

## Sommaire

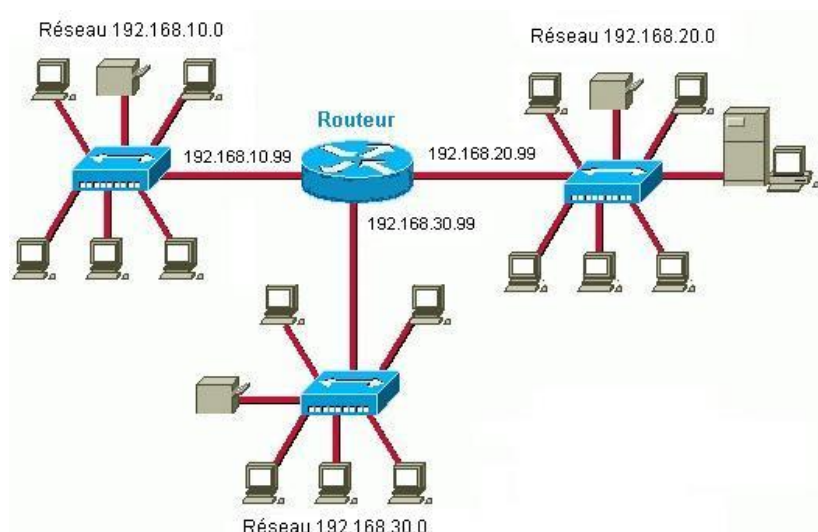
1. Questions – Modèle TCP/IP .....	2
2. Questions – Cartes réseaux d'un routeur .....	2
3. Exercice – Trame Ethernet .....	2
4. Exercice – Adressage IP v4.....	3
5. Exercice – Sous réseau avec adressage IP v4 .....	5
6. Questions – Protocole ARP .....	5
7. Questions – Protocole TCP .....	5
8. Questions – Protocole DNS .....	6
9. Exercice – Décodage de trames .....	7
<i>Format de la trame ETHERNET 802.3.....</i>	<i>8</i>
<i>Les classes d'adresses IP .....</i>	<i>9</i>
<i>Exemple de subdivision d'un réseau de classe B.....</i>	<i>10</i>
<i>Rappel – Structures des entêtes IP, Ethernet, TCP .....</i>	<i>11</i>

## 1. Questions – Modèle TCP/IP

- Q1 - Combien de couches comporte le modèle TCP/IP (utilisé par internet) ? Donner le nom et la fonction de chacune des couches.
- Q2 - Qu'est-ce qu'un protocole ? Citez quelques noms de protocoles connus.
- Q3 - Qu'est-ce que l'encapsulation ?
- Q4 - Qu'est que les « trames » sur un réseau ?

## 2. Questions – Cartes réseaux d'un routeur

- Q1 - Combien de cartes réseaux possède le routeur ?
- Q2 - Combien d'adresses MAC possède le routeur ?
- Q3 - Combien d'adresses IP possède le routeur ?



## 3. Exercice – Trame Ethernet

Il s'agit d'étudier la transmission des trames sur un réseau Ethernet. En annexe page 8 sont présentés le format de la trame 802.3 ainsi que les principaux paramètres du protocole IEEE 802.3.

- Q1 - Quelle est la longueur minimale d'une trame Ethernet ?

Q2 - Que contient le champ *Données* d'une trame ?

Q3 - Quel est le temps d'émission d'une trame de longueur minimale (voir Q1) à 10 Mbps ? À 100 Mbps ?

Q4 - Quel est le temps minimum à respecter entre la fin de l'émission d'une trame et le début de l'émission de la suivante (à 10 Mbps ? à 100 Mbps ?)

Q5 - Combien de trames de taille maximale peuvent être transmises au maximum par seconde sur un réseau à 10 Mbps ? À 100 Mbps ?

#### 4. Exercice – Adressage IP v4

Q1 - De quelle couche du modèle TCP/IP fait partie le protocole IP ? Quel est son rôle ?

Q2 - Par quoi, ou dans quoi est encapsulé un paquet IP ?

Q3 - Convertir en notation décimale l'adresse 0xC0A801FD.

Q4 - Quelle est l'adresse de diffusion pour la machine 192.168.20.0/24 ?

Q5 - Quelle adresse réseau possède la machine 194.45.67.98/26 ?

194.45.67.98	→
/26	→
Adresse réseau	→
Soit	→

##### A. Masque et classe

Q6 - Quelles sont les classes des adresses suivantes ?

- 192.18.97.48 ([www.scrwvs.java.sun.com](http://www.scrwvs.java.sun.com)) → classe
- 138.96.146.2 ([www.inria.fr](http://www.inria.fr)) → classe
- 18.7.22.83 ([www.mi.edu](http://www.mi.edu)) → classe
- 226.192.60.40 → classe
-

Q7 - Pour les classes d'adresses réseau suivantes, donnez le nombre d'hôtes possible :

Classe A → masque 255.0.0.0 → Nb hôtes par réseau =

Classe B → masque 255.255.0.0 → Nb hôtes par réseau =

Classe C → masque 255.255.255.0 → Nb hôtes par réseau =

## B. Masque de sous réseau

Si on souhaite créer un réseau de 1 millions de machines par exemple, il faut utiliser un réseau de classe A. Or, dans ce cas, on perd 15,7 millions d'adresses qui ne seront plus disponibles pour le reste du monde. Ce gaspillage qui a été fait au début d'Internet n'est plus tolérable depuis de nombreuses années, la totalité des adresses disponibles ayant été distribuées. Pour les économiser, on a défini la notion de sous-réseaux (SUBNET).

Dans ce cas, la dernière valeur non nulle du masque peut prendre une valeur autre que 255 ou 0 pour définir ce sous-réseau : Ce sera un nombre décimal correspondant à un nombre binaire composé de 1 contigus en poids fort (1000 0000 ou 1100 0000 ou 1110 000 ou 1111 0000 ou 1111 1000 ou 1111 1100) soit en décimal (128 ou 192 ou 224 ou 240 ou 248 ou 252).

Ainsi on utilise des masques de sous-réseau tels que :

masque 255.255.224.0 définit un sous-réseau d'un réseau de classe B

masque 255.240.0.0 définit un sous-réseau d'un réseau de classe A

masque 255.255.255.192 définit un sous-réseau d'un réseau de classe C

Q8 - Pour ces sous réseaux, donnez le nombre d'hôtes possible:

masque 255.255.224.0 → Nb hôtes par réseau

masque 255.240.0.0 → Nb hôtes par réseau

masque 255.255.255.192 → Nb hôtes par réseau

Q9 - Remplissez le tableau suivant :

Adresse IP	Adresse d'hôte valide ?	@valide → Classe d'adresse @non valide → Pourquoi ?	Masque
150.100.255.256			
175.100.255.18			
195.234.253.0			
100.0.0.23			
3.255.255.255			
134.2.5.255			

## 5. Exercice – Sous réseau avec adressage IP v4

A. Soit un réseau de classe B. L'administrateur veut le tronçonner en sous-réseaux (subnetting) et il décide d'utiliser un masque de 22 bits au lieu de 16.

Q1 - Combien de sous réseaux peut-il utiliser ?

Q2 - Quel sera alors le masque de sous réseau en décimal pointé ?

Q3 - Combien peut-il avoir de machines par sous-réseau ?

B. Un administrateur dispose d'une adresse réseau de classe B 172.16.0.0/16. Il souhaite constituer 7 sous réseaux.

Q1 - Quel masque de sous-réseau peut-il adopter ?

Q2 - Combien de machines pourront être adressées dans chaque sous-réseau ?

Q3 - Pour chacun des 2 premiers sous réseaux : donner le masque du sous réseau, l'adresse IP du sous réseau, les adresses machines de début et de fin, ainsi que l'adresse de diffusion du sous-réseau.

## 6. Questions – Protocole ARP

Q1 - ARP permet de trouver l'adresse IP à partir de l'adresse MAC, vrai ou faux ?

## 7. Questions – Protocole TCP

Q1 - Donnez les numéros des trames correspondant à l'initialisation (three ways handshake) de la communication TCP entre le PC (192.168.189.129) et le serveur activite\_http.olympie.in (178.32.65.67).

Q2 - Que se passe-t-il entre les trames 10 et 37 ?

Q3 - Quelle est la taille maximale des trames Ethernet (en octets) lors du transfert de l'image smiley.jpg (trames 11, 12, ... par exemple).

Q4 - A quoi correspondent les trames n°13, 16, 19 par exemple ?

Q5 - Que signifie le ack=3390 en trame n°13, ou bien le ack=6310 en trame n°16 ? (voir cours TCP)

Q6 - Combien d'octets de données (correspondant au fichier image smiley.jpg) sont transmis par chacune de ces trames de 1514 octets ?

Time	Source	Destination	Protocol	Length	Info
1 0.000000000	192.168.189.129	192.168.189.2	DNS	83	Standard query 0x2374 A activite_http.olymp.e.in
2 0.108399000	192.168.189.2	192.168.189.129	DNS	129	Standard query response 0x2374 CNAME olymp.e.in A 178.32.65.67 A 178.32.167.243
3 0.109360000	192.168.189.129	178.32.65.67	TCP	66	49236->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4 0.145383000	178.32.65.67	192.168.189.129	TCP	60	80->49236 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
5 0.145486000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
6 0.146137000	192.168.189.129	178.32.65.67	HTTP	351	GET / HTTP/1.1
7 0.146382000	178.32.65.67	192.168.189.129	TCP	60	80->49236 [ACK] Seq=1 Ack=298 win=64240 Len=0
8 0.208549000	178.32.65.67	192.168.189.129	HTTP	523	HTTP/1.1 200 OK (text/html)
9 0.279387000	192.168.189.129	178.32.65.67	HTTP	380	GET /images/smiley.jpg HTTP/1.1
10 0.279563000	178.32.65.67	192.168.189.129	TCP	60	80->49236 [ACK] Seq=470 Ack=624 win=64240 Len=0
11 0.319669000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
12 0.320017000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
13 0.320054000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=3390 win=64240 Len=0
14 0.320526000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
15 0.321556000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
16 0.321591000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=6310 win=64240 Len=0
17 0.322991000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
18 0.323674000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
19 0.323716000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=9230 win=64240 Len=0
20 0.325419000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
21 0.326356000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
22 0.326386000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=12150 win=64240 Len=0
23 0.327593000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
24 0.329525000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
25 0.329557000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=15070 win=64240 Len=0
26 0.355920000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
27 0.356837000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
28 0.356873000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=17990 win=64240 Len=0
29 0.357467000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
30 0.358081000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
31 0.358139000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=20910 win=64240 Len=0
32 0.359556000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
33 0.361264000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
34 0.361283000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=23830 win=64240 Len=0
35 0.362006000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
36 0.363794000	178.32.65.67	192.168.189.129	TCP	1514	[TCP segment of a reassembled PDU]
37 0.363829000	192.168.189.129	178.32.65.67	TCP	54	49236->80 [ACK] Seq=624 Ack=26750 win=64240 Len=0

## 8. Questions – Protocole DNS

Observez la capture de trames ci-dessus. Durant cette capture, le navigateur internet du PC (192.168.189.129) émet une requête http GET au serveur activite\_http.olymp.e.in (178.32.65.67) pour lequel il ne connaît pas dans un 1<sup>er</sup> temps l'adresse IP

Q1 - Que se passe-t-il à la trame n°1 ? Qui peut bien être 192.168.189.2 ?

Q2 - Que se passe-t-il au niveau de la trame n°2 ?

## 9. Exercice – Décodage de trames

On a représenté ci-dessous le résultat d'une capture de trame Ethernet avec wireshark par exemple (ni le préambule, ni le FCS ne sont représentés).

Trame 1:

0000	00 12 17 41 c2 c7 00 1a 73 24 44 89 08 00 45 00	...A.... s\$D...E.
0010	00 3c 27 30 00 00 80 01 8f d6 c0 a8 01 69 c0 a8	.<'0.... .....i..
0020	01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66	....MV.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

En analysant cette trame :

Q1 - Entourez en rouge, les octets composant l'entête Ethernet.

Extrayez :

- L'adresse MAC Source :
- L'adresse MAC Destination :
- Le contenu du champ type de protocole. En déduire le protocole encapsulé dans la trame :

Q2 - Entourez en vert les octets composant l'entête IP encapsulée par le protocole Ethernet

Extrayez :

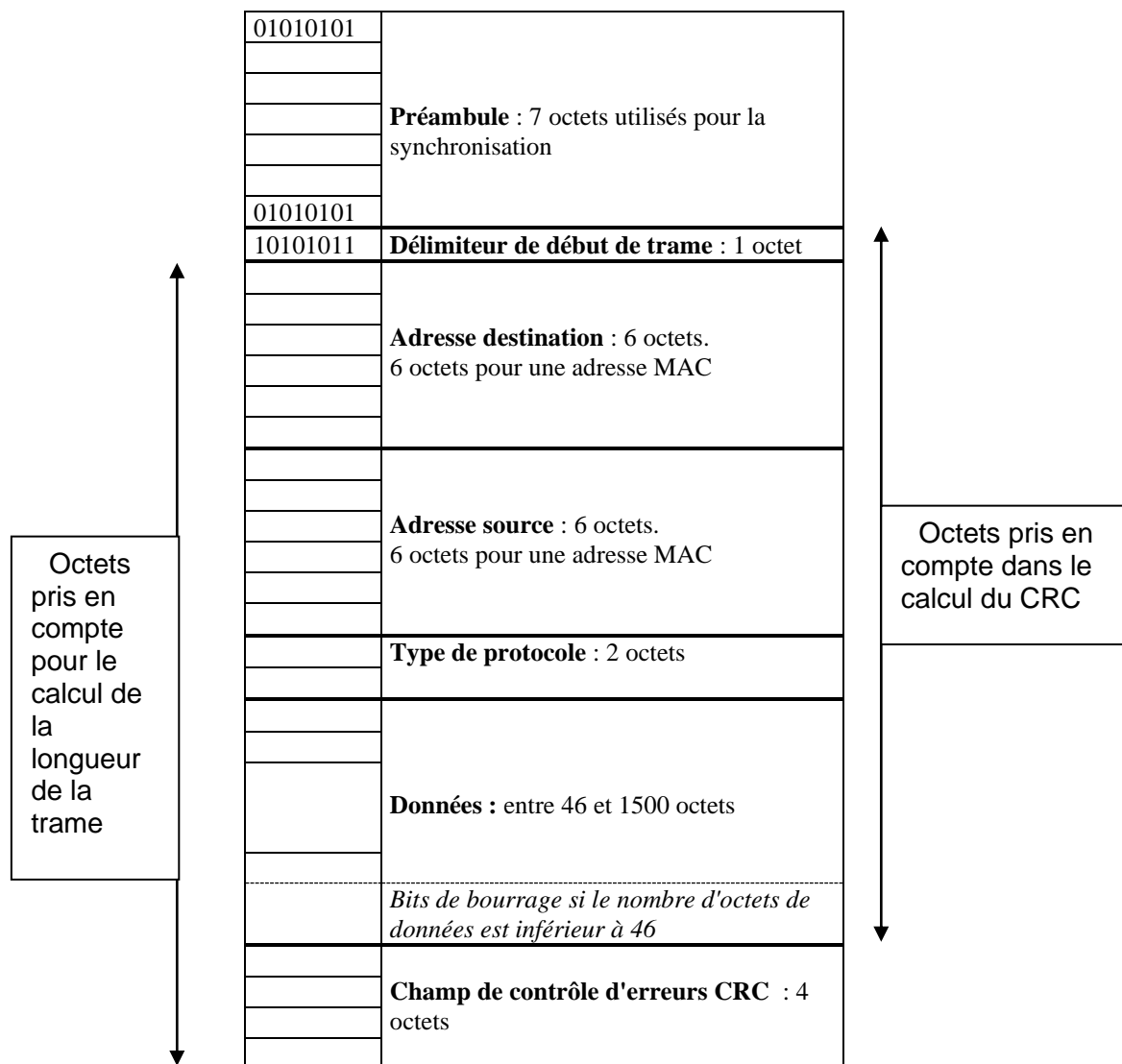
- La version du protocole :
- La longueur de l'entête :
- La longueur totale du datagramme IP :
- La valeur du champ TTL :
- Le contenu du champ protocole. En déduire le protocole encapsulé dans le paquet IP.
- Les adresses IP source et destination :

Q3 - Entourez en bleu, les 4 octets suivants correspondant à l'entête ICMP encapsulé dans le datagramme IP.

Extrayez:

- La valeur du champ type et du champ code. En déduire la nature du message ICMP.

# Format de la trame ETHERNET II



## Paramètres du protocole Ethernet (IEEE 802.3)

- Slot Time : 512 bits-time** (temps de transmission de 512 bits)

Calculé à partir du *round trip delay*, temps total nécessaire à la propagation d'une trame d'un bout à l'autre du réseau, à la détection d'une éventuelle collision provoquée par la trame à l'extrémité du réseau et à la propagation en retour de l'information de collision. Le bit time correspond à la durée de représentation d'un bit.

- Délai minimum inter-trames : 96 bits-time** (temps de transmission de 96 bits)

Calculé de manière à permettre la réinitialisation de la communication et la stabilisation des conditions électriques du support de transmission.

- Jam : 32 bits-time**

Signal de renforcement de collisions. En cas de collision, l'équipement qui détecte la collision diffuse une séquence de bits de bourrage sur le réseau. Il permet d'avertir tous les équipements du réseau de la collision.

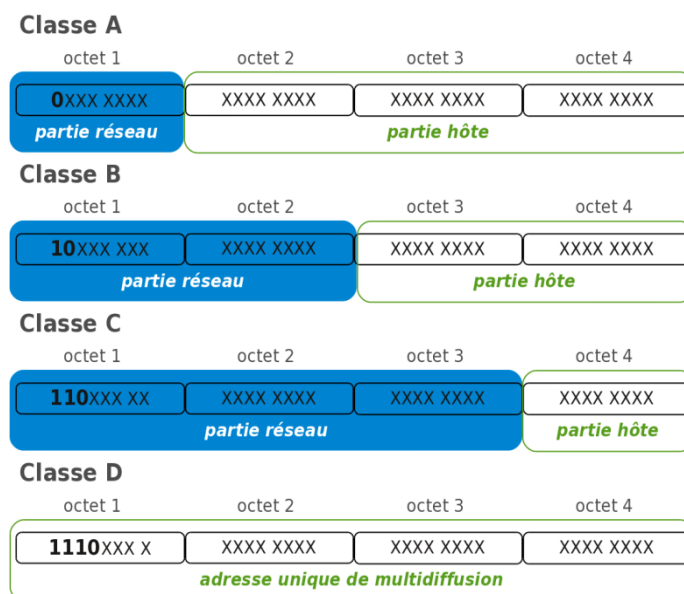
- Calcul du CRC**

Utilisation du polynôme  $G(x) = x^{32} + x^{26} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x$



# Les classes d'adresses IP

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routing) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.



## Classe A

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte. L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

## Classe B

Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

## Classe C

Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

## Classe D

Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

## Classe E

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

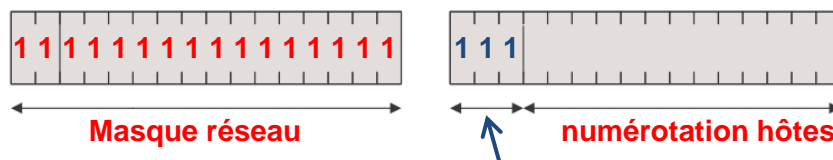
## En résumé : Adresses publiques et privées :

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255 <sup>2</sup>	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		non défini
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

- Les adresses privées de la classe A : **10.0.0.0 à 10.255.255.255**
- Les adresses privées de la classe B : **172.16.0.0 à 172.31.255.255**
- Les adresses privées de la classe C : **192.168.1.0 à 192.168.255.255**

# Exemple de subdivision d'un réseau de classe B

Soit l'adresse de réseau classe B 137.64.0.0 et le masque de réseau 255.255.0.0. Dans un réseau de classe B, il peut y avoir 65534 adresses IP. Nous désirons segmenter ce réseau en au moins 6 sous-réseaux. En se référant au tableau 1, le nombre de bits supplémentaires associés au réseau est 3. On obtient donc le masque de réseau 255.255.224, ce masque génère des adresses IP de la forme suivante :



Bits supplémentaires ajoutés au masque pour la subdivision

Les 8 sous réseaux sont :

Réseau	Adresse réseau décimale	Adresse réseau binaire
1	137.64.0.0	10001001.01000000.00000000.00000000
2	137.64.32.0	10001001.01000000.00100000.00000000
3	137.64.64.0	10001001.01000000.01000000.00000000
4	137.64.96.0	10001001.01000000.01100000.00000000
5	137.64.128.0	10001001.01000000.10000000.00000000
6	137.64.160.0	10001001.01000000.00100000.00000000
7	137.64.192.0	10001001.01000000.11000000.00000000
8	137.64.224.0	10001001.01000000.11100000.00000000

Dans chacun des réseaux il peut y avoir 4094 ( $2^{12} - 2$ ) ordinateurs. Le tableau suivant présente les adresses IP admissibles pour chacun des réseaux :

Réseau	Adresses IP admissibles	Adresse de diffusion
1	137.64.0.1 à 137.64.31.254	137.64.31.255
2	137.64.32.1 à 137.64.63.254	137.64.63.255
3	137.64.64.1 à 137.64.95.254	137.64.95.255
4	137.64.96.1 à 137.64.127.254	137.64.127.255
5	137.64.128.1 à 137.64.159.254	137.64.159.255
6	137.64.160.1 à 137.64.191.254	137.64.191.255

# Rappel – Structures des entêtes IP, Ethernet, TCP

## Structure de la trame Ethernet

```
.....+48bits--+48bits--+16b--+ - - - +.....
.(Pré.)| adresse | adresse |type| données | (CRC) .
.      | dest.   | source   |   |         |
.....+-----+-----+-----+-----+.....
```

Quelques types : 0x0200 = XEROX PUP  
0x0800 = DoD Internet  
0x0806 = ARP  
0x8035 = RARP

## Structure ARP

```
+16b--+16b--+8b+8b+16b--+1gHW--+1gP--+1gHW--+1gP--+
|type|type |lg|lg|Op |Emetteur|Ent.|Récept. |Rcpt|
|HW |Proto|HW|P | |adr. HW |adrP|adr. HW |adrP|
+-----+-----+-----+-----+-----+-----+
```

Quelques types : 0x0001 = Ethernet  
0x0800 = DoD Internet  
Opérations : 0x0001 = Requête  
0x0002 = Réponse

## Structure du paquet IP

```
<-----32bits----->
<-4b->      <-8bits-><-----16bits----->
+-----+-----+-----+-----+
| Ver | IHL | TOS      | Longueur totale (octet) |
+-----+-----+-----+-----+
| Identificateur      | FI | FO |
+-----+-----+-----+-----+
| TTL      | Protocole | Somme de ctrl (entête) |
+-----+-----+-----+-----+
| Adresse Source      |
+-----+-----+-----+-----+
| Adresse Destination |
+-----+-----+-----+-----+
... Options
+-----+-----+-----+-----+
... Données
+-----+-----+-----+-----+
```

Ver = Version d'IP  
IHL = Longueur de l'en-tête IP (en mots de 32 bits)  
TOS = Type de service (zero généralement)  
FI (3 premiers bits) = Bits pour la fragmentation  
\* 1er = Réserve  
\* 2me = Ne pas fragmenter  
\* 3me = Fragment suivant existe  
FO (13 bits suivants) = Décalage du fragment  
TTL = Durée de vie restante

Quelques protocoles transportés :

1 = ICMP	8 = EGP
2 = IGMP	11 = GLOUP
4 = IP (encapsulation)	17 = UDP
5 = Stream	36 = XTP
6 = TCP	46 = RSVP

## Structure du paquet ICMP

```
<-----32bits----->
+-----+-----+-----+-----+
| Type   | Code   | Somme de contrôle (msg) |
+-----+-----+-----+-----+
| Variable (généralement non utilisé) |
+-----+-----+-----+-----+
... Datagramme original + 8 octets
+-----+-----+-----+-----+
```

Quelques types ICMP : 8 = Demande d'écho  
0 = Réponse d'écho  
11 = Durée de vie écoulée  
12 = Erreur de paramètre

## Structure de segment TCP

```
<-----32bits----->
<-4b->      <-6bits-><-----16bits----->
+-----+-----+-----+-----+
| Port Source      | Port Destination |
+-----+-----+-----+-----+
| Numéro de Séquence |
+-----+-----+-----+-----+
| Numéro d'Acquittement |
+-----+-----+-----+-----+
| THL |      | Flag | Taille Fenêtre |
+-----+-----+-----+-----+
| Somme de ctrl (message) | Pointeur d'Urgence |
+-----+-----+-----+-----+
... Options
+-----+-----+-----+-----+
... Données
+-----+-----+-----+-----+
```

THL = Longueur de l'entête TCP sur 4 bits (\*32bits)

Flags = indicateur codé sur 6 bits gauche à droite

- \* 1er = Données urgentes
- \* 2me = Acquiescement (ACK)
- \* 3me = Données immédiates (Push)
- \* 4me = Réinitialisation (Reset)
- \* 5me = Synchronisation (SYN)
- \* 6me = Fin

Options = suites d'option codées sur

- \* 1 octet à 00 = Fin des options
- \* 1 octet à 01 = NOP (pas d'opération)
- \* plusieurs octets de type TLV

T = un octet de type:

- 2 Négociation de la taille max. du segment
- 3 Adaptation de la taille de la fenêtre
- 4 Autorisation des acquiescements sélectifs
- 8 Estampilles temporelles

L = un octet pour la taille totale de l'option

V = valeur de l'option (sur L-2 octets)

## Structure de datagramme UDP

```
<-----32bits----->
+-----+-----+-----+-----+
| Port Source      | Port Destination |
+-----+-----+-----+-----+
| Longueur UDP      | Somme de ctrl (message) |
+-----+-----+-----+-----+
... Données
+-----+-----+-----+-----+
```

## Services associés aux ports

ftp-data	20/tcp		
ftp	21/tcp		
ssh	22/tcp	ssh	22/udp
telnet	23/tcp		
smtp	25/tcp		
domain	53/tcp	domain	53/udp
		tftp	69/udp
finger	79/tcp		
www	80/tcp	www	80/udp
kerberos	88/tcp	kerberos	88/udp
pop-3	110/tcp	pop-3	110/udp
		snmp	161/udp
		snmp-trap	162/udp