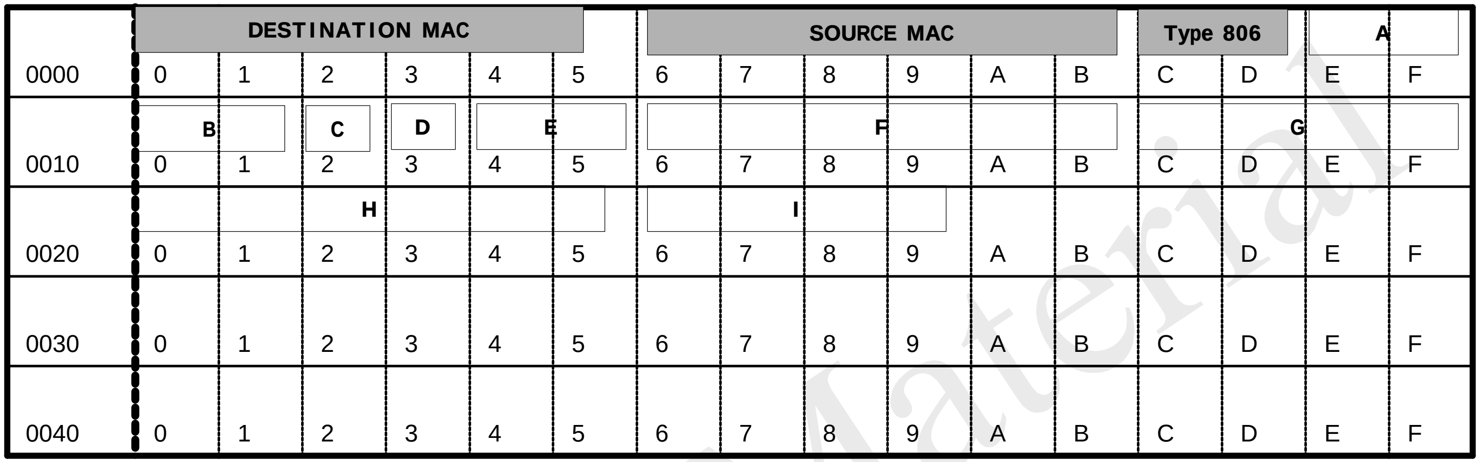
Dissecting ARP

Packet Layout (Ethernet II/Ethertype Format)



	DESTINATION MAC						SOURCE MAC						Type 806		A	
0000	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	B		C	D	E		F						G			
0010	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	H						I									
0020	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0030	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0040	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

A - Hardware Type:**2 Bytes**. Indicates the 'Hardware Type ' used at the Data Link Layer. (1-Ethernet)

B - Protocol Type: **2 Bytes**. This value is typically set to 0x0800 for IP.

C - Hardware Address Length: **1 Byte**. The length of the sender hardware address.

D - Protocol Address Length: **1 Byte**. The length of the sender's protocol address. (4 Bytes for IP)

E - Operation (OPCODE): **2 Bytes**. Identifies the type of ARP frame. (1-ARP Request, 2-ARP Reply)

F - Sender Hardware Address (SHA): **6 Bytes**. Contains the MAC address of the sender.

G - Sender Protocol Address (SPA): **4 Bytes**. Contains the IP address of the sender.

H - Target Hardware Address (SHA): **6 Bytes**. Contains the MAC address of the target.

I - Target Protocol Address (SPA): **4 Bytes**. Contains the IP address of the target.

Microsoft ARP Command

Type arp at the command prompt to see the available options.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

```
C:\WINDOWS\Desktop>arp -a

Interface: 216.254.163.29 on Interface 0x1000002

  Internet Address      Physical Address      Type

  66.54.2.140           20-53-52-43-00-00     dynamic

  216.254.141.3          20-53-52-43-00-00     dynamic
```

Linux ARP Command

```
arp [ -vn ] [ -H type ] [ -i if ] -a [ hostname ]
arp [ -v ] [ -i if ] -d hostname [ pub ]
arp [ -v ] [ -H type ] [ -i if ] -s hostname hw_addr [ temp ]
arp [ -v ] [ -H type ] [ -i if ] -s hostname hw_addr [ netmask nm ] pub
arp [ -v ] [ -H type ] [ -i if ] -Ds hostname ifa [ netmask nm ] pub
arp [ -vnD ] [ -H type ] [ -i if ] -f filename
```

```
Linux heckler 2.4.7-10 #1 Thu Sep 6 17:27:27 EDT 2001 i686 unknown
[danny@heckler danny]$ arp -a
gateway (192.168.1.1) at 00:20:78:CE:A1:B8 [ether] on eth0
```

OPTIONS

-v, --verbose Tell the user what is going on by being verbose.

-n, --umeric shows numerical addresses instead of trying to determine symbolic host, port or user names.

-H type, --hw-type type When setting or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet) , PROnet (pronet) , AX.25 (ax25) and NET/ROM (netrom).

-a [hostname], --display [hostname] Shows the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed.

-d hostname, --delete hostname Remove any entry for the specified host. This can be used if the indicated host is brought down, for example.

-D, --use-device Use the interface ifa 's hardware address.

-i If, --device If Select an interface. When dumping the ARP cache only entries matching the specified interface will be printed. When setting a permanent or temp ARP entry this interface will be associated with the entry; if this option is not used, the kernel will guess based on the routing table. For pub entries the specified interface is the interface on which ARP requests will be answered. NOTE: This has to be different from the interface to which the IP datagrams will be routed.

-s hostname hw_addr, --set hostname Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr format of the hardware address is dependent on the hardware class, but for most classes one can assume that the usual presentation can be used. For the Ethernet class, this is 6 bytes in hexadecimal, separated by colons. When adding proxy arp entries (that is those with the pub lish flag set a netmask may be specified to proxy arp for entire subnets. This is not good practice, but is supported by older kernels because it can be useful. If the temp flag is not supplied entries will be permanent stored into the ARP cache. NOTE: As of kernel 2.2.0 it is no longer possible to set an ARP entry for an entire subnet.

-f filename, --file filename Similar to the -s option, only this time the address info is taken from file filename can be used if ARP entries for a lot of hosts have to be set up. The name of the data file is very often /etc/ethers , but this is not official. The format of the file is simple; it only contains ASCII text lines with a hostname, and a hardware address separated by whitespace. Additionally the pub temp and netmask flags can be used.

In all places where a hostname is expected, one can also enter an IP address in dotted-decimal notation.

Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag.

- **60 second timeout**

Measuring The ARP Cache Aging Process

You can calculate how long it takes a device to ‘age out’ an IP/MAC address from its table.

To do this, simply filter out all packets except ARPs. Locate 2 of the same ARPS and calculate the Delta Time between them.

For Microsoft devices (pre WIN 2000);

- ✓ Referenced ARP cache entries are aged out after 10 minutes.
- ✓ Unreferenced ARP cache entries are aged out after 2 minutes

For Cisco switches:

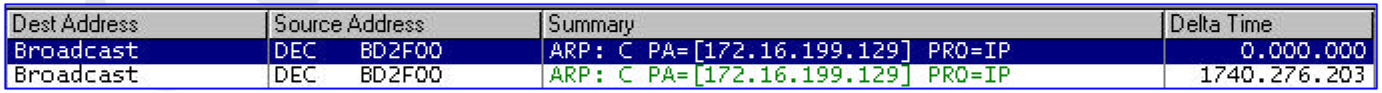
- ✓ The ARP Cache Timeout Value field ranges from 1 to 4,294,967 with a default value of 14,400 seconds.

For Linux:

- ✓ 60 seconds is the default timeout

If a computer is *multihomed*—has more than one NIC—there is a separate ARP cache for each interface.

In the example below, this device takes approximately 29 minutes to age its cache.



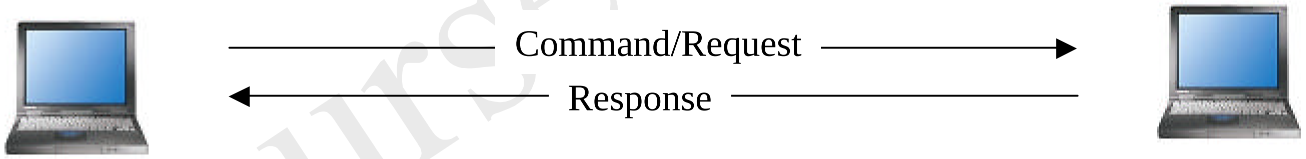
Dest Address	Source Address	Summary	Delta Time
Broadcast	DEC BD2F00	ARP: C PA=[172.16.199.129] PRO=IP	0.000.000
Broadcast	DEC BD2F00	ARP: C PA=[172.16.199.129] PRO=IP	1740.276.203

WIN 2K ARP Cache Aging

- Windows 2000 adjusts the size of the ARP cache automatically to meet the needs of the system.
- If an entry is not used by any outgoing datagram for two minutes, the entry is removed from the ARP cache.
- Entries that are being referenced are given additional time, in two minute increments, up to a maximum lifetime of 10 minutes.
- After 10 minutes, the ARP cache entry is removed and must be rediscovered using an ARP Request frame.
- To adjust the time an unreferenced entry can remain in the ARP cache, change the value of the ArpCacheLife and ArpCacheMinReferencedLife registry entries (HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters).

The ARP Request Frame

- 60 byte packet with an Ethertype of 0x0806 (normal IP traffic is 0x0800).
- This frame is an Ethernet broadcast, containing all F's in the Destination Address field.
- The ARP Reply frame is a directed Ethernet packet, containing the originator of the ARP Request frame in the Destination Address field. The last 28 bytes of the frame contain the ARP header, with the following fields: An Opcode (Operation Code) of 2, which indicates a reply.
- Any implementation of the Address Resolution Protocol (ARP) MUST provide a mechanism to flush out-of-date cache entries. If this mechanism involves a time-out, it SHOULD be possible to configure the time-out value.



```
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender hardware address: 00:e0:03:04:0f:61
    Sender protocol address: 10.10.10.63
    Target hardware address: 00:00:00:00:00:00
    Target protocol address: 10.10.10.200
```

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender hardware address: 00:50:ba:10:ef:1f
    Sender protocol address: 10.10.10.200
    Target hardware address: 00:e0:03:04:0f:61
    Target protocol address: 10.10.10.63
```

Microsoft IP Address Conflict Detection

- IP address conflict detection process applies to stations with either STATIC or DHCP assigned IP addresses.
- If a node sends an ARP request for its own IP address and no ARP reply frames are received, this node assumes its IP address is unique.

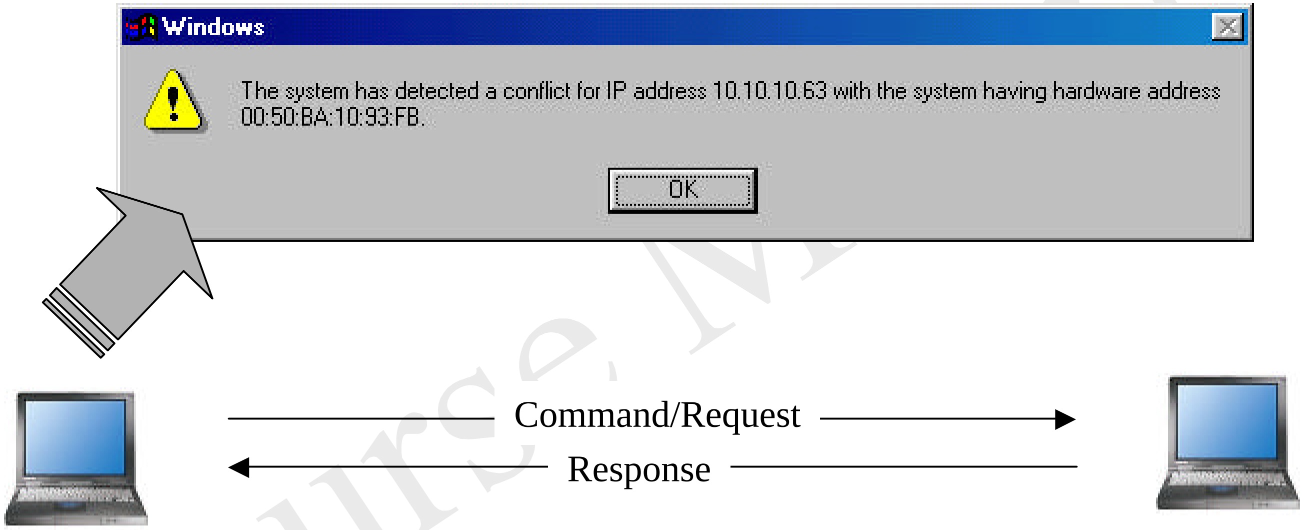
Microsoft defaults to 3 ARP attempts.

- If another node responds to these ARP requests, then we have an address conflict.
- The node with the IP address in question that was turned on first is called the 'defending node'. The node which was just powered on is called the 'offending node'.
- The offending node will prevent its TCP/IP stack from initializing and an error message is displayed.
- Some people believe this detection methodology doesn't work if a station with a duplicate address is turned on and then connected to the network. Not true. Whenever these stations attempt to communicate with another station, they will notice that the SPA is not theirs and the same process will kick in.

Duplicate Address Detection

In the case of a host verifying its IP address is unique, there should not be an ARP Reply frame. If there is, that indicates that the IP address the host is attempting to initialize which is not unique, and the local host does not continue to initialize IP.

- ✓ i.e. Microsoft's Gratuitous ARP.



The system has detected a conflict for IP address 10.10.10.63 with the system having hardware address 00:50:BA:10:93:FB.

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender hardware address: 00:50:ba:10:93:fb
    Sender protocol address: 10.10.10.63
    Target hardware address: 00:00:00:00:00:00
    Target protocol address: 10.10.10.63
```

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender hardware address: 00:e0:03:04:0f:61
    Sender protocol address: 10.10.10.63
    Target hardware address: 00:50:ba:10:93:fb
    Target protocol address: 10.10.10.63
```