Consolidated Notes

Friday, October 28, 2022   6:05 PM

ARP request
- src ip
- src mac
- target Ip
- target mac

ARP reply
- src ip
- src mac
- target Ip
- target mac

ARP - Needs an ethernet header

ARP | eth | arp |

ICMP — | Cth 0x800 | ip type=1 | ICMP |
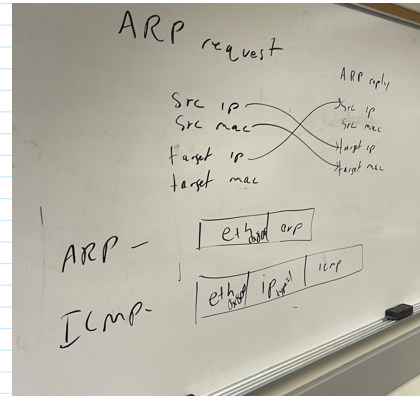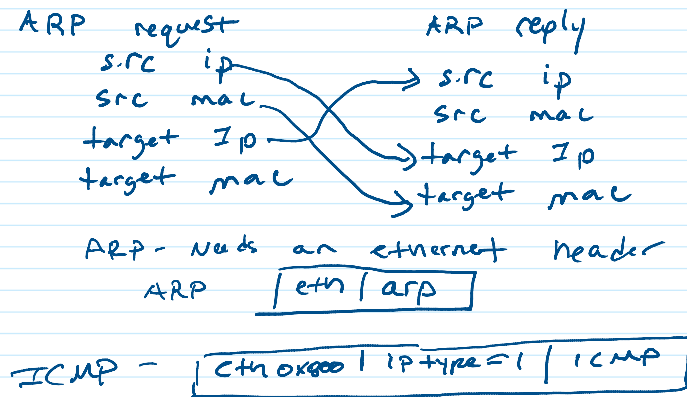
Internet Control Message Protocol (ICMP)

ICMP will have the following layout:
0

Eth type = 0x800	IP protocol = 1	ICMP type #

ICMP type #:
0 = echo reply (used to ping)
8 = echo request (used to ping)

The ARP header (bytes 12-??) must follow the Ethernet (bytes 0 - 11)
We must parse all the data to see what we have. We will take bytes 0-11
and copy them into a Eth header struct.

Then take bytes 12 to 42(for example) and copy that into an ARP struct.

ARP request have to broadcast everywhere

Eth	ARP
Source [source mac]	Operation (request or reply) set based on our needs
Destination [ff:ff:ff:ff:ff:ff] (Broadcast mac address)	Fixed values for every ARP request/reply
Type = 0x806 (ARP Packet)	Hardware type = 1(Ethernet)
	Hardware length = 6 bytes
	Protocol Type = 0x800
	Protocol Length = 4 bytes (for an IP address)
	Source Protocol Address [source IP]
	Source Hardware Address [source mac]
	Target Protocol Address [target IP]
	Target Hardware Address [00:00:00:00:00:00]

    0 - 11 bytes   12 - ?? bytes

ARP Reply has to be unicast to who made the request

Eth	ARP
Source [target mac]	Operation (request or reply) set based on our needs
Destination [Source mac] (unicast)	Fixed values for every ARP request/reply
Type = 0x806 (ARP Packet)	Hardware type = 1(Ethernet)
	Hardware length = 6 bytes
	Protocol Type = 0x800
	Protocol Length = 4 bytes (for an IP address)
	Source Protocol Address [target IP]
	Source Hardware Address [target mac]
	Target Protocol Address [source IP]
	Target Hardware Address [source mac]

If the requested address does not exit we
the requester will not receive an ARP response.
The owner of the address is the only one that can
respond.

    0 - 11 bytes   12 - ?? bytes

Ignore all other packet types. No other packets should occur

Reply

In this event we must send an ICMP "Host unreachable error message"

Eth	IP	ICMP Type
Type = 0x800 (IP Packet)	IP Protocol =1	Type = 0
	Protocol one means that ICMP is next	

A response to a ping is an
ICMP echo response packet

Or if the packet had too many hops send an ICMP "Time exceeded
If someone pings your router you must respond

Eth	IP	ICMP Type
Type = 0x800 (IP Packet)	IP Protocol =1	Type = 8
	Protocol one means that ICMP is next	

A ping is an ICMP echo request packet

For ethernet headers use ethernet.h

/* 10Mb/s ethernet header */
struct ether_header
{
 u_int8_t ether_dhost[ETH_ALEN];   /* destination eth addr   */
 u_int8_t ether_shost[ETH_ALEN];   /* source ether addr   */
 u_int16_t ether_type;   /* packet type ID field   */
}

From <https://sites.uclouvain.be/SystInfo/usr/include/net/ethernet.h.html>

How can we be IP headers and ICMP headers?