ARP - Address Resolution Protocol

```
    30 5.018678      02:42:e7:08:96:52   02:42:0a:00:00:02   ARP      42 Who has 10.0.0.2? Tell 10.0.0.1
    31 5.018686      02:42:0a:00:00:02   02:42:e7:08:96:52   ARP      42 10.0.0.2 is at 02:42:0a:00:00:02
```

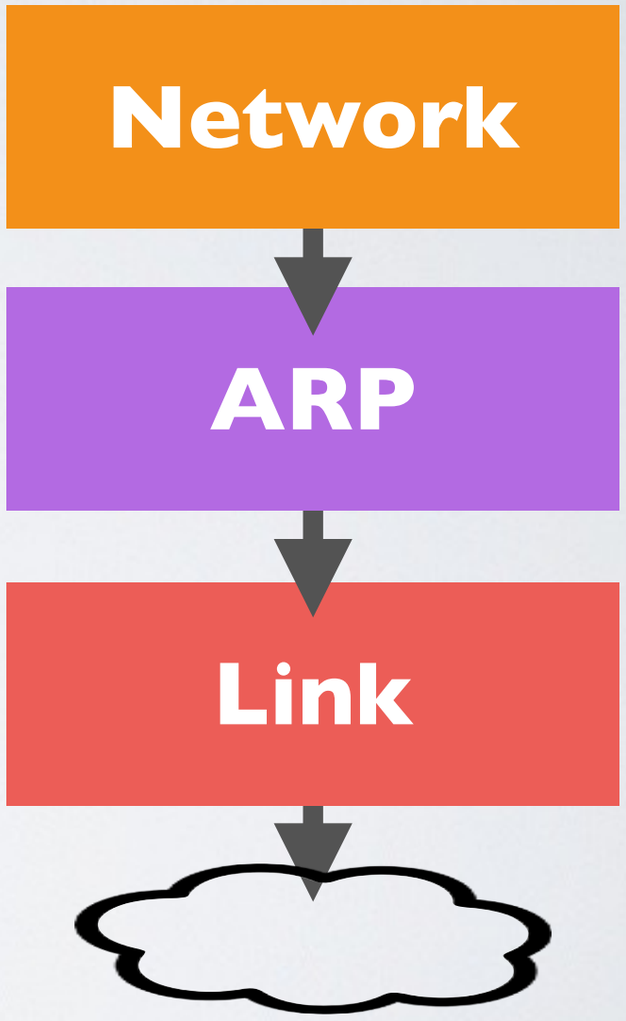
```
▸ Frame 31: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: 02:42:0a:00:00:02 (02:42:0a:00:00:02), Dst: 02:42:e7:08:96:52 (02:42:e7:08:96:52)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 02:42:0a:00:00:02 (02:42:0a:00:00:02)
    Sender IP address: 10.0.0.2
    Target MAC address: 02:42:e7:08:96:52 (02:42:e7:08:96:52)
    Target IP address: 10.0.0.1
```

```
▸ Frame 82: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_30:da:bf (00:0c:29:30:da:bf), Dst: VMware_e7:52:23 (00:50:56:e7:52:23)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_30:da:bf (00:0c:29:30:da:bf)
    Sender IP address: 192.168.23.128
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.23.2
```

```
0010  08 00 06 04 00 01 00 0c  29 30 da bf c0 a8 17 80   ........ )0......
```

Sender IP address (arp.src.proto_ipv4), 4 bytes Packets: 299 · Displayed: 299 (100.0%) Profile: Default

```
student@d27-vm:~/labs-review/packet-sniffing-starter$ ip --brief address show
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             192.168.23.128/24 fe80::7fc8:9a37:c4e:c01b/64
docker0          DOWN           172.17.0.1/16
student@d27-vm:~/labs-review/packet-sniffing-starter$ arp -i ens33
Address                  HWtype  HWaddress           Flags Mask            Iface
169.254.169.254                  (incomplete)                              ens33
192.168.23.254           ether   00:50:56:e5:4f:6c   C                     ens33
_gateway                 ether   00:50:56:e7:52:23   C                     ens33
192.168.23.1             ether   00:50:56:c0:00:08   C                     ens33
student@d27-vm:~/labs-review/packet-sniffing-starter$ ip neigh show
169.254.169.254 dev ens33  FAILED
192.168.23.254 dev ens33 lladdr 00:50:56:e5:4f:6c STALE
192.168.23.2 dev ens33 lladdr 00:50:56:e7:52:23 REACHABLE
192.168.23.1 dev ens33 lladdr 00:50:56:c0:00:08 REACHABLE
student@d27-vm:~/labs-review/packet-sniffing-starter$
```



ARP Cache Poisoning

integrity
availability

➡ An attacker can broadcast fake IP-MAC mappings to the other hosts on the network

e.g. DOS and MITM attacks