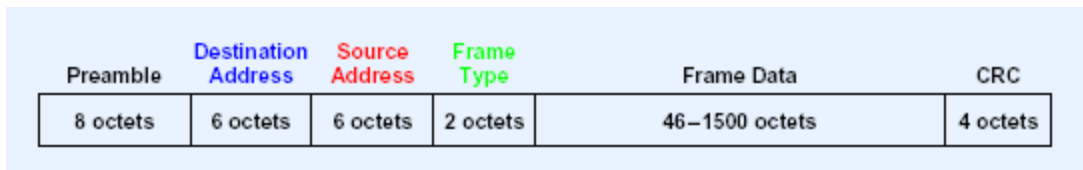


ARP Protocols

(1) Ethernet Address

- ❖ Ethernet Hardware Addresses
 - 48-bit unique number.
 - An address can be unicast, broadcast (all 1s), or multicast address.
- ❖ Ethernet Frame Format
 - Link-level connection among machines
 - Octet:
 - Why not byte (byte refers to a hardware-dependent character size)
 - Octet refers to an 8-bit quantity on all computers.
 - Preamble and CRC: added to the Ethernet frame when the frame is put on the wire. It will be removed by the hardware before the frame is stored into computer's memory. You won't be able to see them using sniffers.
 - Frame Type: For example, 0806 for ARP (on an Ethernet)
 - Maximum size: 1500 octets.



- ❖ An example
 - Destination is **02 07 01 00 27 ba**
 - Source is **08 00 2b 0d 44 a7**
 - Frame type is **08 00 (IP)**

02 07 01 00 27 ba	08 00 2b 0d 44 a7	08 00	45 00
00 54 82 68 00 00	ff 01 35 21 80 0a	02 03 80 0a	
02 08 08 00 73 0b	d4 6d 00 00 04 3b	8c 28 28 20	
0d 00 08 09 0a 0b	0c 0d 0e 0f 10 11	12 13 14 15	
16 17 18 19 1a 1b	1c 1d 1e 1f 20 21	22 23 24 25	
26 27 28 29 2a 2b	2c 2d 2e 2f 30 31	32 33 34 35	
36 37			

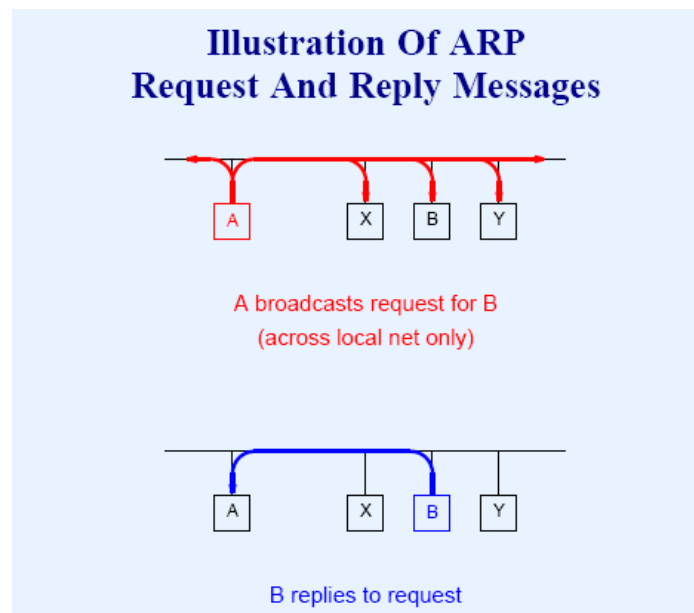
(2) ARP Protocols

❖ Motivation

- What address can Ethernet interface card recognize?
 - Ethernet address (48-bit address, usually hardcoded in the hardware)
- Computer addresses other computers using IP address, which is created to make Internet routing convenient.
- Once the packet reached a LAN, physical address (such as Ethernet address) must be used. How to find out the Ethernet address? Senders usually have no idea about the physical address of the receivers. They don't need to know that.

❖ ARP Protocol

- Machine A wants to send a packet to B, but A only knows B's IP address
- Machine A broadcasts ARP request with B's IP address
- All machines on the local network receive the broadcast
- Machine B replies with its physical address
- Machine A adds B's address information to its table
- Machine A delivers packet directly to B



❖ ARP Encapsulation

- In Ethernet, the Frame Type for ARP is 0806

Ethernet Format

Preamble	Destination Address	Source Address	Frame Type	Frame Data	CRC
8 octets	6 octets	6 octets	2 octets	46–1500 octets	4 octets

ARP Encapsulation



❖ ARP Packet Format

- The format is general enough to allow it to be used with arbitrary physical addresses and arbitrary protocol addresses.
- Hardware Type (2): 1 for Ethernet
- Protocol Type (2): the type of high-level protocol address, e.g. 0800 for IP protocol.
- HLEN (1): length of the hardware address
- PLEN (1): length of the high-level protocol address (e.g. IP)
- Operation (2): ARP request=1, ARP reply=2, RARP request=3, RARP response=4
- SENDER HA(6)
- SENDER IP(4)
- TARGET HA(6)
- TARGET IP(4)

ARP Packet Format When Used With Ethernet

0	8	16	31
ETHERNET ADDRESS TYPE (1)		IP ADDRESS TYPE (0800)	
ETH ADDR LEN (6)	IP ADDR LEN (4)	OPERATION	
SENDER'S ETH ADDR (first 4 octets)			
SENDER'S ETH ADDR (last 2 octets)		SENDER'S IP ADDR (first 2 octets)	
SENDER'S IP ADDR (last 2 octets)		TARGET'S ETH ADDR (first 2 octets)	
TARGET'S ETH ADDR (last 4 octets)			
TARGET'S IP ADDR (all 4 octets)			

❖ ARP Caching

- To reduce communication cost, computers that use ARP maintain a cache of recently acquired IP-to-physical address bindings.
- Each entry has a timer (usual timeout period is 20 minutes)
- The sender's IP-to-address binding is included in every ARP broadcast; receivers update the IP-to-physical address binding information in their cache before processing an ARP packet.

- ARP is stateless, and most of operating systems update their cache when receiving an ARP reply, regardless of whether they have actually sent out a request or not.
 - Gratuitous message (src IP = dest IP, operation code = 2:reply)
 - The same IP address is used for both source IP and dest IP. This is used during the initialization of IP stack to find out whether the IP address is used by other host. Whoever has the same IP replies (this message is a broadcast). Otherwise, every host updates its cache.
-

(3) ARP Cache Poisoning

- ❖ Question: Given how ARP cache works, how do you attack?
 - First, how do you modify a target machine's ARP cache?
 - Second, if you can achieve ARP cache poisoning, how can you use this technique to compromise the security of your victim?
- ❖ ARP Cache Poisoning
 - By sending forged ARP replies, a target system could be convinced to send frames destined for a computer to another computer.
 - There are various ways to conduct cache poisoning: ARP "who is" broadcast, ARP reply, gratuitous ARP message, etc.
 - According to the tests on Windows 9x, NT, 2000, XP, Solaris 8, Linux kernel 2.2 and 2.4, Cisco IOS 12, Nokia IPSO 3.5 operating systems, there were always at least one kind of ARP message to poison the cache.
 - Moreover, on Windows systems (9x/NT/2K), static ARP entry can always be overwritten using a fake ARP message.
- ❖ Man-in-the-middle attack
 - Some servers use IP addresses for authentication. This is the case for many application like Apache ACL, r-commands, NFS, TCP Wrapper, restricted administration tools, etc ...
 - Goal: the server trusts T's IP address; evil host E wants to connect to the server.
 - How: let the server believe the evil host (E) has the legitimate IP.
 - Setting: evil host E, trusted host T, and server S.
 - E: ARP cache poisoning
 - E: Forward existing server-to-T traffic
 - E: use T's IP to communicate with S.
 - Problem: T might broadcast new ARPs, which can correct S's ARP cache. S then sends TCP replies to T, who will send back TCP reset to S (because such TCP connection does not exist between S and T). This will end the evil host's connection with S.
 - How to prevent this from happening? ---> Discussion
 - Shutdown T (denial of service)
 - Flood S with forged ARP message
 - Prevent T from sending ARP broadcast: how? give T everything before it needs them.
- ❖ Other attacks: any IP-based authentication
 - Bypassing Firewalls: many firewalls only allow outgoing traffic from a few identified computers. The evil host (E) can bypass this rule using cache poisoning.

- ❖ How to protect against ARP cache poisoning attacks?
 - Use intrusion detection tools: detect fake ARP messages and maintain consistency of the ARP table. Available on many UNIX platforms, `arpwatch` maintains a database of Ethernet MAC addresses seen on the network, with their associated IP pairs. Alerts the system administrator via e-mail if any change happens.
 - Use strong authentication rather than source IP address. VPN protocols like SSH, SSL or IPSec can greatly improve security by achieving authentication, integrity and confidentiality.