Fireside Fridays

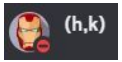
Layer 2 Communication
Week 5

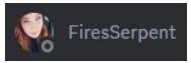
Thanks to our sponsors!

ACTIVE COUNTERMEASURES

Antisyphon Training

Special Thanks to…

- Hermon 

- Emily 

- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thanks" the next time you see them online

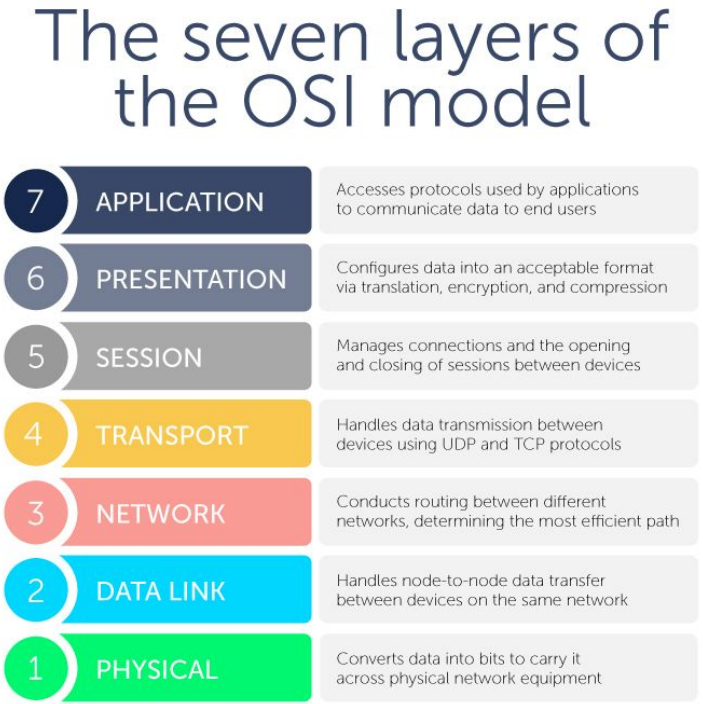
Lab requirements for this section

- Windows or Linux system
- Labs will be at the command line or terminal

Traffic control technologies

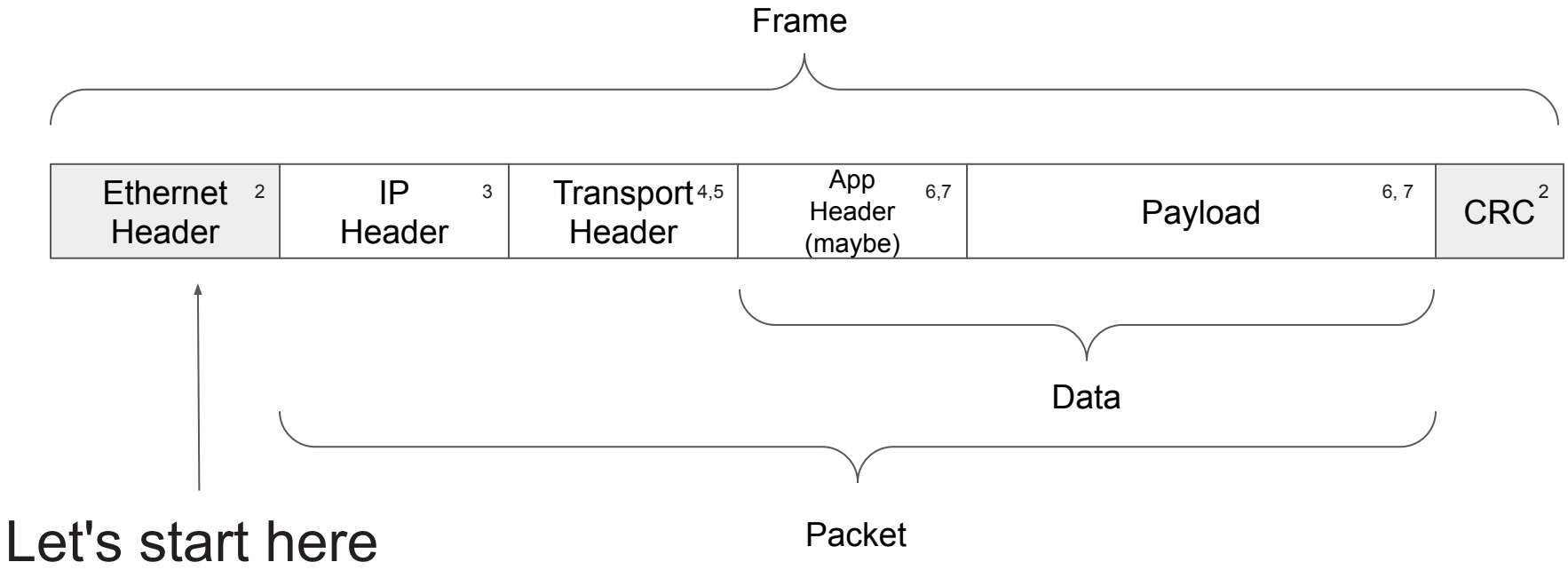
- We'll discuss tech used to modify IP traffic flow
- Need the basics to understand architecture
- Not designed to be a complete tutorial
- Will focus more on the security aspects

OSI model for communications

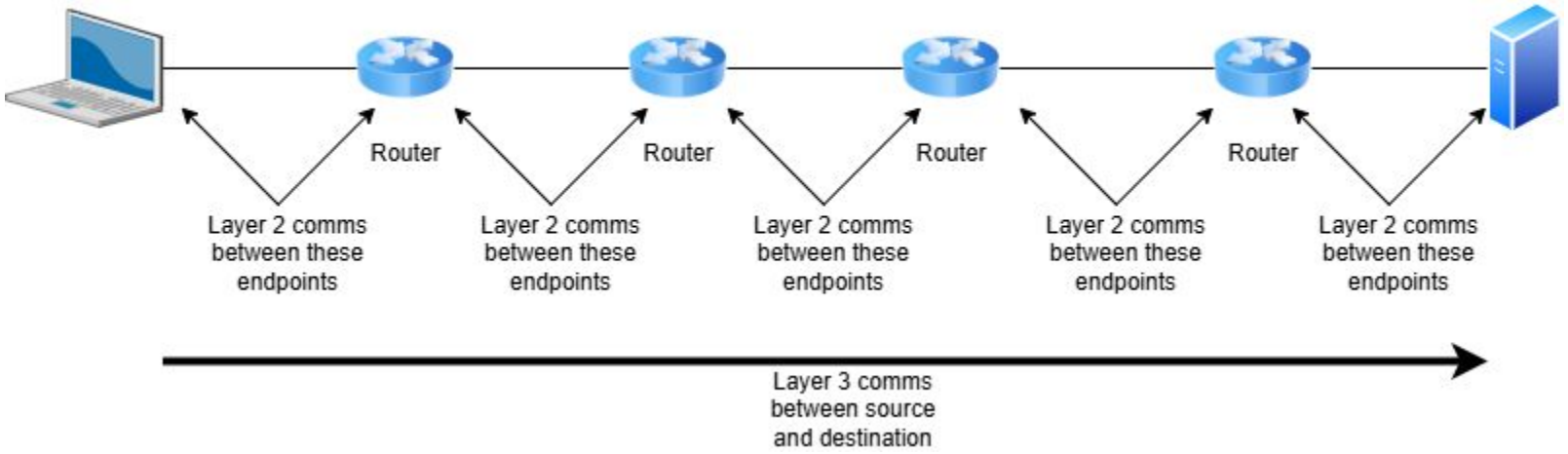


Framework describing communication rules so that dissimilar systems remain compatible with each other

Anatomy of a transmission

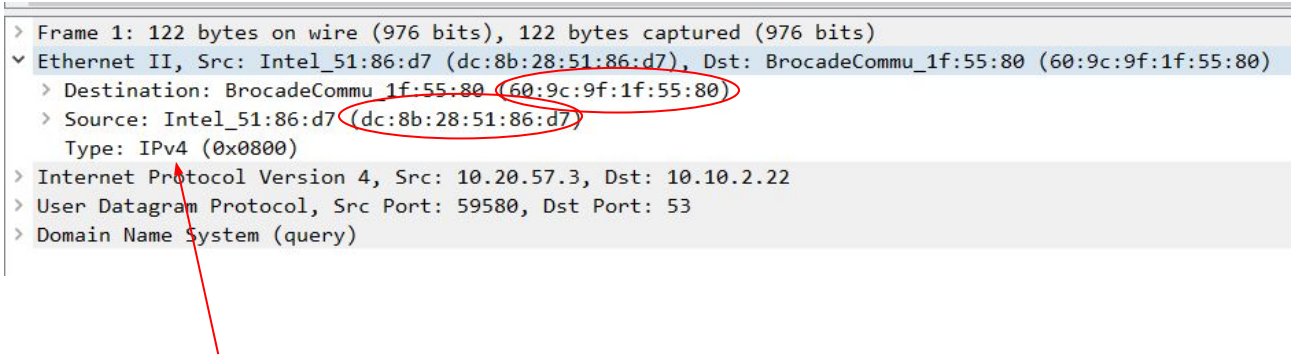


How comms work



Layer 2 info replaced at each router
The means the outer frame is stripped and replaced

What's the Ethernet header look like?

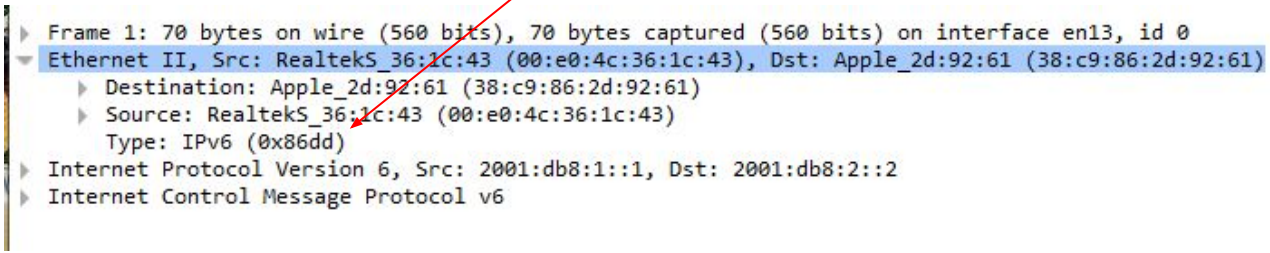


IPv4

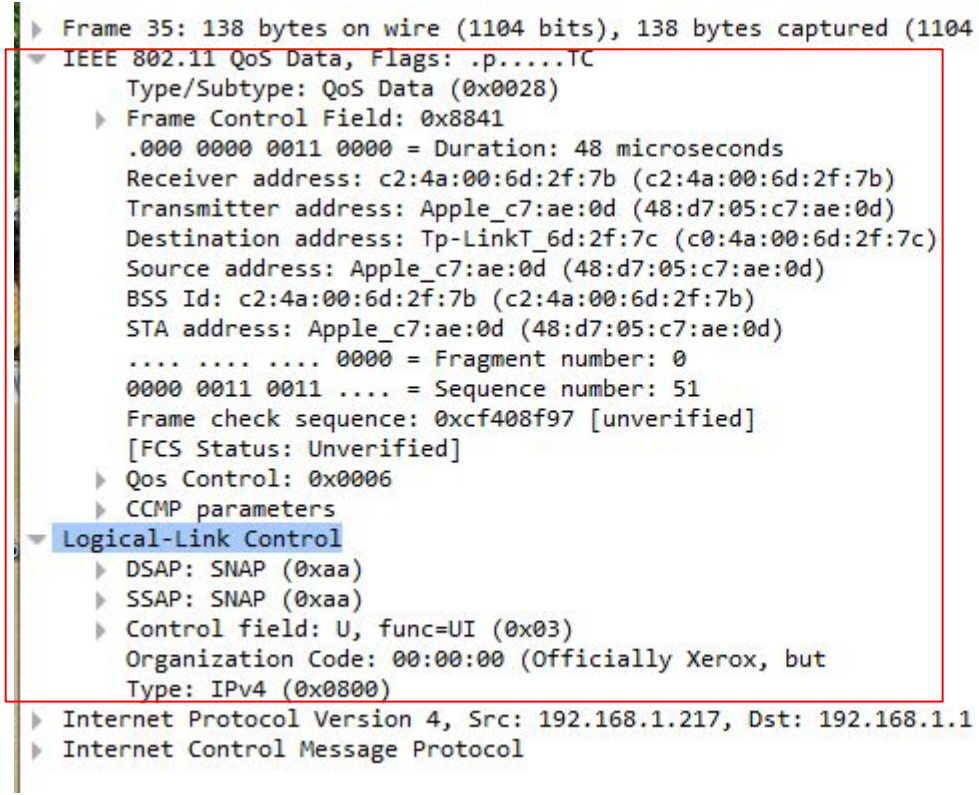
MAC = 6 bytes
Usually in Hex

Byte separators can vary

IPv6



WiFi (802.11) frame

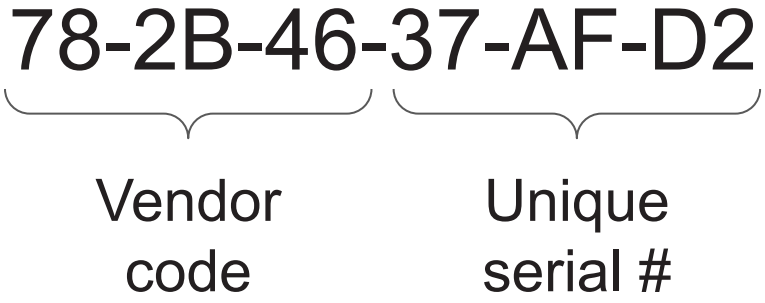


802.11has a lot more header info than Ethernet

Needed to facilitate radio frequency comms

This is why Ethernet at the same speed is more efficient than Wifi

MAC addresses example



Code identifies this as an Intel card

http://standards-oui.ieee.org/oui/oui.txt

MAC address lookup

https://www.wireshark.org/tools/oui-lookup.html

https://www.wireshark.org/download/automated/data/manuf

```
D8:30:62        Apple           Apple, Inc.
D8:31:2C        zte             zte corporation
D8:31:34        Roku            Roku, Inc
D8:31:CF        SamsungElect    Samsung Electronics Co.,Ltd
D8:32:14        TendaTechnol    Tenda Technology Co.,Ltd.Dongguan branch
D8:32:5A        YOUHUATechno    Shenzhen YOUHUA Technology Co., Ltd
D8:32:E3        XiaomiCommun    Xiaomi Communications Co Ltd
```

Hands-on walkthrough - MAC addresses

- This walkthrough will work on Windows, Linux or Mac systems
  - Command is the same on all platforms
  - Output may appear slightly different from examples
- Open a command prompt or terminal window
- Run the following command:

```
arp -a
```

Windows example

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

Interface: 10.0.0.101 --- 0x4
  Internet Address      Physical Address      Type
  10.0.0.1              08-a7-c0-2b-62-84     dynamic
  10.0.0.18             d8-31-34-32-a9-4a     dynamic
  10.0.0.66             84-ea-ed-8f-a2-2e     dynamic
  10.0.0.86             5c-62-5a-81-97-aa     dynamic
  10.0.0.131            bc-d7-d4-6d-75-b6     dynamic
  10.0.0.197            84-ea-ed-19-d6-37     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x10
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Learned from the network via ARP

Preprogrammed (configure at OS)

Limit entries to a single network interface

```
C:\Windows\system32>arp /a /n 192.168.69.223

Interface: 192.168.69.223 --- 0x4
  Internet Address      Physical Address      Type
  192.168.69.1          84-47-09-33-71-db     dynamic
  192.168.69.11         68-1d-ef-34-f6-2e     dynamic
  192.168.69.16         02-60-2d-56-eb-bb     dynamic
  192.168.69.117        36-f0-db-9b-2e-f1     dynamic
  192.168.69.144        84-ea-ed-8f-a2-2e     dynamic
  192.168.69.201        6c-2a-df-e0-5a-72     dynamic
  192.168.69.224        d8-31-34-32-a9-4a     dynamic
  192.168.69.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Windows\system32>
```

ARP on Linux

```
cbrenton@server2:~$ arp -a
? (192.168.69.179) at d4:31:27:4e:46:d5 [ether] on enp2s0
? (192.168.69.161) at 26:6e:a8:3d:98:06 [ether] on enp2s0
? (192.168.69.1) at 84:47:09:33:71:db [ether] on enp2s0
? (192.168.69.224) at d8:31:34:32:a9:4a [ether] on enp2s0
? (192.168.69.16) at 02:60:2d:56:eb:bb [ether] on enp2s0
? (192.168.69.166) at 6e:83:c4:38:03:60 [ether] on enp2s0
? (192.168.69.14) at 5c:62:5a:81:97:aa [ether] on enp2s0
? (192.168.69.223) at 78:2b:46:37:af:d2 [ether] on enp2s0
? (192.168.69.130) at cc:47:40:ad:0b:cd [ether] on enp2s0
? (192.168.69.173) at bc:24:11:83:5a:7f [ether] on enp2s0
? (192.168.69.117) at 36:f0:db:9b:2e:f1 [ether] on enp2s0
? (192.168.69.170) at 84:ea:ed:55:de:de [ether] on enp2s0
? (192.168.69.13) at 40:62:31:03:2d:d1 [ether] on enp2s0
? (192.168.69.237) at bc:24:11:34:b2:7c [ether] on enp2s0
? (192.168.69.144) at 84:ea:ed:8f:a2:2e [ether] on enp2s0
? (192.168.69.10) at 84:47:09:1d:a0:a3 [ether] on enp2s0
? (192.168.69.201) at 6c:2a:df:e0:5a:72 [ether] on enp2s0
? (192.168.69.168) at d0:01:ed:67:4a:21 [ether] on enp2s0
? (192.168.69.234) at 9a:e9:87:db:af:ee [ether] on enp2s0
? (192.168.69.110) at bc:24:11:5b:0e:26 [ether] on enp2s0
cbrenton@server2:~$
```

Some entries may be outdated

```
cbrenton@server2:~$ ip neighbor
192.168.69.179 dev enp2s0 lladdr d4:31:27:4e:46:d5 STALE
192.168.69.161 dev enp2s0 lladdr 26:6e:a8:3d:98:06 STALE
192.168.69.1 dev enp2s0 lladdr 84:47:09:33:71:db REACHABLE
192.168.69.224 dev enp2s0 lladdr d8:31:34:32:a9:4a REACHABLE
192.168.69.16 dev enp2s0 lladdr 02:60:2d:56:eb:bb STALE
192.168.69.166 dev enp2s0 lladdr 6e:83:c4:38:03:60 STALE
192.168.69.14 dev enp2s0 lladdr 5c:62:5a:81:97:aa STALE
192.168.69.223 dev enp2s0 lladdr 78:2b:46:37:af:d2 DELAY
192.168.69.130 dev enp2s0 lladdr cc:47:40:ad:0b:cd STALE
192.168.69.173 dev enp2s0 lladdr bc:24:11:83:5a:7f STALE
192.168.69.117 dev enp2s0 lladdr 36:f0:db:9b:2e:f1 STALE
192.168.69.170 dev enp2s0 lladdr 84:ea:ed:55:de:de STALE
192.168.69.13 dev enp2s0 lladdr 40:62:31:03:2d:d1 STALE
192.168.69.237 dev enp2s0 lladdr bc:24:11:34:b2:7c STALE
192.168.69.144 dev enp2s0 lladdr 84:ea:ed:8f:a2:2e REACHABLE
192.168.69.10 dev enp2s0 lladdr 84:47:09:1d:a0:a3 DELAY
192.168.69.201 dev enp2s0 lladdr 6c:2a:df:e0:5a:72 STALE
192.168.69.168 dev enp2s0 lladdr d0:01:ed:67:4a:21 STALE
192.168.69.234 dev enp2s0 lladdr 9a:e9:87:db:af:ee STALE
192.168.69.110 dev enp2s0 lladdr bc:24:11:5b:0e:26 STALE
cbrenton@server2:~$ _
```

Reachable - Active entry

Stale - entry > 30S old

Delay - Attempting to update stale entry

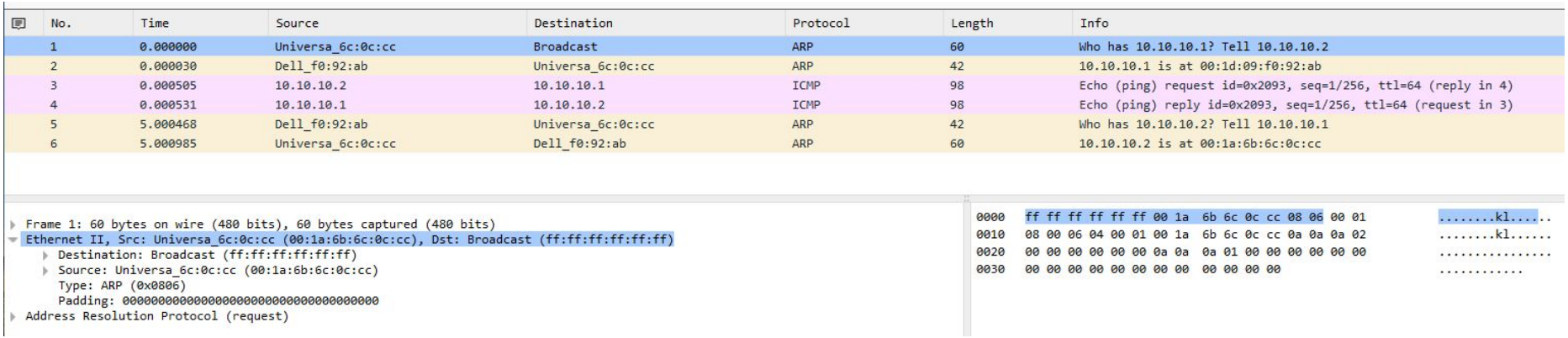
Probe - During delay, move from broadcast to unicast ARP attempt

Linux public cloud example

```
cbrenton@cb-lab:~$ arp -a
? (161.35.113.79) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.112.95) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.122.227) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.117.30) at fe:00:00:00:01:01 [ether] on eth0
antivirus-avg.com (161.35.120.97) at fe:00:00:00:01:01 [ether]
? (161.35.119.216) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.127.107) at fe:00:00:00:01:01 [ether] on eth0
prod-jerry-se-scanners-nyc1-21.do.binaryedge.ninja (161.35.124
her] on eth0
? (161.35.127.194) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.125.12) at fe:00:00:00:01:01 [ether] on eth0
? (161.35.116.178) at fe:00:00:00:01:01 [ether] on eth0
_gateway (161.35.112.1) at fe:00:00:00:01:01 [ether] on eth0
```

Bogus MAC used by provider
Used for traffic isolation

How does ARP work?



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Universa_6c:0c:cc	Broadcast	ARP	60	Who has 10.10.10.1? Tell 10.10.10.2
2	0.000030	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	10.10.10.1 is at 00:1d:09:f0:92:ab
3	0.000505	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) request id=0x2093, seq=1/256, ttl=64 (reply in 4)
4	0.000531	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) reply id=0x2093, seq=1/256, ttl=64 (request in 3)
5	5.000468	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	Who has 10.10.10.2? Tell 10.10.10.1
6	5.000985	Universa_6c:0c:cc	Dell_f0:92:ab	ARP	60	10.10.10.2 is at 00:1a:6b:6c:0c:cc

Have IP address, need MAC for local delivery
Broadcast is sent to find MAC

ARP response

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Universa_6c:0c:cc	Broadcast	ARP	60	Who has 10.10.10.1? Tell 10.10.10.2
2	0.000030	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	10.10.10.1 is at 00:1d:09:f0:92:ab
3	0.000505	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) request id=0x2093, seq=1/256, ttl=64 (reply in 4)
4	0.000531	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) reply id=0x2093, seq=1/256, ttl=64 (request in 3)
5	5.000468	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	Who has 10.10.10.2? Tell 10.10.10.1
6	5.000985	Universa_6c:0c:cc	Dell_f0:92:ab	ARP	60	10.10.10.2 is at 00:1a:6b:6c:0c:cc

```
▸ Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: Dell_f0:92:ab (00:1d:09:f0:92:ab), Dst: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc)
    ▸ Destination: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc)
    ▸ Source: Dell_f0:92:ab (00:1d:09:f0:92:ab)
      Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: reply (2)
      Sender MAC address: Dell_f0:92:ab (00:1d:09:f0:92:ab)
      Sender IP address: 10.10.10.1
      Target MAC address: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc)
      Target IP address: 10.10.10.2
```

```
0000   00 1a 6b 6c 0c cc 00 1d  09 f0 92 ab 08 06 00 01        ..kl..........
0010   08 00 06 04 00 02 00 1d  09 f0 92 ab 0a 0a 0a 01        ..............
0020   00 1a 6b 6c 0c cc 0a 0a  0a 02                          ..kl......
```

MAC returned in ARP response
Notice there is no authentication
Good thing computers never lie ;-)

Data delivery after ARP

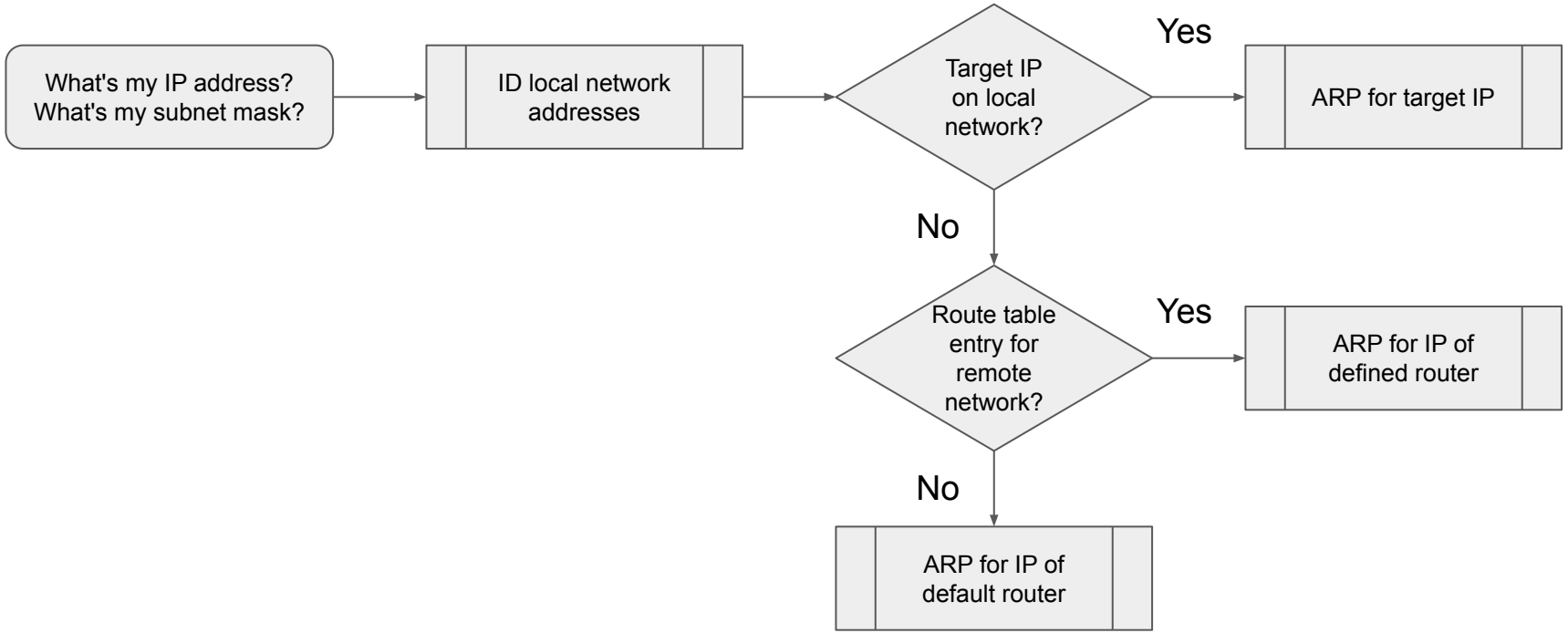
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Universa_6c:0c:cc	Broadcast	ARP	60	Who has 10.10.10.1? Tell 10.10.10.2
2	0.000030	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	10.10.10.1 is at 00:1d:09:f0:92:ab
3	0.000505	10.10.10.2	10.10.10.1	ICMP	98	Echo (ping) request id=0x2093, seq=1/256, ttl=64 (reply in 4)
4	0.000531	10.10.10.1	10.10.10.2	ICMP	98	Echo (ping) reply id=0x2093, seq=1/256, ttl=64 (request in 3)
5	5.000468	Dell_f0:92:ab	Universa_6c:0c:cc	ARP	42	Who has 10.10.10.2? Tell 10.10.10.1
6	5.000985	Universa_6c:0c:cc	Dell_f0:92:ab	ARP	60	10.10.10.2 is at 00:1a:6b:6c:0c:cc

```
▸ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▾ Ethernet II, Src: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc), Dst: Dell_f0:92:ab (00:1d:09:f0:92:ab)
    ▸ Destination: Dell_f0:92:ab (00:1d:09:f0:92:ab)
    ▸ Source: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc)
      Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.1
▸ Internet Control Message Protocol
```

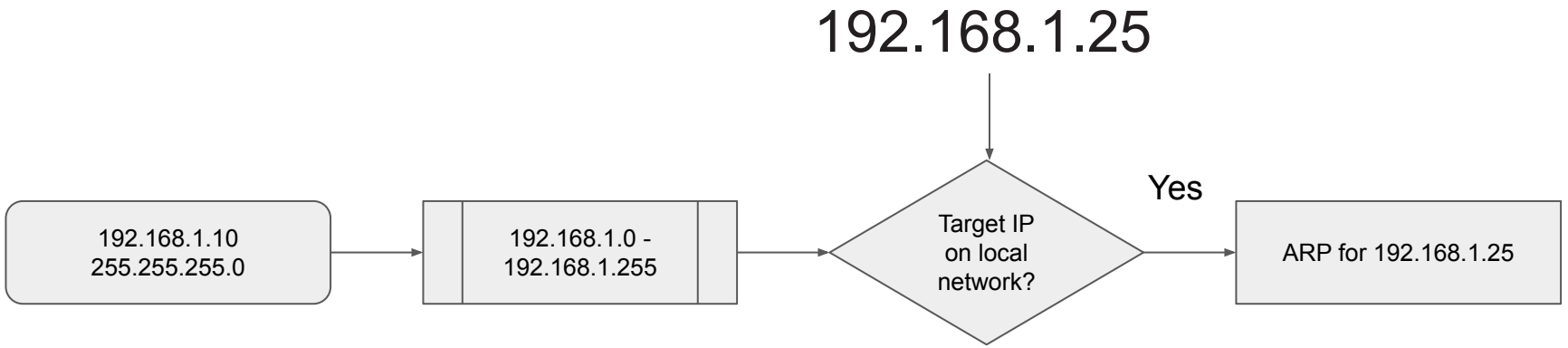
```
0000   00 1d 09 f0 92 ab 00 1a  6b 6c 0c cc 08 00 45 00   ........kl....E.
0010   00 54 00 00 40 00 40 01  12 93 0a 0a 0a 02 0a 0a   .T..@.@.........
0020   0a 01 08 00 9d 7b 20 93  00 01 88 f7 9e 50 1d a5   .....{ ......P..
0030   0a 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ................
0040   16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   .......... !"#$%
0050   26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060   36 37                                             67
```

Once the MAC is learned, data is delivered

IP transmission decision tree

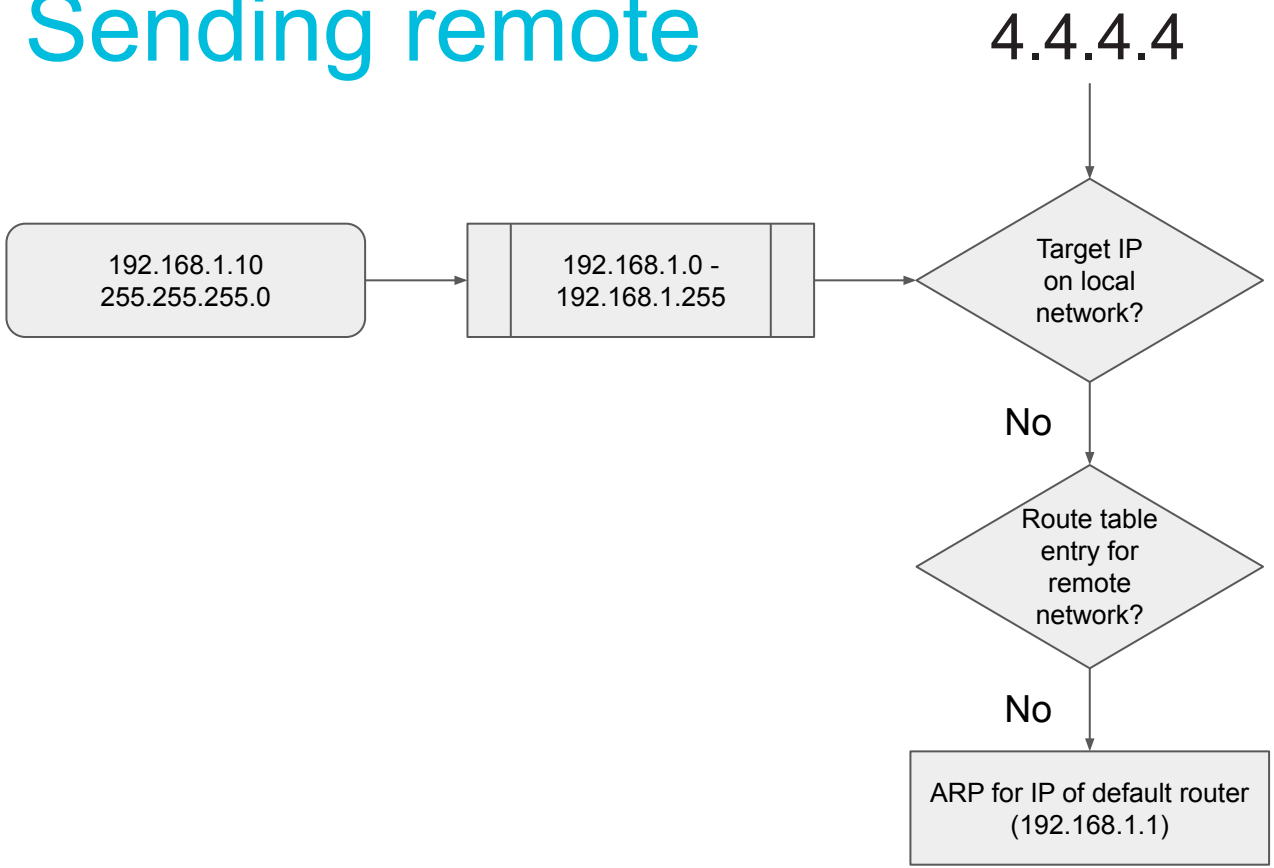


Sending local



Network = 192.168.1
Unique host = 10

Sending remote



Switches

- Works at layer 2 of the OSI (ARP)
- **Ethernet**, FDDI, Frame Relay, WiFi are examples
  - We'll focus on Ethernet & WiFi as most popular
- Learns which MACs are connected to each port
- Forwards traffic to correct port based on target MAC
- MAC is supposed to be globally unique
  - Address can usually can be changed via software
- Broadcasts and multicasts sent to every port

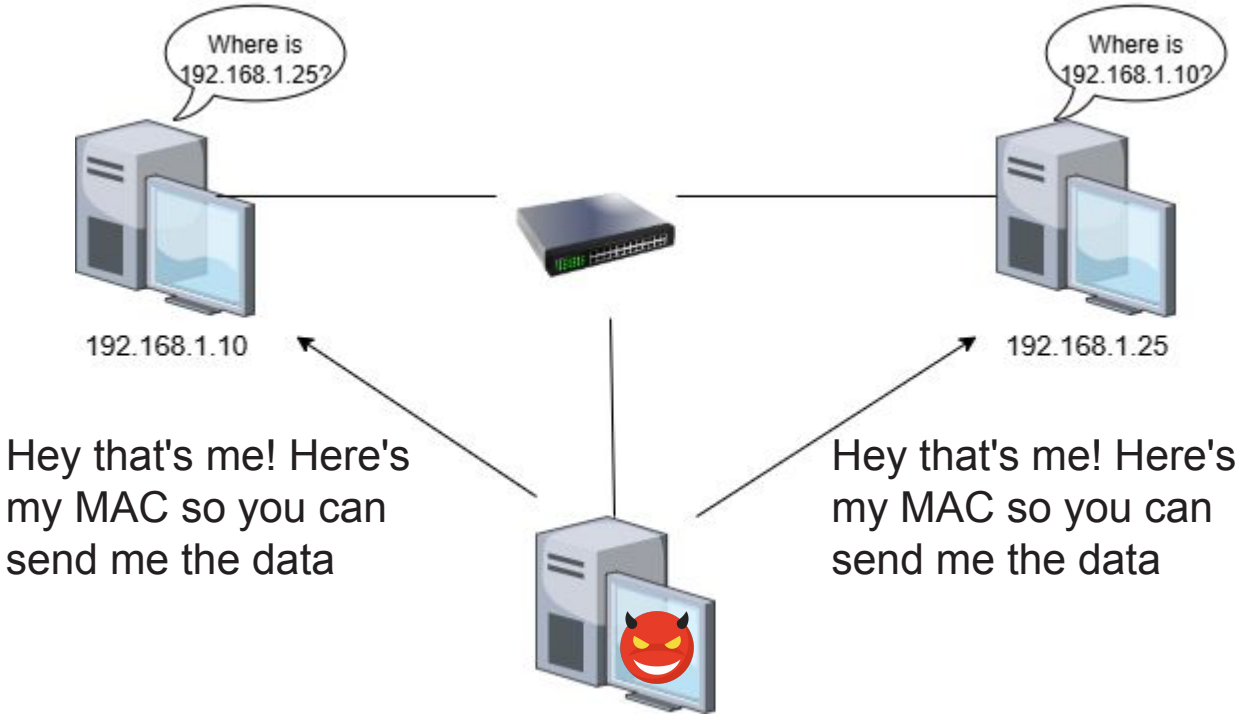
Benefits of a switch

- Reduce network congestion
  - Traffic sent only to where it needs to go
  - Multiple systems can transmit at the same time
- Reduce CPU time on each system
  - Only see traffic you need to process
- Provide security through obscurity
  - Most systems cannot see all traffic
- Admin can set a port to monitor traffic when needs
  - Called "span", "mirror", or "copy" port depending on vendor

How to attack a switch

- Layer 2 is typically unauthenticated
  - Trivial to spoof or forge
- Provides opportunities for traffic hijacking
- Could permit me to see data or change stream
- High end switches have protection features
- But not all techniques are defendable
- *Attacker must have local access to exploit*

ARP spoofing due to no authentication



Common ARP attacks

- ARP cache poisoning
  - Port stealing falls in this category
  - Overwrite ARP cache entry with attacker's MAC
- ARP cache flooding
  - Turn switch into a hub
- DHCP spoofing
- ICMP redirects
  - Type 5, code 0 or 1

ARP defense

- ARP cache poisoning
  - Dynamic ARP inspection
- ARP cache flooding
  - Limit number of MACs per port
- DHCP spoofing
  - DHCP snooping
- ICMP redirects
  - Disable dynamic learning of route info (ouch)

WiFi deauthentication attack

- Most of WiFi comms are encrypted/authenticated
- Deauthentication packets are not
- Disconnects endpoint from wireless Access Point (AP)
- Evil twin attack - connect user to rogue AP
- Force repeated WPA 4-way handshakes
  - Improves the chances of cracking AP password
- Root cause is poor authentication at layer 2
- Will go deeper after covering VPN technology

Next week on Fireside Fridays!!!

- Routing and VLANs!
- VLANs - creating multiple logical networks over a single physical medium
- Routing protocols - Link state, distance vector and static OH MY!
- Same bat time, same bat webcast link :-)

Wrap up

- Thank you for attending!
- Certs & video usually go out in 24 hours
- If you have any lingering questions, the Discord channel will remain active
  - Also a good chance to socialize with others in the class
  - Have other tips and tricks? Please share with others!
  - Posting screenshots can be helpful :-)