ARP and ICMP

Manas Ranjan Lenka
School of Computer Engineering,
KIIT University

Why Address Resolution Protocol(ARP)?

- 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)

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)

- When forwarding a datagram, check ARP cache, if no mapping, invoke ARP

ARP Packet Format

0	8	16	31
Hardware Type (=1)		Protocol Type (=0x0800)	
HLEN (=48)	PLEN (=32)	Operation	
Source Hardware Address (Bytes 0-3)			
Source Hardware Address (Bytes 4-5)		Source Protocol Address (Bytes 0-1)	
Source Protocol Address (Bytes 2-3)		Target Hardware Address (Bytes 0-1)	
Target Hardware Address (Bytes 2-5)			
Target Protocol Address (Bytes 0-3)			

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
  - 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)

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

demux TCP = 6

- ICMP messages carried in IP datagrams

IP → ICMP

demux key : 1

- 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

0	8	16	31
Type	**Code**	**Checksum**	
Type/Code defined information			
Data			

8 bytes

which helps in diagnosing the problem that caused the ICMP message to be generated.

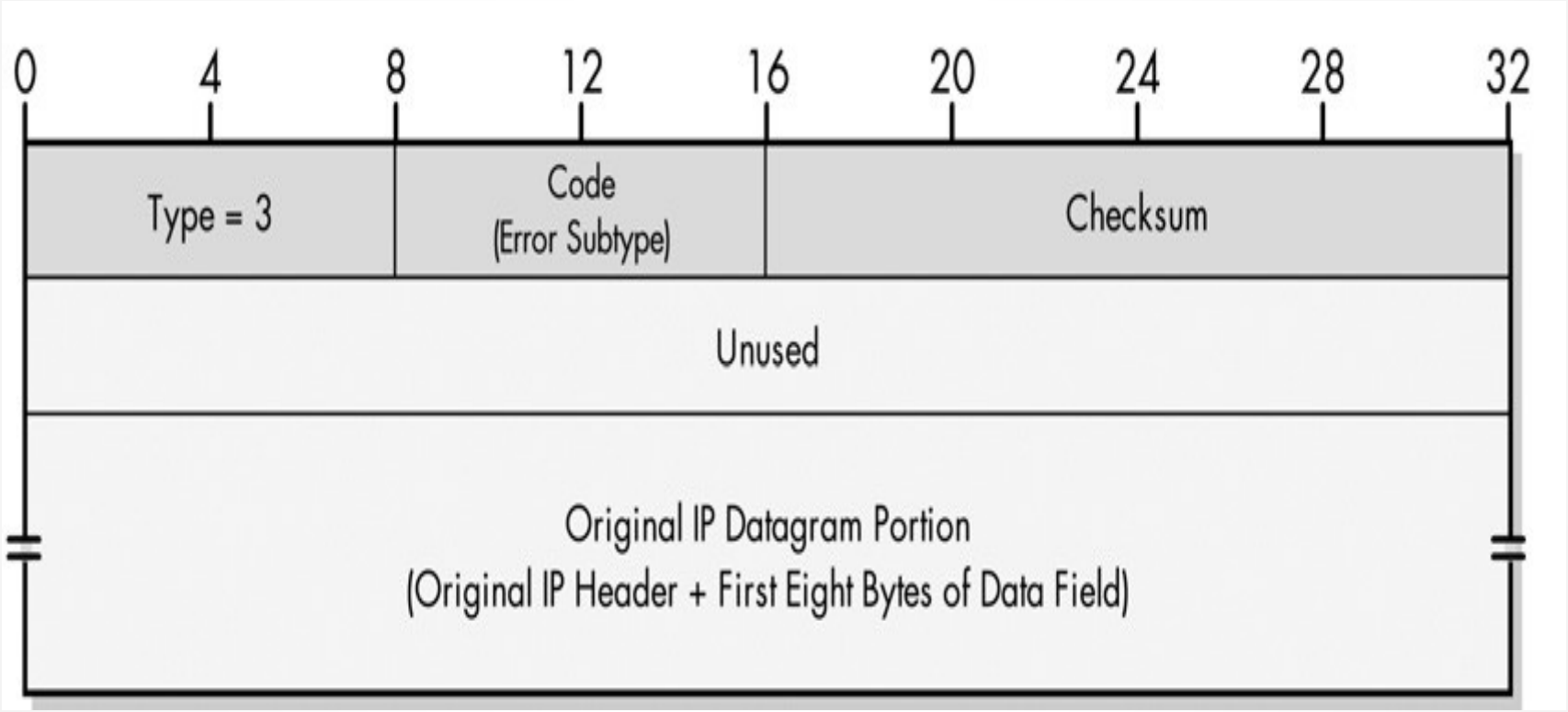
Select ICMP Messages

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

ICMPv4 Destination Unreachable message format



ICMPv4 Destination Unreachable message format

Limitations on ICMP Message Responses

Assume Device A encounters an error and sends an error report to Device B. Device B finds an error in Device A's message and sends an error report back to Device A. This results in a loop thereby clogging the network.

To prevent such problems, an ICMP error message must not be generated in response to any of the following:

- An ICMP Error Message
- A Broadcast or Multicast Datagram
- IP Datagram Fragments Except the First

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
- 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)