Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Gabès

Institut Supérieur d'Informatique et de Multimédia de Gabès

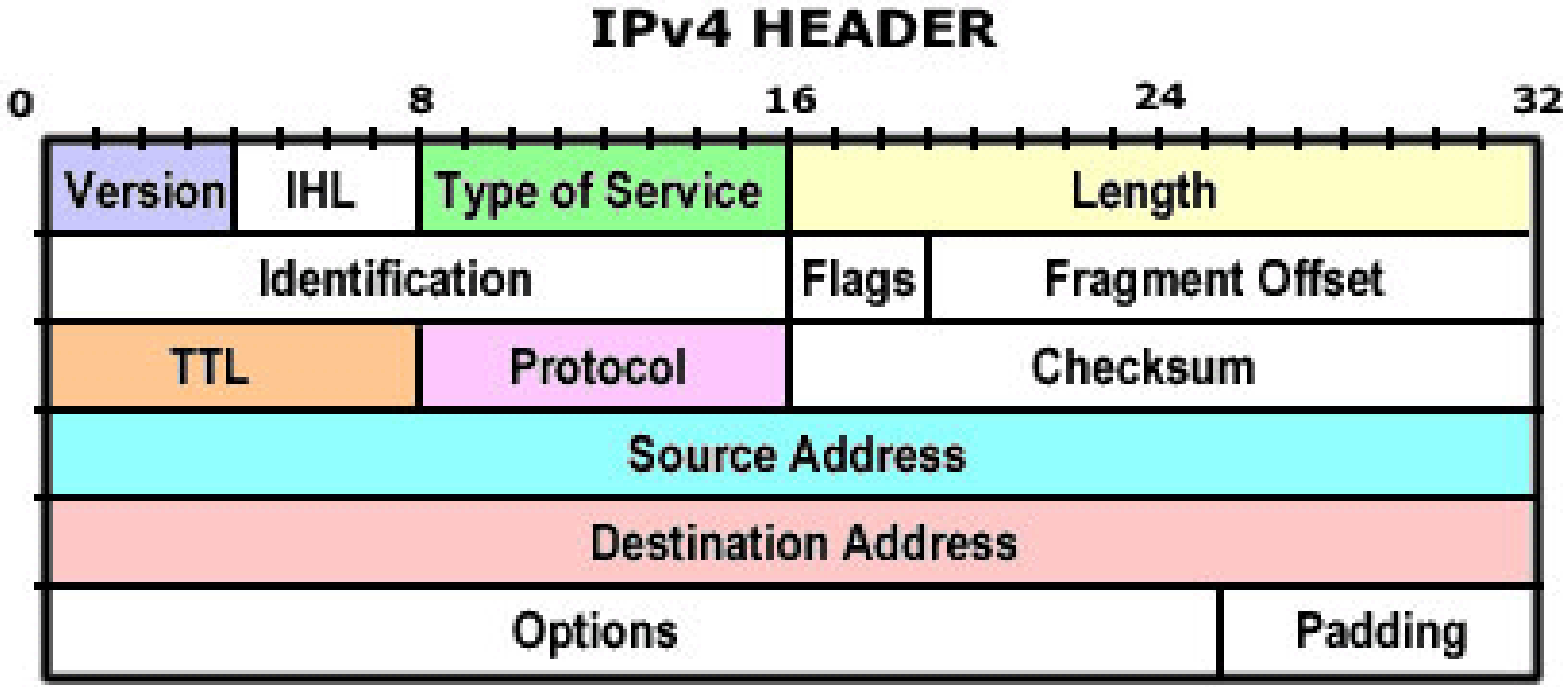
Chapitre 2: Les protocoles de la couche réseau

Réalisé par:

Mayssa Ghribi

Cours Réseaux IP

En-tête de paquet IPv4



En-tête de paquet IPv4

- **Le champ Version:** Il représente le numéro de version du protocole IP (sur 4bits).
- **IHL:** IHL signifie « Internet header length ». Ce champ est codé sur 4 bits et représente la longueur en mots de 32 bits de l'entête IP. Par défaut, il est égal à 5 (20 octets), cependant, avec les options de l'entête IP, il peut être compris entre 6 et 15.

Le fait que le codage soit sur 4 bits, la taille maximum de l'entête IP est donc de 15*32bits/8 = 60 octets.

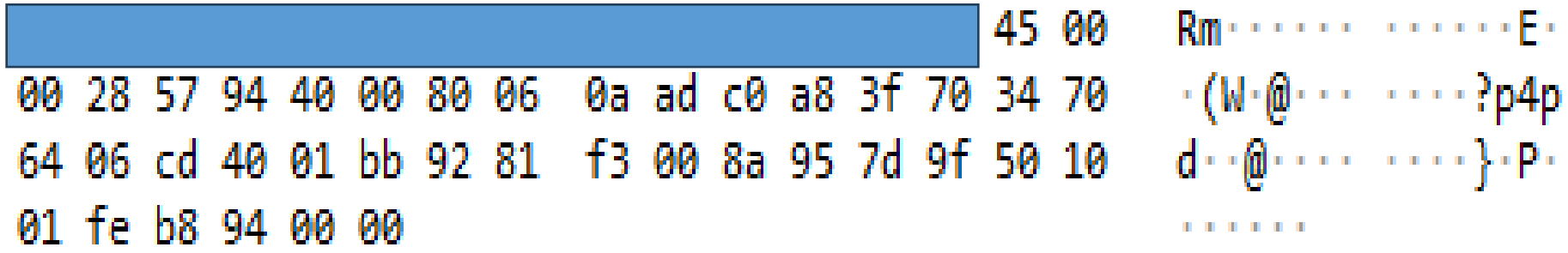
- **Le champs service « Type of Service »** est codé sur 8 bits (priorité du Paquet).
- **Longueur totale:** (16 bits) longueur du paquet incluant l'entête IP et les Data associées.
- **Identification:** (codé sur 16 bits) constitue l'identification utilisée pour reconstituer les différents fragments.

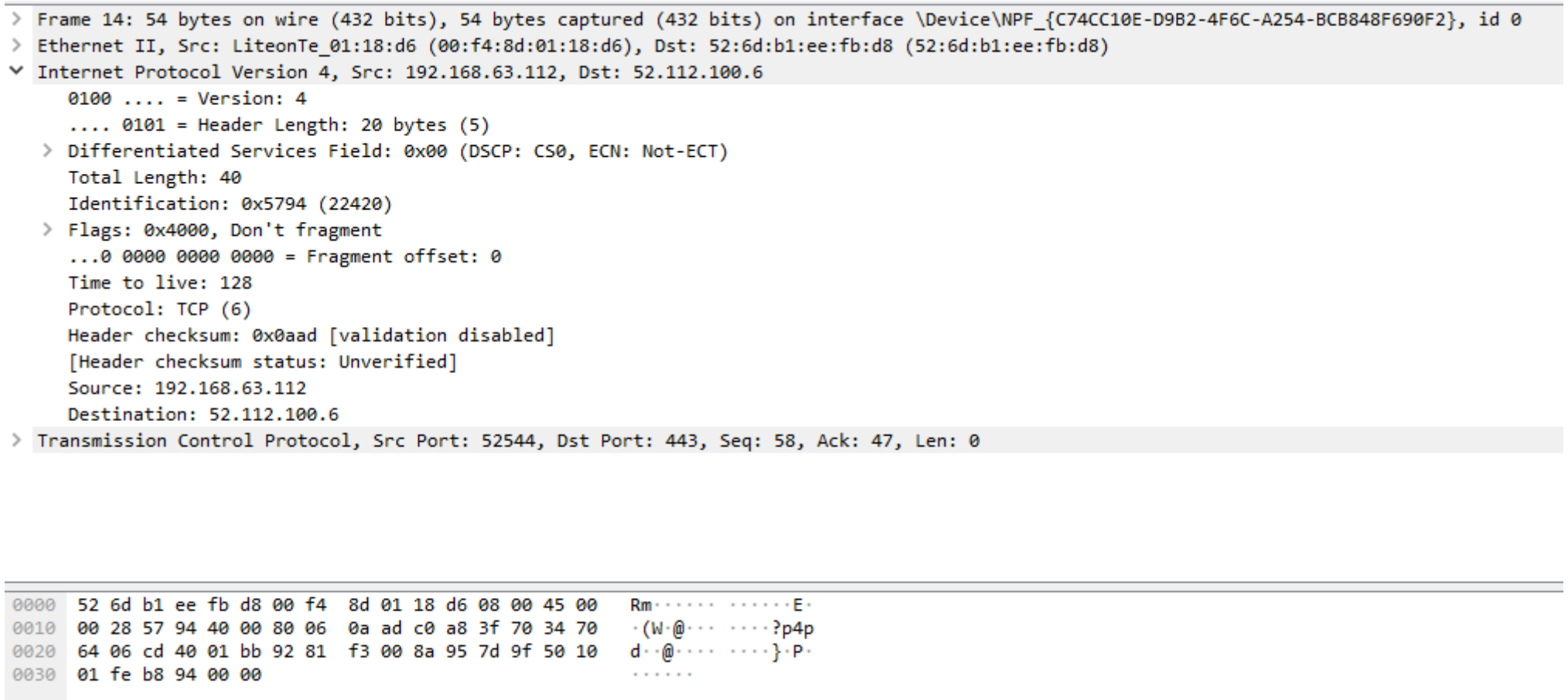
En-tête de paquet IPv4

- **Flags:** Le champ Flags est codé sur 3 bits et indique l'état de la fragmentation
- **Position fragment:** Le champ Position fragment est codé sur 13 bits et indique la position du fragment par rapport à la première trame. Le premier fragment possède donc le champ Position fragment à 0.
- **TTL** (Time To Live) est codé sur 8 bits et indique la durée de vie maximale du paquet. Il représente la durée de vie en nombre de sauts du paquet. Si le TTL arrive à 0, alors l'équipement qui possède le paquet, le détruira.
- **Protocole:** Le champ Protocole est codé sur 8 bits et représente le type de Data qui se trouve derrière l'entête IP. Les valeurs habituelles sont notamment ICMP (1), TCP (6) et UDP (17).
- **Le champ Checksum** est codé sur 16 bits et représente la validité du paquet de la couche 3.
- **Options:** Permet d'ajouter différentes informations optionnelles et rarement utilisées.(0 à 40 octets)

Exercice analyse d'En-tête de paquet IPv4

Analysez l'en-tête IPv4 ci-dessous.




Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C74CC10E-D9B2-4F6C-A254-BCB848F690F2}, id 0
Ethernet II, Src: LiteonTe_01:18:d6 (00:f4:8d:01:18:d6), Dst: 52:6d:b1:ee:fb:d8 (52:6d:b1:ee:fb:d8)
Internet Protocol Version 4, Src: 192.168.63.112, Dst: 52.112.100.6
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5794 (22420)
Flags: 0x4000, Don't fragment
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0aad [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.63.112
Destination: 52.112.100.6
Transmission Control Protocol, Src Port: 52544, Dst Port: 443, Seq: 58, Ack: 47, Len: 0
0000 52 6d b1 ee fb d8 00 f4 8d 01 18 d6 08 00 45 00 Rm E
0010 00 28 57 94 40 00 80 06 0a ad c0 a8 3f 70 34 70 (W@ ?p4p
0020 64 06 cd 40 01 bb 92 81 f3 00 8a 95 7d 9f 50 10 d @ } P
0030 01 fe b8 94 00 00

La fragmentation IP

***Problème:**

- Taille maximale d'un datagramme : 2^{16}= 65535 octet et IP doit s'appuyer sur la couche liaison de données pour la transmission des paquets.
- MTU : On appelle MTU (Maximum Transfer Unit) ou unité de transfert maximale, la taille maximale des données admises dans un réseau en-tête compris. Si la MTU de la liaison ne permet de transporter le paquet entier => fragmentation du paquet.

* **Fonctionnement** :

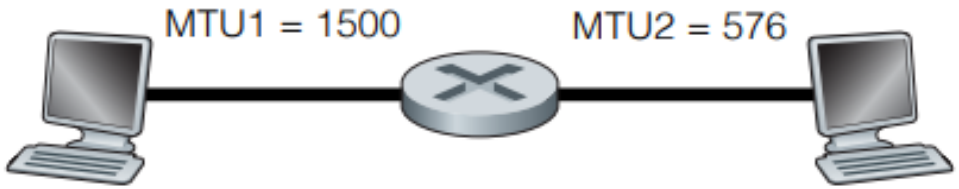
• Lorsqu'un routeur IP réceptionne un datagramme IP il détermine sur quelle interface il va réémettre le datagramme.
• Une fois l'interface identifiée, le routeur détermine le MTU de l'interface.
• Le routeur IP compare le MTU de l'interface avec la taille du datagramme IP.
• Suivant le cas, il va être obligé de fragmenter le datagramme.

La fragmentation d'un datagramme IP est contrôlée par les champs :longueur totale (LEN), offset dans le segment, et le bit MF (More Fragment) du datagramme IP. Le champ offset indique, en multiples de 8 octets, la position du fragment dans le datagramme initial. Le fragment ainsi constitué ne peut avoir, pour longueur, que le multiple de huit le plus proche de la MTU, sauf pour le dernier fragment.

La fragmentation IP

On appelle MTU (Maximum Transfer Unit) ou unité de transfert maximale, la taille maximale des données admises dans un réseau en-tête compris.

- Flags : 3 bits (Réservé : 0, DF, MF)
  - DF : Don't Fragment (les paquets trop grands sont rejetés)
  - MF : More Fragment (positionné si dernier fragment)
- Fragment Offset :
  - taille en octets hors entête des fragments précédant le fragment courant divisée par 8

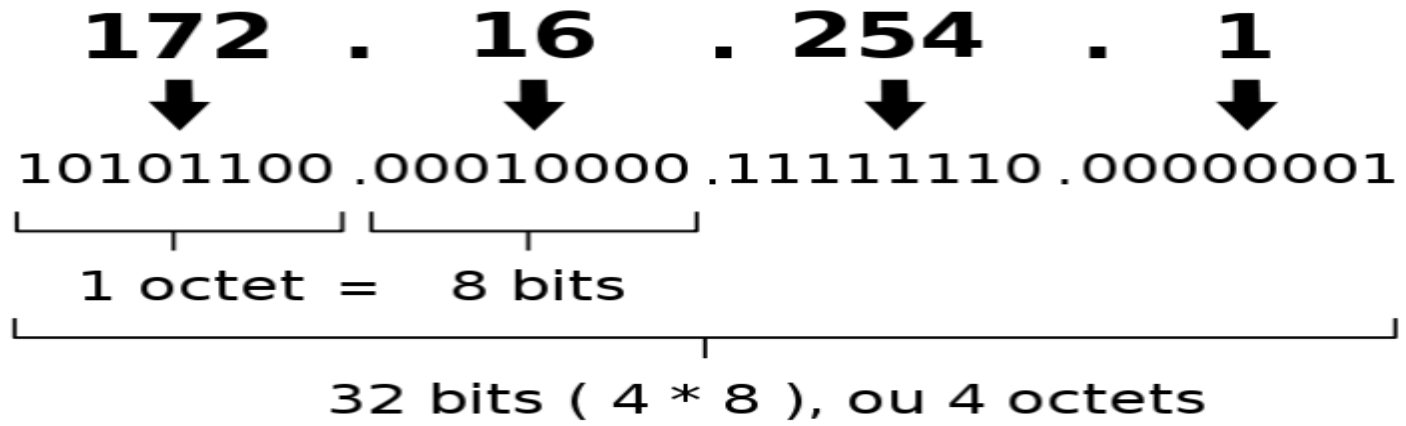


- Exemple :
  - Données encapsulées : 1300 octets
  - Entêtes des fragments sur le réseau 2 :
    - 576 - 20 = 556, valeur multiple de 8 la plus proche : 552 = 69 * 8
    - F1 : offset 0 MF = 1 (taille des données : 552 octets)
    - F2 : offset 69 = 552/8 MF = 1 (taille des données : 552 octets)
    - F3 : offset 69*2 MF = 0 (taille des données : 196 octets)

Adresse IPv4

Une adresse 32 bits notée sous forme de 4 nombres décimaux séparés par des points. On distingue en fait deux parties dans l'adresse IP :

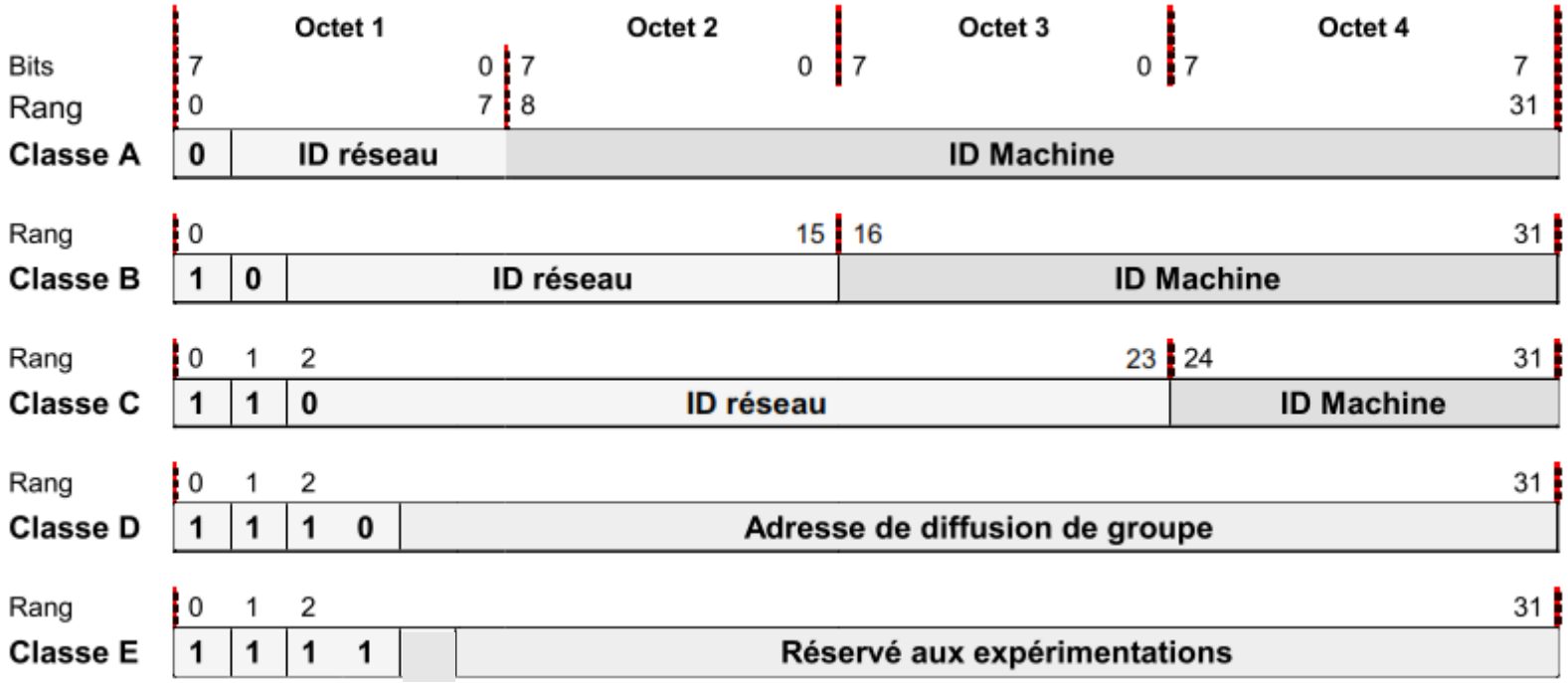
- Une partie désignant le réseau (on l'appelle netID)
- Une partie désignant les hôtes (on l'appelle host-ID)



Les hôtes situés sur un réseau ne peuvent communiquer qu'avec des hôtes situés sur le même réseau, même si des stations se trouvent sur le même segment. C'est ce même numéro qui permet au routeur d'acheminer le paquet au destinataire.

Classe d'adresses IPv4

• Les adresses IP sont réparties en cinq classes, en fonction des bits qui les composent. Les premiers bits du champ adresse réseau(ID réseau ou Net_ID) (On appelle « Bits de poids fort », les premiers bits de l'octet le plus à gauche) permettent de distinguer la classe d'adressage.



Masque de sous réseau

Chaque hôte d'un réseau TCP/IP nécessite **un masque de sous-réseau**. Un masque de sous-réseau est une adresse 32 bits utilisée pour bloquer ou « masquer » une partie de l'adresse IP afin de distinguer l'ID de réseau à partir de l'ID d'hôte. Chaque hôte d'un réseau TCP/IP nécessite un masque de sous-réseau. Il peut s'agir d'un masque de sous-réseau par défaut, utilisé lorsque le réseau n'est pas divisé en sous-réseaux, ou d'un masque de sous-réseau personnalisé, utilisé lorsqu'un réseau est divisé en sous-réseaux.

Il existe deux méthodes d'écriture des masques de sous-réseaux, qui sont équivalentes :
–réseau :192.168.10.0, masque par défaut 255.255.255.0 ;

–ou plus simplement 192.168.10.0/24, (nommée la notation CIDR) le préfixe 24 indique la longueur en bits du masque de sous réseau (longueur du préfixe réseau ou simplement préfixe).(Nombre de bits qui identifie la partie réseau càd le nombre de bits à 1 dans le masque)

Classe d'adresses IPv4

Classe	Bits de poids fort	Plage d'adresses	Plage d'adresses valides	Masque par défaut	Préfixe de réseau CIDR	Nombre d'hôtes/machines
A	0	0.0.0.0 - 127.255.255.255	1.0.0.1 -126.255.255.254	255.0.0.0	/8	$2^{24} - 2$
B	10	128.0.0.0-191.255.255.255	128.0.0.1-191.255.255.254	255.255.0.0	/16	$2^{16} - 2$
C	110	192.0.0.0-223.255.255.255	192.0.0.1- 223.255.255.254	255.255.255.0	/24	$2^{8} - 2$
D	1110	224.0.0.0 -239.255.255.255	-	Non défini	-	-
E	1111	240.0.0.0- 255.255.255.255	-	Non défini	-	-

- Toutes machines d'un réseau IP est identifié par le couple <Net_ID><Host_ID>. Certaines valeurs de ces champs ont une signification particulière. C'est ainsi que l'adresse <Net_ID> <0>, où tous les bits du champ Host_ID sont à zéro, désigne le réseau lui-même.
  - Les adresses de la classe D sont utilisées pour la diffusion (Multicast) vers les machines d'un même groupe. (Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local.)
  - Les adresses de la classe E sont réservées aux expérimentations.

⟶ Plage d'adresses valides c.à.d. les adresses qui peuvent être attribuées à des hôtes

Les adresses spéciales

Adresses réseau et de diffusion

La première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de l'adresse réseau et de l'adresse de diffusion.

Route par défaut

La route IPv4 par défaut est représentée de la manière suivante : 0.0.0.0.
La route par défaut est utilisée comme route « dernier recours » lorsqu'aucune route plus spécifique n'est disponible. L'utilisation de cette adresse réserve également toutes les adresses de la plage 0.0.0.0 - 0.255.255.255

Bouclage

Le réseau 127.0.0.0 (les adresses de la plage 127.0.0.0-127.255.255.255) est réservé pour les tests de boucle locale avec notamment l'adresse IP 127.0.0.1 qui est l'adresse « localhost » c'est-à-dire de boucle locale de votre PC. (cette adresse dite de boucle locale (loopback ou encore localhost). Un ping vers 127.0.0.1 a pour effet de pinguer la machine elle-même. Si une réponse est reçue, cela signifie que TCP/IP est activé sur la machine.

Adresses TEST-NET

Le bloc 192.0.2.0/24 (192.0.2.0 à 192.0.2.255) est dédié aux adresses « TEST-NET » utilisé à des fins d'enseignement ou de documentation. Ces adresses ne doivent pas apparaitre sur le réseau public internet.

Les adresses privées

L'IANA (Internet Assigned Numbers Authority) a réservé trois blocs d'adresses IPv4 pour permettre aux sociétés de les utiliser sur leurs réseaux privés (réseau local).
L'adresse IP Privée est une adresse qui ne fonctionne pas sur Internet et fonctionne uniquement sur les réseaux privés. L'unicité d'adresse privée au plan mondial n'est pas nécessaire alors que par opposition à une adresse publique qui doit être unique au niveau mondial.

Classe **A**: 10.0.0.0 à 10.255.255.255
Classe **B**: 172.16.0.0 à 172.31.255.255
Classe **C**: 192.168.0.0 à 192.168.255.255

Adresses de liaison locale (Link local) ou adresses APIPA (Automatic Private IP Addressing)

Un ordinateur configuré pour utiliser un serveur DHCP peut automatiquement s'attribuer une adresse IP si ce serveur n'est pas disponible. Cela peut se produire par exemple sur un réseau local sans serveur DHCP ou sur un réseau avec un serveur DHCP arrêté temporairement pour maintenance.

La plage d'adresses APIPA (*Automatic Private Internet Protocol Addressing*) est la plage allant de **169.254.0.0 à 169.254.255.255**.

Les plages d'adresses APIPA ne sont pas routables sur Internet et sont exclusivement dédiées à des communications locales.

Attribution des adresses IP

L'IANA (Internet Assigned Numbers Authority) gère l'attribution des adresses IPv4 et IPv6 Jusqu'au milieu des années 1990. À cette époque, la gestion de l'espace d'adressage IPv4 restant était répartie entre différents autres registres, selon le type d'utilisation ou la zone géographique. Ces sociétés d'enregistrement s'appellent des registres Internet régionaux (RIR: Regional Internet registry)

Voici les principaux registres :

- **AfriNIC** (African Network Information Centre) - Région Afrique
- **APNIC** (Asia Pacific Network Information Centre) - Région Asie/Pacifique
- **ARIN** (American Registry for Internet Numbers) - Région Amérique du Nord
- **LACNIC** (Regional Latin-American and Caribbean IP Address Registry) - Amérique du Sud et certaines îles des Caraïbes
- **RIPE NCC** (Réseaux IP européens) - Europe, Moyen Orient, Asie centrale

Les RIR sont chargés d'attribuer des adresses IP aux FAI. La plupart des entreprises ou organisations obtiennent leur bloc d'adresses IPv4 auprès d'un FAI.

Méthode par calcul binaire

L'adresse du réseau, l'adresse de Broadcast et la plage d'adresses utilisables peuvent être obtenues à partir d'un calcul booléen de type ET ou la conjonction logique (une proposition est vraie lorsque les deux termes sont tous les deux vrais) :

Obtenir l'adresse du réseau :

Pour l'adresse IP 140.159.125.25 , adresse de classe B à laquelle on applique un masque par défaut de

10001100.10011111.01111101.00011001	140.159.125.25
11111111.11111111.00000000.00000000	255.255.0.0
---	---
10001100.10011111.00000000.00000000	140.159.0.0

L'adresse du réseau est donc 140.159.0.0. Elle est la première adresse de la plage.

Méthode par calcul binaire

Obtenir l'adresse de Broadcast :

On va remplacer les bits de valeur 0 de la partie hôte du résultat obtenu pour l'adresse de réseau par des bits de valeur 1, soit les deux derniers octets maximisés :

10001100.10011111.00000000.00000000 140.159.0.0

par :

10001100.10011111.11111111.11111111 140.159.255.255

Obtenir la plage d'adresses utilisables de ce réseau :

La plage d'adresse du réseau sera comprise entre la première adresse utilisable et la dernière utilisable, autrement dit, celle qui suit l'adresse du réseau et celle qui précède l'adresse de Broadcast :

De 10001100.10011111.00000000.00000001 140.159.0.1

à 10001100.10011111.11111111.11111110 140.159.255.254

Sous-réseaux (subneting)

- Afin d'augmenter les capacités de gestion de trafic dans un réseau, il est possible de subdiviser ce dernier en plusieurs sous réseaux afin de permettre une segmentation des domaines de broadcast. (Dans l'école par exemple, on trouve SR département informatique, administration, bloc de recherche, etc.)

- En segmentant un réseau en plusieurs domaines de diffusion, on limite naturellement la propagation de code malveillant. Le subnetting devient alors un élément de la panoplie des outils de sécurité.

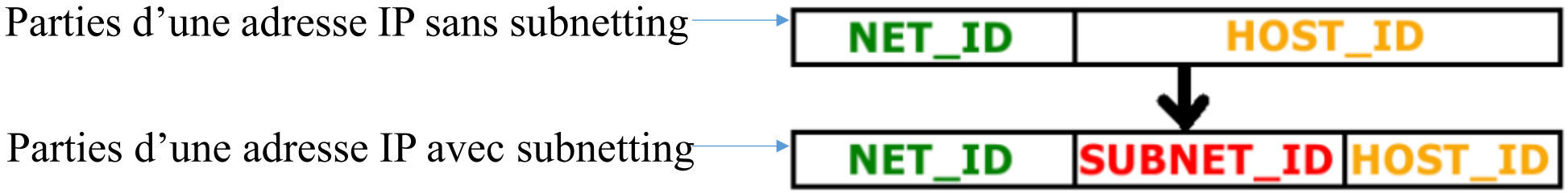
- Le processus qui consiste à diviser une plage d'adresses en espaces plus petits est appelé segmentation en sous-réseaux.

- Les administrateurs réseau peuvent regrouper les appareils dans des sous-réseaux en fonction de leur emplacement, de leur type ou de l'unité organisationnelle.

Sous-réseaux (subneting)

- Pour cela, on emprunte à la partie hôte des bits que l'on désigne comme champ de sous réseaux.

- Autrement dit, pour segmenter un réseau en sous-réseaux, il faut alors décomposer la partie hostid de l'adresse IP en deux parties : une adresse de sous-réseau (subnetid) et une adresse machine (hostid).



1. Méthode classique (RFC 1878) (Règle de 2^n)

Cette méthode se détaille en 5 étapes :

- Empruntez le nombre de bits suffisants
- Calculez le nouveau masque de sous réseau
- Identifiez les différentes plages d'adresses IP
- Identifiez les adresses de réseau et de broadcast pour chaque plage
- Déterminez les plages d'adresses utilisables pour les hôtes.

1. Méthode classique

1.1 Empruntez le nombre de bits suffisants

Calculer les sous-réseaux: Règle de 2^n

- Utilisez la formule suivante pour calculer le nombre de sous-réseaux :

2^n (où n = le nombre de bits empruntés de la partie hôte)

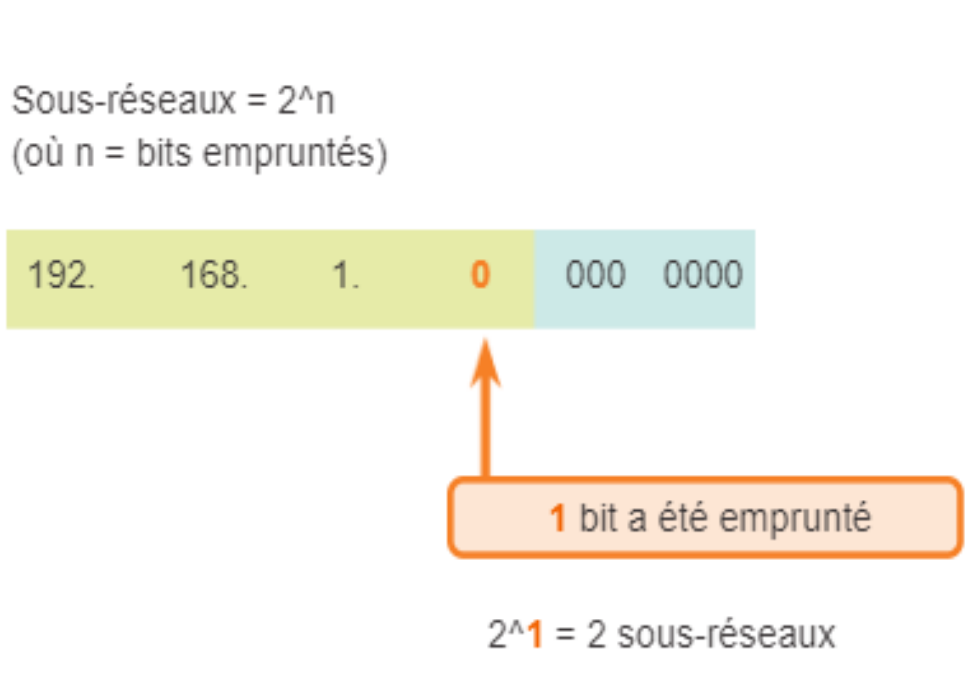
- Par exemple pour créer de 2 sous-réseaux, il faudra :

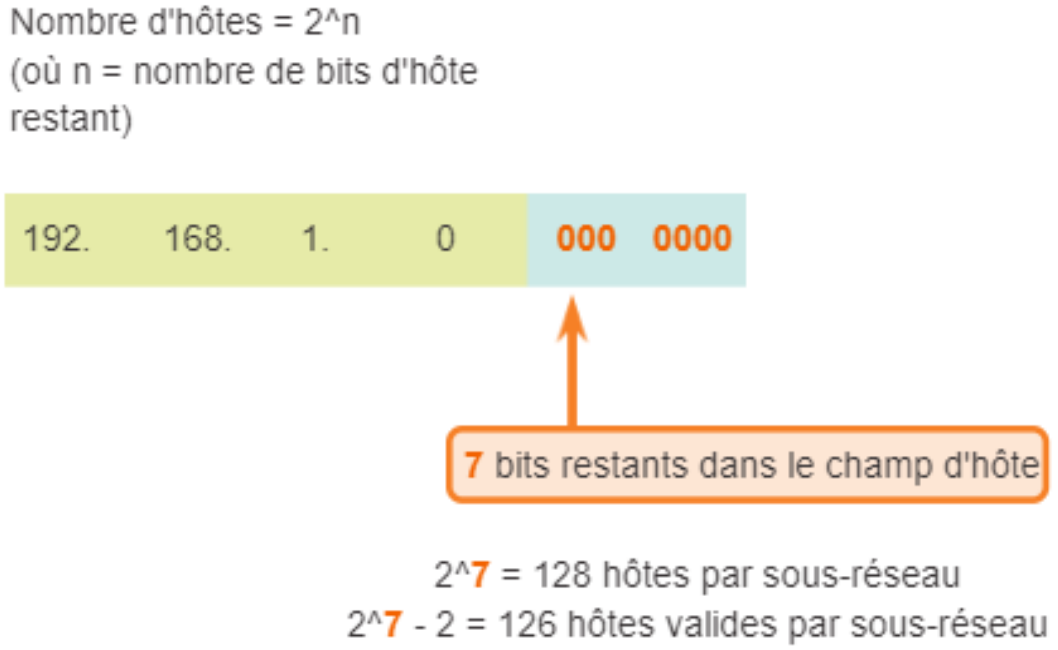
$2^1 = 2$ sous-réseaux => On doit donc emprunter un bit de la partie hôte pour créer deux sous réseaux.

1. Méthode classique

1.1 Empruntez le nombre de bits suffisants

Comme l'illustre la Figure 1, pour l'exemple de 192.168.1.0, le calcul est le suivant (il faut noter que l'adresse 192.168.1.0 est une adresse de classe C c.à.d. on utilise 8 bits pour identifier la partie hôte)





1. Méthode classique

- **Calculez le nouveau masque de sous réseau (subnetmask)**

Le masque de départ change (c.à.d. le masque par défaut 255.255.255.0 ou /24) et doit maintenant englober la partie netid et la partie subnetid. Ce nouveau masque se nomme masque de sous-réseaux.

Pour l'exemple de 192.168.1.0 découpé en deux sous réseaux, le masque de sous-réseau sera:

(netid = 24 bits) + (subnetid = 1 bit) = 25 bits à 1 soit 255.255.255.128 ou /25

1. Méthode classique

- **Identifiez les différentes plages d'adresses**

A l'aide du masque de sous réseau on calcule les différentes plages d'adresses possibles. Pour cela il suffit d'écrire chaque possibilité binaire sur les bits que l'on a empruntés pour la création des sous réseaux.

- **Identifiez les plages de réseau et de broadcast**

Des plages d'adresses qui restent, on retire aussi les premières et dernières adresses. La première servira d'adresse réseau pour la plage d'adresse. La dernière servira d'adresse de broadcast pour la plage spécifiée.

1. Méthode classique

- **Déterminez les plages d'adresses Hôtes**

Maintenant qu'il ne nous reste plus que les plages d'adresses utilisables, on a donc les plages d'adresses IP utilisables par les hôtes pour communiquer sur le sous réseau.

Le nombre de machines adressables dans chaque sous-réseau sera de $2^{\text{nb bits hostid}} - 2$ adresses interdites

Exercice 1: adressage

- Appliquer la méthode de calcul classique pour créer 4 sous-réseaux avec l'adresse 192.168.1.0 :

- pour créer 4 sous-réseaux, il faut emprunter 2 bits de la partie hostid et on obtient donc $2^2 = 4$ sous-réseaux : on a donc 4 possibilités de combinaisons:

  0 0 pour le sous-réseaux n°0 - 1 0 pour le sous-réseaux n°2

  0 1 pour le sous-réseaux n°1 - 1 1 pour le sous-réseaux n°3

Exercice 1: adressage

0 0 pour le sous-réseaux n°0 - 1 0 pour le sous-réseaux n°2

0 1 pour le sous-réseaux n°1 - 1 1 pour le sous-réseaux n°3

- Les adresses de différentes sous réseaux (SR) sont alors:

SR 0 : 192.168.1.0 = 11000000.10101000.00000001.00000000

SR 1 : 11000000.10101000.00000001.01000000 = 192.168.1.64

SR 2 : 11000000.10101000.00000001.10000000 = 192.168.1.128

SR 3 : 11000000.10101000.00000001.11000000 = 192.168.1.192

Exercice 1: adressage

Masque de sous-réseaux (subnetmask)

Pour le réseau 192.168.1.0/24 découpé en 4 sous-réseaux

- netid = 24 bits
- subnetid = 2 bits
- hostid = 32 - 24 - 2 = 6 bits

Le masque de sous-réseau sera : 24 + 2 = 26 bits à 1 soit 255.255.255.192

Plage d'adresses des sous-réseaux

Le nombre de machines adressables dans chaque sous-réseau sera de:

$$2^{\text{nb bits hostid}} - 2 = 2^6 - 2 = 62\ adresses$$

Exercice 1: adressage

N° SR	Sous réseau	Adresse début	Adresse fin	Adresse de diffusion
0	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193	192.168.1.254	192.168.1.255