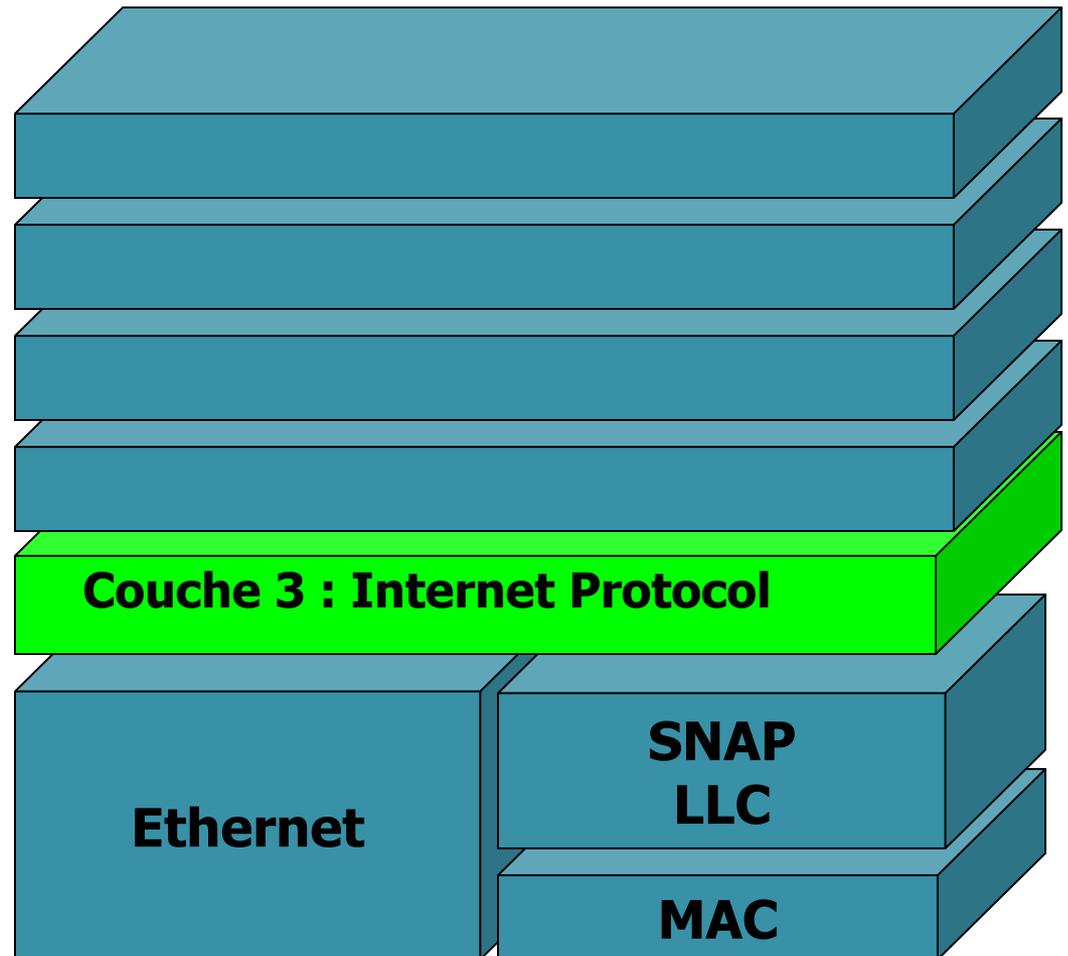


INTRODUCTION AUX RÉSEAU : COUCHE IP

- Protocole Internet



I LE RÉSEAU INTERNET

- Internet Society ou ISOC
- L 'IAB (Internet Architecture Board)
- L 'IRTF (Internet Research Task Force)
- L 'IESG (Internet Engineering Steering Groupage)
 - travaux sur la nouvelle version du protocole IPng
 - l 'administration des réseaux
 - le routage
 - la sécurité
 - la diffusion d 'informations multimédia,
 - ...

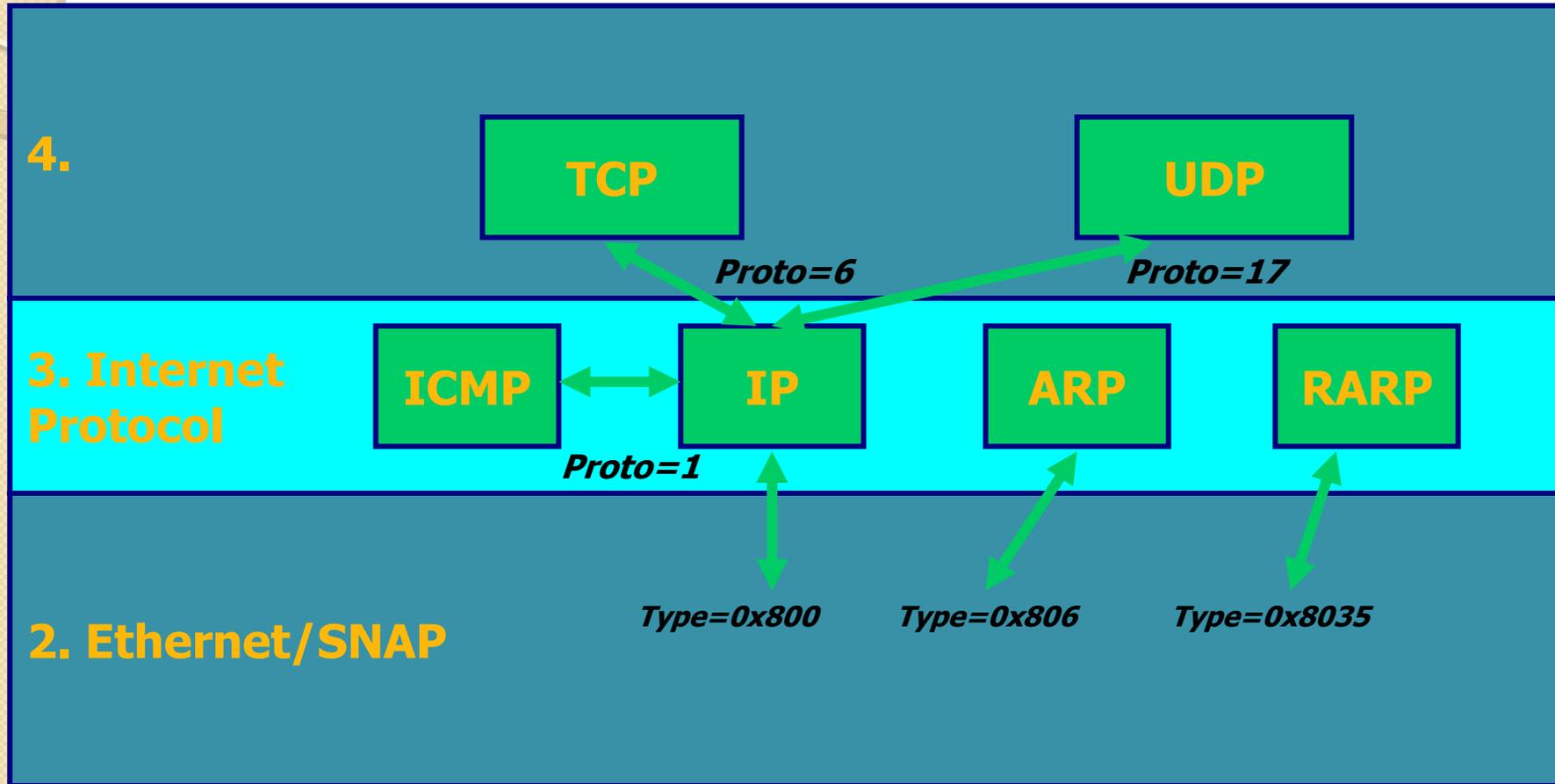
I.I. RFC

- RFC : Request for Comments (gratuit)
- rfc-index : lien sujet/RFC
- Chaque rfc dispose d'un statut qui spécifie son importance:
 - requis : les systèmes doivent mettre en œuvre ce protocole,
 - recommandé: les systèmes devraient mettre en œuvre ce protocole,
 - éligible: il existe plusieurs protocoles effectuant les mêmes fonctions. Le système peut choisir l'un d'entre eux,
 - usage limité: il s'agit généralement de protocole en cours d'expérimentation,
 - non recommandé: il s'agit de protocole très spécifique, expérimental ou dans l'état historique.

I.2. IANA

- IANA (Internet Assigned Number Authority) gère les numéros utilisés dans les piles de protocoles de l'Internet
- rfc 1700 ou sur <ftp://ftp.isi.edu/in-notes/iana/assignments>.
- L'IANA délègue la gestion des adresses des machines connectées au réseau Internet à différents organismes:
 - RIPE NCC (Réseaux IP Européens Network Coordination Center) pour l'Europe,
 - APNIC pour les pays d'Asie et InterNIC pour les Etats-Unis et le reste du monde.
- Ces organismes délèguent à leur tour à des organismes qui gèrent une partie des adresses. Il s'agit soit d'un fournisseur de service, soit d'une entreprise, soit du gestionnaire d'un pays.

2. MISE EN ŒUVRE DES PROTOCOLES TCP/IP



3. LE PROTOCOLE IP

- 3.1. L'adressage Internet
- 3.2. Format des datagrammes

3.1. L'ADRESSAGE INTERNET

- Les classes d'adressage
 - Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (netid, hostid) où netid identifie un réseau et hostid identifie une machine sur ce réseau.
 - Cette paire est structurée de manière à définir cinq classes d'adresse

3.1. L'ADRESSAGE INTERNET

0

8

16

24

31

Classe A



Classe B



Classe C



Classe D



Classe E

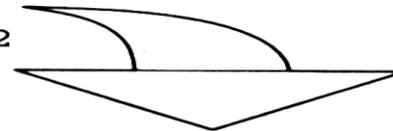


3.1.1. ADRESSES PARTICULIÈRES

- 0 . 0 . 0 . 0 : ne doit pas être employée comme adresse de station.
- 0.<machine> : référence à la machine indiquée sur ce réseau.
- 255.255.255.255 : un datagramme possédant cette adresse sera envoyé à toutes les machines du réseau mais ne sera pas réémis vers les autres réseaux.
- <reseau>.255 ou <réseau>.<sous-réseau>.FF: diffusion vers toutes les machines du réseau ou du sous-réseau.
- 127 . ?? . ?? . ?? : boucle locale.

3.1.2. LE MASQUE DE RÉSEAU

Adresses IP : 192.44.77.79
NetMask : 255.255.255.192



1100 0000.0010 1100.0100 1101.0100 1111
1111 1111.1111 1111.1111 1111.1100 0000



réseau

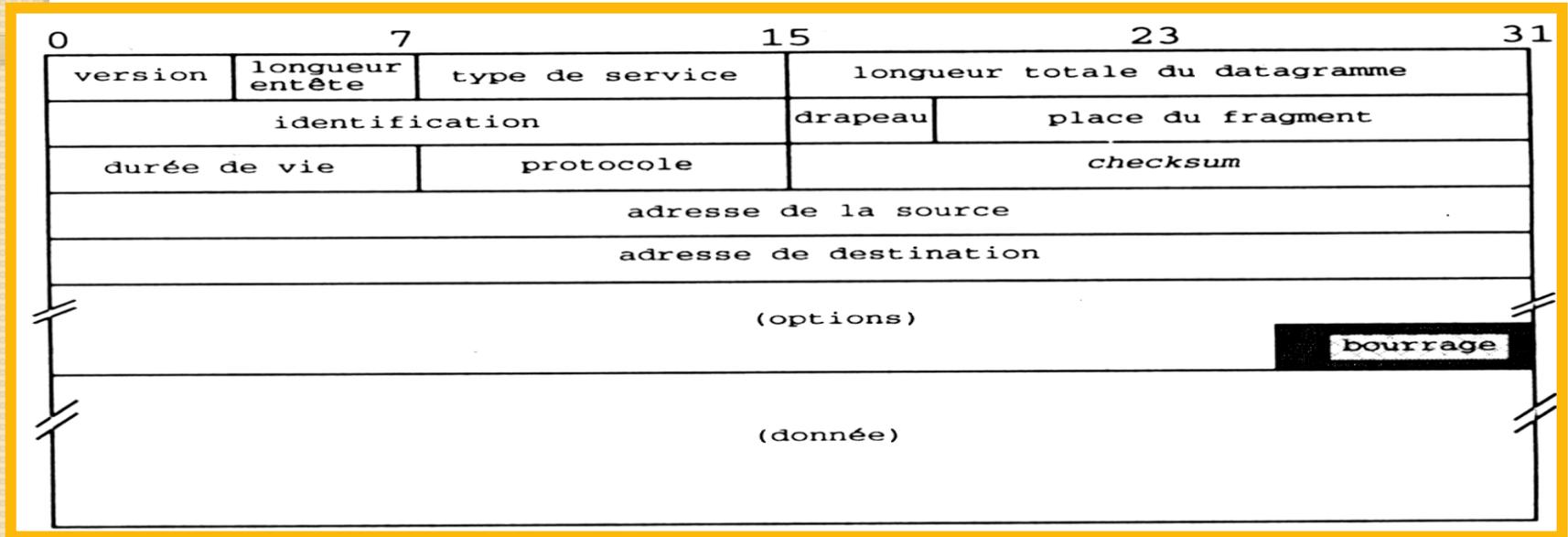
machine



1100 0000.0010 1100.0100 1101.0100 0000
192.44.77.64

1111
15

3.2. FORMAT DES DATAGRAMMES



3.2.1. VERSION

- Champ version
- 4 bits
- différentes versions du protocole IP
- Aujourd'hui tout datagramme de version différente de 4 est éliminé
- IPv4

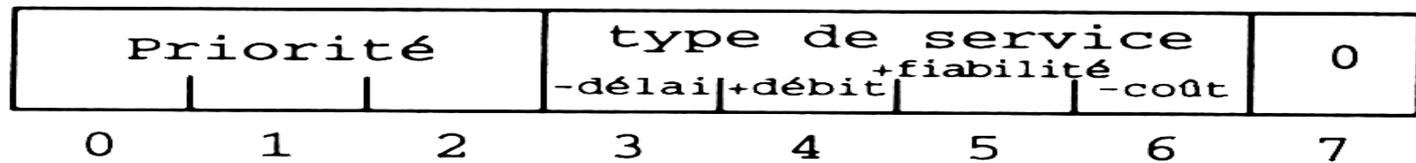
- IPv6 aura pour valeur de version : 6

3.2.2. LONGUEUR DE L'EN-TÊTE

- Champ : Longueur de l'entête ou IHL (Internet Header Length)
- 4 bits
- nombre de mots de 32 bits qui composent l'entête
- La longueur d'un en-tête IP varie à cause du champ option
 - option vide => IHL = 5
 - option souvent complété avec bourrage pour taille multiple de 32 bits

3.2.3. TYPE DE SERVICE

- Champ Type de service ou TOS (Type of Service)
- 8 bits
- contient des informations qui aideront le routeur à choisir le chemin pour le paquet
 - privilégier débit / délai de transmission
 - délai de propagation



3.2.3. TYPE DE SERVICE

application	nature	ToS	
Telnet	Terminal distant	1000	minimise le délai
FTP - contrôle - données	Transfert de fichiers	1000 0100	minimise le délai maximise le débit
TFTP	Transfert de fichiers de configuration	1000	minimise le délai
SMTP - commande - données	Courrier électronique	1000 0100	minimise le délai maximise le débit
NNTP	News	0001	minimise le coût
SNMP	Administration de réseau	0010	maximise la fiabilité

3.2.4. LONGUEUR TOTALE

- Champ longueur totale
- 16 bits
- longueur totale en octet du datagramme (y compris en-tête)
- longueur théorique max est donc : 65535 octets
 - peut-être une limite dans le futur avec de nouvelles technologie
- Remarque : permet dans une trame Ethernet de détecter les bits de bourrage

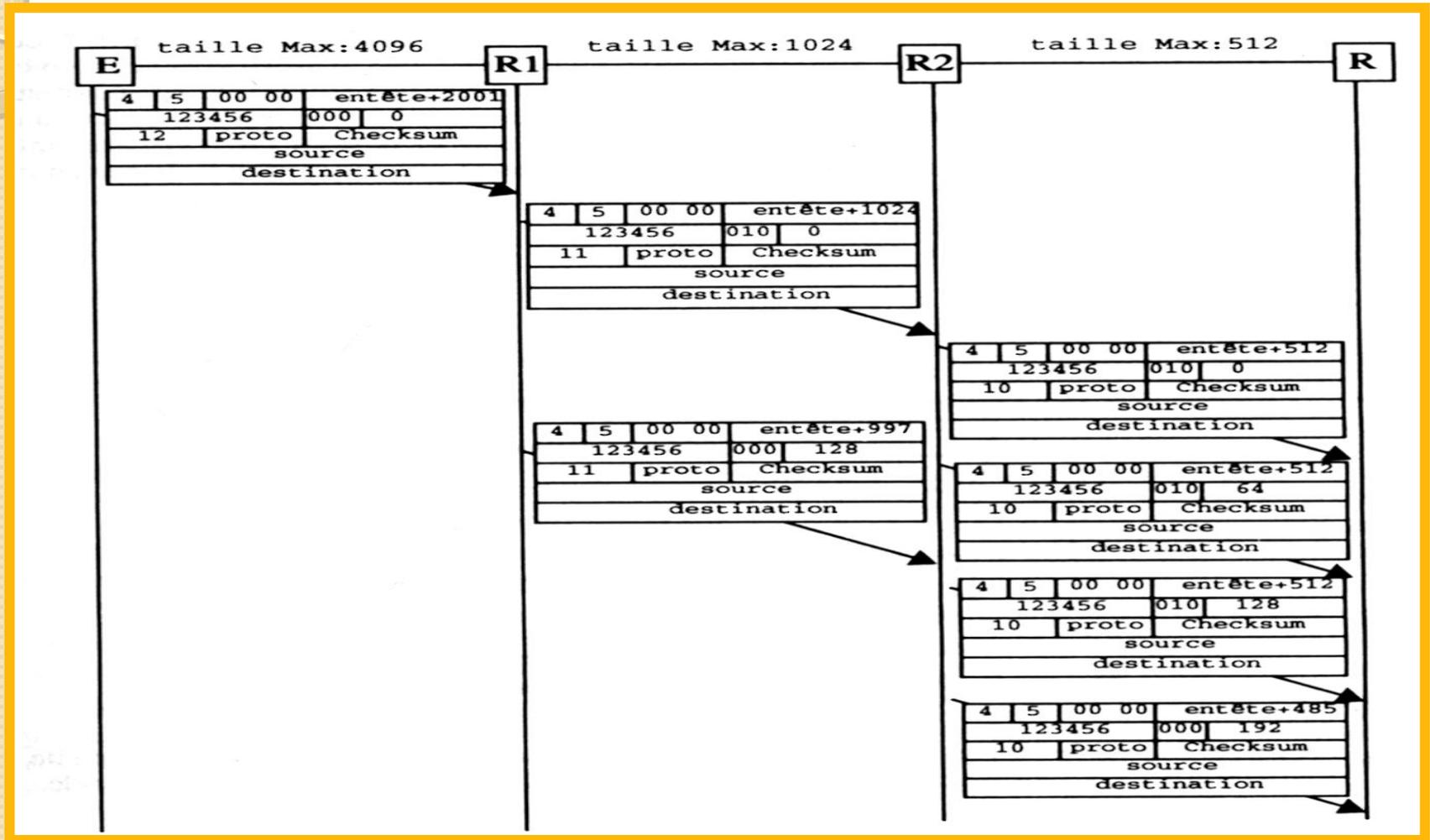
3.2.5. FRAGMENTATION

- Fragmentation si problèmes de taille maximale (MTU Maximum Transmission Unit) entre stations et routeurs
- Découpage en fragments
 - Identification : 16 bits (commun aux fragments)
 - drapeau :

0	MF	DF
----------	-----------	-----------

 - premier bit 0
 - deuxième : Don't Fragment (DF)
 - troisième : (More Fragments) (dernier ou pas)
 - place du fragment (13 bits), par multiple de 8 octets

3.2.5. FRAGMENTATION



3.2.6. DURÉE DE VIE

- Le champ durée de vie
- 8 bits
- temps maximale pendant lequel le paquet peut rester dans le système
 - 0 : le paquet doit être détruit
 - en fait compteur de routeur (décrémenté par chaque routeur qui traite le paquet) = nombre de routeur max que le paquet peut passer : éviter les boucles perpétuelles
- borne le temps de séjour lors du réassemblage des paquets sur le site destinataire (décrémentée d'au moins une unité chaque seconde)

3.2.7. PROTOCOLE

- Champ protocole
- 8 bits
- indique le protocole de la couche supérieure
- voir RFC 1700
 - icmp : 1 (internet control message protocol)
 - tcp : 6 (transmission control protocol)
 - udp : 17 (user datagram protocol)

3.2.8 .CHECKSUM (RFC 1071, RFC 1141)

- Champ checksum
- RFC 1071, 1141
- égal au complément à 1 de la somme en complément à 1 des mots de 16 bits de l'en-tête vu comme un tableau de mots de 16 bits
- Pendant le calcul la valeur de checksum est mise à 0
- Ex : Checksum de l'en-tête suivante :
 - 4500 05dc e733 222b ff11 91f7 c02c 4d60 c02c 4d01
 - addition = 4 6e 04, on replie la retenue : 6e 04 + 00 04 = 6e 08, puis complément à 1 : 91 f7

3.2.9 ADRESSES DE LA SOURCE ET DE LA DESTINATION

- Champs adresse de la source et adresse de la destination
- 32 bits chacun
- adresse de la source peut être de classe A, B ou C
- adresse de la destination peut être de classe A, B, C ou D

3.2.10. OPTIONS

- Champ option
- de longueur variable (peut-être 0)
- Les options sont passées à la couche supérieure

- Le type de l'option est codée sur un octet
 - le premier bit à 1, option recopiée dans tous les fragments, à 0 seulement dans le premier

 - deux bits suivants : classe de l'option
 - 00 : contrôle
 - 01 : réservé pour un usage ultérieur
 - 10 : option pour le débogage et les mesures
 - 11 : réservé pour un usage ultérieur

3.2.10. OPTIONS

- Dans le cas où l'option nécessite des arguments, on ajoute un champ longueur codé sur un octet (multiple de 32 bits, avec bourrage si nécessaire)

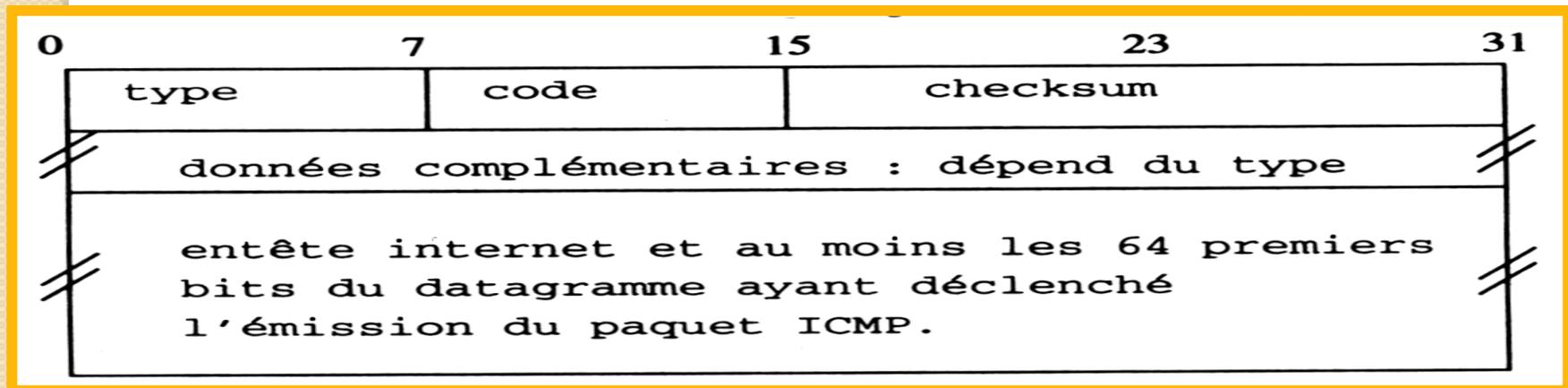
3.2.10. OPTIONS

- Deux files d'attente mise en œuvre dans les routeurs
 - la première pour les paquets sans option
 - la deuxième pour les autres (moins prioritaire)
- Les paquets avec option seront donc plus lents
- exemple : 130 1 00 00010 : SEC (Security) (Rfc 1108), cette option permet de marquer le niveau de sécurité du datagramme
- exemple : 7 0 00 00111 : RR (Record Route), les routeurs ajoutent leur adresse dans le champ paramètre

4. LE PROTOCOLE ICMP (INTERNET CONTROL MESSAGE PROTOCOL) (RFC 792)

- Deux types de paquets ICMP :
 - les messages d'indication d'erreur
 - les messages de demande d'information
- Les messages ICMP sont transportés dans des paquets IP :
 - version 4
 - type de service 0
 - protocole I
- Les émetteur peuvent aussi bien être des stations que des routeurs
- Le paquet ICMP sera envoyé à l'émetteur du paquet initial
- Un paquet ICMP ne peut provoquer l'émission d'un paquet ICMP

4. LE PROTOCOLE ICMP (INTERNET CONTROL MESSAGE PROTOCOL) (RFC 792)



4.1. LE MESSAGE NE PEUT ATTEINDRE SA DESTINATION

- Emis quand un datagramme IP ne peut atteindre sa destination
- Le routeur ou la station qui détecte la faute émet un paquet ICMP avec 3 pour le champ type
- Le champ données complémentaires contient un mots de 32 bits à 0
- Le champ code indique le type de la faute

4.2. DURÉE DE VIE EXPIRÉE ET LE PROGRAMME TRACEROUTE

- Message émis par un routeur quand il reçoit un paquet avec une durée de vie égale à 0
- champ type à 11
- Le champs données complémentaires contient un mots de 32 bits à 0
- Une utilisation détournée du champ durée de vie permet de tracer la route empruntée par un paquet
- Cf. traceroute en TPs

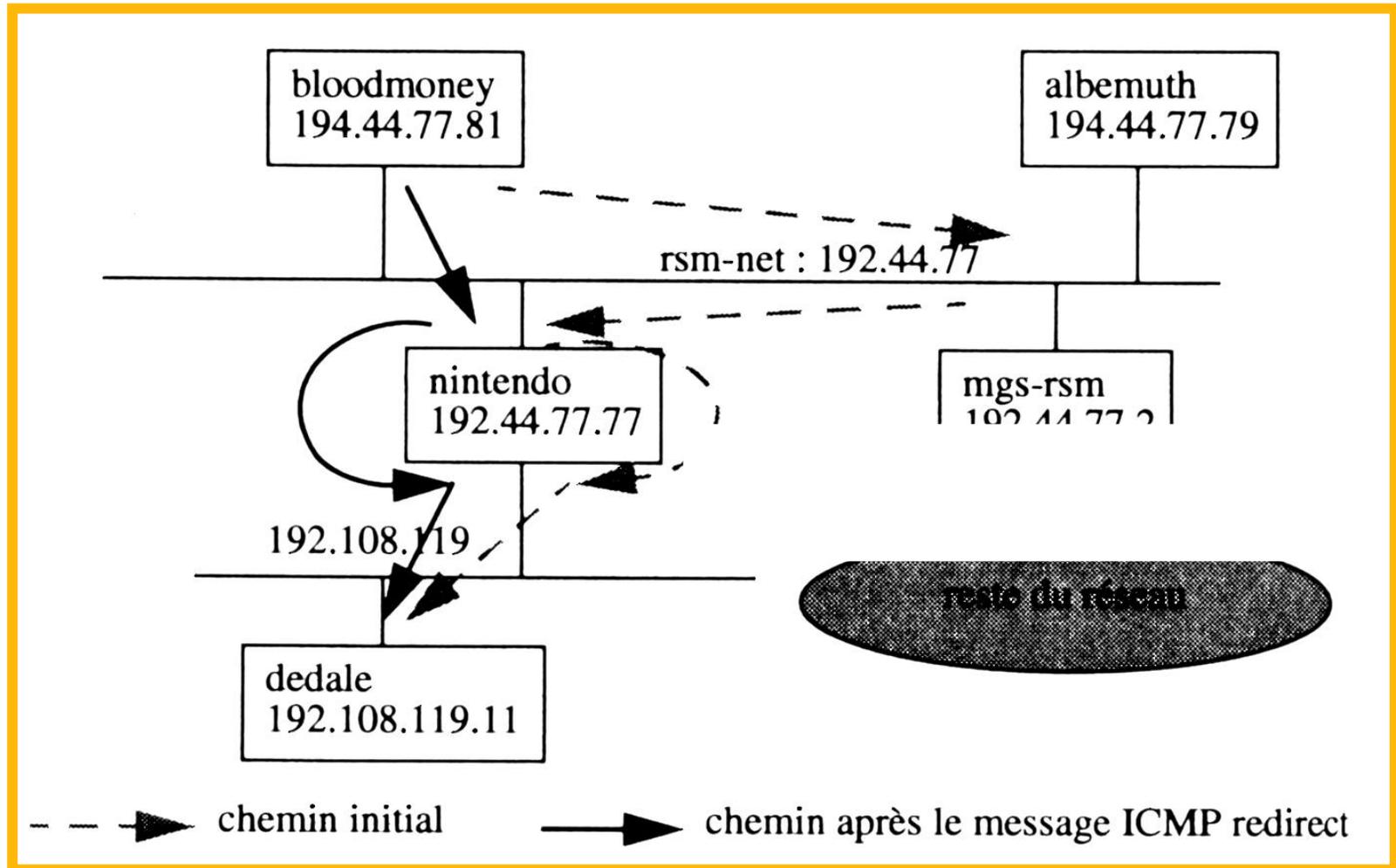
4.3. SOURCE QUENCH

- Le récepteur (station ou routeur) émet avec le champ type 4, pour indiquer que l'émetteur doit réduire sa vitesse d'émission tant qu'il reçoit ce message du routeur
- L'émetteur peut alors augmenter graduellement sa vitesse d'émission jusqu'à ce qu'il reçoive un « source quench ».
- Champs de données complémentaires est un mot de 32 bits à 0
- Le champ code est à 0
- Obsolète

4.4. INDICATION DE REDIRECTION

- Paquet émis quand un routeur connaît une route plus courte pour joindre une machine
- champ type : 5
- champs données complémentaires contient l'adresse du routeur offrant une meilleure route

4.4. INDICATION DE REDIRECTION



4.5. ECHO/LA COMMANDE PING

- La commande ping permet de tester l'accessibilité d'une station
- elle émet un paquet ICMP : demande d'écho (type 8, code 0)
- elle reçoit si la machine distante est active, un paquet ICMP réponse d'écho (type 0, code 0)
- Le champ données complémentaires est divisée en deux champs de 16 bits
 - le premier contient un identificateur du paquet (distinction entre deux utilisateurs faisant un ping simultané)
 - le deuxième champ contient un numéro de séquence pour mesurer les temps d'aller retour sur le réseau et les pertes, quand la commande ping envoie continuellement des paquets

4.5. ECHO/LA COMMANDE PING

- La commande ping crim.eecs.umich.edu donne le résultat crim.eecs.umich.edu is alive

```
#etherfind3 -x -host sega -proto icmp
Using interface le0
icmp type
lnth proto          source          destination
98 icmp            sega            crim.eecs.umich      echo
00 00 0c 06 09 a6 08 00 20 18 87 ba 08 00 45 00
00 54 c2 4d 00 00 ff 01 39 01 c0 0c 4d 49 8d d4
24 10 08 00 ca 19 1e fd 00 00 2d 7c 92 06 00 0b
64 58 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37

98 icmp crim.eecs.umich      sega            echo reply
00 00 20 18 87 ba 08 00 00 06 09 36 08 00 45 00
00 54 f5 aa 00 00 e9 01 1c a4 8d d4 04 10 00 2c
4d 49 00 00 d2 19 1e fd 00 00 2d 7c 92 06 00 0b
64 58 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37
```

4.5.1. OPTION D'ENREGISTREMENT DE LA ROUTE

- Avec l'option -R, ping crée un paquet ICMP permettant d'enregistrer les adresses des routeurs intermédiaires.
- La commande ping ftp.ensta.fr produit les paquets suivants :

```

138 icmp          bloodmoney ici-paris.ensta          echo
00 00 00 06 00  a6 08 00 20  1: 74 34 03 00 14f 00
00 7c 6c e5 00  00 1f 01 96  e8 c0 2c 4d 51 93 fa
01 14 07 27 04  00 00 00 00 00  00 00 00 00 00  00 00 00 00
00 00 00 00 00  00 00 00 00 00  00 00 00 00
00 00 00 00 00  00 00 00 00  00 08 00 e7 c9 19 b6
00 01 30 15 05  8a 00 01 d5  db 08 09 0a 0b 0c 0d
0e 0f 10 11 12  13 14 15 16  17 18 19 1a 1b 1c 1d
1e 1f 20 21 22  23 24 25 26  27 28 29 2a 2b 2c 2d
2e 2f 30 31 32  33 34 35 36  37

138 icmp ici-paris.ensta          bloodmoney          echo reply
00 00 00 1c 74  34 00 00 00  00 09 a6 08 00 14f 00
00 7c 36 e5 00  00 1f 01 fb  93 93 fa 01 14 c0 3c
4d 51 07 27 28  c1 34 48 02  c1 30 4e 2a  c1 30 4e
1b c0 5d 2b d1  c0 5d 2b 89  c0 5d 2b 74  c1 30 35
11 c1 30 35 21  c1 30 4b 31  00 00 00 ef c9 19 b6
00 01 30 15 05  8a 00 01 d5  db 08 09 0a 0b 0c 0d
0e 0f 10 11 12  13 14 15 16  17 18 19 1a 1b 1c 1d
1e 1f 20 21 22  23 24 25 26  27 28 29 2a 2b 2c 2d
2e 2f 30 31 32  33 34 35 36  37

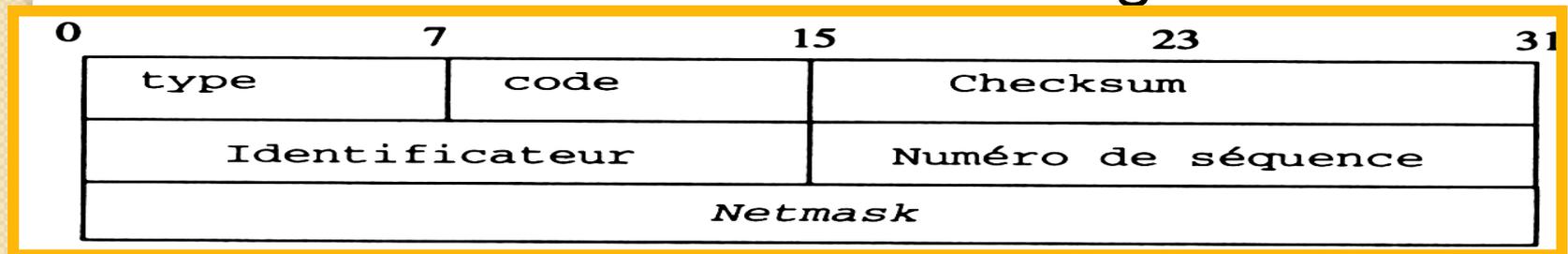
```

4.5.2. ADRESSE DE DIFFUSION

- Dans certaines conditions, si le routeur l'autorise, le ping peut prendre une adresse de diffusion
- La commande ping envoie un paquet en diffusion sur le réseau distant
- Chaque machine du réseau reçoit une requête et y répond

4.6. DEMANDE DE NETMASK/RÉPONSE AU NETMASK

- RFC 950
- Une station pour se configurer peut émettre sur le réseau un paquet ICMP (type 17) demandant le netmask employé sur ce réseau.
- Un routeur ou une station configurée retourne

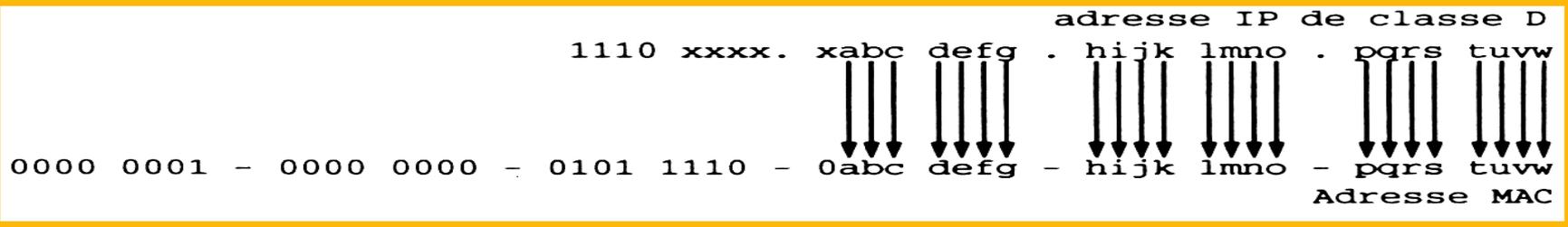


4.7. INFORMATION SUR LES ROUTEURS (RFC 1256)

- Une station, pour émettre des données vers des stations que se trouvent sur un autre réseau, doit connaître l'adresse de routeurs
- Le protocole ICMP router discovery permet aux routeurs d'annoncer périodiquement leur présence
 - soit en utilisant l'adresse de multicast 224.0.0.1
 - soit en diffusant sur le réseau local avec l'adresse de diffusion 255.255.255.255
- Le message ICMP type 10 contient la liste des routeurs et un champ de préférence
- Les stations doivent choisir celui qui a la valeur la plus élevée
- La liste est diffusée sur le réseau toutes les 7 à 10 minutes, mais une station peut demander une retransmission en émettant un message ICP type 9

5. INTERNET ET LE MULTICAST (RFC 1112)

- Trois méthodes de transmission :
 - le point à point ou unicast
 - la diffusion généralisée ou broadcast
 - la diffusion restreinte ou multicast
 - adresses de classe D



5.1. EMISSION/RÉCEPTION DE DONNÉES MULTICAST

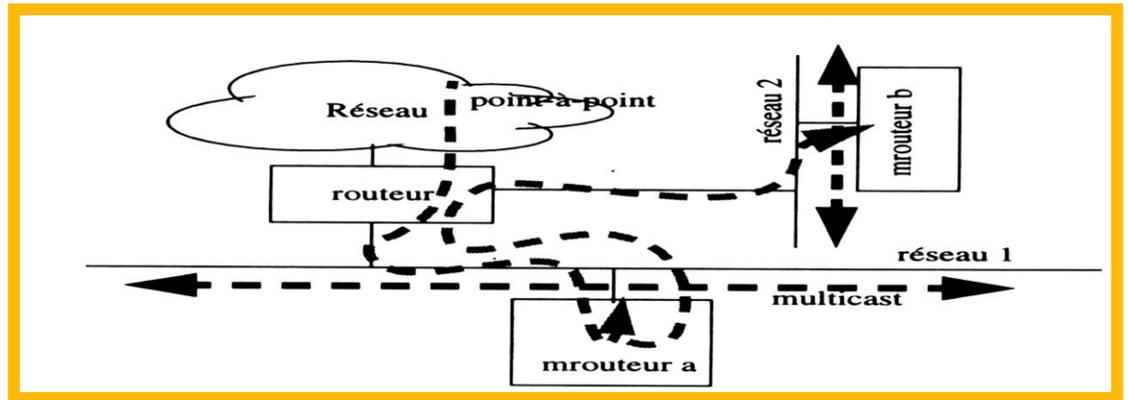
- 5.1.1. Emission
 - au niveau MAC, l'émission d'une trame multicast ou point-à-point est identique
 - il suffit de mettre l'adresse de multicast dans le champ destination de la trame
- 5.1.2. Réception
 - plus compliquée
 - mécanisme de reconnaissance d'autres adresses au niveau Mac (cf. notion de groupes d'adresses)

5.2. PROPAGATION DU TRAFIC MULTICAST

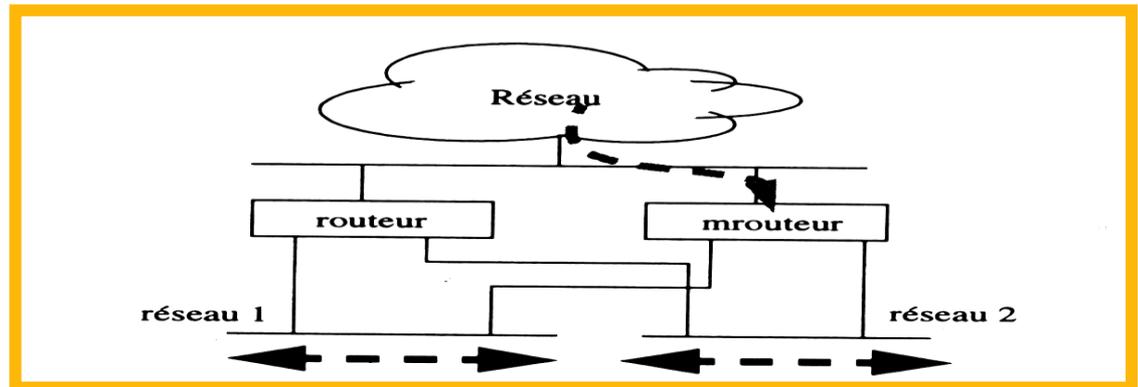
- 5.2.1. Les mrouteurs
- 5.2.2. Portée d'une adresse multicast

5.2.1. LES MROUTEURS

- Multicast avec mrouteurs dans les stations



- Multicast avec mrouteur dédié



5.2.2. PORTÉE D'UNE ADRESSE MULTICAST

TTL	portée
0	limitée à la machine, les paquets ne sont pas émis sur le réseau,
1	limitée au sous-réseau, les paquets ne traverseront pas les mrouteurs,
32	limitée au site,
64	limitée à une région,
128	limitée à un continent,
255	aucune limitation.

5.3. ADRESSES DE CLASSE D RÉSERVÉES

- Les adresses comprises entre 224.0.0.0 et 224.0.0.255 sont réservées aux équipements du sous-réseau et ne sont pas prises en compte

adresse	TTL	seuil	
224.0.0.0	1		Réservé
224.0.0.1	1		Tous les équipements du sous-réseau
224.0.0.2	1		Tous les routeurs du sous-réseau
224.0.0.4	1		DVMRP
224.0.0.5	1		OSPF OSPF tous les routeurs
224.0.0.6	1		OSPF OSPF Routeurs désignés
224.0.0.9	1		RIP-2
224.0.1.10	255	224	IETF-1-LOW-AUDIO (gsm)
224.0.1.11	191	160	IETF-1 AUDIO
224.0.1.12	127	96	IETF-1-VIDEO
224.0.1.13	223	192	IETF-2-LOW-AUDIO (gsm)
224.0.1.14	159	128	IETF-2-AUDIO
224.0.1.15	95	64	IETF-2-VIDEO
224.0.1.16			MUSIC-SERVICE
224.0.6.0 - 224.0.6.127			Cornell ISIS Project

6. CONFIGURATION D'UNE STATION UNIX

- 6.1. L'interface réseau
 - 6.1.1. Consultation
 - 6.1.2. Configuration

6.1. L'INTERFACE RÉSEAU

interface	système	
lo	tous	Loopback. Il s'agit d'une interface qui ne met en œuvre aucun protocole ni matériel. Les données ne sont émises vers aucun support physique. Cette interface est utilisée par les applications client/serveur (comme X-window) quand le client et le serveur sont sur la même machine. Cette interface est utilisée lorsque l'on envoie des paquets IP à l'adresse IP : 127.0.0.1.
le ie lan en	sun sun hp next	Interface Ethernet/IEEE 802.3. Pour les machines sun, le et ie désignent le type de circuit Ethernet.
llc	sun	Couche de protocole contenant LLC.
iip	sun	Protocole SNAP. Ce protocole doit obligatoirement être utilisé au dessus de LLC pour pouvoir utiliser IP.
slip	sun	Protocole SLIP. Protocole utilisé pour encapsuler de l'IP dans une liaison série.
ppp	sun	Protocole PPP. Protocole utilisé pour encapsuler de l'IP dans une liaison série.
sa	sun	Interface ATM.

6.1.1. CONSULTATION

```
>ifconfig -a
le0: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
    inet 193.52.74.81 netmask fffffffc0 broadcast 193.52.74.64
    ether 8:0:20:c:56:62
lo0: flags=49<UP,LOOPBACK,RUNNING>
    inet 127.0.0.1 netmask ff000000
```

6.1.2. CONFIGURATION

- Ifconfig
- adresse MAC :
 - ifconfig le0 82:1:2:3:4:5
- IEEE 802.3 et 802.5
 - ...
- protocole IP :
 - ifconfig le0 ' hostname ' netmask + broadcast
 - /etc/hosts
 - /etc/netmask