Network Protocols

Address Resolution Protocol (ARP)
ARP overview

• Primarily used by IP to find a layer 2 address
• What L2 destination address to use on the LAN?
  • ARP on the LAN/broadcast medium to find out
• You will either send it directly or to a router
  • If direct, L2 and L3 daddrs are the destination's
  • If nondirect, L2 is a router, L3 is final destination
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
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
- Gratutious 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”