Supporting Protocols ARP and ICMP

Kameswari Chebrolu

Recap

- Forwarding needs IP to MAC address mapping
  - Service provided by ARP protocol
- Network layer needs to provide means for debugging (error signaling) and for router-host communication (determine MTU size, indicate better routes, provide netmask info etc)
  - Service provided by ICMP protocol

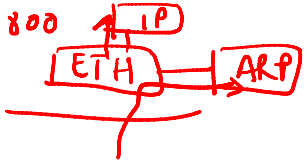
Problem Statement

- IP layer forwarding is based on IP addresses
- Next-hop delivery based on Link addresses (MAC)
- Need to perform IP to MAC address translation
- Answer: Address Resolution Protocol (ARP)

- what layer?
- How do you ensure ARP process gets the relevant packets? → demux
- what address should the frame carry?
- what messages would you send & how do you act on a message received message?

Address Resolution Protocol (ARP)

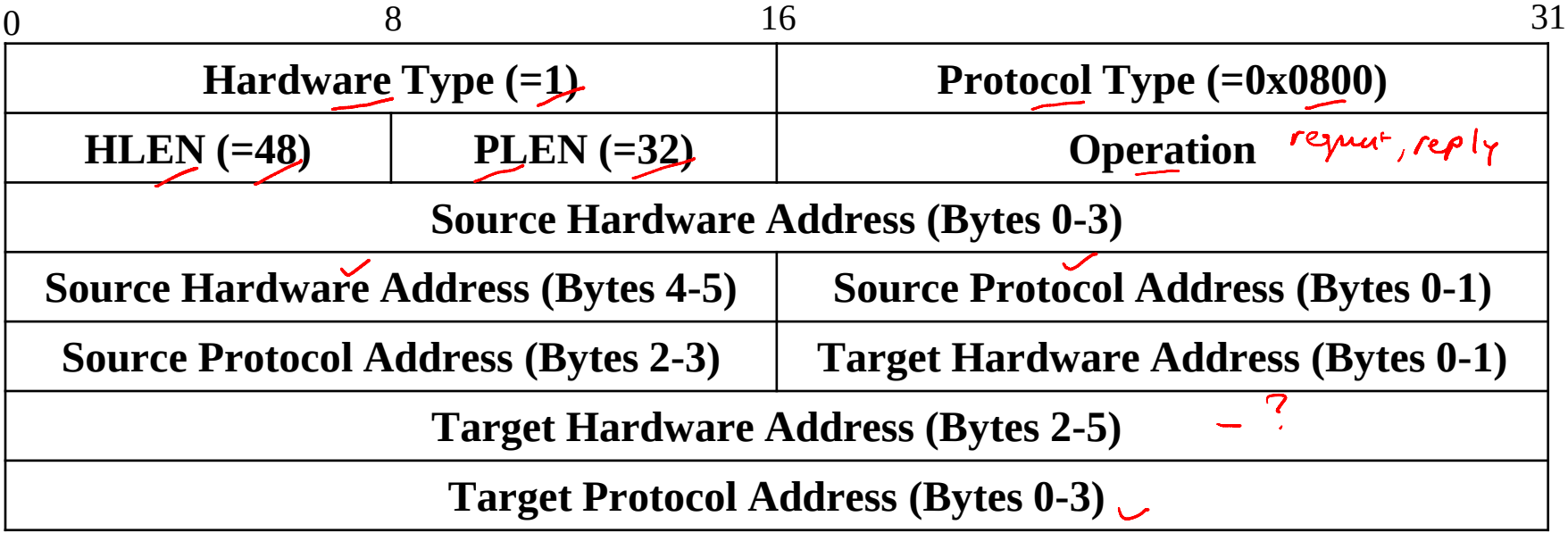
- Operates at Link layer (Frame type = 0x0806)
- Based on broadcast: "What is the MAC address corresponding to given IP address?"
  - Host with matching IP address replies
- Each host maintains a cache with IP to MAC translations
  - Entries in cache timed out periodically (15 min)



Address Resolution Protocol (ARP)

- Originator: Add entry to cache corresponding to target
- Target: Add entry to cache corresponding to the originator (sender)
- Intermediate hosts: Refresh existing entries
- When forwarding a datagram, check cache, if no mapping, invoke ARP

ARP Packet Format



Numbers in brackets capture mapping
IP addresses to Ethernet addresses

Gratuitous ARPs

- Generated by a host to inform others of its IP to MAC mapping
- Could be a request or reply
  - If request, no reply will occur
  - If reply, there was no preceding request
  - Source IP = destination IP = IP of machine generating gratuitous ARP
  - Target MAC: ff:ff:ff:ff:ff:ff

Uses of Gratuitous ARPs

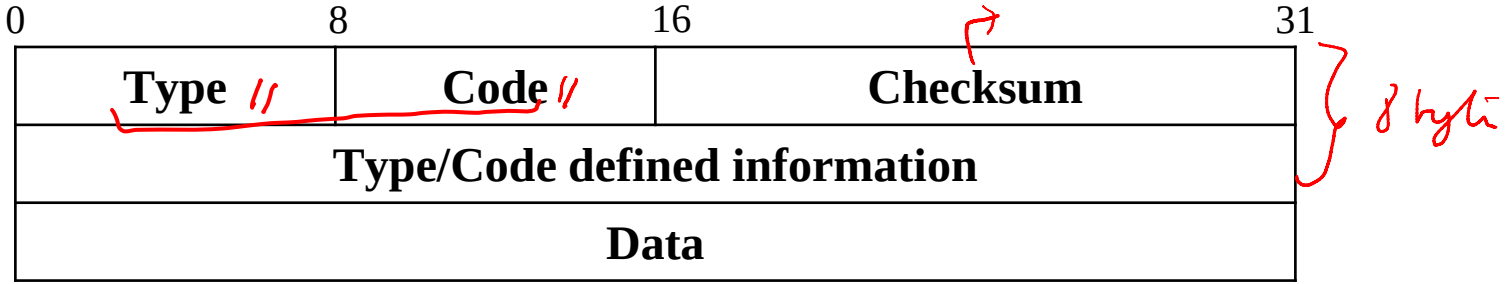
- Issued whenever IP or MAC address of an interface changes or brought up from down state
  - Help rectify cached ARP entries
  - Report IP address conflicts (duplicate IP)
  - Inform bridges of the location of new host

ICMP: Internet Control Message Protocol

- Used by hosts & routers to communicate network-level information
  - Error reporting: unreachable host, network, port, protocol
  - Diagnostic purposes: Echo request/reply (used by ping)
  - Routing: Source quench

ICMP Packet Format

- ICMP messages carried in IP datagrams
- 8 bytes of header followed by data.
- Data field in error messages carry
  - entire IP header and first 8 bytes of data of IP packet that caused the error



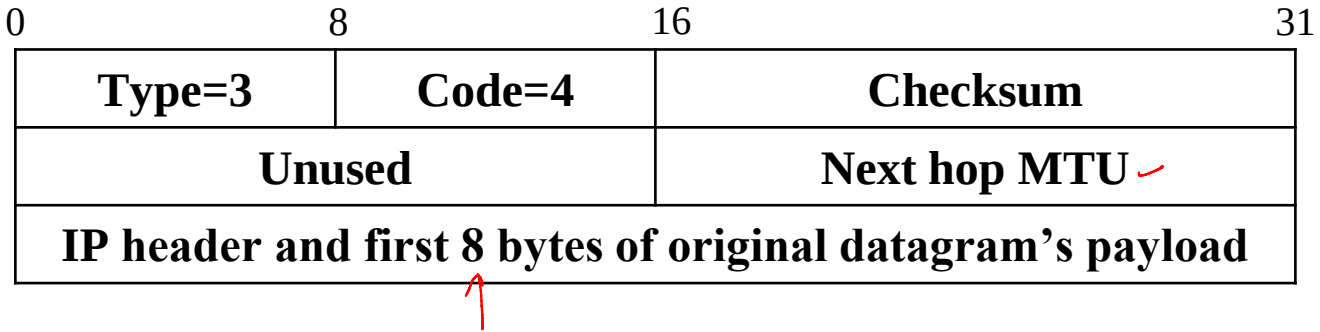
Select ICMP Messages

Type	Code	Description
0	0	Echo Reply (Ping)
3	0	Destination network unreachable
3	1	Destination host unreachable
3	3	Destination port unreachable
3	4	Fragmentation required, DF flag set
3	6	Destination network unknown
3	7	Destination host unknown

Select ICMP Messages

Type	Code	Description
4	0	Source Quench
5	0	Redirect datagram for the network
8	0	Echo request (Ping)
11	0	TTL expired
12	0	Bad IP header
13	0	Timestamp
14	0	Timestamp reply
17	0	Address mask request
18	0	Address mask reply

Example: Fragmentation Required



Traceroute

- Source sends series of UDP segments to destination one after another
  - First has TTL =1
  - Second has TTL=2, etc.
  - Destination port is set to an unlikely number

Traceroute

- When n^{th} datagram arrives to nth router:
  - Router discards datagram
  - Sends to source an ICMP message (type 11, code 0)
  - Message includes name of router& IP address
- For each ICMP message, sending host notes router id and RTT time
- Sending host stops when it gets ICMP message (type 3, code 3)

Summary

- Studied two useful protocols: ARP and ICMP
- ARP is needed for forwarding
  - Performs IP to MAC address translation
- ICMP helps with error reporting and host signaling