Network Protocols

Address Resolution Protocol (ARP)
ARP overview

• Primarily used by IP to find a layer 2 address
• Problem statement: What L2 daddr do you use?
• If L3 daddr is on your subnet, L2 daddr = L3 host
• Else, L2 daddr is the router
• Use ARP on the local net to find the L2 daddr
Typical ARP process...

Step 1: Sender
- Put in own L2/L3 saddrs
- Fill in known L3 daddr
- Send to L2 broadcast daddr

Step 2: Receiver
- “Is that my L3 daddr?!”
- Fill in missing fields
- Reply directly to sender
**ARP frame format**

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE ADDRESS TYPE</td>
<td>PROTOCOL ADDRESS TYPE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HADDR LEN</td>
<td>PADDR LEN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENDER HADDR (first 4 octets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENDER HADDR (last 2 octets)</td>
<td>SENDER PADDR (first 2 octets)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SENDER PADDR (last 2 octets)</td>
<td>TARGET HADDR (first 2 octets)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TARGET HADDR (last 4 octets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TARGET PADDR (all 4 octets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Variations of ARP

• Inverse ARP - get a L2 daddr when L3 is known
• Reverse ARP – IP address auto-configuration
• DHCP ARP - Used to validate a DHCP lease
• Gratuitous ARP - update others of your mapping
• UnARP - notify others to flush your mapping
Some ARP security thoughts

- Hosts and routers build/maintain ARP table/cache
  - This might be a good thing to monitor (few do)
- Learn ARP mappings we didn't initiate?
  - Responders usually cache sender's mapping
  - Hosts seeing the broadcast and having the sender's mapping cached usually refresh
- Lack of security means MiTM attacks possible
- LAN switches with "port security"