

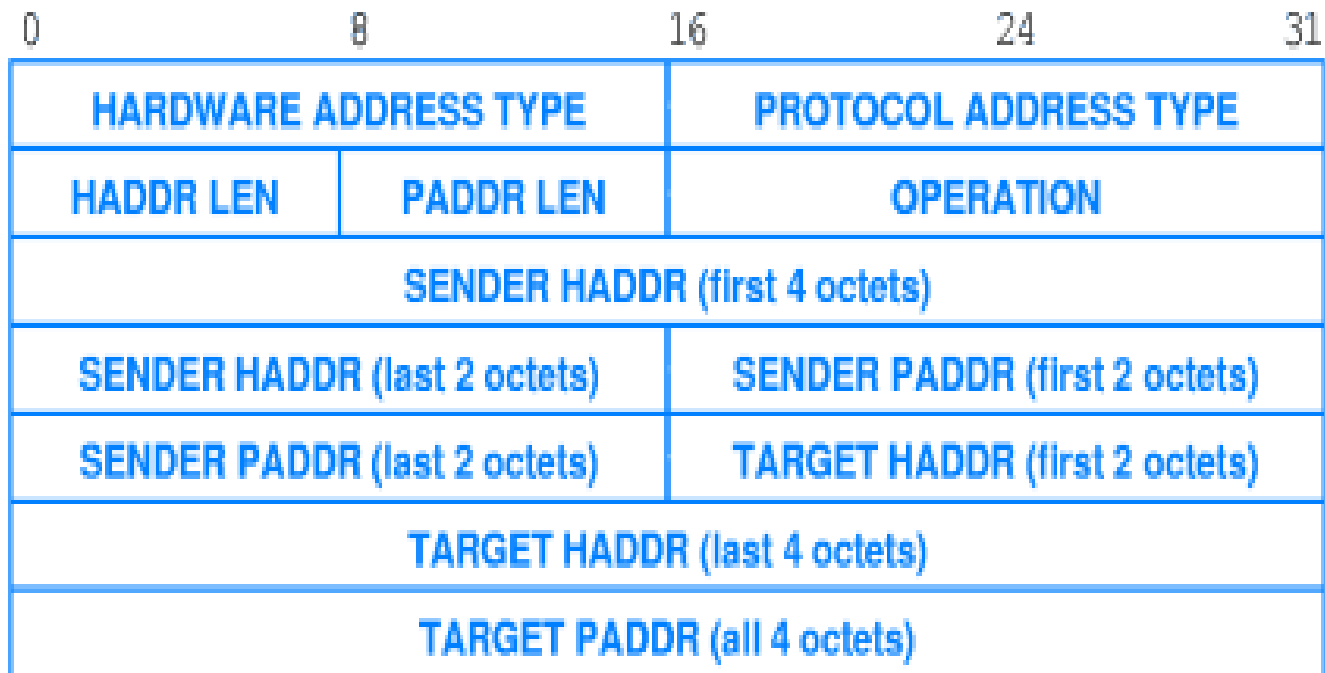
# Network Protocols

## 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



# 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