

Re-cap

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Network layer
 - ▶ Ethernet
- ▶ IP
- ▶ ARP
- ▶ ICMP
- ▶ UDP
- ▶ TCP
- ▶ DHCP
- ▶ DNS
- ▶ Applications

Ubiquitous network hardware utilised in LANs with speeds from 10Mbit up to 10Gbit. IEEE 802.3.

- ▶ MAC Address
- ▶ Ethernet frame
- ▶ Hardware

MAC Address

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

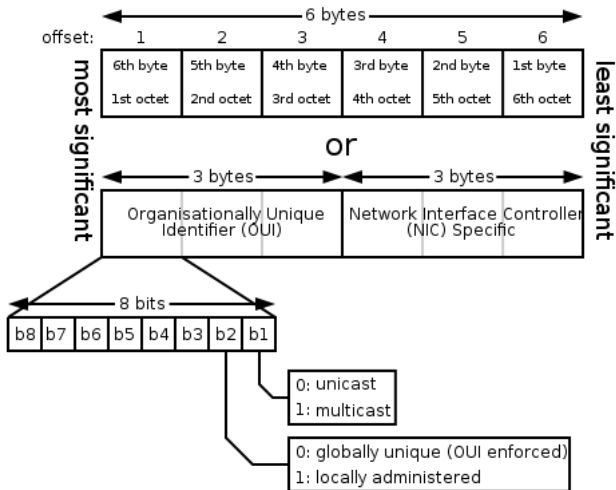


Image taken from Wikipedia

MAC Address

Useful information is the manufacturer specific first three bytes. E.g

http://coffer.com/mac_find/

08:00:69:02:01:FC Take the prefix 080069, manufacturer is Silicon Graphics

Broadcast address is FF:FF:FF:FF:FF:FF

Use ifconfig/ipconfig in linux/windows to view the address

Ethernet frame

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Destination address
- ▶ Source address
- ▶ Type field
- ▶ Data

Ethernet hardware

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Hubs
- ▶ Switches - Managed Switches

IP Numbers

- ▶ IP address
 - ▶ quad dotted notation - 192.168.1.2
 - ▶ Can be represented in decimal 3232235778
- ▶ Addresses allocated by the Internet Assigned Numbers Authority (IANA) to Regional Internet Registries (RIR).
 - ▶ ARIN - North America/Canada
 - ▶ RIPE - Europe, Middle East and Central Asia
 - ▶ APNIC - Asia and Pacific
 - ▶ LACNIC - Latin America/Carribbean
 - ▶ AfriNIC - Africa
- ▶ Classes and CIDR (Classless InterDomain Routing)
- ▶ Private addresses
 - ▶ 10.0.0.0/8
 - ▶ 172.16.0.0/12
 - ▶ 192.168.0.0/16

IP Packet

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

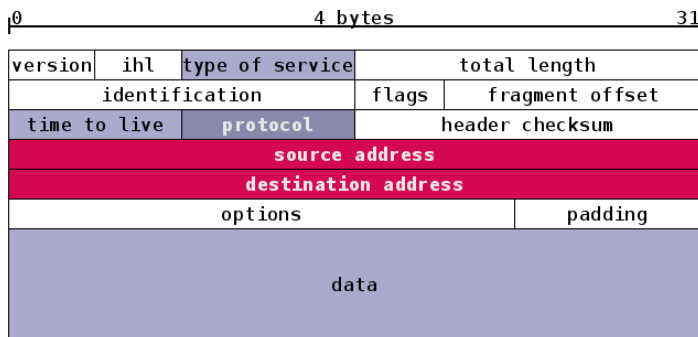


Image from postfixvirtual.net

Relevant fields are

- ▶ Identification and Fragment Offset, More flag
- ▶ Time To Live
- ▶ Protocol
- ▶ Source and Destination address
- ▶ Options - Loose and Strict Source routing

Source Routing

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

A packet sender stores the route to take in the packet. Thus the sender can explicitly route packets as desired. Strict states the explicit route. Loose states some of the hops.

Packet Fragmentation

Packets too large for the MTU are modified

- ▶ Total length set to the shorter size
- ▶ More flag set in all but the last fragment
- ▶ Fragment offset records the position of the fragment in the original datagram
- ▶ Header checksum is recalculated

Address Resolution Protocol (ARP)

Converts from IP to an Ethernet MAC address

- ▶ Host maintains a MAC:IP lookup table
- ▶ Connect to IP is requested, if it's not in the table a ARP Request is issued
 - ▶ Request contains source IP and MAC address
 - ▶ Destination is broadcast address, FF:FF:FF:FF:FF:FF
- ▶ NIC with associated IP responds and updates its own table with the senders MAC and IP.
- ▶ Requester receives response, stores in table and connection is initiated.

Extensions to ARP

- ▶ Proxy ARP
- ▶ Gratuitous ARP
- ▶ ARP Probe
- ▶ RARP - Reverse ARP

Internet Control Message Protocol (ICMP)

Used to transmit error and diagnostic messages. In the event of an error, the header and first 64 bits of the original payload are sent back as payload in the ICMP packet, with the type of control message marked.

- ▶ Error Messages
 - ▶ Destination unreachable
 - ▶ Redirect
 - ▶ Source Quench
 - ▶ Time Exceeded
 - ▶ Parameter problem
- ▶ Query Messages
 - ▶ Echo
 - ▶ Information
 - ▶ Timestamp
 - ▶ Address mask

User Datagram Protocol

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Unreliable transmission with no hand-shaking, error-correction or ordering
- ▶ Stateless
- ▶ DNS uses UDP for data under 512 bytes, TCP otherwise
- ▶ UDP is fast.

Transmission Control Protocol (TCP)

A reliable, connection oriented protocol. Error checking, packet ordering etc. A TCP header consists of, amongst other things,

- ▶ Source and Destination ports (16 bit)
- ▶ Sequence Number
- ▶ Ack Number
- ▶ Flags - ACK, RST, SYN, FIN (and more)
- ▶ Options - MSS

TCP Handshake

Three way conversation to establish a connection, Syn, Syn Ack, Ack. Sequence numbers are used to keep track of messages recieved and to order the packets. The sequence works as follows

- ▶ The client sends a SYN packet to the server with a random SEQ value, x
- ▶ The server responds with an ACK number, $x + 1$, SEQ number y and SYN
- ▶ The client responds with an ACK, $SEQ = x + 1$ and $ACK = y + 1$
- ▶ The client or server begins a connection request with its SEQ number and ack of the other party.
- ▶ Each SEQ number is then incremented by the size of the packets recieved.

A TCP/IP stack is expected to respond to packets in a certain manner, as defined in RFC 793

- ▶ If a socket is closed, send a RST packet
- ▶ If a packet arrives out of order, unacceptable ACK when in LISTEN, SYN-SENT or SYN-RECEIVED, send a RST.

Dynamic Host Configuration Protocol

- ▶ RARP, BOOTP, DHCP
- ▶ Configures IP address, DNS server, gateway router
- ▶ Lease has a duration

Bootstrap Protocol (BOOTP)

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Precursor to DHCP
- ▶ As well as IP address, can be used to download a boot image
- ▶ Can be used in conjunction with TFTP

Domain Naming System (DNS)

Convert from human readable name to IP

- ▶ Hosts file
- ▶ Hierarchical system with 13 root servers
- ▶ Time to Live
- ▶ UDP port 53. TCP for requests over 512 bytes

Domain Naming System (DNS)

Resource records (RRs)

- ▶ Basic element of data
- ▶ Most relevant are A, CNAME, MX, TXT
- ▶ Query this data with nslookup, dig

Domain Naming System (DNS)

```
gavin@dellbot:~$ dig mx dcu.ie

; <<>> DiG 9.5.0-P2 <<>> mx dcu.ie
[...]
```

```
;; QUESTION SECTION:
;dcu.ie. IN MX

;; ANSWER SECTION:
dcu.ie. 86340 IN MX 50 scan5.dcu.ie.
dcu.ie. 86340 IN MX 50 scan4.dcu.ie.

;; AUTHORITY SECTION:
dcu.ie. 24199 IN NS ns5.univie.ac.at.
dcu.ie. 24199 IN NS ns1-ext.dcu.ie.
[...]
```

```
;; Query time: 68 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Feb  9 10:31:21 2009
;; MSG SIZE rcvd: 299
```

- ▶ Names allocated by Domain Name Registrars
- ▶ DNRs accredited by ICANN
- ▶ When registering a domain, must provide
 - ▶ Administrative contact
 - ▶ Technical contact
 - ▶ Billing contact
 - ▶ Name servers

Whois

CA645

Gavin O' Gorman

```
gavin@dellbot:~$ whois dcu.ie
[..]
domain:          dcu.ie
descr:          Dublin City University
descr:          School/Educational Institution
descr:          School/Educational Institution Name
admin-c:        BC116-IEDR
tech-c:         SGD2-IEDR
renewal:        31-December-2009
status:         Active
nserver:        ns1-ext.dcu.ie 136.206.1.1
[..]
source:         IEDR
person:         Fergus Donohue
nic-hdl:        BC116-IEDR
source:         IEDR
person:         Systems Group Dublin City University
nic-hdl:        SGD2-IEDR
source:         IEDR
```

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

Ping

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Technique to determine the roundtrip time between nodes
- ▶ ICMP Echo
- ▶ Other packet types also usable (UDP)
- ▶ Ping a broadcast address

Traceroute

CA645

Gavin O' Gorman

Network layer

IP

ARP

ICMP

UDP

TCP

DHCP

DNS

Applications

- ▶ Determine the route to a particular node
- ▶ Send packets of increasing TTLs to target