
# Electronic Security Meeting #2: ARP Cache Poisoning

# Quick intro to network Layer 2/Layer 3 protocol communication

Layer2:

**'Data' layer**

- Defines how data is formatted right before it touches the media
- wifi, ethernet, ATM, PPPoE....
- data units typically refered to as "frames"
- the most basic 'LAN' exists in this space

Layer3:

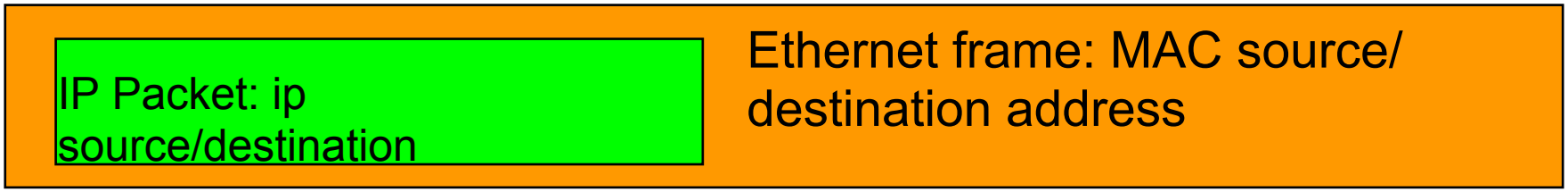
'Network' Layer

- Logically defines a 'network' and provides means for inter and intra network communication
- Routing happens here
- IPv4, IPv6, IPX/SPX...

**Ethernet** is a Layer 2 protocol, IP is Layer 3

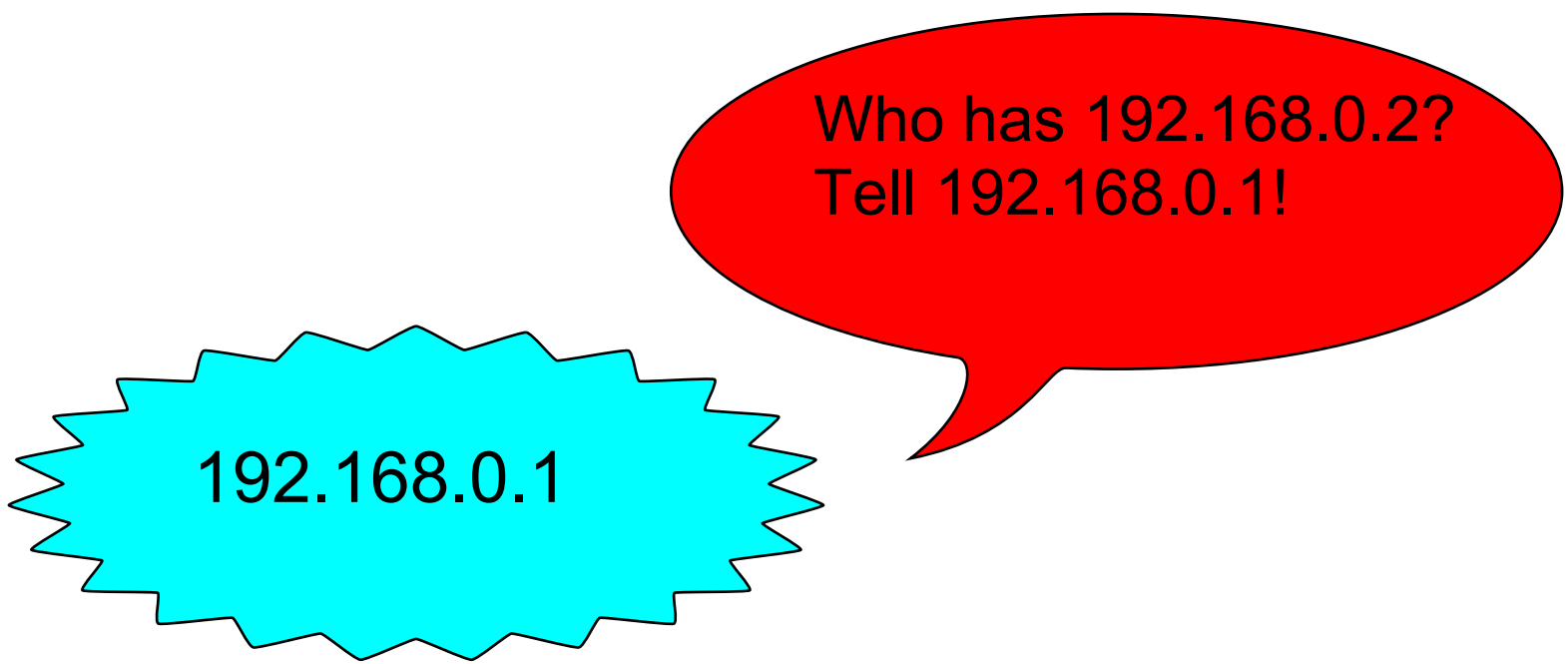
**ARP/RARP** lives between Layer 2 and Layer 3

# Protocol Multiplexing/Encapsulation: Layer2/3




ARP **translates** IP addresses in to **MAC addresses** for an ip enabled ethernet host

- Each host has an "ARP Cache" where it stores ip address -> MAC address mapings
- Allows ip enabled applications to operate oblivious of LAN type



# When Good Packets LIE

MAC: ff:ff:ff:ff:12
IP: 192.168.0.1

GARP message:
Hey ff:ff:ff:ff:01!
**ff:ff:ff:ff:23** has
**192.168.0.1!**

MAC: ff:ff:ff:ff:01
IP: 192.168.0.3

MAC: ff:ff:ff:ff:23
IP: **192.168.0.6**

## Consequence:

host ff:ff:ff:ff:01updates their ARP cache map of ff:ff:ff:ff:12->192.168.0.1 to ff:ff:ff:ff:23->192.168.0.1
ALL traffic sent to 192.168.0.1 never makes it to the indended host, and we **NEVER KNOW**!

## GARP: Gratuitous ARP

- Allows any host to send a directed update to a specific host
- Useful when a host switches Layer2 devices (ie, wired to wireless)