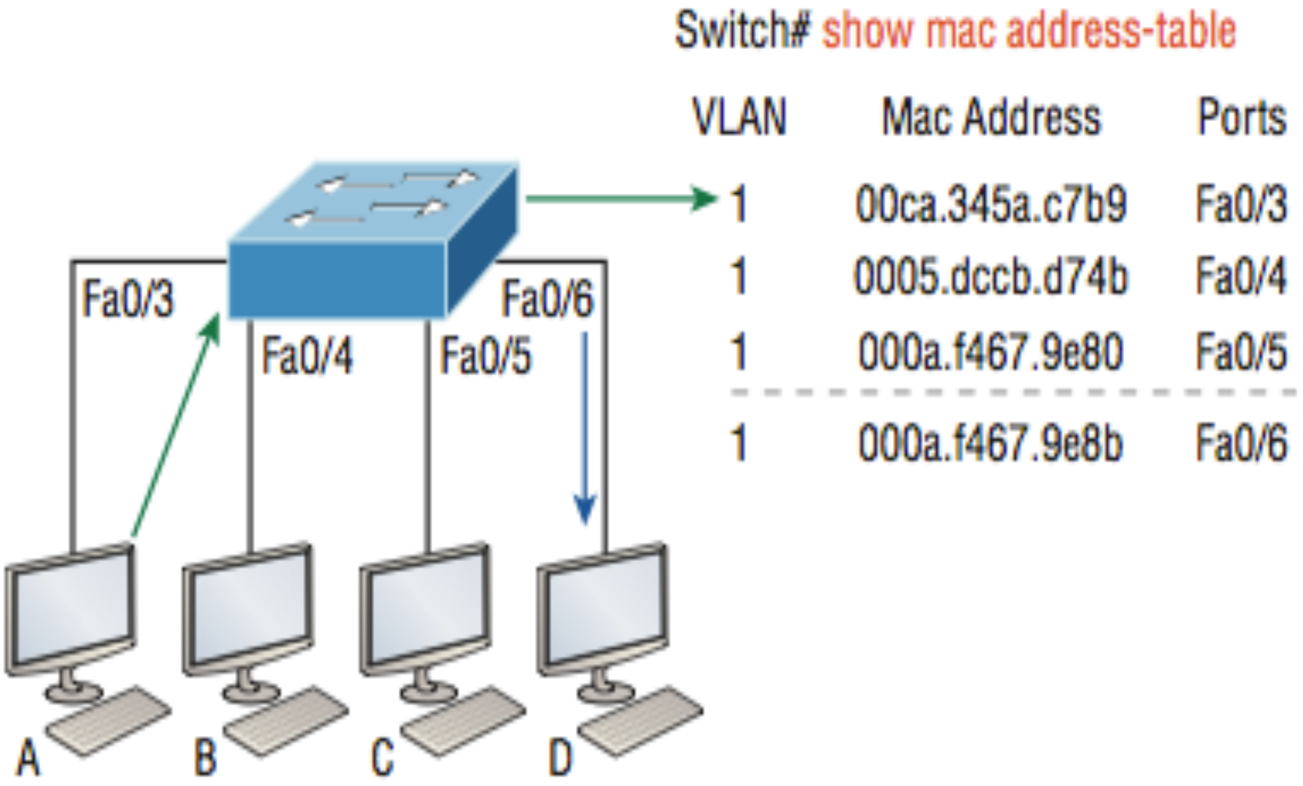


```
Switch# show mac address-table

VLAN     Mac Address        Ports

  1      0005.dccb.d74b     Fa0/4
  1      000a.f467.9e80     Fa0/5
  1      000a.f467.9e8b     Fa0/6
```

Forward/Filter Example (A→D)



```
Switch# show mac address-table

VLAN      Mac Address        Ports

1         00ca.345a.c7b9     Fa0/3
1         0005.dccb.d74b     Fa0/4
1         000a.f467.9e80     Fa0/5
- - - - - - - - - - - - - - - - - -
1         000a.f467.9e8b     Fa0/6
```

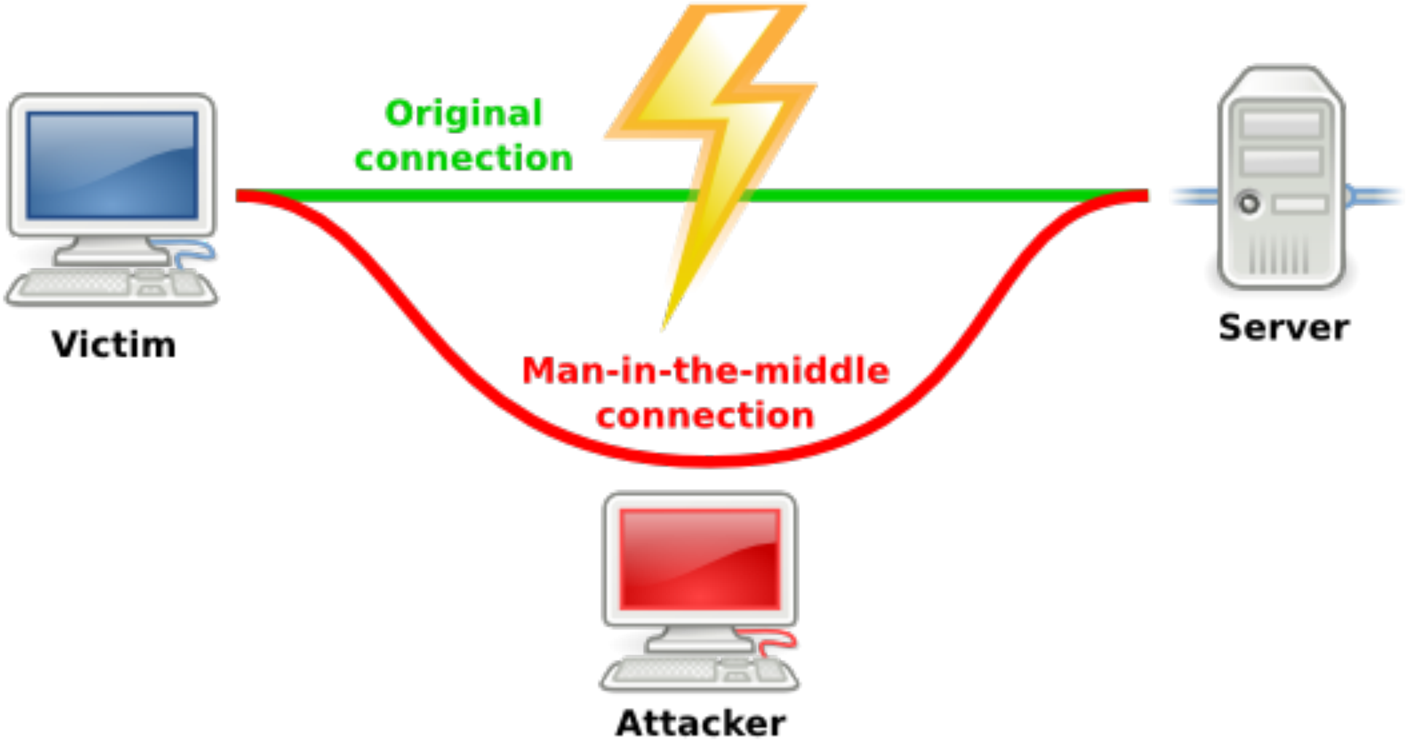
Switch View

```
BH_SecCam#sh mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  36    0040.8cb1.d9fd    DYNAMIC     Gi0/1
  36    0040.8cb1.d9fe    DYNAMIC     Gi0/1
  36    0040.8cd9.e729    DYNAMIC     Gi0/1
  36    0040.8cda.4e87    DYNAMIC     Gi0/1
  36    0040.8cda.4e8a    DYNAMIC     Gi0/1
   1    588d.090d.d630    DYNAMIC     Gi0/1
   1    8875.563c.5840    DYNAMIC     Gi0/1
   3    588d.090d.d630    DYNAMIC     Gi0/1
   4    588d.090d.d630    DYNAMIC     Gi0/1
BH_SecCam#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  138.247.36.1            0   8875.563c.5840  ARPA   Vlan36
Internet  138.247.38.233          -   64ae.0c61.ebc1  ARPA   Vlan36
```

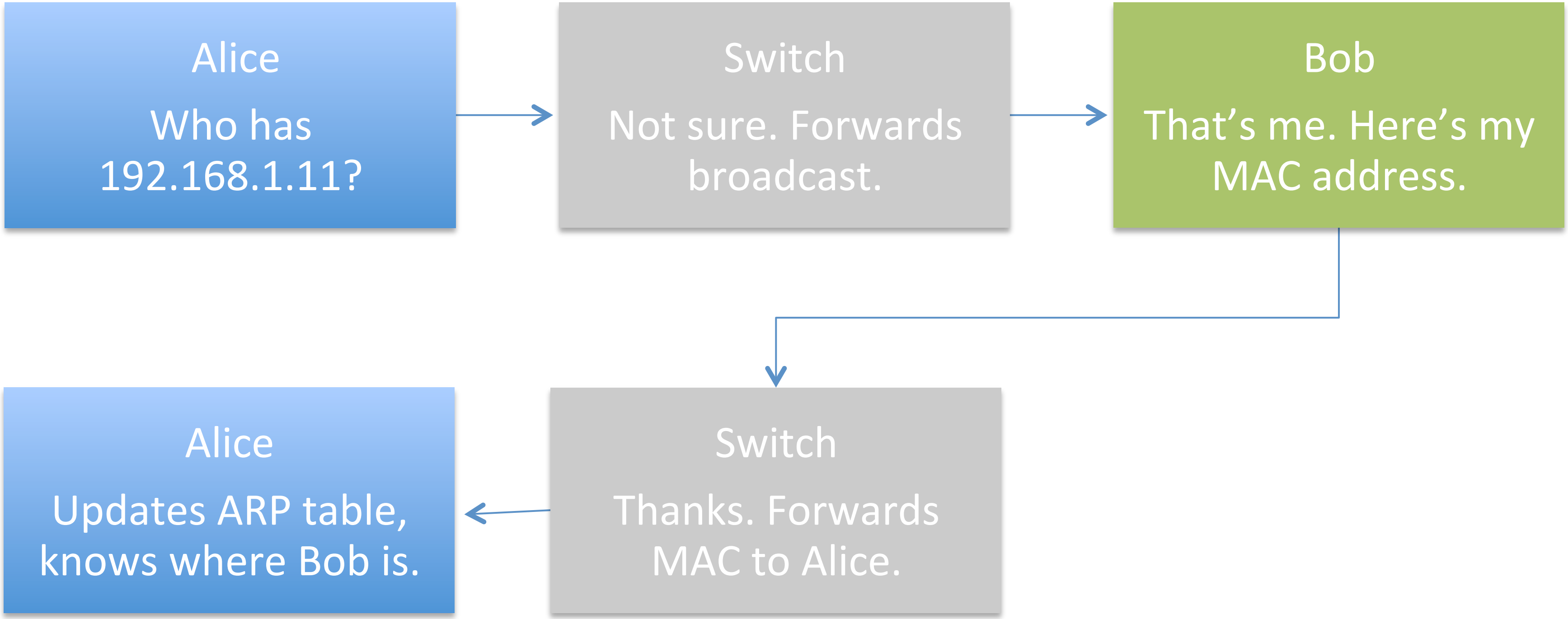
ARP Poisoning

- Also referred to as **ARP Spoofing**
- Attacker sends fake ARP messages out on network to single host or group of devices
  - Poisoned hosts then link the MAC address with the IP of a legitimate computer/server on the network
- The attacker can then intercept, modify, or redirect network traffic as they please
  - Stolen credentials, redirected to malware, etc.

Man-in-the-Middle (MITM) Attack



Simple ARP Request/Response



Alice

Who has 192.168.1.11?

Switch

Not sure. Forwards broadcast.

Bob

That’s me. Here’s my MAC address.

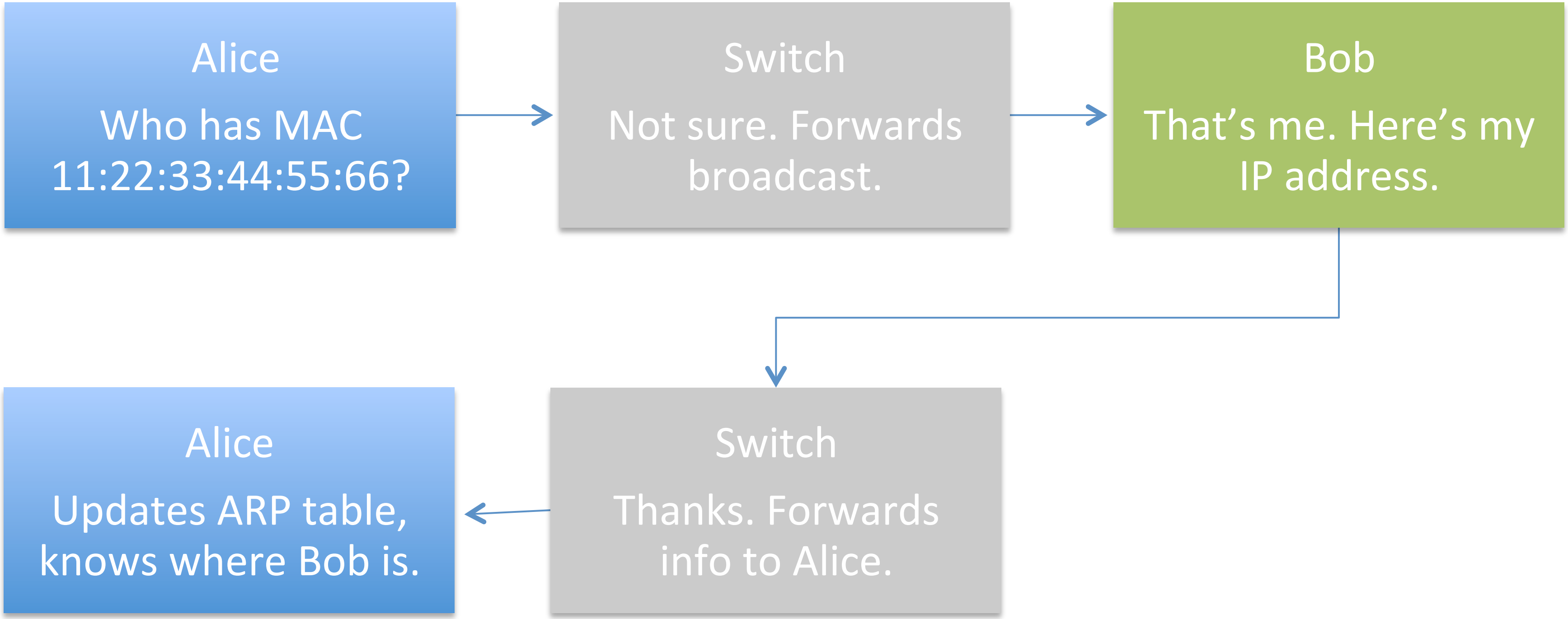
Switch

Thanks. Forwards MAC to Alice.

Alice

Updates ARP table, knows where Bob is.

Reverse ARP Request (RARP)



Alice

Who has MAC 11:22:33:44:55:66?

Switch

Not sure. Forwards broadcast.

Bob

That’s me. Here’s my IP address.

Switch

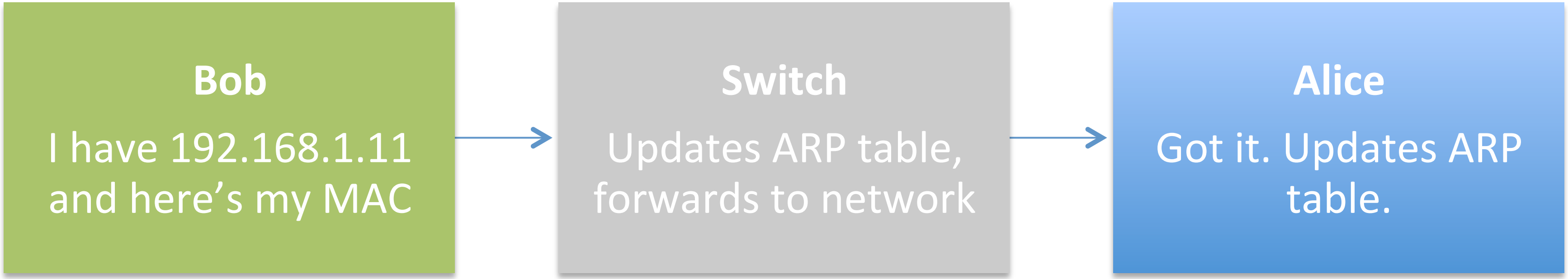
Thanks. Forwards info to Alice.

Alice

Updates ARP table, knows where Bob is.

Reverse ARP Reply (RARP)

- Same concept as a ARP Request/Response only backwards.



Bob

I have 192.168.1.11 and here's my MAC

Switch

Updates ARP table, forwards to network

Alice

Got it. Updates ARP table.

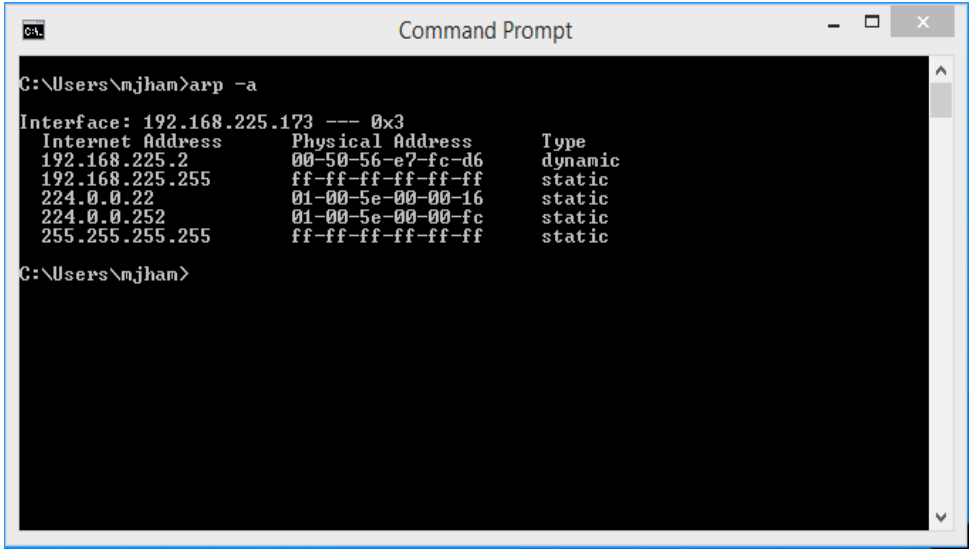
Can’t I just sniff traffic anyways?

- If I’m plugged into a switch, can I see everybody’s traffic?
  - No
- What if I put my adapter into promiscuous mode with Wireshark?
  - Still no
- Remember: switches breakup collision domains – this means that you see your traffic and your traffic only by default
  - Hubs do allow for all traffic to be seen by everyone
  - On a switch, you will need to troll people into connecting to you, then you can pass their traffic on as if all were normal

Activity: Record ARP Table

- Since we are going to perform an ARP Poisoning attack, take a minute to record what your ARP table looks like on your host machine
- If the attacks are successful, it will be good to have a baseline to look at and see how the networking changes

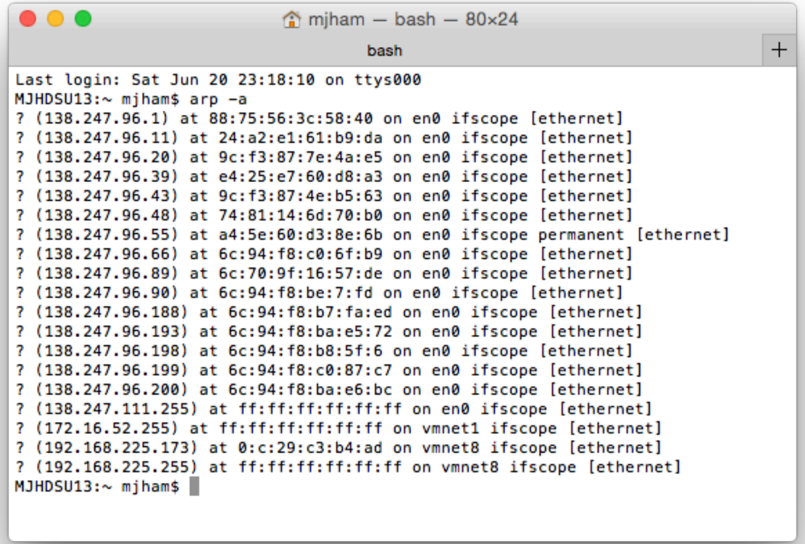
ARP Tables



```
C:\Users\mjham>arp -a

Interface: 192.168.225.173 --- 0x3
  Internet Address      Physical Address      Type
  192.168.225.2         00-50-56-e7-fc-d6     dynamic
  192.168.225.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\mjham>
```



```
Last login: Sat Jun 20 23:18:10 on ttys000
MJHDSU13:~ mjham$ arp -a
? (138.247.96.1) at 88:75:56:3c:58:40 on en0 ifscope [ethernet]
? (138.247.96.11) at 24:a2:e1:61:b9:da on en0 ifscope [ethernet]
? (138.247.96.20) at 9c:f3:87:7e:4a:e5 on en0 ifscope [ethernet]
? (138.247.96.39) at e4:25:e7:60:d8:a3 on en0 ifscope [ethernet]
? (138.247.96.43) at 9c:f3:87:4e:b5:63 on en0 ifscope [ethernet]
? (138.247.96.48) at 74:81:14:6d:70:b0 on en0 ifscope [ethernet]
? (138.247.96.55) at a4:5e:60:d3:8e:6b on en0 ifscope permanent [ethernet]
? (138.247.96.66) at 6c:94:f8:c0:6f:b9 on en0 ifscope [ethernet]
? (138.247.96.89) at 6c:70:9f:16:57:de on en0 ifscope [ethernet]
? (138.247.96.90) at 6c:94:f8:be:7:fd on en0 ifscope [ethernet]
? (138.247.96.188) at 6c:94:f8:b7:fa:ed on en0 ifscope [ethernet]
? (138.247.96.193) at 6c:94:f8:ba:e5:72 on en0 ifscope [ethernet]
? (138.247.96.198) at 6c:94:f8:b8:5f:6 on en0 ifscope [ethernet]
? (138.247.96.199) at 6c:94:f8:c0:87:c7 on en0 ifscope [ethernet]
? (138.247.96.200) at 6c:94:f8:ba:e6:bc on en0 ifscope [ethernet]
? (138.247.111.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (172.16.52.255) at ff:ff:ff:ff:ff:ff on vmnet1 ifscope [ethernet]
? (192.168.225.173) at 0:c:29:c3:b4:ad on vmnet8 ifscope [ethernet]
? (192.168.225.255) at ff:ff:ff:ff:ff:ff on vmnet8 ifscope [ethernet]
MJHDSU13:~ mjham$
```

Attackers Know ARP is Gullible

- ARP has no method of authentication
- ARP replies are assumed to be trusted
- Legitimate ARP traffic happens at certain intervals, but there is no time limit/triggers on replies

Team Up!

- Form groups, you will need one attacker and one or two victims (nothing bad will actually happen to your machines)

Write this Down

- On the victim machine, view your ARP table, and record the MAC address of the telnet server
  - **arp –a**

- What is the victim's Windows 8 IP address?
  - **ipconfig**

- What is the attacker's Kali MAC address?
- What is the attacker's Kali IP address?
  - **ifconfig**

Command

- Start Wireshark on the attacker machine

- Have the client try to ftp to the server
  - **ftp X.X.X.X**
  - Enter in a fake username/password (not your real one)

- ettercap -T -M arp:remote /<gateway>/ /<host or range>/
- View the ARP table on the victim to make sure the MAC has changed
- Have the victim machine FTP to the server again
- Stop the Wireshark capture on the attack machine

You’re not so sneaky…

- Take a look at what your ARP poisoning attack looks like in Wireshark
- This would be very obvious to a system administrator (yes we look for this type of stuff on campus)
- Real world, there are ways to be more stealthy, but I’m going to leave that up to you to figure out
    - Diving into this stuff is really fun, you’ll learn a lot and have better understanding of the attack

Examples In the Wild

- Denial of Service
- MAC Flooding
- Man-in-the-Middle
  - Capture authentication credentials
  - Spoof services – SMB, SMTP

ARP Spoofing Defense

- Small networks: static IP and ARP table
- Large networks: switch port security
  - Allows only one MAC per switch port
- Everything else: ARP monitoring tools
  - IDS/IPS
  - ARPwatch