PROTOCOLE IP

Architecture D'une Ipv4

RFC791 publié en 1980

Taille : 32 bits = 4 octets
Exemple :

1000 0110	1100 1110	0010 1000	0000 1011
134	206	40	11

Elle est divisible en 2 parties

A cette IP la notation CIDR (Classless InterDomain Routing) peut être indiqué afin de determiner L'ID_RESEAU (Le nombre de bits du CIDR) Et L'ID_HOTE (le reste de bits du CIDR) d'une IP

Exemple :134.206.40.11 / 16 (CIDR)

– ID_réseau : 134.206

– ID_hôte : 40.11

Adresses particulières

Si la partie hôte d'une IP est nul elle ne sert qu'a identifier le réseau, elle ne peut jamais servir comme source ou destination

L'ADRESSE RESEAU

💡 Tips :
Pour calculer une adresse réseau avec un CIDR multiple de 8

Exemple :134.206.40.11 / 16
On LOCK les 16 premiers bits, ici 134.206, L'adresse réseau ressemblera à 134.206.0.0

😭 Malheureusement on ne peut pas tomber que sur des multiples de 8
Exemple :134.206.40.11 / 19
Ici on va prendre le multiple de 8 le plus inférieur
Donc 19>16 , On LOCK les 16 premiers bits et on garde les 3 restant,

134.206

Donc notre 3ème octet correspond à 40

On prend donc les 3 premiers en partant de la gauche, en se rapprochant le + possible du chiffre 40 sans le dépasser

128	64	32	16	8	4	2	1
0	0	1	0	0	0	0	0
1er	2ème	3ème	4ème	5ème	6ème	7ème	8ème

128 n'est pas possible = 1er bit
64 n'est pas possible = 2ème bit
32 est possible = 3ème bits

Donc 16 + 3 = 19 on retrouve notre CIDR

Donc notre IP réseau = 134.206.32.0

Dans ce cas précis seulement 32 peut être ajouté mais si il y avait 128 et 64, cela aurait été 128+64+32 = 224 et donc l'IP aurait été 134.206.224.0

L'ADRESSE DE DIFFUSION

Pour calculer une adresse de diffusion avec un CIDR multiple de 8

Exemple :134.206.40.11 / 16
On LOCK les 16 premiers bits, ici 134.206, L'adresse de diffusion ressemblera à 134.206.255.255

😭 Malheureusement on ne peut pas tomber que sur des multiples de 8
Exemple :134.206.40.11 / 19
Ici on va prendre le multiple de 8 le plus inférieur
Donc 19>16 , On LOCK les 16 premiers bits et on garde les 3 restant, 134.206

Donc notre 3 octets correspond à 40

Sauf que cette fois-ci les bits suivant la troisième passe tous à un

Tableau des bits de 16 à 24

128	64	32	16	8	4	2	1
0	0	1	1	1	1	1	1
1er	2ème	3ème	4ème	5ème	6ème	7ème	8ème

Tableau des bits de 24 à 16

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1
9ème	10ème	11ème	12ème	13ème	14ème	15ème	16ème

Donc notre adresse de diffusion ressemblera à
134.206.63.255

63 car 32+16+8+4+2+1 ET 255 car 128+64+32+16+8+4+2+1

LE MASQUE

Pour calculer un masque avec un CIDR multiple de 8

Exemple :134.206.40.11 / 16
le 1er octets (8bits) vaut 255, le 2ème vaut 255,car on LOCK les 16 premiers bits et les autres valent 0
Donc 255.255.0.0

😱 Malheureusement on ne peut pas tomber que sur des multiples de 8
Exemple :134.206.40.11 / 19
Ici on va prendre le multiple de 8 le plus inférieur
Donc 19>16 , On LOCK les 16 premiers bits et on garde les 3 restant, 255.255

Les 3 premiers bits passent à 1

Tableau des bits de 16 à 24

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0
1er	2ème	3ème	4ème	5ème	6ème	7ème	8ème

Tableau des bits de 24 à 16

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0
9ème	10ème	11ème	12ème	13ème	14ème	15ème	16ème

Donc notre masque ressemblera à
255.255.224.0

224 car 192+64+32

INFO

Un masque inverse c'est le masque contraire
Exemple : 255.255.224.0
Deviendra 0.0.31.255

❓ Comment savoir si 2 IP sont sur le même réseau
Si elles ont le même masque c'est qu'elles sont sur le même réseau.

Adresses Spécial bis

Address Block	Name	Source	Destination
0.0.0.0/8	This network	Oui	Non
0.0.0.0/32	This host on this network	Oui	Non
127.0.0.0/8	Loopback	Oui/Non	Oui/Non
224.0.0.0/4	Multicast	Non	Oui
240.0.0.0/4	Reserved	Non	Non
255.255.255.255/32	Limited Broadcast	Non	Oui

169.254.0.0/16
– Adresses locales au lien **auto-attribuées**

● Adresses privées
– = Non routables sur Internet (local au lien)
– 10.0.0.0/8
10.0.0.0→10.255.255.255

– 172.16.0.0/12
172.16.0.0→172.31.255.255

– 192.168.0.0/16
192.168.0.0→192.168.255.255

DATAGRAMME

La version d'un DATAGRAMME IPv4 est 4
La version d'un DATAGRAMME IPv6 est 6

Concernant les datagrammes, ils seront dans les annexes mais on peut expliquer la fragmentation IP

Si DF (Don't Fragments)
A comme Valeur 0 Fragmentation Obligatoire
A comme Valeur 1 Pas de Fragmentation

Si MF (More fragments)
A comme Valeur 0 C'est le dernier fragment
A comme Valeur 1 on doit encore fragmenter

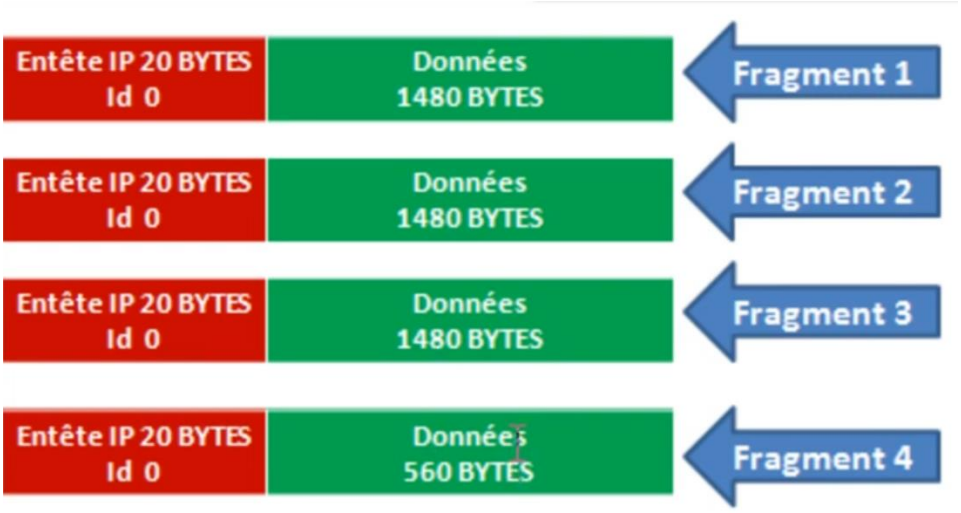
Le Fragment offset : ce champ de 13 bits spécifie la position du fragment dans le paquet IP fragmenté d'origine

Le premier fragment a un fragment offset dont la valeur est 0

Pour le 2ème fragment
Valeur du fragment offset = (taille du premiers fragment – Entête) / 8

EXEMPLE

Premier fragment = 1500 octets --> Fragment offset = 0
MF 1
Deuxième fragment = 1500 octets --> Fragment offset = (1500-20)/8 = 185



Fragment offset = 0
MF = 1

total du paquet = 1500
Fragment offset = (1500-20)/8 =185
MF = 1

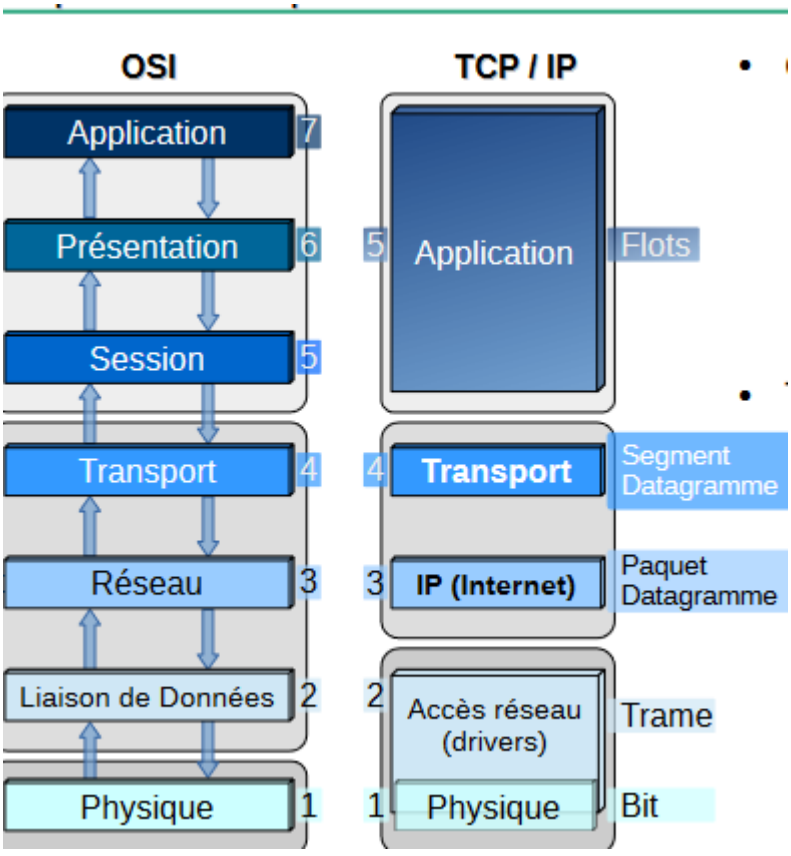
total du paquet = 1500
F offset = (1480+1500-20)/8 =370
MF 1

total du paquet = 580
F offset = (1480+1480+580-20)/8
= 370
MF 0

Pile de communication

Pour les pratiquer il faut seulement lire les datagrammes dans les annexes et les utilisé sur les trames

Concernant les Modèle OSI et Les TCP/IP



Une adresse MAC est une adresse Physique

Le type d'une trame ETHERNET est 2 (II)

IPV6

POURQUOI ❓
Pénurie d'adresses
Complexité de l'en-tête
Explosion de la taille des tables de routages
Besoins de services supplémentaires

Hexadécimal

Séparateur « : » tous les 2 octets (16 bits = mot)

FE80 : 0000 : 0000 : 0000 : 0123 : 0000 : 0000 : 4560

Simplifications.

- « 0 » non significatifs

  FE80 : ~~000~~ 0 : ~~000~~ 0 : 0000 : ~~0~~ 123 : ~~000~~ 0 : ~~000~~ 0 : 4560

  => FE80 : 0 : 0 : 0 : 123 : 0 : 0 : 4560

- Enlever la première plus longue suite de mots nuls

  FE80 : ~~0 : 0 : 0~~ : 123 : 0 : 0 : 4560

  => FE80 : : 123 : 0 : 0 : 4560

Lisibilité : Lettres en minuscules

FE80 : : 123 : 0 : 0 : **B8D0**

=> **fe80 : : 123 : 0 : 0 : b8d0**

Nouveau type de diffusion

ROUTAGE

Si une table de routage na pas un nuage à la fin cela veut dire que les utilisateurs n'ont pas accès à internet

Machine	Itf nom	Itf adresse	Masque	Passerelle
PC1	eth0	192.168.192.1	255.255.255.0	192.168.192.251
PC2	eth0	172.16.43.21	255.255.0.0	172.16.10.1 172.16.10.3
PC3	eth0	10.1.1.23	255.0.0.0	10.1.1.1

Socket (IP + Port)

- IPv4 : 172.18.49.25 : 80
- IPv6 : [fe80::2e41:38ff:feb4:7ebc] : 80

URL : http :[fe80::2e41:38ff:feb4:7ebc]:80/index.html

Liaison spécifique

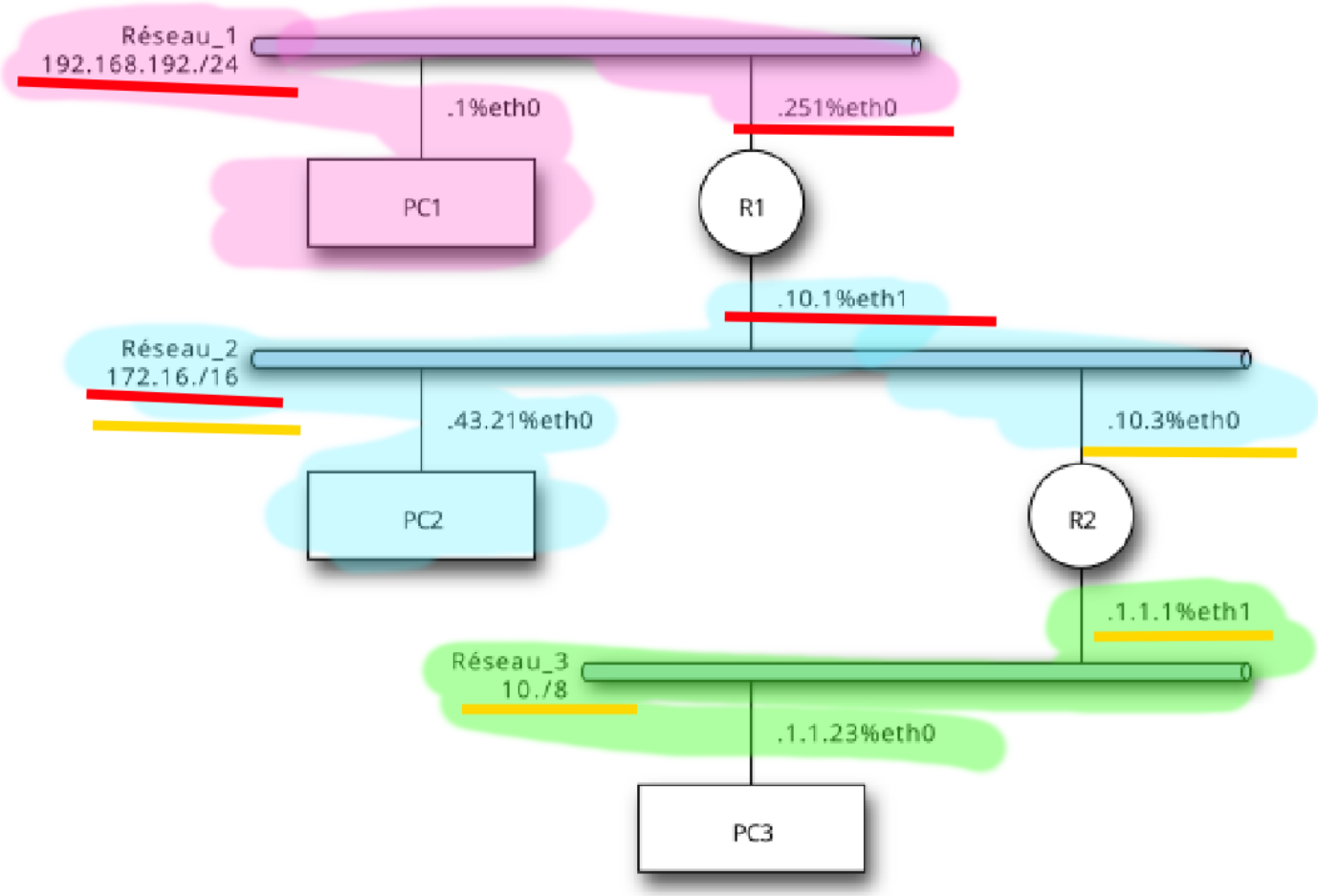
- fe80::2e41:38ff:feb4:7ebc%eth0

Masque : Notation CIDR

- Usage générique comme préfixe (i.e. partie non modifiable)

  Compatible avec la notion de (sous-)réseau

Machine	Destination	Passerelle	Itf nom
R1	192.168.192.0	192.168.192.251	eth0
	172.16.0.0	172.16.10.1	eth1
R2	172.16.0.0	172.16.10.3	eth0
	10.0.0.0	10.1.1.1	eth1



PROTOCOLE

Le protocole “TCP” : (Transmission Control Protocol). Il fait en sorte que l’envoi d’information soit assorti d’une réponse automatique du destinataire afin de s’assurer de l’arrivée des données émises.

Le Protocole “UDP”: (User Datagram Protocol). Il se contente d’envoyer des données sur le réseau. Ici, il n’y a aucune vérification concernant la réception des informations.

Le Protocole “ICMP”: (Internet Control Message Protocol). Il sert à récupérer des informations sur l’état de votre connexion . En envoyant un “ping” ou un “traceroute” vers votre machine, on peut savoir très facilement si vous êtes connecté. Si votre poste répond à la requête, cela signifie qu’il est présent donc accessible.

Le Protocole “SMTP” : (Simple Mail Transfert Protocol). Protocole de transfert des messages électroniques.
Un serveur SMTP permettent l’envoi d’emails.

Le Protocole “FTP” : (File Transfert Protocol). Protocole de transfert de fichiers. Le protocole FTP permet l’enregistrement de fichiers entre ordinateurs sur le modèle “client-serveur”.

Le Protocole “HTTP” : (HyperText Transport Protocol). Le protocole HTTP permet le transfert de documents Hypertext.

Le Protocole “HTTPS” (avec S pour secured, soit « sécurisé ») est la variante du HTTP sécurisée par l’usage des protocoles SSL ou TLS.

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol).

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, 194.153.205.26 est une adresse IP donnée sous une forme technique.

NDP (Neighbor Discovery Protocol) est un protocole utilisé par IPv6. Il opère en couche 3 et est responsable de la découverte des autres hôtes sur le même lien, de la détermination de leur adresse et de l'identification des routeurs présents.

DHCP (Dynamic Host Configuration Protocol) est un protocole de gestion de réseau utilisé pour attribuer dynamiquement une adresse IP à tout appareil ou nœud d'un réseau afin qu'il puisse communiquer à l'aide de l'IP.