Internet Security

Data Link Layer (MAC)

Packet's Hop-by-hop transmission

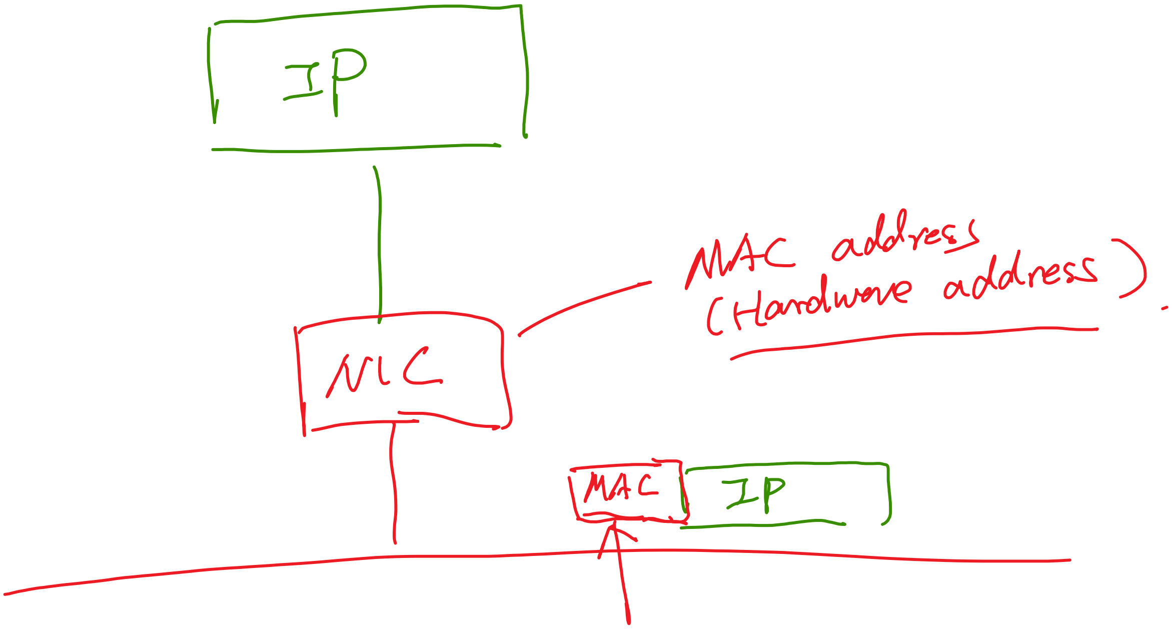
Network Layer (IP) Layer 3

MAC Layer

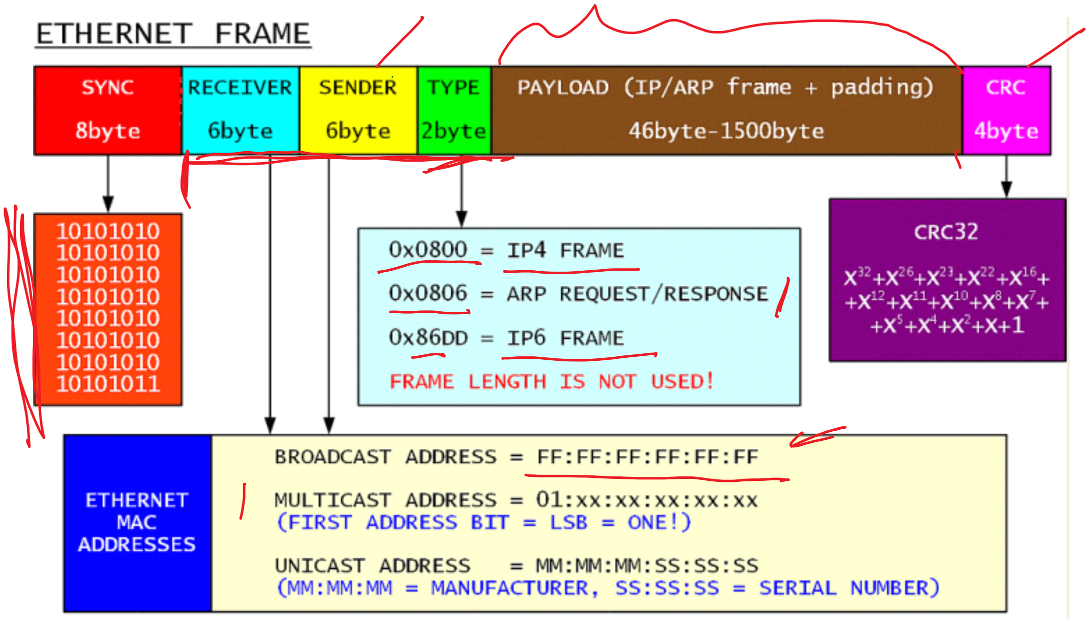
Data Link Layer Layer 2

physical Layer : Layer 1

Data Link Layer (MAC Layer)



Ethernet Frame



ETHERNET FRAME

SYNC	RECEIVER	SENDER	TYPE	PAYLOAD (IP/ARP frame + padding)	CRC
8byte	6byte	6byte	2byte	46byte-1500byte	4byte

10101010
10101010
10101010
10101010
10101010
10101010
10101010
10101011

0x0800 = IP4 FRAME

0x0806 = ARP REQUEST/RESPONSE

0x86DD = IP6 FRAME

FRAME LENGTH IS NOT USED!

CRC32

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

ETHERNET MAC ADDRESSES

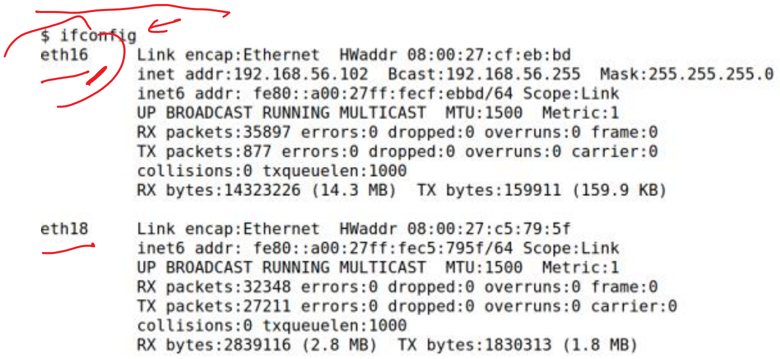
BROADCAST ADDRESS = FF:FF:FF:FF:FF:FF

MULTICAST ADDRESS = 01:xx:xx:xx:xx:xx
(FIRST ADDRESS BIT = LSB = ONE!)

UNICAST ADDRESS = MM:MM:MM:SS:SS:SS
(MM:MM:MM = MANUFACTURER, SS:SS:SS = SERIAL NUMBER)

MAC Address Example

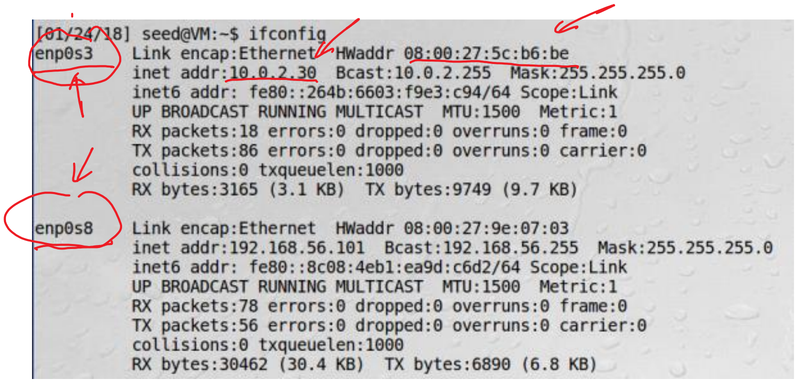
Ubuntu 12.04



```
$ ifconfig
eth16     Link encap:Ethernet  HWaddr 08:00:27:cf:eb:bd
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecf:ebbd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:35897 errors:0 dropped:0 overruns:0 frame:0
          TX packets:877 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14323226 (14.3 MB)  TX bytes:159911 (159.9 KB)

eth18     Link encap:Ethernet  HWaddr 08:00:27:c5:79:5f
          inet6 addr: fe80::a00:27ff:fec5:795f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32348 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27211 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2839116 (2.8 MB)  TX bytes:1830313 (1.8 MB)
```

Ubuntu 16.04

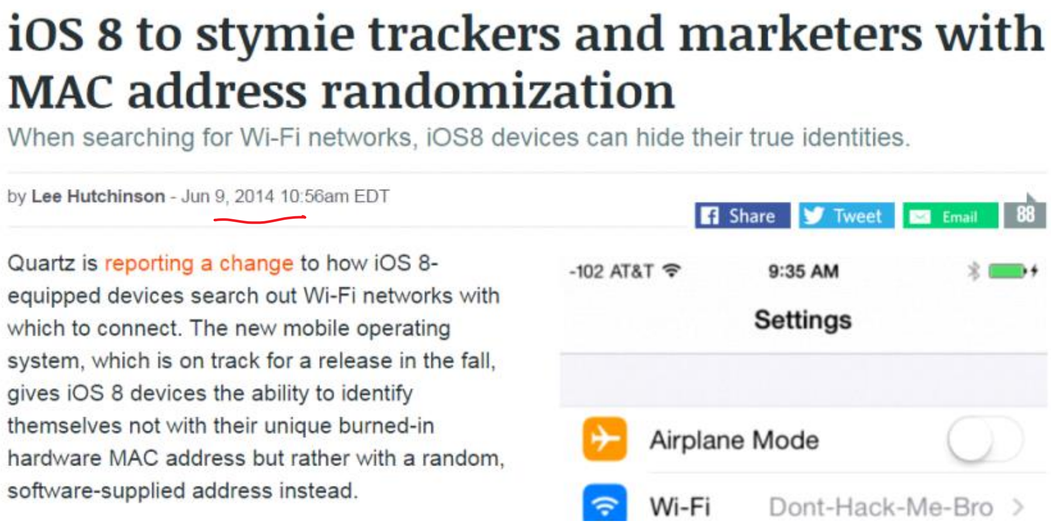


```
[01/24/18] seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5c:b6:be
          inet addr:10.0.2.30  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::264b:6603:f9e3:c94/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3165 (3.1 KB)  TX bytes:9749 (9.7 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:9e:07:03
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::8c08:4eb1:ea9d:c6d2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30462 (30.4 KB)  TX bytes:6890 (6.8 KB)
```

Privacy Issue Related to MAC

Wi-Fi



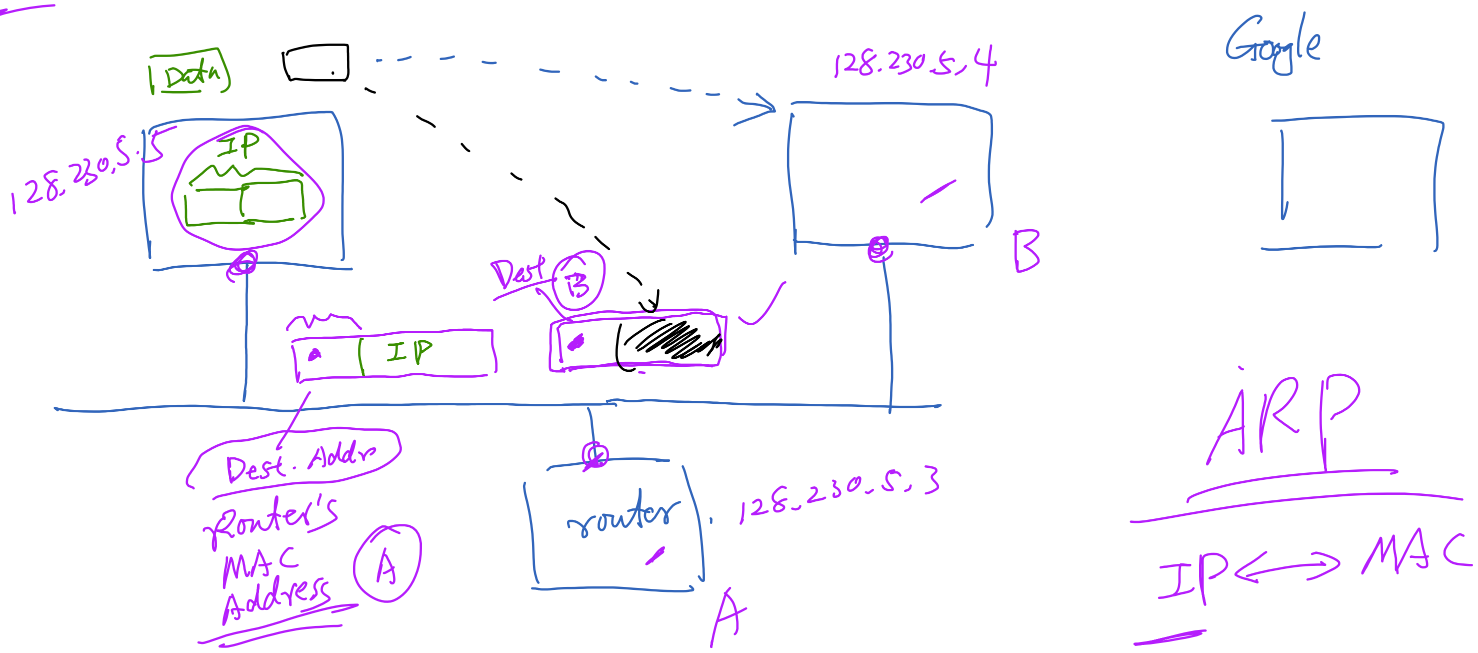
iOS 8 to stymie trackers and marketers with MAC address randomization

When searching for Wi-Fi networks, iOS8 devices can hide their true identities.

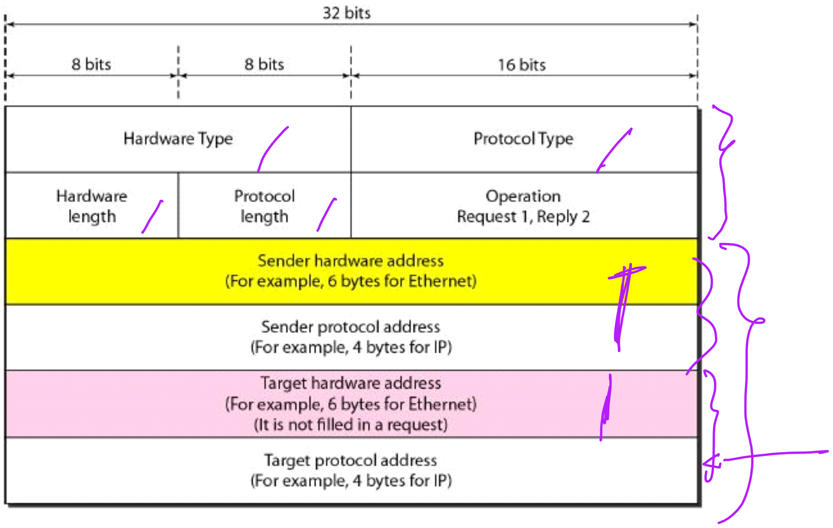
by **Lee Hutchinson** - Jun 9, 2014 10:56am EDT

Quartz is reporting a change to how iOS 8-equipped devices search out Wi-Fi networks with which to connect. The new mobile operating system, which is on track for a release in the fall, gives iOS 8 devices the ability to identify themselves not with their unique burned-in hardware MAC address but rather with a random, software-supplied address instead.

ARP: IP Address to Ethernet Address



ARP Format



32 bits		
8 bits	8 bits	16 bits
Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

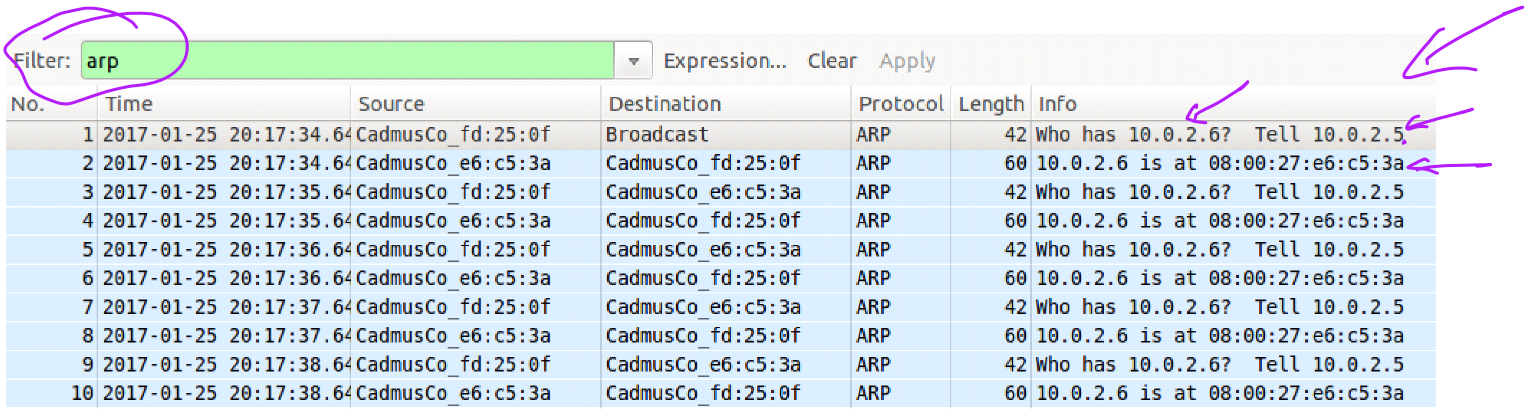
APR

Prot 1 → Prot 2

IPV4 → MAC

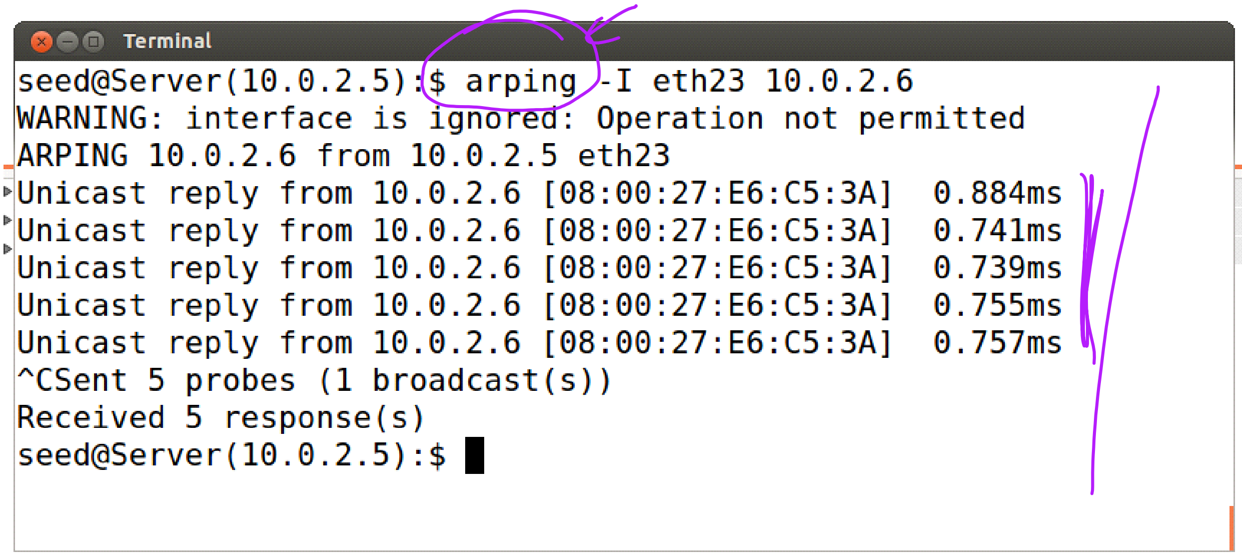
IPV6 → MAC

Send ARP Requests



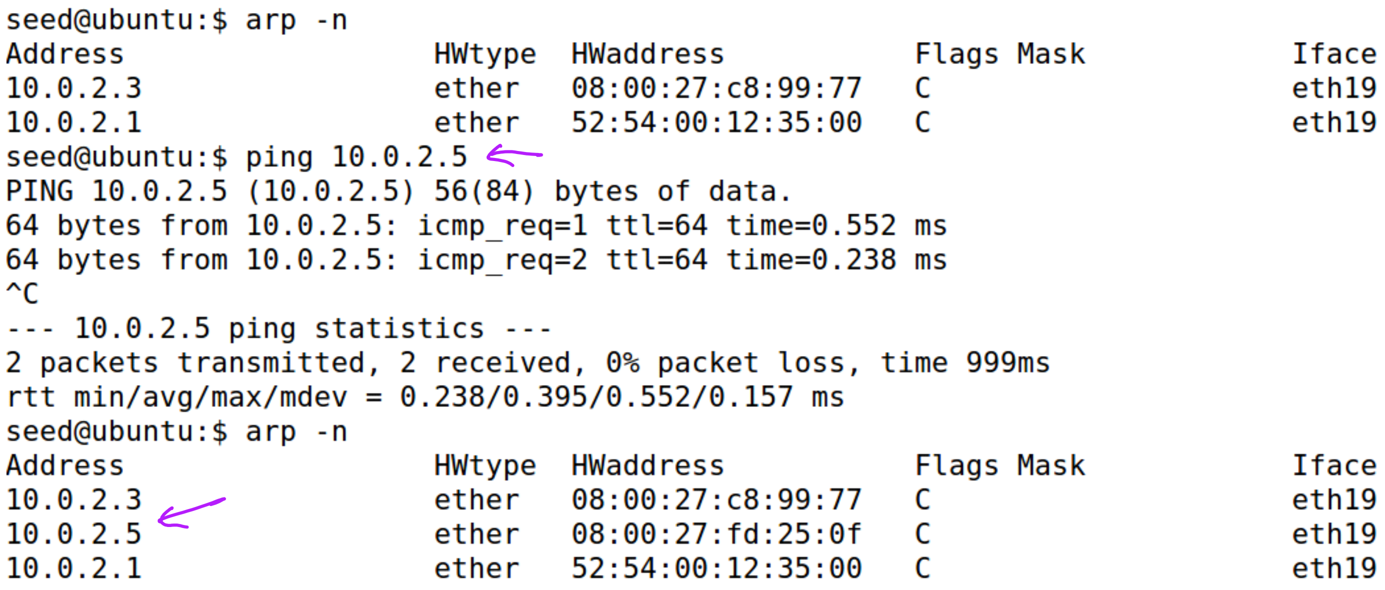
Filter: arp

No.	Time	Source	Destination	Protocol	Length	Info
1	2017-01-25 20:17:34.64	CadmusCo_fd:25:0f	Broadcast	ARP	42	Who has 10.0.2.6? Tell 10.0.2.5
2	2017-01-25 20:17:34.64	CadmusCo_e6:c5:3a	CadmusCo_fd:25:0f	ARP	60	10.0.2.6 is at 08:00:27:e6:c5:3a
3	2017-01-25 20:17:35.64	CadmusCo_fd:25:0f	CadmusCo_e6:c5:3a	ARP	42	Who has 10.0.2.6? Tell 10.0.2.5
4	2017-01-25 20:17:35.64	CadmusCo_e6:c5:3a	CadmusCo_fd:25:0f	ARP	60	10.0.2.6 is at 08:00:27:e6:c5:3a
5	2017-01-25 20:17:36.64	CadmusCo_fd:25:0f	CadmusCo_e6:c5:3a	ARP	42	Who has 10.0.2.6? Tell 10.0.2.5
6	2017-01-25 20:17:36.64	CadmusCo_e6:c5:3a	CadmusCo_fd:25:0f	ARP	60	10.0.2.6 is at 08:00:27:e6:c5:3a
7	2017-01-25 20:17:37.64	CadmusCo_fd:25:0f	CadmusCo_e6:c5:3a	ARP	42	Who has 10.0.2.6? Tell 10.0.2.5
8	2017-01-25 20:17:37.64	CadmusCo_e6:c5:3a	CadmusCo_fd:25:0f	ARP	60	10.0.2.6 is at 08:00:27:e6:c5:3a
9	2017-01-25 20:17:38.64	CadmusCo_fd:25:0f	CadmusCo_e6:c5:3a	ARP	42	Who has 10.0.2.6? Tell 10.0.2.5
10	2017-01-25 20:17:38.64	CadmusCo_e6:c5:3a	CadmusCo_fd:25:0f	ARP	60	10.0.2.6 is at 08:00:27:e6:c5:3a



```
seed@Server(10.0.2.5):$ arping -I eth23 10.0.2.6
WARNING: interface is ignored: Operation not permitted
ARPING 10.0.2.6 from 10.0.2.5 eth23
Unicast reply from 10.0.2.6 [08:00:27:E6:C5:3A]  0.884ms
Unicast reply from 10.0.2.6 [08:00:27:E6:C5:3A]  0.741ms
Unicast reply from 10.0.2.6 [08:00:27:E6:C5:3A]  0.739ms
Unicast reply from 10.0.2.6 [08:00:27:E6:C5:3A]  0.755ms
Unicast reply from 10.0.2.6 [08:00:27:E6:C5:3A]  0.757ms
^CSent 5 probes (1 broadcast(s))
Received 5 response(s)
seed@Server(10.0.2.5):$ 
```

ARP Cache



```
seed@ubuntu:$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:c8:99:77   C                     eth19
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth19
seed@ubuntu:$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.552 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.238 ms
^C
--- 10.0.2.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.238/0.395/0.552/0.157 ms
seed@ubuntu:$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:c8:99:77   C                     eth19
10.0.2.5                 ether   08:00:27:fd:25:0f   C                     eth19
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth19
```

Question

Observe the diffence of the following two commands, and explain your observation.

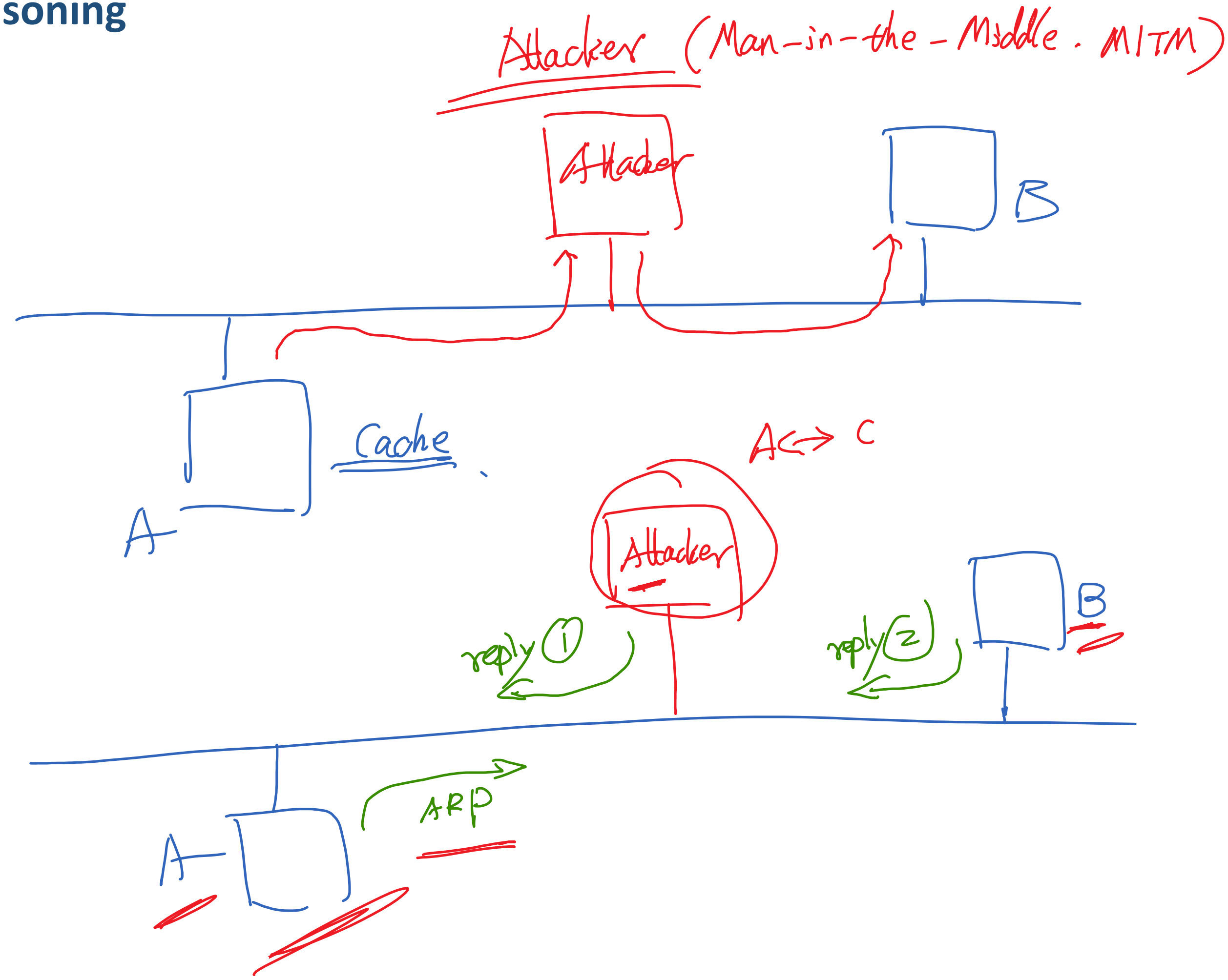
- `ping 1.2.3.4` (non-existing, not on the local network)
- `ping 10.0.2.9` (non-existing, on local network)

1.2.3.4 → Router's MAC

10.0.2.9 → 10.0.2.9's MAC

10.0.2.5

ARP Cache Poisoning



Potential Damage

Question: ARP Cache Poisoning

President Trump claims that hackers have launched an ARP cache-poisoning attack from Russia on the computer networks inside the Trump Tower. Is this claim true or false?

Monitor

Wifi

Sniffing

Ether