ARP (Address Resolution Protocol)

ICMP (Internet Control Message Protocol)

Address Translation

- Map IP addresses into physical addresses
  - destination host
  - next hop router
- Techniques
  - encode physical address in host part of IP address
  - table-based
- ARP
  - table of IP to physical address bindings
  - broadcast request if IP address not in table
  - target machine responds with its physical address
  - table entries are discarded if not refreshed

Address Translation Details

- Request Format
  - HardwareType: type of physical network (e.g., Ethernet)
  - ProtocolType: type of higher layer protocol (e.g., IP)
  - HLEN & PLEN: length of physical and protocol addresses
  - Operation: request or response
  - Source/Target-Physical/Protocol addresses

- Notes
  - table entries timeout in about 15 minutes
  - update table with source when you are the target
  - update table if already have an entry
  - do not refresh table entries upon reference

ARP Packet Format

<table>
<thead>
<tr>
<th></th>
<th>bytes 0</th>
<th>bytes 1</th>
<th>bytes 2</th>
<th>bytes 2-3</th>
<th>bytes 4-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Type</td>
<td>0x0806</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProtocolType</td>
<td>0x0800</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HLen</td>
<td>48</td>
<td>PLen</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td></td>
<td></td>
<td></td>
<td>Source Hardware Addr</td>
<td>Source Protocol Addr</td>
</tr>
<tr>
<td>Source Hardware Addr</td>
<td>bytes 0-3</td>
<td>bytes 4-5</td>
<td>bytes 2-3</td>
<td>bytes 4-5</td>
<td>bytes 2-3</td>
</tr>
<tr>
<td>Target Hardware Addr</td>
<td>bytes 0-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Target Protocol Addr</td>
<td>bytes 0-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sending an ARP message

- Sender constructs ARP message
- ARP message carried as data in hardware frame - encapsulation

Frame type = 0X0806

Processing ARP messages

- Receiver extracts sender's hardware address and updates local ARP table
- Receiver checks operation - request or response
- Response:
  - Adds sender's address to local cache
  - Sends pending IP packet(s)
- Request:
  - If receiver is target,
    - forms response, unicasts to sender
    - Adds sender's address to local cache
  - Else refresh the cache if sender is already there
- Note:
  - Target likely to respond "soon"
  - Computers have finite storage for ARP cache
  - Only target adds sender to cache; others only update if target already in cache
Internet Control Message Protocol (ICMP)

- Internet layer can detect a variety of errors:
  - Checksum (header only?)
  - TTL expires
  - No route to destination network
  - Can't deliver to destination host (e.g., no ARP reply)
- Internet layer discards datagrams with problems
- Some - e.g., checksum error - can't trigger error messages (hard to determine to whom to report the error)

Types of messages

- Internet Control Message Protocol (ICMP) defines error and informational messages
- Error messages:
  - Source quench (no buffer space)
  - Time exceeded (TTL, or reassembly timer expires)
  - Destination unreachable (network or host unreachable)
  - Redirect
  - Fragmentation required
- Informational messages:
  - Echo request/reply
  - Address mask request/reply
  - Router discovery

ICMP message transport

- ICMP encapsulated in IP
  - ICMP messages sent in response to incoming datagrams with problems
  - ICMP message not sent for ICMP message

ICMP and reachability

- An internet host, A, is reachable from another host, B, if datagrams can be delivered from A to B
- ping program tests reachability - sends datagram from B to A that A echoes back to B
- Uses ICMP echo request and echo reply messages
- Internet layer includes code to reply to incoming ICMP echo request messages

ICMP and internet routes

- List of all routers on path from A to B is called the route from A to B
- traceroute uses UDP to non-existent port and TTL field to find route via expanding ring search
- Sends ICMP echo messages with increasing TTL
  - Router that decrements TTL to 0 sends ICMP time exceeded message, with router's address as source address
  - First, with TTL 1, gets to first router, which discards and sends time exceeded message
  - Next, with TTL 1, gets through first router to second router
  - Continue until message from destination received
- traceroute must accommodate varying network delays
- Must also accommodate dynamically changing routes

ICMP and path MTU discovery

- Fragmentation should be avoided
- How can source configure outgoing datagrams to avoid fragmentation?
- Source determines path MTU - smallest network MTU on path from source to destination
- Source probes path using IP datagrams with don't fragment flag
- Router responds with ICMP fragmentation required message
- Source sends smaller probes until destination reached
ICMP and router discovery

- Router can fail, causing "black-hole" or isolating host from internet
- **ICMP router discovery** used to find new router
- Host can broadcast request for router announcements to auto-configure default route
- Host can broadcast request if router fails
- Router can broadcast advertisement of existence when first connected

ICMP redirect

- Default route may cause *extra hop*
- Router that forwards datagram on same interface sends **ICMP redirect**
- Host installs new route with correct router as next hop