Ethernet Basics

David Morgan

Ethernet Frame

Ethernet Frame consists of:

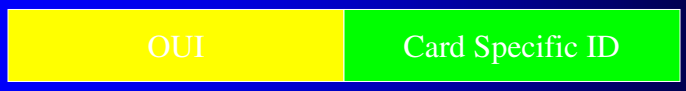
- 6 Byte Destination MAC address
- 6 Byte Source MAC address
- 2 Byte Ethertype
- 46 - 1500 Bytes Payload

There are other ethernet frame formats but they are the minority

MAC Addresses

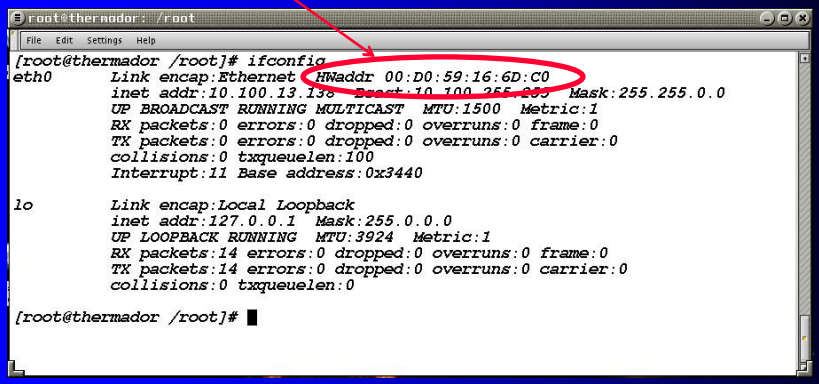
MAC address (also known as hardware address or physical address) is a 6 byte address assigned by the IEEE Standards Association and is unique for every Ethernet device ever manufactured.

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

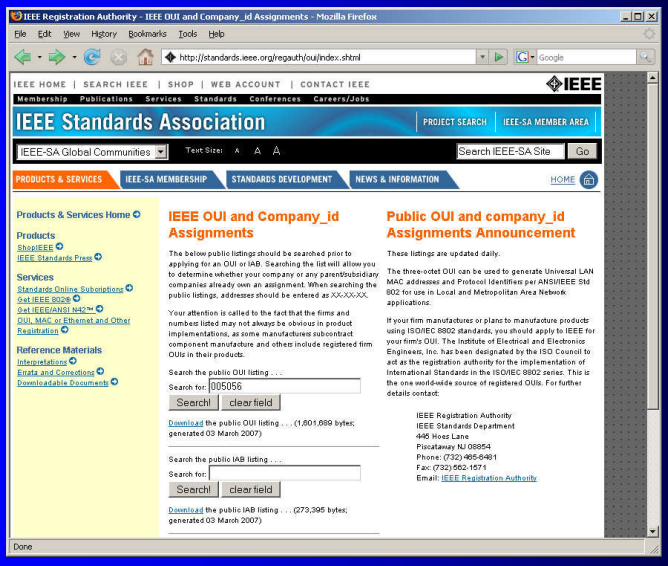


MAC Address

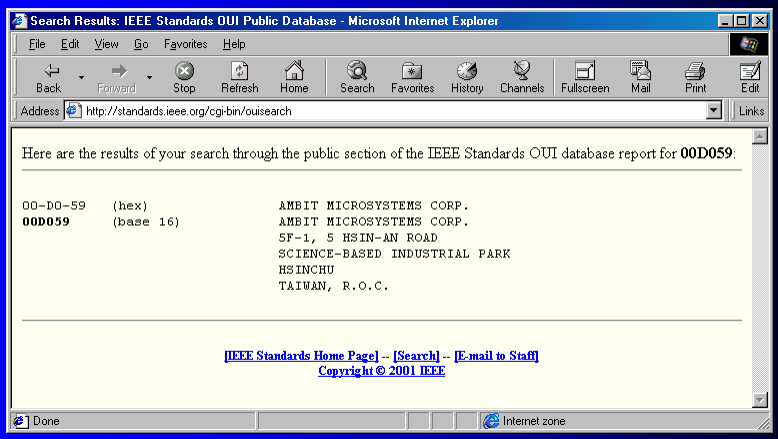
MAC Address of Ethernet NIC



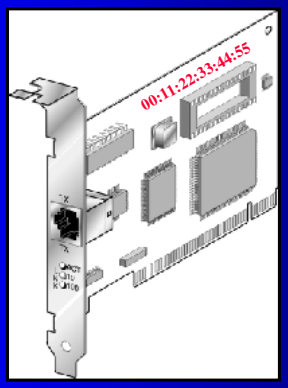
IEEE has the OUI codes...



Each 3 byte pattern is registered to an OEM



Manufacturer burns MAC into NIC

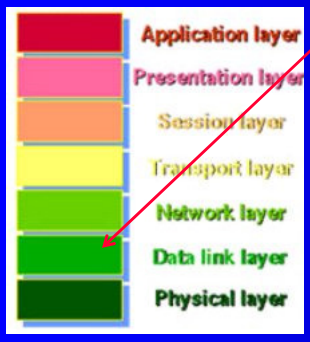


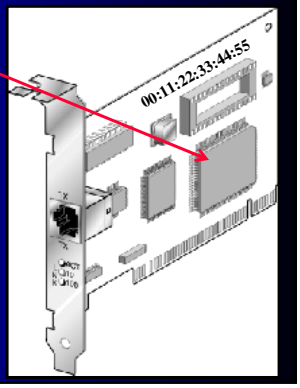
MAC is used by ethernet software

locus of ethernet software

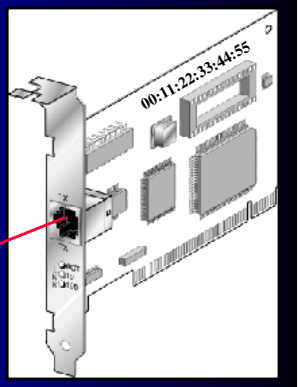
conceptual

physical





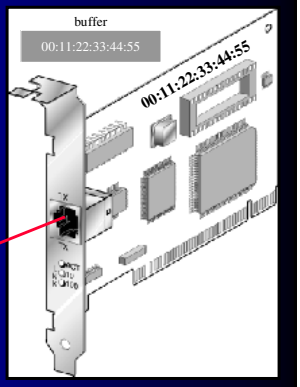
ethernet makes frames, writes MAC into each as source



to World

DEST MAC	00:11:22:33:44:55	ET	PAYLOAD	CRC

Buffers MAC – copies MAC to buffer, buffer to frame



DEST MAC	00:11:22:33:44:55	ET	PAYLOAD	CRC

Spoofing MAC –

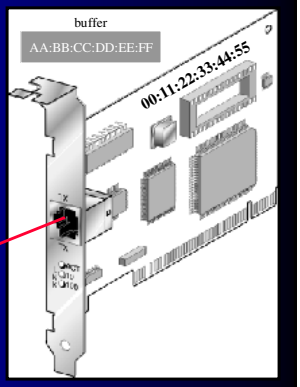
MAC is read-only, but buffer is read-write

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

DEST MAC	AA:BB:CC:DD:EE:FF	ET	PAYLOAD	CRC

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

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)

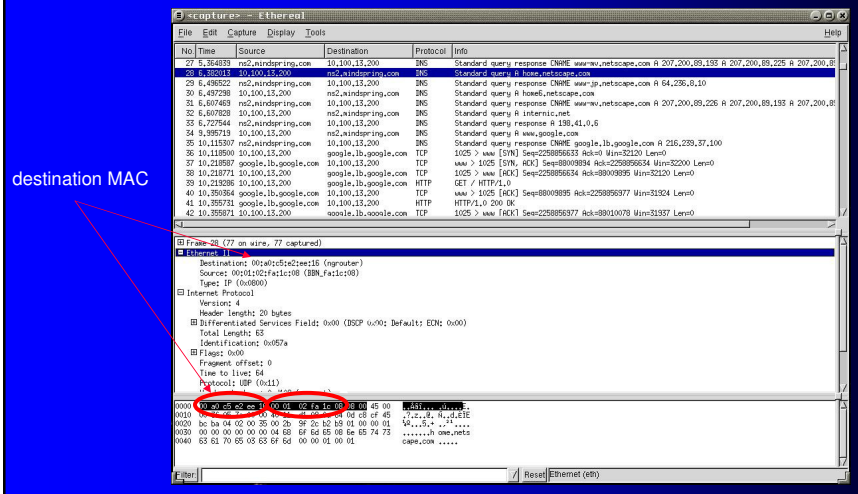
Following the 14 bytes of Ethernet header will be between 46 and 1500 bytes of payload. This will give a minimum Ethernet frame of 60 bytes and a maximum of 1514 bytes

- 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

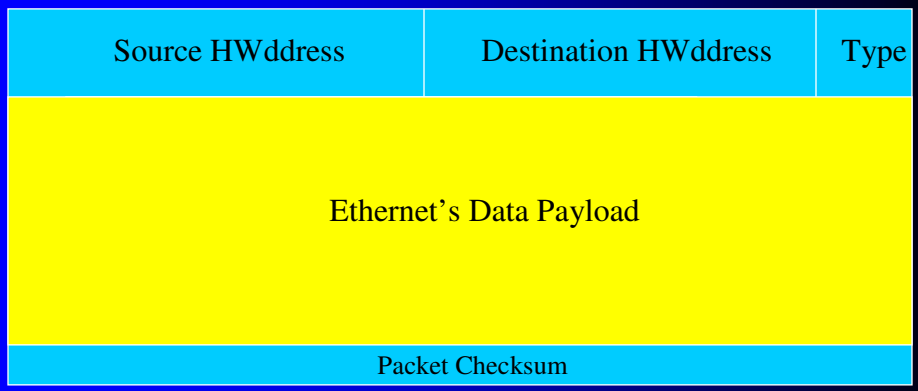
Live Capture



Basic Concepts

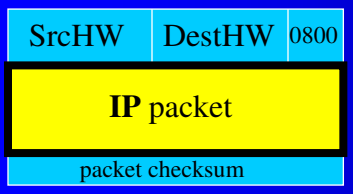
- To address a particular network node you *must* have the hardware MAC address
- If the destination MAC isn't right, it doesn't get there
- All higher level protocols sent over ethernet are encapsulated in an ethernet frame

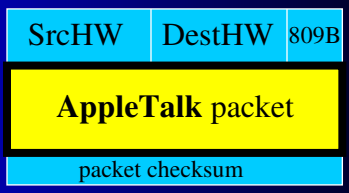
Ethernet frame structure

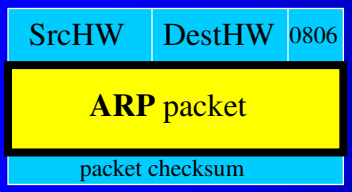


Ethernet types –

type examples and their codes



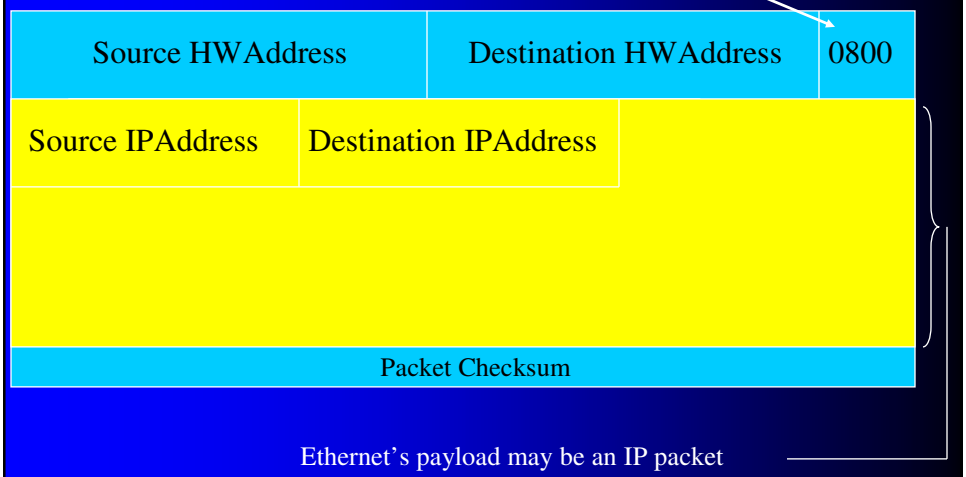




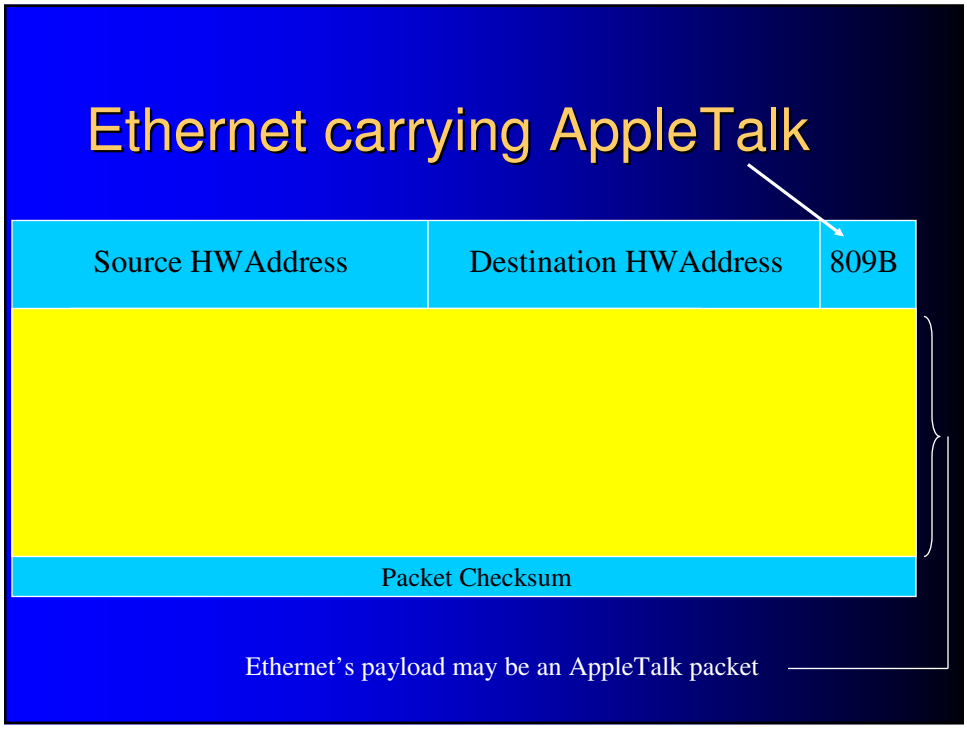
… and many others

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

Ethernet carrying IP



Ethernet carrying AppleTalk



Ethernet carrying ARP