Network Protocols

Address Resolution Protocol (ARP)
ARP overview

• Datalink to network layer address mapping
  • e.g. 0000.1234.abcd <--- 192.0.2.1

• Hosts and routers build ARP table/cache
  • ARP entries associated with a local interface
  • Timers used to age old table entries

• Potential security problems with ARP
  • No authentication, can lead to impersonation
### ARP frame format

<table>
<thead>
<tr>
<th></th>
<th>Hardware Address Type</th>
<th>Protocol Address Type</th>
<th>Hardlen</th>
<th>Paddr len</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-8</td>
<td>hardware address</td>
<td>protocol address</td>
<td>0-8</td>
<td>0-8</td>
<td></td>
</tr>
<tr>
<td>16-24</td>
<td>0</td>
<td>0</td>
<td>16-24</td>
<td>16-24</td>
<td>operation</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>0</td>
<td>31</td>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>

- Sender Haddr (first 4 octets)
- Sender Haddr (last 2 octets)
- Sender Paddr (first 2 octets)
- Sender Paddr (last 2 octets)
- Target Haddr (first 2 octets)
- Target Haddr (last 4 octets)
- Target Paddr (all 4 octets)
Typical ARP process...

**Sender**
- Send L2 broadcast
- Fill in known target IP

**Receiver**
- Fill in missing fields
- Learn sender's IP/MAC
- Reply directly to sender
Variations on typical ARP theme

- Inverse ARP - get your MAC when your IP is known
- Reverse ARP - request an IP address
- DHCP ARP - Used to validate a DHCP lease
- Gratuitous ARP - update others of your IP/MAC
- UnARP - notify others to flush your IP/MAC
ARP security

- Impersonation is probably the biggest risk
  - forge ARP replies
  - send bogus gratuitous ARPs
- Use LAN switch w/ port security and 1 host per port
- Use port-level authentication (e.g. 802.1x)
- Monitor for ARP table changes and for overflows
- Maintain router/host ARP table history