Computer Networks and Data Systems

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

*diagram courtesy of http://www.netbook.cs.purdue.edu
Variations of ARP

- Inverse ARP - get a L3 daddr when L2 is known
- Reverse ARP – IP address auto-configuration
  - get a L3 saddr, precursor to BOOTP/DHCP
- DHCP ARP - Used to validate a DHCP lease
  - ARP request own L3 daddr, L3 saddr = 0.0.0.0
- Gratuitous ARP - update others of your mapping
  - ARP request where L3 saddr = L3 daddr
- UnARP - notify others to flush your mapping
- Proxy ARP – router that ARPs for non-local host
Some ARP security thoughts

• Hosts and routers build/maintain ARP table/cache
  • This might be a good thing to monitor (some 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”