TCP/IP v4

Étude de la suite protocolaire standardisée

TCP/IP v4 - Sommaire

- Présentation
- Principe des protocoles de la couche 3 du modèle OSI
- ARP : Address Resolution Protocol
- IPv4 : Internet Protocol v4
- Aspect protocolaire
- Adressage IPv4
- Le sous-adressage : CIDR
- Le sous-adressage : VLSM
- Routage
- ICMP : Internet Control Message Protocol
- UDP : User Datagram Protocol
- TCP : Transmission Control Protocol

TCP/IP v4 - Histoire

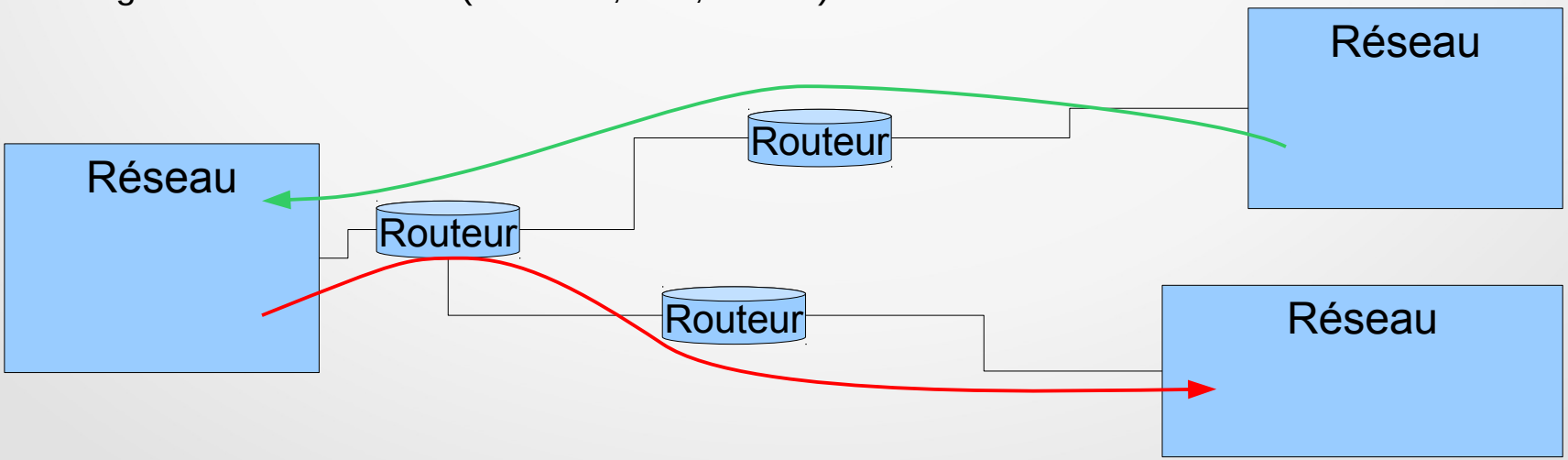
- Développement d'IP conjointement au réseau Internet
- Evolution du réseau ARPANET développé en 1972 par le DARPA (Defense Advanced Research Projects Agency)
- A partir de 1973, refonte du réseau et des protocoles : ce sont les hôtes qui assurent la cohérence du réseau.
- Vinton Cerf (université de Stanford) et Robert Kahn (DARPA) sont chargés de cette refonte.
- Les premiers travaux donnèrent naissance à 4 versions de TCP/IP.

TCP/IP v4 - Histoire

- Les premiers réseaux IPv4 sont mis en place :
  - 1975 : Université de Stanford
  - 1975 : London College
  - 1977 : en Norvège
  - Extensions des travaux jusqu'en 1983
- 1982 : utilisation officielle de TCP/IP v4 par le DoD pour ses réseaux militaires.
- La démocratisation d'internet a rendu quasiment obligatoire l'utilisation de TCP/IP dans les réseaux locaux d'entreprise.

TCP/IP v4 - Principes

- Le but de TCP/IP est de permettre la communication entre des hôtes appartenant à des réseaux différents : principe de l'interconnexion.
- Internet = **inter**connected **net**works (réseaux interconnectés)
- Les équipements intermédiaires réalisant cette interconnexion s'appellent les « **routeurs** ».
- La communication entre les hôtes se fait sur la base de l'adresse du destinataire.
- Pas de machine prioritaire.
- Technologie publique diffusée au travers de RFC.
- TCP/IP est indépendant du matériel réseau sous-jacent, du support de transmission et des technologies réseau utilisées (Ethernet, Wifi, ATM...)



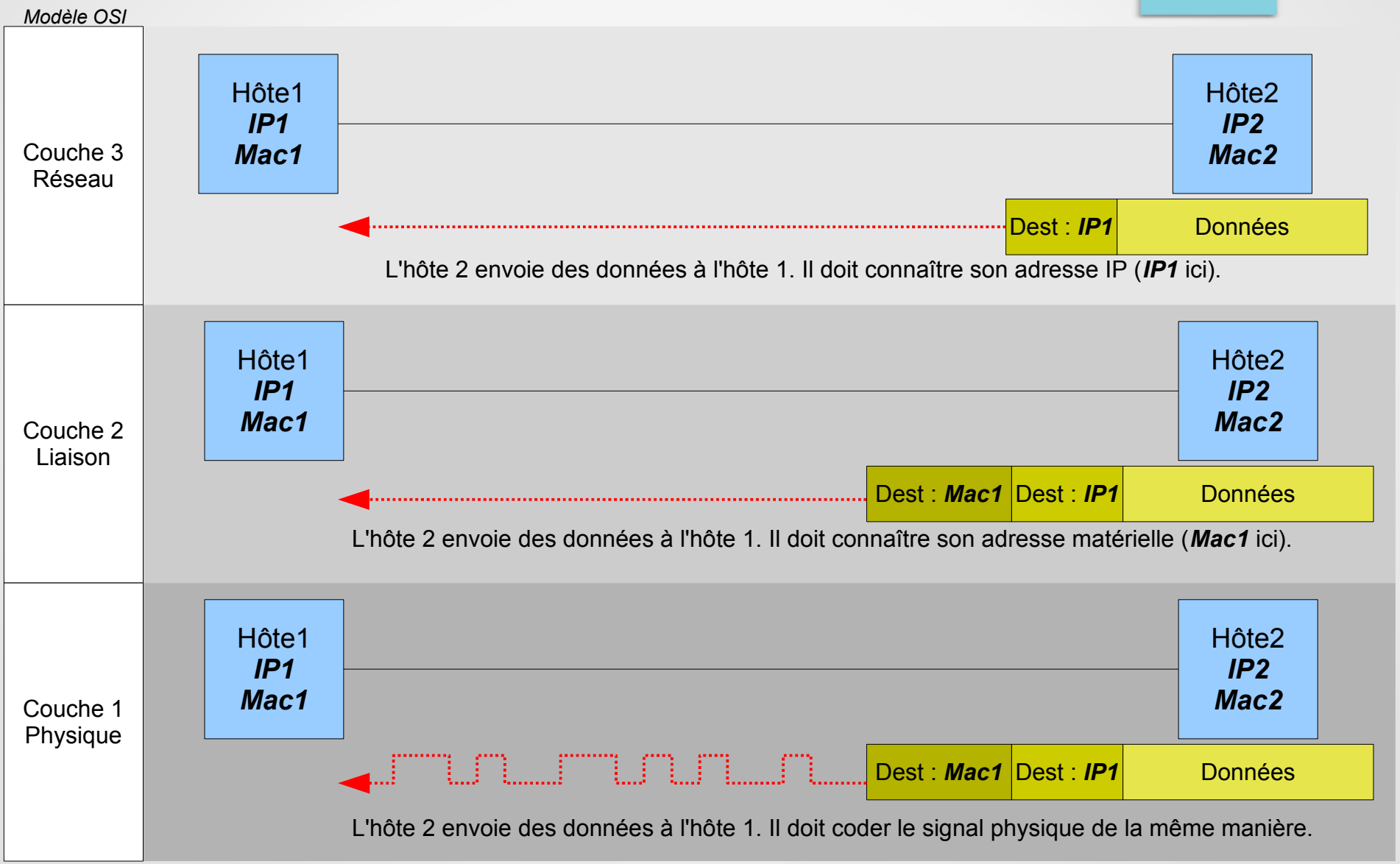
TCP/IP v4 : Principes

- TCP/IP v4 est composé de plusieurs protocoles ayant leur utilité dans une communication
  - ARP : permet de trouve l'adresse matérielle à partir de l'adresse IP.
  - IP : permet la transmission de données d'un réseau à un autre par l'intermédiaire d'une adresse logicielle.
  - ICMP : permet de contrôler et seconder IP en informant les hôtes.
  - TCP : Permet le transport de l'information de manière fiable entre 2 hôtes.
  - UDP : permet le transport non fiable de l'information entre 2 hôtes.
- Tous ces protocoles seront abordés dans ce cours.

TCP/IP v4 - ARP

- Pour que la communication entre 2 hôtes IP sont fonctionnelle, il faut qu'elle le soit sur les couches inférieures du modèle OSI.
- Pour joindre un poste présent sur un segment réseau, il faut connaître l'adresse logicielle de ce poste mais aussi connaître son adresse matérielle et les codages de signaux utilisés au niveau physique par son interface réseau.
- Pour un poste présent dans un autre segment réseau, il faut connaître la adresse logicielle de la destination mais aussi l'adresse matérielle et les codages physiques du routeur qui permettra de joindre cet hôte.

TCP/IP v4 - ARP

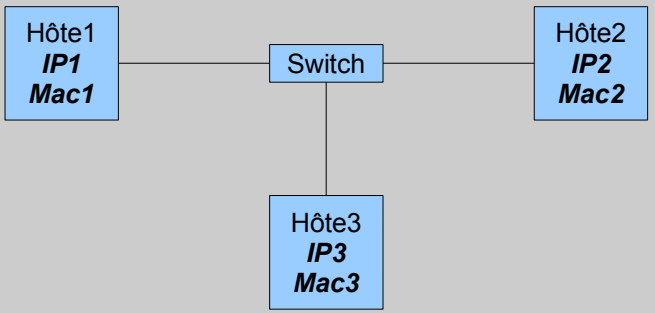

Modèle OSI
Couche 3
Réseau
Hôte1
IP1
Mac1
Hôte2
IP2
Mac2
Dest : IP1
Données
L'hôte 2 envoie des données à l'hôte 1. Il doit connaître son adresse IP (IP1 ici).
Couche 2
Liaison
Hôte1
IP1
Mac1
Hôte2
IP2
Mac2
Dest : Mac1
Dest : IP1
Données
L'hôte 2 envoie des données à l'hôte 1. Il doit connaître son adresse matérielle (Mac1 ici).
Couche 1
Physique
Hôte1
IP1
Mac1
Hôte2
IP2
Mac2
Dest : Mac1
Dest : IP1
Données
L'hôte 2 envoie des données à l'hôte 1. Il doit coder le signal physique de la même manière.

TCP/IP v4 - ARP

- Le rôle d'ARP (Address Resolution Protocol) est de trouver l'adresse matérielle correspondant à une adresse IP.
- Une fois cette adresse matérielle récupérée, l'hôte peut créer la trame de niveau 2 à envoyer par l'interface réseau.
- Théoriquement, ARP peut fonctionner avec n'importe quel protocole de la couche 3 et n'importe quel protocole de la couche 2.
- La résolution est effectuée en envoyant des diffusions (broadcast) de niveau 2.
- Un cache des résolutions est entretenu afin de ne pas avoir à envoyer de requête ARP à chaque transmission IP.

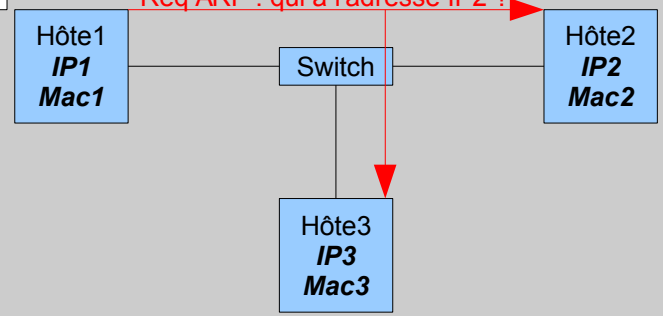
TCP/IP v4 - ARP

1



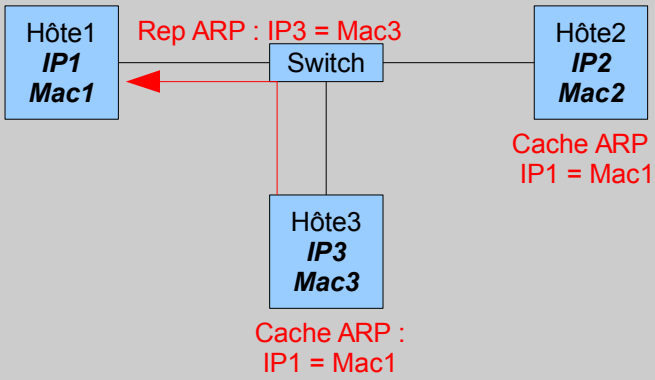
L'hôte 1 veut récupérer l'adresse matérielle de l'hôte 3.

2



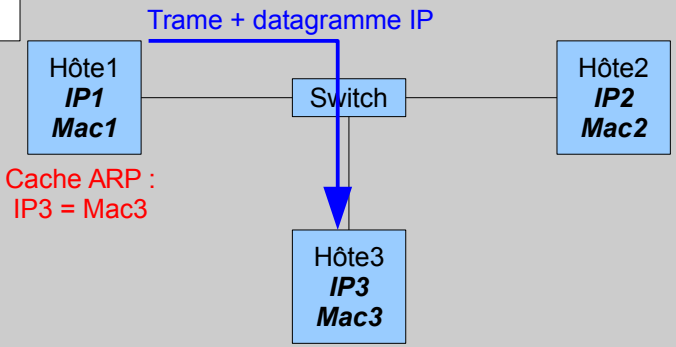
L'hôte 1 demande à tous les hôtes (diffusion) qui a l'adresse IP2.

3



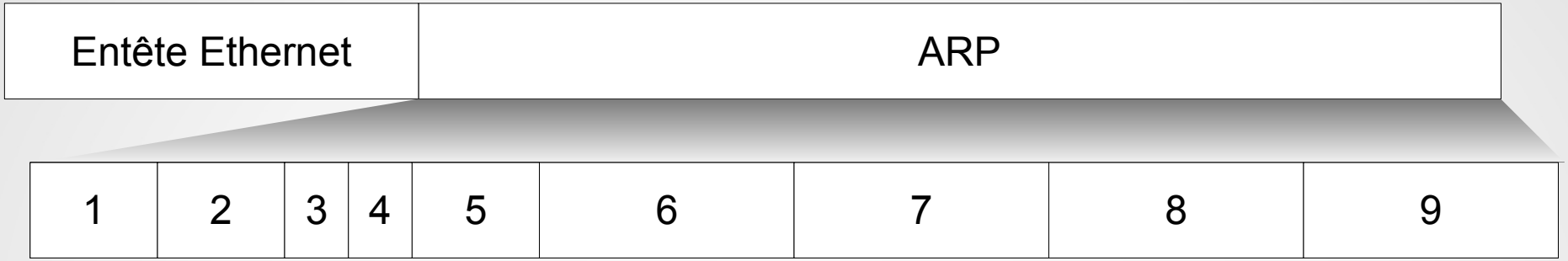
Les 2 hôtes stockent les infos de l'émetteur dans leur Cache et seul l'hôte 3 répond à la requête.

4



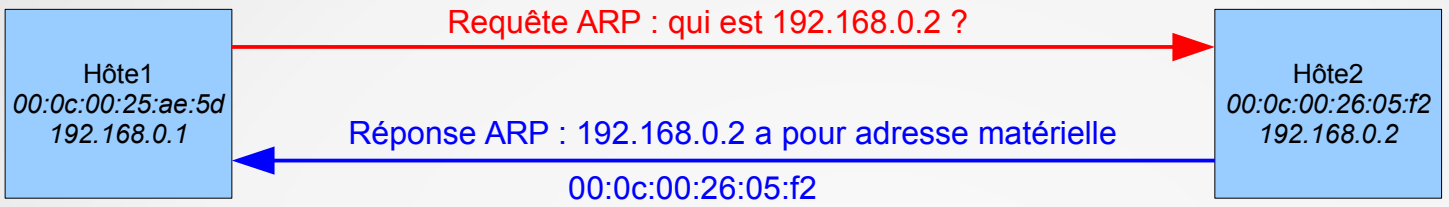
L'hôte 1 stocke la réponse dans son cache et peut construire l'entête de la trame à transmettre.

TCP/IP v4 - ARP



1. Hardware type : protocole concerné sur la couche n°2 (1 → Ethernet, 19--> ATM)
2. Protocol type : protocole concerné sur la couche n°3 (0x800 → IP)
3. Hardware address length : taille de l'adresse matérielle
4. Protocol address length : taill de l'adresse logicielle (IPv4)
5. Opcode : type de message ARP (1 → request, 2 → reply)
6. Source hardware address : adresse matérielle source
7. Source protocol address : adresse logicielle source
8. Destination hardware address : adresse matérielle de destination
9. Destination protocol address : adresse logicielle de destination

TCP/IP v4 - ARP



Requête ARP : qui est 192.168.0.2 ?

0x1	0x800	0x6	0x4	0x1	00:0c:00:25:ae:5d	192.168.0.1	0x0	192.168.0.2

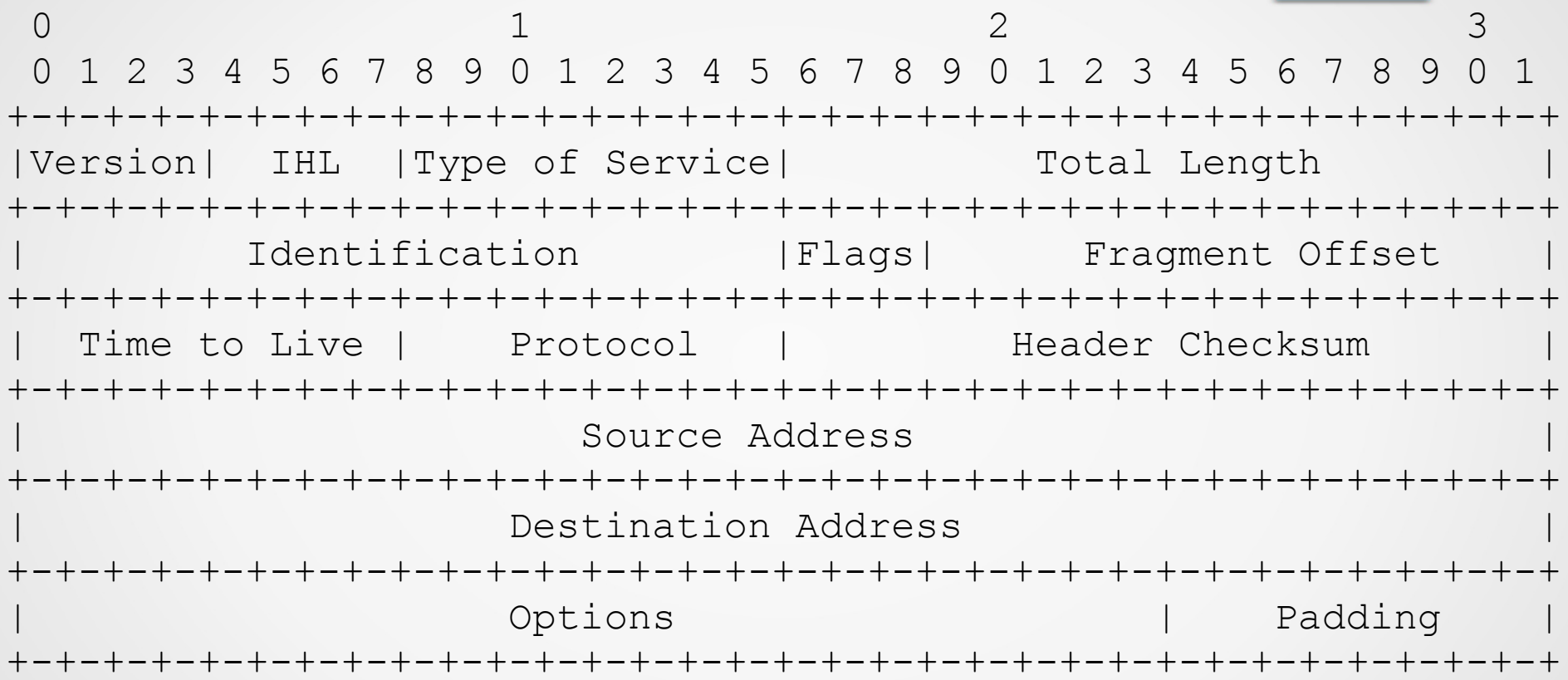
Réponse ARP : 192.168.0.2 a pour adresse matérielle 00:0c:00:26:05:f2

0x1	0x800	0x6	0x4	0x2	00:0c:00:26:05:f2	192.168.0.2	00:0c:00:25:ae:5d	192.168.0.1

TCP/IPv4 : Aspect protocolaire

- IP (internet protocol) est le protocole non connecté de la couche n°3 du modèle OSI (réseau) permettant la transmission de donnée d'un hôte à un autre, même s'il est situé sur un autre segment réseau.
- Il est non connecté car il ne garantit pas la fiabilité de la transmission.
- IP utilise une adresse logicielle afin de permettre un routage indépendant des technologies réseaux utilisées.
- L'unité de transmission est appelée le « datagramme ».
- Le routeur est l'équipement permettant de transmettre un datagramme IP d'un réseau vers un autre.

TCP/IP v4 : Entête



Source : RFC 791

TCP/IP v4 : Entête

- **Version** (4 bits) : format de l'entête IP. Actuellement, 2 versions cohabitent : v4 et v6
- **IHL** (Internet Header Length) (4 bits) : taille de l'entête en nombre de mots de 32 bits. Un entête IP sans option a une taille de 20 octets, soit 5 mots de 32 bit.
- **Type of Service** (16 bits) : ce champ a évolué au cours des années. Il sert généralement à différencier le trafic afin de créer une certaine qualité de service (QoS). Il est maintenant utilisé sous la forme DSCP (Differentiated Services Code Point).
- **Total length** (16 bits) : taille du datagramme en octets (entête + données)
- **Identification** (16 bits) : valeur aléatoire assignée dans le but d'aider au ré-assemblage des fragments.

TCP/IPv4 : Entête

- **Flags** (3 bits) : sert à gérer la fragmentation. Il précise si le datagramme est le dernier fragment ou pas et s'il a la possibilité d'être fragmenté.
- **Fragment Offset** (13 bits) : définit le décalage du fragment dans le datagramme d'origine.
- **Time To Live** (8 bits) : cette valeur est décrémenté à chaque traversé de routeur de 1 ou du nombre de secondes passées dan le routeur. Cela permet, soit de limiter la portée d'un datagramme, soit d'éliminer les datagrammes bloqués dans une boucle de routage.
- **Protocol** (8 bits) : identifie le protocole encapsulé dans le datagramme IP.
  - 1 → ICMP
  - 6 → TCP
  - 17 → UDP
  - 47 → GRE
  - 50 → ESP
  - 51 → AH

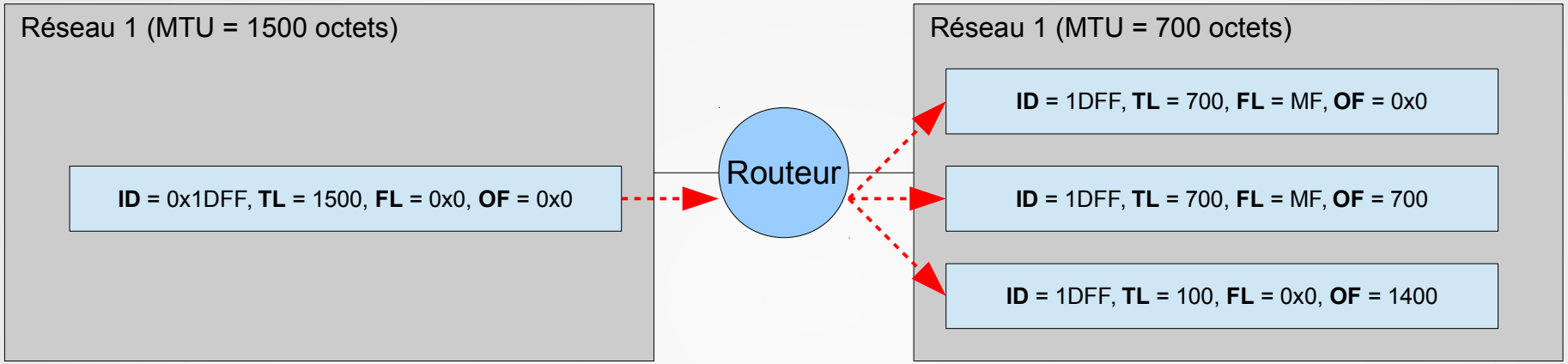
TCP/IP v4 : Entête

- **Header Checksum** (16 bits) : somme de contrôle permettant de vérifier la validité de l'entête. Comme certains champs changent de valeurs au cours d'une transmission, cette somme est recalculée à chaque fois
- Source Address (32 bits) : addresse IP de l'émetteur du datagramme.
- Destination address (32 bits) : addresse IP du destinataire du datagramme.
- Options : un datagramme IP peut disposer d'options permettant d'utiliser des fonctionnalités supplémentaires. Actuellement, ces options sont rarement utilisées.

TCP/IP v4 : Fragmentation

- Le protocole IP a été prévu pour faire transiter des données à travers des réseaux ayant des MTU (Maximum Transfer Unit) de tailles différentes.
- Le routeur faisant transiter un datagramme vers un réseau ayant une MTU plus petite n'aura que 2 possibilités :
  - Rejeter le datagramme s'il le flag « Do not fragment » est positionné.
  - Fragmenter le datagramme afin qu'ils puissent transiter sur ce réseau.
- C'est le destinataire du datagramme qui se chargera du ré-assemblage des fragments.
- Cette opération peut-être coûteuse en terme de latence si de nombreux fragments sont créés.
- La fragmentation se produit très rarement sur les réseaux actuels.

TCP/IP v4 - Fragmentation



Le datagramme a été forgé depuis une machine connectée à un réseau ayant une MTU de 1500 octets (Ethernet).

Il est envoyé vers un réseau ayant une MTU de 700 octets.

Le routeur chargé de faire transiter ce datagramme constate que le flag DF (Do not fragment) n'est pas présent : il va donc le fragmenter.

3 fragments (2 x 700 octets + 1 x 100 octets) sont créés.

Le poste de destination pourra reconstituer le datagramme d'origine :
- le champ ID permettra de trouver les fragments provenant du même datagramme.
- les champs OF et TL permettront de positionner le fragment dans le datagramme
- le champ FL permettra de définir s'il s'agit du dernier fragment.

Légende

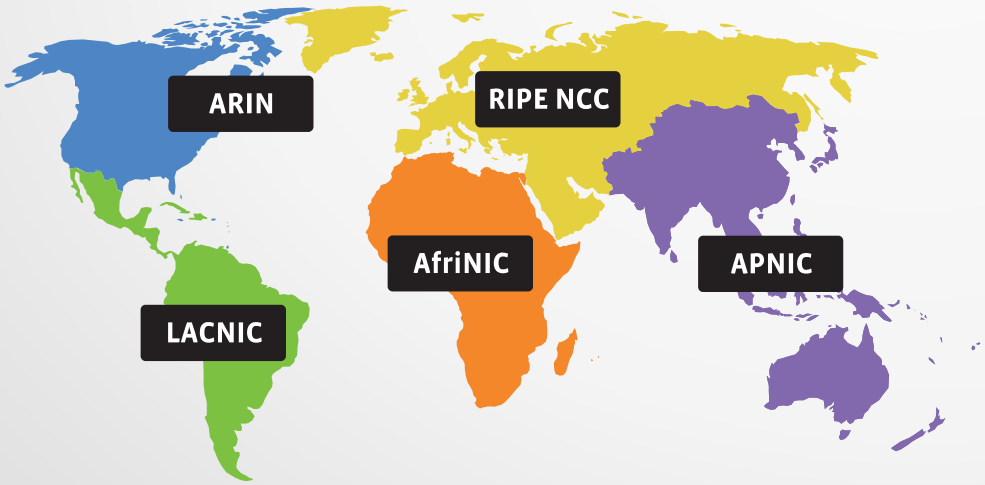
ID : Identification
TL : Total Length
FL : Flag
OF : Offset

TCP/IP v4 - Adressage

- L'adresse IP permet de localiser un poste quelque soit le réseau auquel il appartient.
- L'adresse IP doit identifier de manière unique chaque poste du réseau.
- Sur internet, l'attribution de ces adresses IP est très réglementée et passe par plusieurs organismes.
- L'IANA (Internet Assigned Numbers Authority) est chargée de définir comment seront utilisées les adresses IP.
- Cet organisme sélectionne des plages d'IP pour des utilisations spécifiques (bouclage local, adresses privées...etc) et délègues les autres adresses à des organismes régionaux (RIR).

TCP/IP v4 - Adressage

- Un utilisateur désirant obtenir une adresse IP fera sa demande à son fournisseur d'accès (**FAI**).
- Le fournisseur d'accès obtient des plages d'adresses IP auprès d'un **LIR** (Local Internet Registry), d'un **NIR** (National Internet Registry) ou directement auprès d'un **RIR** (Regional Internet Registry).



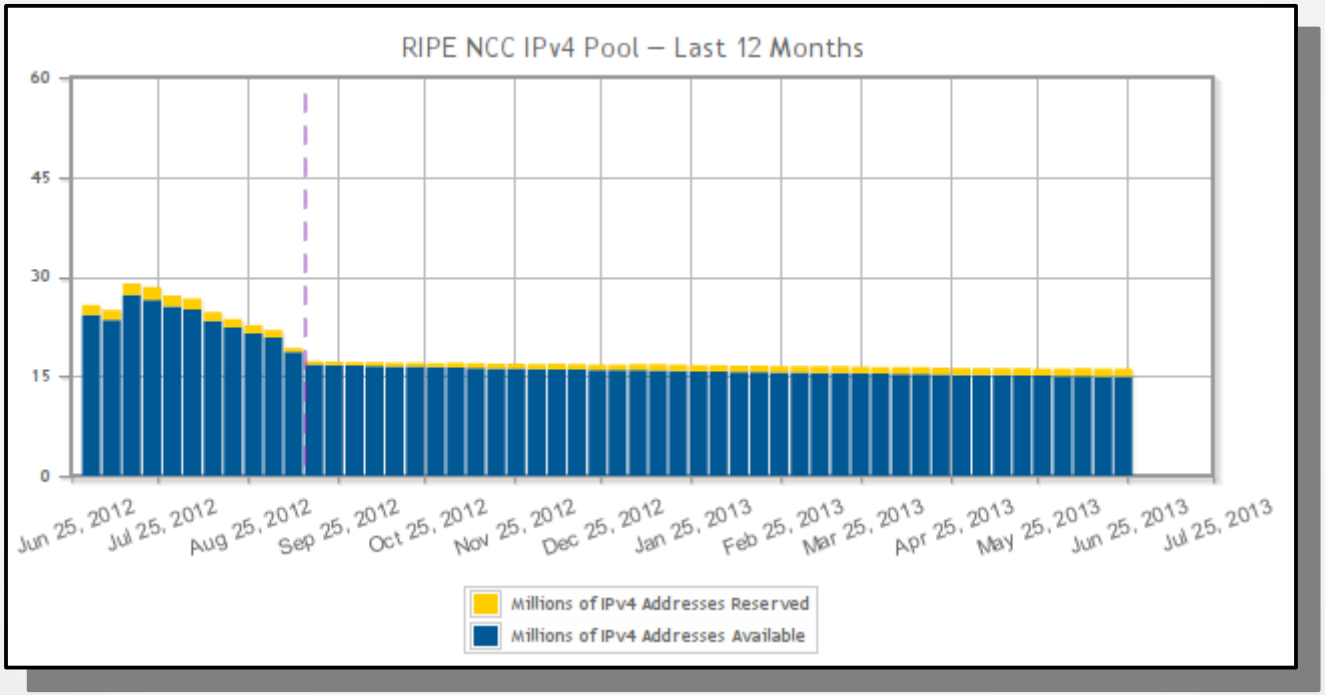
Registre	Zone couverte
AfriNIC	Afrique
APNIC	Asie / Pacifique
ARIN	Amérique du Nord
LACNIC	Amérique latine + quelques îles des Caraïbes
RIPE NCC	Europe, Moyen Orient et Asie centrale

source : iana.org

TCP/IP v4 - Adressage

- L'adresse IP est codée sur 4 octets (32 bit).
  Il y a donc 2^{32} = 4 294 967 296 adresses IP possibles.
- Ce nombre était suffisant à la création du protocole mais ça n'est plus le cas.
- Des technologies ont été développées pour retarder cette pénurie (NAT, adresses IP privées...).
- Depuis février 2011, l'IANA ne dispose plus d'adresse à attribuer aux RIR.
- Les RIR voient leur réserve d'adresse IP diminuer différemment.
- Depuis septembre 2012, le RIPE NCC a commencé à attribuer le dernier bloc de 17 millions d'adresses. Celles-ci sont maintenant distribuées de manière plus restrictive :
  - Un bloc de 1024 adresses pourra être attribué uniquement aux membres du RIPE NCC disposant déjà d'IPv6.
  - Aucun nouveau fournisseur indépendant d'IPv4 ne sera accepté.

TCP/IP v4 – Adressage



État du nombre d'adresses IPv4 disponibles et réservées en juillet 2013

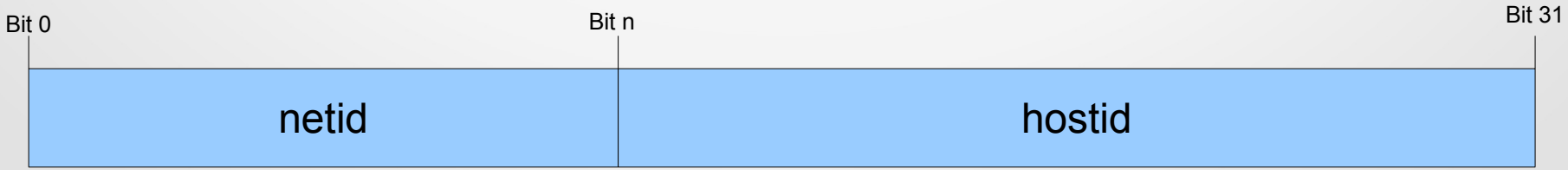
Source : ripe.net

TCP/IP v4 - Adressage

- Codage sur **32 bits**, soit **4 octets**
- **Notation décimale pointée** (plus simple à retenir qu'une adresse IP)

	Notation binaire	Notation décimale pointée
Adresse minimale	`00000000.00000000.00000000.00000000`	`0.0.0.0`
Adresse maximale	`11111111.11111111.11111111.11111111`	`255.255.255.255`

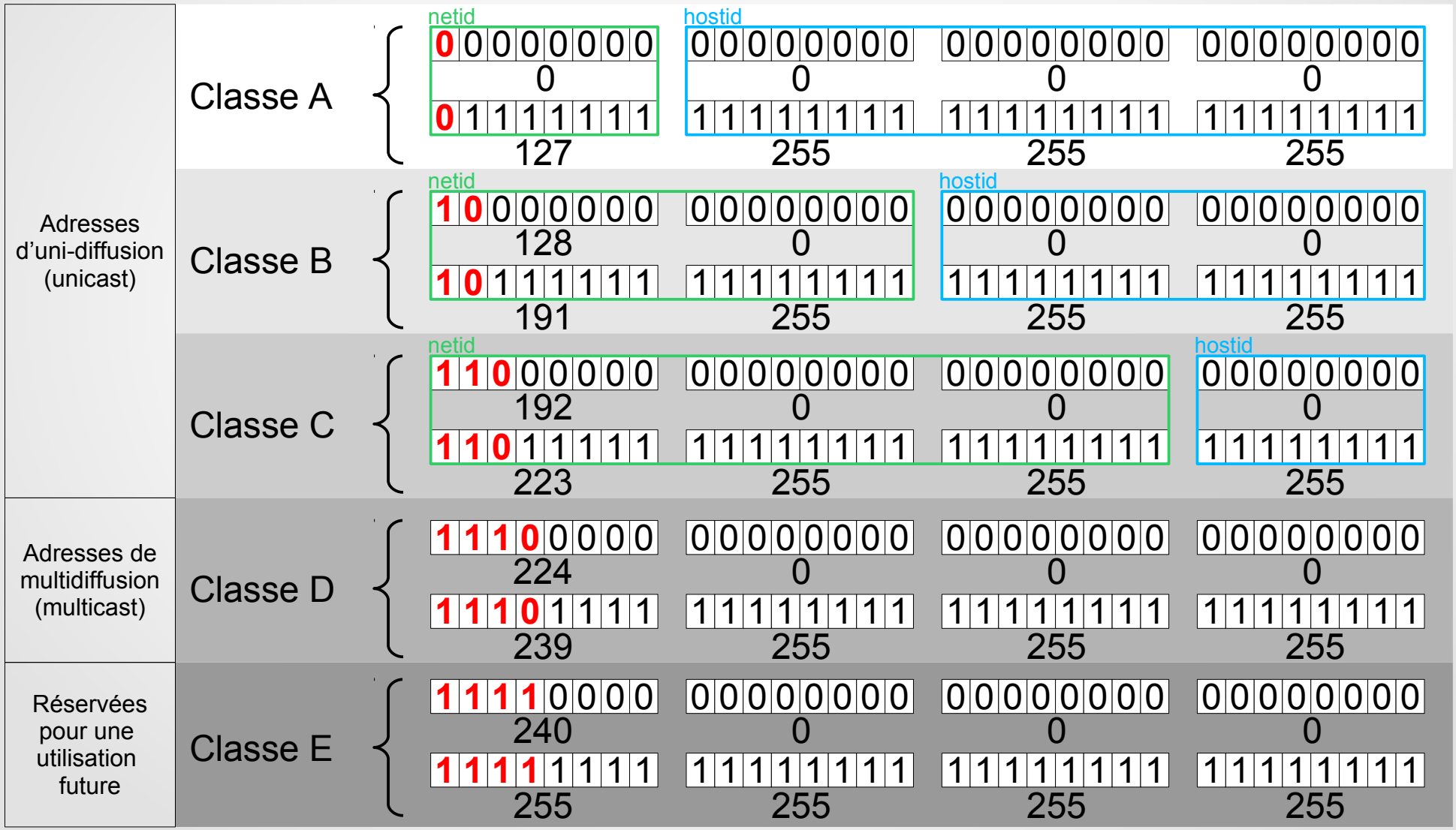
- L'utilisation de ces 4 milliards d'adresses doit être ordonné afin de permettre de différentier des réseaux IP.
- Pour cela, une partie de l'adresse désigne l'identifiant de réseau (**netid** = **net**work **id**entifier) et l'autre désigne l'identifiant de l'hôte dans un réseau (**hostid** = **host id**entifier)
- Les hôtes ayant un même netid peuvent communiquer directement.
- Les hôtes ayant un netid différents doivent passer par une passerelle (routeur) pour pouvoir communiquer.
- Des hôtes ayant un même netid doivent disposer d'un hostid différent (adresses unicast)



TCP/IP v4 – Adressage - Classes

- A la création du protocole, des classes d'adresses IP ont été définies.
- Celles-ci servent à définir les contextes d'utilisation :
  - Uni-diffusion
  - Multi-diffusion
  - Réseaux de petites, moyennes et grandes tailles
- Cette notion de classe a moins d'importance maintenant car la taille des réseaux est définie par le masque de sous-réseau.

TCP/IP v4 – Adressage - Classes

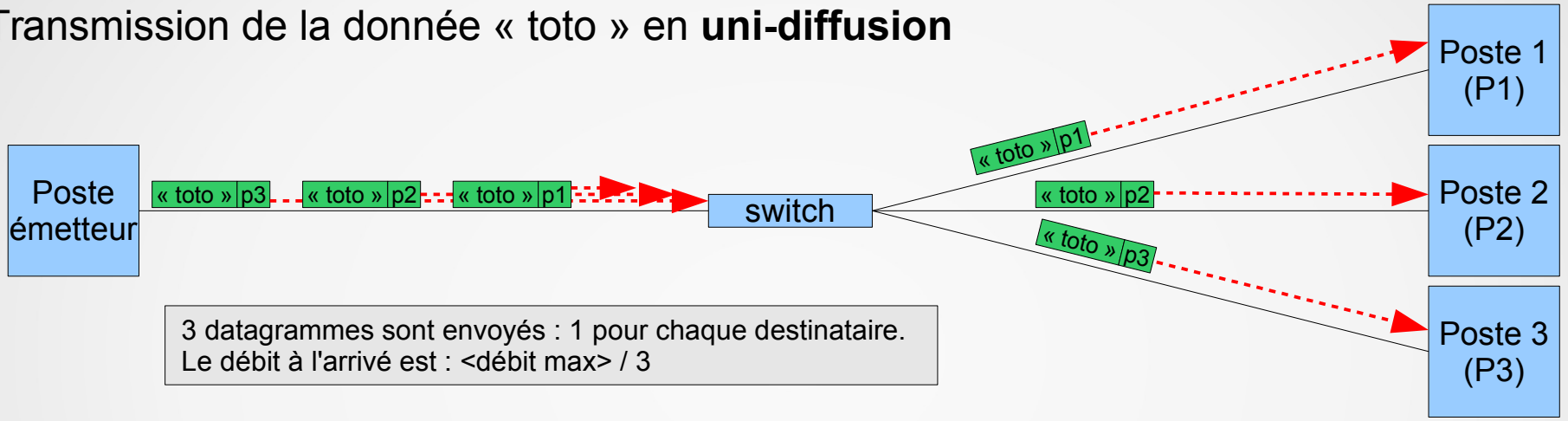


TCP/IP v4 – Adressage - Classes

- Les adresses de classe A sont adaptées pour les réseaux de grande taille :
  1 réseau de classe A→ **17 millions d'adresses**
- Les adresses de classe B sont adaptées pour les réseaux de taille moyenne :
  1 réseau de classe B → **65 000 adresses**
- Les adresses de classe C sont adaptées pour les réseaux de petite taille :
  1 réseau de classe C → **254 adresses**
- Les adresses de **classe A, B et C** sont des adresses d'unidiffusion (**unicast**).
  - Elles permettent la communication d'un hôte vers un autre hôte.
  - 2 mêmes adresses d'uni-diffusion ne peuvent cohabiter sur le même réseau.
  - Ce sont les adresses les plus couramment utilisées, elles conviennent à quasiment toutes les situations.
- Les adresses de **classe D** sont des adresses de multidiffusion (**multicast**).
  - Elles permettent la communication entre 1 hôte et un groupe d'hôte.
  - Le champ d'application est réduit : déploiement d'images systèmes, diffusion vidéo...etc
  - Ces adresses ne sont pas routables sans un protocole spécifique.
- Les adresses de **classe E** sont des adresses non utilisées, **réservées pour une utilisation future**. Actuellement, mis à part quelques adresses spéciales, aucune d'entre elles n'est utilisable.

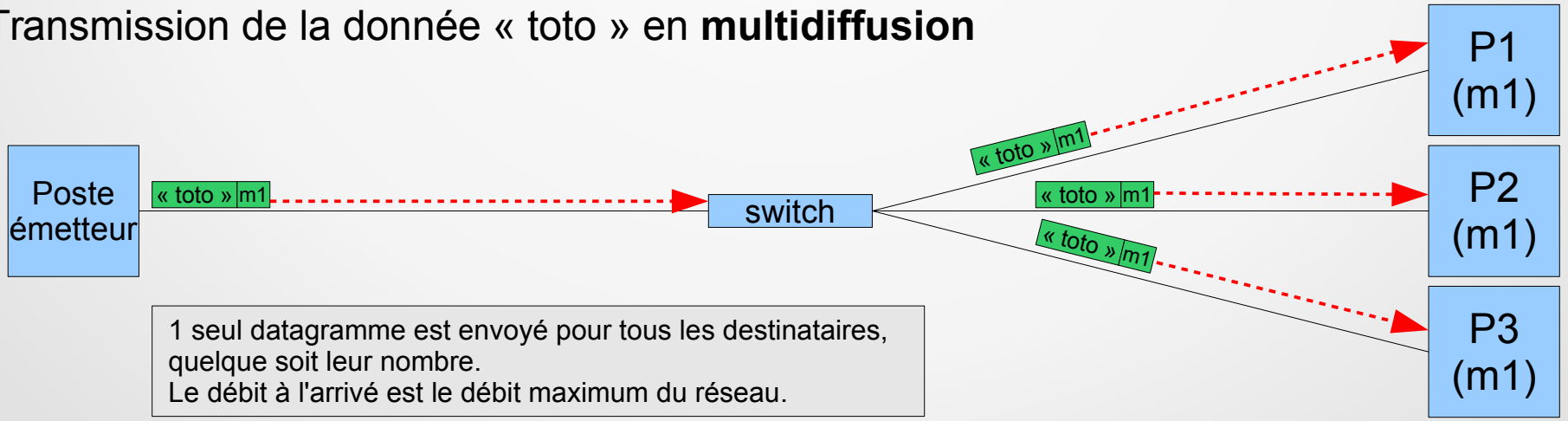
TCP/IP v4 – Adressage - Multicast

Transmission de la donnée « toto » en **uni-diffusion**



3 datagrammes sont envoyés : 1 pour chaque destinataire.
Le débit à l'arrivé est : <débit max> / 3

Transmission de la donnée « toto » en **multidiffusion**



1 seul datagramme est envoyé pour tous les destinataires, quelque soit leur nombre.
Le débit à l'arrivé est le débit maximum du réseau.

TCP/IP v4 – Adresses non attribuables

- Parmi les adresses unicast, certaines ne peuvent pas être utilisées pour adresser des hôtes.
  - **0.0.0.0** → **0.255.255.255** : réservées pour l'auto-identification (peu utilisées)
  - **0.0.0.0** : utilisée comme adresse temporaire d'un client DHCP en attente de réception d'un bail.
  - **127.0.0.0** → **127.255.255.255** : réservées pour le bouclage local.
  - **127.0.0.1** : adresse de bouclage local utilisée sur tous les hôtes TCP/IP v4.
  - **Adresses réseaux** : cette adresse permet de définir l'identité d'un réseau IP. Tous les bits de la partie hostid de l'adresse sont à 0.
  - **Adresses de diffusions dirigées** : cette adresse permet d'envoyer des données à toutes les machines ayant un même « netid ».
    Tous les bits de la partie « hostid » de l'adresse sont à 1.
  - **255.255.255.255** : adresse de diffusion limitée (limited broadcast). Cette adresse permet d'envoyer des données à tous les hôtes ayant la couche TCP/IP v4 installée. Ce trafic n'est pas routable.

TCP/IP v4 – Adresses spéciales

- Certaines adresses ont un rôle spécial et sont utilisées dans des contextes particuliers.
- **Adresses privées** : la RFC 1918 (février 1996) a instauré l'utilisation de plages d'adresses privées.
  - Non-routables : les routeurs de l'infrastructure internet ne disposent pas de route vers ces réseaux
  - Utilisables dans tous les réseaux privés. Contrairement à une adresse publique qui doit être unique, il est possible de trouver une même adresse privée dans plusieurs réseaux connectés à internet.
  - Utilisables sans réservation / achat auprès d'un RIR / LIR / NIR / FAI : le choix d'un de ces réseaux est indépendant du fournisseur.

Réseau	Adresse minimum	Adresse maximum	Adresses privées dispo.
10.0.0.0/8	10.0.0.0	10.255.255.255	16 777 216
172.16.0.0/12	172.16.0.0	172.31.255.255	1 048 576
192.168.0.0/16	192.168.0.0	192.168.255.255	65 536

TCP/IP v4 – Adresses spéciales

- **Adresses de type lien local (local link)** : la RFC 3927 (Mai 2005) a normalisé l'utilisation des adresses de type lien local.
  - Utilisées à l'origine par le client DHCP Microsoft : lorsqu'un celui-ci ne réussissait pas à récupérer un bail. (**APIPA** : Automatic Private Internet Protocol Addressing)
  - Cette adresse sert à la communication directe IP entre les hôtes d'un même segment réseau.
  - Une adresse est choisie au hasard dans la plage d'adresses suivante : **169.254.0.0 → 169.254.255.255**
  - Si l'adresse choisie a déjà été affectée à un autre poste sur le segment, une autre adresse sera sélectionnée.
  - Aucun autre paramètre IP (passerelle par défaut, DNS...) sera configurée sur la machine.
- Autres adresses spéciales : quelques autres plages d'adresses ont été réservées par l'**IANA** pour des rôles bien spécifiques (6to4 relai anycast, réseaux de test...etc)
- La page suivante référence toutes les adresses spéciales : http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

TCP/IP v4 – Masque de sous-réseau

- La notion de classe est obsolète car elle ne permet pas de créer des réseaux avec une taille adaptée. Il n'est possible de créer que des réseaux de :
  - 16 777 214 adresses (2^{24}) → classe A
  - 65 534 adresses (2^{16}) → classe B
  - 254 adresses (2^{8}) → classe C
- Ainsi, si une entreprise a besoin de 1000 adresses, elle pourra :
  - Acheter un réseau de classe B ou de classe A ce qui gaspillerait énormément d'adresses.
  - Acheter plusieurs réseaux de classe C (4) ce qui obligerait l'entreprise à router le trafic entre ces 4 réseaux.
- La RFC 950 (août 1985) définit les premiers mécanismes permettant de créer des sous-réseaux par l'intermédiaire de masques de sous-réseaux.
- Le masque n’apparaît dans l'entête IP et un hôte ne connaît pas le masque de l'hôte de destination.

TCP/IP v4 – Masque de sous-réseau

- A l'origine, ce masque sert à créer plusieurs sous-réseaux à partir d'un réseau de classe A, B ou C.
- Actuellement, il est principalement utilisé afin d'identifier la partie « netid » et la partie « hostid » d'une adresse.
- Il s'agit d'une valeur codée sur 32 bit à associer à chaque adresse.
- Si le masque de sous-réseau n'est pas précisé, le « netid » a une taille correspondant à la classe de l'adresse.
- Les bits à 1 dans le masque de sous-réseau identifient les bits correspondants dans l'adresse IP faisant partis du « netid ».
- Les bits à 1 doivent être contigus.
- Deux notations sont possibles :
  - Notation décimale pointée (ex : 255.255.255.0) similaire à la notation de l'adresse IP.
  - Notation CIDR (ex : /24) : le nombre représente la taille (en bits) du « netid »

TCP/IP v4 – Masque de sous-réseau

Not. décimale	Not. CIDR	Notation binaire
128.0.0.0	/1	10000000000000000000000000000000
192.0.0.0	/2	11000000000000000000000000000000
224.0.0.0	/3	11100000000000000000000000000000
240.0.0.0	/4	11110000000000000000000000000000
248.0.0.0	/5	11111000000000000000000000000000
252.0.0.0	/6	11111100000000000000000000000000
254.0.0.0	/7	11111110000000000000000000000000
255.0.0.0	/8	11111111000000000000000000000000
255.128.0.0	/9	11111111100000000000000000000000
255.192.0.0	/10	11111111110000000000000000000000
255.224.0.0	/11	11111111111000000000000000000000
255.240.0.0	/12	11111111111100000000000000000000
255.248.0.0	/13	11111111111110000000000000000000
255.252.0.0	/14	11111111111111000000000000000000
255.254.0.0	/15	11111111111111100000000000000000
255.255.0.0	/16	11111111111111110000000000000000

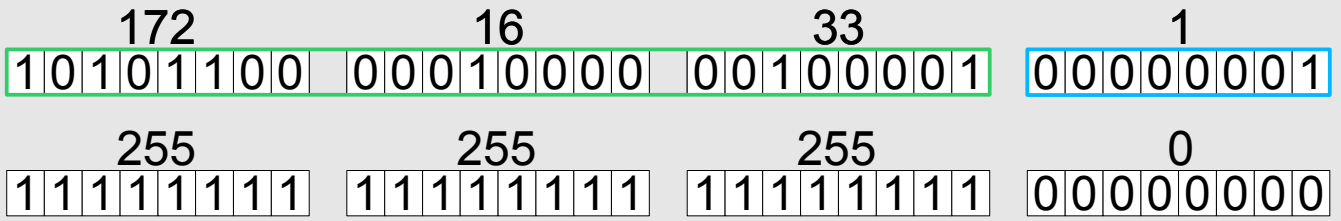
Not. décimale	Not. CIDR	Notation binaire
255.255.128.0	/17	11111111111111111000000000000000
255.255.192.0	/18	11111111111111111100000000000000
255.255.224.0	/19	11111111111111111110000000000000
255.255.240.0	/20	11111111111111111111000000000000
255.255.248.0	/21	11111111111111111111100000000000
255.255.252.0	/22	11111111111111111111110000000000
255.255.254.0	/23	11111111111111111111111000000000
255.255.255.0	/24	11111111111111111111111100000000
255.255.255.128	/25	11111111111111111111111110000000
255.255.255.192	/26	11111111111111111111111111000000
255.255.255.224	/27	11111111111111111111111111100000
255.255.255.240	/28	11111111111111111111111111110000
255.255.255.248	/29	11111111111111111111111111111000
255.255.255.252	/30	11111111111111111111111111111100
255.255.255.254	/31	11111111111111111111111111111110
255.255.255.255	/32	11111111111111111111111111111111

TCP/IP v4 – Masque de sous-réseau

`172. 16. 33.1`
`255.255.255.0`

peut s'écrire `172.16.33.1`**`/24`**

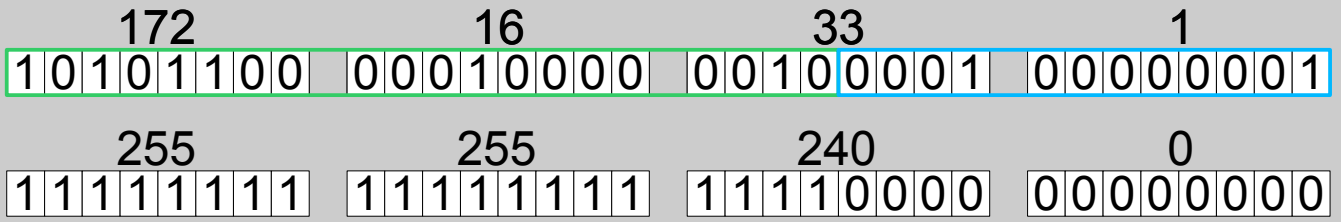
Il s'agit d'une adresse de classe B mais le masque impose la taille du « netid »



`172. 16. 33.1`
`255.255.240.0`

peut s'écrire `172.16.33.1`**`/20`**

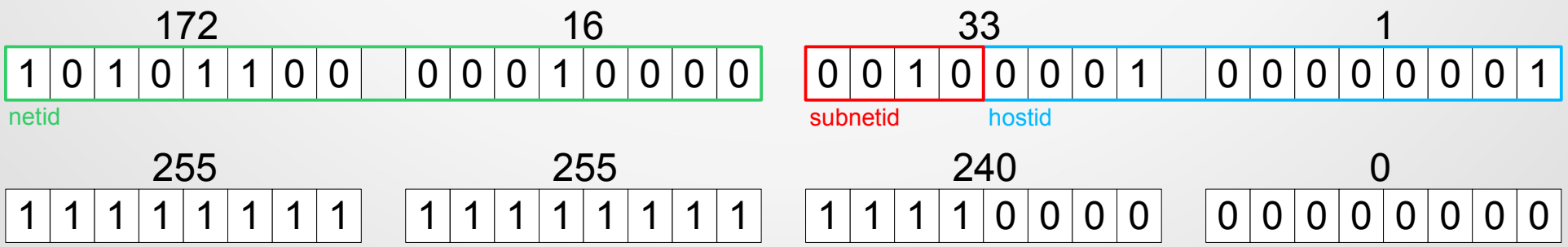
Il s'agit d'une adresse de classe B mais le masque impose la taille du « netid »



TCP/IP v4 – Masque de sous-réseau

- A l'origine, ce masque de sous-réseau permettait de mettre en évidence un identifiant de sous réseau (*subnetid*).
- La RFC 950 ne permettait pas que ce « *subnetid* » soit entièrement à 0 (binaire) ou entièrement à 1 (binaire).
- La RFC 1878 a autorisé ces deux valeurs.
- Étant donné que tous les appareils actuels sont conformes à la RFC 1878, cette notion n'a plus lieu d'être.

Dans l'exemple ci-dessous, 172.16.33.1 est une adresse de classe B. Les 2 premiers octets sont donc le « netid » de l'adresse.
Le masque (255.255.240.0) permettent de mettre en évidence le « subnetid » qui est situé sur les 4 premiers bits du 3° octet.



TCP/IP v4 – Masque de sous-réseau

- A partir d'une adresse IP et d'un masque de sous-réseau, il est possible de calculer plusieurs valeurs.
  - Adresse réseau : partie « hostid » à 0 en binaire
  - Adresse de diffusion dirigée : partie « hostid » à 1 en binaire
  - Plus petite adresse attribuable : adresse réseau + 1 au dernier octet.
  - Plus grande adresse attribuable : adresse de diffusion dirigée – 1 au dernier octet.
  - Nombre d'adresses attribuables : $2^n - 2$

TCP/IP v4 – Masque de sous-réseau

Adresse IP / Masque	11000000.10101000.00001010.00001000
	192. 168. 10. 4/21
Adresse réseau	11000000.10101000.00001000.00000000
	192.168.8.0
Adresse de diffusion dirigée	11000000.10101000.00001111.11111111
	192.168.15.255
Adresse minimum attribuable	11000000.10101000.00001000.00000001
	192.168.8.1
Adresse maximum attribuable	11000000.10101000.00001111.11111110
	192.168.15.254
Nombre d'adresses attribuables	$2^{(32-21)}-2 = 2^{11} - 2$
	2046

TCP/IP v4 – Sous-réseaux

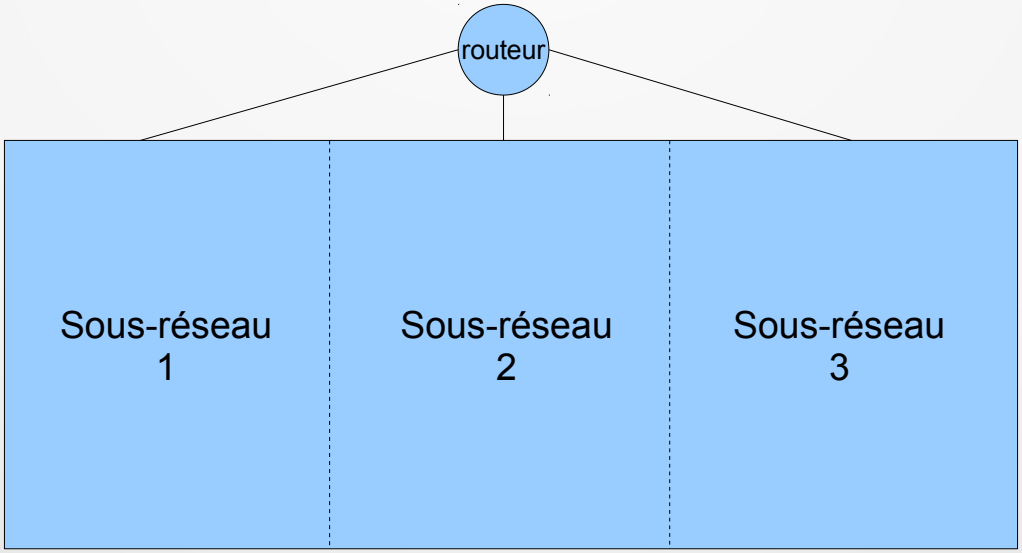
- La technique du « **subnetting** » (création de sous-réseaux) consiste à découper un réseau en plusieurs sous-réseaux afin de pouvoir le segmenter.
- L'intérêt d'utiliser plusieurs sous-réseaux est multiple :
  - **Sécurité** : les sous-réseaux seront indépendants et pourront communiquer uniquement en passant par un routeur / pare-feu.
  - **Performance** : domaines de collision / diffusion limités
  - **Architecture** : utilisation des technologie réseaux différentes (Ethernet, Wifi...)
- Deux techniques de création de sous-réseaux existent :
  - **CIDR** : Classless InterDomain Routing
  - **VLSM** : Variable Length Subnet Mask
- L'utilisation d'adresses privées rend les techniques de subnetting moins importantes dans de nombreuses situations.

TCP/IP v4 – Sous-réseaux - CIDR

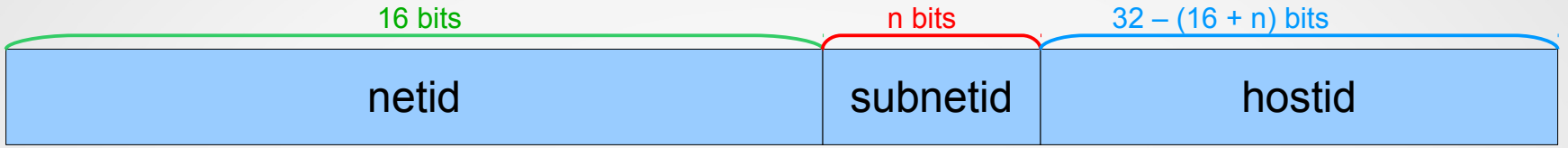
- Cette technique consiste à créer un nombre de sous-réseaux défini disposant du même masque.
- Permet d'obtenir un nombre maximal d'adresses pour chaque sous-réseau créé.
- Ne met pas l'accent sur l'économie des plages d'adresses.
- Plutôt adaptée pour les réseaux d'entreprise disposant d'une plage d'adresse initiale largement suffisante.

TCP/IP v4 – Sous-réseaux – CIDR - Exemple

- Nous disposons de la plage d'adresse 172.16.0.0/16 pour notre réseau.
- Pour des raisons de sécurité, nous souhaitons utiliser 3 réseaux IP.
- Pour chacun de ces réseaux IP, il faut qu'un maximum d'adresses soient disponibles.



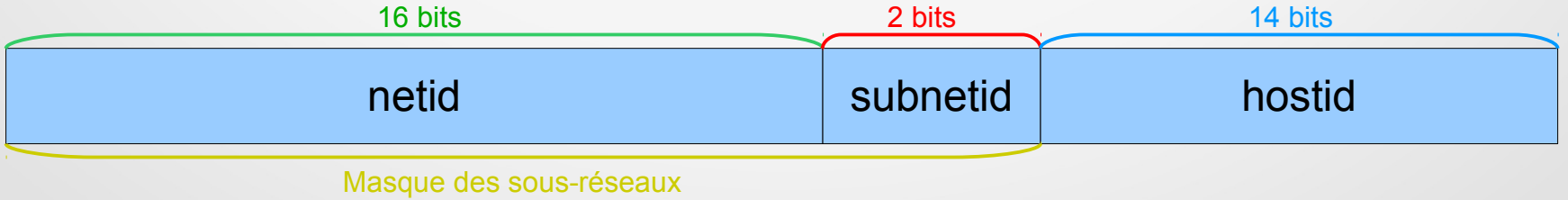
TCP/IP v4 – Sous-réseaux – CIDR - Exemple



- 3 sous-réseaux = le « subnetid » doit permettre de coder 3 valeurs minimum

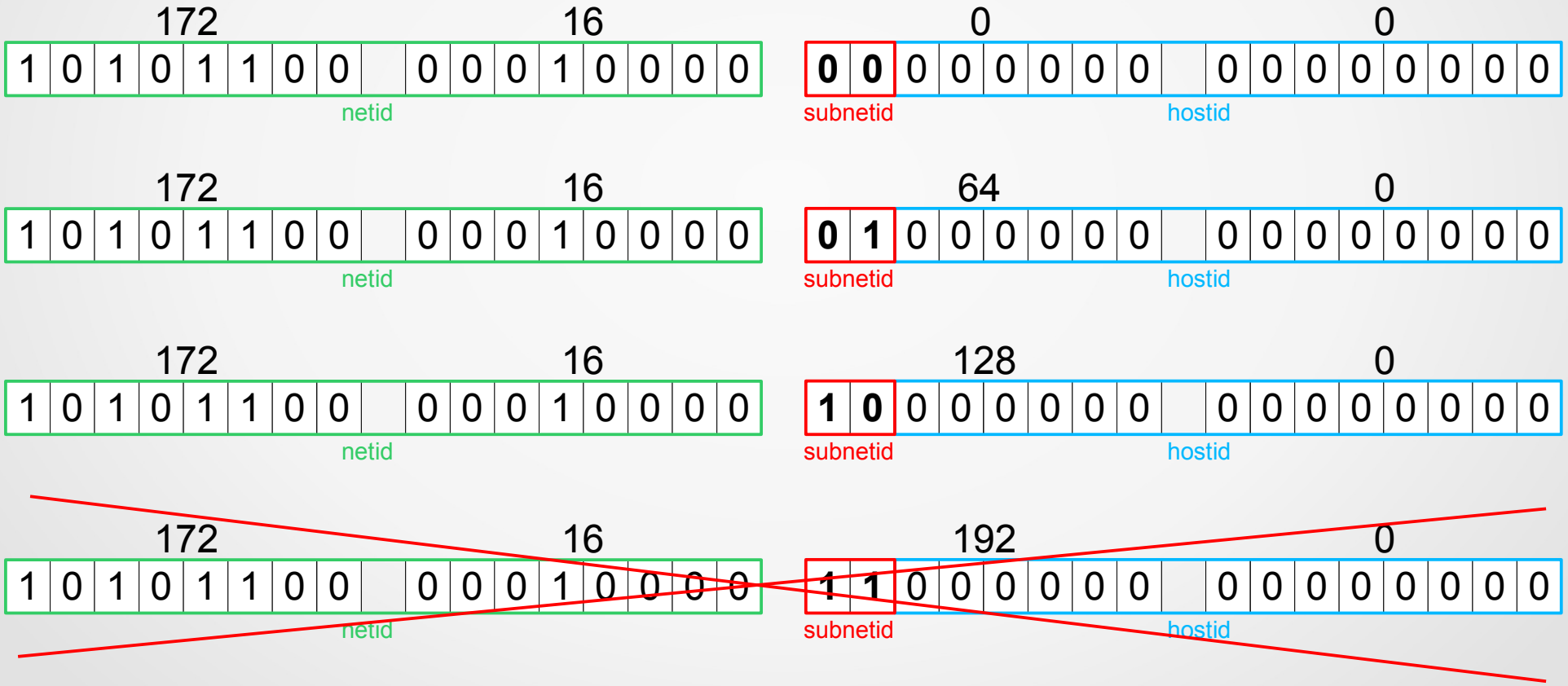
$$2^n = 3 \Leftrightarrow n = \frac{\ln 3}{\ln 2} \simeq 1{,}58496$$

- Il faut donc au minimum 2 bits pour coder 3 valeurs dans le « subnetid ».
- Il sera possible de créer 4 sous-réseaux mais seuls 3 d'entre eux vont nous intéresser
- Le masque des sous-réseaux aura une taille de 18 bits : /18 (255.255.192.0)



TCP/IP v4 – Sous-réseaux – CIDR - Exemple

Voici les 4 sous-réseaux possibles en faisant varier les 2 bits du « subnetid ».
Nous ne retenons que les 3 premiers.



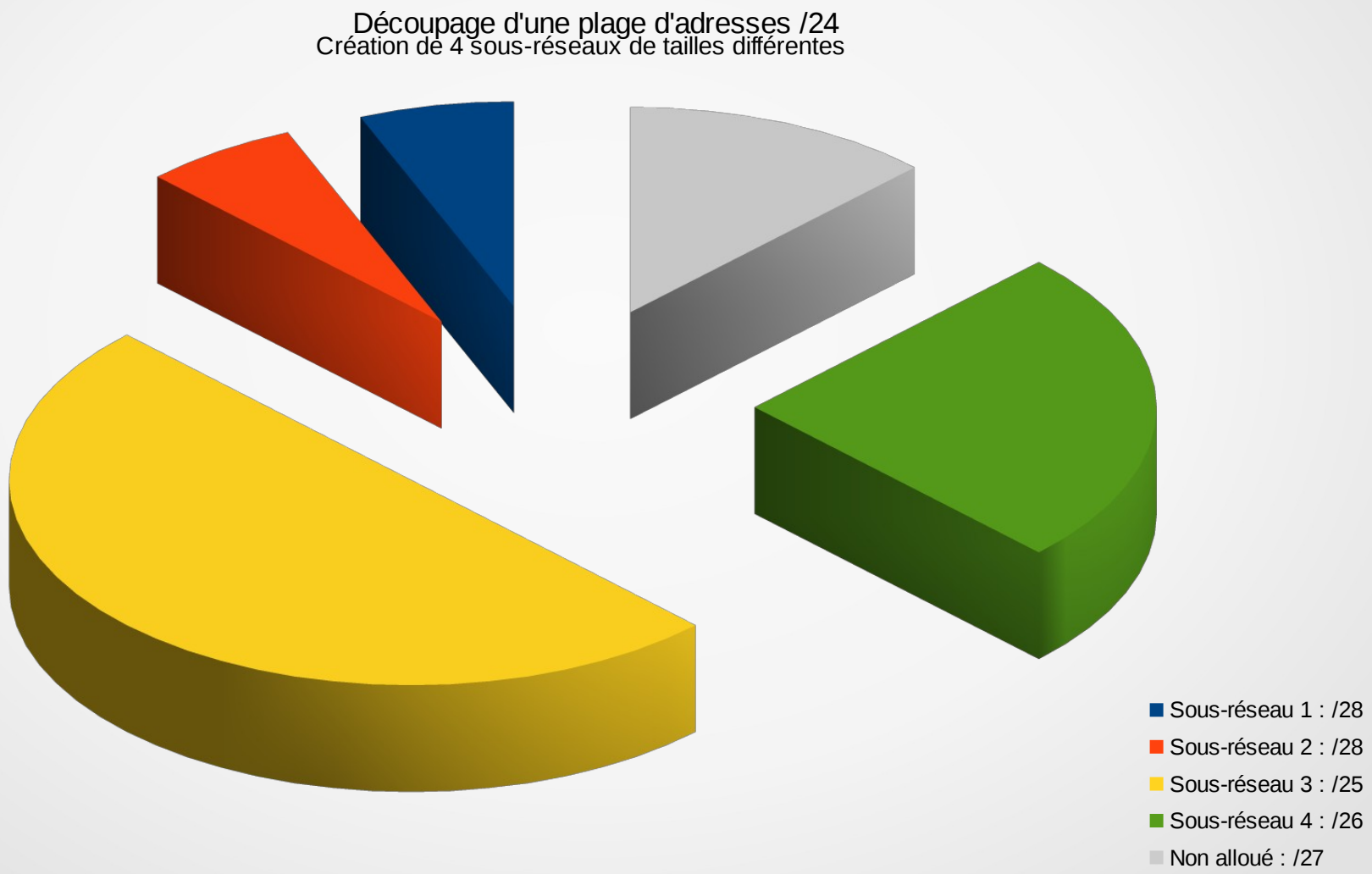
TCP/IP v4 – Sous-réseaux – CIDR - Exemple

	Sous-réseau 1	Sous-réseau 2	Sous-réseau 3
Adresse de sous-réseau	**172.16.0.0**	**172.16.64.0**	**172.16.128.0**
Masque de sous-réseau		**/18** **255.255.192.0**	
Adresse de diffusion dirigée	172.16.63.255	172.16.127.255	172.16.191.255
Adresse minimum attribuable	172.16.0.1	172.16.64.1	172.16.128.1
Adresse maximum attribuable	172.16.63.254	172.16.127.254	172.16.191.254
Nombre d'adresses attribuables		$2^{(32-18)}-2 = 2^{14}-2 =$ **4094**	

TCP/IP v4 – Sous-réseaux - VLSM

- La technique précédente permet de créer des sous-réseaux de taille équivalente (même masque).
- Pas forcément adapté à toutes les situations.
- Une entreprise disposant de plages d'adresses assez réduites peut vouloir créer des sous-réseaux de tailles différentes et adaptées afin de laisser des plages d'adresses pour de futurs sous-réseaux.
- Cas des fournisseurs d'accès Internet :
  - Ils disposent de plages d'adresses très réduites et la pénuries d'adresses IPv4 n'arrange pas les choses.
  - Leurs clients ont besoin de plages d'adresses adaptées à ce qu'ils veulent faire. Une plage trop grande coûtera trop cher.
- **VLSM (Variable Length Subnet Mask)** permet de créer plusieurs sous réseaux de tailles différentes (masques différents).

TCP/IP v4 – Sous-réseaux - VLSM

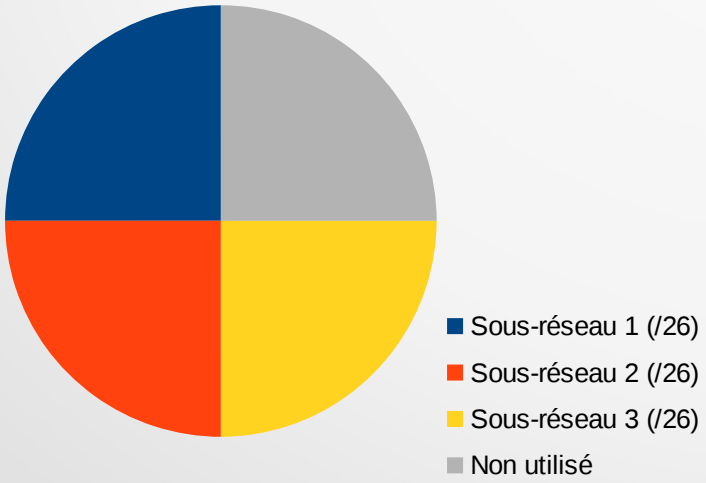


TCP/IP v4 – Sous-réseaux - VLSM

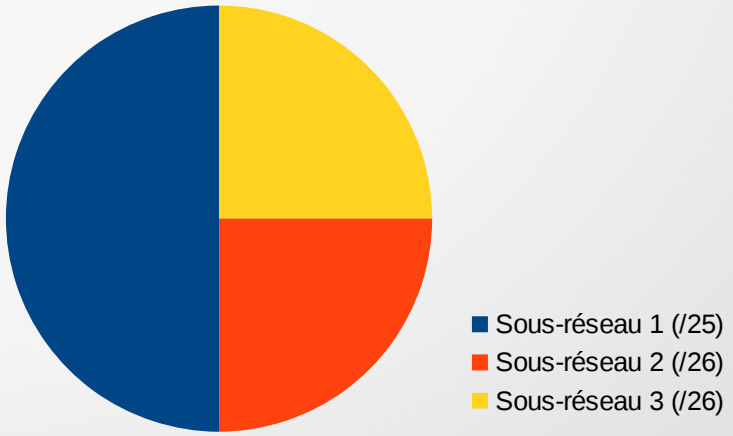
- VLSM permet de répondre à des cas non solubles par CIDR.

Exemple :
Nous disposons d'un /24 et nous voulons créer 3 sous-réseaux :
• 1 de 100 machines
• 2 de 50 machines

CIDR
Création de 3 sous-réseaux en /26 (64 adresses)



VLSM
Création d'un /25 (126 adresses) et de 2 /26 (62 adresses)

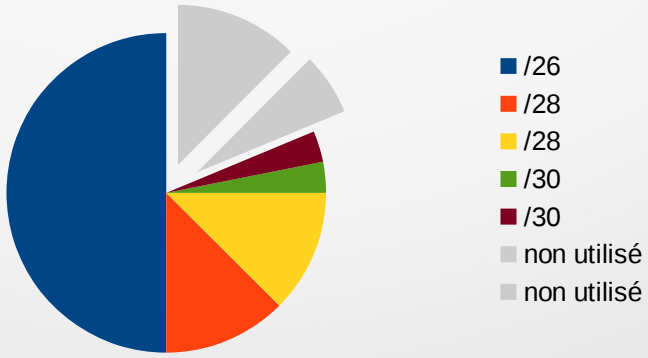


TCP/IP v4 – Sous-réseaux – VLSM - Exemple

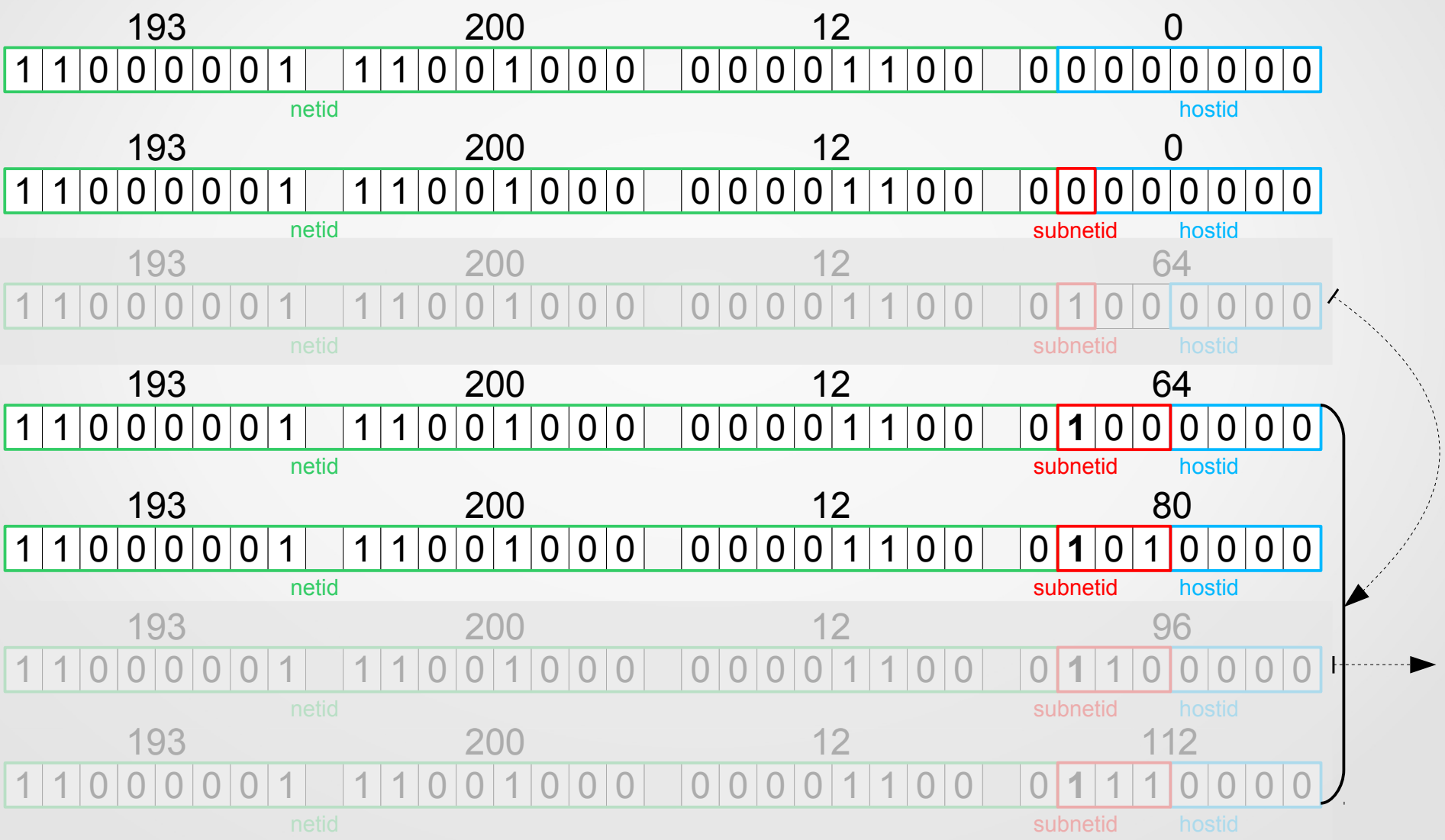
*Nous disposons de la plage d'adresse **193.200.12.0/25**.*
Nous souhaitons attribuer :
- *1 réseau de 50 adresses*
- *2 réseaux de 15 adresses*
- *2 réseaux de 2 adresses*

1.Trouver les masques de sous-réseaux à utiliser.

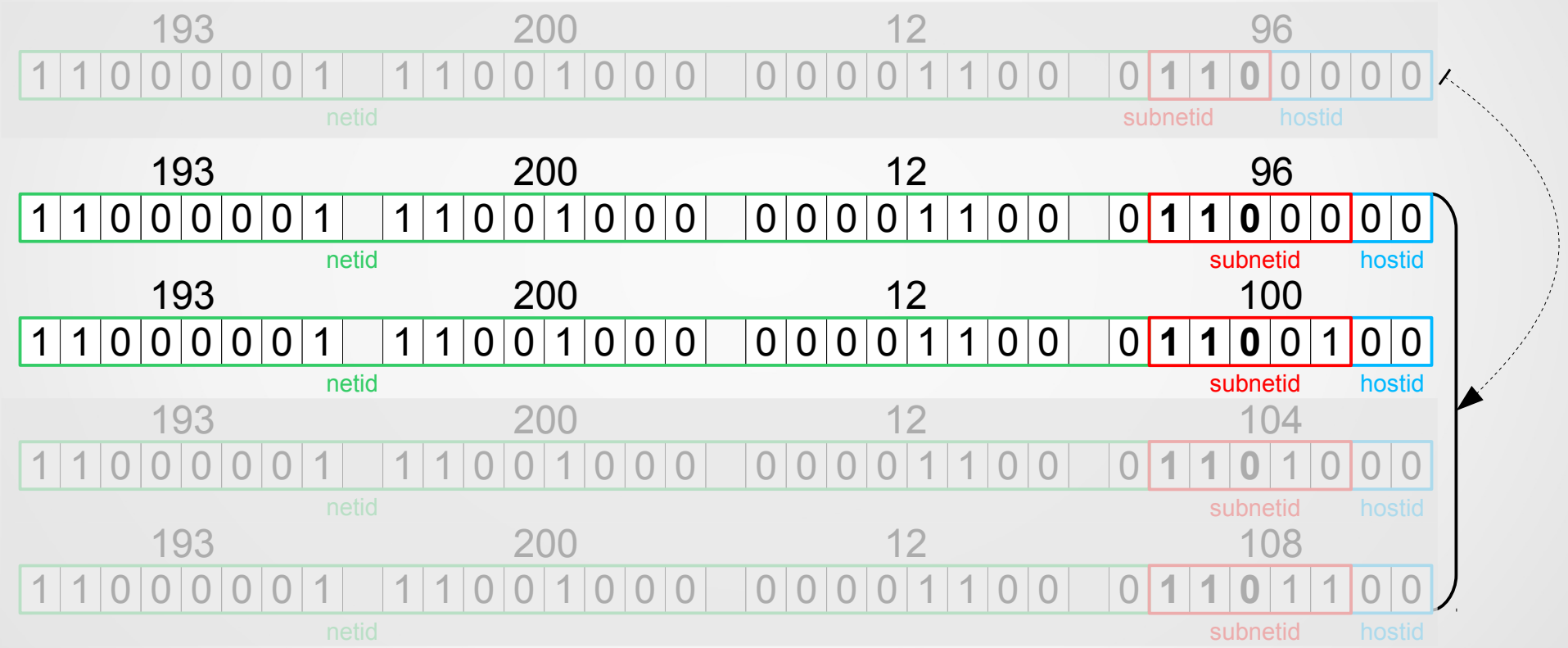
Réseaux	Nombre	Taille du « hostid » (bits)	Taille du « netid » (bits)
50 adresses	1	6	**/26**
15 adresses	2	4	**/28**
2 adresses	2	2	**/30**



TCP/IP v4 – Sous-réseaux – VLSM - Exemple



TCP/IP v4 – Sous-réseaux – VLSM - Exemple

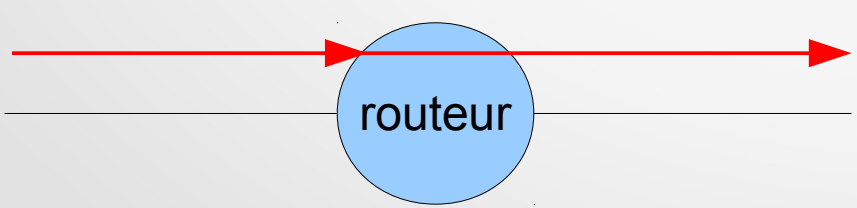


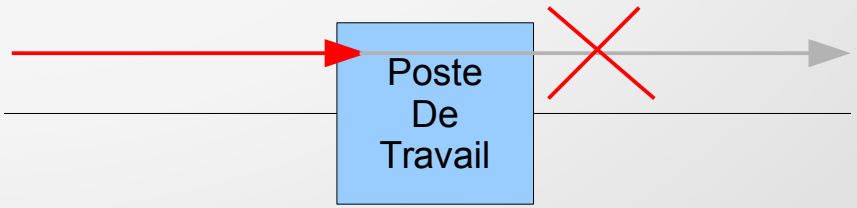
TCP/IP v4 – Sous-réseaux – VLSM - Exemple

	Sous-réseau 1	Sous-réseau 2	Sous-réseau 3	Sous-réseau 4	Sous-réseau 5
Adresse de sous-réseau	193.200.12.0	193.200.12.64	193.200.12.80	193.200.12.96	193.200.12.100
Masque de sous-réseau	/26 255.255.255.192	/28 255.255.255.240	/28 255.255.255.240	/30 255.255.255.252	/30 255.255.255.252
Adresse de diffusion dirigée	193.200.12.63	193.200.12.79	193.200.12.95	193.200.12.99	193.200.13.103
Adresse minimum attribuable	193.200.12.1	193.200.12.65	193.200.12.81	193.200.12.97	193.200.12.101
Adresse maximum attribuable	193.200.12.62	193.200.12.78	193.200.12.94	193.200.12.98	193.200.12.102
Nombre d'adresses attribuables	$2^6 - 2 =$ **62**	$2^4 - 2 =$ **14**	$2^4 - 2 =$ **14**	$2^2 - 2 =$ **2**	$2^2 - 2 =$ **2**

TCP/IP v4 - Routage

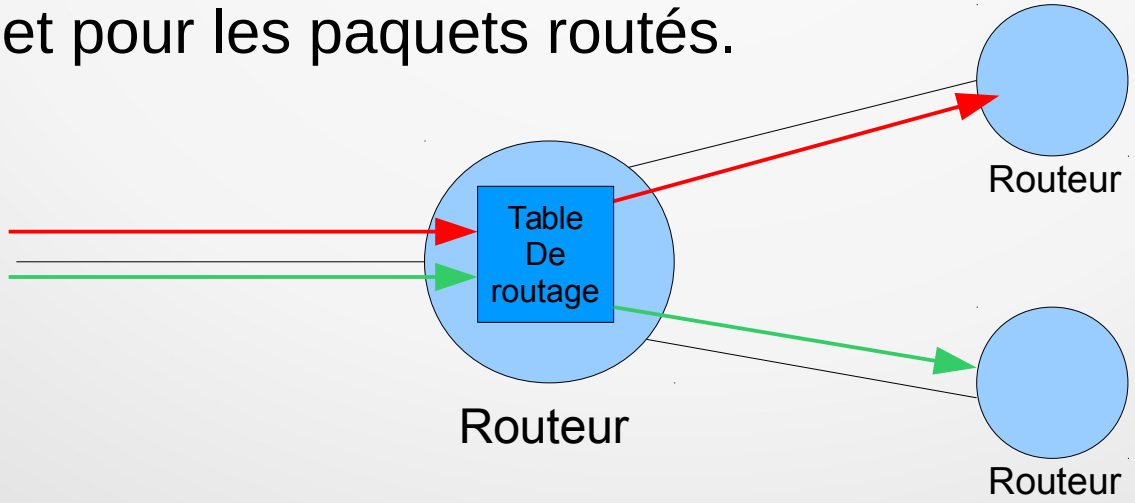
- Le routage est l'opération qui consiste à transmettre un datagramme IP entrant vers un autre réseau.
- Cette opération est réalisée par les routeurs.
- Habituellement, un datagramme entrant, dont l'IP de destination n'est pas celle du poste, est rejeté.
- La fonctionnalité de routage peut être activée sur quasiment tous les systèmes équipés de la couche TCP/IP.
- Un routeur doit être équipé au minimum de 2 interfaces réseaux.





TCP/IP v4 : Routage

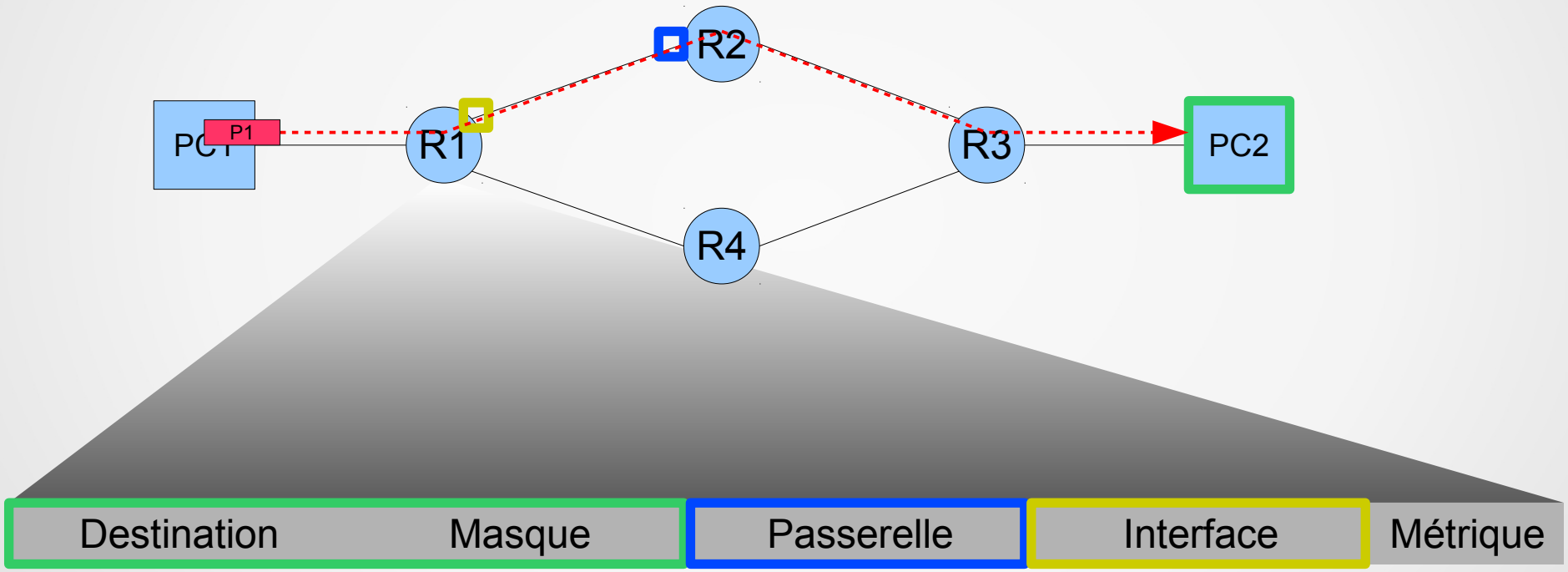
- La table de routage est l'organe d'un système TCP/IP permettant de définir comment et à qui envoyer un datagramme.
- Tout système IP dispose d'une table de routage.
- Un système non routeur analysera sa table de routage uniquement pour les paquets sortants émis par le poste.
- Un routeur analysera sa table de routage pour les paquets sortant et pour les paquets routés.



TCP/IP v4 : Routage

- La table de routage est composé de plusieurs champs
  - **Destination / Masque** : La combinaison de ces 2 champs permet de spécifier quelles sont les adresses IP de destination concernées par la route.
  - **Passerelle** : Adresse IP du routeur auquel envoyer le datagramme pour joindre la destination.
  - **Interface** : interface physique par laquelle le datagramme sera envoyé.
  - **Métrique** : indice donné à une route pour caractériser la longueur de celle-ci. Cela permet essentiellement de privilégier une route quand 2 routes mènent à la même destination.

TCP/IP v4 : Routage



TCP/IP v4 : Routage

Formalisme UNIX/Linux

Destination	Masque	Passerelle	Interface	Métrique
192.168.0.0	255.255.255.0	0.0.0.0	eth0	1
192.168.1.0	255.255.255.0	192.168.0.254	eth0	1
192.168.255.0	255.255.255.0	0.0.0.0	eth1	1
193.200.12.5	255.255.255.255	192.168.0.253	eth0	1
0.0.0.0	0.0.0.0	192.168.0.252	eth0	1

Formalisme Microsoft

Destination	Masque	Passerelle	Interface	Métrique
192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.1	1
192.168.1.0	255.255.255.0	192.168.0.254	192.168.0.1	1
192.168.255.0	255.255.255.0	192.168.255.1	192.168.255.1	1
193.200.12.5	255.255.255.255	192.168.0.253	192.168.0.1	1
0.0.0.0	0.0.0.0	192.168.0.252	192.168.0.1	1

TCP/IP v4 : Routage

192.168.2.10

192.168.1.1

192.168.0.254

10.0.0.1

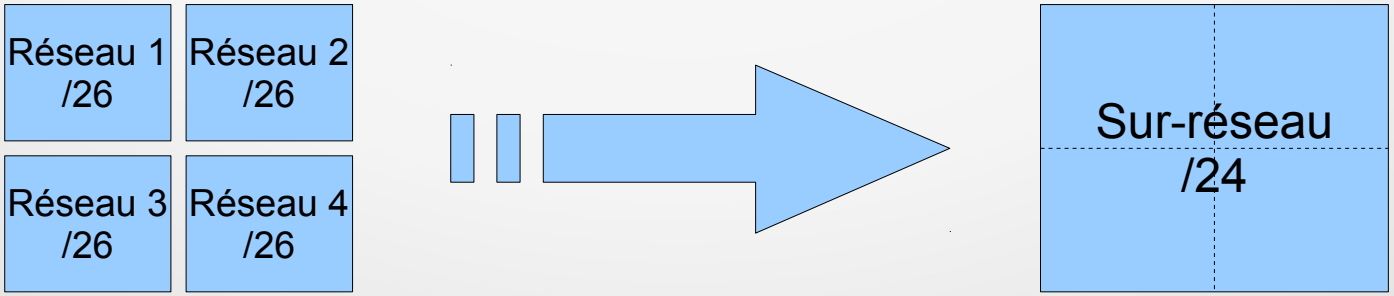
193.200.12.5

8.8.8.8

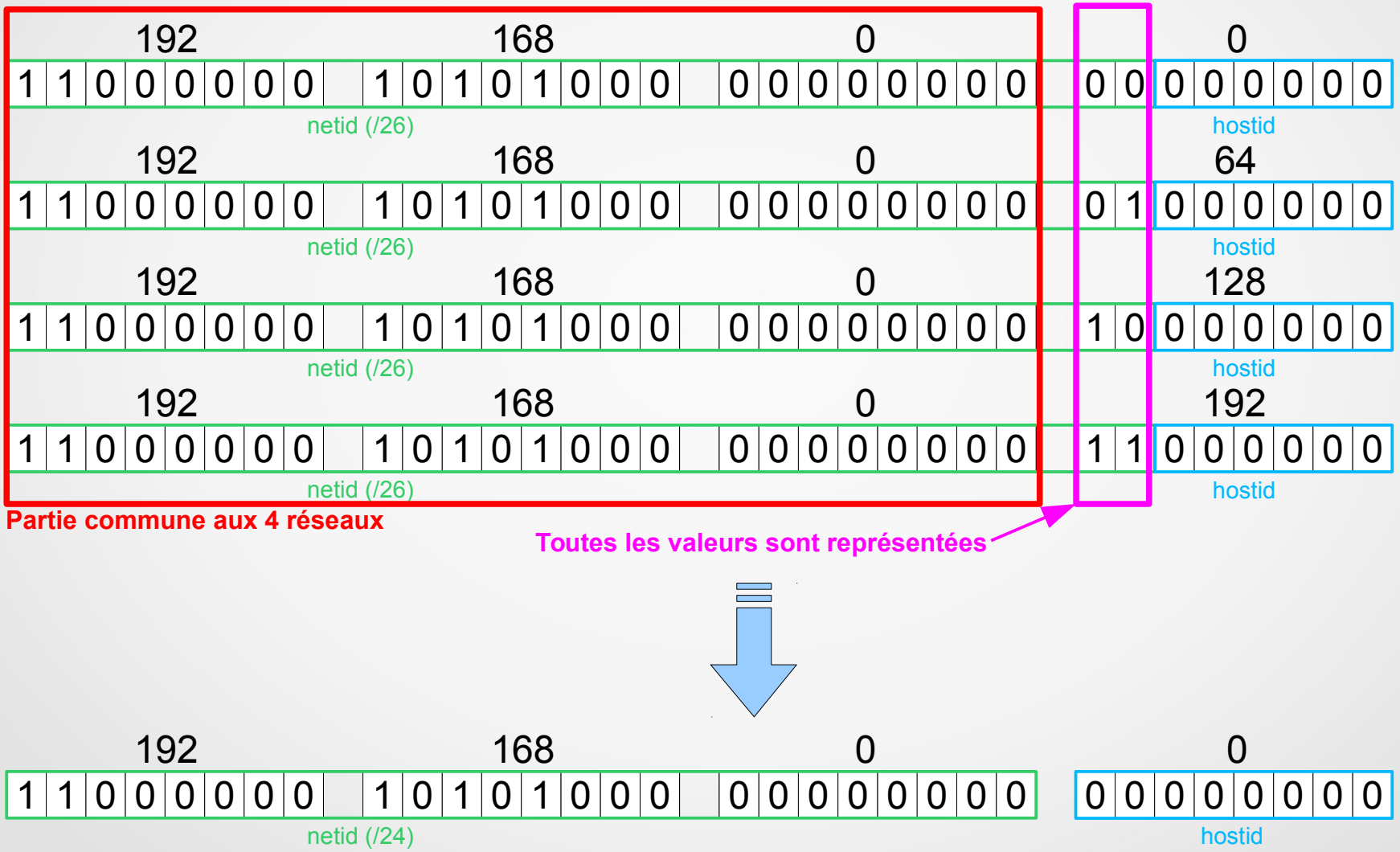
Destination	Masque	Passerelle	Interface	Métrique
192.168.0.0	255.255.255.0	0.0.0.0	eth0	1
192.168.1.0	255.255.255.0	192.168.0.254	eth0	1
193.200.12.5	255.255.255.255	192.168.0.253	eth0	1
192.168.2.0	255.255.255.0	192.168.0.254	eth0	1
192.168.2.0	255.255.255.0	192.168.0.253	eth0	2
0.0.0.0	0.0.0.0	192.168.0.252	eth0	1

TCP/IP v4 : Routage – résumés de route

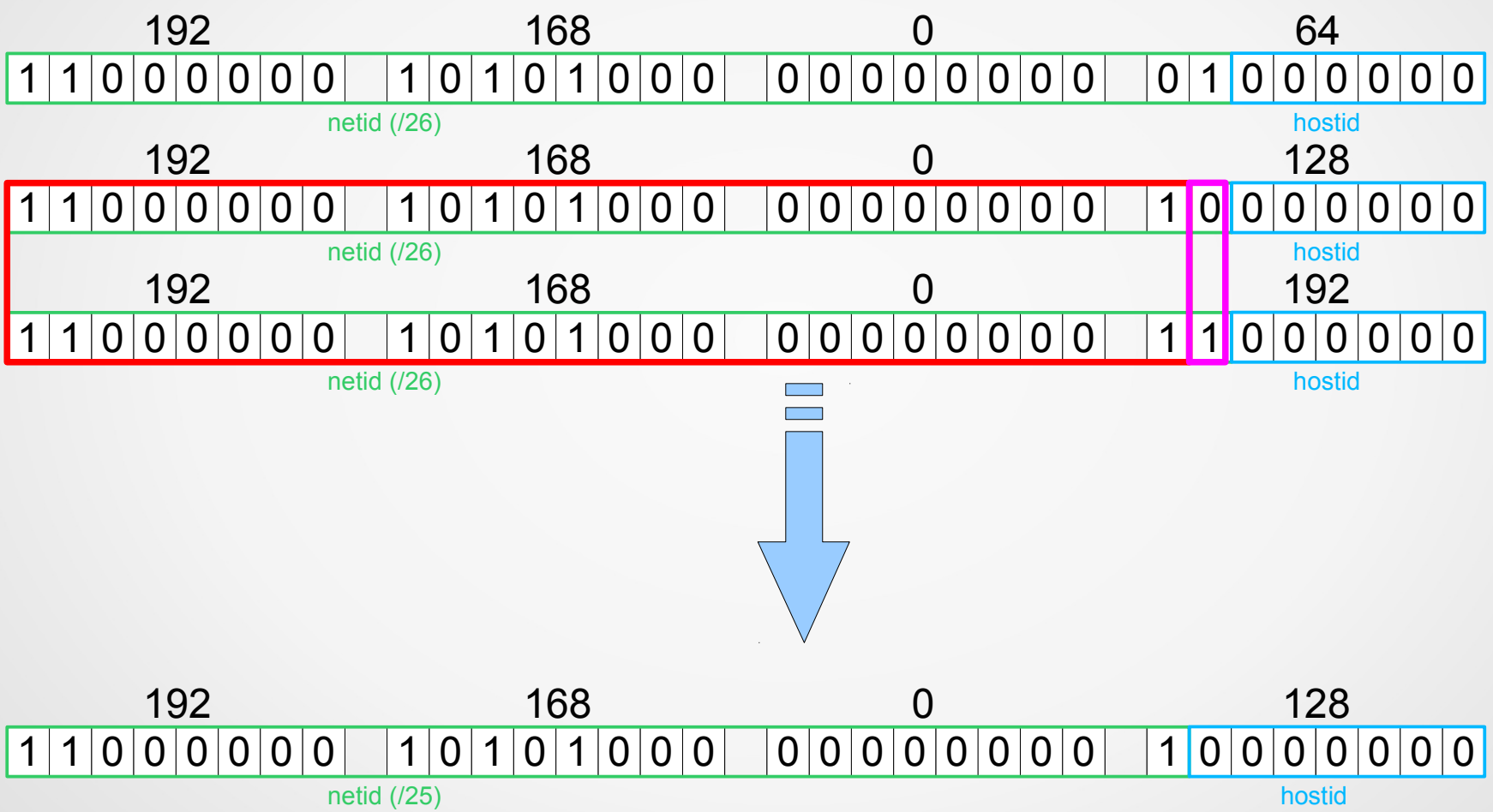
- Le résumé de route (**agrégation de routes**) consiste à regrouper plusieurs routes en une seule.
- L'objectif est de diminuer la taille des tables de routage et d'améliorer les performances des routeurs.
- La technique utilisée s'appelle le « **supernetting** » par opposition au « subnetting ».
- Le but est de trouver un « sur-réseau » contenant un ensemble de réseaux. Il s'agit de retrouver le réseau à partir duquel nous aurions pu créer les sous-réseaux actuels.
- Le masque du sur-réseau sera plus court.
- Peut servir à adresser un seul réseau IP à partir de plusieurs réseaux.
  Par exemple, si on dispose de 4 plages d'adresses en /26 contiguës, il est possible d'utiliser un sur-réseau en /24.



TCP/IP v4 : Routage – résumés de route

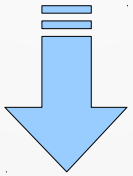


TCP/IP v4 : Routage – résumés de route



TCP/IP v4 : Routage – résumés de route

Destination	Masque	Passerelle	Interface	Métrique
192.168.33.0	255.255.255.0	0.0.0.0	eth0	1
192.168.0.64	255.255.255.192	192.168.0.254	eth0	1
192.168.0.128	255.255.255.192	192.168.0.254	eth0	1
192.168.0.192	255.255.255.192	192.168.0.254	eth0	1
0.0.0.0	0.0.0.0	192.168.0.252	eth0	1



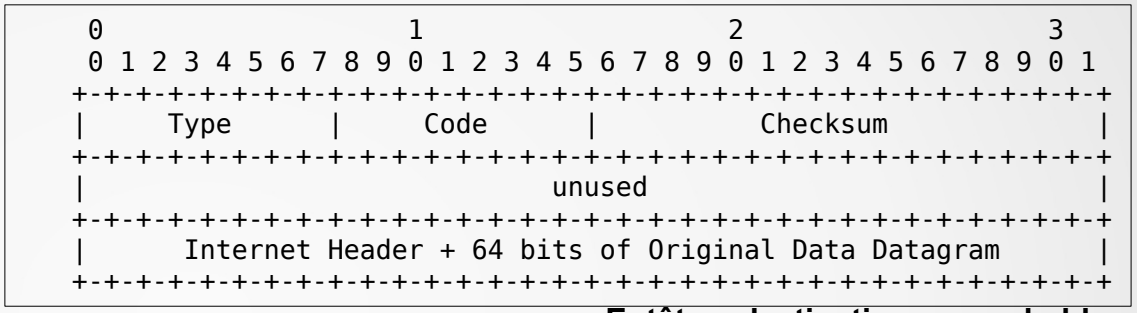
Destination	Masque	Passerelle	Interface	Métrique
192.168.33.0	255.255.255.0	0.0.0.0	eth0	1
192.168.0.64	255.255.255.192	192.168.0.254	eth0	1
192.168.0.128	255.255.255.128	192.168.0.254	eth0	1
0.0.0.0	0.0.0.0	192.168.0.252	eth0	1

TCP/IP v4 - ICMP

- ICMP (Internet Control Message Protocol) est le protocole permettant d'envoyer des messages de natures diverses aux hôtes d'une communication IP.
- Pas indispensable mais utile pour contrôler le fonctionnement d'une communication IP.
- Les commandes « ping » et « traceroute » utilisent ce protocole.
- Il est possible d'activer ou de désactiver ces messages ICMP sur la plupart des systèmes.

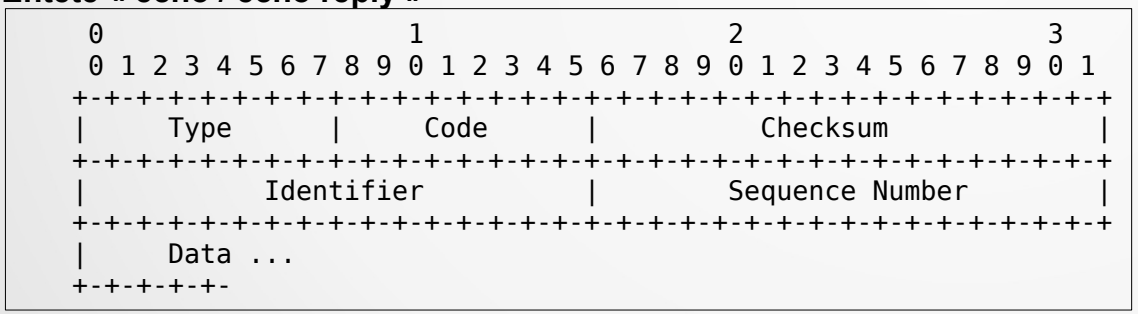
TCP/IP v4 - ICMP

L'entête ICMP varie en fonction du message. Seuls les 4 premiers octets sont communs.

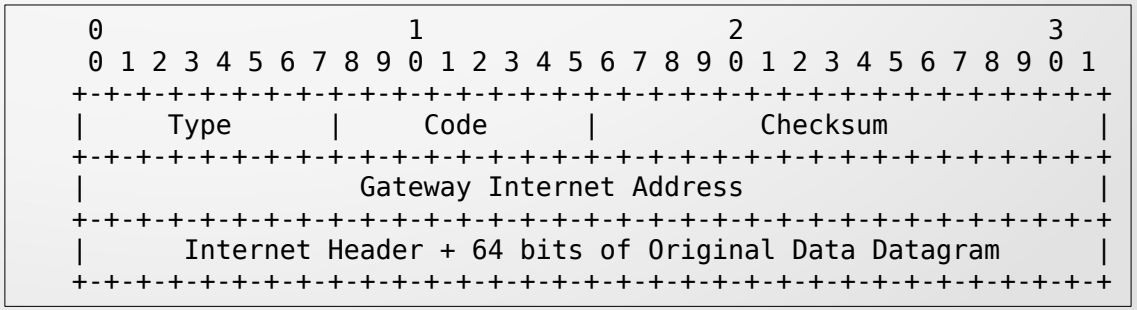


Entête « destination unreachable »

Entête « echo / echo reply »



Entête « redirect »



TCP/IP v4 - ICMP

- Le champ « Type » permet d'identifier la catégorie de message ICMP.

Type	Signification
0	Echo reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench (Deprecated)
5	Redirect
6	Alternate Host Address (Deprecated)
7	Unassigned
8	Echo
9	Unassigned

Type	Signification
10	Unassigned
11	Time exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp reply
15	Information request (deprecated)
16	Information reply (deprecated)
17	Address Mask Request (deprecated)
18	Address Mask Reply (deprecated)

TCP/IP v4 - ICMP

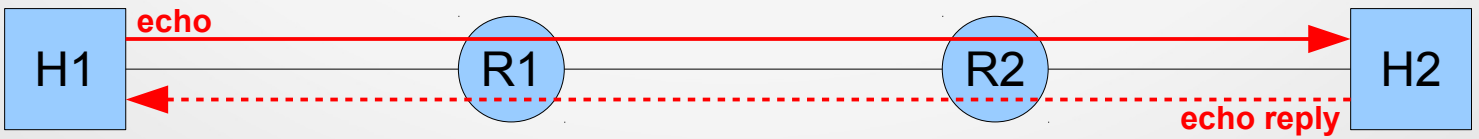
- Le champ « Code » précise la nature du message en fonction du « Type ».
- Il y a une liste de codes pour chaque type.
- De nombreux types ne disposent que du code « 0 ».

Codes	Description
0	Net Unreachable
1	Host unreachable
2	Protocol Unreachable
3	Port unreachable
4	Fragmentation Needed and Don't Fragment was set
5	Source route failed
6	Destination Network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network is administratively prohibited
10	Communication with destination host is administratively prohibited
11	Destination network unreachable for type of service
12	Destination host unreachable for type of service
13	Communication administratively prohibited
14	Host precedence violation
15	Precedence cutoff in effect

Table des codes pour le type 3 « Destination unreachable »

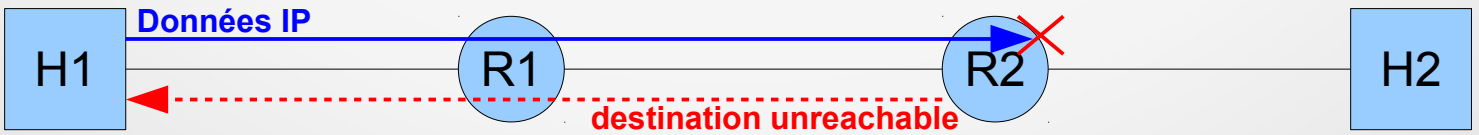
TCP/IP v4 – ICMP – echo / echo reply

- echo (type 8), echo reply (type 0)
- Utilisé principalement par la commande « ping »
- Permet de tester la connectivité IP entre 2 hôtes.
- Permet de mesurer la latence entre 2 hôtes.
- Est souvent bloqué par des pare-feu.
- Utilisé par « traceroute » afin de trouver les routeurs situés entre 2 hôtes.



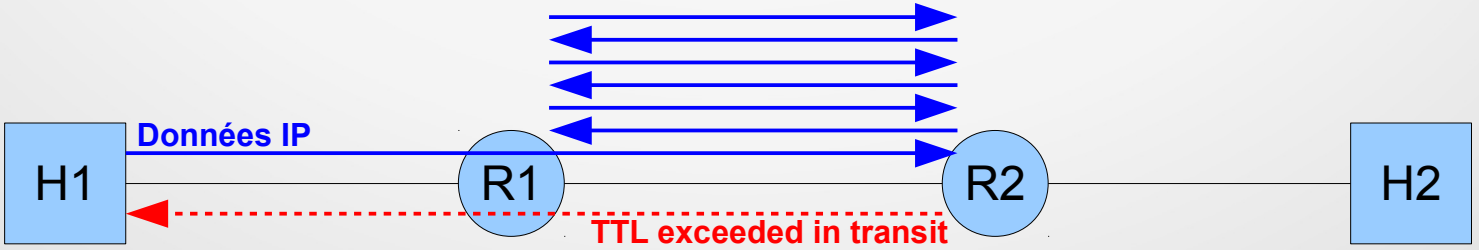
TCP/IP v4 – ICMP – Destination unreachable

- Type 3
- Permet de spécifier à l'émetteur que la destination n'est pas joignable.
- Le code permet de préciser la cause de ce dysfonctionnement (réseau injoignable, port bloqué, ...etc)



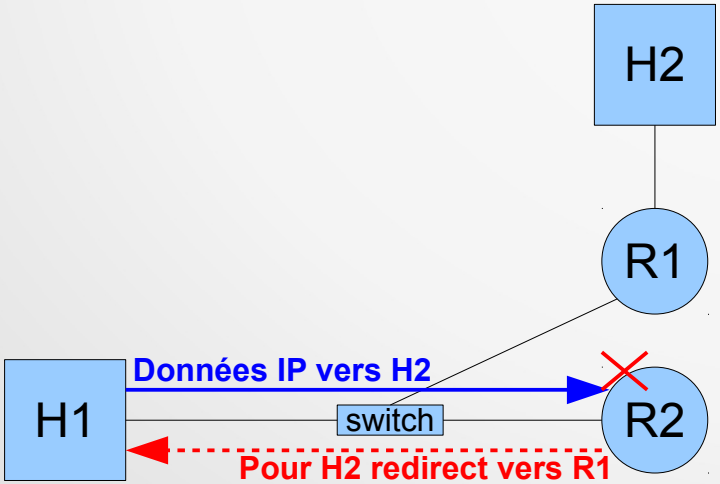
TCP/IP v4 – ICMP – Time exceeded

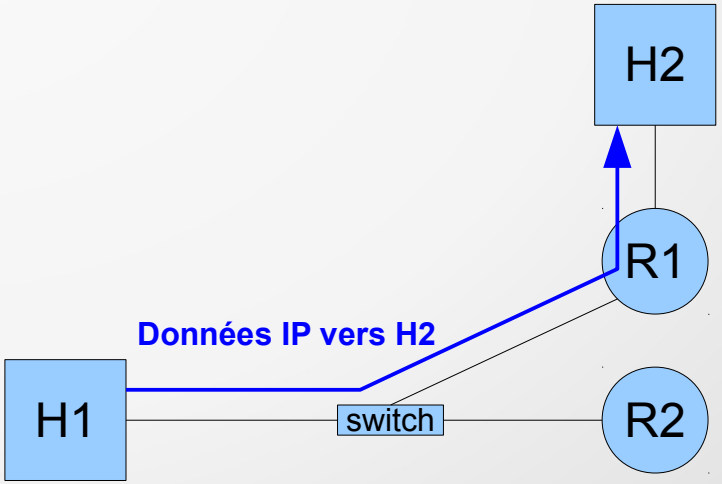
- Type 11
- Intervient lorsque que le TTL expire ou lorsque que le temps de ré-assemblage des fragments est expiré.
- Cause de l'expiration du TTL :
  - Bouclage de routes
  - TTL initial trop faible



TCP/IP v4 – ICMP – Redirect

- Type 5
- Intervient lorsque qu'un routeur détecte que la route utilisée par l'émetteur n'est pas optimale.
- Le routeur envoie à l’émetteur l'adresse du routeur à utiliser.



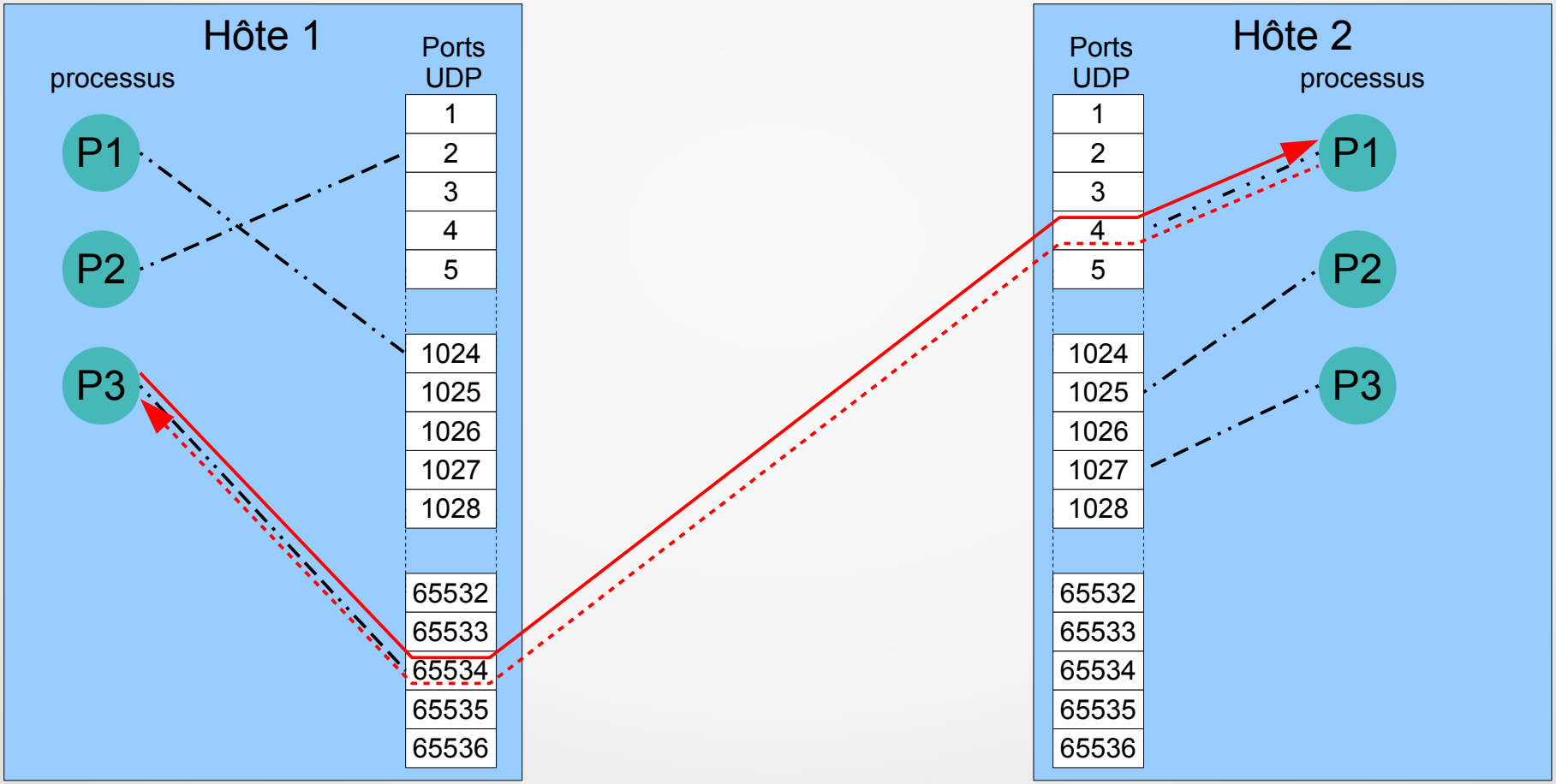


TCP/IP v4 - UDP

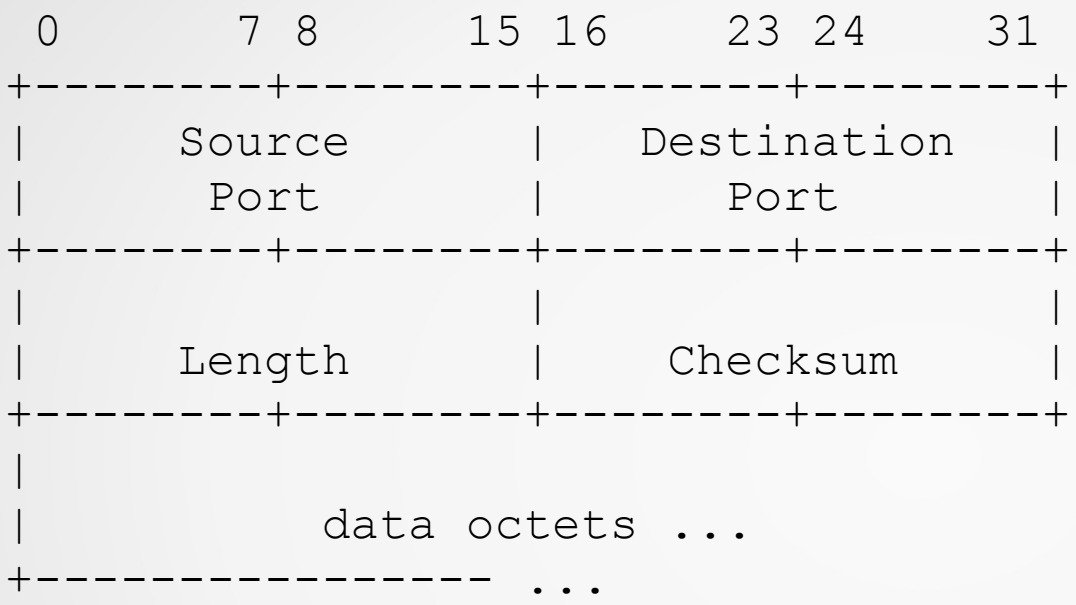
- UDP (User Datagram Protocol) est un protocole de la couche Transport (4).
- Son rôle est de transmettre des données d'un processus sur un hôte à un processus sur un autre hôte.
- Un processus voulant utiliser UDP devra être lié à un numéro de **port de service**.
- UDP est un protocole **non connecté** : il ne garanti pas la fiabilité de la transmission.
- UDP ne peut pas préciser à l'émetteur si le paquet est bien arrivé sur le destinataire.
- UDP ne peut pas réguler le débit d'émission des données. C'est au processus de réaliser cette opération.
- UDP est adapté pour :
  - Transmissions de données de petites tailles ne nécessitant **pas de segmentation** (taille <= MTU).
  - Transmissions de paquets vers des destinations « **multicast** » ou « **broadcast** ».
  - Transmissions peu consommatrices de ressources (peu de paramètres à gérer)
  - Transmissions proches du **temps réel** (pas de latence induite par le protocole)

TCP/IP v4 - UDP

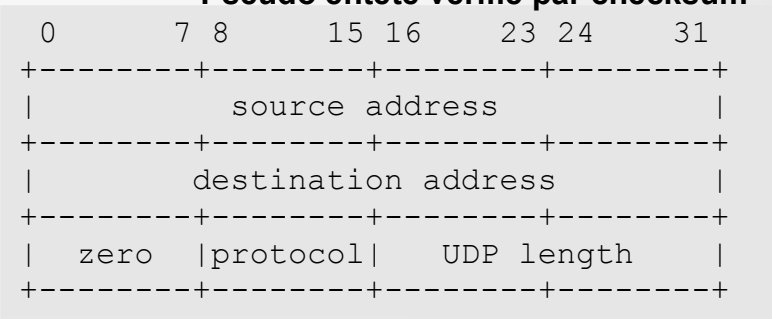
Communication UDP entre les processus de 2 hôtes



TCP/IP v4 - UDP



Pseudo entête vérifié par checksum



- Source port (16 bits) : port de l'émetteur du paquet
- Destination port (16 bits) : port du destinataire du paquet
- Length (16 bits) : taille du paquet (entête + données)
- Checksum : somme de contrôle vérifiant la validité du pseudo entête.

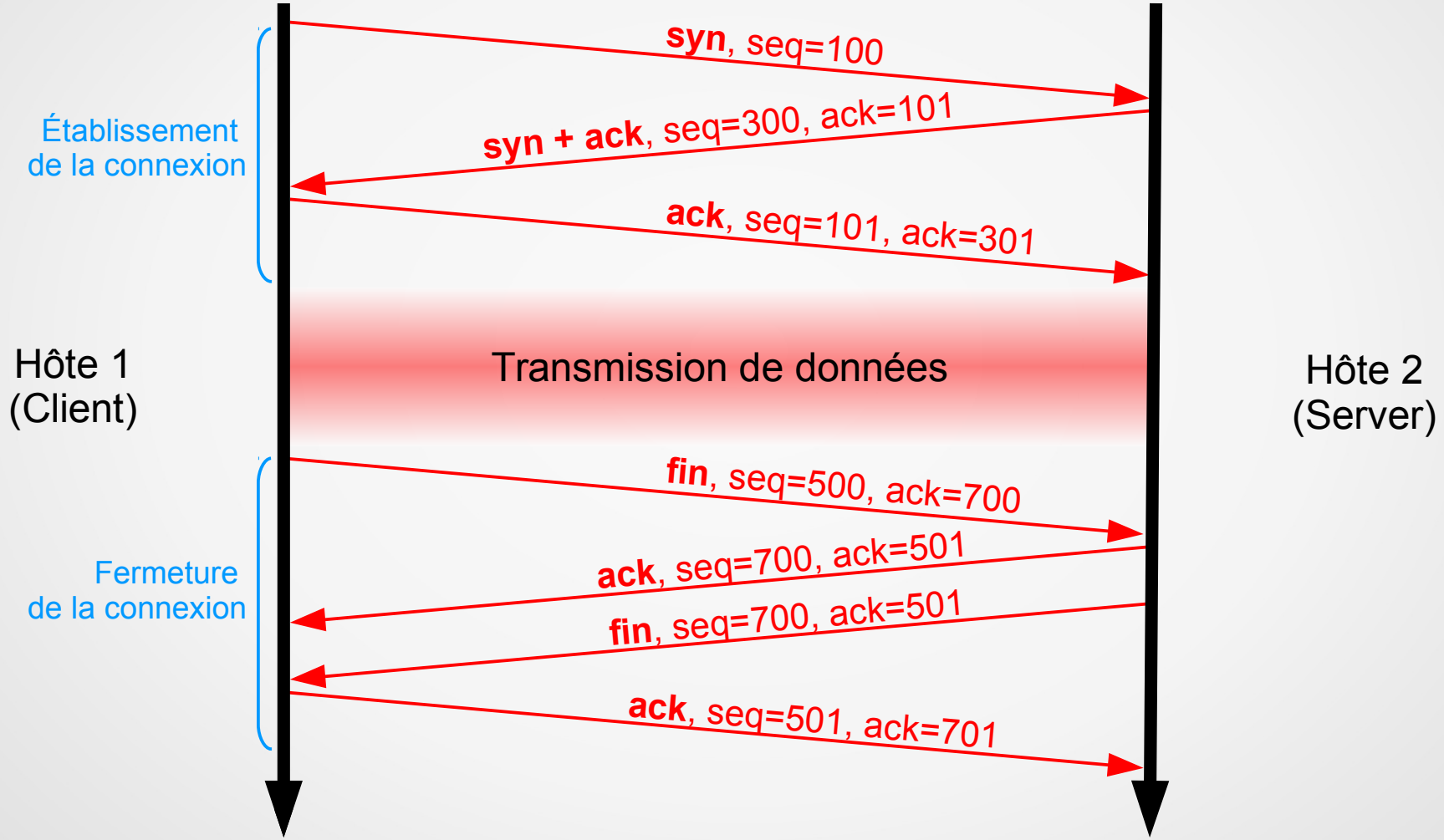
TCP/IP v4 - TCP

- TCP (Transmission Control Protocol) est un protocole de la couche Transport (4) du modèle OSI.
- Utilisation de ports de service pour les communications.
- TCP est un protocole connecté :
  - Établissement d'une connexion.
  - Contrôle de la bonne transmission des données (système d’acquittement)
  - Gestion de la segmentation des données
  - Gestion de la congestion du réseau.
- Plus complexe qu'UDP, TCP prend en charge la « fiabilisation » de la transmission, ce qui facilite le travail du processus l'utilisant.
- Une latence est ajoutée pour l'établissement et la gestion de la connexion.
- TCP est adapté pour :
  - Transmission de volumes de données importants
  - Transmissions nécessitant la fiabilité.

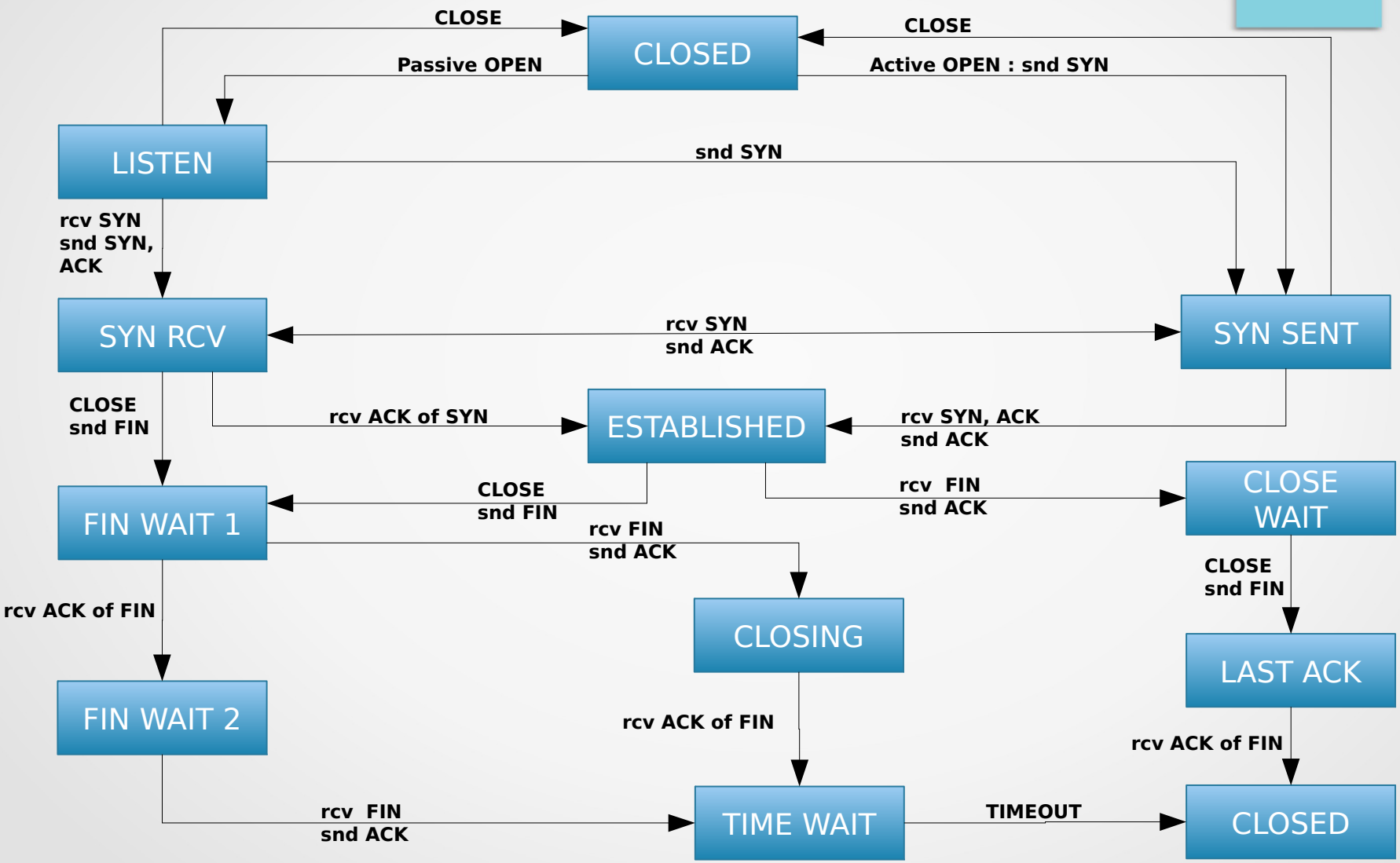
TCP/IP v4 - TCP

- Avant de transférer des données, TCP établit une connexion.
- La connexion est identifiée par :
  [(IP hôte1, Port hôte1) ↔ (IP hôte2, Port hôte2)]
- Une déconnexion doit avoir lieu pour libérer les ressources sur les 2 hôtes.
- La connexion reste active s'il n'y pas de « timeout » ni de déconnexion explicite.
- Transmission de données bidirectionnelle avec une seule connexion.

TCP/IP v4 - TCP

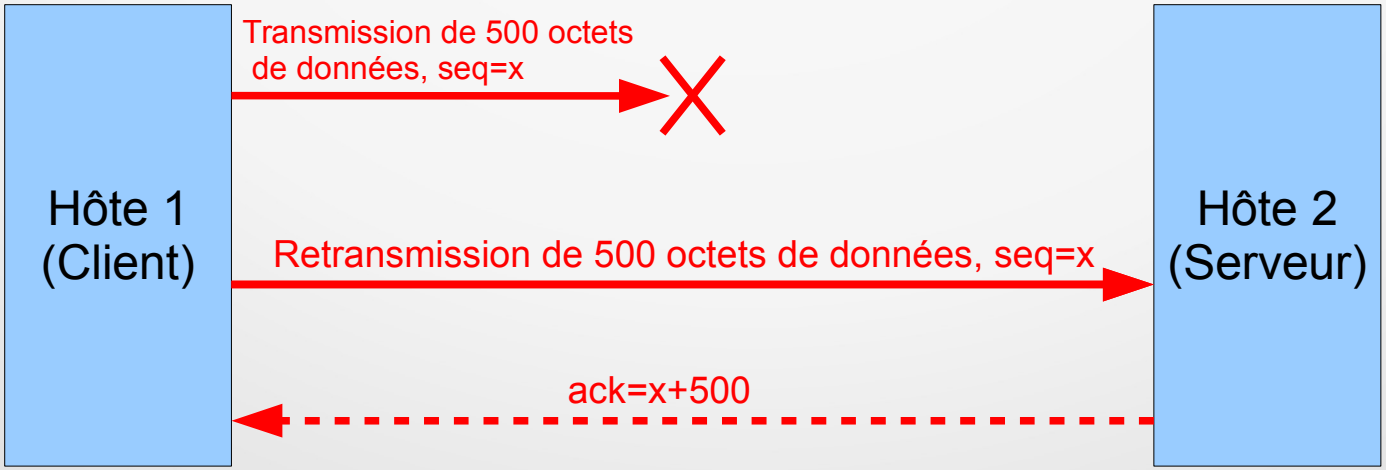

Établissement de la connexion
syn, seq=100
syn + ack, seq=300, ack=101
ack, seq=101, ack=301
Hôte 1 (Client)
Transmission de données
Hôte 2 (Server)
Fermeture de la connexion
fin, seq=500, ack=700
ack, seq=700, ack=501
fin, seq=700, ack=501
ack, seq=501, ack=701

TCP/IP v4 – TCP - Automate



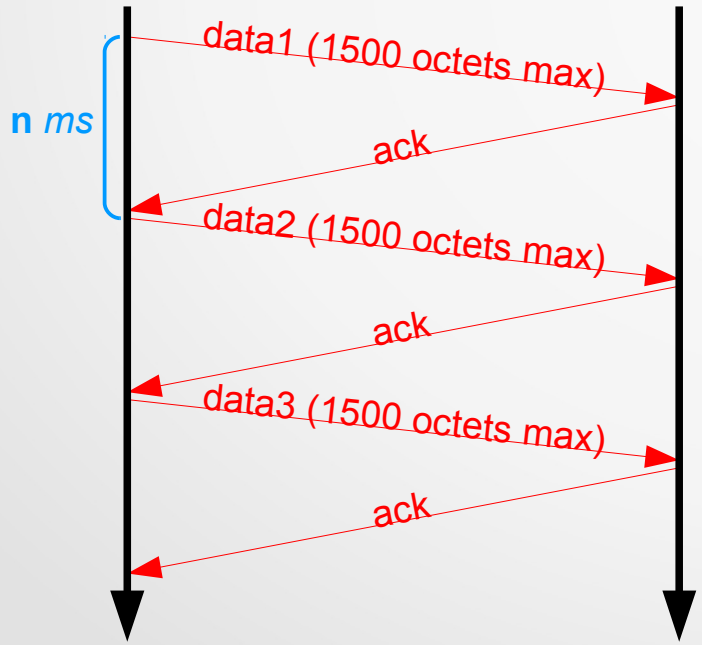
TCP/IP v4 – TCP

- TCP permet de vérifier qu'un paquet est bien arrivé en transmettant un paquet d'acquittement.
- Le numéro de séquence et le numéro d'acquittement sont sélectionnés par un générateur aléatoire à l'établissement de la connexion.
- A chaque transmission de données, un acquittement est transmis avec la valeur de séquence incrémentée de la quantité de données transmises.
- En cas d'échec de la transmission, le paquet est envoyé à nouveau.
- Le délai de retransmission est calculé dynamiquement en fonction du RTT (Round Trip Time) calculé.



TCP/IP v4 - TCP

- Le système d'acquittement fiabilise la connexion.
- Le système d'acquittement est sensible à la latence et impacte le débit de la transmission.



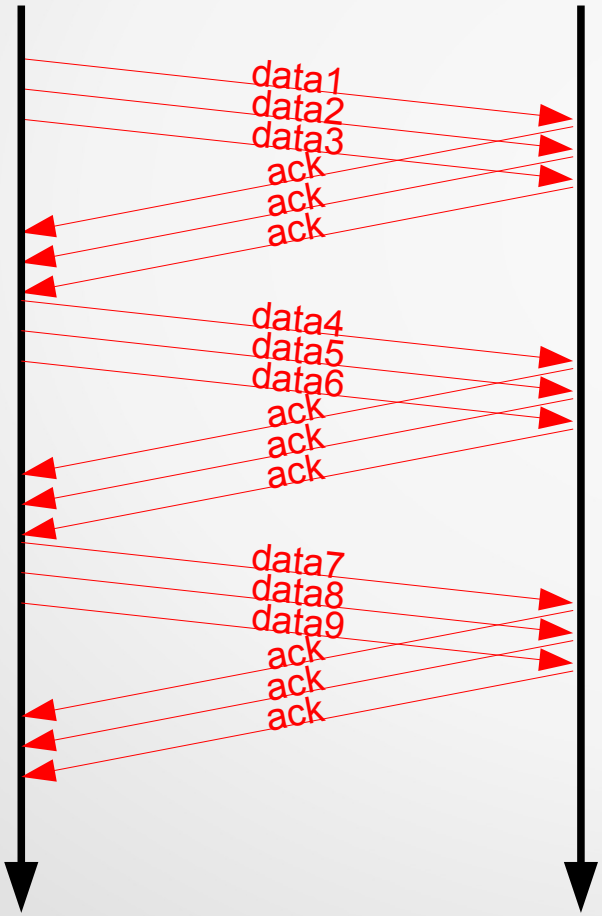
Latence « n » (ms)	Débit max approximatif
1	1,5 Mo/s
15	100 Ko/s
90	17 Ko/s

TCP/IP v4 - TCP

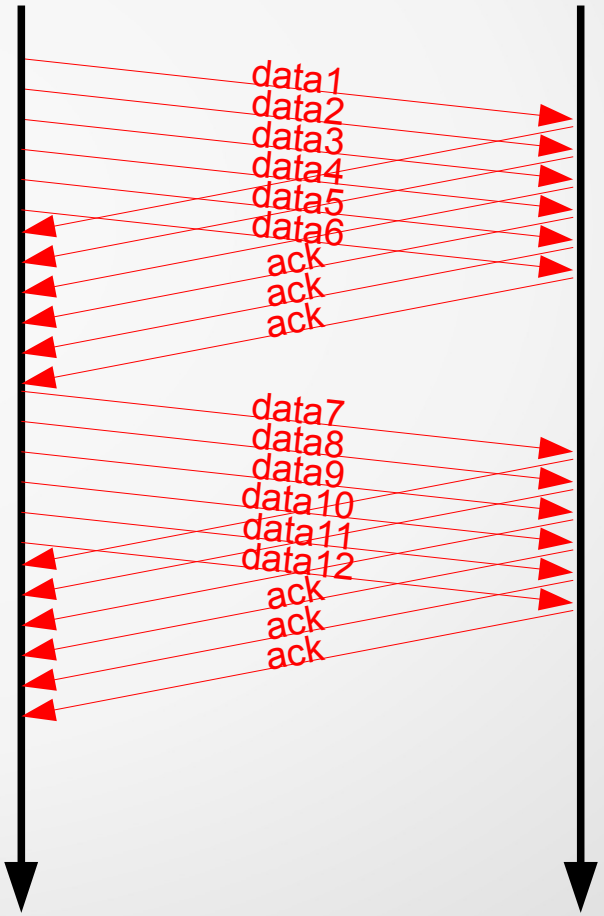
- Le système de **fenêtrage** va permettre d'adapter le flux de transmission en fonction de l'état du réseau.
- Cela permet de réduire le débit en cas de congestion ou de réduction du débit du réseau.
- Cela permet d'augmenter le débit en cas d'amélioration des conditions du réseau.
- Une certaine quantité de données (taille de la fenêtre) pourra être transmise sans attendre d'acquittement.
- La taille de la fenêtre est modifiée dynamiquement au cours d'une transmission.
- Gestion des transmissions / retransmissions par « fenêtre glissante ».
- Un nombre d'échec important de transmission de paquets entraîne une réduction de la taille de la fenêtre.
- Si le pourcentage d'erreur est faible, la taille de la fenêtre augmente progressivement.

TCP/IP v4 - TCP

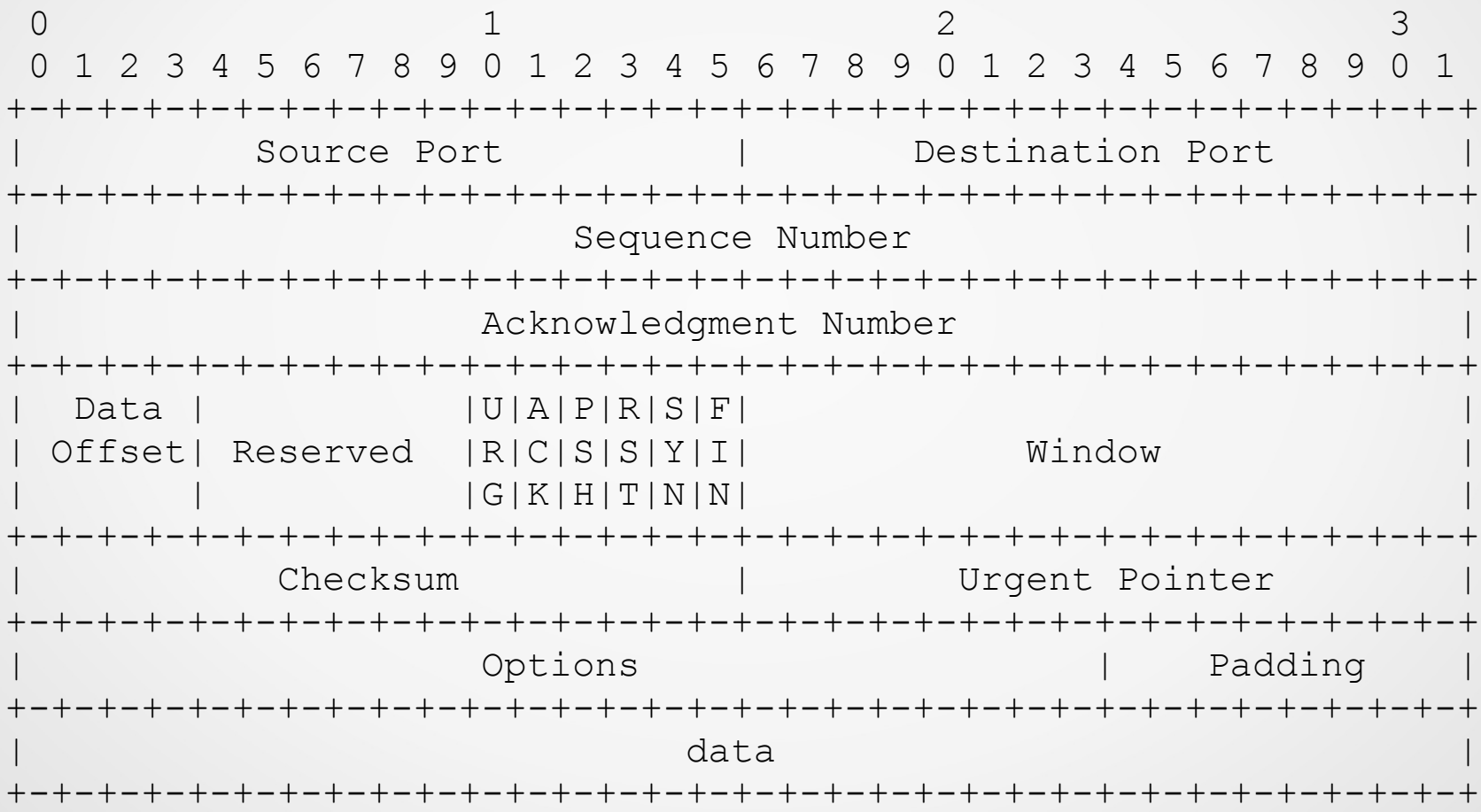
Taille de la fenêtre
4500 (3 x 1500)



Taille de la fenêtre
9000 (6 x 1500)



TCP/IP v4 - TCP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
Reserved
U R G
A C K
P S H
R S T
S Y N
F I N
Window
Checksum
Urgent Pointer
Options
Padding
data

TCP/IP v4 - TCP

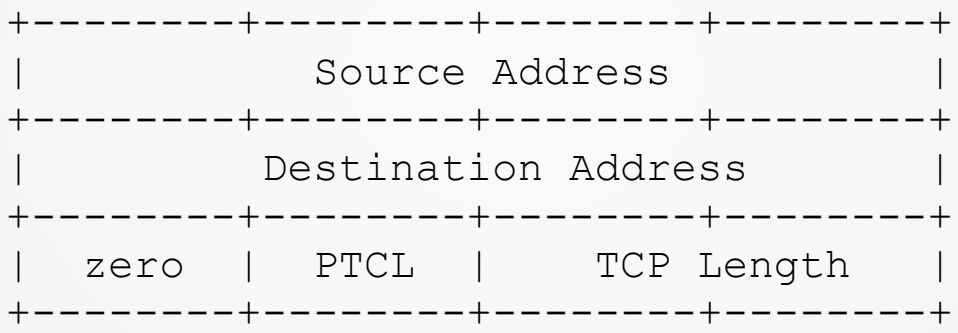
- **Source port** (16 bits) : port TCP de l'émetteur.
- **Destination port** (16 bits) : port TCP du destinataire.
- **Sequence Number** (32 bits) : numéro de séquence du premier octet, incrémenté de la quantité de données transmises. Il est généré à l'ouverture de la connexion (Syn).
- **Acknowledgment Number** (32 bits) : valeur du prochain numéro de séquence attendu.
- **Data offset** (4 bits) : taille de l'entête en mots de 32 bits.

TCP/IP v4 - TCP

- **Control bits** (6 bits) :
  - URG : signale la présence de données urgentes.
  - ACK : le paquet acquitte un précédent paquet.
  - PSH : indique au destinataire qu'il ne doit plus attendre de données et qu'il peut vider son tampon.
  - RST : indique au destinataire d'arrêter d'utiliser cette connexion. Cela peut mener à un nouvel établissement de connexion.
  - SYN : initie la synchronisation du numéro de séquence.
  - FIN : initie la fin de la connexion.

TCP/IP v4 - TCP

- **Window** (16 bits) : taille de la fenêtre (octets)
- **Checksum** (16 bits) : somme de contrôle calculée à partir d'un pseudo entête.



Pseudo entête

- **Urgent Pointer** (16 bits) : indique la position des données urgentes pour les paquets ayant le flag URG de positionné.

TCP/IP v4 - TCP

- **Options** (taille variable) : 3 options ont été défini au début et de nombreuses ont été définies plus tard dans des RFC.
  - End of option list : indique la fin de la liste des options.
  - No-Operation : permet d'aligner la liste des options.
  - Maximum Segment Size : permet de définir la taille maximum d'un segment sur une connection.
  - Timestamp : permet d'éviter les duplication de paquets
  - Window scale factor : augmente la capacité de la fenêtre
- https://www.iana.org/assignments/tcp-parameters/tcp-parameters.xhtml

TCP/IP v4 – Ports communs

UDP	
Port	**Service**
53	DNS
67	DHCP Server
68	DHCP Client
69	TFTP
123	NTP
161	SNMP
162	SNMP Trap
1194	OpenVPN

TCP	
Port	**Service**
21	FTP
22	SSH
25	SMTP
80	HTTP
110	POP3
143	IMAP4
443	HTTPS
993	IMAPS

http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml