

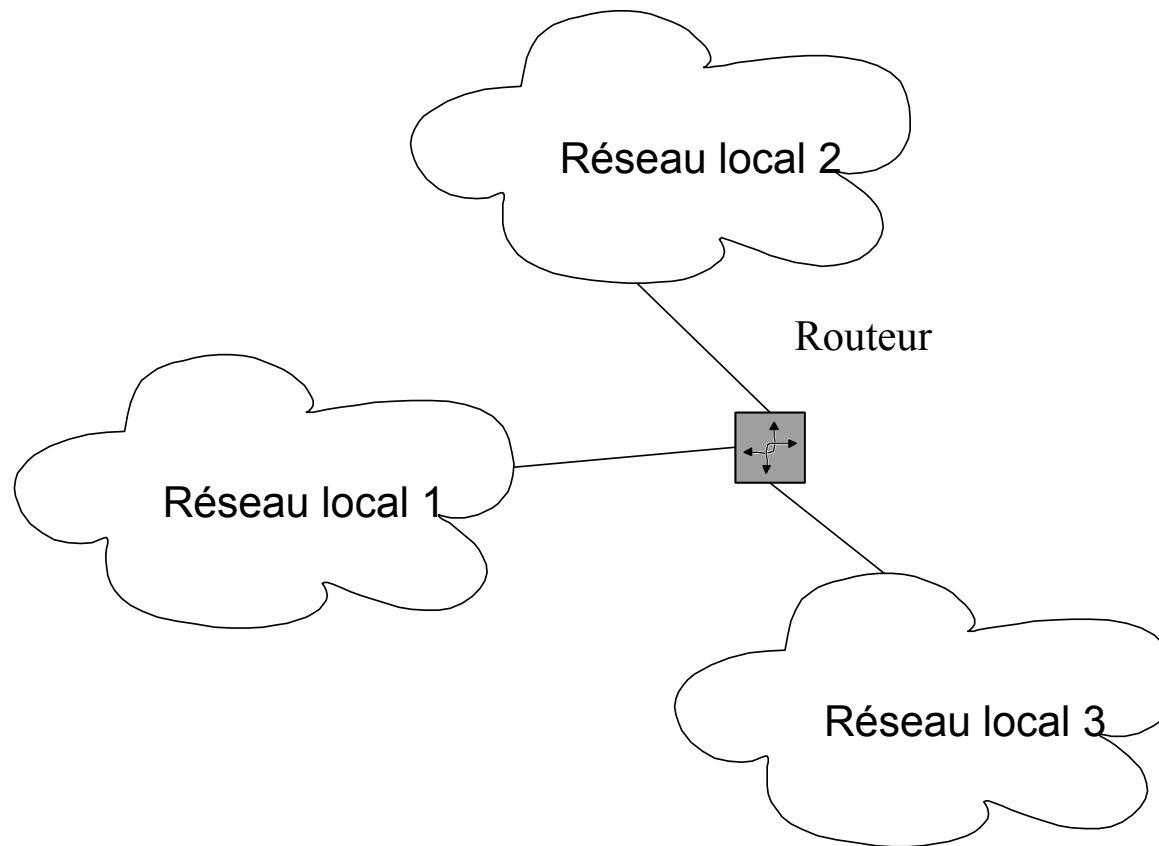


Couche réseau

Principe d'interconnexion de réseaux (1/2)

Synthèse

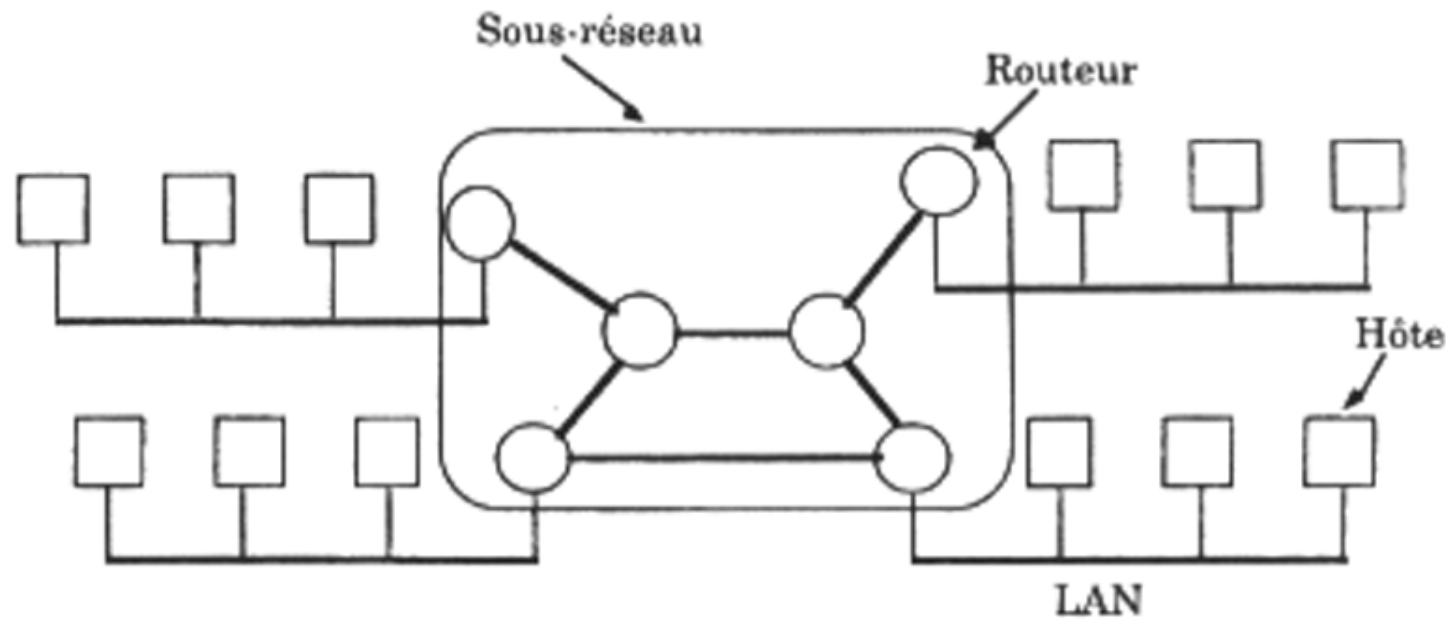
- des réseaux locaux à diffusion ;
- quand les distances augmentent il faut utiliser du point à point ;
- les machines doivent disposer d'un adressage pour pouvoir être jointe ;
- cet adressage doit être commun entre tous les réseaux ;
- il n'est pas nécessaire d'utiliser le même adressage à l'intérieur d'un réseau.



Principe d'interconnexion de réseaux (2/2)

Autre schéma

Ici il y a un sous réseau d'inter-connexion.



Exemple : Renater

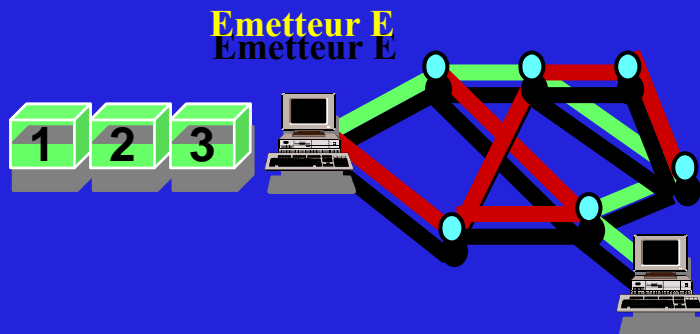
L'acheminement des paquets

Commutation et routage

Il existe deux techniques principales d'acheminement

1^{ère} technique : Commutation

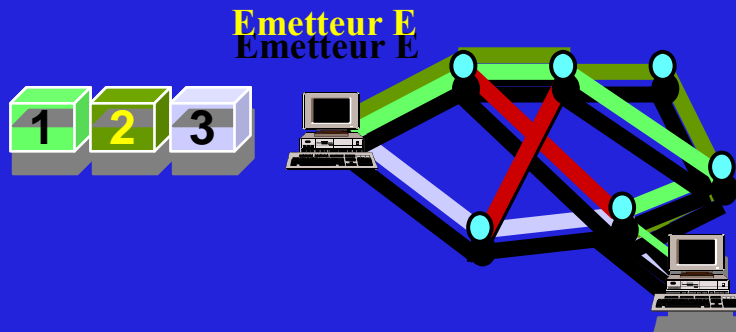
Les informations d'un même client suivent toujours un chemin déterminé à l'avance



- 1 info contient 1 référence décrivant le « circuit virtuel »
- Technique utilisée pour ATM

2^{nde} technique : Routage

Les informations d'un même client peuvent prendre des chemins différents



- 1 info contient 1 adresse complète de R
- Gestion d'une table de routage
- Technique utilisée pour Internet

Adresse IP

Adresse IP : <adresse réseau>.<adresse machine>

L'adresse IP est décomposée en deux parties :

- un identifiant de réseau
- un identifiant d'ordinateur dans ce réseau

Chaque ordinateur et chaque routeur du réseau Internet possède une **adresse IP**.

Chaque adresse IP est **unique**.

Elle est codée sur 32 bits.

Elle est représentée par commodité sous forme de 4 entiers variant entre 0 et 255 séparés par des points.

Exemple : 164 . 81 . 60 . 43 *une machine dans le bâtiment Jidé*

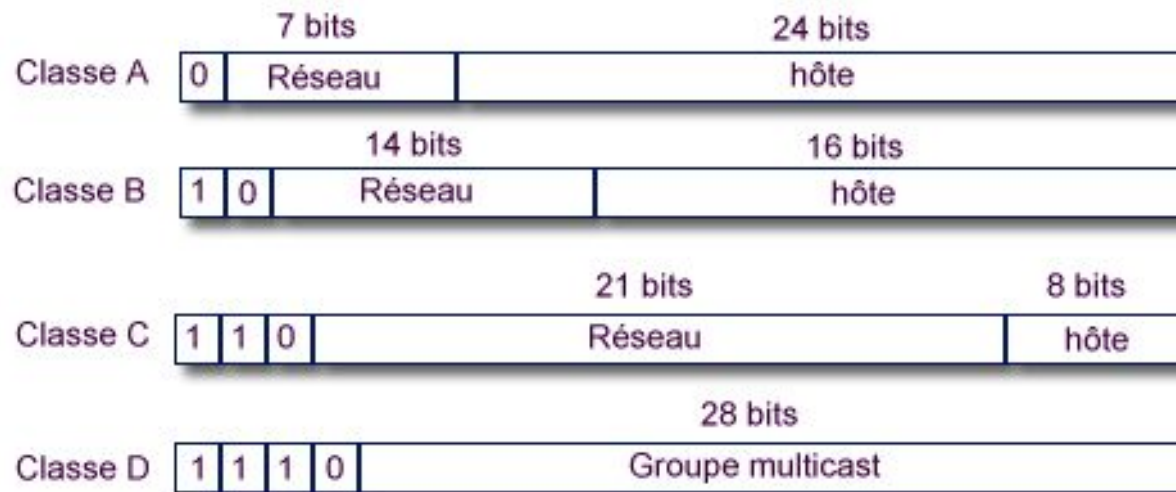
Un organisme officiel, le "NIC" (*Network Information Center*) est seul habilité à délivrer des numéros d'identification des réseaux.

Dans le cas d'un routeur interconnectant 2 réseaux différents, il possède une adresse IP pour chacun des réseaux.

Il existe différentes répartitions des 32 bits entre identifiant réseau et identifiant machine.

Ces différentes répartitions définissent un ensemble de **classes de réseaux**.

Les classes de réseaux



Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

Adresses IP réservées

Des adresses particulières

Ces adresses permettent d'effectuer :

- des envois de messages multi-destinataires
- désigner la machine courante
- désigner le réseau courant.

Tout à zéro		L'ordinateur lui-même
Tout à zéro	id. de machine	Un ordinateur sur le réseau lui-même
Tout à 1		Diffusion limitée au réseau lui-même
Id. de réseau	Tout à 1	Diffusion dirigée vers ce réseau
127	Nombre quelconque	Boucle

L'adresse de boucle (127.X.Y.Z) permet d'effectuer :

- des communications inter-programme sur la même machine
- des tests de logiciels réseaux.

Dans ces cas là, les paquets ne sont pas réellement émis sur le réseau.

- 0.0.0.0 est utilisé par une machine pour connaître sa propre adresse IP lors d'un processus d'amorçage. *Elle devra se procurer une adresse IP par l'intermédiaire d'une autre machine.*
- 255.255.255.255 est une adresse de diffusion locale car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. *pas de connaissance du réseau.*
- Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés appelés **intranet**.

La notion de sous-réseau

Partition d'un réseau en différents sous-réseaux.

Avantages :

Éviter d'avoir recours à plusieurs numéros de réseaux (classe A, B, ou C) pour regrouper différentes machines au sein d'une même entité (l'université de Limoges par exemple avec les machines du site de Jidé, du campus de Vanteaux, du campus de La Borie...).

L'ensemble des sous-réseaux est vu de l'extérieur comme un unique réseau (gestion du courrier...).

La mise en œuvre est logicielle :

- Définition de sous-réseaux en découpant l'identificateur machine en deux parties :
<id. de réseaux sur 16 bits>.<id. de sous-réseau sur 8 bits><id. de machine sur 8 bits>.

Le découpage autour du point facilite le travail des routeurs.

Une machine connecté à un sous-réseau doit connaître :

- son adresse IP,
- le nombre de bits attribués à l'identificateur du sous-réseau et à celui de la machine.

Masque de sous-réseau (*subnet mask*) :

c'est un mot de 32 bits contenant :

- des bits à 1 à la place de l'identificateur de réseau et de sous-réseau,
- des bits à zéro au lieu et place de l'identificateur de machine.

Ainsi, 255.255.255.0 indique que les premiers 24 bits désignent le sous-réseau.

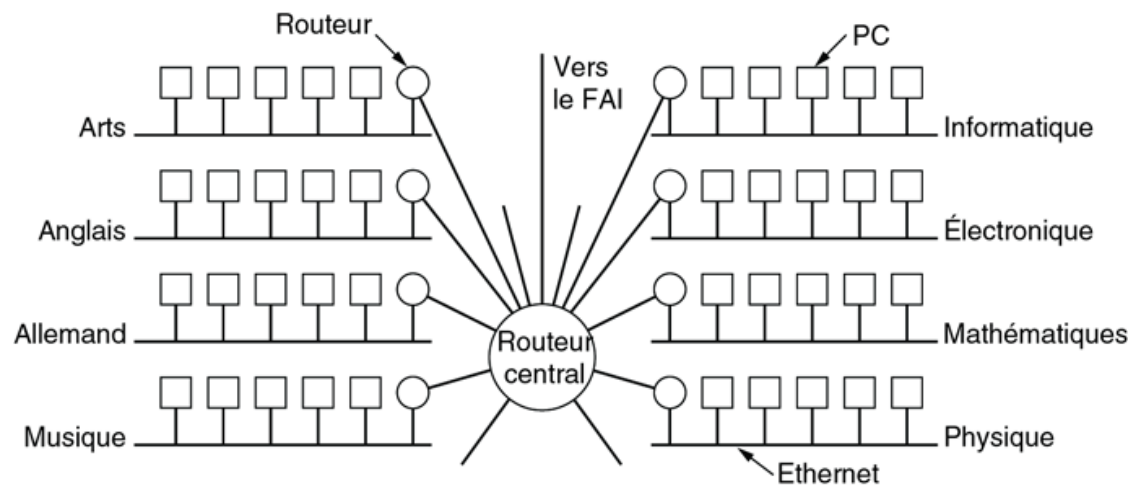
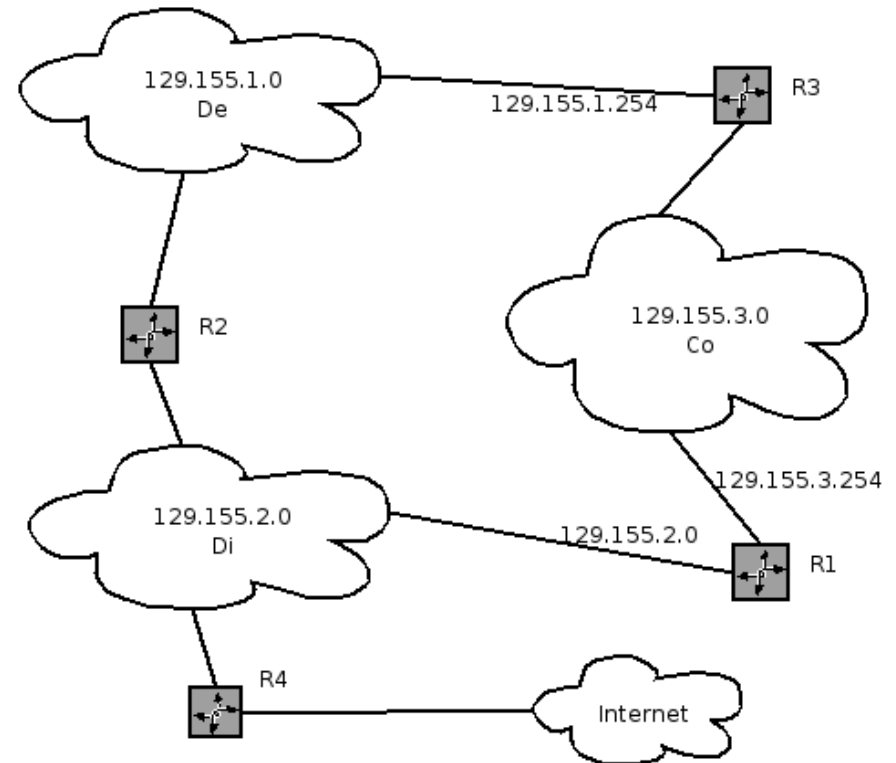
De cette manière à partir de l'adresse d'un datagramme et de son masque de sous-réseau une machine peut déterminer si le datagramme est destiné à une machine sur son propre sous-réseau ou à une machine extérieure.

Exemple de réseaux et notion de routage

On remarque :

- 3 sous réseaux
- le réseau internet
- 4 routeurs avec chacun 2 IP !
- plusieurs routages possibles

On peut localiser une machine dans les sous-réseaux



Création d'un réseau

Il faut :

- choisir une classe de réseau en fonction du nombre de machines à connecter en prenant en compte les besoins actuels et futurs ;

- choisir une adresse de réseau dans la classe choisie.

Exemple : 192.168.12.0 pour un réseau intranet

- affecter une adresse IP unique à chaque machine connectée au réseau :

Exemple : <192.168.12>.<1> la machine de Paul

<192.168.12>.<2> la machine de Nathalie

<192.168.12>.<20>

...

10 adresses réservées pour les postes des élèves

<192.168.12>.<29>

- noter chaque adresse et la machine à laquelle elle est affectée.

Cela facilite le travail de l'administrateur du réseau !

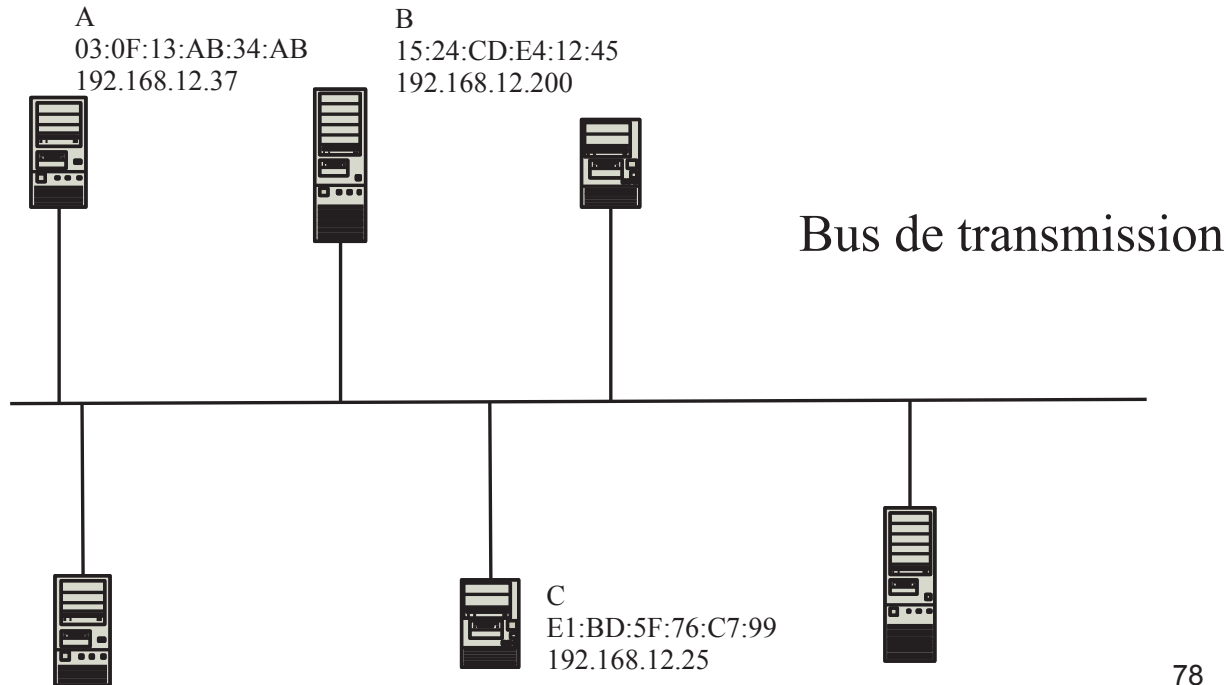
Dialogue dans un réseau local

Comment échanger réellement sur un réseau local à diffusion ?

Les machines ont chacune une carte réseau ;

Chaque carte a une adresse **MAC unique** donnée par le constructeur ;

Chaque machine dispose d'une **adresse IP** donnée par l'administrateur du réseau.



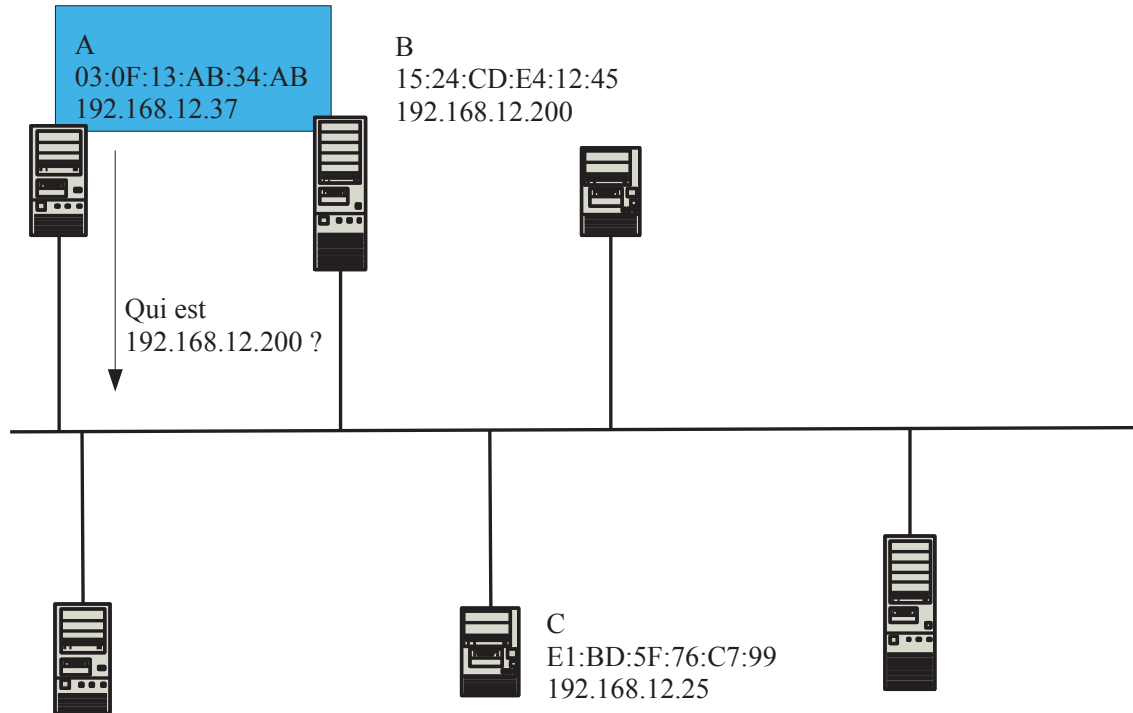
Dialogue dans un réseau local

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



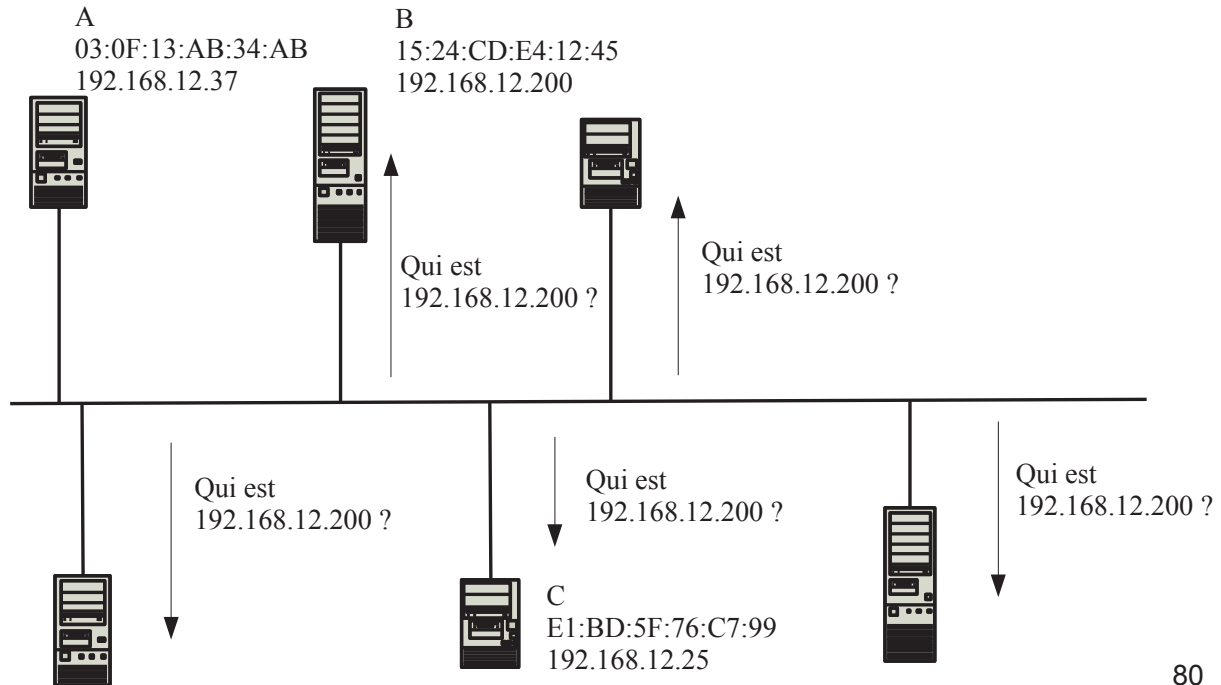
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



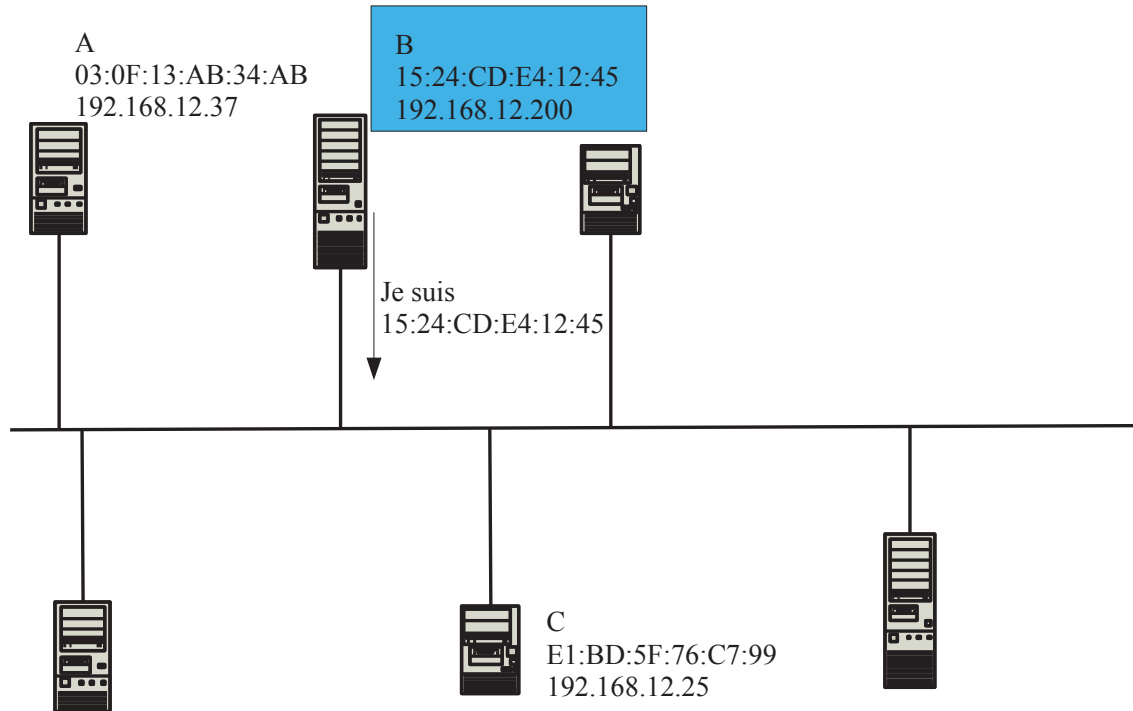
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



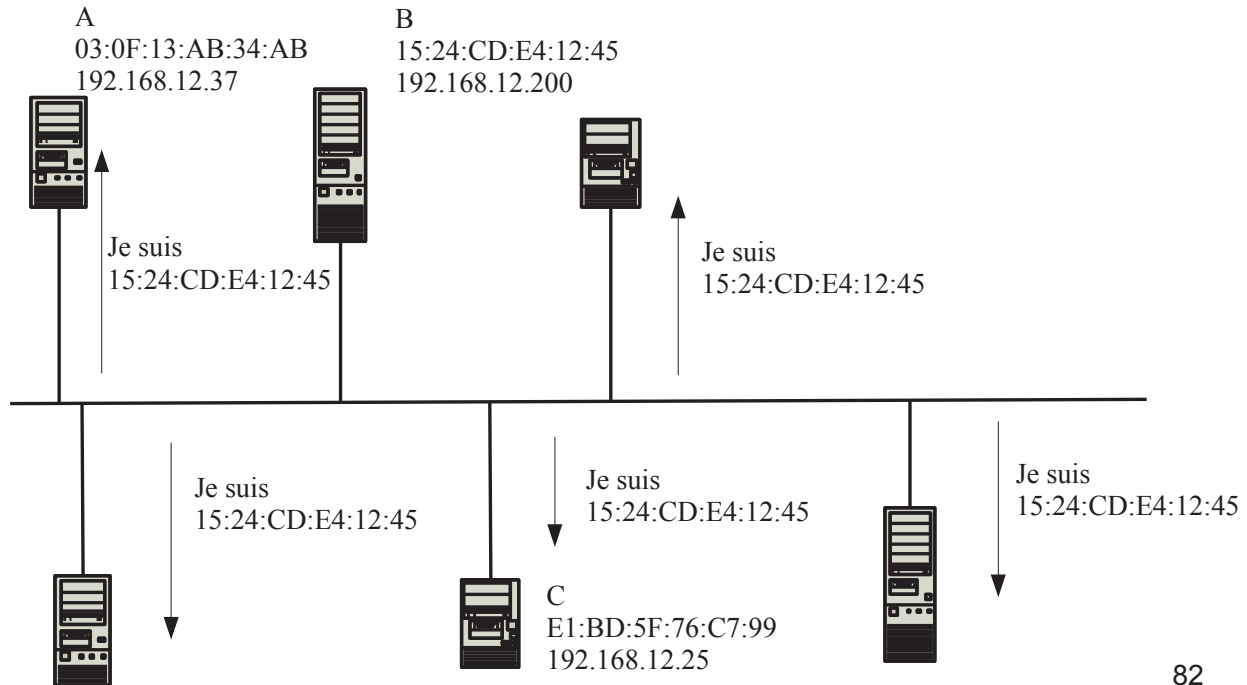
Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.

Comment obtenir l'adresse MAC de B ?

Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Dialogue dans un réseau local : trouver le destinataire

A connaît maintenant l'adresse MAC de B elle peut communiquer avec B.

Les autres machines ont également reçu le message de B, elles peuvent le conserver au cas où elles ont auraient besoin !

Correspondance entre adresses physiques MAC et adresses IP

Le protocole **ARP** "*Address Resolution Protocol*" :

il fournit une correspondance dynamique entre une adresse IP connue et l'adresse matérielle lui correspondant.

On parle de requête ARP pour la demande envoyée par une machine.

Le protocole **RARP** "*Reverse Address Resolution Protocol*" :

Il réalise l'opération inverse : une machine sans adresse IP connue peut envoyer une requête RARP pour demander son adresse IP.

Une machine particulière (un serveur gérant le réseau) lui répond et lui affecte son adresse IP.

Cette machine dispose d'une table de correspondance : (adresse physique, adresse IP).

Le protocole RARP est utile pour amorcer une station sans disque ou un Terminal X-Window.

Routage

Algorithme de routage par sauts successifs “next hop routing”

L’entité réseau (ordinateur ou routeur) doit déterminer l’adresse de prochain saut, c-à-d. la première étape du chemin d’acheminement du paquet à transmettre.

Un saut correspond à la transmission d’un paquet à un routeur ou à la machine destinataire.

Deux possibilités :

- le routage direct : Si la destination se trouve sur le même réseau, l’adresse de prochain saut est l’adresse IP simplement.
- le routage indirect : Sinon l’adresse de prochain saut doit être un routeur, c-à-d. qu’au moins un routeur sépare l’expéditeur initial et le destinataire final.

Localisation de la machine destinataire

Chaque ordinateur connecté au réseau Internet dispose d’une adresse IP et d’un masque de sous-réseau (indiquant la répartition des 32 bits d’adresse IP entre l’identification du réseau ou sous-réseau auquel il appartient et son identification au sein de ce réseau).

Lors de l’envoi d’un paquet à destination d’une machine D, l’algorithme de routage est le suivant :

- comparaison de l’adresse de D avec le masque de sous-réseau et le sous-réseau
- si égalité alors la destination est sur le même réseau physique

Utilisation de la diffusion pour assurer le transfert direct

- sinon c’est un **routage indirect** on diffuse jusqu’au routeur par défaut (car il appartient au réseau local) et c’est lui routera ensuite le paquet vers le bon sous réseau en fonction ses tables de routage

=> On est sorti de son sous-réseau grâce au routeur !

Le paquet IP (1/2)

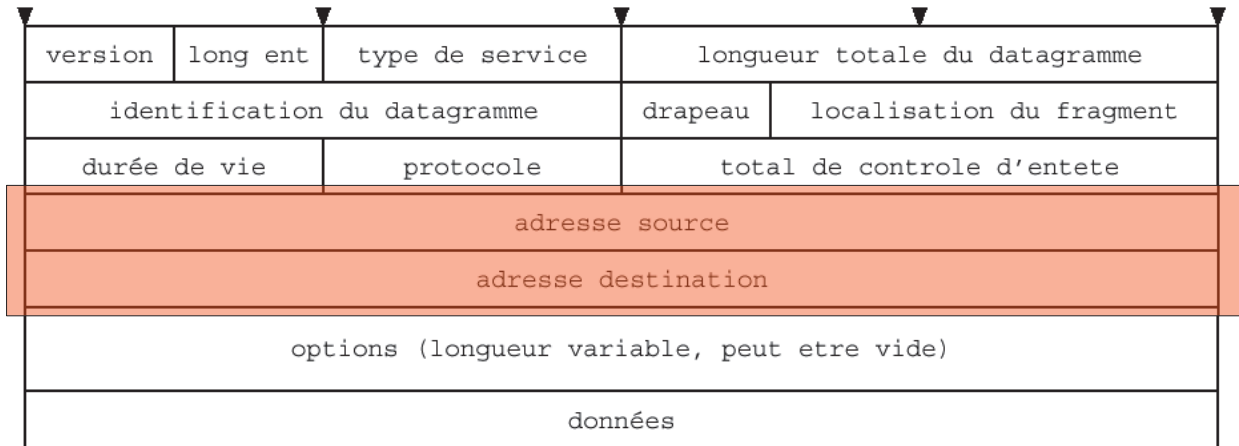
Le paquet ou datagramme IP

Il contient :

- l'adresse IP de la machine qui a envoyé le paquet ;
- l'adresse IP de la machine cible.

Munis de ces informations le paquet devient un datagramme.

Il est autonome et peut être « router », c-à-d. acheminer à travers le réseau.



Le paquet IP (2/2)

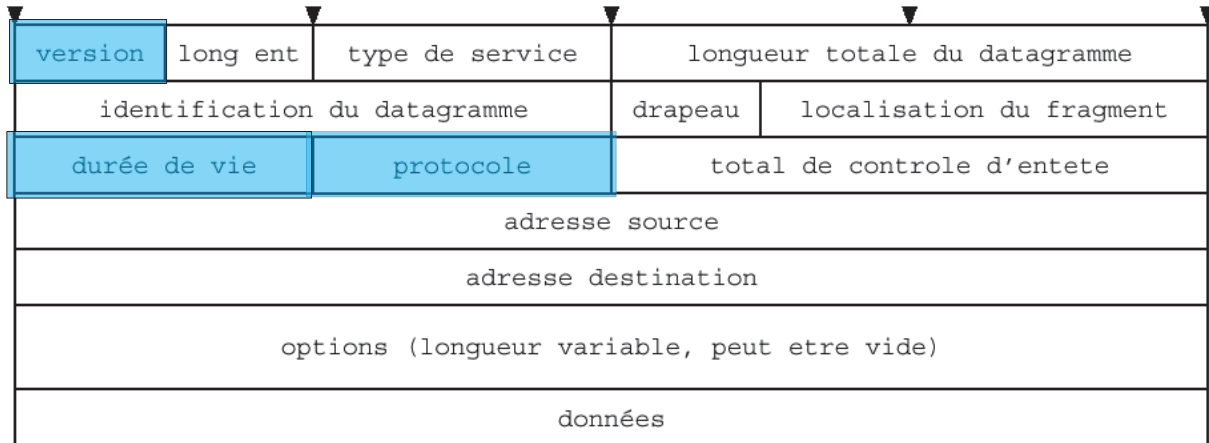
Le paquet ou datagramme IP

Le datagramme contient également :

- un **numéro de version** : actuellement on est à la version 4 ;
- une **durée de vie** : le paquet est détruit s'il reste trop longtemps dans le réseau :
 - la destination n'est pas accessible ;
 - le routage a été mal fait...

Cela permet de ne pas saturer le réseau !

- le **type de protocole** : cela correspond à la forme du dialogue (mode connecté ou non – *cf plus loin*).



ICMP (½)

Le protocole ICMP (Internet Control Message Protocol) :

Il permet de gérer les informations relatives aux erreurs aux machines connectées.

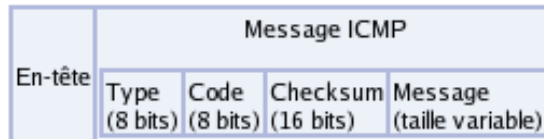
Étant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem).

Les messages ICMP sont encapsulés

Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs.

Toutefois, en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet "**boule de neige**" en cas d'incident sur le réseau.

Voici à quoi ressemble un message ICMP encapsulé dans un datagramme IP:



ICMP (2/2)

Signification des messages ICMP

Type	Code	Message	Signification du message
8	0	Demande d'ECHO	Ce message est utilisé lorsqu'on utilise la commande <i>PING</i> . Cette commande, permettant de tester le réseau, envoie un datagramme à un destinataire et lui demande de le restituer
3	0	destinataire inaccessible	Le réseau n'est pas accessible
3	1	destinataire inaccessible	La machine n'est pas accessible
3	2	destinataire inaccessible	Le protocole n'est pas accessible
3	3	destinataire inaccessible	Le port n'est pas accessible
3	4	destinataire inaccessible	Fragmentation nécessaire mais impossible à cause du drapeau (flag) DF
3	5	destinataire inaccessible	Le routage a échoué
3	6	destinataire inaccessible	Réseau inconnu
3	7	destinataire inaccessible	Machine inconnue
3	8	destinataire inaccessible	Machine non connectée au réseau (inutilisé)
3	9	destinataire inaccessible	Communication avec le réseau interdite
3	10	destinataire inaccessible	Communication avec la machine interdite
3	11	destinataire inaccessible	Réseau inaccessible pour ce service
3	12	destinataire inaccessible	Machine inaccessible pour ce service
3	11	destinataire inaccessible	Communication interdite (filtrage)
4	0	Source Quench	Le volume de données envoyé est trop important, le routeur envoie ce message pour prévenir qu'il sature afin de demander de réduire la vitesse de transmission
5	0	Redirection pour un hôte	Le routeur remarque que la route d'un ordinateur n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur
5	1	Redirection pour un hôte et un service donné	Le routeur remarque que la route d'un ordinateur n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur
5	2	Redirection pour un réseau	Le routeur remarque que la route d'un réseau entier n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau
5	3	Redirection pour un réseau et un service donné	Le routeur remarque que la route d'un réseau entier n'est pas optimale pour un service donné et envoie l'adresse du routeur à rajouter dans la table de routage des ordinateurs du réseau
11	0	Temps dépassé	Ce message est envoyé lorsque le temps de vie d'un datagramme est dépassé. L'en-tête du datagramme est renvoyé pour que l'utilisateur sache quel datagramme a été détruit
11	1	Temps de ré-assemblage de fragment dépassé	Ce message est envoyé lorsque le temps de ré-assemblage des fragments d'un datagramme est dépassé.
12	0	en-tête erroné	Ce message est envoyé lorsqu'un champ d'un en-tête est erroné. La position de l'erreur est retournée
13	0	Timestamp request	Une machine demande à une autre son heure et sa date système (universelle)
14	0	Timestamp reply	La machine réceptrice donne son heure et sa date système afin que la machine émettrice puisse déterminer le temps de transfert des données
15	0	Demande d'adresse réseau	Ce message permet de demander au réseau une adresse IP
16	0	réponse d'adresse réseau	Ce message répond au message précédent
17	0	Demande de masque de sous-réseau	Ce message permet de demander au réseau un masque de sous-réseau
18	0	réponse de masque de sous-réseau	Ce message répond au message précédent
17	0	Timestamp reply	La machine réceptrice donne son heure et sa date système afin que la machine émettrice puisse déterminer le temps de transfert des données

DHCP (1/2)

DHCP signifie Dynamic Host Configuration Protocol.

C'est un protocole qui permet à un ordinateur qui se connecte sur un réseau d'**obtenir dynamiquement sa configuration**(principalement, sa configuration réseau).

=> l'ordinateur trouve tout seul une adresse IP par DHCP.

Le but principal étant la simplification de l'administration d'un réseau.

Il sert principalement à distribuer des adresses IP sur un réseau.

Au départ, il a été conçu comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé, par exemple, lorsque l'on installe une machine à travers un réseau.

Par ailleurs, BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur.

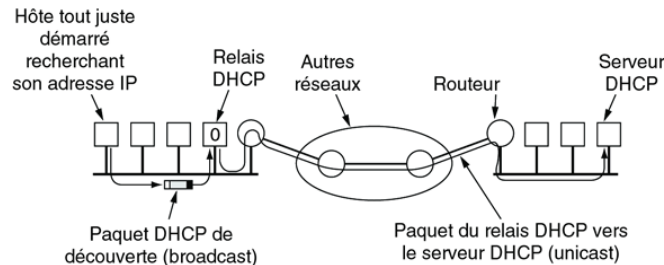
Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configuration propres à un hôte donné.

DHCP (2/2)

Fonctionnement du protocole DHCP

- un **serveur DHCP qui distribue des adresses IP**. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.
- Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP.
- => Pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (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 (n'oubliez pas que le **client** n'a pas forcément son adresse IP et que donc il n'est pas joignable directement) contenant toutes les informations requises pour le client.
- notion de **baux** ! (libération des ressources)

On a ici un fonctionnement client/serveur pour la distribution des IP dans un réseau.



NAT (Network Address Translation) (1/2)

Principe du NAT : mécanisme de translation d'adresses

Objectif : répondre à la pénurie d'adresses IP avec le protocole Ipv4.

Le principe du NAT consiste donc à utiliser une ou plusieurs adresses IP routables pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.

NAT statique :

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur permet donc d'associer à une adresse IP privée une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

Avantage : permet ainsi de connecter des machines du réseau interne à internet de manière transparente ;

Inconvénient : ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

NAT (Network Address Translation) (2/2)

NAT dynamique

Il permet de partager une adresse IP routable entre plusieurs machines en adressage privé. Ainsi toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

=> "mascarade IP" (en anglais IP masquerading) pour désigner le mécanisme de NAT.

Afin de pouvoir multiplexer les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise la **translation de port (PAT - Port Address Translation)**.

Cela consiste à affecter un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.