Nancy-Université
Université Nancy 2

UE 503

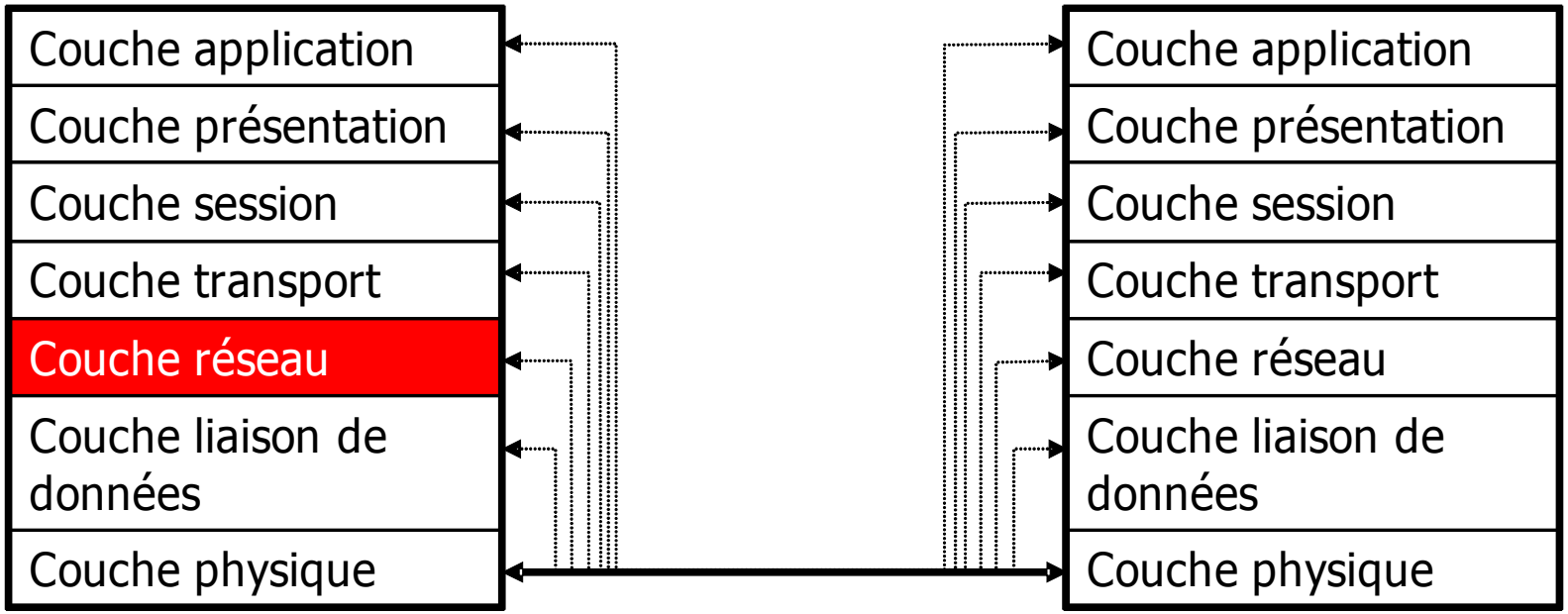
L3 MIAGE

Initiation Réseau et Programmation Web

A. Belaïd
abelaid@loria.fr
http://www.loria.fr/~abelaid/

Année Universitaire 2011/2012

La couche réseau



Introduction

- Rôle
  - C'est la couche qui permet de gérer le réseau
    - i.e. l'interconnexion des différents réseaux entre eux et le routage des données sur ces réseaux
  - Elle contrôle également l'engorgement du réseau

Les protocoles

- Suivant l'importance du réseau, son encombrement, plusieurs protocoles sont utilisés
  - Les protocoles d'adressage IP, DHPC, ARP
  - Le protocole de routage
  - Le protocole DNS
  - Les protocoles de transport TCP, UDP

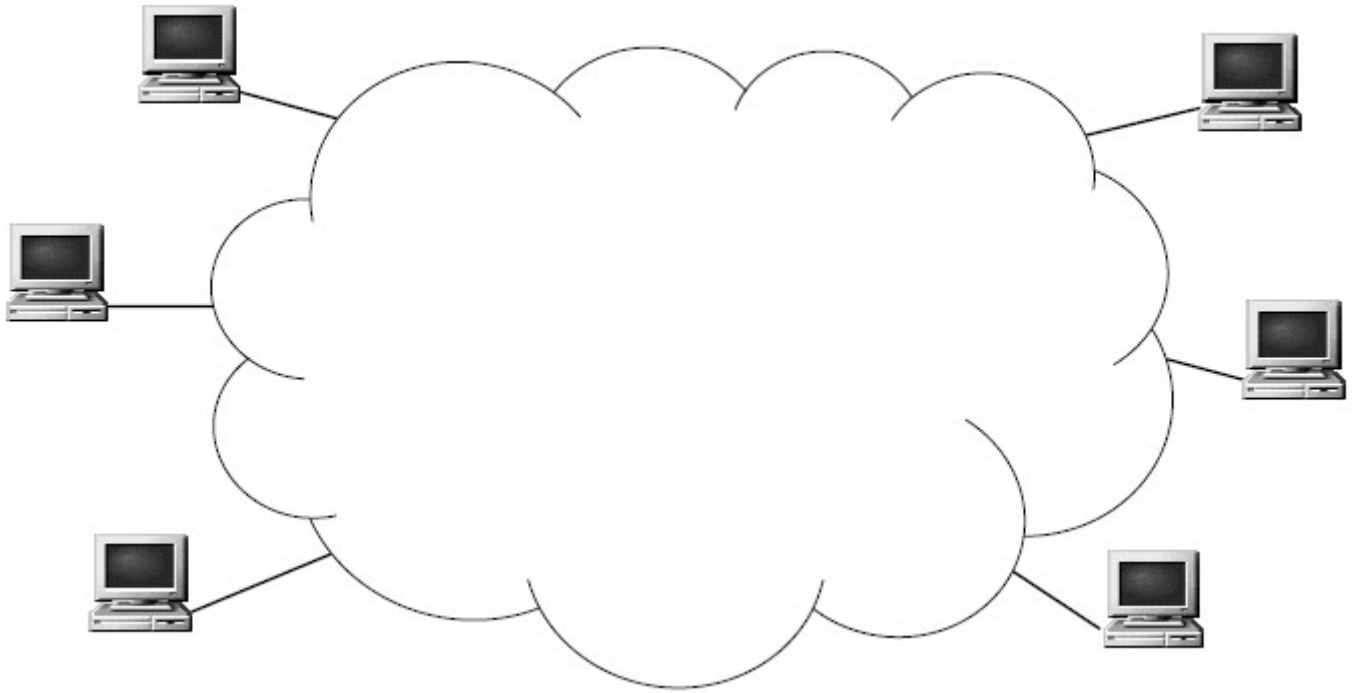
- Ce cours s'inspire largement du cours de Christian Bulfone : la pile TCP/IP

Les protocoles d'adressage IP

- C'est quoi ?
  - Famille de protocoles de communication de réseaux informatiques conçus pour être utilisés par Internet
  - Les protocoles IP permettent un service d'adressage unique pour l'ensemble des terminaux connectés

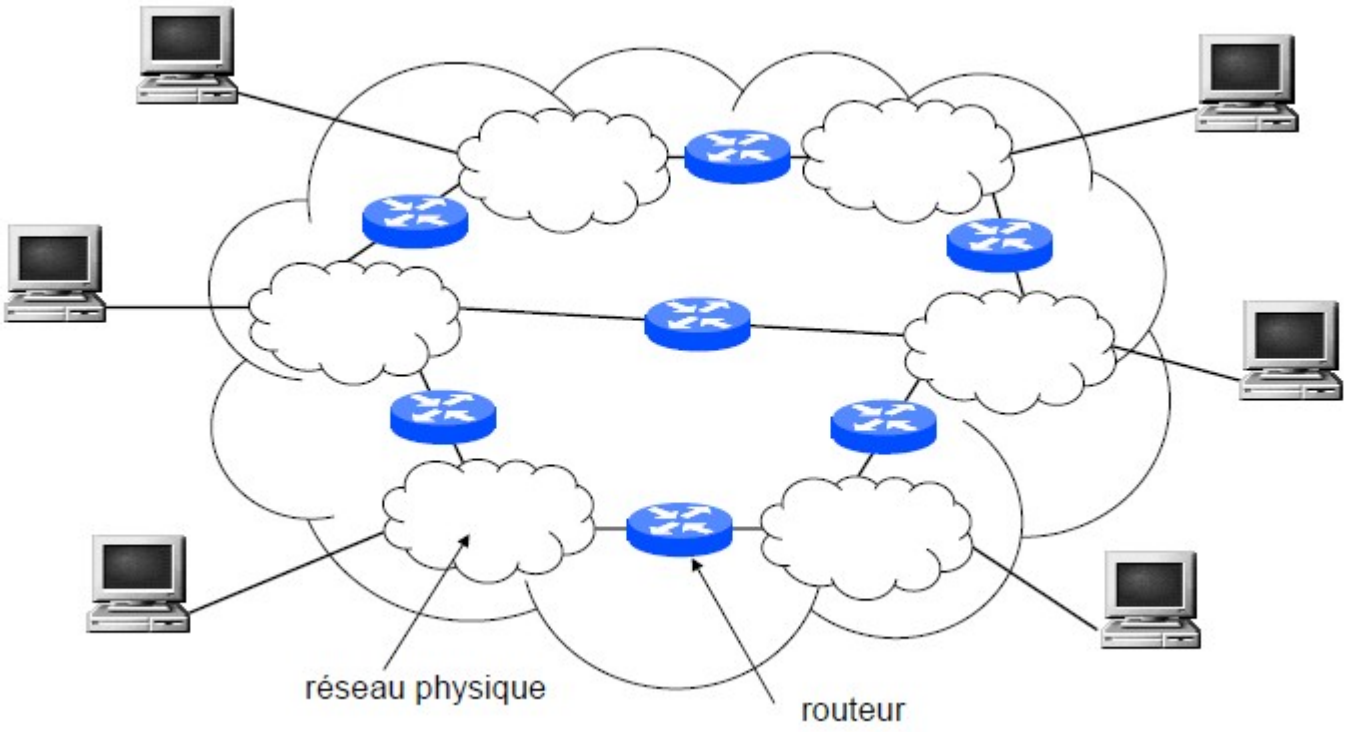
Internet

- Vu par l'utilisateur



Internet

- La réalité



Le protocole IP

- Notion d'adresse IP
  - Pour établir une liaison entre deux postes par l'intermédiaire d'un réseau mondialisé comme Internet, on ne peut se contenter du système d'adressage vu au cours précédent
  - En effet, dans un réseau local
    - le nombre d'adresses est limité
    - les commutateurs peuvent donc les gérer
  - Sur Internet
    - Il y a des millions de postes et d'utilisateurs
    - Les commutateurs sont incapables de les gérer
    - On crée des regroupements, appelés réseaux, avec **une adresse réseau**

- Ensuite, pour chaque poste
  - On va associer à l'adresse de la carte réseau (appelée adresse MAC) une adresse logique unique qui permettra d'identifier l'appartenance du poste au regroupement
  - C'est ce qu'on appelle actuellement une adresse IP

Deux versions du protocole

- Ipv4
  - Version actuellement répandue
  - Codage des adresses sur 32 bits
- Ipv6
  - Version en cours de déploiement
  - Codage des adresses sur 128 bits
  - Cohabite avec la version 4
  - Nécessite une nouvelle pile de protocoles
  - Implémenté sur la plupart des OS modernes

Deux versions du protocole

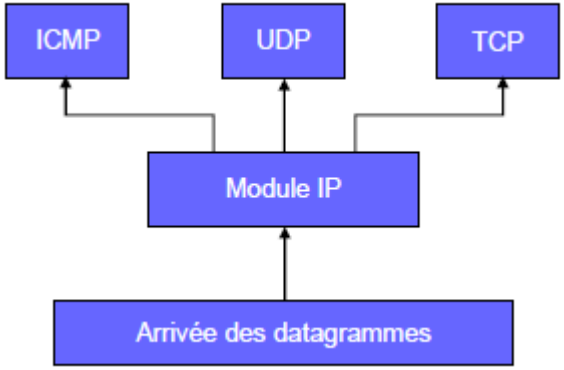
- Apports Ipv6
  - Supporte des milliards d'ordinateurs, sans l'inefficacité de l'espace des adresses IP actuelles
  - Réduit la taille des tables de routage
  - Simplifie le protocole pour permettre aux routeurs
  - Fournit une meilleure sécurité (authentification et confidentialité)
  - Facilite la diffusion multi-destinataire
  - Donne la possibilité à un ordinateur de se déplacer sans changer son adresse
  - Est évolutif

Le protocole IP

- Fonctions d'IP
  - Transporter des **datagrammes** de bout en bout
    - Il faut connaître l'adresse IP d'un équipement pour communiquer avec lui
  - Mode sans connexion
    - Chaque datagramme est traité indépendamment des autres
  - Pas de garantie de remise des datagrammes
    - Stratégie de type « best effort »
  - Assure le routage
  - Peut fragmenter les messages

Le protocole IP

- Fonctions d'IP
  - Le démultiplexage



  - Ce qu'IP ne fait pas
  - Le multiplexage
    - La vérification du séquencement
    - La détection de pertes
    - La retransmission en cas d'erreur
    - Le contrôle de flux

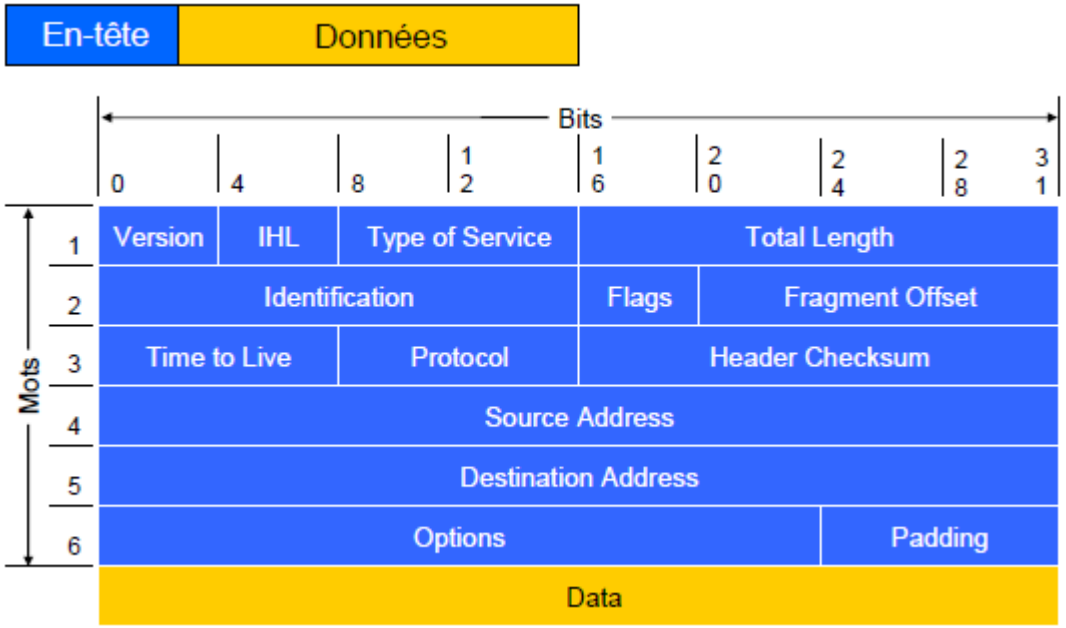
Le protocole IPv4

- Format du datagramme
  - Lors de l'émission, les données sont découpées en petits paquets, appelés datagrammes IP
  - Les datagrammes sont tous composés
  - d'un en-tête
  - suivi d'une zone de données

  - L'en-tête contient les adresses de l'émetteur et du destinataire
  - Le routage est basé sur l'adresse du destinataire

Format du datagramme IP (v4)

- IHL : donne le numéro de la version, pour connaitre la taille de l'en-tête
- Time to live : durée maximale de vie du datagramme sur le réseau
- Protocol : indique quel protocole de couche supérieure recevra les données IP (6=TCP, 1=ICMP, 17=UDP)

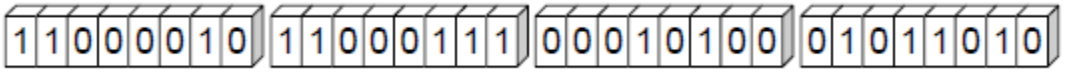


Format du datagramme IP (v4)

- Explication du phénomène de fragmentation
  - La fragmentation intervient lorsqu'un datagramme est plus grand que la MTU (Maximum Transfer Unit) supportée par le réseau
  - Exemple
  - Un datagramme de 1500 octets est envoyé sur un réseau Ethernet. En chemin, il doit passer sur une liaison série dont la MTU est de 525 octets
  - Le datagramme sera alors fragmenté en 3 datagrammes chacun avec une taille < 525 octets
  - Le message sera réassemblé tout à la fin par le destinataire et non pas par le routeur suivant
  - Donc, le champ Fragment Offset (décalage de la fragmentation) précise à quelle partie du datagramme correspond ce fragment

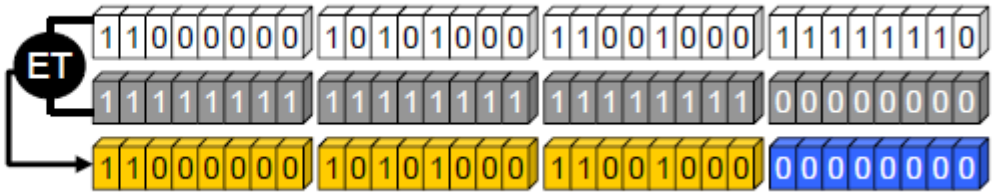
Le protocole IP

- Structure de l'adresse IP (v4)
  - Chaque interface réseau d'un poste possède une adresse IP unique au monde
    - Configurable par logiciel
    - Attribuée par le NIC (Network Information Center)
    - Codée sur 32 bits
    - Exemple : 194.199.20.90



- Structure de l'adresse IP (v4)
  - Adresse hiérarchique
    - Une relation existe entre les adresses d'équipements voisins
  - Structurée en deux parties
    - Le préfixe, donnant le numéro du réseau : ID de réseau ou netid
    - Le suffixe, donnant le numéro de la machine (hôte) dans ce réseau : ID de station ou hosid
  - Un masque (netmask) est associé à cette adresse
    - Il permet au logiciel IP de déterminer le préfixe du réseau d'une adresse en calculant un ET logique avec le masque

Adresse IP : 192.168.200.254
Masque réseau : 255.255.255.0
Préfixe réseau : 192.168.200.0



- Structure de l'adresse IP (v4)
  - Lorsque le masque est spécifié, on l'écrit généralement sous la forme :
  - Adresse IP/masque de réseau, par ex. 192.168.200.254/255.255.255.0
  - Il existe également une notation condensée dans laquelle, on écrit l'adresse IP suivie simplement du nombre de bits à 1 du masque, par ex. 192.168.200.254/24

Le protocole IP

- Composition de l'adresse IP
  - Comme le réseau Internet est important, on crée, au niveau de l'adressage, des sous-réseaux
  - Un sous-réseau correspond typiquement à un réseau local sous-jacent
  - L'adresse IP sera composée de deux parties
    - La partie correspondant à l'adresse du réseau local, utilisée pour le routage
    - La partie correspondant au poste, utilisée pour identifier des postes sur ce réseau local

Le protocole IP

- Composition de l'adresse
  - Dans la norme Ipv4 (première version d'IP, encore active en 2011), une adresse est composée de 4 octets exprimés sous forme décimale, exemple :
    - 10.169.27.50
    - La partie identifiant le réseau local (net-id) est
      - 10.169.27
    - la partie identifiant le poste ou l'hôte (*host-id*) est
      - 50

Le protocole IP

- Le masque de sous-réseau
  - Sert à différencier la partie identifiant le réseau et la partie identifiant le poste
  - Le masque 255.255.255.0 associé à l'adresse 210.169.27.50 définit le poste 50 sur le réseau 210.169.27.0
- L'adresse du réseau
  - est obtenue en appliquant le masque de sous-réseau sur son adresse IP à l'aide de l'opérateur logique ET

Le protocole IP

- Exemple
  - Adresse 192.168.1.2 et masque 255.255.255.0
    - 192.168.1.2 & 255.255.255.0 = 192.168.1.0
    - 192.168.1.2 & 0.0.0.255 = 0.0.0.2
  - Soit en binaire :
    - 11000000.10101000.00000001.00000010 &
      11111111.11111111.11111111.00000000 =
      11000000.10101000.00000001.00000000
    - 11000000.10101000.00000001.00000010 &
      00000000.00000000.00000000.11111111 =
      00000000.00000000.00000000.00000010

Le protocole IP

- Un réseau (ou sous-réseau) IP
  - est un ensemble d'hôtes partageant la même adresse réseau
  - Seuls les hôtes appartenant à un même réseau IP peuvent communiquer directement entre eux
    - Autrement, on passe par un routeur (entre réseaux)
  - Deux adresses IP appartiennent à un même sous-réseau si elles ont en commun les bits du masque de sous-réseau

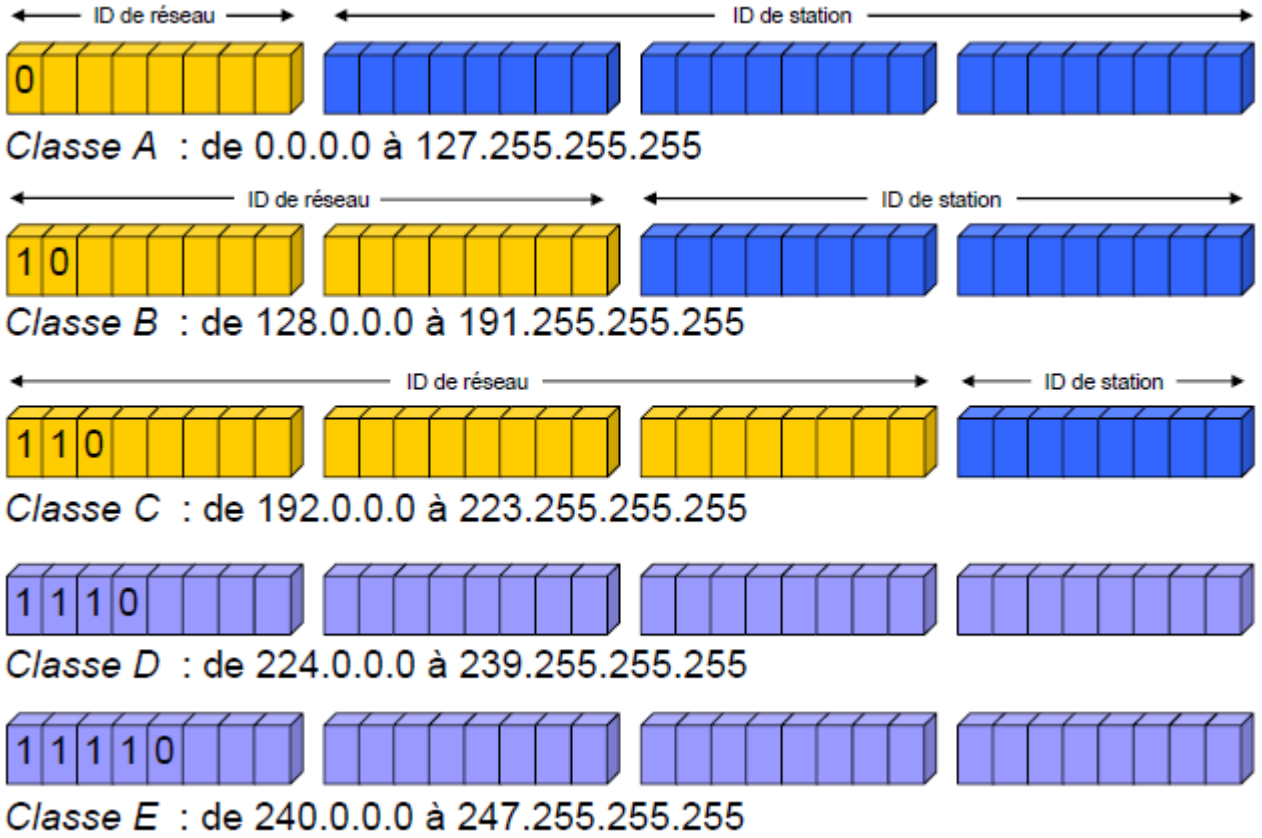
Le protocole IP

- Nombre d'hôtes sur un sous-réseau
  - À partir de la connaissance de l'adresse IPv4 et du masque de sous-réseau, il est possible de calculer le nombre de machines que l'on peut numéroter à l'intérieur d'un sous-réseau
  - Ce nombre = $\mathbf{2^{r-n}}$, n représente le nombre de bits à 1 dans le masque réseau et r le nombre de bits du masque de sous-réseau
  - Ici = $2^{32-n}-2$, deux adresses de ce sous-réseau étant réservées au sous-réseau lui-même et au broadcast et ne peuvent pas être utilisées pour numéroter une interface

- Classes d'adresses
  - Il existe différents découpages possibles que l'on appelle «classes d'adresses» en fonction de l'importance du réseau représenté
  - À chacune de ces classes correspond un masque réseau différent :

classe	premiers bits	premier octet	masque
A	0	0-127	255.0.0.0
B	10	128-191	255.255.0.0
C	110	192-223	255.255.255.0
D	1110	224-239	
E	1111	240-255	

  - Les adresses de classe A permettent donc de créer des réseaux avec plus de machines, par contre, il y a beaucoup plus de réseaux de classe C possibles que de réseaux de classe A ou B
  - La classe D est une classe utilisée pour le « multicast » (envoie à plusieurs destinataires) et la classe E est réservée



- Classe A : 1 octet moins le premier bit à 0 pour l'identification de réseau
- Classe B : 2 octets moins les 2 premier bits à 10 pour l'identification de réseau
- Classe C : 3 octets moins les 3 premiers bits à 110 pour l'identification de réseau
- Classe D : cas particulier, pas de distinction réseau/hôte; 4 premiers bits à 1110 puis 28 bits pour l'adresse de diffusion de groupe
- Classe E : 5 premiers bits à 11110 puis 27 bits réservés pour une utilisation future

Adresses spécifiques

- Adresse réseau et adresse de diffusion
  - Une adresse réseau est une adresse IP qui désigne un réseau et non pas une machine de ce réseau
    - Elle est obtenue en plaçant tous les bits de la partie machine (poste) à zéro
  - Une adresse de diffusion (« broadcast » en anglais) est une adresse permettant de désigner toutes les machines d'un réseau
    - elle est obtenue en plaçant tous les bits de la partie machine à un
    - Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le net-ID

Les adresses IP réservées ou interdites

- Exemple :
  - 200.100.40.12 masque 255.255.255.0
    - Le réseau désigné par le masque appliqué à cette adresse est : 200.100.40.0
    - L'adresse de broadcast IP sur ce réseau est 200.100.40.255
    - Remarque : cette adresse peut passer un routeur

– D'autres exemples :

IP (classe)	masque	adresse réseau	adresse de diffusion
10.10.10.10 (A)	255.0.0.0	10.0.0.0	10.255.255.255
192.168.150.35 (C)	255.255.255.0	192.168.150.0	192.168.150.255

- Adresse de **réseau** :
  - Identificateur de réseau suivi de bits à 0
  - Exemples :
    - 125.0.0.0 = réseau 125 de classe A
    - 129.15.0.0 = réseau 129.15 de classe B
    - 192.168.30.0 = réseau 192.168.30 de classe C
- Adresse de **diffusion** ou *broadcast* :
  - Identificateur de réseau suivi de bits à 1
  - Exemples :
    - 125.255.255.255 = diffusion sur le réseau 125 de classe A
    - 129.15.255.255 = diffusion sur le réseau 129.15 de classe B
    - 192.168.30.255 = diffusion sur le réseau 192.168.30 de classe C

Le protocole IP

- Adresses déconseillées et réseaux privés
  - Pour éviter les ambiguïtés avec les adresses de réseau et les adresses de diffusion, les adresses « tout à zéro » et « tout à un » sont déconseillées pour désigner des machines sur un réseau
  - Dans chaque classe d'adresses, certaines adresses réseaux sont réservées aux réseaux privés

classe	réseau privé
A	10.0.0.0
A	127.0.0.0
B	de 172.16.0.0 à 172.31.0.0
C	de 192.168.0.0 à 192.168.255.0

Le cas du réseau 127.0.0.1 est particulier : il désigne la boucle locale ou le réseau local (localhost)

Les adresses IP réservées ou interdites

- L'adresse de bouclage (loopback)
  - Cette adresse est utilisée pour désigner le réseau dans lequel on est (le réseau local) ou le poste sur lequel on est (la machine locale)
  - Il s'agit des adresses :
    - 127.0.0.0 et 127.0.0.1
      - (en principe de 127.0.0.0 à 127.255.255.255)
  - C'est une adresse toujours utilisée en interne sur le poste

Les adresses IP réservées ou interdites

- Rappel : l'adresse tout à zéro
  - Lorsque la partie net-id ne comporte que des zéros, elle fait référence au réseau sur lequel on se trouve
  - Cette adresse est intéressante dans le cas où un ordinateur veut communiquer sur le réseau qui le dessert mais qu'il n'en connaît pas encore l'adresse
  - Par extension, une adresse IP « tout à zéro » dans les tables de routage désignera une route par défaut

Les adresses IP réservées ou interdites

- Rappel : l'adresse tout à un
  - Cette adresse permet de diffuser sans préciser le réseau (*utilisée notamment par DHCP)*
  - Il s'agit de l'adresse 255.255.255.255
  - Cette adresse n'est jamais routée

Exemples

- Adresse de **machine** ou d'**hôte**
  - Exemples :
    - 125.5.6.7 = machine 5.6.7 du réseau 125 de classe A
    - 129.15.106.213 = machine 106.213 du réseau 129.15 de classe B
    - 192.168.30.11 = machine 11 du réseau 192.168.30 de classe C
- 127.x.x.x
  - adresse de **bouclage** (*loopback localhost*)
  - désigne la machine locale
- 0.0.0.0
  - utilisé quand une machine ne connaît pas son adresse
  - utilisé pour désigner la route par défaut dans la table de routage

Adresses IP privées et adresses publiques

- Remarque
  - Pour permettre la communication inter-réseaux, il faut que les adresses IP des réseaux et des postes soient uniques
  - Sur Internet, cette règle peut être contraignante
  - On peut cependant utiliser en interne des adresses privées qui seront rejetées par les routeurs d'Internet

Adresses IP privées et adresses publiques

- Les adresses privées
  - Ces adresses sont réservées à la communication au sein d'un réseau local
  - Elles ne sont pas utilisables dans des communications sur INTERNET
  - Il y a une plage d'adresses réservées dans chaque classe (A, B et C)
    - 10.0.0.0 à 10.255.255.255
    - 172.16.0.0 à 172.31.255.255
    - 192.168.0.0 à 192.168.255.255

Adresses IP privées et adresses publiques

- Attribution des adresses IP publiques
  - Pour communiquer sur Internet
    - les adresses publiques doivent être uniques
  - Il faut donc un organisme qui dirige leur attribution
  - Au niveau international, il s'agit de l'IANA (*Internet Assigned Number Authority*)
  - Il y a bien sûr des délégations au niveau de chaque pays

Sous-réseaux IP (v4)

- Découpage d'un réseau en entités plus petites
  - Sous-réseau ou « subnet »
  - Permet meilleure structuration du réseau du site
  - Décidé par l'administrateur du site
  - Adresse de sous-réseaux prélevé sur la partie host-id
  - Longueur complétée en bits décidée par l'administrateur
  - Tous les équipements réseaux doivent utiliser la la notion de sous-réseau (station, serveurs de terminaux, routeurs, imprimantes...)
  - Interconnexion des sous-réseaux impérativement par des routeurs

Adressage de sous-réseaux

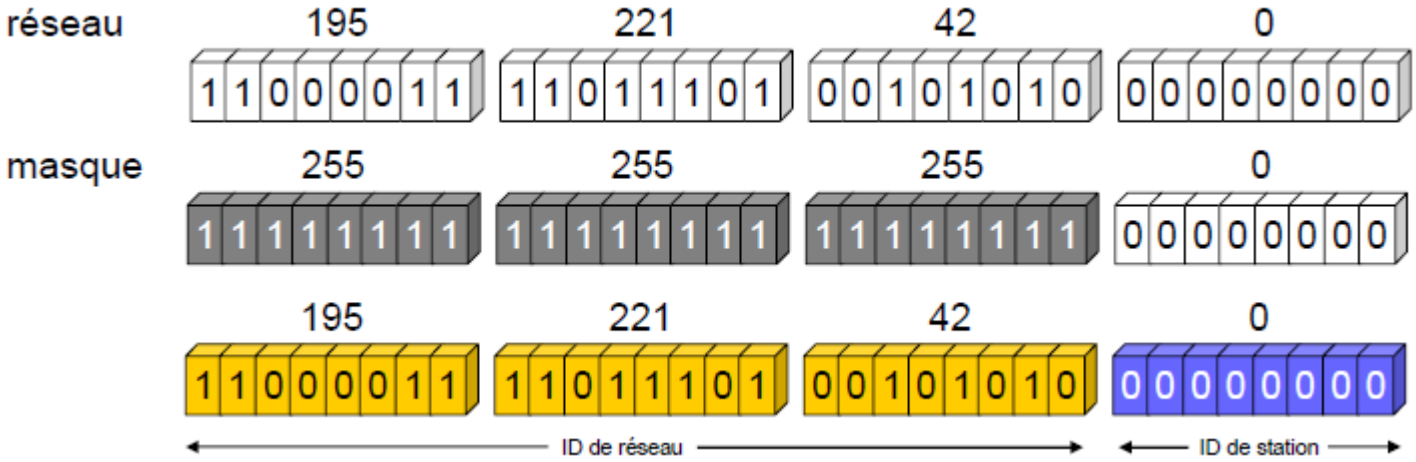
- Exemple : réseau de classe B : 140.30.0.0

  - Masque de réseau par défaut : 255.255.0.0 si aucun sous-réseau n'est défini
  - Masque 255.255.255.0 si présence de (au plus 254) sous-réseaux (de 254 hôtes chacun)

Adressage de sous-réseaux

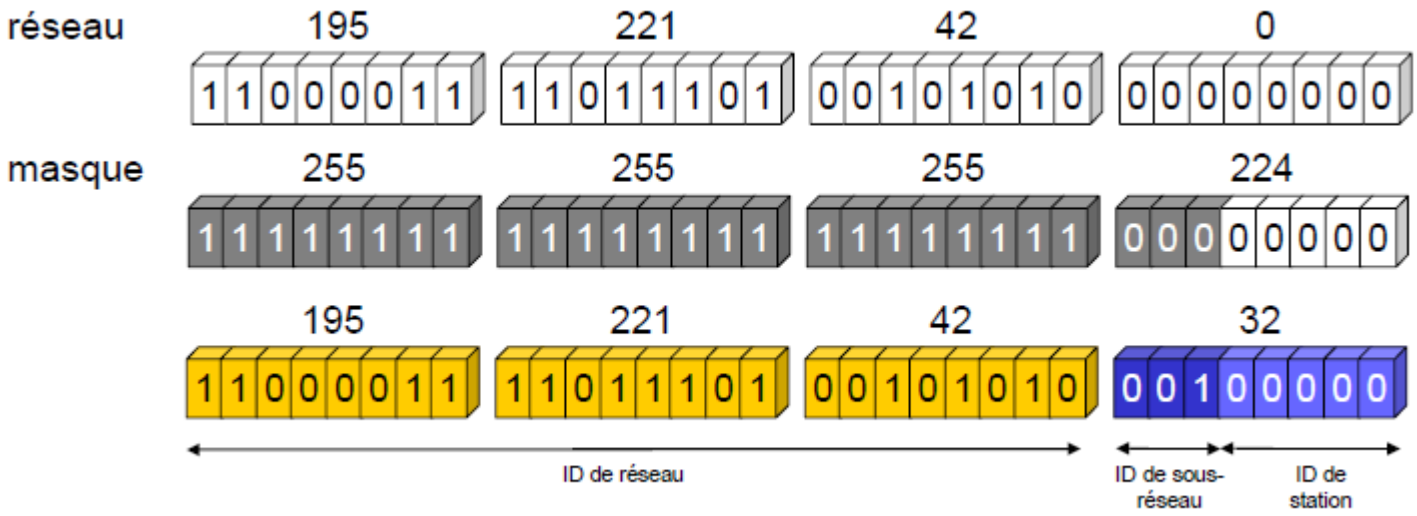
- Découpage en sous-réseau
  - Le découpage en sous-réseaux est inconnu de l'extérieur
  - Il passe par l'utilisation d'un masque de sous-réseau (subnet mask)
  - On utilise la même notation que l'adresse IP
    - Bits réseau à 1
    - Bits de la partie sous-réseau à 1
    - Bits de la partie host à 0

Exemple sans sous-réseaux



- Adresse réseau : 195.221.42.0
- Masque : 255.255.255.0
- Adresses des hôtes : 195.221.42.1 à 195.221.42.254
- Adresse de broadcast : 195.221.42.255

Exemple avec sous-réseaux

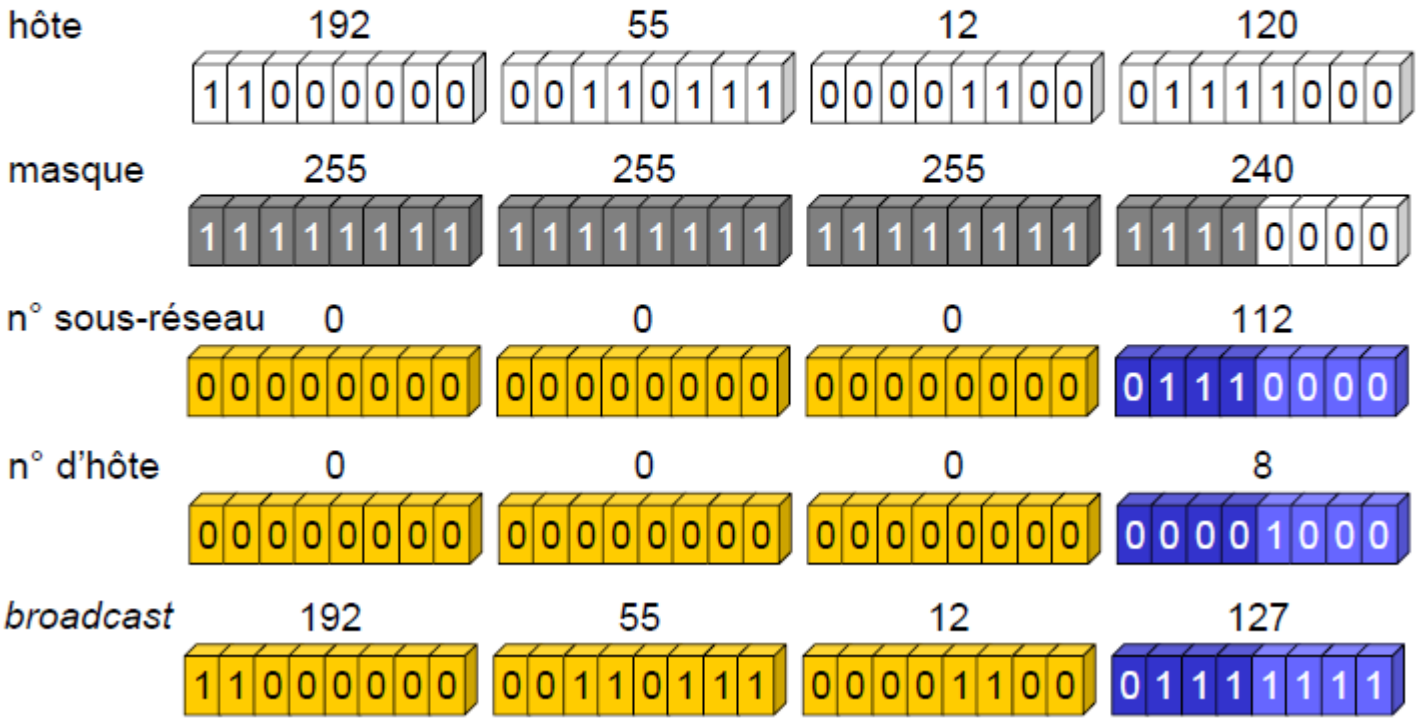


- Adresse réseau : 195.221.42.0,
- Masque : 255.255.255.224
- Dans le dernier octet, les 3 premiers bits représentent les numéros des sous-réseaux, et les 5 derniers, les numéros d'hôtes par sous-réseau. Avec 3 bits, on peut représenter 2^3 sous-réseaux numérotés en binaire : 000, 001, 010, 011, 100, 101, 110 et 111

- Dans chaque sous-réseau si le host-id est codé sur les m bits restants, en enlevant l'adresse du sous-réseau lui-même (tous les bits du host-id à 0) et l'adresse de broadcast (tous les bits du hostid à 1), peur représenter 2^m-2 hôtes

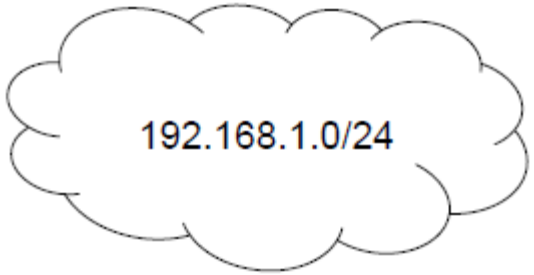
Adresses réseaux	Adresses des hôtes	Broadcast
Sous-réseau 0 195.221.42.0	195.221.42.1 - 195.221.42.30	195.221.42.31
Sous-réseau 1 195.221.42.32	195.221.42.33 - 195.221.42.62	195.221.42.63
Sous-réseau 2 195.221.42.64	195.221.42.65 - 195.221.42.94	195.221.42.95
Sous-réseau 3 195.221.42.96	195.221.42.97 - 195.221.42.126	195.221.42.127
Sous-réseau 4 195.221.42.128	195.221.42.129 - 195.221.42.158	195.221.42.159
Sous-réseau 5 195.221.42.160	195.221.42.161 - 195.221.42.190	195.221.42.191
Sous-réseau 6 195.221.42.192	195.221.42.193 - 195.221.42.222	195.221.42.223
Sous-réseau 7 195.221.42.224	195.221.42.225 - 195.221.42.254	195.221.42.255

Exemple 2

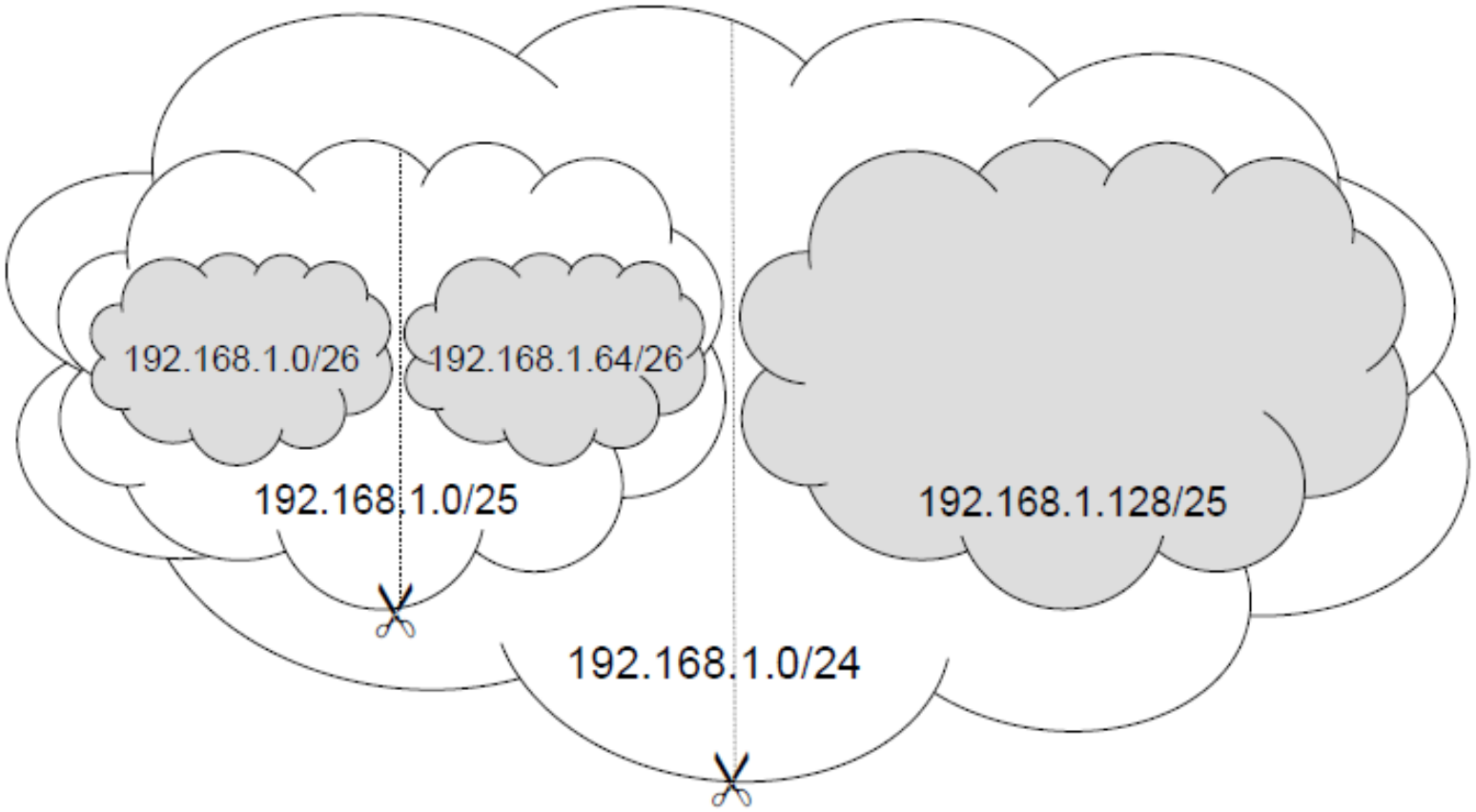

hôte
192
1 1 0 0 0 0 0 0
55
0 0 1 1 0 1 1 1
12
0 0 0 0 1 1 0 0
120
0 1 1 1 1 0 0 0
masque
255
1 1 1 1 1 1 1 1
255
1 1 1 1 1 1 1 1
255
1 1 1 1 1 1 1 1
240
1 1 1 1 0 0 0 0
n° sous-réseau
0
0 0 0 0 0 0 0 0
0
0 0 0 0 0 0 0 0
0
0 0 0 0 0 0 0 0
112
0 1 1 1 0 0 0 0
n° d'hôte
0
0 0 0 0 0 0 0 0
0
0 0 0 0 0 0 0 0
0
0 0 0 0 0 0 0 0
8
0 0 0 0 1 0 0 0
broadcast
192
1 1 0 0 0 0 0 0
55
0 0 1 1 0 1 1 1
12
0 0 0 0 1 1 0 0
127
0 1 1 1 1 1 1 1

Découpage en sous-réseaux

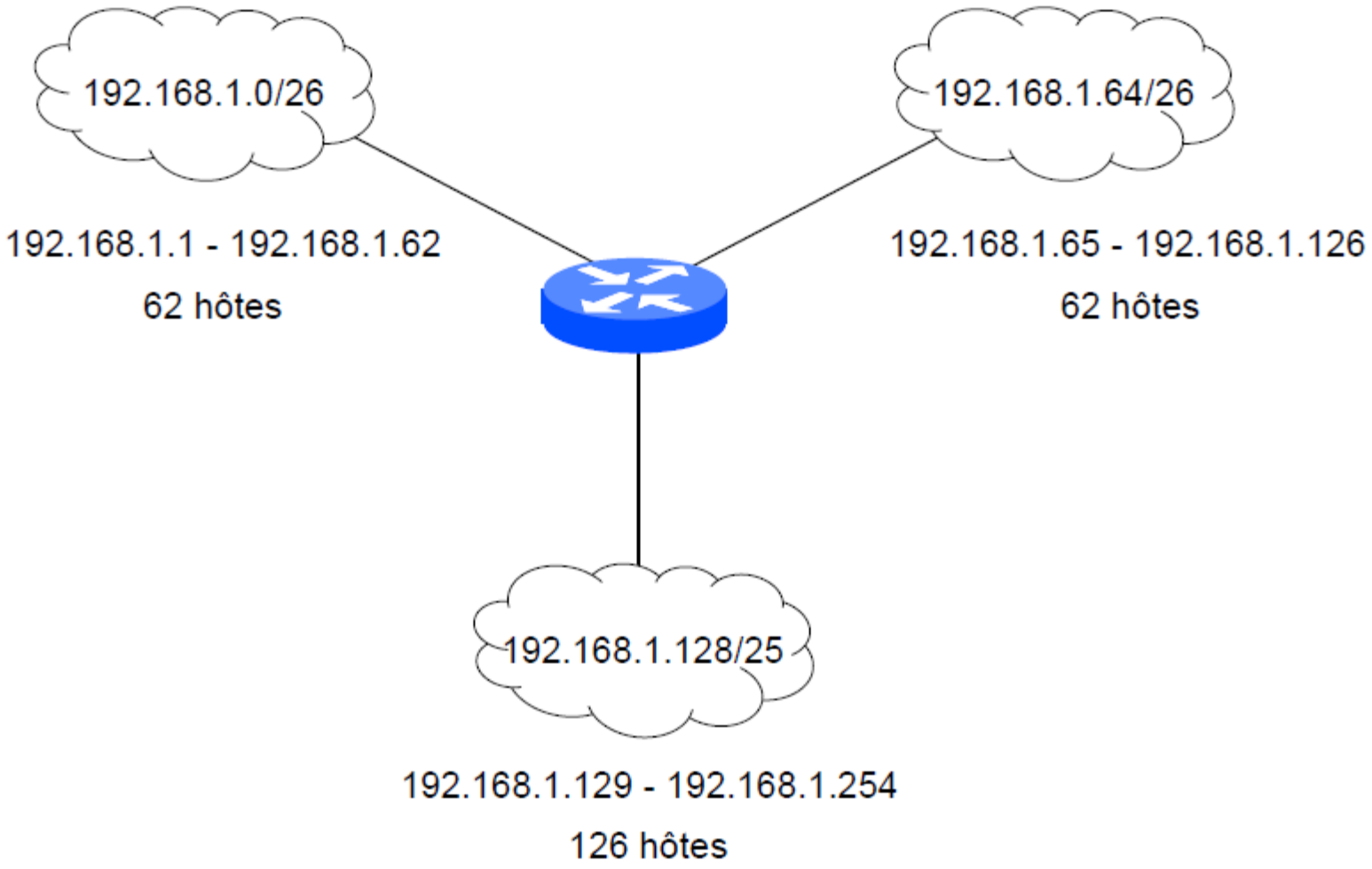
- Comment découper le réseau 192.168.1.0/24 en sous-réseaux pour avoir :
  - 2 sous réseaux d'au plus 60 machines
  - 1 sous-réseau d'au plus 124 machines
- Le nombre d'hôtes est différent pour au moins un sous-réseau
  - ➔On ne peut pas utiliser le même masque



Découpage en sous-réseaux



Découpage en sous-réseaux



Le protocole DHPC

(Dynamic Host Configuration Protocol)

- Son rôle
  - Permettre à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration réseau, en se faisant adresser une adresse IP et un masque de sous-réseau
  - Ainsi, la machine cherche toute seule une adresse IP par DHCP
  - Cela concerne certaines qui se connectent de manière épisodique sur certains réseaux
  - Il faut pour cela qu'elle soit configurée pour aller chercher son adresse IP au démarrage

Le protocole DHPC

(Dynamic Host Configuration Protocol)

- Pour cela
  - Il faut dans ce cas un serveur DHCP qui distribue des adresses IP
  - Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe
  - Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP

- Fonctionnement
  - La machine va dialoguer avec un serveur DHCP
    - Elle émet un paquet spécial de broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion... sur le réseau local
    - Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client
- Notion de bail
  - Pour des raisons d'optimisation des ressources réseau, les adresses IP sont délivrées avec une date de début et une date de fin de validité

Le protocole DHPC

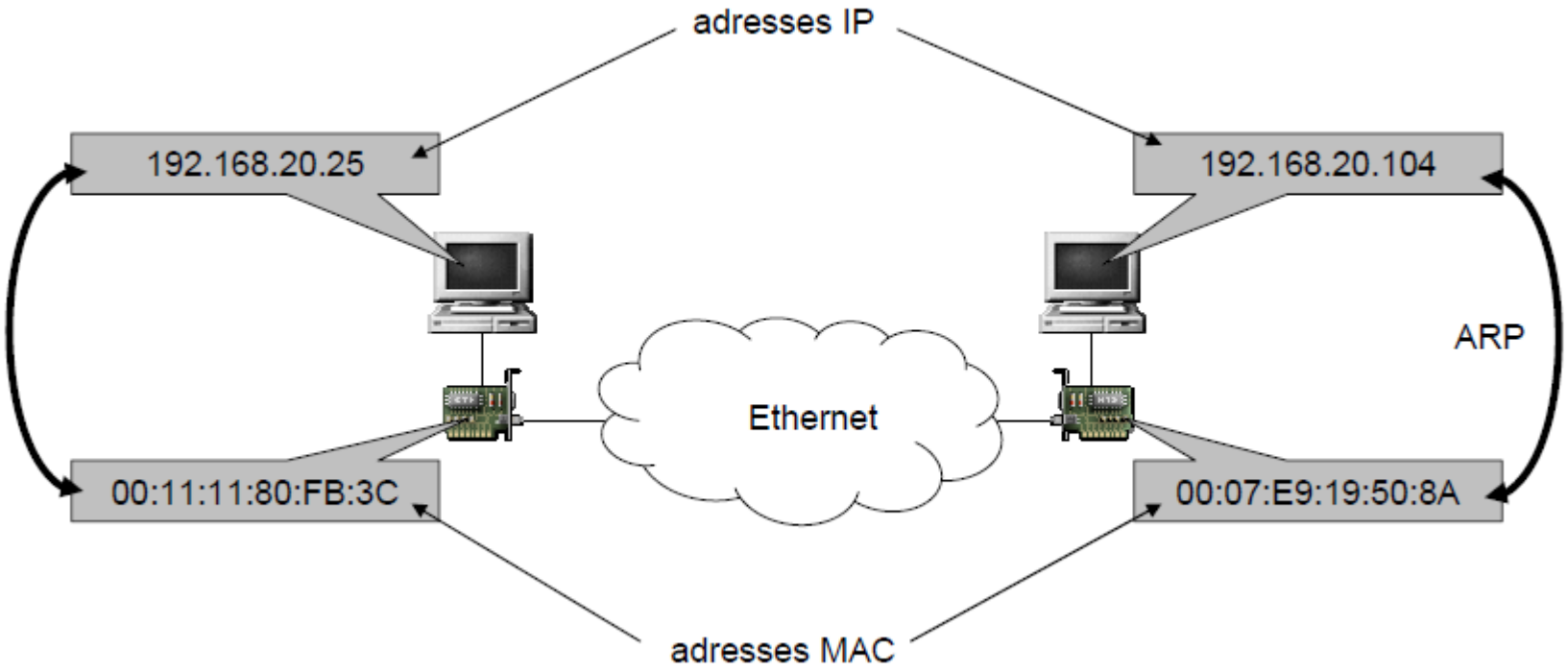
- Les avantages de DHCP dans l'administration d'un réseau sont les suivants :
  - La distribution d'adresses est centralisée sur un serveur
    - ce qui permet de contrôler les différentes affectations
  - Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution
    - les postes itinérants sont plus faciles à gérer
  - Enfin dans un contexte de pénurie d'adresses IP
    - un fournisseur d'accès par exemple attribue une adresse à la demande le temps d'une connexion et la réaffecte dès que celle-ci se libère

Le protocole ARP
(Address Resolution Protocol)

- Objectif
  - Traduire les adresses MAC en adresse IP
- En effet
  - Chaque machine connectée au réseau possède un numéro d'identification : adresse MAC
  - Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine
  - Toutefois, la communication sur Internet ne se fait pas directement à partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs à chaque fois que l'on change une carte réseau) mais à partir d'une adresse dite logique attribuée par un organisme : l'adresse IP

ARP

- Correspondance entre une adresse Ethernet (32 bits) et une adresse « physique » (Ethernet sur 48 bits)



Le protocole ARP
(Address Resolution Protocol)

- Ainsi,
  - Pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique (adresse MAC), puis crée une table de correspondance entre les adresses logiques (adresses IP) et les adresses physiques (adresses MAC) dans une mémoire cache

Le protocole ARP
(Address Resolution Protocol)

- Fonctionnement
  - Une trame transmise par une carte réseau possède un entête contenant l'adresse MAC du destinataire et l'adresse MAC de l'émetteur
  - L'adresse MAC source ne pose pas de problème puisqu'elle correspond à l'adresse MAC de la carte réseau de l'émetteur
  - Mais l'adresse MAC destinataire, comment la connaître ?

Le protocole ARP

- Qui connaît sur le réseau l'association adresse IP / adresse MAC recherchée ?
  - Le poste destinataire des trames
  - Il faut donc le lui demander
- Oui mais comment demander à un poste dont on ne connaît pas l'adresse MAC ?
  - En utilisant l'adresse de broadcast

Le protocole ARP

- Le protocole ARP consiste à envoyer une trame de broadcast contenant un "request arp" :
  - "Quelle est l'adresse MAC correspondant à l'adresse IP suivante ?"
- Le poste qui reconnaît son adresse IP répond en fournissant son adresse MAC
  - Cette association adresse IP/adresse MAC est mise en cache et sera utilisée ultérieurement dans l'échange
  - Au passage, les postes qui ont reçu la demande ARP diffusée mettent en cache l'association adresse IP/adresse MAC du demandeur

Le protocole ARP

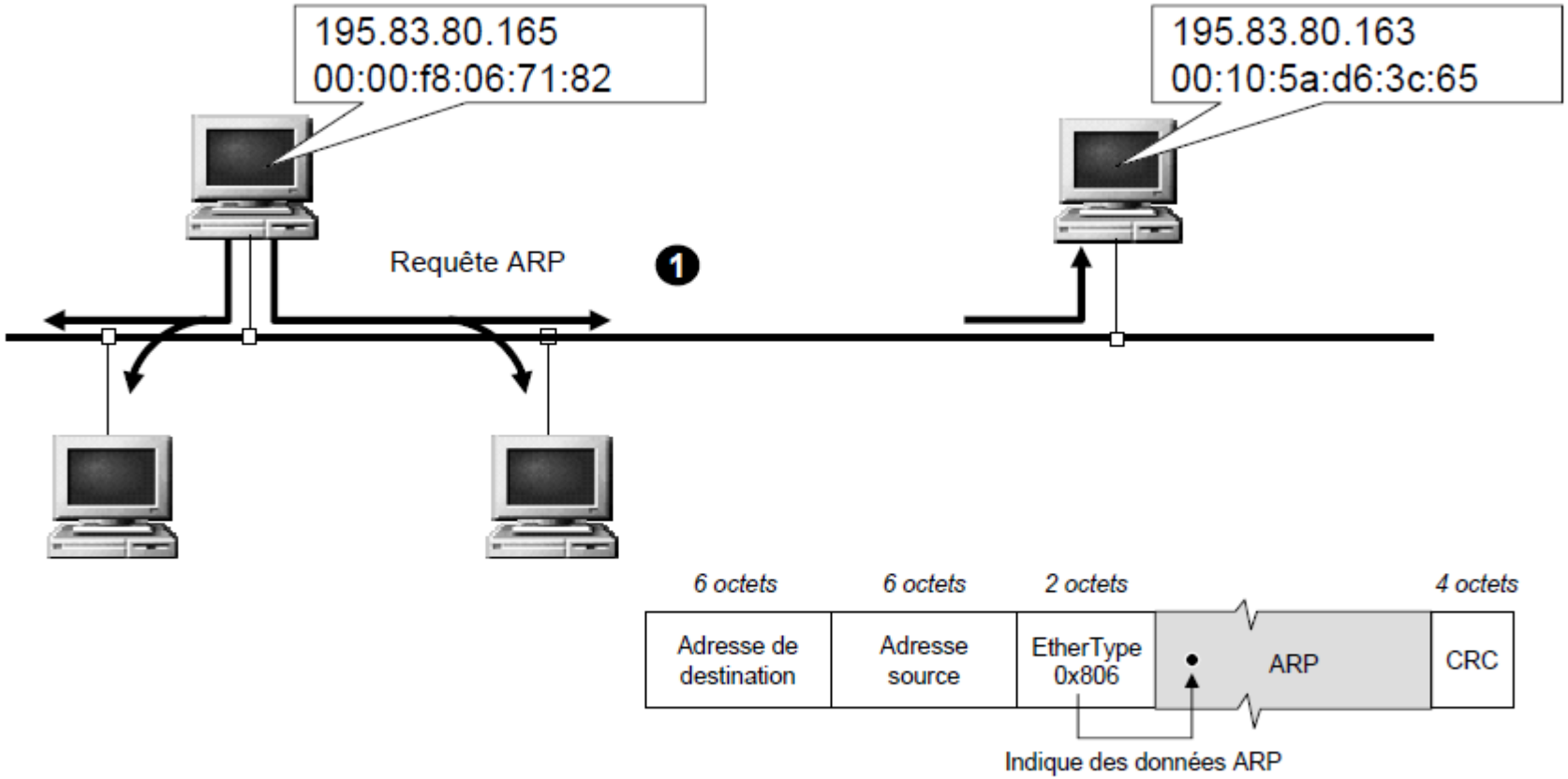
- Détail du fonctionnement
  - Lors de l'envoi d'un datagramme IP
    - On connait l'adresse IP destination
    - On ne connait pas l'adresse Ethernet

      ➔protocole ARP
  - Au boot d'une machine sans disque (Terminal X par exemple)
    - On connait l'adresse Ethernet
    - On ne connait pas l'adresse IP

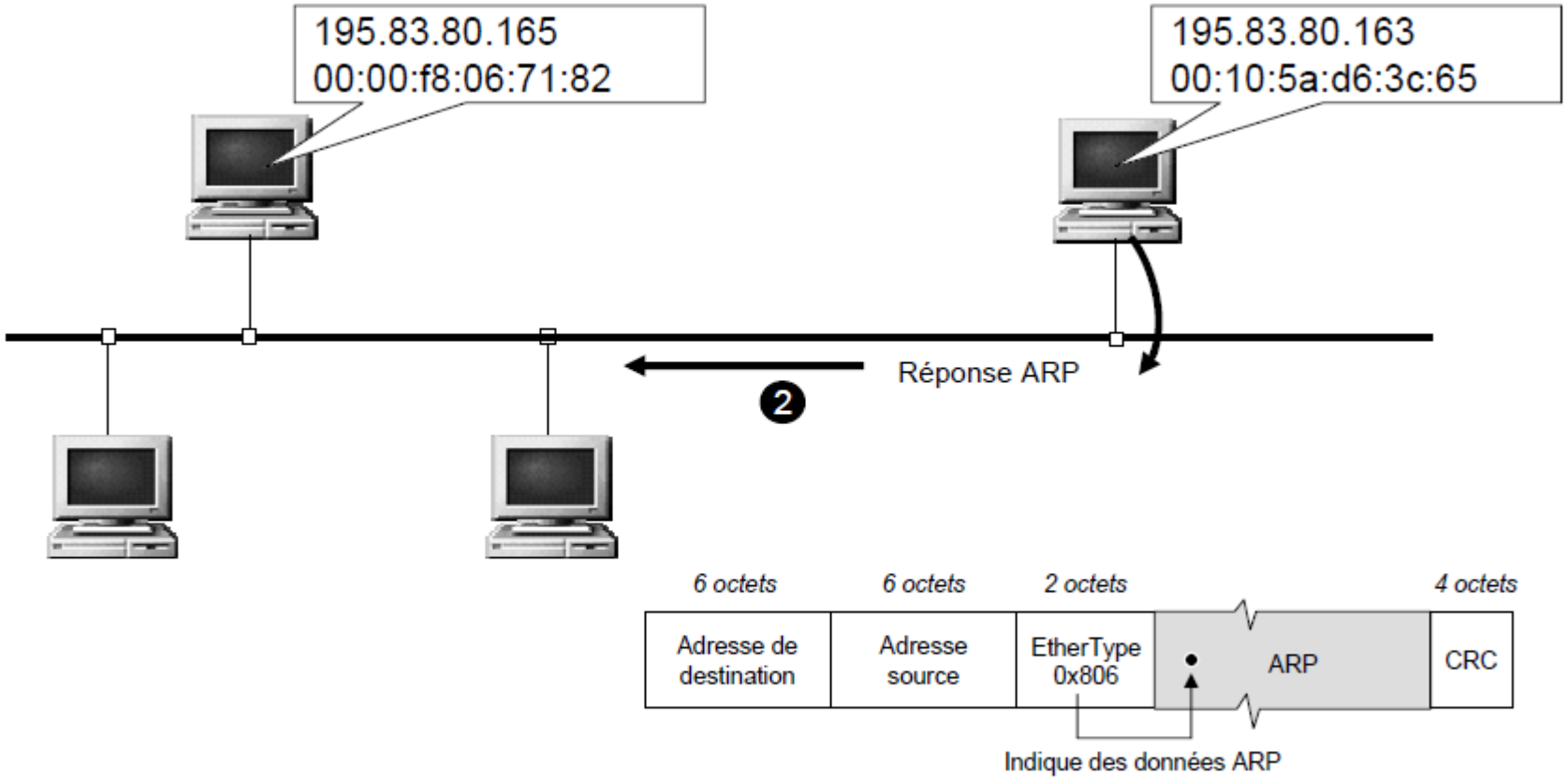
      ➔protocole RARP (Reverse ARP)

Le protocole ARP

- Détail du fonctionnement (suite 1)
  - A, d'@ IP Ia et d'@ Ethernet EA veut envoyer un message à B d'@ IP Ib
    - A diffuse un message ARP avec l'adresse de diffusion matérielle (FF:FF:FF:FF:FF:FF)
    - Toutes les machines reçoivent la requête
    - Seul B renvoie un message contenant son adresse physique Eb
    - A met à jour sa table ARP en mémorisant Ib ⇔ Eb
    - B met à jour sa table ARP en mémorisant Ia ⇔ Ea




```
1 00:00:f8:06:71:82 ff:ff:ff:ff:ff:ff  ARP  Who has 195.83.80.163? Tell 195.83.80.165
```




```
1 00:00:f8:06:71:82 ff:ff:ff:ff:ff:ff  ARP  Who has 195.83.80.163? Tell 195.83.80.165
2 00:10:5a:d6:3c:65 00:00:f8:06:71:82  ARP  195.83.80.163 is at 00:10:5a:d6:3c:65
```

Le protocole ICMP
(Internet Control Message Protocol)

- Définition
  - ICMP est un module obligatoire d'IP qui assure deux fonctions principales :
    - rendre compte d'un problème réseau
    - tester l'accessibilité d'une machine
    - les messages ICMP sont de deux natures :
      - les messages d'erreurs : suite a une erreur constatee sur un datagramme (qui entra^ne le plus souvent sa destruction)
      - les messages d'interrogation/information : messages divers contribuant au (ou informant sur le) bon fonctionnement des equipements

Le protocole ICMP

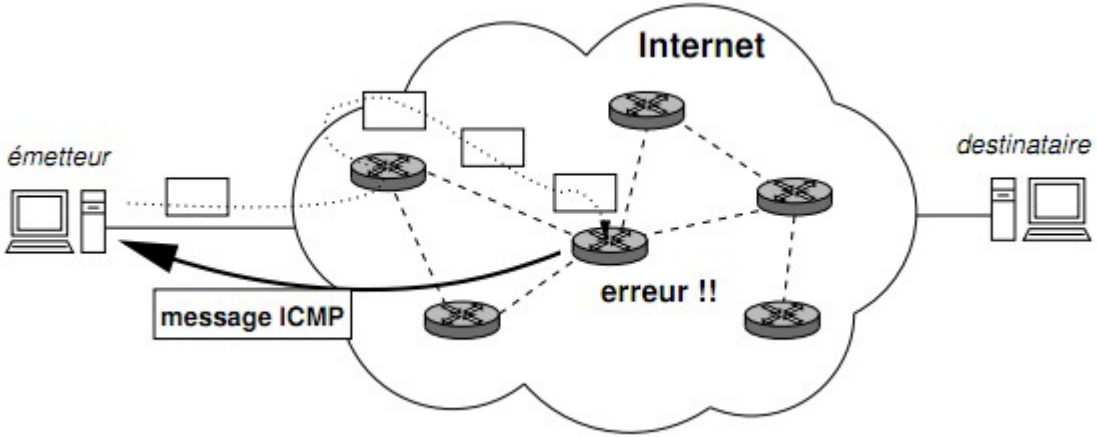
- Causes des erreurs
  - les causes rendant impossible la remise d'un datagramme peuvent être nombreuses :
    - panne de ligne de transmission, ou d'un processeur
    - destinataire deconnecté
    - TTL (temps moyen d'aller-retour à une machine) insuffisant
    - congestion des routeurs intermédiaires
    - checksum erroné
    - mauvaises tables de routage
    - . . .
  - néanmoins, les erreurs ne sont pas toutes détectables

Le protocole ICMP

- Causes des erreurs
  - lorsqu'une erreur (dans la remise d'un datagramme) est détectée par un routeur ou la station destinataire, un rapport d'erreur (message ICMP) est envoyé a l'émetteur (d'origine) du datagramme

Le protocole ICMP

- Les messages d'erreur ICMP



  - Le message inclut au moins 28 octets (l'en-tête et les 64 premiers bits) du datagramme ayant causé l'erreur, contenant les en-têtes des protocoles de niveau supérieur, ce qui permet notamment de déterminer le processus émetteur pour l'informer

Le protocole ICMP

- La commande **ping**
  - Envoie un message ICMP de demande d'écho
  - La destination renvoie un message ICMP de réponse d'écho
  - Permet de savoir si une machine est en route et accessible
  - Mesure le temps moyen aller-retour à cette machine (RTT)

Le protocole ICMP

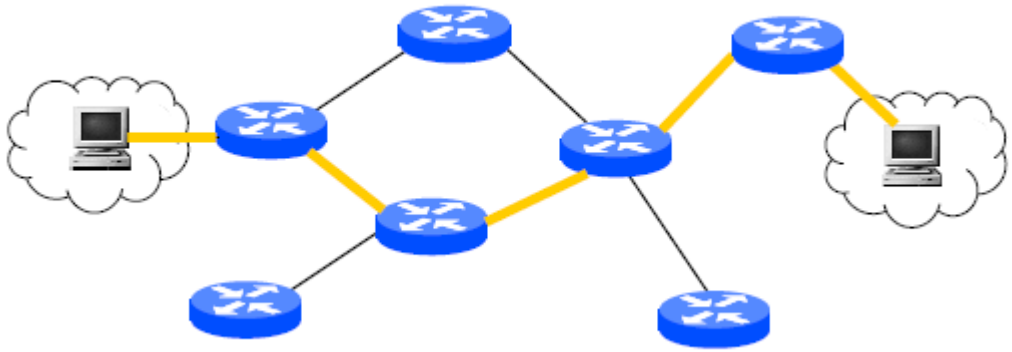
- La commande **traceroute**
  - Envoie un paquet UDP avec un TTL égal à 1
  - Puis recommence en augmentant le TTL de 1 à chaque envoi
  - À chaque fois que le TTL arrive à 0, le routeur renvoie un message ICMP d'erreur (« Time-to-live exceeded »)
  - Permet de connaître la route exacte empruntée

Routage IP

- Principes
  - Le protocole IP est capable de choisir un chemin (une route) suivant lequel les paquets de données sont relayés de proche en proche jusqu'au destinataire
  - A chaque relais sur la route correspond un routeur (gateway)
    - L'ordinateur émetteur du paquet de données doit trouver le premier relais
    - Chaque routeur remet le paquet sur le réseau destinataire
  - Le routage IP fonctionne de façon décentralisée : aucun nœud du réseau n'a une vision globale de la route que prendront les paquets de données

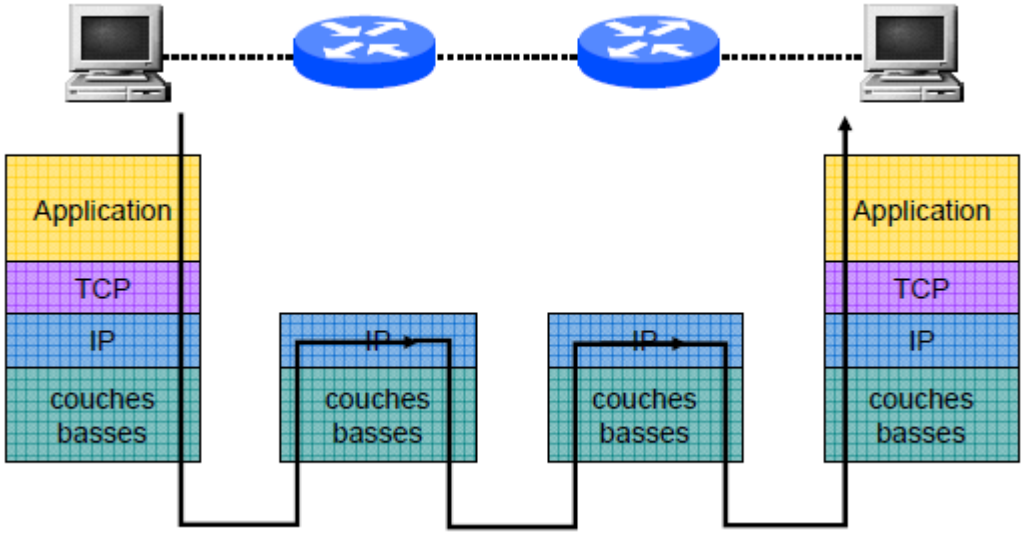
Routage IP

- Principes
  - Chaque routeur ne connaît que le prochain routeur sur le chemin
  - Le datagramme est ainsi acheminé de routeur en routeur jusqu'à la destination



Routage IP

- Cheminement du datagramme



Les tables de routage

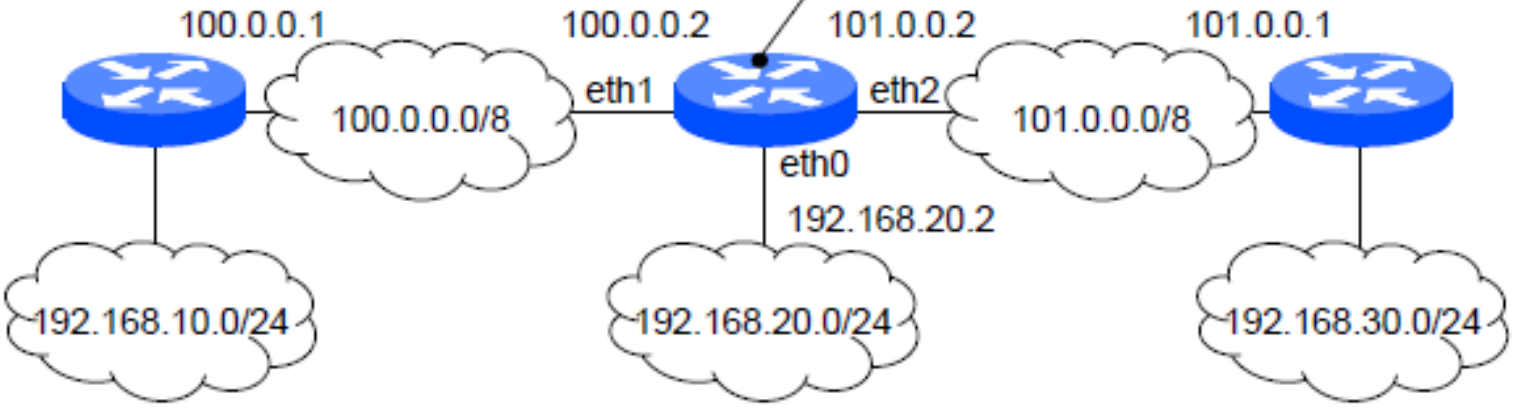
- Chaque équipement possède
  - Une interface sur chaque réseau sur lequel il est connecté
    - Sous Linux, ces interfaces portent les noms eth0, eth1...
  - Une table de routage qui contient essentiellement deux types d'information
    - des adresses réseau
    - et le moyen de les atteindre
    - si le réseau est directement connecté à l'appareil, le moyen d'atteindre le réseau est le nom de l'interface
    - sinon, il s'agit de l'adresse du routeur de prochain pas (« next hop ») situé sur la route vers ce réseau

Les tables de routage

- La table de routage est présente dans les hôtes comme dans les routeurs
  - Un hôte ne traite que les paquets dont il est l'émetteur
  - Un routeur traite tous les paquets reçus et dont il n'est pas l'émetteur
- La mise à jour de la table de routage peut être
  - Manuelle : routage STATIQUE
  - Automatique : routage DYNAMIQUE
- Accès à la table de routage
  - d'une station Unix : netstat -r[n]
  - d'un routeur (CISCO) : show ip route [sum]

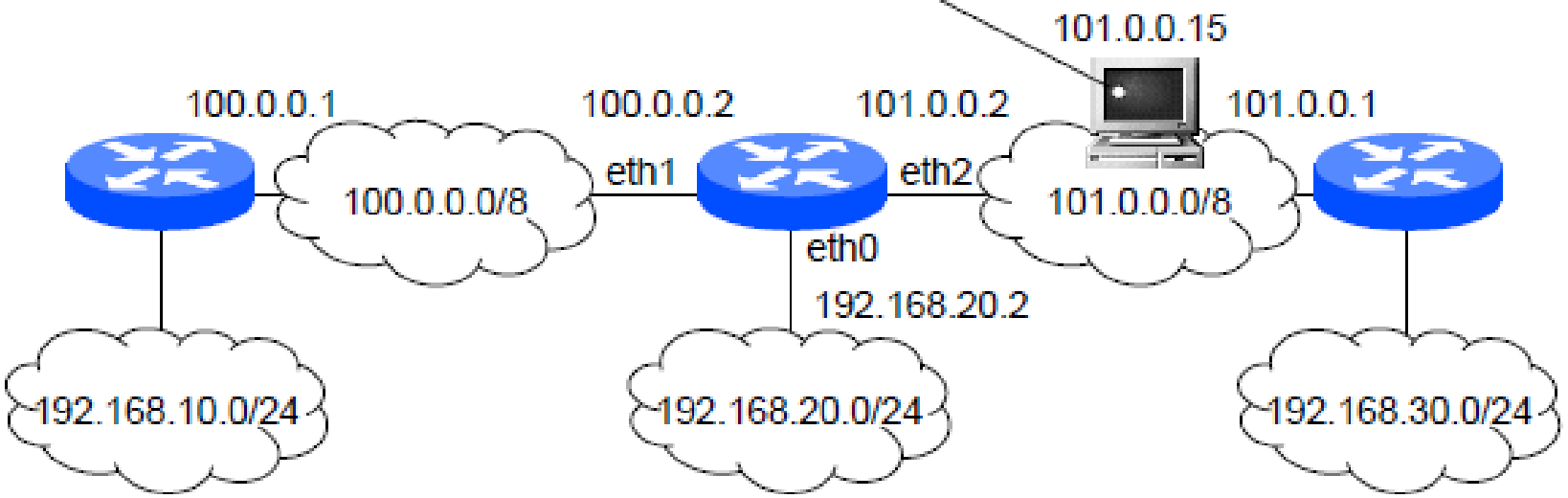
Les tables de routage

Destination	Moyen de l'atteindre
192.168.20.0/24	eth0
100.0.0.0/8	eth1
101.0.0.0/8	eth2
192.168.10.0/24	100.0.0.1
192.168.30.0/24	101.0.0.1

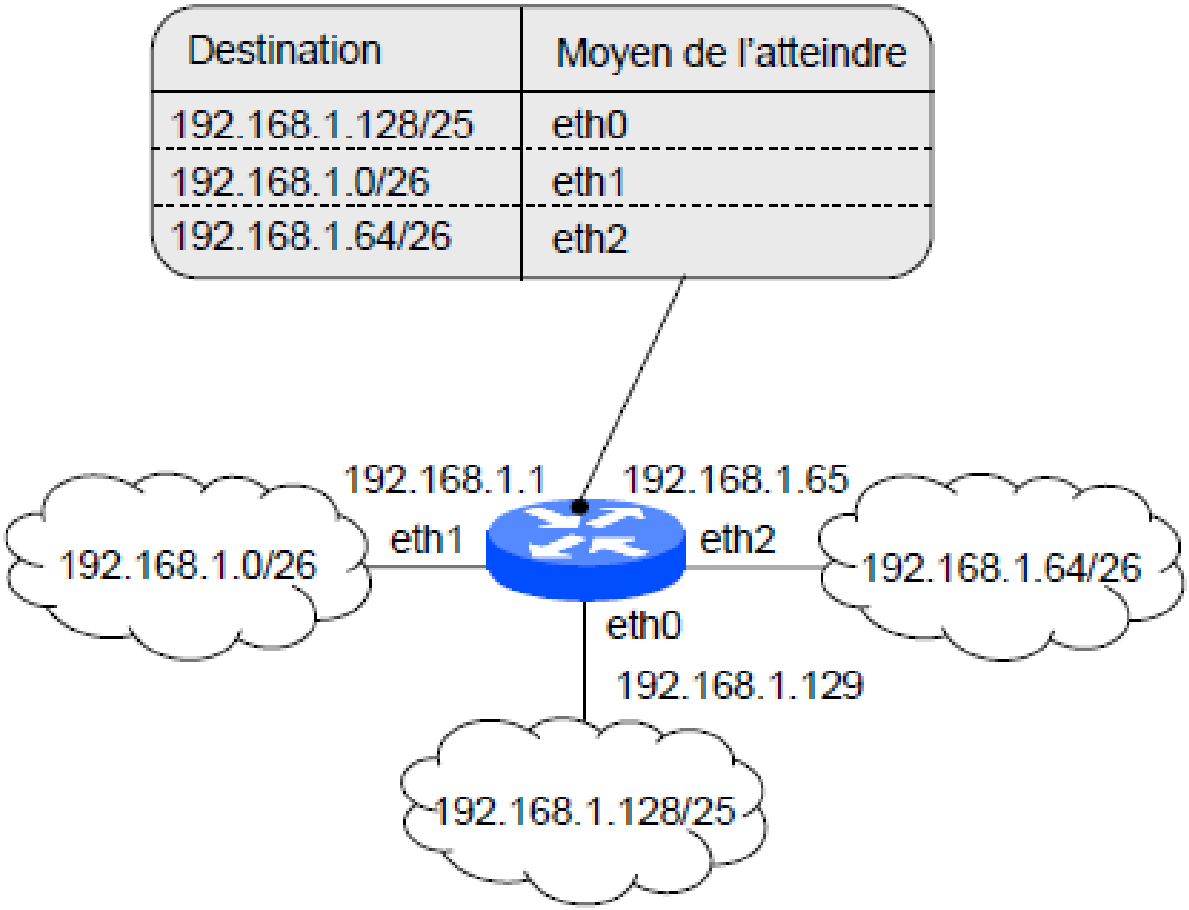


Les tables de routage

Destination	Moyen de l'atteindre
101.0.0.0/8	eth0
192.168.30.0/24	101.0.0.1
0.0.0.0	101.0.0.2



Routage entre sous-réseaux



La table de routage et la passerelle

- La table de routage
  - Les lignes de la table sont composées ainsi :
    - L'adresse IP du réseau IP de destination (ou l'adresse IP d'un poste)
    - Le masque de sous réseau correspondant à cette adresse (qui sera tout à 255 si l'adresse précédente est l'adresse d'un poste)
    - L'adresse IP du routeur (passerelle) qui est le premier routeur permettant de se diriger vers ce réseau (où vers ce poste)
    - L'adresse IP de l'interface réseau (carte ou autre) qui permet d'atteindre ce routeur

- Le routage se déroule ainsi :
  - on applique sur l'adresse IP destinataire du paquet le masque de sous-réseau pour extraire la partie réseau de cette adresse
  - on compare cette adresse avec l'adresse IP de destination de la table de routage
  - si cette adresse est différente on passe à la ligne suivante
  - si cette adresse correspond, on récupère via le protocole ARP l'adresse MAC du routeur et on transmet le paquet via l'interface spécifiée sur la ligne (l'entête de la trame est donc constituée de l'adresse MAC du routeur et de l'adresse MAC de le l'interface alors que les adresses IP du paquet n'ont pas été modifiées)
  - si aucune adresse réseau de la table ne correspond à l'adresse réseau demandée, le paquet est routé vers une route par défaut si elle existe ou bien n'est pas routé si cette route par défaut n'existe pas
  - L'adresse par défaut s'exprime souvent de la façon suivante : 0.0.0.0 masque 0.0.0.0 (mais peut s'exprimer avec le mot réservé ***default***)

Établir des routes

- Qu'est-ce qu'une passerelle ?
  - C'est le premier routeur de votre réseau local vers l'extérieur

Établir des routes

- Comment sont construites les tables de routage ?
  - La table de routage d'un poste est construite automatiquement dans un premier temps à partir de son adresse IP, de son masque et de son adresse de passerelle
    - donc il y aura autant de lignes que d'adresses IP

Établir des routes

- Interconnexion de réseaux distants
  - Un routeur est connecté à plusieurs réseaux
  - Sur chacun de ces réseaux, **il peut remettre directement les paquets**
  - Mais comment fait-il si ces paquets ne sont pas destinés au réseau auquel il est connecté ?
    - Il doit connaître un routeur à qui les remettre
    - L'adresse IP de ce routeur lui est donnée par sa table de routage
  - Cela sous-entend qu'un routeur prend en charge des paquets à destination de réseaux sur lesquels il n'est pas connecté. **Il fait de la remise indirecte**

Établir des routes

- Interconnexion de réseaux distants
  - Une route est constituée par l'ensemble des postes traversés par un paquet entre le poste désigné par l'adresse IP source et le poste désigné par l'adresse IP destinataire
  - Avec IP, les postes ne connaissent pas la totalité des postes constituant la route mais uniquement le prochain poste sur la route
  - Chaque paquet est routé individuellement

Établir des routes

- Une route indirecte ne peut pas être connue automatiquement par le routeur
- Cette information doit lui être donnée :
  - soit statiquement : dans ce cas, l'administrateur réseau rajoute manuellement la ligne
  - soit dynamiquement : dans ce cas, la ligne est rajoutée par un **protocole de routage** (les protocoles de routage sont RIP, OSPF, etc.)

Le protocole de routage

- Principe
  - Un protocole de routage permet aux routeurs de s'informer sur les routes à prendre par :
    - propagation automatique des informations de routage
    - mise à jour permanente des informations
  - Il y a deux familles de protocoles
    - routage à vecteur de distance
    - routage à états de liaison

Le protocole de routage

- Routage à vecteur de distance
  - Chaque routeur démarre avec un ensemble initial de routes auquel il est relié
  - Chaque entrée identifie un réseau de destination mais indique la distance exprimée en nombre de sauts (bonds) qui sépare le routeur de ce réseau
    - Cette distance est exprimée sous la forme d'un entier
    - Une valeur de 1 correspond à une remise directe
  - Les routeurs s'échangent les couples : adresse destination + distance

- Le protocole RIP
  - RIP (*Routing Information Protocol*) est le protocole le plus couramment utilisé dans les réseaux locaux
    - *démon routed* sur unix, service RIP sur windows
  - Principe :
    - diffusion toutes les 30s des couples (adresse destination + distance) aux routeurs adjacents
    - le routeur qui reçoit le message, incrémente la distance puis insère la destination dans sa table si cette destination est nouvelle ou si la distance est inférieure à la distance déjà enregistrée pour cette destination
    - lorsqu'un routeur ne reçoit pas de message d'un routeur adjacent pendant 3 intervalles de temps, il invalide les routes associées à ce routeur
    - une distance de 16 invalide la route

D'autres protocoles

La couche Transport

Couche Transport

- Deux protocoles pour la communication entre applications
  - TCP : Transmission Control Protocol
    - Protocole orienté connexion
    - Offre de la fiabilité (pas de perte, pas d'erreur)
    - Ordonné
    - Contrôle de flux
  - UDP : User Dtagram Protocol
    - Mode sans connexion
    - Pas de contrôle d'erreur (sans garantie)

Couche Transport

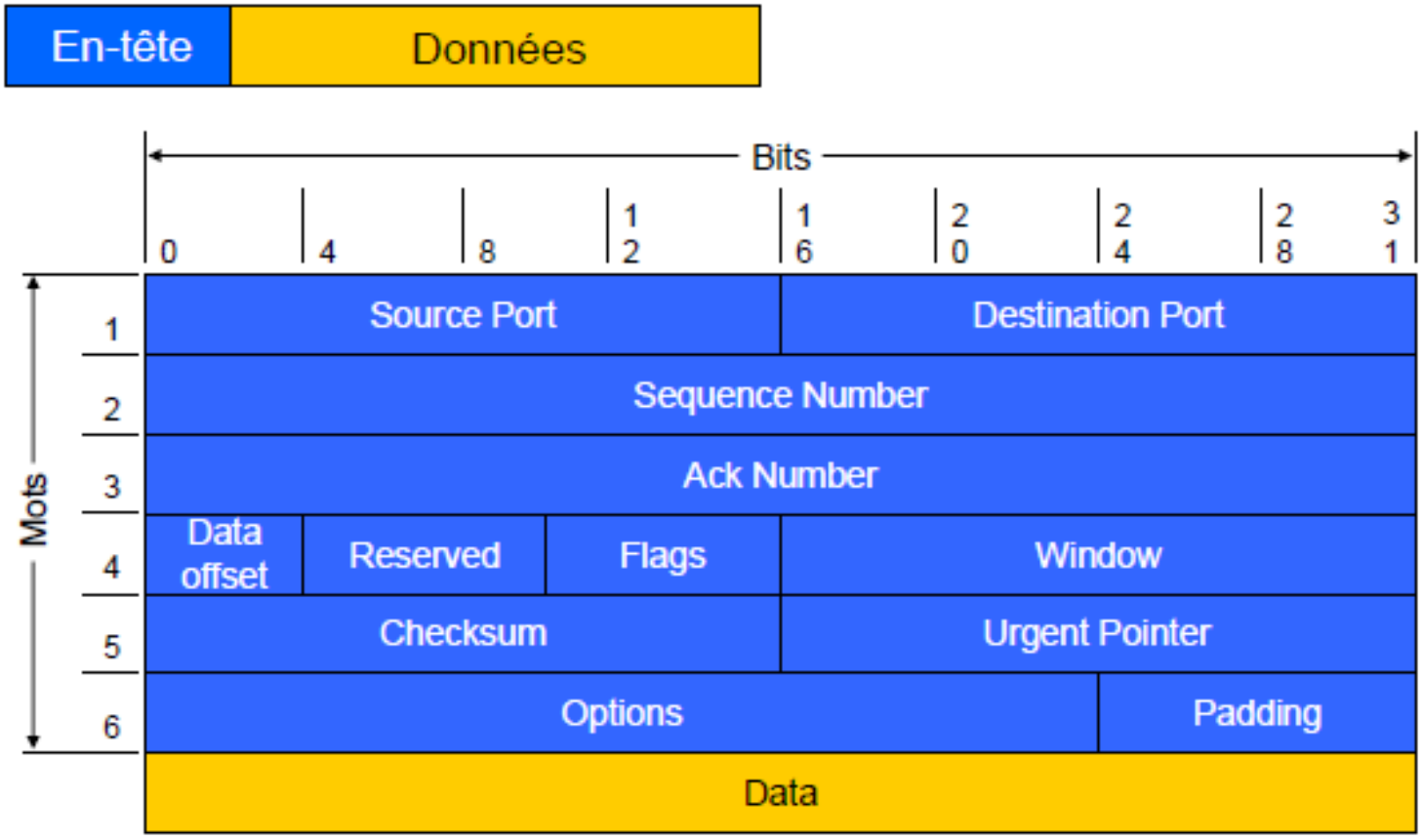
- Identification d'une application par un numéro de port
- Socket : combinaison d'une @ IP et d'un numéro de port
- La combinaison de 2 sockets définit complètement une connexion TCP ou un échange UDP
- Ports prédéfinis (RFC 1060) pour les services :
  - 20 : FTP
  - 22 : SSH
  - 23 : Telnet
  - 25 : SMDP
  - 53 : DNS
  - 69 : TFTP
  - 80 : HTTP

Le protocole TCP

- Le protocole de transport TCP
  - Par rapport au protocole IP, le protocole TCP a un rôle de fiabilisation du transport entre deux extrémités
  - TCP fabrique les paquets qui seront routés par IP à partir des données fournies par les protocoles clients ou serveurs
  - La taille de ces paquets est déterminée par le **MTU (Maximum Transfer Unit)** de la couche liaison
  - TCP numérote chaque paquet
  - Ce numéro sert à remettre dans l'ordre les paquets si ceux-ci arrivent dans le désordre
  - Mais ce numéro sert aussi à vérifier que les paquets sont bien arrivés

- Tous les paquets ne sont pas acquittés
  - Le protocole TCP émetteur négocie avec le protocole TCP récepteur le nombre de paquets transmis sans accusé de réception
  - Lorsque TCP acquitte un paquet, cela signifie qu'il a reçu tous les paquets intermédiaires
  - En cas de non-acquittement, le protocole TCP émetteur renvoie les paquets
- Pour pouvoir mettre en œuvre l'acquittement des paquets, il faut que le récepteur soit actif
  - TCP au niveau émetteur établit une connexion avec le protocole TCP au niveau du récepteur
  - Les paquets ne sont transmis que si la connexion est établie
  - En cas de rupture de connexion, il y a abandon de la remise des paquets et signalement à l'application utilisatrice du service TCP
- Une analogie peut-être établie avec le téléphone

Format du segment TCP

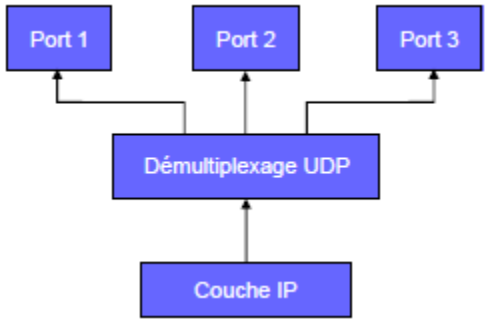


Le protocole de transport UDP

- Principe
  - UDP est un protocole allégé par rapport à TCP
  - UDP fabrique les paquets et les envoie
  - Par contre il n'établit pas de connexion préalable et ne peut donc garantir une remise fiable
  - C'est donc au niveau application que doivent être détectés les problèmes de transmission
  - Une analogie peut-être établie avec la boite aux lettres

UDP

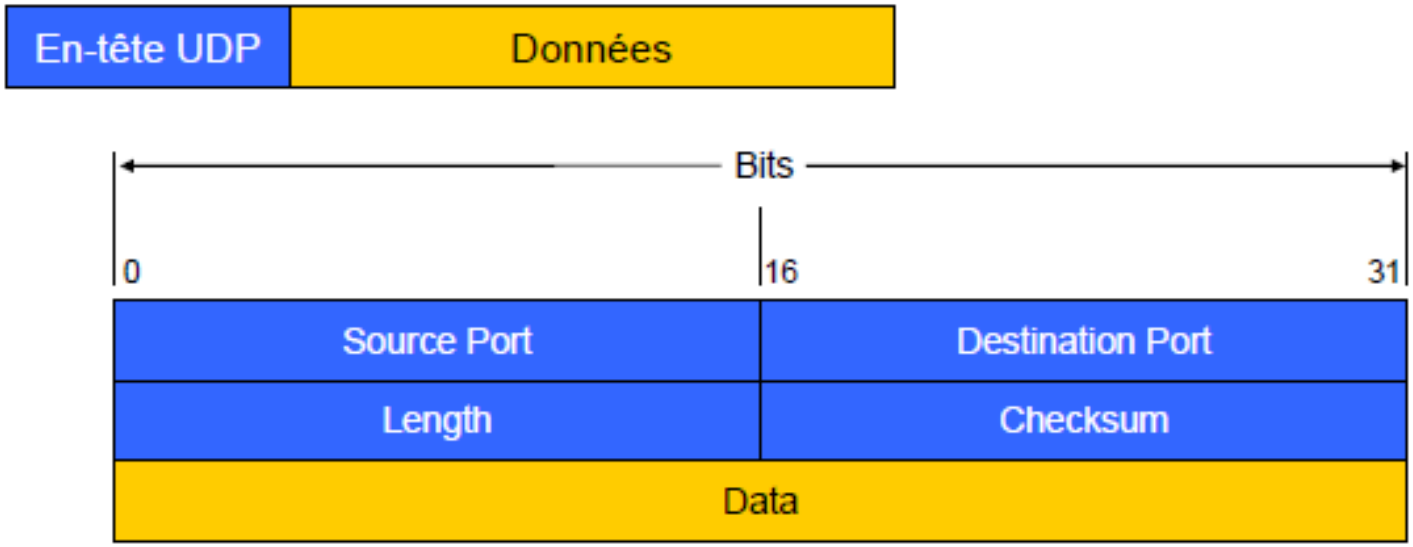
- Le démultiplexage



- Ce que UDP ne fait pas
  - Mode connecté
  - Retransmission en cas d'erreur
  - Séquencement
  - Contrôle de flux

Format du paquet UDP

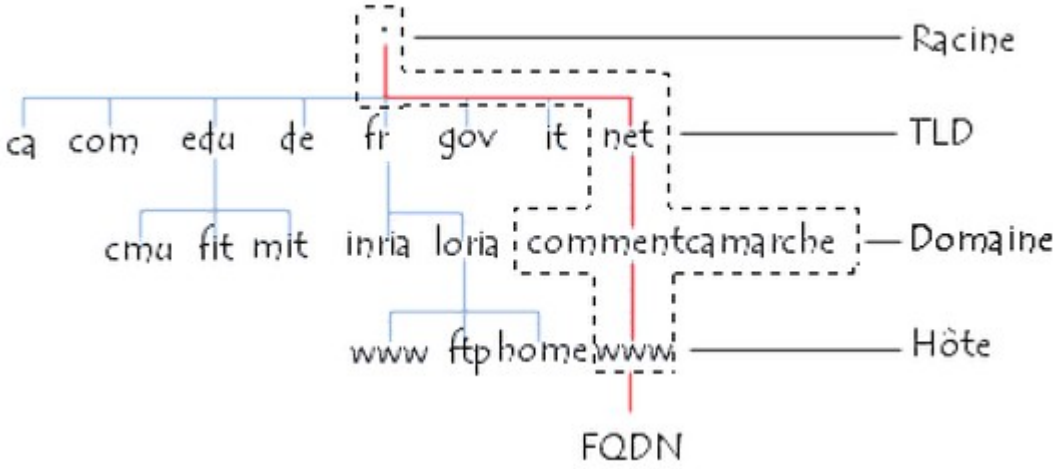
- UDP (RFC 768)
  - Service sans connexion, sans garantie, utilisant IP pour le transport de messages

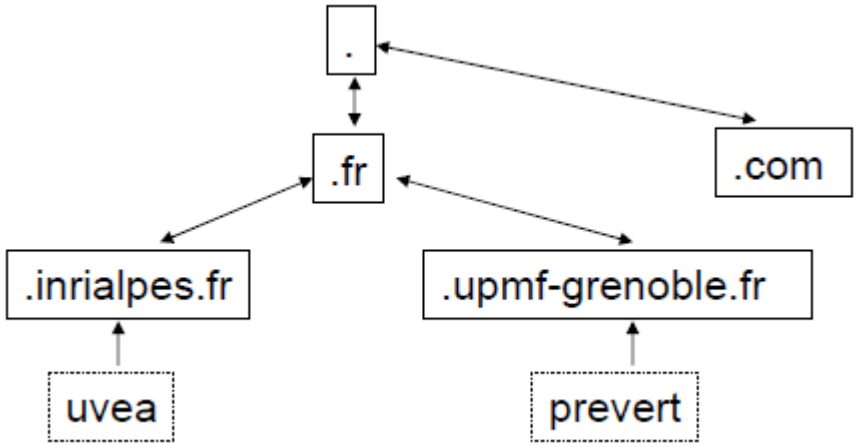


Le protocole DNS

- Domain Name Server
  - Correspondance entre un nom et une adresse IP
  - Exemple :
    - prevert.umpf-grenoble.fr ⇔ 195.221.42.159
  - Noms plus faciles à retenir que les adresses IP

- Hiérarchie des serveurs
  - L'espace de noms est organisé en une hiérarchie au sommet de laquelle figure la racine et immédiatement en dessous les TLD (Top-Level Domain) ou domaines de niveau supérieur :





DNS

- L'ICANN (Internet Corporation for Assigned Names and Numbers)
  - a en charge la création des TLD et a créé notamment les TLD suivants :
    - com : entreprises commerciales
    - edu : établissements d'enseignement
    - org : organisations diverses
    - un TLD par code pays sur 2 lettres (norme ISO 3166) :
      - fr : France
      - uk : Royaume-Uni
      - de : Allemagne
      - tv : île Tuvalu (qui en prote bien. . .)

DNS

- La résolution de noms
  - Tout hôte doit connaître au moins un serveur de noms (en principe de son domaine)
  - Sur un hôte, le client DNS effectuant la résolution de noms est appelé solveur de noms
  - Pour résoudre un nom, il a deux possibilités :
    - résolution récursive : demanderà son serveur de le résoudre et si le serveur ne connaît pas la réponse, il contactera un autre serveur, etc., et la réponse reviendra
    - résolution iterative : demander à son serveur de le résoudre et si le serveur ne connaît pas la réponse, il lui dira quel serveur est susceptible de la connaître. Le solveur contactera alors ce serveur, etc., jusqu'à contacter un serveur en mesure de lui répondre

- La résolution de nom
  - Exemple où la machine uvea.inriaalpes.fr veut obtenir l'adresse IP prevert.upmf-grenoble.fr :
    - Uvea demande au serveur de DND de .inriaalpes.fr l'adresse IP de prevert.upmf-grenoble.fr
    - Si ce serveur ne connaît pas l'adresse de prevert, il va la demander au DNS de .fr
    - Si ce dernier ne connaît pas l'adresse de prevert.upmf-grenoble.fr, il va la demander au serveur de DNS de .ump-grenoble.fr dont il connaît l'adresse
    - Le serveur de DNS de .umpf-grenoble.fr renvoie alors l'adresse de prevert au serveur de DNS de .fr qui la renvoie au serveur de DNS de .inrialpes.fr qui finalement la renvoie à uvea.inrialpes.fr

Achat/dépôt d'un sous-domaine

- Se fait généralement pour une durée limitée (1 à 10 ans) auprès d'un enregistreur
- Doit être associé à l'identité et l'adresse postale d'une personne qui doit fournir 3 types d'informations :
  - Administrative Contact : responsable du sous-domaine
  - Billing Contact : payeur du sous-domaine
  - Technical Contact : responsable technique du sous-domaine
  - le tout pouvant être la même personne
- Ces informations sont publiques et consultables par tout le monde :
  - sous Unix, en utilisant la commande whois
  - sur le Web, grâce à des serveurs WHOIS (ex : http://www.whois.net)

FTP (File Transfert Protocol)

- Application pour transférer des fichiers (RFC 959)
- Utilise 2 connexions TCP (==> transfert fiable)
  - 1 de contrôle (commandes et réponses) : port 21
  - 1 de transfert de données : port 20
  - Cette connexion est ouverte puis fermée à chaque transfert
- Mode
  - Client : processus d'un utilisateur, par exemple
  - Serveur : démon ftpd traditionnellement par inetd sous Unix
- Le client ouvre la connexion
- Le serveur attend

FTP (File Transfert Protocol)

- FTP « classique »
  - Un nom d'utilisateur et un mot de passe sont fournis à l'ouverture de la connexion
- FTP anonyme
  - Autorise l'accès FTP à tout le monde
  - Connexion sous le nom d'utilisateur « anonymous »
  - Généralement réservé à des serveurs

FTP (File Transfert Protocol)

- Le transfert de fichiers peut être réalisé
  - En mode texte (ASCII sous Unix)
    - Suite d'octets avec 7 bits significatifs
    - Les fins de ligne, de page... sont détectées et transformées si besoin pour être adaptées à la machine cible
    - Il peut y avoir un transcodage : ASCII-EBCDIC
  - En mode binaire (Image)
    - Suite d'octets avec 8 bits significatifs
    - Aucune transformation est apportée

TELNET (Terminal NETwork Protocol)

- Terminal virtuel, remote terminal, terminal à distance (RFC 854)
- Utilise une une connexion TCP
  - Fiable mais gourmand en bande passante
  - Utilise le port 23 pour le serveur
- Modes
  - Client : processus d'un utilisateur
  - Serveur : démon telnetd qui est lancé par inetd sur Unix
- Le client ouvre la connexion

TELNET (Terminal NETwork Protocol)

- Un nom d'utilisateur et un mot de passe sont fournis à l'ouverture de la connexion
- L'utilisateur doit être déclaré sur le serveur
- Lorsque la connexion est ouverte, c'est une suite d'octets qui s'échangent
- Attention
- Les informations, dont le nom de l'utilisateur et son mot de passe, circulent en clair (sans chiffrement) entre le client et le serveur
- rlogin est le concurrent de telnet sous Unix