ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 5: Layer 2 attacks and Defenses

Outline

- TCP/IP Network Layers Recap
- Layer 2 definition and addressing scheme
- Layer 3 definition and addressing scheme
- Why both addressing modes?
- Address Resolution Protocol (ARP)
- ARP Cache Poisoning

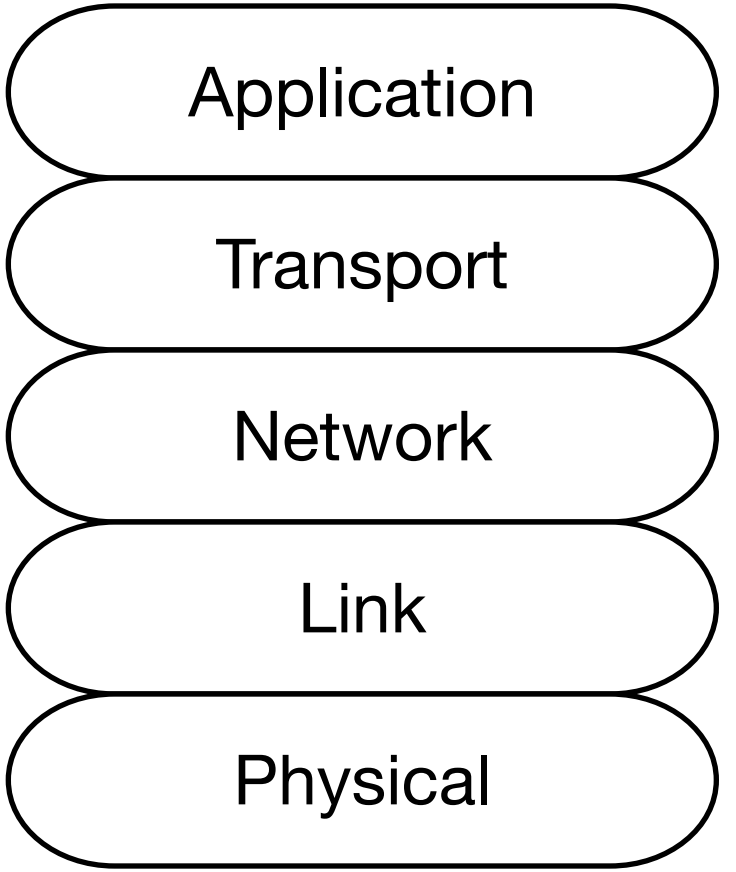
TCP/IP Protocol Stack

Layer 3: Network layer

- Supports end-end source to destination routing

Layer 2: Data Link layer

- Supports data transfer between neighbors



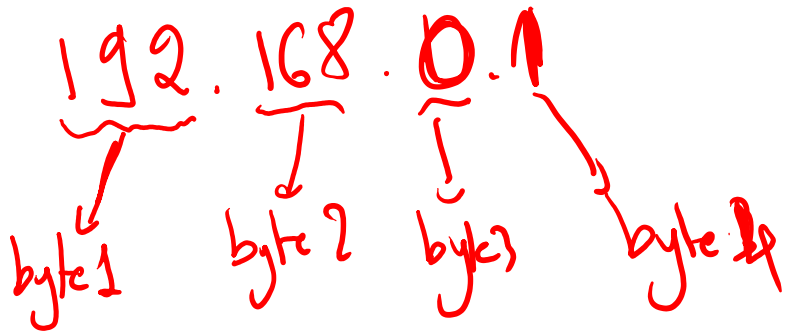
The Network Layer (Layer 3)

- Provides end-to-end communication
- Every host is associate with (at least) one Internet Protocol (IP) address
- Layer 3 packet is called a **datagram**

Provides two functions:

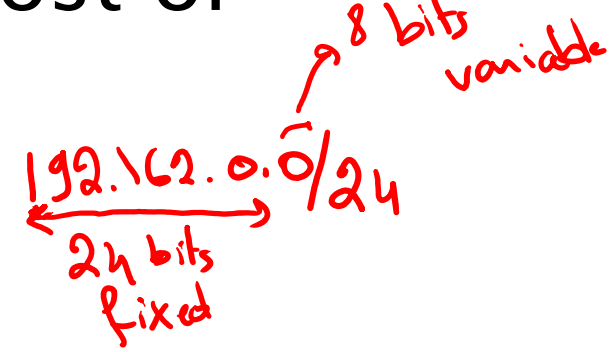
- Forwarding
- Routing

Layer 3 Addressing



IP Address

- 32-bit identifier associate with each host or interface to a router
- 64-bits identified for IP version 6



Interface

- Connection between a host/router and a physical link

The Data Link Layer (Layer 2)

- Hop to hop communication
- Directly connects to the physical layer (Network Interface Card, Wifi Access Card, etc.)
- Layer 2 packet is called a **frame**
- Responsible for moving datagrams ***between physically adjacent*** nodes in a network

Layer 2 Addressing

- Media Access Control (MAC) address
- 48 bits on the wire

00:aa:ff:bb

- NIC has a **local network-unique** MAC address
  - Traditionally imprinted at manufacturing time
  - Now being software generated ➔ Collisions!

Ethernet Frame

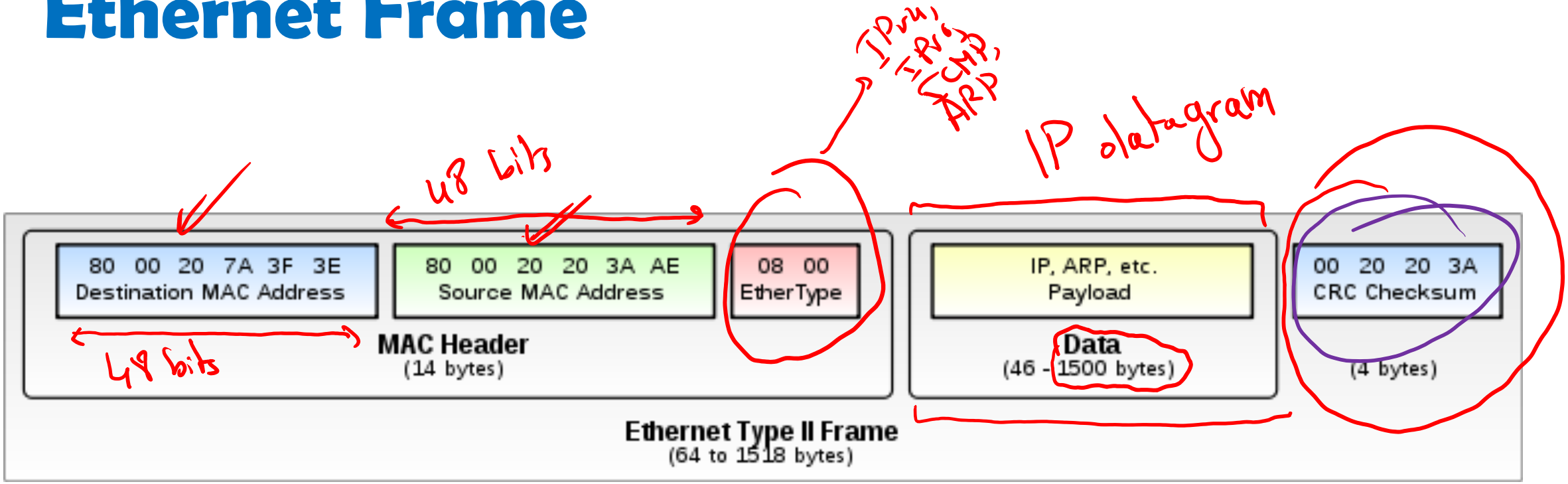
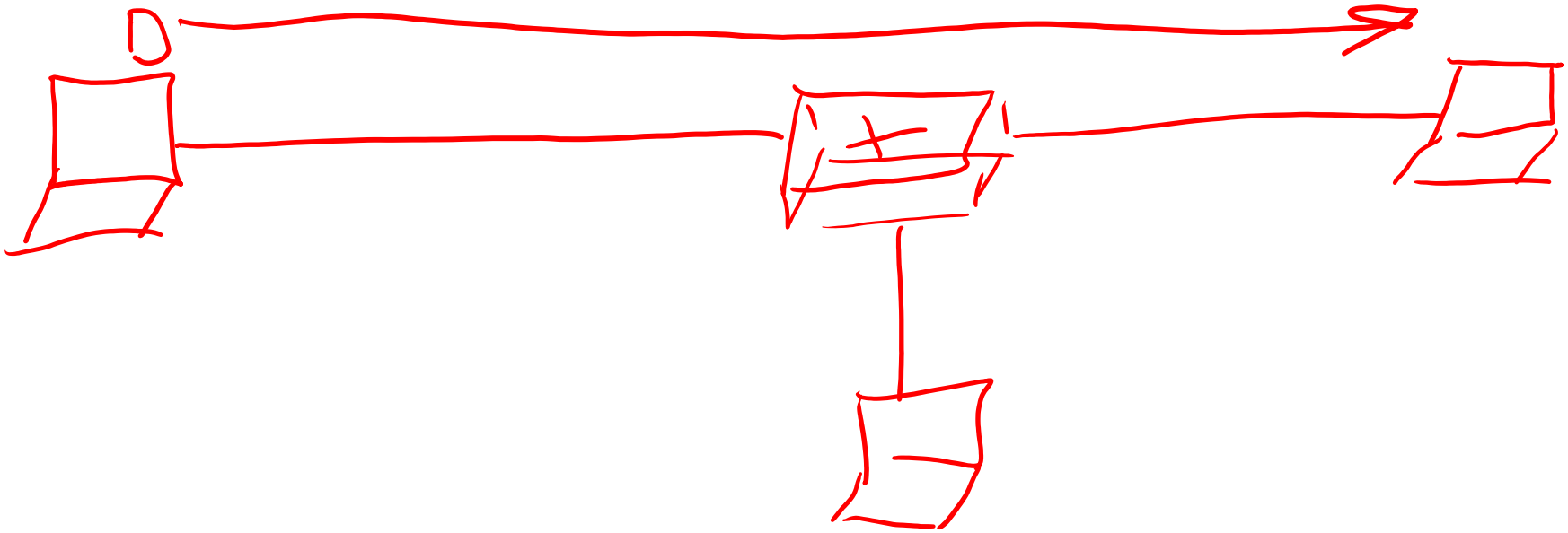


Image source: https://en.wikipedia.org/wiki/Ethernet_frame

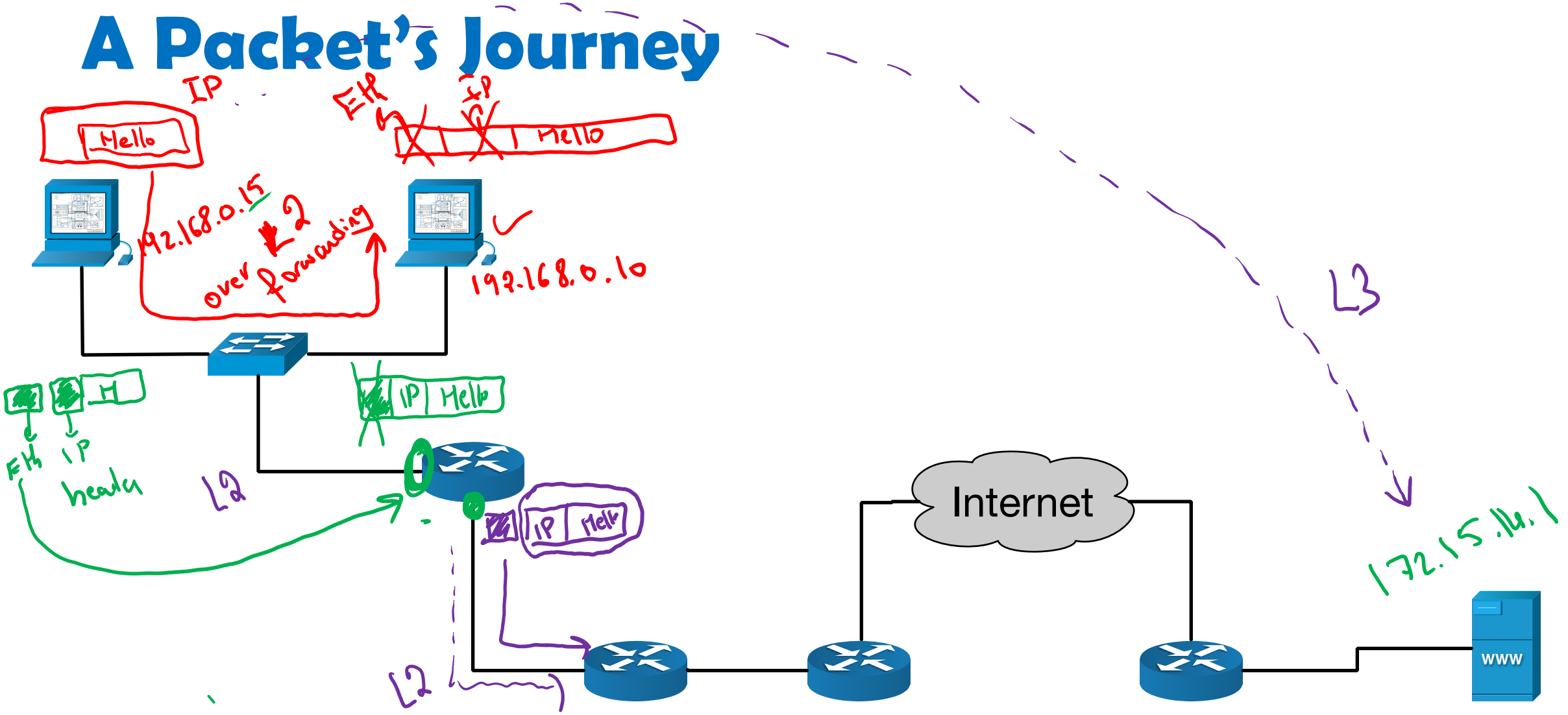
Question time

① IP addresses are not static

- Why do we need two types of addresses?



A Packet's Journey



Address Resolution Protocol (ARP)

- MAC addresses and IP addresses are independent
- ARP correlates a MAC address with an IP address

- Note: IP addresses are volatile these days
- So mappings must be able to change

ARP Message Format

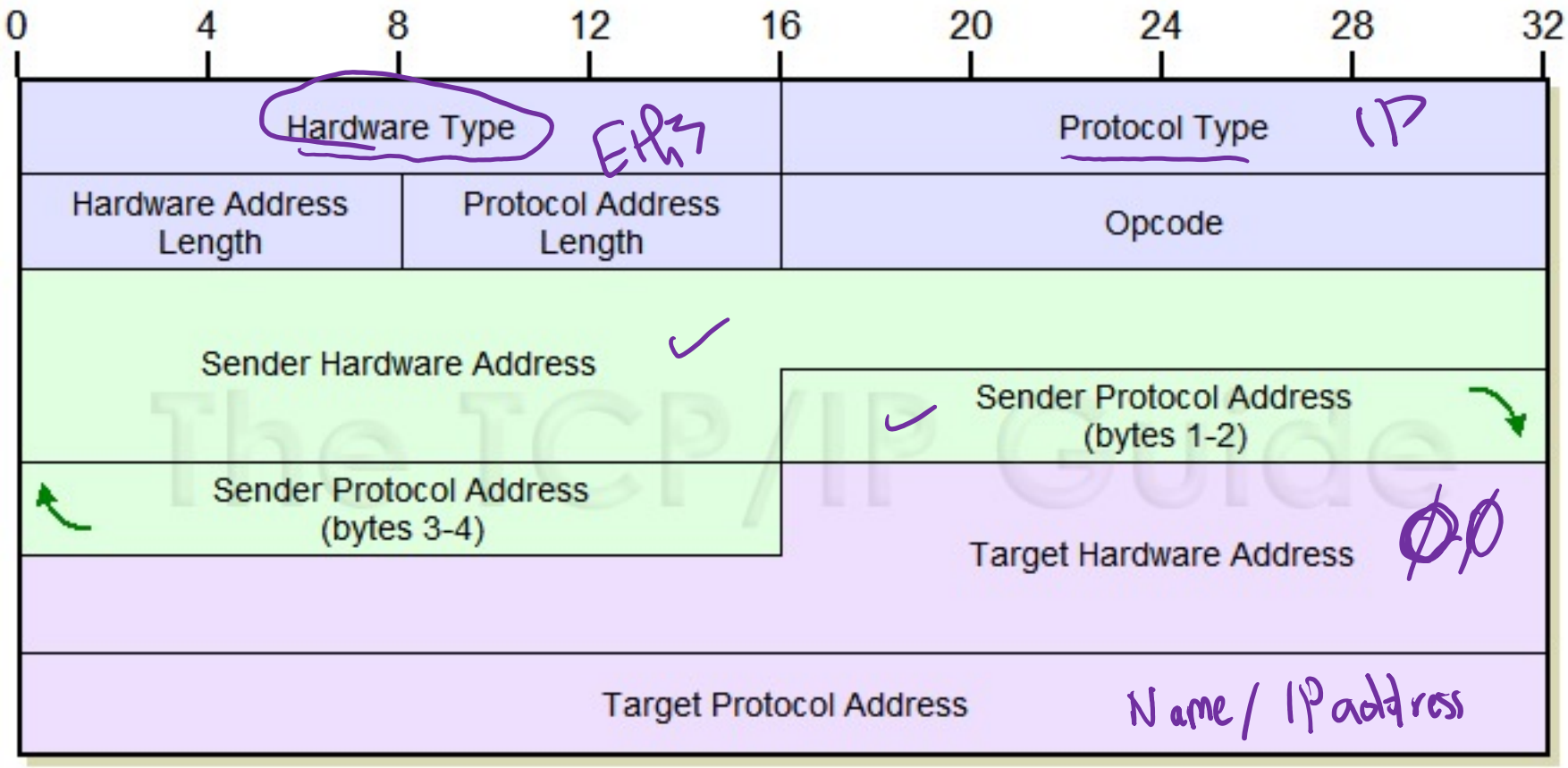


Image source: http://www.tcpipguide.com/free/t_ARPMessageFormat.htm

ARP Demo

- Use packet captures from the GitHub repo

The ARP Cache

- Hosts cache IP to MAC mapping in ARP cache
- Checkout `arp -n`
- Each entry will timeout and will be removed

ARP Cache Refresh

The ARP Cache can be refreshed upon 3 events:

1. Receiving an **ARP Request**

2. Receiving an **ARP Reply**

3. Receiving an **ARP gratuitous message**

Challenges

- ARP is **stateless**
  - No correlation between an ARP request and an ARP reply
- **No authentication**
  - Cannot really verify who is sending the messages

ARP Cache Poisoning