

Ethernet Basics

David Morgan

Ethernet Frame



Ethernet Frame consists of:

- 6 Byte Destination MAC address
- 6 Byte Source MAC address
- 2 Byte Ethertype
- 46 - 1500 Bytes Payload

There are other ethernet frame formats but they are the minority

MAC Addresses

MAC address (also known as hardware address or physical address) is a 6 byte address assigned by the IEEE Standards Association and is unique for every Ethernet device ever manufactured.

The first three bytes are the OUI (Organizationally Unique Identifier) the second three bytes is a unique identifier assigned by the vendor



MAC Address

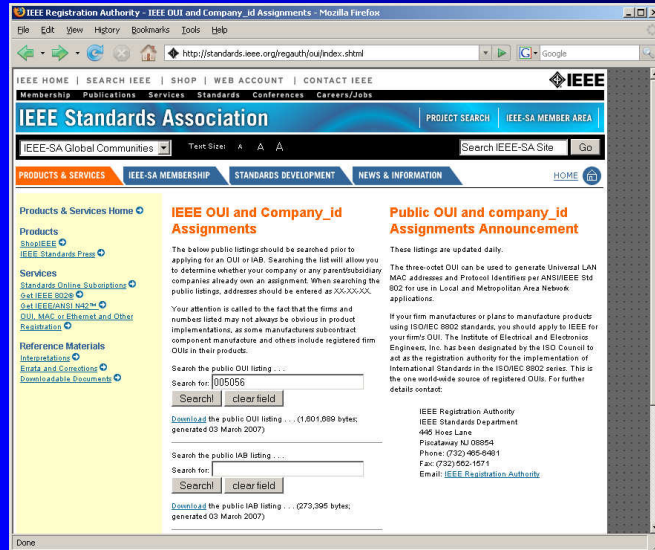
MAC Address of Ethernet NIC

```
[root@thermador: /root]# ifconfig
eth0      Link encap:Ethernet HWaddr 00:D0:59:16:6D:C0
          inet addr:10.100.13.138 Bcast:10.100.255.255 Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0x3440

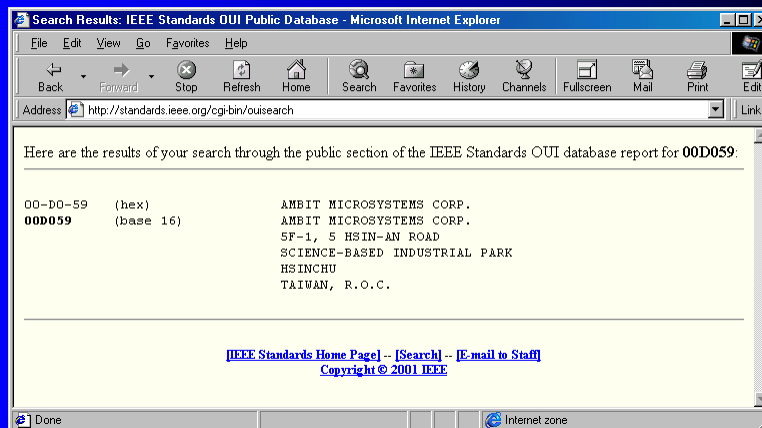
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

[root@thermador: /root]#
```

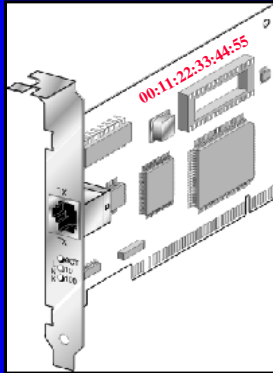
IEEE has the OUI codes...



Each 3 byte pattern is registered to an OEM



Manufacturer burns MAC into NIC

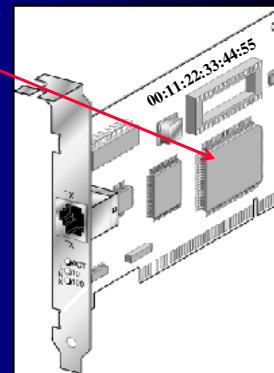
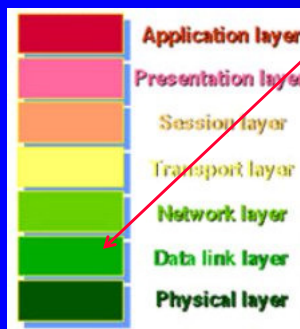


MAC is used by ethernet software

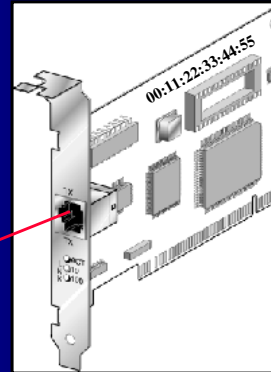
locus of ethernet software

conceptual

physical

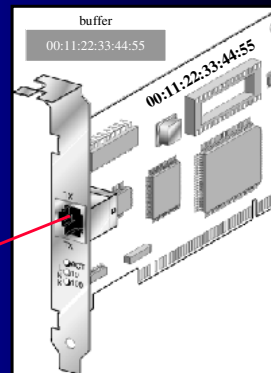


ethernet makes frames,
writes MAC into each as source



to
World

Buffers MAC –
copies MAC to buffer, buffer to frame



Spoofing MAC –

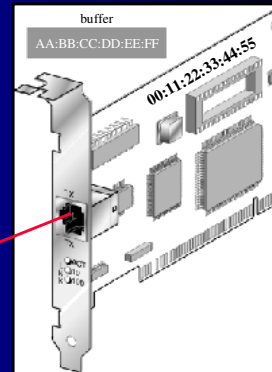
MAC is read-only, but buffer is read-write

```
ifconfig ethX hw ether AA:BB:CC:DD:EE:FF
```

or

```
ip link set ethX address AA:BB:CC:DD:EE:FF
```

writes the buffer



Spoofed



Special MAC Addresses

Broadcast:

A MAC with all bits set FF FF FF FF FF FF is a BROADCAST. It is received by all devices on the Ethernet segment

Multicast:

A MAC address with the least significant bit of the most significant byte set is a MULTICAST address.

01 00 00 00 00 00 00

Note: Ethernet frames are always displayed from most significant to least significant. In actual transmission, each *byte* is transmitted from least significant bit to most significant bit. Some RFCs reference this as “first bit transmitted”. Be aware.

Ethertype

The two bytes after the source MAC in Ethernet II are the Ethertype

Identifies the type of frame:

0800 is IP

0806 is ARP

8137 is Novell IPX

8100 is VLAN

802.3 Ethernet uses these two bytes as a length field

How does a device know which the field refers to???

Data (Payload)

Following the 14 bytes of Ethernet header will be between 46 and 1500 bytes of payload. This will give a minimum Ethernet frame of 60 bytes and a maximum of 1514 bytes

14 bytes header + 46 bytes payload = 60

14 bytes header + 1500 bytes payload = 1514

PDU Encapsulation

The “payload” portion of the ethernet frame usually contains the protocol information from higher layer PDUs such as IP and TCP



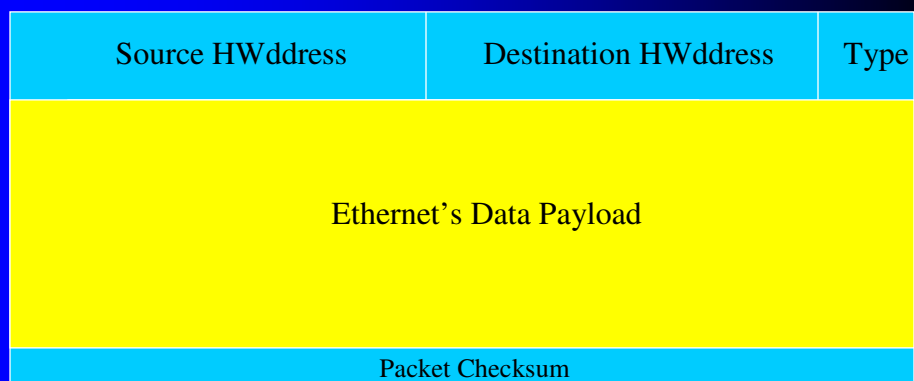
Live Capture

The screenshot shows a network capture tool interface. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. Packet 28 is selected, showing a destination MAC of 08:00:27:00:00:00. A red arrow points from the text "destination MAC" to this value. The bottom pane shows the detailed structure of the selected Ethernet II frame, including fields for Destination, Source, Type, and Protocol. The hex dump at the bottom shows the raw bytes of the frame, with the destination MAC address (08:00:27:00:00:00) circled in red.

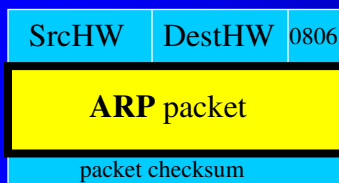
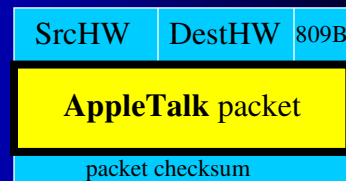
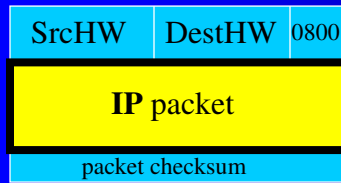
Basic Concepts

- To address a particular network node you *must* have the hardware MAC address
- If the destination MAC isn't right, it doesn't get there
- All higher level protocols sent over ethernet are encapsulated in an ethernet frame

Ethernet frame structure



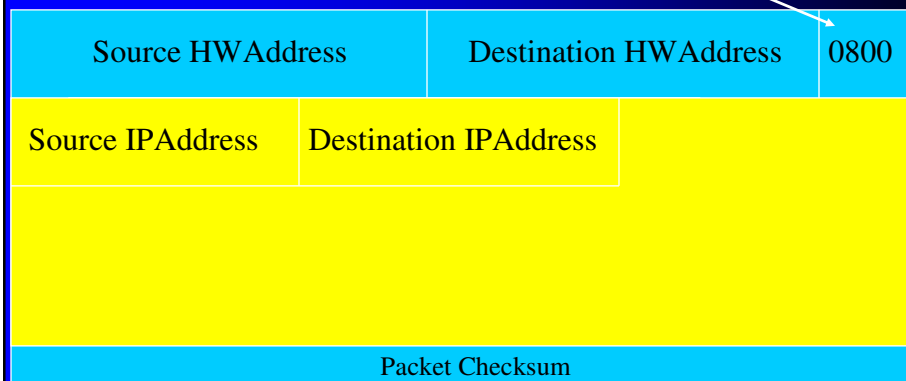
Ethernet types – type examples and their codes



... and many others

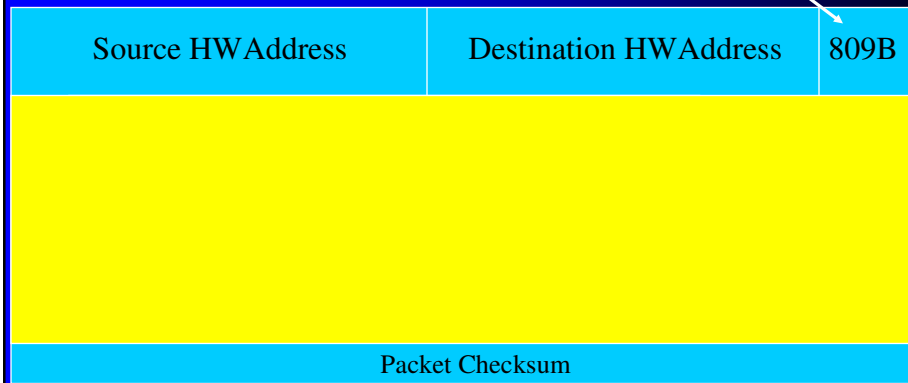
<http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xml>

Ethernet carrying IP



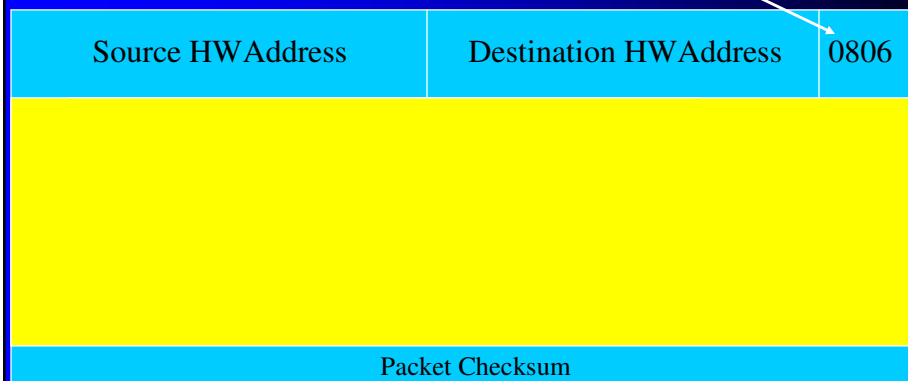
Ethernet's payload may be an IP packet

Ethernet carrying AppleTalk



Ethernet's payload may be an AppleTalk packet

Ethernet carrying ARP



Ethernet's payload may be an Address Resolution Protocol message