Support de cours

Initiation aux réseaux d'entreprise

Enseignant: Professeur Samuel OUYA

Objectifs :

- Appréhender l'environnement informatique
- Apprendre les notions de base de l'adressage IPv4
- Comprendre le rôle d'une passerelle et d'un serveur de noms
- Connaître l’architecture physique des systèmes informatiques
- Maîtriser les principes de base de l’administration d’un système d’exploitation réseaux et de gestion des utilisateurs

Compétences visées :

- Utiliser l'environnement informatique du réseau de l’école (connexion, comptes utilisateurs,
- lancement des machines virtuelles, brassage dans les salles de TP...)
- Connaître les principes de base de l'adressage IPv4 et savoir configurer les paramètres de
- base IPv4 d'une machine (adresse IPv4, masque, passerelle, DNS) comprendre le rôle d'un
- serveur DHCP dans un réseau local
- .1Installer un système d'exploitation
- Gérer les ressources d'un système informatique (partage, droits d’accès et sauvegarde...)
- Déployer des postes informatiques, gérer des utilisateurs (comptes, droits, profil...)

1. Introduction au réseau IP

1.1 Les réseaux : terminologie et vocabulaire

La notion de protocole

Un protocole est un ensemble de règles régissant les échanges entre 2–N parties (ou entités protocolaires)

Les protocoles réseaux sont basés sur l'échange de messages.

Pour que l'échange se déroule correctement, il faut que toutes les entités suivent le même protocole

Un protocole indique les actions à réaliser dans certains contextes.

Exemple de règle appliquée par un logiciel de messagerie :

- Contexte : je reçois un mail.
- Actions à réaliser :
  1. Si le mail m'est bien destiné, j'envoie un accusé de réception
  2. Sinon j'envoie un message erreur, destinataire incorrect

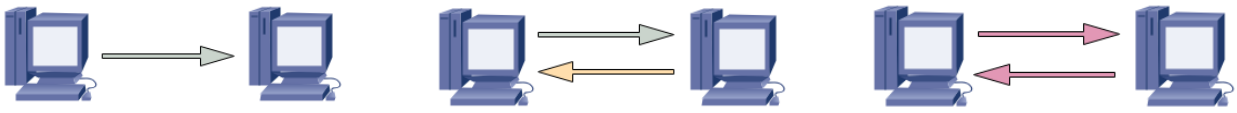
Liaisons simplex, half duplex et full duplex

Il existe 3 sens de transmission dans un réseau pour les liaisons point-à-point (entre 2 machines) :

Simplex : toujours de la gauche vers la droit

Half duplex : l'un après l'autre

Full duplex : les deux en même temps



En half-duplex, une machine ne sait pas forcément si l'autre est en train de transmettre des données.

Elle peut commencer sa transmission alors que des données lui arrivent.

Les deux messages vont se rencontrer sur le câble : on parle de **collision**

Les deux machines devront alors retenter leurs transmissions plus tard.

La notion d'adresse

Pour les besoins de la communication, il est nécessaire de pouvoir désigner les machines sur le réseau.

On utilise pour cela les adresses. L'adresse identifie une machine sur le réseau.

Pour que l'échange se fasse correctement il faut que ces adresses soient uniques : **deux machines ne peuvent pas partager la même adresse.**

Nous allons voir l'adressage IP utilisé sur Internet mais il y en a d'autres.

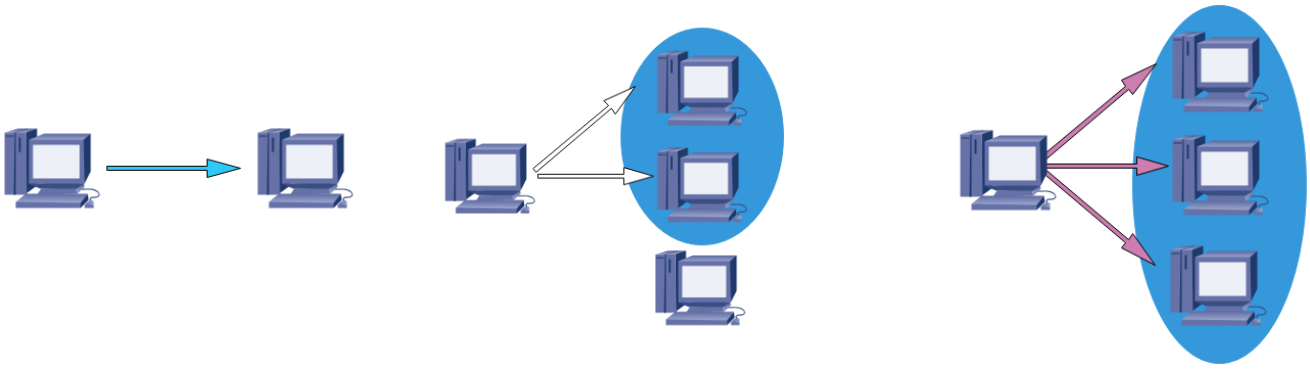
Destinataires d'un message

Il existe globalement 3 modes de transmission à savoir : **unicast, multicast, broadcast** (ou diffusion) permettent de caractériser l'envoi d'un message par rapport au nombre de destinataires sur le réseau.

Unicast
1 vers 1

multicast
1 vers plusieurs

broadcast
1 vers tous



Dans le cas du multicast et du broadcast, une même adresse désigne plusieurs machines.

Interfaces réseau

Une **interface réseau** est le **moyen** utilisé par l'ordinateur pour envoyer/recevoir des données sur le réseau.

Les machines sont dotées généralement de 2 cartes réseaux :

- une carte Ethernet pour le réseau filaire (connexion par câble)
- une carte Wifi pour le réseau sans fil

La figure ci-dessous montre une carte Ethernet :

Sous Linux les interfaces réseau sont désignées par un nom de la forme typeN avec :

- type = type de réseau(eth=Ethernet, wlan=Wi-Fi,...)
- N = numéro de la carte de ce type (la numérotation démarre à 0)

Utiliser la commande **ifconfig** pour afficher le nom de votre carte réseau comme le montre la figure ci-dessous :

```
aly@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:20:3a
          inet addr:192.168.1.33  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe23:203a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:327 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41549 (41.5 KB)  TX bytes:12952 (12.9 KB)
```

Depuis l'arrivée de Ubuntu 16, le daemon **udevd** a changé la façon dont il attribue des noms aux périphériques Ethernet.

en = ethernet **p2** = le numéro de bus **s3** = le numéro d'emplacement comme le montre la figure ci-après avec la commande **ifconfig** :

```
ec2lt@xensesver:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:63:9c:ca
          inet adr:192.168.1.140  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::97fc:db0:facd:e7dd/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:24477 erreurs:0 :0 overruns:0 frame:0
          TX packets:16699 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:36330811 (36.3 MB) Octets transmis:1270990 (1.2 MB)
```

1.2 Le réseau Internet et le protocole IP

Les acteurs de l'Internet

Il existe différentes organisations/sociétés internationales qui sont liées au développement et à la gestion de l'Internet :

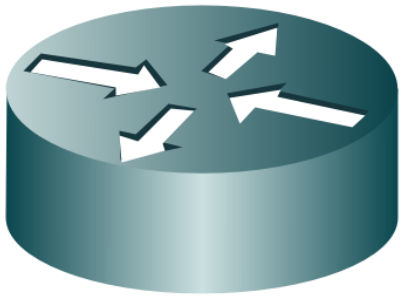
- **ISOC** (InternetSOCiety) permet de promouvoir le développement de l'Internet
- **IETF** (Internet Engineering Task Force) permet de définir et d'expérimenter les protocoles de l'Internet
- **IANA** (Internet Assigned Number Authority) permet de gérer les numéros utilisés sur Internet (les adresses IP, par exemple)
- **ICANN** gére le système des noms de domaine, coordonne l'affectation et l'attribution des identificateurs uniques d'Internet, comme les adresses IP

Le réseau Internet

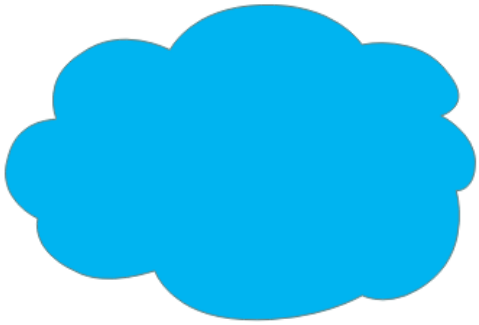
L’Internet est une interconnexion de millions de réseaux aux caractéristiques différentes (Wifi, Ethernet, satelitte, . . .) interconnectés par des routeurs qui se chargent de faire circuler l’information entre les réseaux.

Un Routeur est n’importe quel équipement qui a plusieurs interfaces réseau et qui est à la frontière entre plusieurs réseaux comme le montre la figure ci-dessous :

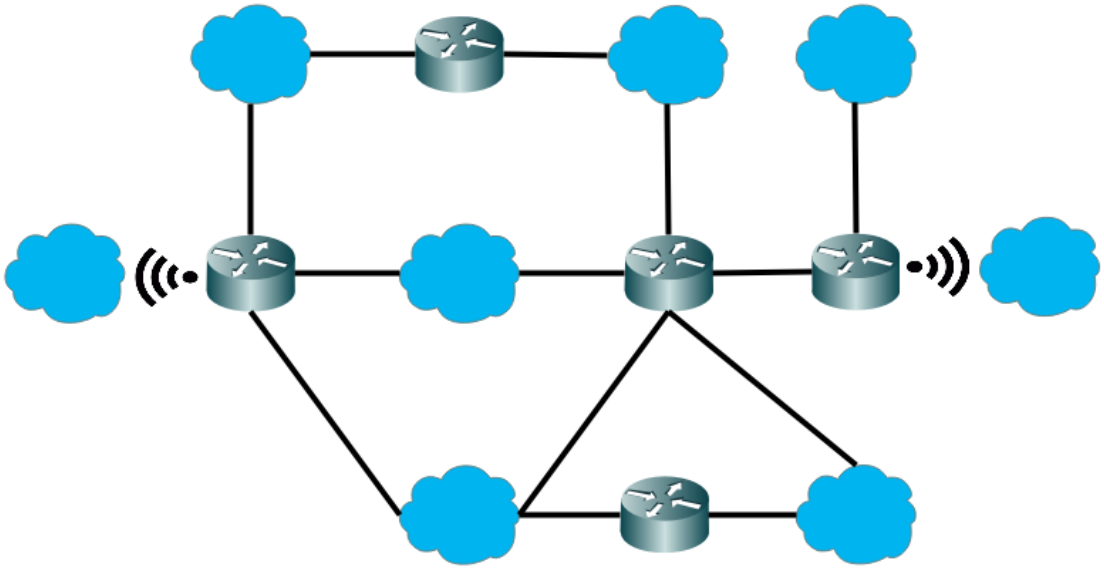
Un routeur est représenté par les logiciels d’émulation tels que GNS3, EVE-NG, etc sous la forme suivante comme le montre la figure ci-dessous :



Un réseau est un ensemble de machines qui peuvent communiquer entre elles sans intermédiaire. Un réseau est représenté sous la forme d’un nuage comme le montre la figure ci-dessous :



Exemple : des machines sur un même réseau Wifi ou Ethernet comme le montre la figure ci-dessous :



Plusieurs types d'équipement peuvent jouer le rôle de routeur :

- des équipements dédiés. Exemple : un routeur CISCO

- un ordinateur de bureau ou portable
- une box Internet
- un téléphone portable

Le protocole IP

Pour s'échanger des données, les machines connectées à Internet utilise le protocole IP : Internet Protocol.

Le protocole IP définit principalement :

- le mode d'adressage des machines sur le réseau Internet : l'adresse IP ;
- la structure des messages échangés ;
- et la façon d'acheminer des messages d'une machine A à une machine B du réseau Internet : le routage.

Remarque : il existe plusieurs versions du protocole qui sont IPv4 et IPv6.

Les paquets IP

Les messages échangés dans le cadre du protocole IP s'appellent des **paquets.**

La structure de ces paquets est normalisée, tout paquet IP a une forme bien précise et est constitué :

- **d'un en-tête** : principalement, les informations nécessaires au routage du paquet (emballage du paquet avec l'adresse)
- **et d'un corps** : les informations envoyées par la machine émettrice (contenu du paquet).

L'en-tête contient, entre autres :

- l'adresse IP de la machine destinataire (nécessaire pour que le paquet arrive à destination).
- l'adresse IP de la machine émettrice (nécessaire en cas de réponse du destinataire).

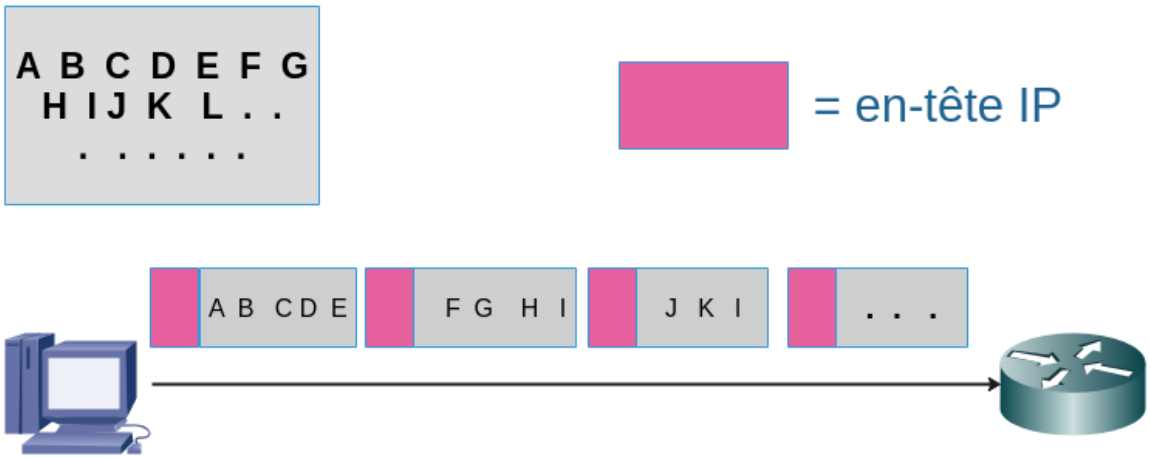
Le découpage en paquets

- Pour des raisons techniques **la taille des paquets est limitée.**

  Exemple: taille maximale d'un paquet est sensiblement égal à 2300 octets sur un réseau WiFi.

  - Si la taille des données à envoyer **est supérieure** taille maximale, on doit découper les données en plusieurs paquets. C'est ce qu'on appelle la **fragmentation.**
- L'en-tête IP se retrouve dans chaque paquet car chaque paquet doit arriver à destination.

Exemple : on désire envoyer une suite d'octets abcdef…



N.B : En réalité, on peut avoir d'autres en-têtes (d'autres protocoles) dans chaque paquet.

1.3 L'adressage IP

Structure d’une adresse IP

Une adresse IP est composée de **32 bits**

On a donc 2^{32} = 4 294 967 296 d’adresses IP disponibles à peu près car certaines adresses sont nécessaires au fonctionnement du protocole et ne peuvent pas être attribuées à des machines. On dit qu’elles sont **réservées.**

En réalité on a donc un peu moins de 2^{32} adresses IP disponibles.

On la note sous la forme de 4 octets (en notation décimale) séparés par des points. On parle de **notation décimale pointée**

Rappel : 1 octet = 8 bits

On retrouve bien **4 x 8 = 32 bits.**

Les nombres qui composent une adresse IP sont dans l’intervalle [0, 255].

Exemple d’adresse IP :

192.168.1.20

dont la représentation binaire est :

11000000.10101000.00000001. 00010100

Anatomie d’une adresse IP

Toute adresse IP se décompose en deux parties :

- un identifiant de réseau (ou **net-id**)qui identifie le réseau sur lequel se trouve la machine ;
- suivi d’un identifiant de machine (ou **host-id**) qui identifie la machine (ou l’hôte) au sein du réseau

La partie **net-id** est déterminée par les bits de poids fort de l’adresse IP.

La partie **host-id** est déterminée par les bits de poids faible de l’adresse IP

Le nombre de bits utilisés pour représenter le net-id est variable et dépend du réseau sur lequel on se trouve. On a alors besoin d’une autre information pour pouvoir différencier les bits du net-id de ceux du host-id appelée **le masque**

Le masque

Le masque indique le nombre de bits dans l’adresse IP qui forment le **net-id.** Il est associé à un réseau et donc à toutes les machines de ce réseau.

On le note comme une adresse IP :

- dont tous les bits de poids fort correspondant au **net-id** valent 1 ;

- et tous les bits de poids faible correspondant au **host-id** valent 0

Un masque est donc une série de bits à **1** suivie de bits à **0**.

Le nombre de bits à **1** permet de déterminer le nombre de bits dans l'adresse IP qui représentent le **net-id.**

Exemple : soit l'adresse 192.168.1.20 de masque 255.255.255.0

En binaire le masque s'écrit 11111111 11111111 11111111 00000000.

Conséquences

- Les 24 premiers bits `a 1 dans le masque indiquent que les 24 premiers bits (ou 3 premiers octets) de l'adresse IP forment son **net-id.**
- L'octet restant est le **host-id** de la machine.

  On a donc :

Notation du masque

Pour la notation du masque complet (avec la notation décimale pointée), on préfère généralement utiliser la notation **"/".**

On note l'adresse IP de la machine suivie de "/N" où N est le nombre de bits à 1 dans le masque de réseau et on appelle **N** la **longueur du masque.**

Exemple :

soit l'adresse 192.168.1.20/24

Dans le masque, il y a **24 bits à 1** suivis de 32 - 24 = **8 bits à 0**.

On a donc :

192.168.1.20/24 ⇔ 192.168.1.20 avec le masque 255.255.255.0

L'adresse de réseau

Une adresse de réseau désigne un réseau sur Internet.

Les adresses de réseau sont nécessaires au fonctionnement du routage.

C'est une adresse réservée : elle ne peut pas être attribuée à une machine du réseau.

A partir d'une adresse IP et de son masque, on obtient l'adresse de son réseau en mettant les bits du host-id à 0.

L’adresse de réseau

Une adresse de réseau désigne un réseau sur Internet.

Les adresses de réseau sont nécessaires au fonctionnement du routage.

Une adresse réseau est une adresse réservée : elle ne peut pas être attribuée à une machine du réseau.

A partir d’une adresse IP et de son masque, on obtient l’adresse de son réseau en mettant les bits du host-id à **0.**

Exemple : soit l’adresse 192.168.1.20/24.

On a vu que l’adresse se décompose ainsi

L’adresse de son réseau est donc : 192.168.1**.0**

Remarque : deux machines sur un même réseau doivent forcément avoir la même adresse de réseau.

L’adresse de diffusion de réseau

L’adresse de diffusion d’un réseau désigne toutes ses machines.

Une adresse de diffusion est **une adresse réservée.**

Un paquet envoyé à cette adresse est reçu par toutes les machines du réseau.

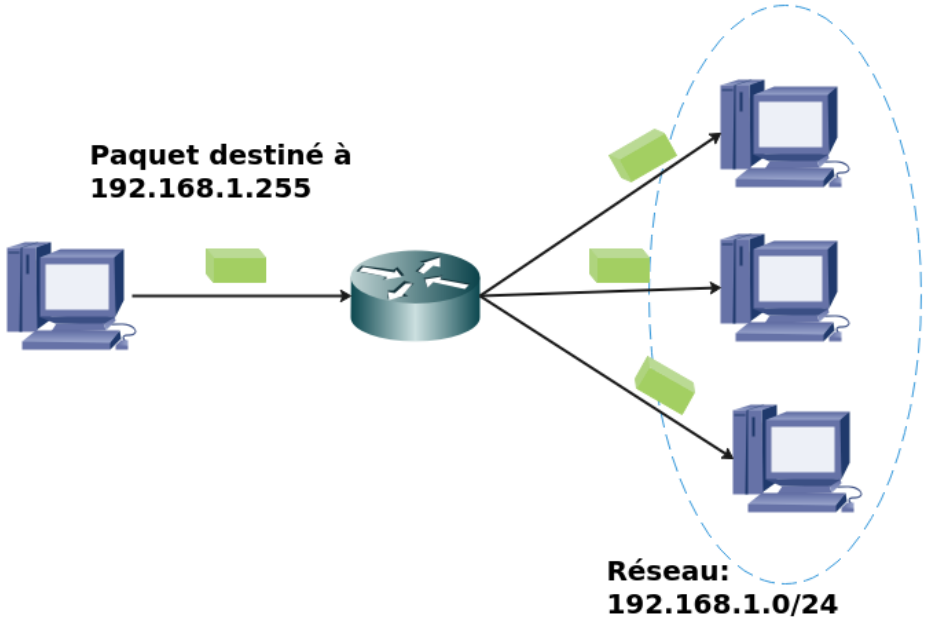
A partir d’une adresse IP et de son masque, on obtient l’adresse de diffusion de son réseau en mettant les bits du **host-id à 1.**

Exemple :

soit l’adresse 192.168.1/24

on a vu que l’adresse se décompose ainsi :

L’adresse de diffusion de son réseau est donc : 192.168.1.**255**.



L'adresse de diffusion locale

Dans certaines situations, une machine a besoin d'envoyer un paquet sur son réseau alors qu'elle n'a pas encore d'adresse IP par exemple au démarrage.

Elle utilise alors l'adresse de diffusion locale pour envoyer un paquet à toutes les machines de son réseau.

L'adresse de diffusion locale est une adresse réservée et elle vaut **255.255.255.255**

Les paquets envoyés à cette adresse ne sont pas relayés par les routeurs :

ils restent sur le réseau

L'adresse de diffusion locale utilisée dans le protocole DHCP lorsqu'une machine n'a pas encore d'adresse IP.

Utilisation du masque

L'opération effectuée pour connaître l'adresse de réseau à partir d'une adresse IP et d'un masque est le **ET logique**.

Cette opération consiste à mettre à 0 les bits du **host-id** et de ne conserver que les bits du **net-id** autrement dit de masquer les bits du host-id pour ne garder que ceux du **net-id**.

Exemple :

Soit l'adresse 192.168.1.0/24.

Son adresse de réseau peut être calculée ainsi :

```
      192 . 168 . 1 . 20
ET
      255 . 255 . 255 . 0
-------------------------------------
      192 . 168 . 1 . 0     =  l'adresse réseau
```

ou en binaire :

```
      11000000 . 10101000 . 00000001 . 00010100
ET    11111111 . 11111111 . 11111111 . 00000000
-------------------------------------------------------------
      11000000 . 10101000 . 00000001 . 00000000   =  l'adresse réseau
```

Attribution d'adresses IP

Les règles à respecter lors de l'attribution une adresse IP :

- net-id cohérent avec l'adresse de réseau
- ne pas choisir l'adresse de réseau (réservée)
- ne pas choisir l'adresse de diffusion (réservée)

Conséquences :

- La première adresse disponible est (adresse de réseau + 1).
- La dernière adresse disponible est (adresse de diffusion - 1).

Pour un réseau en **/N,** le nombre d'adresses IP disponibles est $2^{(32-N)}-2$

- 32 – N correspond au nombre de bits dans la partie **host-id**
- $2^{(32-N)}$ correspond nombre de host-ids que l'on peut former avec 32 -N bits.
- Et on retranche les 2 adresses réservées du réseau (l'adresse réseau et l'adresse de diffusion)

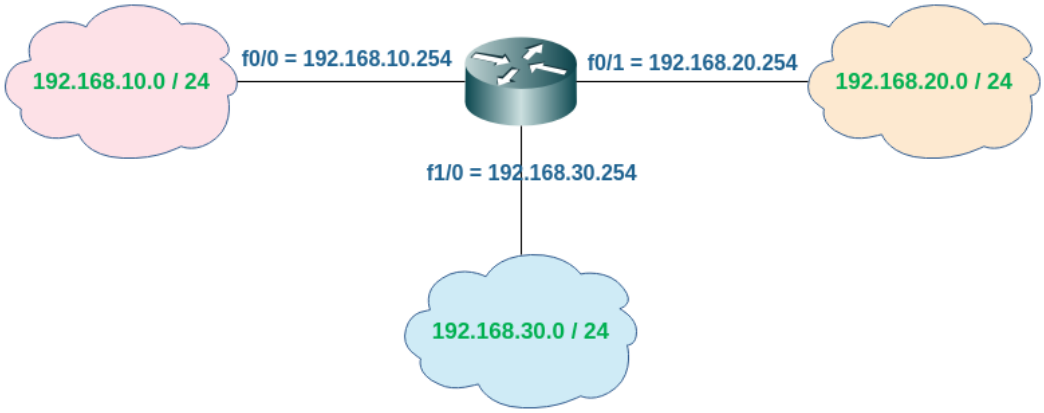
Exemples :

Réseau	**1ère adresse disponible**	**Dernière adresse disponible**	**Nombre d'adresses disponibles**
192.168.1.0/24 172.16.0.0/16	192.168.1.1 172.16.0.1	192.168.1.254 172.16.0.254	$2^{(32-24)}-2=254$ $2^{(32-16)}-2=65534$

Qui possède une adresse IP ?

- Toute machine connectée à Internet doit posséder une adresse IP mais elle peut en avoir plusieurs. C'est le cas, par exemple, des routeurs.
- Un routeur étant connecté à plusieurs réseaux, il est nécessaire qu'il ait une adresse IP par réseau auquel il est connecté on a donc une adresse IP par interface utilisée par le routeur.

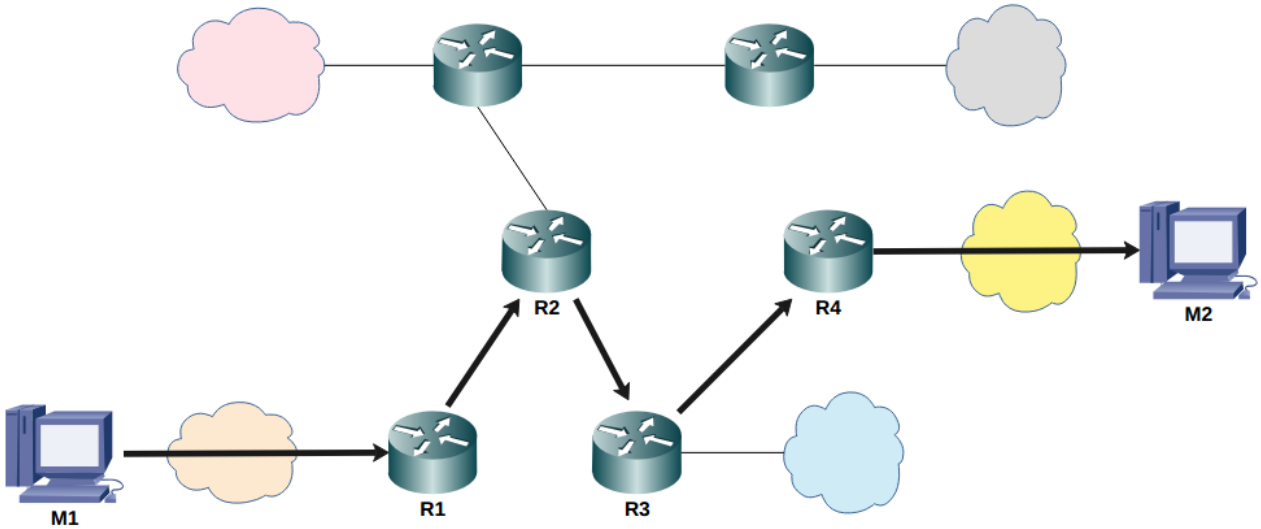
Exemple : un routeur R relié à 3 réseaux par 3 interfaces Ethernet.



1.4 Introduction au routage sur Internet

Définition du routage

Le routage est un processus de sélection d'une route dans l'acheminement d'un paquet à son destinataire final comme le montre la figure ci-dessous :

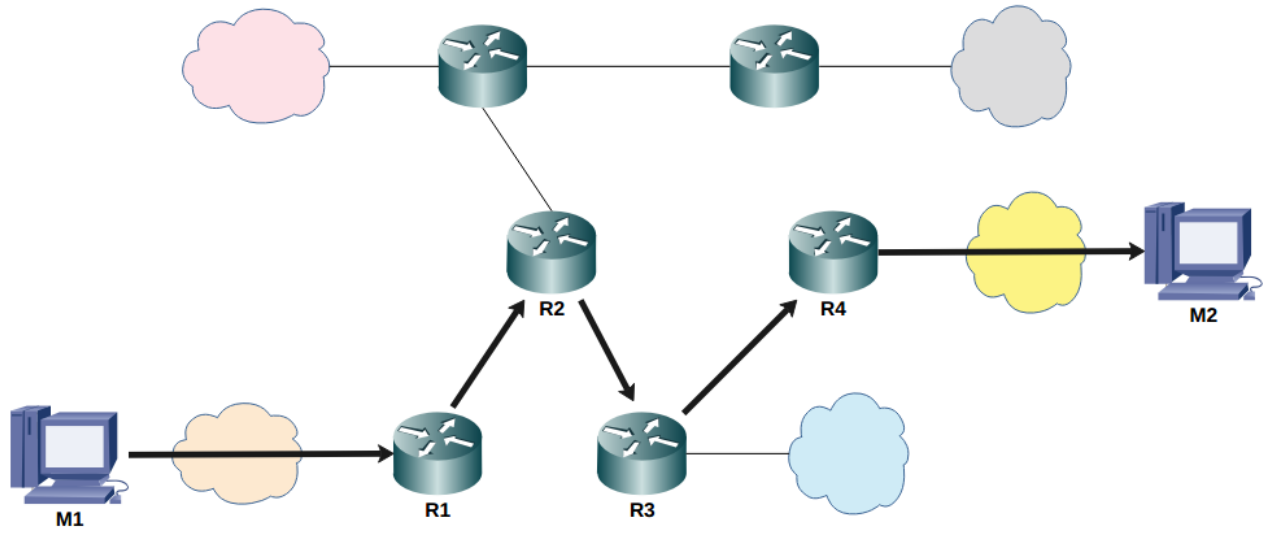


Sur Internet le routage est effectué par tous les routeurs sur le chemin emprunté.

Les routeurs n'ont pas de carte globale d'Internet. Ils ont connaissance des autres routeurs auxquels ils sont directement connectés et les réseaux se trouvant derrière ces routeurs.

Pour déterminer la route `a emprunter pour joindre le destinataire, le routeur consulte **une table de routage.**

Exemple d'acheminement d'un paquet



Situation :

M1 veut envoyé un paquet à destination de M2

Le paquet va suivre la route suivante **M1 ⇒ R1 ⇒ R2 ⇒ R3 ⇒ R4 ⇒ M2**

Comment ?

- Chaque routeur, à la réception du paquet, de même que M1 au tout début, va consulter sa table de routage.
- La table de routage va lui permettre de répondre à la question **à qui envoyer un paquet destiné à M2** ?
- Dans chaque cas, la table indiquera le routeur suivant sur le chemin.
  - pour M1 ⇒ R1, pour R1 ⇒ R2, . . .

Mais un routeur ne connaît pas le chemin complet suivi par un paquet par exemple, R1 ne sait pas ce que R2 fera du paquet.

La table de routage

La table de routage est consultée par une machine A dès qu'elle doit acheminer un paquet à une machine B et donc déterminer à qui envoyer ce paquet.

Deux situations sont possibles de consultation :

- si le paquet est routé par A (cas pour R1, R2, R3 et R4 dans la diapo précédente)
- si le paquet est directement envoyé par A (cas pour M1 dans la diapo précédente)

Toute machine (qu'elle soit routeur ou non) a une table de routage.

En consultant sa table de routage, une machine A peut obtenir 3 types de réponse :

- **remise directe**
- **remise indirecte**
- **hôte inaccessible**

Types de réponse

- La machine A est la machine devant transmettre le paquet et qui consulte sa table de routage
- La machine B est la machine destinataire du paquet

Remise directe , A et B sont sur un même réseau

Les machines A et B se trouvent dans un même réseau donc la machine A n'a pas besoin de passer par un routeur pour envoyer le paquet à la machine B.

L'opération de consultation de la table de routage indique l'interface à utiliser pour envoyer le paquet à la machine B. Ce processus de routage est appelé **routage direct.**

Remise indirecte , A et B sont sur des réseaux différents

Les machines A et B sont situées sur des réseaux différents, il faut au moins un routeur (passerelle) entre A et B.

L'opération de consultation de la table de routage indique l'adresse IP du routeur R sur le chemin qui mène à la machine B et l'interface à utiliser pour envoyer le paquet à R.

Hôte inaccessible, la table n'indique pas comment router le paquet

Toute machine qui n'as pas l'information qui lui permette de router un paquet après avoir consulté sa table de routage **ignore simplement le paquet.**

Les lignes de la table de routage

Une table de routage est un ensemble ligne composé d'un **quadruplet** (D, M, R, I) avec :

- **Destination**
- **Routeur**
- **Masque**
- **Interface**

Une ligne dans la table de routage indique comment envoyer un paquet à une machine du réseau de destination **D** dont le masque est **M.**

Il existe 2 possibilités pour R et I :

- **remise directe :**
  - **R** = vide
  - **I** = interface connectée au réseau D
- **remise indirecte :**
  - **R** = adresse du routeur sur la route vers le réseau D
  - **I** = interface connectée au réseau sur lequel se trouve R

La route par défaut

La route par défaut est une ligne de la table de routage utilisée lors de la consultation quand aucune des autres lignes ne permet de déterminer la route vers le destinataire.

- Les autres lignes indiquent comment joindre certains réseaux.
- La route par défaut indique comment joindre tous les autres réseaux (c'est-à-dire le reste du réseau Internet).

Remarques :

- Pour la route par défaut, on a toujours D = M = 0.0.0.0.
- Il ne peut pas y avoir plusieurs routes par défaut dans une table de routage.

Exemple de table de routage d'une machine sous linux

Pour afficher la table de routage d'une machine sous Linux on exécute la commande **route -n** ou **netstat -rn** comme le montre la figure ci-dessous :

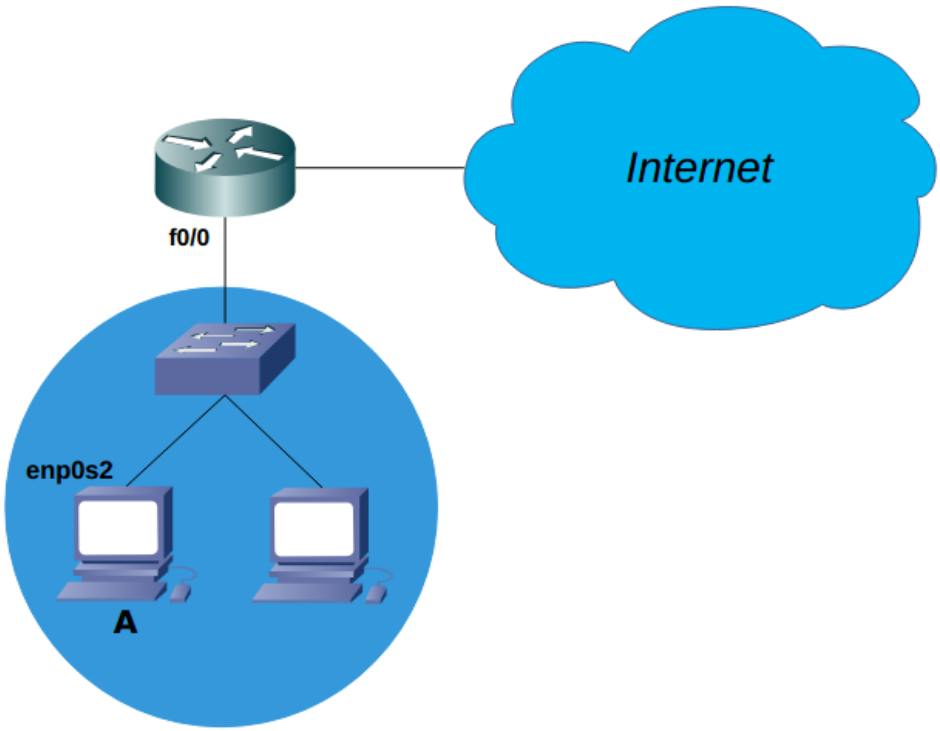
```
root@tireraPC:~# route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 enp2s0
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
172.16.126.0    0.0.0.0         255.255.255.0   U     0      0        0 vmnet8
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 enp2s0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp1s0
192.168.67.0    0.0.0.0         255.255.255.0   U     0      0        0 vmnet1
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
root@tireraPC:~#
```

Sous Windows pour afficher la table de routage de votre machine exécuter la commande suivante netstat -rn.

Cette table peut se lire ainsi :

- ligne 1 et 2 (route par défaut) : pour envoyer un paquet à une machine de n'importe quel autre réseau : **remise indirecte** au routeur **192.168.1.1** (adresse IP de la passerelle) en utilisant l'interface de la carte Ethernet **enp2s0** ou l'interface de la carte wifi **wlp1s0** .
- ligne 5 : pour envoyer un paquet à une machine du réseau **172.17.0.0/24** : **remise directe sur l'interface docker0.**
- ligne 6 : pour envoyer un paquet à une machine du réseau **192.168.1.0/24** : **remise directe sur l'interface enp2s0.**

La topologie du réseau est donc la suivante comme le montre la figure ci-dessous :



Décision de routage

Soit la situation suivante :

- A la machine devant transmettre un paquet
- B la machine destinataire du paquet

La machine A va chercher dans sa table de routage la ligne (D, M, R, I) qui indique comment joindre la machine B.

Cette ligne est telle que ***B ET M = D*** *autrement dit : on teste si B est sur le réseau D.*

Si une telle ligne existe alors la réponse est :

- remise directe si R est vide
- remise indirecte si R n'est pas vide

Si aucune ligne ne vérifie cette condition, alors la réponse est :

- **hôte inaccessible** indique qu'aucune ligne n'indique comment envoyer un paquet à B

Routage en présence d'une route par défaut

On a vu que la route par défaut est telle que D = M = 0.0.0.0.

La route par défaut vérifie toujours la condition B ET M = D. (puisque, quel que soit B, on a toujours, B ET 0.0.0.0 = 0.0.0.0).

- **Conséquence** est que : si une route par défaut est présente dans la table de routage, alors la réponse **ne sera jamais hôte inaccessible.**
- Mais la route par défaut est toujours la dernière ligne lue dans la table : On cherche d'abord une ligne contenant le réseau de B puis, seulement si on ne trouve pas cette ligne, alors on suit la route par défaut.

Routage statique et routage dynamique

Comment les tables de routage des routeurs sont-elles remplies ?

Pour le remplissage des tables de routages il existe 2 possibilités :

- **routage statique** correspond au remplissage manuel par un administrateur du réseau.
- **routage dynamique** correspond au remplissage automatique par le routeur lui-même par l'échange entre routeurs **d'informations de routage** afin de découvrir de nouvelles routes grâce aux protocoles de routage tels que **RIP, OSPF.**

Équipements d'interconnexion Ethernet

Les équipements d'interconnexion Ethernet permettent d'interconnecter des machines.

Ils ont des ports en entrée qui permettent de brancher des machines avec un câble Ethernet.

Les **hubs** et les **switchs** sont des exemples d'équipements d'interconnexion.

La Différence entre un hub et un switch est quand il reçoit des données sur un port :

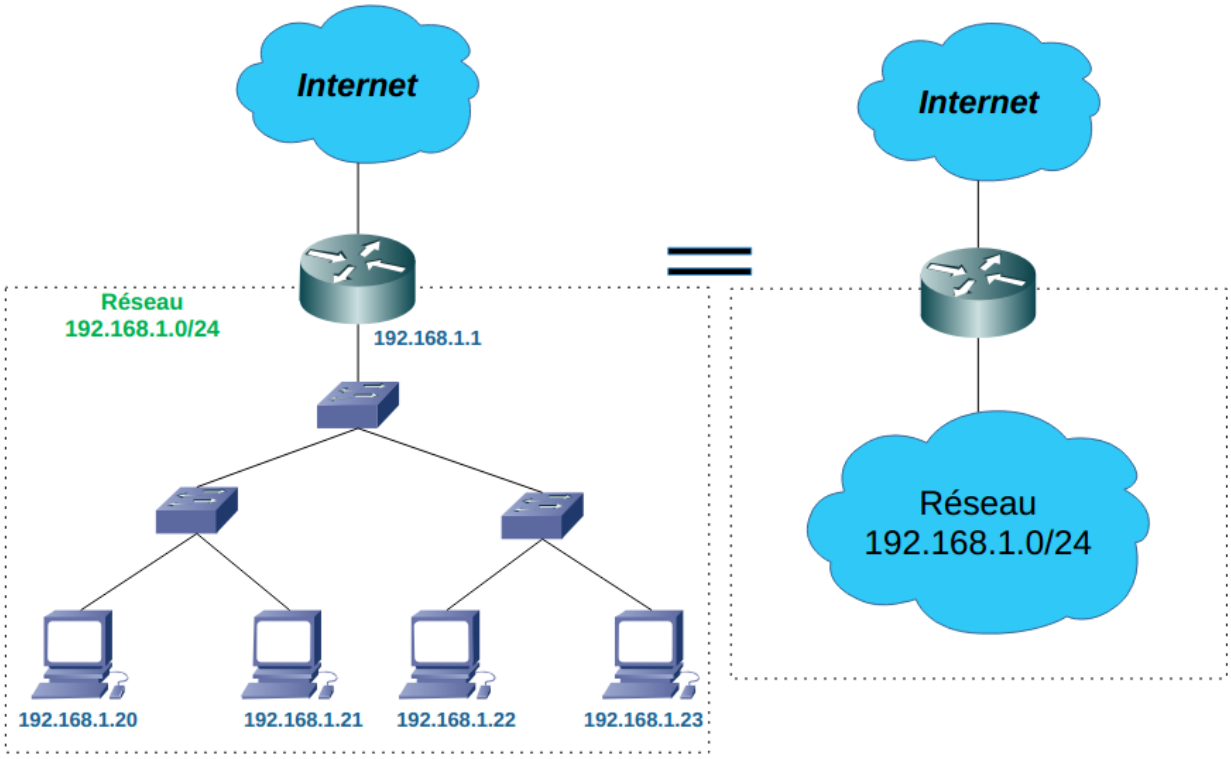
- le hub les retransmet sur tous les autres ports
- alors que le switch les retransmet uniquement sur le port qui permet de joindre la machine destinataire.

La différence entre un **switch/hub** et un **routeur** est que :

- Le switch interconnecte des machines d'un **même réseau**.
- Le routeur interconnecte des machines de **réseaux différents**.
- Le switch n'a pas d'adresse IP (il n'intervient pas dans le protocole IP).

Exemple de réseau utilisant des switchs

Un réseau 192.168.1.0/24 composé de switchs qui correspond à l'architecture classique dans les structures de taille moyenne en cascade comme le montre la figure ci-dessous :



Câbles RJ45

En Ethernet, les câbles les plus utilisés sont des câbles RJ45 (Registered Jack 45) ou prise enregistrée n°45.

Dans un câble RJ45 il existe 8 fils électriques soit 4 paires torsadées.

Chaque paire torsadée est identifiée par leur couleur.

Les câbles RJ45 ont d'autres applications que les réseaux informatiques par exemple la téléphonie aux USA.

En ethernet, 4 fils seulement sont utilisés :

- 2 fils pour la réception de signaux (R^+et R^-)
- 2 fils pour la transmission de signaux (T^+ et T^-)

Pourquoi utiliser 2 fils pour la réception (ou pour l'émission) ?

- bits correspond aux signaux électriques mesurés par des tensions
- la tension correspond différence de potentiels entre 2 points, donc 2 fils
- signal de réception correspond différence de potentiel entre R^+ et R^-
- signal de transmission correspond différence de potentiel entre T^+ et T^-

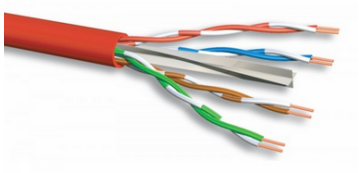
Types d'équipements pour le câblage

Lors d'un câblage avec du RJ45 on distingue 2 types d'équipements :

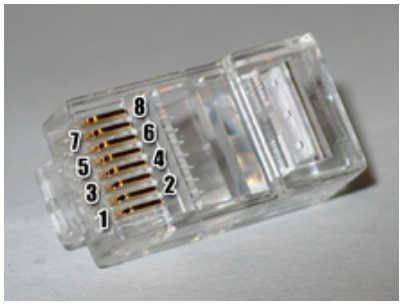
- DCE = Data Communication Equipment = équipements d'interconnexion dans un réseau (hubs et switchs)
- DTE = Data Terminal Equipment = équipements terminaux d'un réseau (routeurs et ordinateurs)

Broche	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
DCE	**R $^{+}$**	**R $^{-}$**	**T $^{+}$**	**-**	**-**	**T $^{-}$**	**-**	**-**
DTE	**T $^{+}$**	**T $^{-}$**	**R $^{+}$**	**-**	**-**	**R $^{-}$**	**-**	**-**

Un câble RJ45 dénudé :



Connecteur RJ45 avec les 8 broches :



Câbles droits et câbles croisés

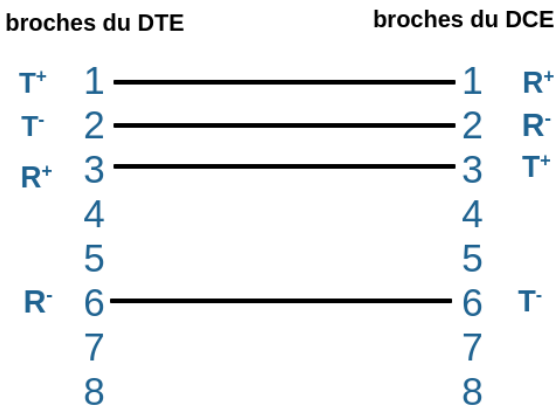
Comment câbler deux équipements ?

Pour que la transmission fonctionne, il faut que les broches affectées à la transmission d'un côté soit reliées aux broches affectées à la réception de l'autre côté.

- T $^{+}$ de l'un relié au R $^{+}$ de l'autre
- T $^{-}$ de l'un relié au R $^{-}$ de l'autre
- et inversement

Pour relier un DTE à un DCE, on utilise donc **un câble droit** (qui relie chaque broche d'un côté à la broche de même numéro de l'autre côté).

On obtient alors le schéma suivant :



Par contre, pour relier deux DTEs ou deux DCEs, le câble droit n'est pas adapté.

On obtiendrait alors le T^+ de l'un relié au T^+ de l'autre, le T^- de l'un relié au T^- de l'autre et ainsi de suite.

On utilise alors un câble croisé qui relie :

- la broche 1 de l'un à la broche 3 de l'autre
- la broche 2 de l'un à la broche 6 de l'autre
- et inversement

2. Services réseau

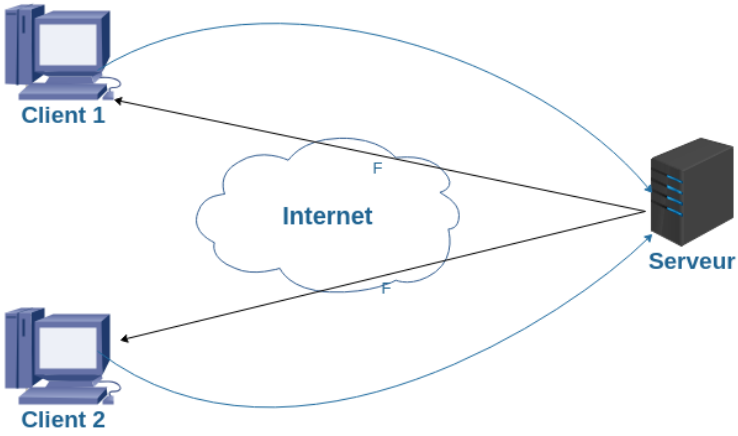
Le modèle client-serveur

Le modèle client-serveur est l'ensemble des protocoles qui font intervenir des processus qui proposent des services (les serveurs) à des processus qui peuvent en bénéficier (les clients) et qui s'exécutent sur différentes machines d'un réseau.

Rappel :

- un processus est un programme en cours d'exécution

Les échanges sont sous forme de questions (ou requêtes) du client suivies de réponses du serveur comme le montre la figure ci-dessous :



Il est à noter que :

- Le terme "**client**" désignera à la fois le processus client et la machine sur laquelle ce processus s'exécute. idem pour le serveur
- C'est toujours le client qui est à l'initiative de l'échange : un serveur n'enverra jamais de messages à un client si celui-ci ne l'a pas sollicité.

Service réseau

Un service réseau est un processus qui attend du réseau des demandes ou requêtes en provenance de processus clients et traite ces requêtes puis, généralement, envoie au client une réponse.

Quand le service n'a rien à faire (il ne reçoit aucune requête du réseau) on dit qu'il est en **sommeil.**
Le service est réveillé par le système d'exploitation à la réception d'une requête.
Les services doivent être lancés par l'utilisateur root.
Le client et le serveur utilisent le même protocole de service pour communiquer.
Exemples de protocoles de service :

- **HTTP, FTP** : transfert de fichiers
- **SMTP** : envoi de mails
- **POP, IMAP** : réception de mails

Dans le répertoire /etc/rc.d/init.d on trouve des scripts permettant de lancer des services. Ce sont les daemons. Dans chaque script il y a une petite description de ce que le daemon (ou service) est sensé faire. On peut activer ou désactiver ou redémarrer ou voir l'état d'un service de la façon suivante :

Actions courantes :

- **start** = démarrer le service

- **stop** = arrêter le service
- **status** = voir l'état du service (arrêté/démarré, temps d'exécution, . . .)
- **restart** = redémarrer le service

Interaction avec le protocole IP

Dans le cours 2 on a vu que sur Internet l'information circule dans des **paquets IP** ou **datagramme IP.**

Un paquet IP correspond au regroupement d'**un en-tête IP** (adresses IP source et dest., . . .) + un corps (l'information transportée).

Dans le cas des protocoles de service, le corps du paquet du message correspond aux données du protocole de service.

Remarque: on dit que les données du protocole de service sont **encapsulées dans le paquet IP.**

2.2 Le service DNS — Résolution de noms

Pour pouvoir communiquer sur Internet une machine a besoin de :

- une adresse IP + le masque de son réseau
- connaître l'adresse IP du routeur qui le relie au monde extérieur sinon elle peut uniquement
- communiquer avec les machines de son réseau.
- connaître l'adresse IP d'un serveur DNS sinon la machine ne pourra pas faire de la résolution de noms.

Ces éléments TCP/IP forment **une configuration IP.**

Il existe 2 mode de configuration IP des machines :

- **statique** ce cas c'est l'administrateur du réseau qui choisit une adresse IP et l'écrit dans le fichier de configuration de l'interface réseau, il renseigne les tables de routage des machines (commande route) et enfin il indique l'adresse IP d'un serveur DNS dans le fichier /etc/resolv.conf sous Linux.
- **dynamique** c'est la machine qui obtient elle-même cette configuration en interrogeant un serveur DHCP (Dynamic Host Configuration Protocol).

Avantages de la solution dynamique :

La configuration dynamique a pour avantage :

- d’éviter des erreurs par exemple de donner la même adresse IP à 2 machines différentes.
- de faciliter aussi la maintenance (un seul fichier de configuration DHCP à modifier).

Client et serveur DHCP

Le service DHCP fonctionne en mode client serveur :

- le **client DHCP** est une machine qui veut obtenir une configuration IP
- le **serveur DHCP** est la machine qui va lui fournir cette configuration

Les deux machines (le **client DHCP, le serveur DHCP)** doivent se trouver sur le même réseau.

Le client DHCP et le serveur échangent des informations lorsque le client veut se connecter à un nouveau réseau ou au démarrage du client.

Le serveur possède une base de données d’adresses IP qu’il peut attribuer aux clients et toutes les informations sur le réseau nécessaires pour pouvoir communiquer sur Internet.

Ces informations sont stockées sur le serveur dans un fichier de configuration DHCP (/etc/dhcp/dhcpd.conf généralement)

Fonctionnement du protocole DHCP

Initialement, le client ne connaît pas l’adresse IP de son serveur DHCP.

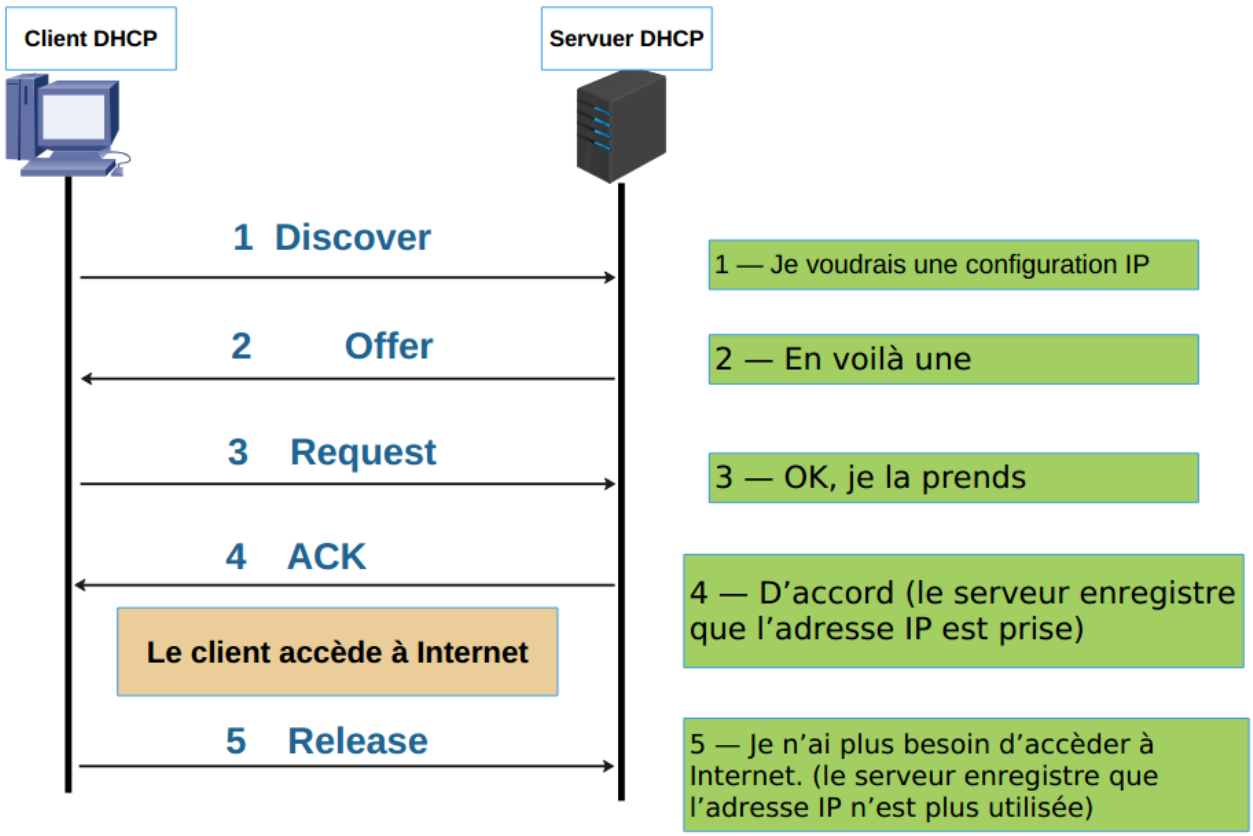
1. Il envoie un message de diffusion appelé **Discover** à toutes les machines du réseau (en utilisant l’adresse de diffusion locale 255.255.255.255).
   Ce message est ignoré par toute machine qui n’est pas serveur DHCP.
   Ce message Discover a pour but de demander une configuration IP à un serveur DHCP
2. Après réception d’un message Discover, le serveur détermine la configuration du client et lui attribue une adresse IP.
   Il envoie ces informations dans un message **Offer.**
3. Le client qui reçoit une configuration peut l’accepter ou la refuser.
   Exemple de refus : le client a déjà accepté une autre configuration (dans le cas où il y a plusieurs serveurs DHCP sur le réseau).
4. Dans tous les cas, il envoie un message **Request** à 255.255.255.255 pour que tous les serveurs DHCP connaissent sa décision.
5. Le serveur dont la proposition a été acceptée envoie un message **Ack** pour confirmer au client qu’il peut utiliser la configuration proposée. (Ack = Acknowledgment, acquittement)

La libération

Dès que le client n’a plus besoin d’accéder à Internet, il envoie au serveur un message **Release.**

L’adresse IP qui était utilisée par le client devient libre et peut être utilisée par une autre machin

Exemple de scénario DHCP



Les baux

Toute attribution d’une configuration IP a une durée de validité et cette durée est fixée par le serveur à l’attribution.

C’est le principe du bail DHCP.

Avant l’expiration du bail, le client peut demander un prolongement en retransmettant un message **Request.**

Plusieurs cas possibles :

1. le serveur accepte le prolongement il répond avec un **message Ack** au client qui peut continuer à utiliser la configuration IP
2. le serveur refuse il répond avec un **message Nak** au client
   - Le client peut interroger d’autres serveurs (en envoyant d’autres Request) jusqu’à ce qu’un serveur lui réponde positivement avec un Ack ;
   - ou il abandonne et ne peut plus accéder à Internet.

Le service DNS — Résolution de noms

Problématique

I Quand deux machines communiquent sur Internet, elles utilisent leurs adresses IP uniquement.

I L'adressage IP est utilisé par toutes les protocoles sur l'Internet (web, messagerie, transfert de fichiers, . . .).

I Or, une adresse IP est difficile à mémoriser pour un utilisateur humain