# ARP, RARP, IP FRAGMENTATION AND REASSEMBLY

## ARP (Address Resolution Protocol)

- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP) specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.
- The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet.
- It is also used for IP over other LAN technologies, such as Token Ring, FDDI, or IEEE 802.11, and for IP over ATM.
- ARP is a Link Layer protocol because it only operates on the local area network or point-to-point link that a host is connected to.
- The hardware address is also known as the Medium Access Control (MAC) address, in reference to the standards which define Ethernet.
- The Ethernet address is a link layer address and is dependent on the interface card which is used.
- IP operates at the network layer and is not concerned with the link addresses of individual nodes which are to be used. The ARP is therefore used to translate IP addresses into MAC address.

- In the below figure suppose host H1 wants to send an IP packet to H3, but does not know the MAC address of H3. H1 first broadcast an ARP request packet asking the destination host, which is identified by H3's IP address, to reply. All hosts in the network receive the packet, but only the intended host, which is H3, responds to H1.
- The ARP response packet contains H3's MAC address and IP addresses.
- H1 caches H3's MAC address in its ARP table so that H1 can simply look up H3's MAC address in the table for future use.

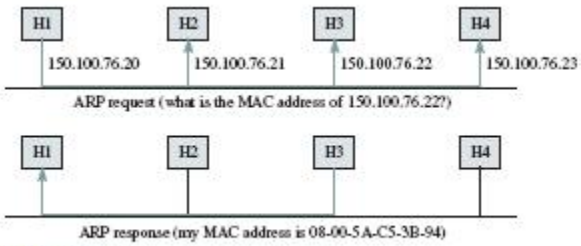

FIGURE 8.8 Address Resolution Protocol

- The ARP client and server processes operate on all computers using IP over Ethernet. The processes are normally implemented as part of the software driver that drives the network interface card.

## RARP (Reverse Address Resolution Protocol)

- RARP is a link layer networking protocol, used to resolve an IP address from a given hardware address (such as an Ethernet address).
- RARP requires one or more server hosts to maintain a database of mappings from Link Layer address to protocol address.
- To obtain its IP address, the host broadcasts an RARP request packet containing its MAC address on the network.
- All hosts in the network receive the packet, but only the server replies to the host by sending an RARP response containing the host's MAC and IP address.

## IP fragmentation and Reassembly

- The Internet Protocol allows IP fragmentation so that datagrams can be fragmented into pieces small enough to pass over a link with a smaller MTU than the original datagram size.
- The Identification field, and Fragment offset field along with Don't Fragment and More Fragment Flags are used for Fragmentation and Reassembly of IP datagrams.
- In a case where a router in the network receives a PDU larger than the next hop's MTU, it has two options. Drop the PDU and send an ICMP message which says "Packet too Big", or to Fragment the IP packet and send over the link with a smaller MTU.
- If a receiving host receives an IP packet which is fragmented, it has to reassemble the IP packet and hand it over to the higher layer.
- Reassembly is intended to happen in the receiving host but in practice it may be done by an intermediate router, for example network address translation requires re-calculating checksums across entire packets, and so routers supporting this will often recombine packets as part of the process.

- The details of the fragmentation mechanism, as well as the overall architectural approach to fragmentation, are different in IPv4 and IPv6.
- In IPv4, routers do the fragmentation, whereas in IPv6, routers do not fragment, but drop the packets that are larger than the MTU size. Though the header formats are different for IPv4 and IPv6, similar fields are used for fragmentation, so the algorithm can be reused for fragmentation and reassembly.
- IP fragmentation can cause excessive retransmissions when fragments encounter packet loss and reliable protocols such as TCP must retransmit all of the fragments in order to recover from the loss of a single fragment.
- Thus senders typically use two approaches to decide the size of IP datagrams to send over the network.
- The first is for the sending host to send an IP datagram of size equal to the MTU of the first hop of the source destination pair.
- The second is to run the "Path MTU discovery" algorithm, to determine the path MTU between two IP hosts, so that IP fragmentation can be avoided.

- The flag field has three bits, one unused bit, one “don’t fragment”(DF) bit, and one “more fragment”(MF) bit.
- If DF bit is set to 1, it forces the router not to fragment the packet. If the packet length is greater than MTU, the router will discard the packet and send an error message to the source host.
- The MF bit tells the destination host whether or not more fragments follow. If there are more, the MF bit is set to 1; otherwise, it is set to 0.
- Fragment offset field identifies the location of a fragment in a packet.

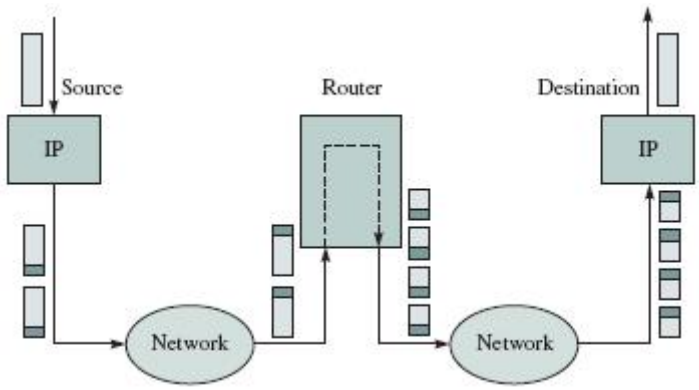


Figure: Packet fragmentation

**Example—Fragmenting a Packet**

Suppose a packet arrives at a router and is to be forwarded to an X.25 network having an MTU of 576 bytes. The packet has an IP header of 20 bytes and a data part of 1484 bytes. Perform fragmentation and include the pertinent values of the IP header of the original packet and of each fragment.

The maximum possible data length per fragment $= 576 - 20 = 556$ bytes. However, 556 is not a multiple of 8. Thus we need to set the maximum data length to 552 bytes. We can break 1484 into $552 + 552 + 380$ (other combinations are also possible).

Table 8.1 shows the pertinent values for the IP header where x denotes a unique identification value. Other values, except the header checksum, are the same as in the original packet.

| | Total length | ID | MF | Fragment offset |
|---|---|---|---|---|
| *Original packet* | 1504 | x | 0 | 0 |
| *Fragment 1* | 572 | x | 1 | 0 |
| *Fragment 2* | 572 | x | 1 | 69 |
| *Fragment 3* | 400 | x | 0 | 138 |

TABLE 8.1 Values of the IP header in a fragmented packet

Deficiencies of IP

- Lack of error control, flow control and congestion control
- Lack of assistance mechanisms

What happens if something goes wrong?

- If a router must discard a datagram because it can not find a router to the final destination
- The time-to-leave field has a zero value
- If the final destination host must discard all fragments of a datagram because it has not received all fragments within a pre-determined time limit

IP has no built in mechanisms to notify the original hosts, in erroneous situations
IP also lacks a mechanism for host and management queries
• A host wants to know whether a router or another host is active
• Sometimes network manager needs information from another host or router

Source : http://elearningatria.files.wordpress.com/2013/10/unit2.pdf