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)

ARP Packet Format

0	8	16	31
Hardware Type (=1)		Protocol Type (=0x0800)	
HLEN (=48)	PLEN (=32)	Operation	*request, reply*
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

Address Resolution Protocol (ARP)

- Originator: Add entry to cache corresponding to target

  → ARP Request

- ARP Reply

  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

Example

(A) : MAC corresponding to IP of B

ARP request → MAC header   src add   dst add → ff:ff: . . . .
    ↓   Payload
broadcast

src MAC   src IP   Target mac   Target IP
  ↑   ↑   ?   ↓
  A   A   B

ARP reply → MAC → src add B   dst : A
from B   → Payload   src MAC   src IP   Target MAC   Target IP
  ↓   B ← B   A   A
"unicast"

Cache A
  ↑
B IP → B MAC

Cache B
A IP → A MAC
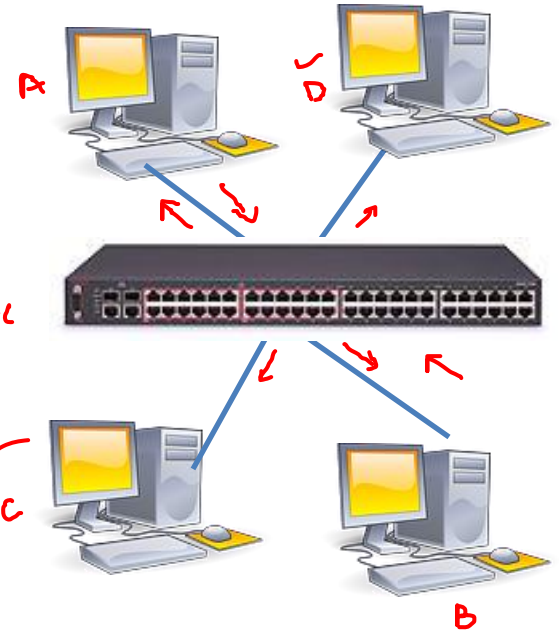
C,D   ARP request
        ↳ A → refresh   (reset timer)   C,D

      no entry A , ignore ARP request

Address Resolution Protocol (ARP)

- Originator: Add entry to cache corresponding to target IPaddr, MAC

- 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

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 = ?

(handwritten annotations:)

→ broadcast

own

MAC header   src MAC   dest
↑host   ff:ff...

ARP

Ethernet
ARP
    src, Target
   IP=?   IP=?

   src → MAC
   MAC

ff:ff → request } window
MAC → reply

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

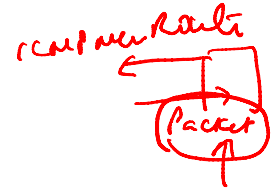# ICMP: Internet Control Message Protocol

- Used by hosts & routers to communicate network-level information

  - Error reporting: unreachable host, network, port, protocol

  - Diagnostic purposes: Echo request/reply (used by ping)
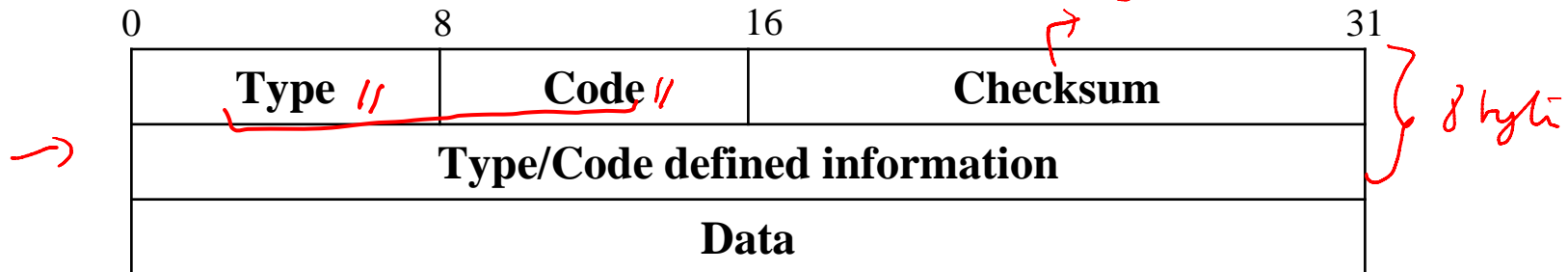
  - Routing: Source quench

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

[Handwritten annotations: demux, TCP = 6, IP → ICMP, demux key: 1, icmp new Route, Packet, entire ICMP message, 8 byte]

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

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

0	8	16	31

Type=3	Code=4	Checksum
Unused		Next hop MTU
IP header and first 8 bytes of original datagram's payload		

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   ← UDP
  ICMP error mssg

- Sending host stops when it gets ICMP message (type 3, code 3)   → destinal a port

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