Networking - Part 3

Michel FACERIAS

Polytech - Université de Montpellier

16 décembre 2022

In the early years of the Internet, the assignment of addresses to end networks consisted of granting the first octet of the address to this network.

```
Network (dec)      255     .     0     .     0     .     0

Network (bin)   1111 1111 . 0000 0000 . 0000 0000 . 0000 0000
```

That is to say that :

- 256 networks ;
- 16 million possible addresses on each.

Faced with the limitation imposed by this model, in 1981, a new addressing model appears.

RFC 790 [1] provides that an IP address is divided into two parts :

- a part used to identify the network (net id) ;
- a part used to identify a station on this network (host id) ;
- some special ranges of addresses, named **classes** [2].

This addressing method divides the IP address into **five separate classes** based on address four first bits.
Here, classes **A, B, C** offers addresses for networks of **three distinct network sizes**.
Class **D** is only used for **multicast**.
Class **E** reserved exclusively for **experimental** purposes.

1. https://datatracker.ietf.org/doc/html/rfc790
2. Classfull network is now obsolete

Class adressing

A Class

This Class IP address always has its first bit as 0, next 7 bits as a network address and following 24 bits as the host address.

```
Network (bin)  11nn nnnn . hhhh hhhh . hhhh hhhh . hhhh hhhh

               0<--net->   <-------------hosts------------->

Netmask (bin)  1111 1111 . 0000 0000 . 0000 0000 . 0000 0000

Netmask (dec)     255    .     0     .     0     .     0
```

This class of IP address is used for a very large network, for big organisation :

- The range of IP addresses is 0.0.0.0 to 127.255.255.255 ;
- It means that it allows 2^7 networks and 2^{24} hosts per network.

This Class IP address always has its first bit as 10, next 14 bits as a network address and following 16 bits as the host address.

```
Address (bin)  10nn nnnn . nnnn nnnn . hhhh hhhh . hhhh hhhh

               10<----network------>  <-------hosts------->

Netmask (bin)  1111 1111 . 1111 1111 . 0000 0000 . 0000 0000

Netmask (dec)     255    .    255    .     0     .     0
```

This class of IP address is used for a medium network like multinational companies :

- The range of IP addresses is 128.0.0.0 to 191.255.255.255 ;
- It means that it allows 2^{14} networks and 2^{16} hosts per network.

Class adressing

C Class

This Class IP address always has its first bit as 110, next 21 bits as a network address and following 8 bits as the host address.

```
Address (bin)  110n nnnn . nnnn nnnn . nnnn nnnn . hhhh hhhh

               110<----------network----------->  <-hosts->

Netmask (bin)  1111 1111 . 1111 1111 . 1111 1111 . 0000 0000

Netmask (dec)     255    .    255    .    255    .     0
```

This class of IP address is used for a small network such as small companies :

- The first range of IP addresses is 192.0.0.0 to 223.255.255.255 ;
- It means that it allows 2^{21} networks and 2^{8} hosts per network.

This IP address class always has its first bit as 1110, next 28 bits as a **multicast** address.

```
Address (bin)  1110 mmmm . mmmm mmmm . mmmm mmmm . mmmm mmmm

               1110 <----------multicas address ----------->
```

This class of IP address is used for sending a datagram directed to multiple hosts :

- The first range of IP addresses is 224.0.0.0 to 239.255.255.255 ;
- Multicast addresses belongs to different blocs, depending on uses.

This IP address class always has its first bit as 1111, next 28 bits as reserved uses.

```
Address (bin)  1111 rrrr . rrrr rrrr . rrrr rrrr . rrrr rrrr

               1111 <---------- reserved uses ------------->
```

This class of IP address is reserved for future use, research, and development purpose.

From 1984, we begin to see the limitations in the model imposed by classes A B and C :

- class A gives too large networks (2^{24} possible addresses) ;
- class C gives too small networks (255 possible addresses) ;

Two strategies will appear :

- **subnetting**, to break the big network, from 1984 ;
- **supernetting** to aggregate small networks, from 1992.

In 1984, RFC 917 [3] created the concept of sub-network which introduced an additional hierarchical level between the network number and the host number.

It makes possible, for example, to use a **class B network** such as **256 subnets of 254 computers** instead of a single network of 65 534 computers.

```
B Net    (dec)    172     .    16     .     0     .     0
B Net    (bin) 1010 1100 . 0001 0000 . 0000 0000 . 0000 0000
               10<---- network ---->   <------ hosts ------>

Sub  0   (bin) 1010 1100 . 0001 0000 . 0000 0000 . 0000 0000
Sub  0   (dec)    172     .     16    .     0     .     0
               <----------- network ----------->   <-hosts->

Sub 255  (bin) 1010 1100 . 0001 0000 . 1111 1111 . 0000 00000
Sub 255  (dec)    172     .     16    .    255    .     0
               <----------- network ----------->   <-hosts->
```

3. https://datatracker.ietf.org/doc/html/rfc917

In 1992, RFC 1338 [4] proposes to join networks to make bigger ones. It makes possible, for example, to use **255 class C network** such as a single network of 65 534 computers.

```
C     #0 (bin) 1100 0001 . 1111 1100 . 0000 0000 . 0000 0000
C     #0 (dec)    193    .    252    .     0     .     0
               <----------- network ----------->   <-hosts->

C   #255 (bin) 1100 0001 . 1111 1100 . 1111 1111 . 0000 00000
C   #255 (dec)    193    .    252    .    255    .     0
               <----------- network ----------->   <-hosts->

Super N (dec)     193    .    252    .     0     .     0
Super N (bin)  1100 0001 . 1111 1100 . 0000 0000 . 0000 0000
               <----- network -----> <------ hosts ------>
```

4. https://datatracker.ietf.org/doc/html/rfc1338

The notion of class A, B and C has been obsolete since the mid-1990s. Classless Inter-Domain Routing (CIDR) was first developed in 1993 to reduce the size of the routing table contained in routers.
This goal is achieved by aggregating multiple entries in this table into one like virtual supernetting.
Modern routing protocols explicitly indicate the mask network as */NumberOfBits* :

```
Msk (dec)     255     .    255      .     255     .      0

Msk (bin) 1111 1111 . 1111 1111 . 1111 1111 . 0000 0000

Msk (as number of bits)       /28
```

IPv4 can use several material infrastructures to carry its datagrams. We can cite among the most common :

- Local networks, today mainly Ethernet ;
- ATM networks ;
- Serial lines, directly or through POST or ISDN [5] ;
- ...

Each has its own methods of identifying a host. For **Ethernet**, it's based on a layer 2 address, this is **PHY address** (i/e Physical address).

5. Plain Old Telephony System - Integrated Services Digital Network

Ethernet PHY address :

- is an 6 part string, delimited by : ;
- each part is a number representing a byte, often in hexadecimal base ;
- 3 left parts are mostly an Organizationally Unique Identifier [6] assigned by IEEE [7].

These are examples of PHY addresses :

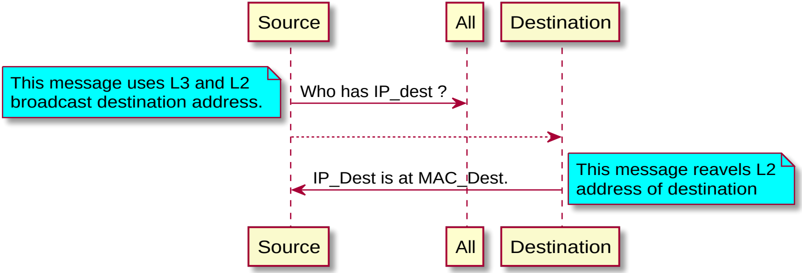
```
<-- OUI -->:<- Network Interface Controler ID ->
   80:00:0b:88:b4:8b

<--- broadcast PHY --->
   ff:ff:ff:ff:ff:ff
```

6. An OUI is a 24-bit number that identifies a manufacturer or organization. See https://macaddress.io/

7. Institute of Electrical and Electronics Engineers is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity - https://www.ieee.org/

ARP[8] stands in IPv4 layer. It's a sub-protocol of IPv4 himself. It is used to discover the PHY address of a destination to make layer 2 transmission possible.



8. Address Resolution Protocol

Each host keeps PHY [9] vs IPv4 matches in a cache, the ARP table :

```
# ip neigh show
192.168.100.42 dev vlan100 lladdr 5c:85:7e:49:0b:18 STALE
192.168.100.39 dev vlan100  FAILED
169.254.185.33 dev vlan100 lladdr b0:7b:25:56:c8:10 STALE
192.168.22.81 dev vlan22 lladdr 00:0b:82:2a:01:01 REACHABLE
192.168.254.229 dev vlan254 lladdr 3c:2a:f4:6f:5e:1d STALE
192.168.70.254 dev vlan70 lladdr 18:1e:78:47:06:74 REACHABLE
```

If ARP request **FAILED**, it's also recorded in ARP table.
When the record is to old, it changes from **REACHABLE** to **STALE**.
In this case, if needed, ARP tries before to verify in **unicast mode** to do a full broadcast ARP request, *a priori* only soliciting the concerned host.

9. Called also MAC address because of the Medium Acces Control layer, or *lladdr* because of Link Layer, both are parts of OSI layer 2.