USTHB-Info |2024

COURS
INTRODUCTION AUX RÉSEAUX INFORMATIQUE

Par
Dr. k. CHAOUI

PLAN

I. Introduction aux réseaux

II. Couche physique

III. Couche Liaison de données

IV. Couche réseau

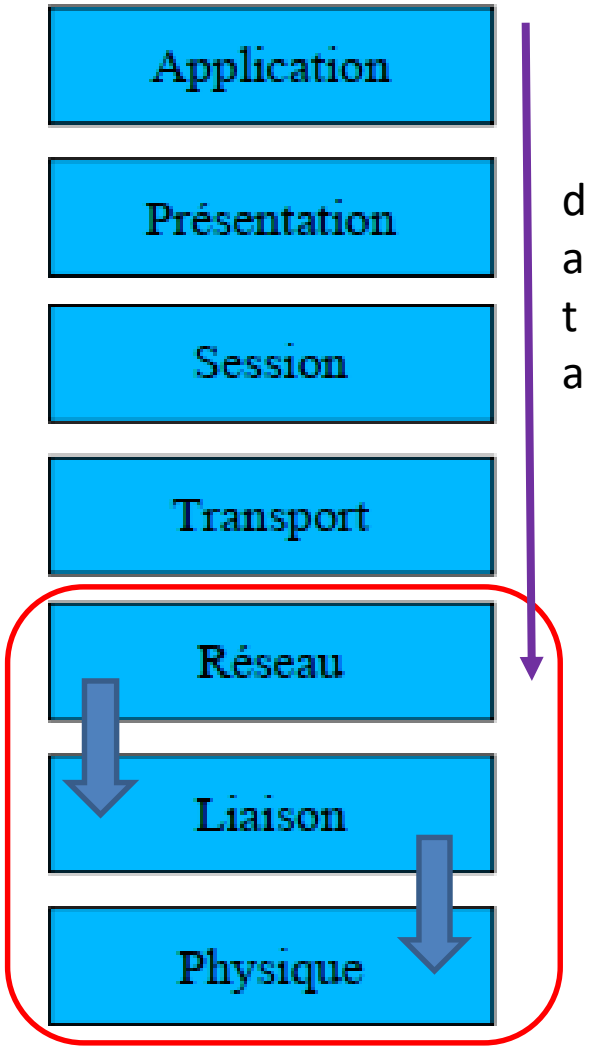
V. Couche transport

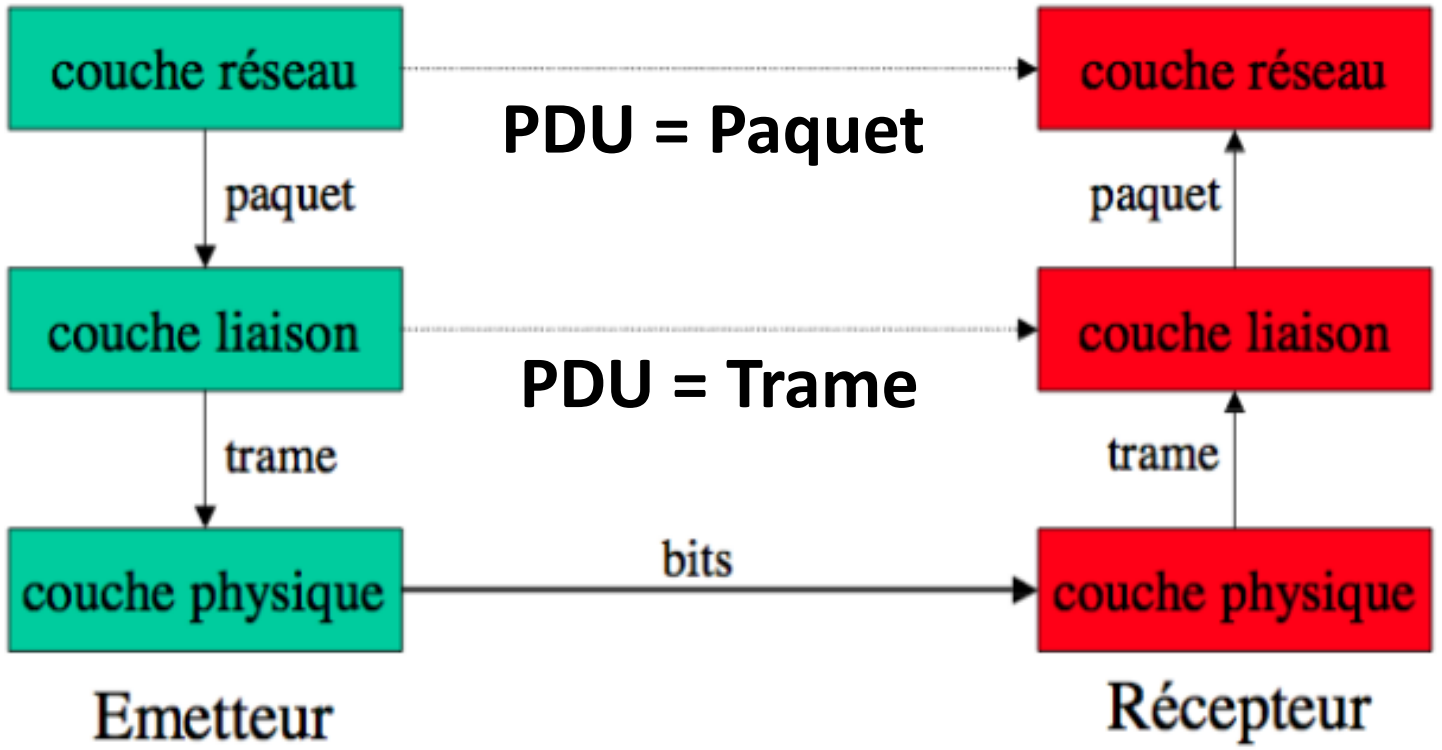
VI. Couche application

CHAPITRE IV

Couche réseau

MODE DE FONCTIONNEMENT DANS LE MODÈLE EN COUCHES





- Le rôle principal de la couche réseau est de :

-Transporter des paquets de la source vers la destination via les différentes nœuds de commutation du réseaux traversés

-Trouver un chemin tout en assurant une régulation et répartition de la charge des réseaux

Ce rôle est assuré par un ensemble de fonctions :

- Fragmentation et réassemblage
- Adressage et routage

PROTOCOLES DE LA COUCHE RÉSEAU

IP - Internet Protocol
ARP - Address Resolution Protocol
ICMP - Internet Control Message Protocol

Dans un réseau les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses logique, appelées adresses IP. Ainsi chaque ordinateur du réseau possède une adresse IP unique sur ce réseau : c'est l'adressage IP.

NB. **@MAC** adressage physique pour identifier un périphérique unique au monde
@IP adressage logique pour identifier un périphérique sur un réseau

1. L’adressage IP

1.1 Définition d’une adresse IP

- Chaque ordinateur, d’un même réseau, doit dispose d'une adresse IP unique (codée sur 32bits pour IPv4).
- Une adresse IP est représentée dans une notation décimale pointée, constituée de 4 nombres compris chacun entre 0 et 255 et séparés par un point.:

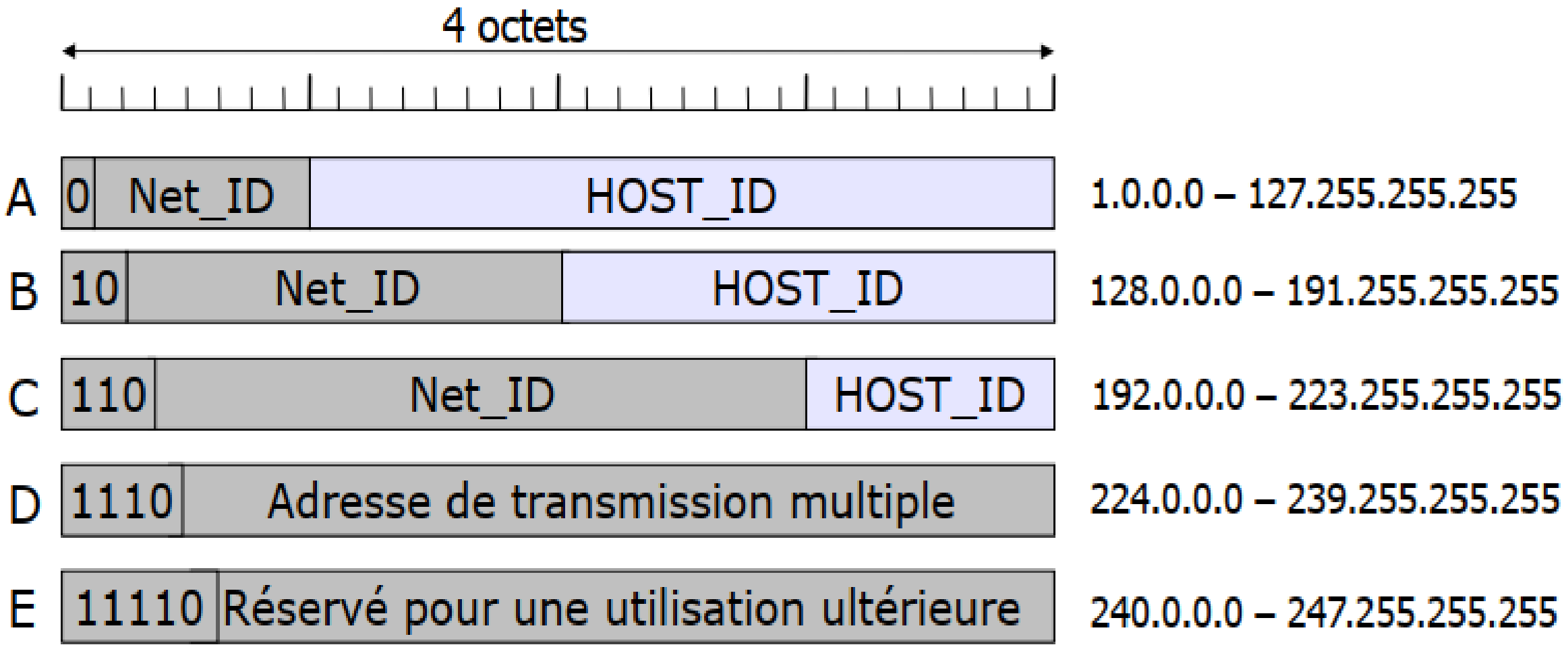
197 . 75 . 200 . 22

11000101. 01001011. 11001000. 00010110

- Une adresse IP se décompose en :
  - **Partie réseau:** située à l'extrême gauche de l'adresse qui indique le réseau dont l'adresse IP est membre. Tous les périphériques du même réseau ont, dans leur adresse IP, la même partie réseau
  - **Partie machine:** représente la partie restante de l'adresse qui identifie un appareil spécifique sur le réseau. Cette partie est unique pour chaque appareil ou interface sur le réseau.

- Initialement, 5 classes d'adresse (*A*, *B*, *C, D* et *E*) ont été définies qui instaurent une certaine hiérarchie. Une adresse IP appartient à une classe donnée selon la valeur de son premier octet.

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques	adresses uniques


4 octets
A
0
Net_ID
HOST_ID
1.0.0.0 – 127.255.255.255
B
10
Net_ID
HOST_ID
128.0.0.0 – 191.255.255.255
C
110
Net_ID
HOST_ID
192.0.0.0 – 223.255.255.255
D
1110
Adresse de transmission multiple
224.0.0.0 – 239.255.255.255
E
11110
Réservé pour une utilisation ultérieure
240.0.0.0 – 247.255.255.255

- *Si le premier bit est 0,* l'adresse est de *classe A*. On dispose de 7 bits pour identifier le réseau et de 24 bits pour identifier l'hôte. On a donc les réseaux de 1 à 127 et 224 hôtes possibles, c'est à dire 16 777 216 machines différentes (de 0 à 16 777 215).
- *Si les deux premiers bits sont 10,* l'adresse est de *classe B*. Il reste 14 bits pour identifier le réseau et 16 bits pour identifier la machine. Ce qui fait 2^{14} = 16 384 réseaux (128.0 à 191.255) et 65 534 (65 536 − 2) machines.
- *Si les trois premiers bits sont 110,* l'adresse est de *classe C*. Il reste 21 bits pour identifier le réseau et 8 bits pour identifier la machine. Ce qui fait 2^{21} = 2 097 152 réseaux (de 192.0.0 à 223.255.255) et 254 (256−2) machines.
- *Si les quatre premiers bits de l'adresse sont 1110*, il s'agit d'une classe d'adressage spéciale, la *classe D*. Cette classe est prévue pour faire du "multicast ", ou multipoint. (RFC 1112 [S. Deering, 1989]), contrairement aux trois premières classes qui sont dédiées à l'unicast ou point à point.
- *Si les quatre premiers bits de l'adresse sont 1111*, il s'agit d'une classe expérimentale, la *classe E*. La RFC 1700 précise "*Class E addresses are reserved for future use*".

1.2 Adresses particulières

- *<id. de réseau nul>.<id. de machine>* est utilisée pour désigner une machine sur son réseau lors d'un boot (processus d'amorçage). 0.0.0.0 est aussi utilisée par une machine pour connaître sa propre adresse IP lors d'un processus d'amorçage par exemple.
- *<id. de réseau>.<id. de machine nul>* permet de désigner le réseau lui-même.
- *<id. de réseau>.<id. de machine avec tous ses bits à 1>* est une adresse de *diffusion* ou de *broadcasting*, c'est-à-dire qu'elle désigne toutes les machines du réseau identifié. Un datagramme adressé à cette adresse sera ainsi envoyé à toutes les machines du réseau *<id. de réseau>*.
- *255.255.255.255* est une adresse de diffusion locale, car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. L'avantage par rapport à l'adresse précédente est que l'émetteur n'est pas obligé de connaître l'adresse du réseau auquel il appartient.
- *127.0.0.0* est un réseau d'adresses de bouclage qui est utilisée pour permettre les communications interprocessus sur un même ordinateur ou réaliser des tests de logiciels, car tout logiciel de communication recevant des données pour ces adresses les retourne simplement à l'émetteur.

- Les adresses de classe *A* de 10.0.0.0 à 10.255.255.255, de classe *B* de 172.16.0.0 à 172.31.255.255 et de classe *C* de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux locaux privés (*Intranet).*
- On les appelle les *adresses privées*, à l'inverse des *adresses publiques* qui sont celles utilisées pour identifier les machines sur Internet.
- Un *Intranet* est un réseau d'étendue géographique très limitée, par exemple pour une entreprise, basé sur la technologie TCP/IP mais non relié à Internet. Un *Extranet* est également un réseau privé bâti sur TCP/IP, non connecté à Internet, mais réparti sur des sites géographiques distants.
- Les adresses de réseaux publique d'Internet sont affectées par un organisme international: *ICANN (Internet Corporation for Assigned Names and Numbers)*.

1.3 Types des adresses

Il existe différentes types adresses

- ***Unicast*** : l'adresse IP est associée à un seul hôte ;
- ***Multicast*** : l'adresse IP est associée à un groupe de machine, n'importe quel machine peut faire partie du groupe, il n'y a pas d'authentification ;
- ***Broadcast*** : tous les hôtes d'un même sous-réseau recevrons le message ;
- ***Anycast*** : technique de routage qui consiste à envoyer les données à la machine la plus proche du client.

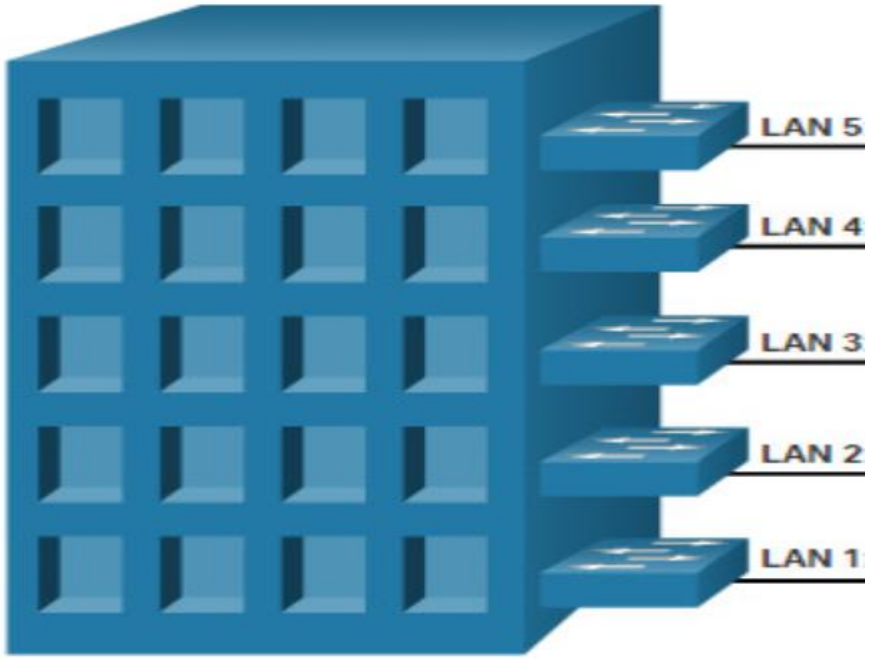
1.4 Adressage des sous réseaux

- Le système des adresses IP permet également la définition d'adresses de sous-réseaux en découpant *la partie <ID machine>* en deux parties :
  - Un *identificateur* de sous-réseau : Nombre de bits nécessaire pour identifier tous les sous réseaux
  - Un identificateur machine : Le reste de bits pour identifier toutes les machines de chaque sous réseau
  - **Exemple :** Un réseau de classe *B*, sur lequel on pourrait nommer 65 534 machines pourra être décomposé en 254 sous-réseaux de 254 machines comme suit :
- ***<id. de réseau sur 16 bits>. <id. de sous-réseau sur 8 bits>. <id. de machine sur 8 bits>***
- L'administrateur d'un réseau peut décider de découper où il veut la zone des identificateurs de machines, ce découpage facilite le travail des routeurs. Cette technique a pour effet de provoquer un routage hiérarchique.

1.5 Le masque de sous réseau

- Pour permettre au routeur de faire la séparation entre la partie réseau et la partie machine de l'adresse IP, on introduit la *masque de sous réseaux.*
- **Adresse machine AND Masque de réseau = Adresse du réseau de destination**

2. Segmentation de réseaux



La base de la segmentation

l'utilisation de bits hôtes pour créer des sous-réseaux supplémentaires

2.1 Découpage statique (FLSM)

- Pour créer des sous-réseaux IPv4, on utilise un ou plusieurs bits d'hôte en tant que bits réseau. Pour cela, il convient de développer le masque pour emprunter quelques bits de la partie hôte de l'adresse et créer d'autres bits réseau

- Pour chaque **N** bit emprunté, nous avons 2^N sous-réseaux

- Par exemple, si vous empruntez 1 bit, vous pouvez créer 2 sous-réseaux. Si vous empruntez 2 bits, 4 sous-réseaux sont créés, si vous empruntez 3 bits, 8 sous-réseaux sont créés et ainsi de suite.

- Toutefois, pour chaque bit emprunté, le nombre d'adresses disponibles par sous-réseau décroît.

- Les bits peuvent être empruntés uniquement dans la partie hôte de l'adresse. La partie réseau de l'adresse est attribuée par le fournisseur d'accès et ne peut pas être modifiée.

Exemple

192.168.1.0/24

Sans les bits d'hôte empruntés, la partie hôte de l'adresse réseau et du masque ne contient que les bits 0.

Empruntez 1 bit à la partie hôte de l'adresse.

Trame	192.	168.	1.	0	000	0000	1 Réseau
Masque	255.	255.	255.	0	000	0000	

La valeur du bit emprunté est **0** pour l'adresse du réseau 0.

Réseau 0	192.	168.	1.	0	000	0000	2 sous-réseaux

La valeur du bit emprunté est **1** pour l'adresse du réseau 1.

Réseau 1	192.	168.	1.	1	000	0000	

Les nouveaux sous-réseaux ont le **MÊME** masque de sous-réseau.

Masque	255.	255.	255.	1	000	0000

Représentation décimale

Trame	192.	168.	1.	0	000	0000	Réseau : 192.168.1.0/24
Masque	255.	255.	255.	0	000	0000	Masque : 255.255.255.0

L'emprunt de 1 bit entraîne la création de 2 sous-réseaux utilisant le même masque.

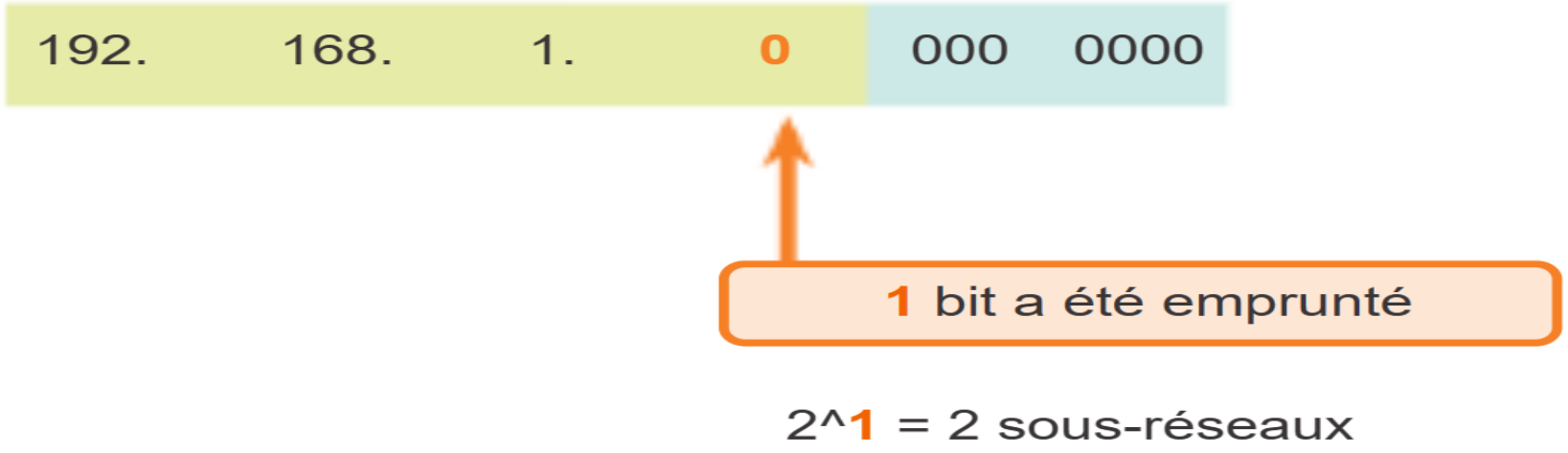
Réseau 0	192.	168.	1.	0	000	0000	Réseau : 192.168.1.**0**/**25**
Masque	255.	255.	255.	1	000	0000	Masque : 255.255.255.**128**
Réseau 1	192.	168.	1.	1	000	0000	Réseau : 192.168.1.**128**/**25**
Masque	255.	255.	255.	1	000	0000	Masque : 255.255.255.**128**

Calculer les sous-réseaux

Utilisez la formule suivante pour calculer le nombre de sous-réseaux :
2^n (où n = le nombre de bits empruntés)

Exemple

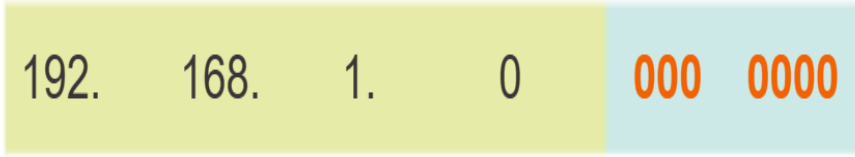
Sous-réseaux = 2^n
(où n = bits empruntés)



Calculer les hôtes

2^n-2 (où n = le nombre de bits restants dans le champ d'hôte)

Nombre d'hôtes = 2^n
(où n = nombre de bits d'hôte restant)

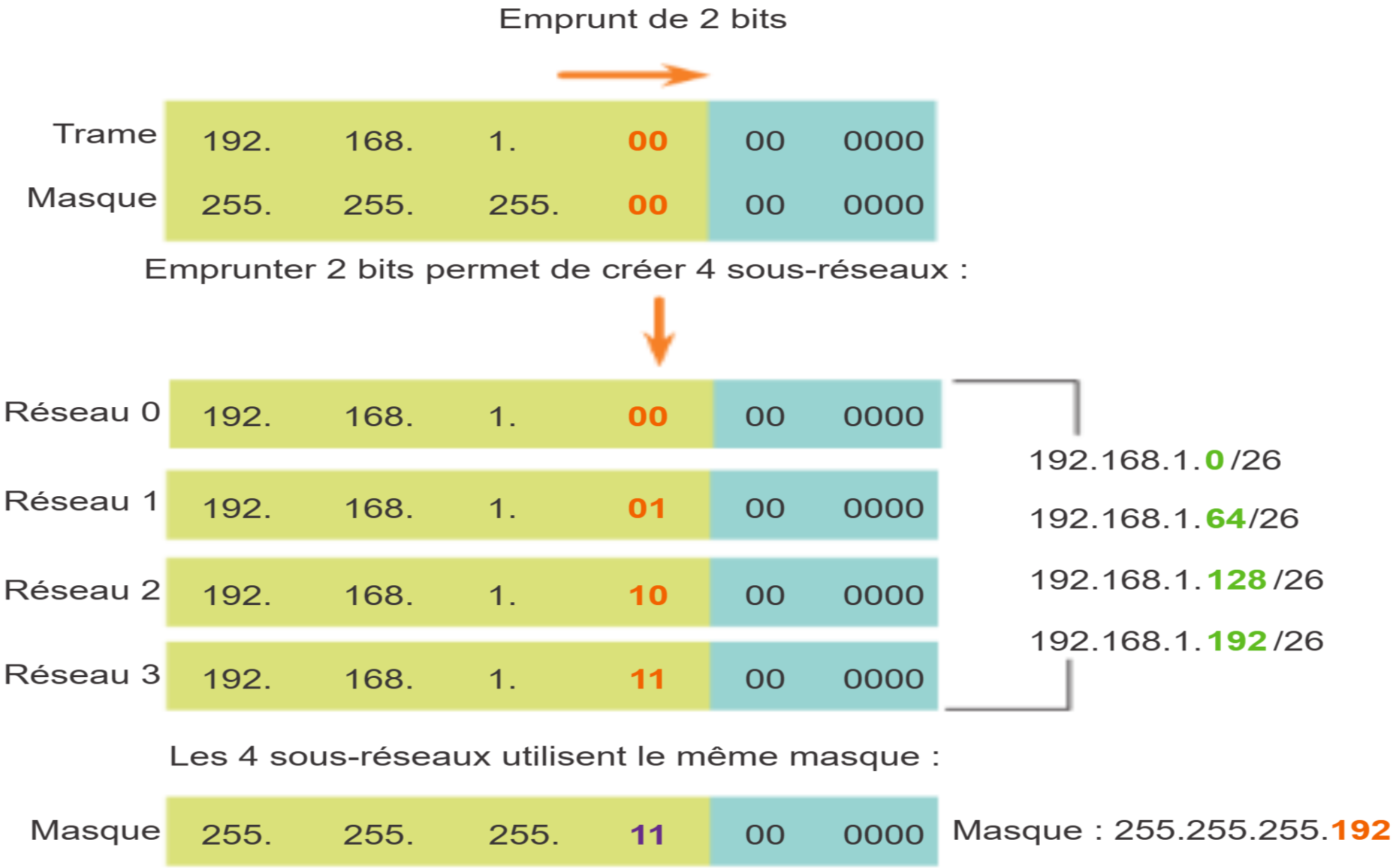


7 bits restants dans le champ d'hôte

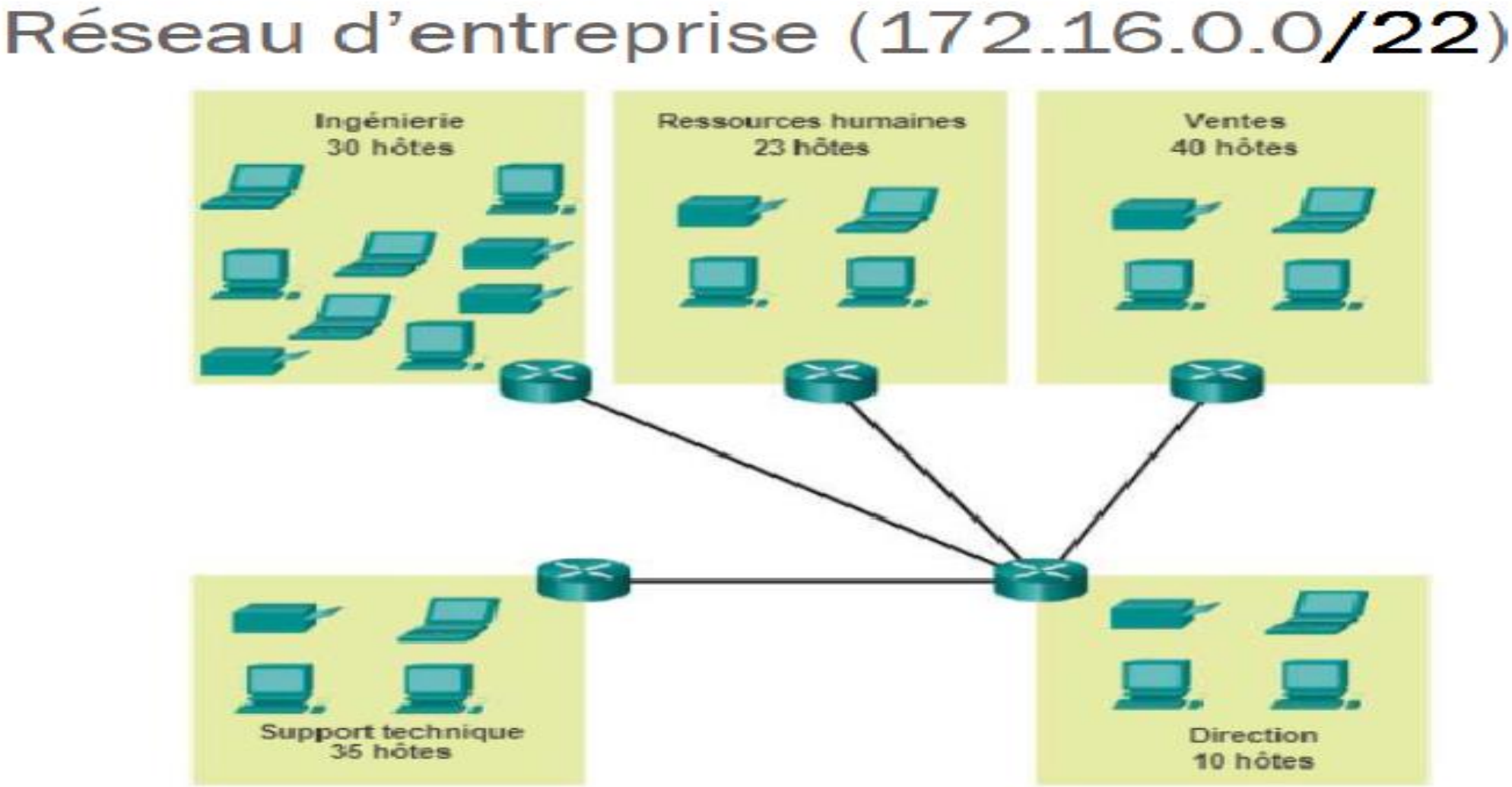
2^7 = 128 hôtes par sous-réseau

2^7 - 2 = 126 hôtes valides par sous-réseau

Exemple


Emprunt de 2 bits
Trame 192. 168. 1. 00 00 0000
Masque 255. 255. 255. 00 00 0000
Emprunter 2 bits permet de créer 4 sous-réseaux :
Réseau 0 192. 168. 1. 00 00 0000
Réseau 1 192. 168. 1. 01 00 0000
Réseau 2 192. 168. 1. 10 00 0000
Réseau 3 192. 168. 1. 11 00 0000
192.168.1.0 /26
192.168.1.64/26
192.168.1.128 /26
192.168.1.192 /26
Les 4 sous-réseaux utilisent le même masque :
Masque 255. 255. 255. 11 00 0000
Masque : 255.255.255.192

2.2 Découpage dynamique (VLSM)

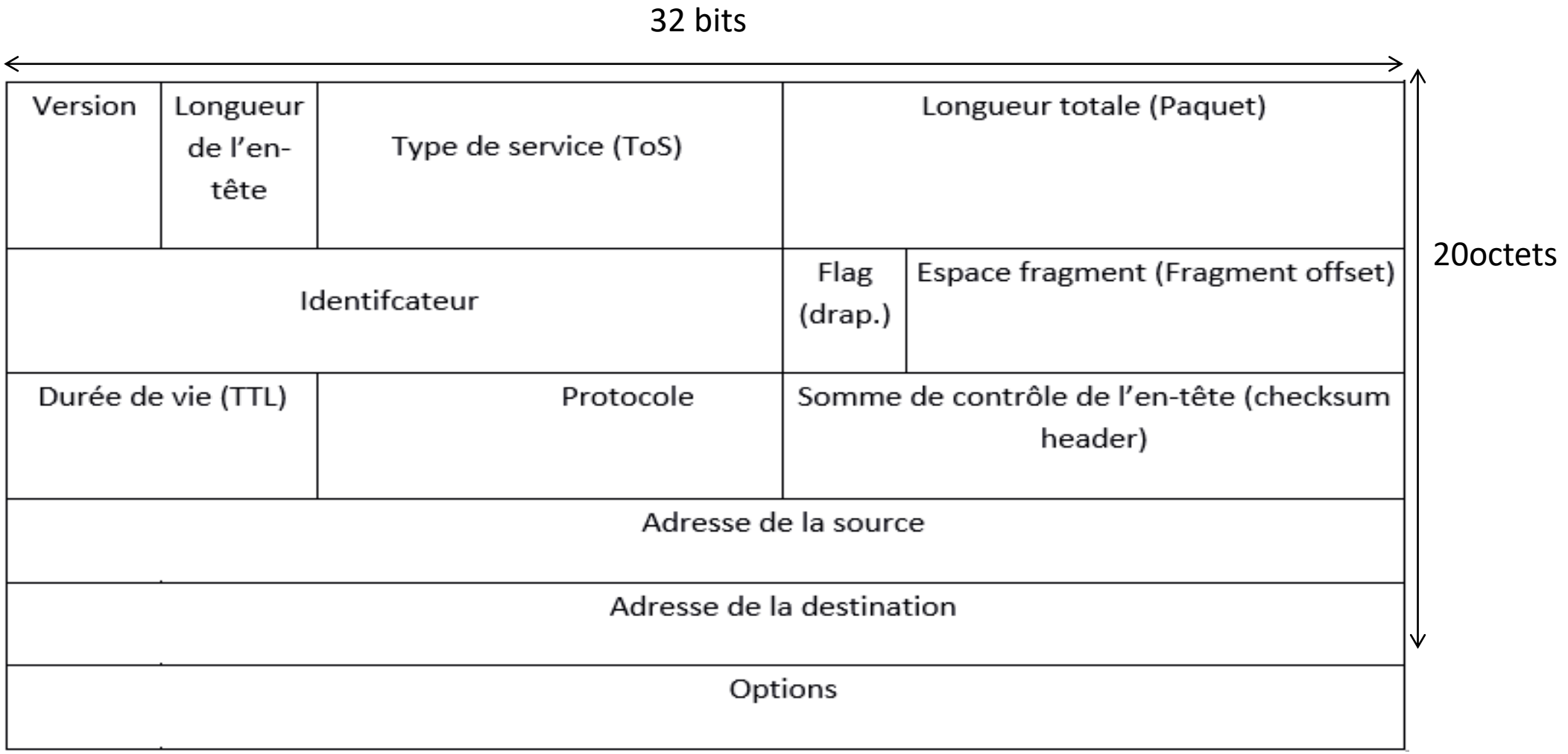


3. Le protocole IP

- Le protocole IP (Internet Protocol, RFC 791) est au cœur du fonctionnement d'un internet. Son rôle est centré autour de trois fonctionnalités :
  - Définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet.
  - Définir le routage dans Internet.
  - Définir la gestion de la remise non fiable des datagrammes.
- Le protocole IP assure un service *non fiable* de délivrance de datagrammes IP. En effet, il n'existe aucune garantie pour que les datagrammes IP arrivent à destination, puisqu'il est *sans connexion*. Certains datagrammes peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre.

3.1 Le datagramme IPv4

Un datagramme IP est constitué d'un en-tête suivi d'un champ de données.



- *Le champ version* du protocole IP utilisé, codé sur 4 bits (0100).
- *Le champ longueur d'en-tête* du datagramme IP codé sur 4 bits (20 octets – 60 octets).
- *Le champ TOS(Type Of Service)* codé sur 8 bits: indique la façon dont le datagramme doit être traité et se décompose en six sous champs comme suit :

0	1	2	3	4	5	6	7
Priorité			D	T	R	C	0

  - *Le champ priorité* varie de 0 (000) priorité normale (valeur par défaut) à 7 (111) priorité maximale et permet d'indiquer l'importance de chaque datagramme : Suivant les valeurs de ce champ, le routeur peut privilégier un datagramme par rapport à un autre.
  - Les 4 bits *D, T, R, C* indiquent au routeur l'attitude à avoir vis à vis de ce datagramme :

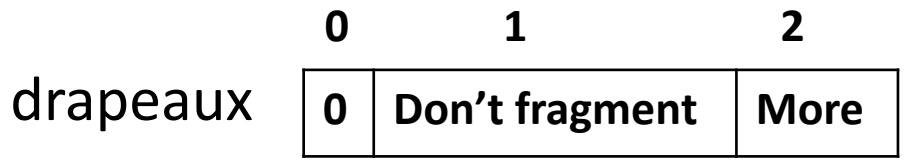
- *D* est mis à 1 pour essayer de minimiser le délai d'acheminement (ex : choisir un câble sous-marin plutôt qu'une liaison satellite),
- *T* est mis à 1 pour maximiser le débit de transmission,
- *R* est mis à 1 pour assurer une plus grande fiabilité et
- *C* est mis à 1 pour minimiser les coûts de transmission (coût).

Ces 4 bits servent à améliorer la qualité du routage et ne sont pas exigées. Simplement, si un routeur connaît plusieurs voies de sortie pour une même destination, il pourra choisir celle qui correspond le mieux à la demande.

Application	**Maximiser le délai**	**Maximiser le débit**	**Maximiser la fiabilité**	**Minimiser le coût**
Telnet	1	0	0	0
FTP Transfert	0	1	0	0
SNMP	0	0	1	0

- *Le champ longueur totale* en octets du datagramme. Ce champ est sur 2 octets on en déduit que la taille complète d'un datagramme ne peut dépasser *65535 octets*. Utilisée avec la longueur de l'en-tête elle permet de déterminer où commencent exactement les données transportées.

- *Les champs identification (16 bits), drapeaux (3bits) et déplacement de fragment (13 bits) :* interviennent dans le processus de ***fragmentation*** des datagrammes IP.



- *Le champ durée de vie (TTL)* codé sur 8 bits indique le nombre maximal de routeurs que peut traverser le datagramme IP. Il est initialisé à *N (souvent 32 ou 64)* par la station émettrice et décrémenté de 1 (il perd une vie) par chaque routeur qui le reçoit et le réexpédie. Lorsqu'un routeur reçoit un datagramme dont la durée de vie est nulle (TTL = 0), il le détruit et de ce fait, il est impossible qu'un datagramme tourne indéfiniment dans le réseau.

- *Le champ déplacement de fragment (offset)* précise la localisation du début du fragment dans le datagramme initial.

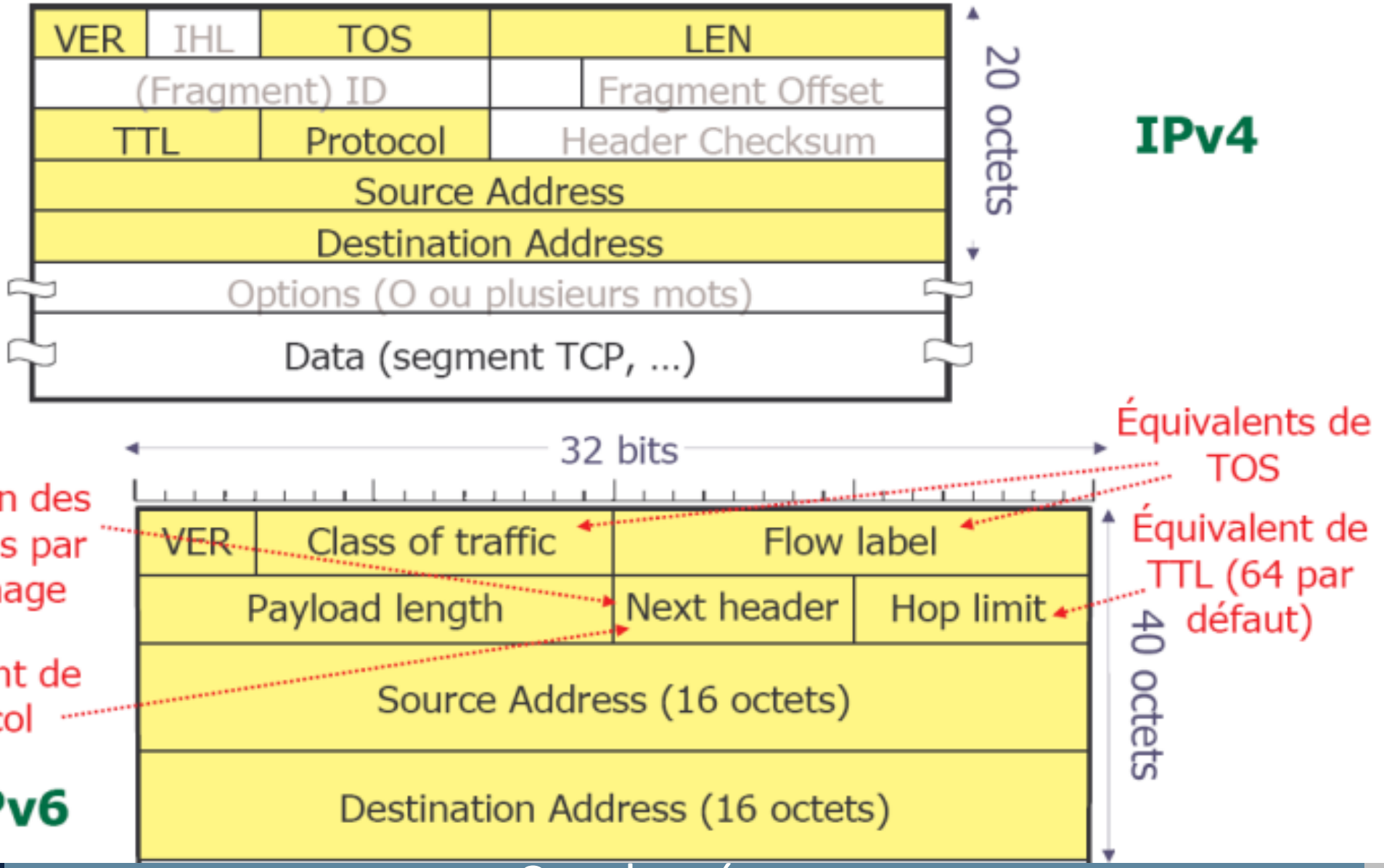
- *Le champ protocole* codé sur 8 bits identifie le protocole de plus haut niveau qui a servi a créé ce datagramme. Les valeurs sont **1** pour ICMP, **2** pour IGMP, **6** pour TCP et **17** pour UDP. Ainsi, la couche IP de la station destinatrice qui reçoit le datagramme IP pourra diriger les données qu'il contient vers le protocole supérieur adéquat.

- *Le champ Total de contrôle d'en tête* (HEADER CHECKSUM), codé sur 16 bits pour s'assurer de l'intégrité de l'en-tête.

- *Les adresses IP source et destination* sur 32 bits.

- *Le champ options* est une liste de longueur variable, mais toujours complétée par des bits de bourrage pour atteindre une taille multiple de 32 bits. Ces options sont très peu utilisées car peu de machines sont aptes à les gérer. Parmi elles, on trouve des options de sécurité et de gestion (domaine militaire), d'enregistrement de la route, d'estampille horaire, routage strict, etc...

3.2 Le datagramme IPv6



- *Le champ version* du protocole IP utilisé (IPv6)
- *Classe trafic* utilisé pour la qualité de service
- *Identificateur de flux* interviennent dans le processus de fragmentation des datagrammes IP
- *Longueur de données* désigne la taille du contenu du paquet
- *En-tête suivant* numéro correspondant au protocole utilisé dans la couche suivante
- *Nb de sauts* nombre maximal de nœuds traversé
- *Adresses IP source*
- *Adresses IP destination*
- *Options* est une liste de longueur variable

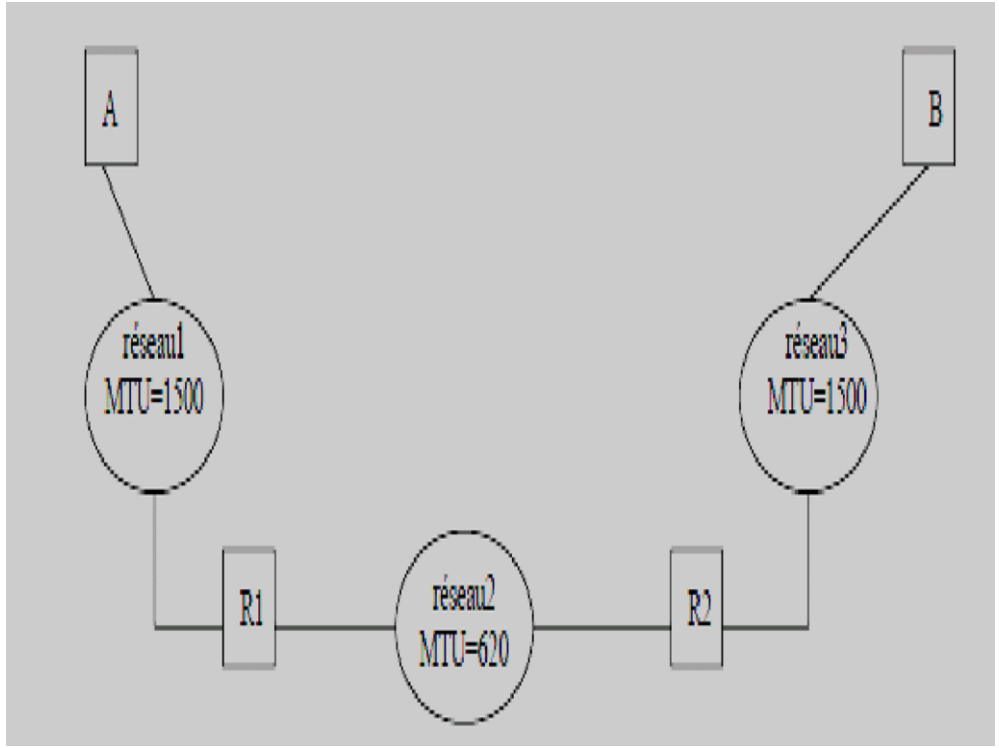
4. Fragmentation des datagrammes IP

- La taille maximale d'un datagramme IP est de **65535 octets**.

- Chaque réseau est caractérisé par une taille maximale d'une trame, appelée *la MTU (Maximum Transfert Unit).*

- Ceci cause un problème lorsqu'un routeur reçoit des datagrammes issus d'un réseau à grande *MTU* et doit les réexpédier vers un réseau à plus petite *MTU*.
- Pour remédier à ce problème, on a recourt à la *fragmentation des datagrammes*. Celle-ci se fait au niveau d'un routeur. La *MTU* est utilisée pour fragmenter les datagrammes trop grands pour le réseau qu'ils traversent. Si le *MTU* d'un réseau traversé est suffisamment grand pour accepter un datagramme, évidemment il sera encapsulé tel quel dans la trame du réseau traversé.

Exemple : Si la station *A*, reliée à un réseau Ethernet, envoie un datagramme de 1300 octets à destination de la station *B*, reliée également à un réseau Ethernet, le routeur R_1 relié à un réseau de *MTU=620* octets ne pourra faire le routage des datagrammes. Le routeur R_1 va fragmenter le datagramme de 1300 octets envoyé par la station *A* à destination de la station *B*, de la manière suivante :

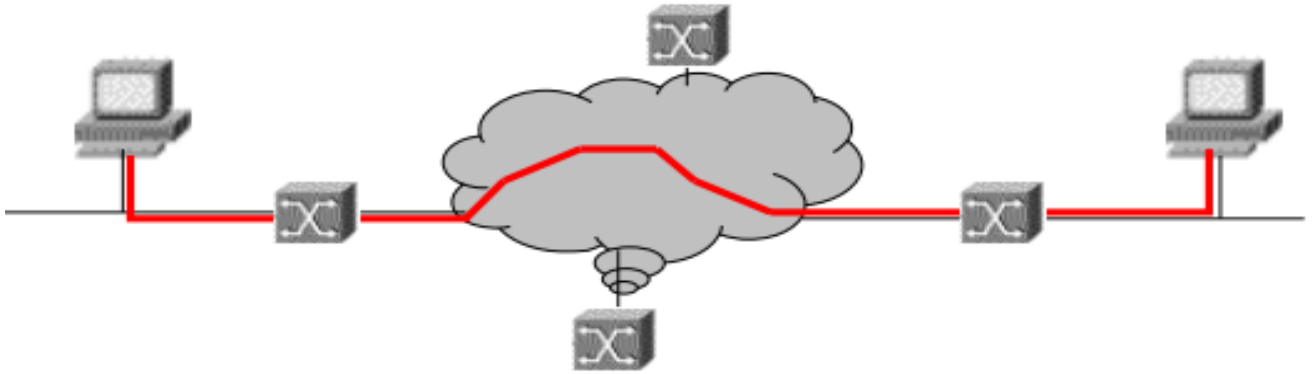


datagramme initial	en-tête du datagramme	données1 600 octets	données2 600 octets	données3 80 octets
fragment1	en-tête du fragment1	données1 600 octets	déplacement 0	
fragment2	en-tête du fragment2	données2 600 octets	déplacement 600	
fragment3	en-tête du fragment3	données3 80 octets	déplacement 1200	

5. Routage

Quel chemin empruntent les datagrammes pour arriver à destination ?

Routage : mécanisme par lequel les données d'un équipement expéditeur sont acheminées jusqu'à leur destinataire



Routeur

- dispositif permettant de ***choisir le chemin*** que les datagrammes vont emprunter
- utilise la ***table de routage*** qui définit le chemin à emprunter pour une adresse donnée

Table de routage

Définit la correspondance entre l'adresse de la machine visée et le nœud suivant auquel le routeur doit délivrer le message

Contenu de la table de routage

destination	IP d'une machine ou d'un réseau de destination
passerelle (gateway)	IP du prochain routeur vers lequel il faut envoyer le datagramme
masque (mask)	masque associé au réseau de destination
interface	interface physique par laquelle le datagramme doit réellement être expédié
métrique (cost)	utilisé pour le calcul du meilleur chemin

Commandes pour afficher le contenu de la table

netstat -r , route PRINT

Exemple

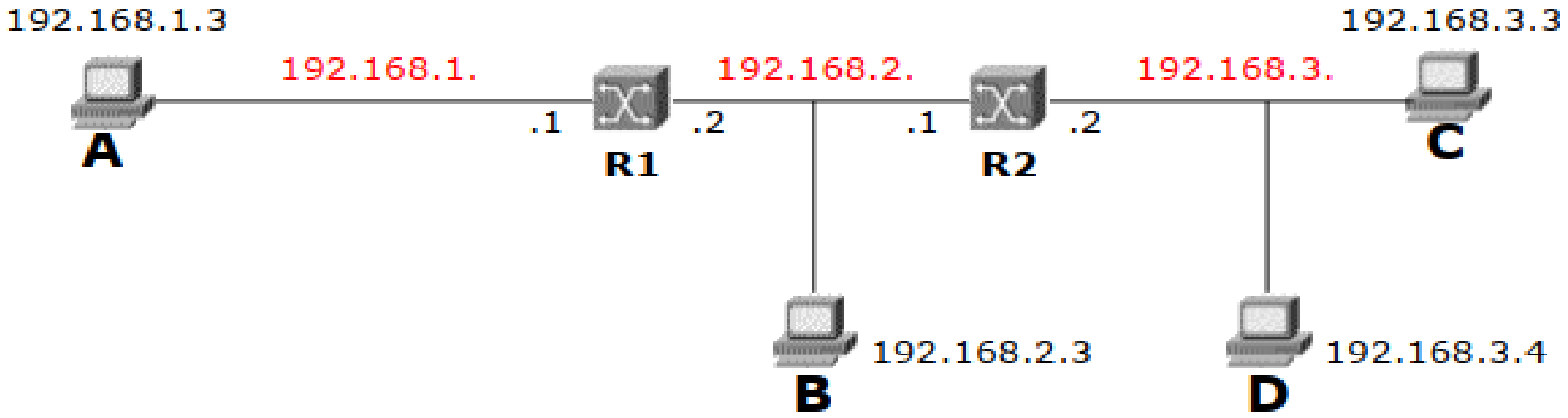


Table de routage de A

Destination	Netmask	Gateway	Interface	Cost
192.168.1.0	255.255.255.0	-	192.168.1.3	0
192.168.2.0	255.255.255.0	192.168.1.1	192.168.1.3	1
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.3	0

Routage

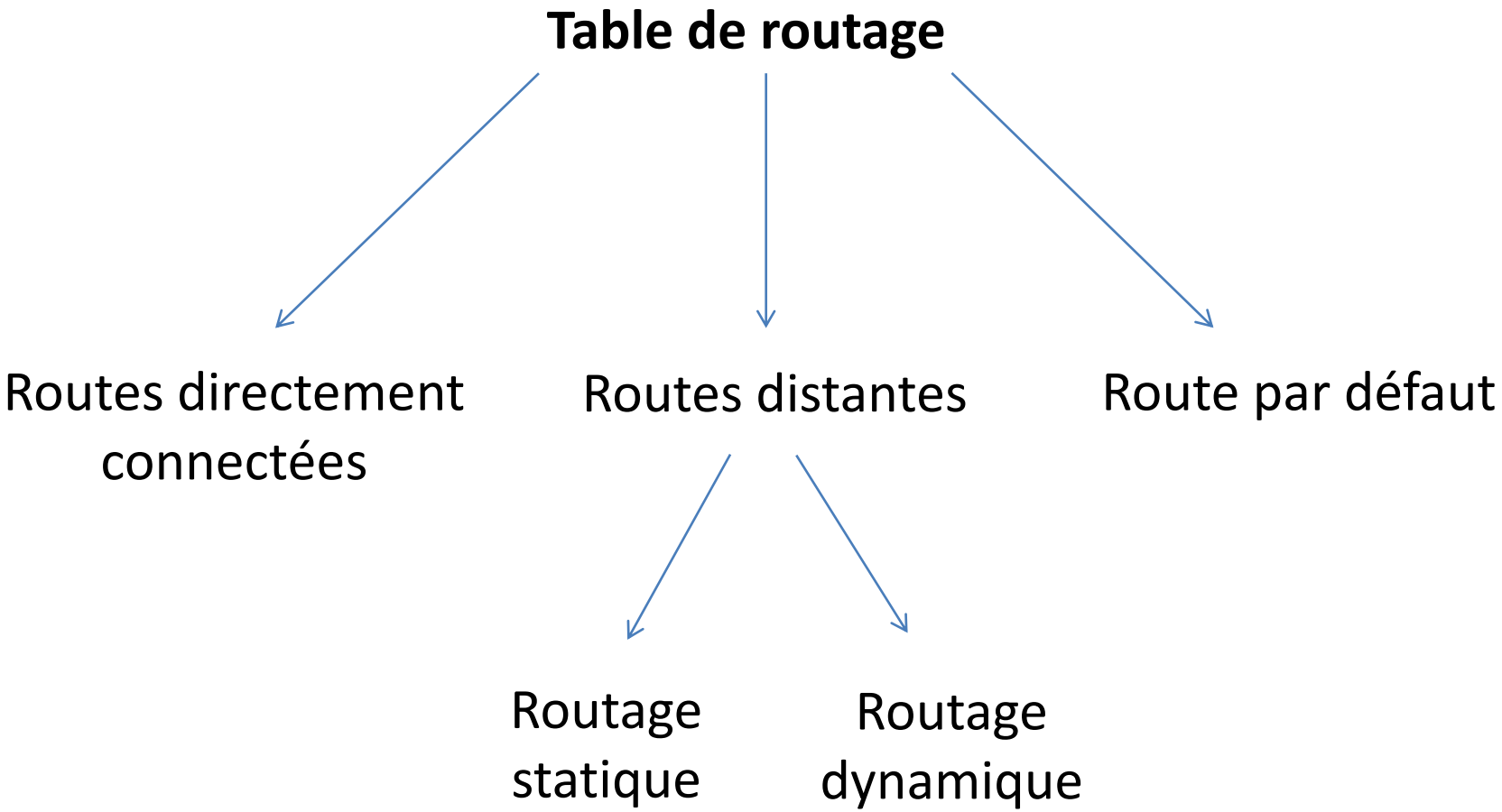


Table de routage
Routes directement connectées
Routes distantes
Route par défaut
Routage statique
Routage dynamique

Routage

Manuelle « routage statique »

- table de routage entrée manuellement par l'administrateur
- langage de commande des routeurs (ip route...)

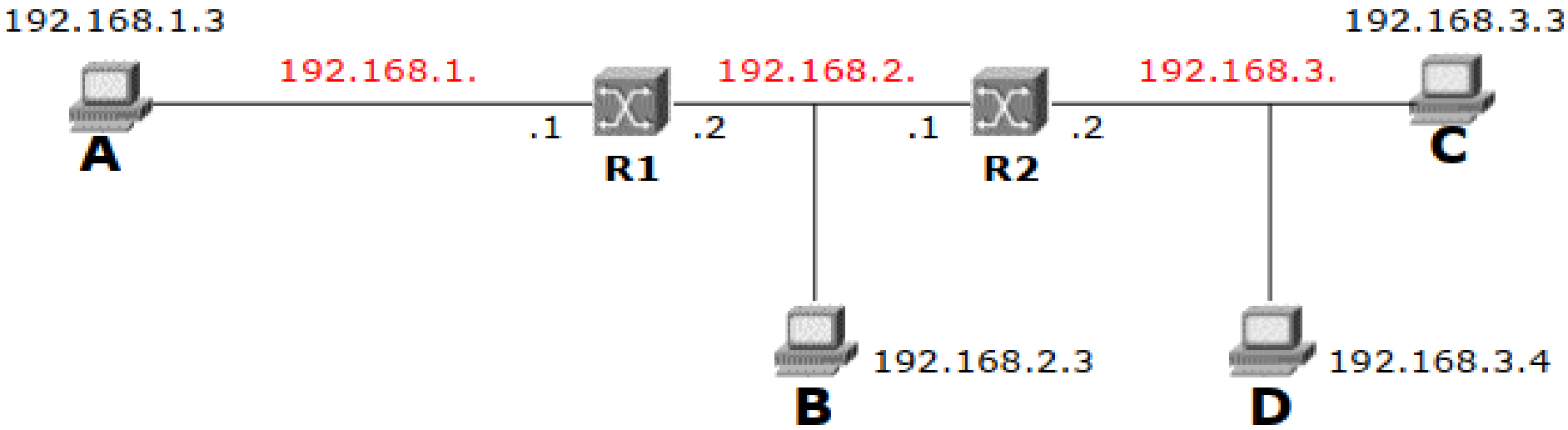
Automatique « dynamique »

- table de routage mis à jour dynamiquement par le routeur
- échanges d'informations de routage : ***protocoles de routage***

➢Routage basé sur un vecteur de distance

➢Routage basé sur l'état des liens

5.1 Routage statique



- La commande en mode de **configuration globale**:

ip route <réseau de destination> <masque du réseau de destination> <adresse IP du prochain saut>

5.2 Routage dynamique

Vecteur de distance – Bellman-Ford

Chaque noeud stocke un "vecteur" pour toutes destinations

- Ce vecteur contient la distance à chacune d'entre elles
- Distance = coût

Pré condition

- Chaque noeud connaît la distance vers tous ses voisins directs

État des liens – Dijkstra

Chaque nœud possède une carte complète du réseau

- Contrairement au "vecteur de distance", chaque noeud ne connaît que les états voisins

Exemples protocoles de routage dynamique

RIP (Routing information protocol)

Protocole de type ***Vecteur de Distance***

- Chaque 30 seconde le routeur diffuse à ses voisins ses vecteurs de distance
    - vecteur de distance : (destination, nombre de sauts)
    - nombre de sauts maximum = 16 (pour éviter les boucles)
    - utilisable uniquement à l'intérieur de domaines peu étendus
- Si aucun message pendant 180s, route inaccessible
- un noeud construit sa table de routage en fonction des vecteurs de distance reçus de ses voisins

OSPF - Open Shortest Path First

- Protocole de type ***état des liens***

- Chaque noeud évalue le coût pour rejoindre ses voisins selon une certaine métrique (***plusieurs métrique peuvent être utilisées simultanément***)
  - -construit un paquet contenant les informations relatives à chacun de ses liens (voisins)
  - -le diffuse à tout le monde (par inondation)
  - -calcule la route de moindre coût pour atteindre chaque entité du réseau
  - -ensuite, les routeurs s'échangent uniquement les changements détectés dans la topologie
  - -chaque noeud a une vision globale de la cartographie du réseau

Types de routeurs

Routeurs noyaux
relient les réseaux

Routeurs externes
permettent une liaison des réseaux autonomes entre eux
*Protocoles : **EGP** (Exterior Gateway Protocol)*
***BGP** (Border Gateway protocol)*

Routeurs internes
routage à l'intérieur d'un réseau autonome
*Protocole : **IGP** (Interior Gateway Protocol)*
RIP, OSPF, EIGRP