- ARP: Address Resolution Protocol
- **4.1 Introduction**
- Address Resolution Protocol (ARP) - provides a dynamic mapping between IPv4 addresses and the hardware addresses used by various network technologies
- IPv6 uses Neighbor Discovery Protocol
- IP addresses are typically derived from a pool of addresses maintained near the network attachment point and are installed when systems are turned on or configured
- Address resolution - is the process of discovering the mapping from one address to another
- TCP/IP protocol suite using IPv4 - address resolution accomplished by running ARP
- ARP - provides a dynamic mapping from a network-layer address to a corresponding hardware address
- **4.2 An Example**
- Internet services must determine how to contact the server in which we are interested
- Local or remote service
- remote
  - router is required to reach the destination
  - ARP operates only when reach those systems on the same IP subnet
- **4.2.1 Direct Delivery and ARP**
- Direct delivery takes place when an IP datagram is sent to an IP address with the same IP prefix as the sender's
- Basic operation of direct delivery with IPv4
  - 1. application calls a special function to parse the URL to see if it contains a host name. Here it does not, so the application uses the 32-bit IPv4 address 10.0.0.1
  - 2. the application asks the TCP protocol to establish a connection with 10.0.0.1
  - 3. TCP attempts to send a connection request segment to the remote host by sending an IPv4 datagram to 10.0.0.1
  - 4. because we are assuming that the address 10.0.0.1 is using the same network prefix as our sending host, the datagram can be sent directly to that address without going through a router
  - 5. A translation is required from a logical Internet address to its corresponding physical hardware address. This is the function of ARP.
    - ARP works in its normal form only for broadcast networks, where the link layer is able to deliver a single message to all attached network devices
    - This is an important requirement imposed by the operation of ARP
    - On non-broadcast networks, other, more complex mapping protocols may be required.
  - 6. Link layer broadcast - ARP sends an Ethernet frame called an ARP request to every host on the shared link-layer segment.
    - ARP request contains the IPv4 address of the destination host (10.0.0.1) and seeks an answer to the following question: "If you are configured with IPv4 address 10.0.0.1 as one of your own, please respond to me with your MAC address"
  - 7. ARP, all systems in the same broadcast domain receive ARP requests. This includes systems that may not be running the IPv4 or IPv6 protocols at all but does not include systems on different VLANs
    - Provided there exists an attached system using the IPv4 address specified in the request, it alone responds with an ARP reply.
      - The reply contains the IPv4 address and the corresponding MAC address
      - The reply does not ordinarily use broadcast but is directed only to the sender
      - The host receiving the ARP request also learns of the sender's IPv4-to-MAC address mapping at this time and records it in memory for later use

- 8. The ARP reply is then received by the original sender of the request, and the datagram that forced the ARP request/reply to be exchanged can now be sent
- 9. The sender now sends the datagram directly to the destination host by encapsulating it in an Ethernet frame and using the Ethernet address learned by the ARP exchange as the destination Ethernet address. Because the Ethernet address refers only to the correct destination host, no other hosts or routers receive the datagram. Thus, when only direct delivery is used, no router is required

- ARP is used in multi-access link-layer networks running IPv4, where each host has its own primary hardware address
- **4.3 ARP Cache**
- ARP cache on each host and router
  - cache maintains the recent mappings from network-layer addresses to hardware addresses for each interface that uses address resolution
  - timed removal

```
Linux% arp
Address                  HWtype  HWaddress           Flags Mask Iface
gw.home                  ether   00:0D:66:4F:60:00   C          eth1
printer.home             ether   00:0A:95:87:38:6A   C          eth1

Linux% arp -a
printer.home (10.0.0.4) at     00:0A:95:87:38:6A [ether] on eth1
gw.home (10.0.0.1) at 00:0D:66:4F:60:00 [ether] on eth1
```

- Flags
  - C-type entries have been learned dynamically by the ARP protocol
  - M-type entires are entered by hand
  - P-type means publish
    - That is for any P entry, the host responds to incoming ARP requests with an ARP response
    - This option is for configuring proxy ARP
- **4.4 ARP Frame Format**

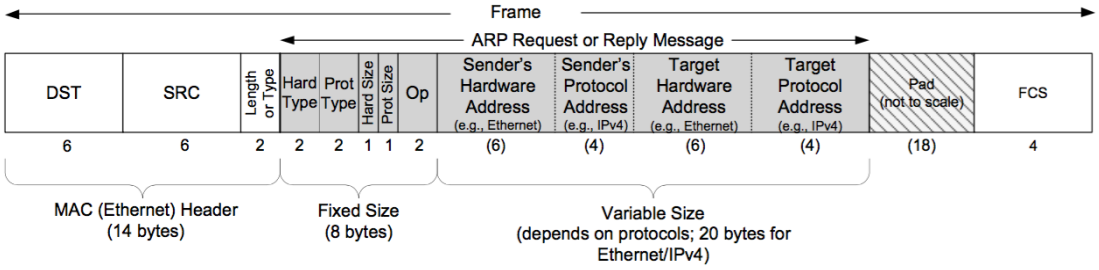

Figure 4-2 ARP frame format as used when mapping IPv4 addresses to 48-bit MAC (Ethernet) addresses

- ARP is general enough to be used with addresses other than IPv4 addresses
- Ethernet Header
  - destination - ARP requests, the special Ethernet destination address of ff:ff:ff:ff:ff:ff means the broadcast address—all Ethernet interfaces in the same broadcast domain receive these frames
  - Length or type - required to be 0x0806 for ARP

- Next 8 bytes
  - Hardware address - MAC, physical, or link-layer address
  - Hard Type - 1 for Ethernet
  - Prot Type - 0x0800 for IPv4
  - Hard and Prot size - ARP request or reply for an IPv4 address on an Ethernet they are 6 and 4, respectively
  - Op - specifies the operation
- Remaining bytes before pad
  - Sender's Hardware Address
  - Sender's Protocol Address
  - Target Hardware Address
  - Target Protocol Address
- For an ARP request, all the fields are filled in except the Target Hardware Address (which is set to 0)
- When a system receives an ARP request directed to it, it fills in its hardware address, swaps the two sender addresses with the two target addresses , sets the Op field to 2, and sends the reply
- **4.5 ARP Examples**
- Telnet - simple application that can establish a TCP/IP connection between two systems
- tcpdump - command to see what really happens with ARP when we execute normal TCP/IP utilities such as Telnet
- **4.5.1 Normal Example**

```
Linux#  tcpdump -e
1       0.0 0:0:c0:6f:2d:40 ff:ff:ff:ff:ff:ff arp 60:
        arp who-has 10.0.0.3 tell 10.0.0.56
2       0.002174 (0.0022)0:0:c0:c2:9b:26 0:0:c0:6f:2d:40 arp 60:
        arp reply 10.0.0.3 is-at 0:0:c0:c2:9b:26

3       0.002831 (0.0007)0:0:c0:6f:2d:40 0:0:c0:c2:9b:26 ip 60:
        10.0.0.56.1030 > 10.0.0.3.www: S 596459521:596459521(0)
        win 4096 <mss 1024> [tos 0x10]
4       0.007834 (0.0050)0:0:c0:c2:9b:26 0:0:c0:6f:2d:40 ip 60:
        10.0.0.3.www > 10.0.0.56.1030: S 3562228225:3562228225(0)
        ack 596459522 win 4096 <mss 1024>
5       0.009615 (0.0018)0:0:c0:6f:2d:40 0:0:c0:c2:9b:26 ip 60:
        10.0.0.56.1030 > 10.0.0.3.discard: . ack 1 win 4096 [tos 0x10]
```

- arp means that the Frame Type field is 0x0806
- the value 60 printed after the words arp and ip in each of the five packets is the length of the Ethernet frame
  - The size of an ARP request or ARP reply is the length of the Ethernet frame. The size of an ARP request or ARP reply is always 42 bytes. Each frame has been padded to the Ethernet minimum: 60 bytes of data plus 4-byte CRC
- arpwho-has, identifies the frame as an ARP request with the IPv4 address of 10.0.0.3 as the target address and IPv4 address of 10.0.0.56 as the sender's address
- the number printed after the packet number is the relative time (in seconds) when the packet was received by tcpdump
  - each packet except the first also contains the time difference in parentheses following the relative time
- **4.5.2 ARP Request to a Nonexistent Host**
- **4.6 ARP Cache Timeout**

- A timeout is normally associated with each entry in the ARP cache
- 20 minutes for completed entry
- 3 minutes for incomplete entry
- restart the timeout each time the entry is used
- soft state - information that is discarded if not refreshed before some timeout is reached
  - many internet protocols use soft state because it helps to initiate automatic reconfiguration if network conditions change
  - the cost of soft state is that some protocol must refresh the state to avoid expiration. “Soft state refreshes” are often incorporated in a protocol design to keep the soft state active
- **4.7 Proxy ARP**
- Proxy ARP lets a system answer ARP requests for a different host
  - not commonly used and is generally to be avoided if possible
- historical use
  - hide two physical networks from each other
- Linux supports auto-proxy ARP - supports the ability of using proxy ARP without having to manually enter ARP entries for every possible IPv4 address that is being proxied.
- **4.8 Gratuitous ARP and Address Conflict Detection (ACD)**
- gratuitous ARP - occurs when a host sends an ARP request looking for its own address
  - achieves two goals
    - 1. It lets a host determine if another host is already configured with the same IPv4 address.
    - 2. If the host sending the gratuitous ARP has just changed its hardware address, this frame causes any other host receiving the broadcast that has an entry in its cache for the old hardware address to update its ARP cache entry accordingly.
- IPv4 Address Conflict Detection (ACD)
  - defines ARP probe and ARP announcement packets
  - ARP probe - is an ARP request packet in which the Sender’s Protocol (IPv4) Address field is set to 0
    - probes are used to see if a candidate IPv4 address is being used by any other systems in the broadcast domain.
    - Setting the Sender’s protocol address to 0 avoids cache pollution should the candidate IPv4 address already be in se by another host, a difference from the way gratuitous ARP works.
  - ARP announcement
    - identical to an ARP probe, except both the Sender’s Protocol Address and the Target Protocol Address fields are filled in with the candidate IPv4 address. It is used to announce the sender’s intention to use the candidate IPv4 address as its own.
  - Performing ARP
    - host sends an ARP probe when an interface is brought up or out of sleep, or when a new link is established
    - waits a random amount of time before sending up to three probes
      - each probe is spaced 1 or 2 seconds apart
    - While sending its probes, a requesting station may receive ARP request or replies
      - reply to a probe indicates that a station is already using the candidate IP address
      - a request containing the same candidate IPv4 address in the Target Protocol Address field sent from a different system indicates that the other system is simultaneously attempting to acquire the candidate IPv4 address.

    - If the requesting host does not discover a conflict according to the procedure just described, it sends two ARP announcements spaced 2s apart to indicate to systems in the broadcast domain the IPv4 address it is now using.
      - in announcements, both the Sender's Protocol Address and the Target Protocol Address fields are set to the address being claimed
      - purpose of sending these announcements is to ensure that any preexisting cached address mappings are updated to reflect the sender's current use of the address
  - ACD is considered to be an ongoing process, and in this way it differs from gratuitous ARP
    - continues to inspect ARP traffic to see if its address appears in the sender's protocol address field.
      - three possible solutions
        - cease using the address
        - keep the address bit send "defensive" ARP announcement and cease using it if the conflict continues
        - continue to use the address despite the conflict
- **4.9 The arp Command**
- -a flag on Windows and Linux to display all the entries in the ARP cache
- -d option to delete an entry from the ARP cache
- -s option entries can be added
  - requires an IPv4 address and an Ethernet address
  - The IPv4 and Ethernet address are added to the cache as an entry
  - This entry is made semipermanent (i.e. it does not time out from the cache, but it disappears when the system is rebooted.)
- Linux
  - when the temp keyword is supplied at the end of the command line when adding an entry using -s, the entry is considered to be temporary and times out in the same way that other ARP entries do.
  - keyword pub at the end of a command line, also used with the -s option, causes the system to act as an ARP responder for that entry.
    - The system answers ARP requests for the IPv4 address, replying with the specified Ethernet address.
- **4.10 Using ARP to Set and Embedded Device's IPv4 Address**
- Common to find network attach devices that have no direct way to enter their network configuration information
  - Devices configured in two ways
    - DHCP can be used to automatically assign an address and other information.
    - Use ARP to set an IPv4 address
- ARP device configuration
  - manually establish an ARP mapping for the device (using the arp -s command), then send an IP packet to the address.
  - Because the ARP entry is already present, no ARP request/reply is generated.
  - The hardware address can be used immediately
  - Ethernet (MAC) address of the device must be known
  - When the device receives a packet destined for its hardware address, whatever destination address is contained in the datagram is used to assign its initial IPv4 address.
- **4.11 Attacks Involving ARP**
- use proxy ARP facility to masquerade as some host, respond to ARP requests for it

    - if the victim host is not present, this straightforward and may not be detected. It is considerably more difficult if the host is still running, as more than one response may be generated per an arp request, which is easily detected
- A machine is attached to more than one network, and ARP entries from one interface leak over to the ARP table of the other
    - can be exploited to improperly direct traffic onto the wrong the network segment.
- Static entries
    - static entries may be used to avoid the ARP request/reply when seeking the Ethernet (MAC) address corresponding to particular IP address.
        - the idea is that static entries placed in the ARP cache for important hosts would soon detect any hosts masquerading with that IP address.
        - most implementations have replaced static cache entries with entries provided by ARP replies.
        - The consequence of this is that a machine receiving an ARP reply would be coaxed into replacing its static entries with those provided by an attacker
- **4.12 Summary**
- ARP is a basic protocol in almost every TCP/IP implementation
- ARP is used to determine the hardware addresses corresponding to the IPv4 addresses in use on the locally reachable IPv4 subnet.
- It is invoked when forwarding datagrams destined for the same subnet as the sending host's and is also used to reach a router when the destination of a datagram is not on the subnet
- ARP cache
    - fundamental to its operation
    - each entry in the cache has a timer that is used to remove both incomplete and completed entries
- proxy ARP
    - when a router answers ARP requests for host accessible on another of the router's interfaces
- gratuitous ARP
    - sending an ARP request for your own IP address, normally when bootstrapping
- address conflict detection for IPv4
    - which uses a continually operating gratuitous ARP-like exchange to avoid address duplication within the same broadcast domain