

# **CCNA 2 - Essentiel**

---

Configuration des routeurs et routage basique

By DhiaEddineSaied

# 1. Réseaux WAN

## 1.1. Définition


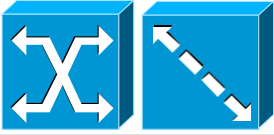
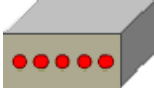

Par définition, un réseau WAN est :

- Un réseau longue distance
- Un réseau qui interconnecte des réseaux LAN qui sont habituellement séparés par de vastes étendues géographiques

Les principales caractéristiques des réseaux WAN sont les suivantes :

- Ils fonctionnent au niveau des couches physique et liaison de données du modèle de référence OSI.
- Ils fonctionnent au-delà de la portée géographique des réseaux LAN.
- Ils utilisent les services d'opérateurs Télécoms.
- Ils utilisent diverses connexions série pour communiquer.

## 1.2. Dispositifs WAN

	<b>Routeur</b>
	<b>Commutateur</b> (ATM, Frame Relay, RNIS)
	<b>Modem et unité CSU/DSU</b> (modem analogique, modem câble, unité CSU/DSU pour T1/E1, TA et NT1 pour RNIS)
	<b>Serveur de communication</b> (PABX)

Les dispositifs WAN les plus courants sont les suivants :

- **Routeur** : Dispositif de couche 3, il base ses décisions d'acheminement sur les adresses de couche 3 (IP, IPX, etc.). Il offre des interfaces LAN et WAN permettant l'interconnexion des réseaux locaux au réseau mondial (Internet).
- **Commutateur** : C'est un dispositif de couche 2 qui assure la commutation du trafic WAN. Ce dispositif est présent au cœur d'un réseau WAN.
- **Modem et unité CSU/DSU** : C'est une unité de couche 1, car elle n'agit qu'au niveau de la forme du signal électrique. Ce dispositif se place aux extrémités des liaisons WAN, adaptant ainsi les signaux au format désiré pour chaque côté.
- **Serveur de communication** : Il concentre les communications utilisateur entrantes et sortantes.

## 1.3. Normes WAN

Les principaux organismes définissant et gérant les normes WAN sont les suivants :

- **UIT-T** (Union Internationale des Télécommunications - secteur de normalisation des Télécommunications)
- **ISO** (International Organization for Standardization)
- **IETF** (Internet Engineering Task Force)
- **EIA** (Electrical Industries Association)
- **TIA** (Telecommunications Industry Association)

On peut classifier les normes WAN en fonction de la couche du modèle OSI correspondante. On obtient donc ceci :

- Normes de la couche physique
- Normes de la couche liaison de données

### 1.3.1. Normes WAN de la couche physique

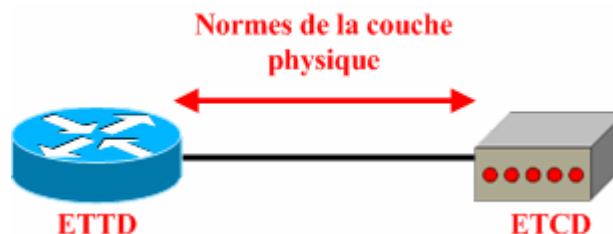
Les normes WAN de la couche physique décrivent comment fournir des connexions électriques, mécaniques, opérationnelles et fonctionnelles pour les services WAN.

Y sont décrits :

- L'équipement terminal de traitement des données (ETTD, ou DTE en Anglais)
- L'équipement de terminaison de circuit de données (ETCD, ou DCE en Anglais)

D'un point de vue définition :

- L'ETTD est la partie client d'une liaison WAN. C'est lui qui gère les données.
- L'ETCD est la partie fournisseur de services de la liaison WAN. Il a pour but d'acheminer les données fournies par l'ETTD.

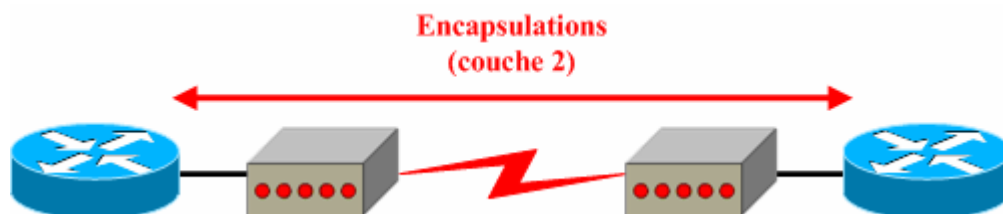


La couche physique d'un réseau WAN décrit principalement l'interface entre l'ETTD et l'ETCD :

- EIA/TIA-232
- EIA/TIA-449
- EIA/TIA-612/613
- V.24
- V.35
- X.21
- G.703

### 1.3.2. Normes WAN de la couche liaison de données

Les normes WAN de la couche liaison de données décrivent la façon dont les trames sont transportées entre des systèmes par une liaison unique. Elles définissent donc le mode d'encapsulation et les caractéristiques de transmission de ces données.



Les encapsulations les plus courantes sont les suivantes :

- **HDLC :**
  - Encapsulation par défaut pour les interfaces WAN d'un routeur Cisco
  - Peut être incompatible entre différents constructeurs, à cause de différences d'implémentation
  - Dérivé et remplaçant de SDLC
- **PPP :**
  - Comprend un champ identifiant le protocole de couche réseau
  - Gère l'authentification grâce aux protocoles PAP et CHAP
  - Remplace SLIP car plus polyvalent
- **Frame Relay :**
  - Encapsulation simplifiée, dérivée de LAPB
  - Dépourvue de mécanismes de correction d'erreurs
  - Prévüe pour des unités numériques haut de gamme
- **LAPB :**
  - Utilisée sur les réseaux X.25
- **LAPD :**
  - Utilisée sur les canaux D des liaisons RNIS

## 1.4. Technologies WAN

Les technologies WAN sont classifiées en fonction des catégories suivantes :

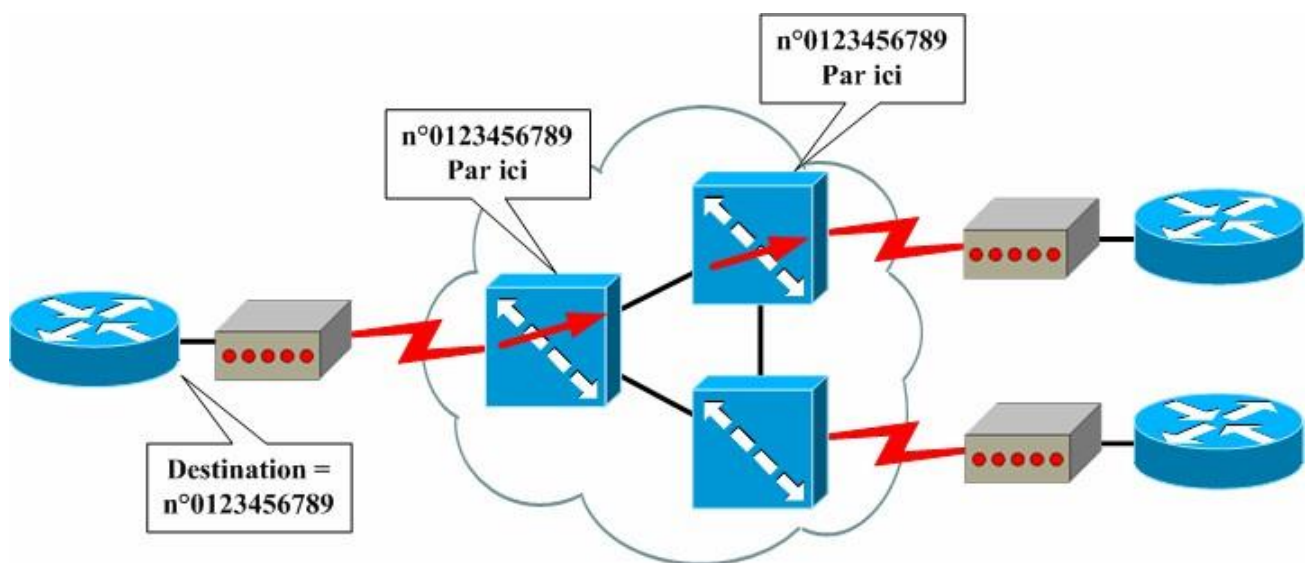
- Services à commutation de circuits
- Services à commutation de paquets
- Services à commutation de cellules
- Services dédiés
- Autres services

Les liaisons WAN doivent toujours être des liaisons point-à-point entre les équipements d'extrémité. Ceci peut être obtenu de deux façons :

- Utilisation d'une liaison physique distincte (services à commutation de circuits ou services dédiés)
- Utilisation d'un circuit virtuel au travers d'un environnement commuté (services à commutation de paquets/cellules)

### 1.4.1. Services à commutation de circuits

Les services à commutation de circuits se servent du réseau téléphonique (analogique ou numérique) pour créer une liaison dédiée non permanente entre la source et la destination.



La liaison est établie grâce à un identifiant, à savoir un numéro de téléphone, pour indiquer au réseau téléphonique la destination avec laquelle on souhaite créer une liaison. Après établissement de l'appel, la liaison dédiée est établie. Il s'agit donc d'une commutation physique des différents centraux téléphoniques.

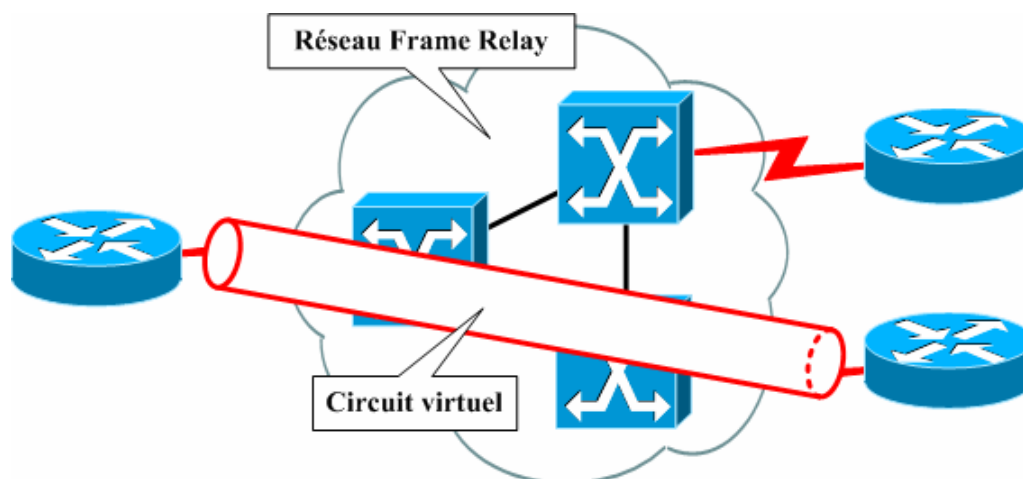
Les technologies basées sur ce type de service offrent la bande passante maximale du lien mais uniquement pour la durée de l'appel.

Les exemples de services à commutation de circuits sont :

- **POTS** (Plain Old Telephone Service)
- **RNIS** (Réseau Numérique à Intégration de Services)

### 1.4.2. Services à commutation de paquets/cellules

Le principe de base est de fournir une connectivité au travers de commutateurs. On a par conséquent la possibilité d'accéder à toutes les destinations possibles via des liaisons point-à-point ou point-à-multipoint (aussi appelé plus simplement multipoint).



L'utilisation de circuits virtuels par dessus un réseau commuté permet de respecter le principe de connexion point-à-point entre la source et la destination. Le résultat est donc d'avoir un circuit virtuel par destination.

La différence entre les services à commutation de paquets et de cellules est sur la taille des trames ainsi que sur leur traitement :

- Pour la commutation de paquets, les trames ont une taille variable et le traitement est logiciel.
- Pour la commutation de cellules, les trames ont une taille fixe et réduite permettant un traitement matériel.

Les technologies basées sur ces services offrent une bande passante partagée entre les différents trafics (partage de bande passante) de façon permanente.

Les technologies basées sur le service à commutation de paquets sont :

- **Frame Relay**
- **X.25**

Le seul exemple de service à commutation de cellules est :

- **ATM** (Asynchronous Transfer Mode)

### 1.4.3. Services dédiés

Les services dédiés offrent, comme leur nom l'indique, un lien physique dédié entre chaque source et destination. Le nombre de liens nécessaires s'accroît donc en fonction du nombre de clients à interconnecter.

Parmi les technologies existantes proposant un service dédié, on peut citer les suivants :

- **T1, T3, E1, E3**
- **SDH** (Synchronous Digital Hierarchy)

### 1.4.4. Autres services

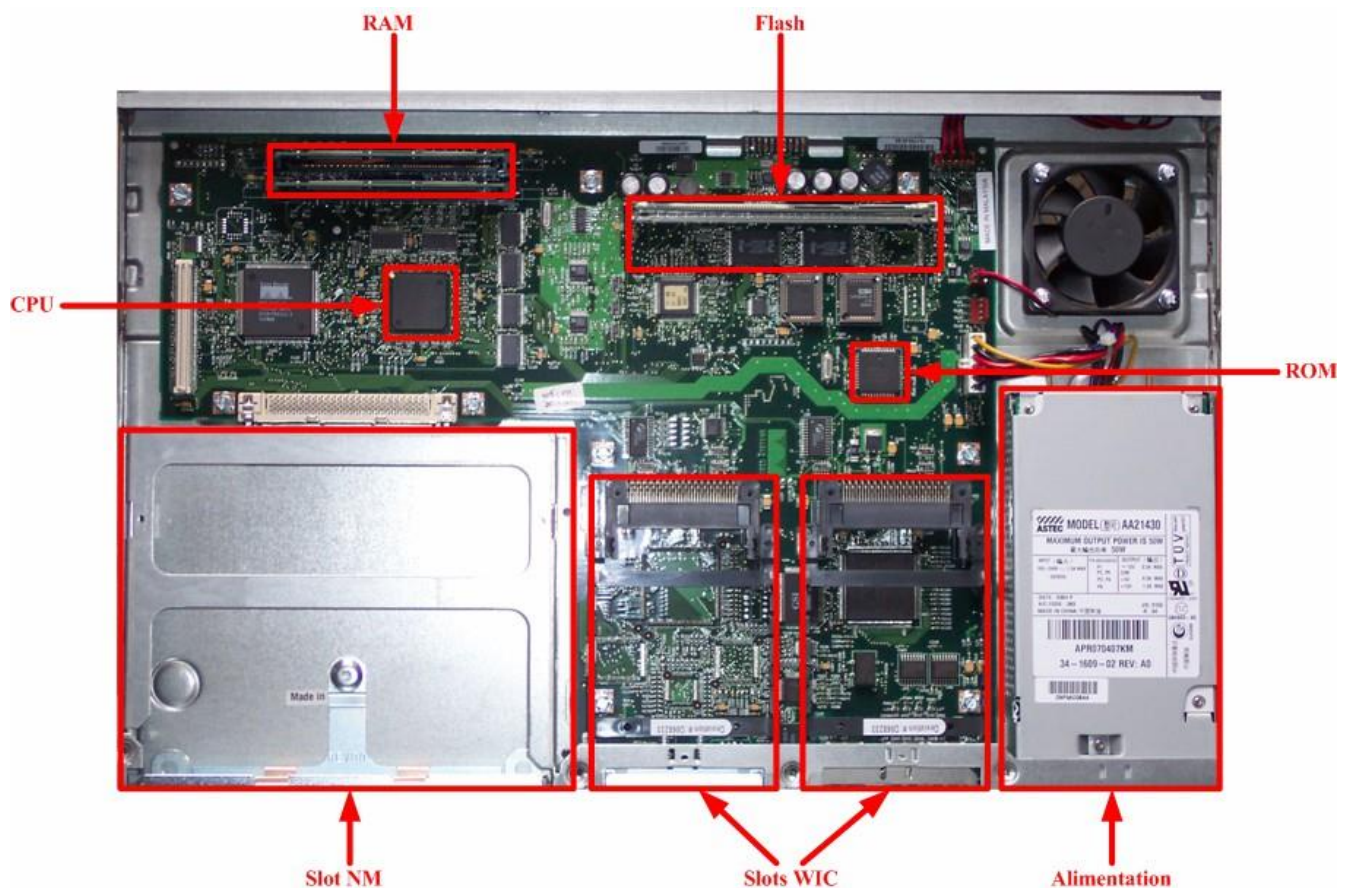
Toutes les technologies non référencées dans les catégories de services précédentes, principalement de nouvelles technologies, sont présentes dans cette dernière :

- **Modem câble**
- **Satellite**
- **Sans fil**

## 2. Introduction aux routeurs

### 2.1. Présentation d'un routeur Cisco

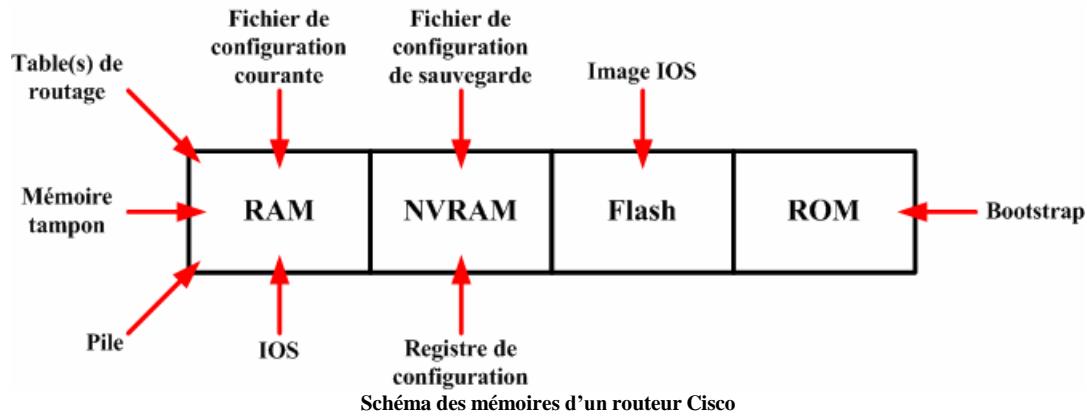
#### 2.1.1. Composants internes



Vue interne d'un routeur Cisco 2620XM

La connaissance exacte de l'emplacement de chaque composant interne n'est pas importante. Il peut tout de même être utile de savoir reconnaître les slots pour les barrettes de RAM et de Flash au cas où l'on souhaiterait effectuer une mise à jour.

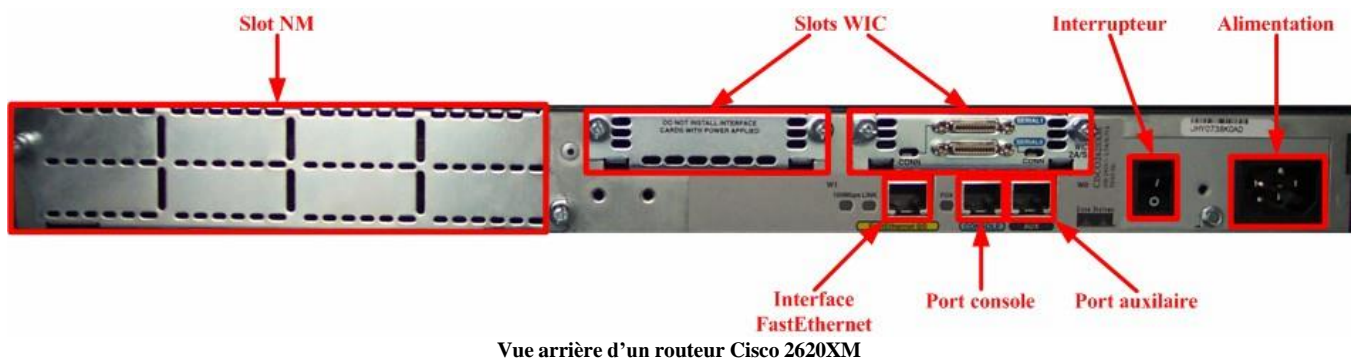




Schématiquement, les composants internes nous intéressant principalement sont les différentes mémoires utilisées par un routeur Cisco :

- **RAM** : C'est la mémoire principale de travail du routeur. Elle contient entre autres le système d'exploitation une fois chargé, le fichier de configuration active, la ou les tables de routage, ainsi que les mémoires tampon utilisées par les interfaces et la pile utilisée par les processus logiciels. Sa taille varie en fonction du modèle de routeur (64 ou 96 Mo sur un 2620XM). Le contenu de cette mémoire est perdu lors de la mise hors tension ou du redémarrage.
- **NVRAM (Non-Volatile RAM)** : Cette mémoire est non volatile, c'est-à-dire que son contenu n'est pas perdu lorsque l'alimentation est coupée. Sa très petite capacité de stockage (32 Ko sur un 2620XM) ne lui permet pas de stocker autre chose que le registre de configuration et le fichier de configuration de sauvegarde.
- **Flash** : C'est la mémoire de stockage principale du routeur. Elle contient l'image du système d'exploitation Cisco IOS (32 Mo sur un 2620XM). Son contenu est conservé lors de la mise hors tension et du redémarrage.
- **ROM** : Elle contient le bootstrap ainsi que la séquence d'amorçage du routeur. Ceci est donc uniquement utilisé au démarrage du routeur.

### 2.1.2. Composants externes



Un routeur Cisco peut offrir plusieurs types de connectiques parmi les suivantes :

- **Port console** : Accès de base pour configuration
- **Port auxiliaire** : Accès pour configuration au travers d'une ligne analogique et modems interposés
- **Interface(s) LAN**
- **Interface(s) WAN**
- **Slot(s) NM** (Network Module)
- **Slot(s) WIC** (WAN Interface Card)

## 2.2. Branchements

### 2.2.1. Interfaces LAN et WAN

Les interfaces réseaux fournies par un routeur Cisco peuvent être de divers types et sont classifiées en fonction du type de réseau à connecter (LAN ou WAN).

Elles peuvent être fixées au châssis ou livrées sous la forme de cartes (WIC ou NM) pour les routeurs modulaires.

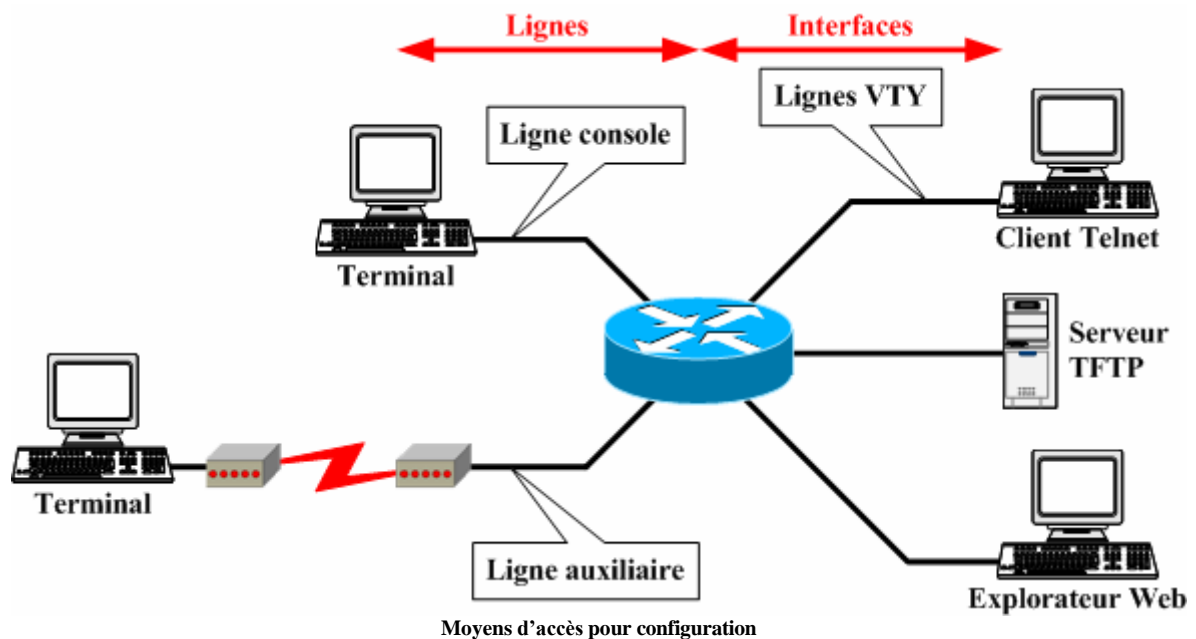
Ces interfaces seront utilisées par les protocoles de couche 3 du modèle OSI pour le routage.



Carte WIC-2A/S

### 2.2.2. Accès pour configuration

La configuration d'un routeur se fait par l'intermédiaire de lignes.

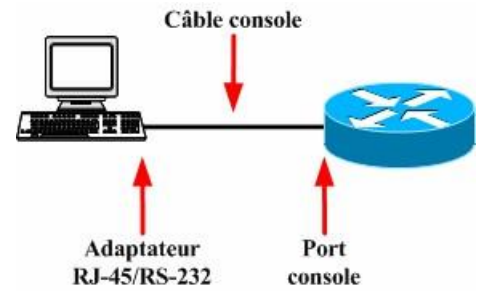


Un routeur peut être configuré à partir des sources externes suivantes :

- **Ligne console** : Accès primaire, à utiliser si aucun autre accès de configuration n'est disponible
- **Ligne auxiliaire** : Accès à distance via une liaison RTC et modems interposés
- **Ligne(s) VTY** : Accès via un client Telnet (5 ou 16 lignes disponibles par routeur en fonction du modèle)
- **Explorateur Web** : Accès utilisant le serveur HTTP interne du routeur
- **Serveur TFTP** : Import/export de fichiers de configuration
- **Serveur FTP** : Idem qu'avec un serveur TFTP

La ligne console est l'accès de configuration à utiliser lorsque aucune configuration n'est chargée ou si cette dernière ne permet pas l'accès par un autre moyen (Telnet, etc.).

Il faut connecter le port console du routeur à un port série (RS-232) en utilisant un câble console (rollover).

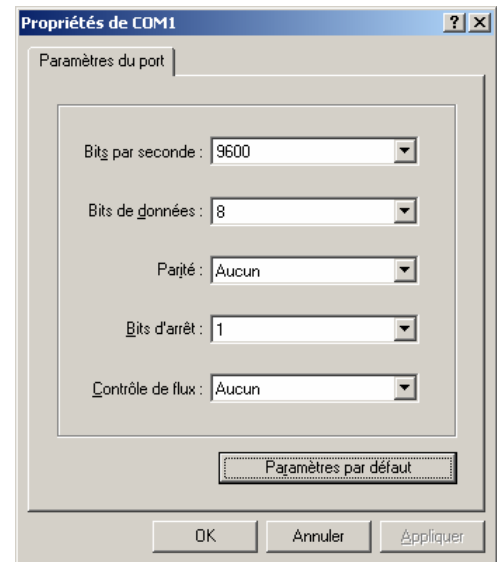


Un émulateur de terminaux (exemple : HyperTerminal sous Windows) permet l'accès à l'interface de configuration du routeur.

Les paramètres à utiliser sont les suivants :

- Vitesse : 9600 bauds
- Bits de données : 8
- Parité : Aucun
- Bits d'arrêt : 1
- Contrôle de flux : Aucun

Sous HyperTerminal, le bouton "Paramètres par défaut" permet de spécifier automatiquement ces paramètres.



Paramètres de connexion pour HyperTerminal

## 2.3. Système d'exploitation Cisco IOS

### 2.3.1. Principes et spécifications

IOS (Internetwork Operating System) est le système d'exploitation propriétaire Cisco utilisé sur la plupart des produits Cisco. Ce système d'exploitation offre une CLI (Command Line Interface).

Le programme d'exécution des commandes, ou EXEC, est l'un des composants de la plateforme logicielle Cisco IOS. EXEC reçoit et exécute les commandes entrées dans le CLI.

Pour arrêter l'exécution d'une commande, il faut utiliser une des combinaisons de touches suivantes :

- **CTRL+MAJ+6**
  - Pour toutes les commandes
- **CTRL+C**
  - Fonctionne avec les commandes **show** et pour le mode **SETUP**

EXEC transmet des messages de notification sur le terminal ainsi que les messages de déboguage. Par défaut, ces messages arrivent uniquement sur le terminal connecté via la ligne console. Pour activer ou désactiver l'affichage de ces messages, il faut utiliser la commande **[no] terminal monitor** depuis le mode utilisateur ou privilégié.

La commande **reload** permet de redémarrer à chaud le routeur.

### 2.3.2. Modes de commandes

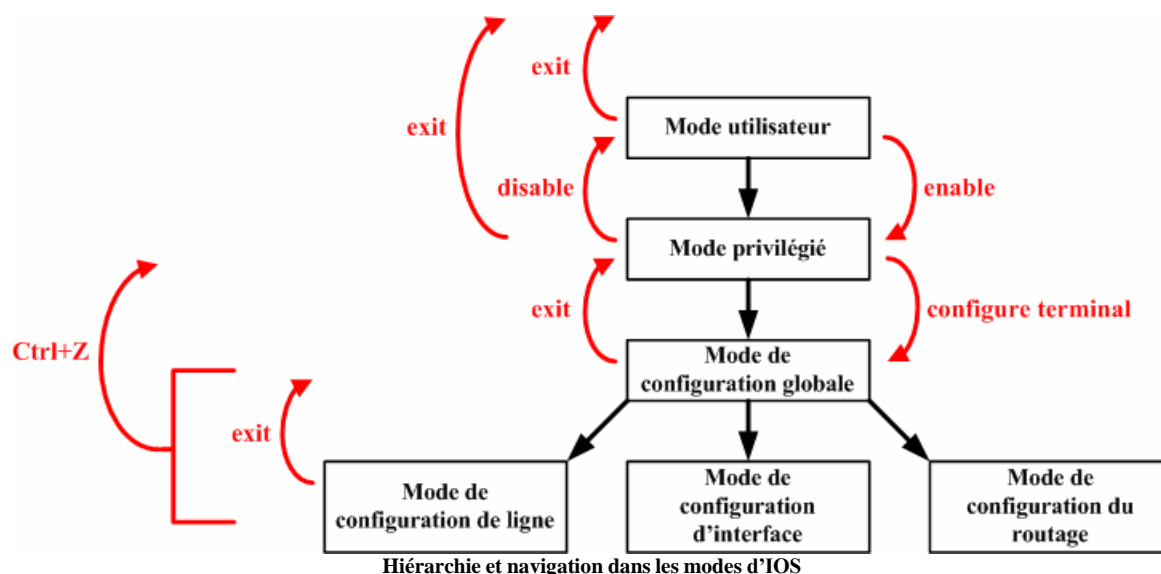
Il existe une multitude de modes différents accessibles en CLI sur un routeur Cisco :

- **Mode utilisateur** : Mode lecture qui permet à l'utilisateur de consulter des informations sur le routeur, mais ne lui permet pas d'effectuer des modifications. Dans ce mode, on dispose uniquement de commandes de visualisation d'état de fonctionnement du routeur. C'est dans ce mode que l'on arrive lorsque l'on se connecte au routeur.
- **Mode privilégié** : Mode lecture avec pouvoir. On dispose d'une panoplie complète de commandes pour visualiser l'état de fonctionnement du routeur, ainsi que pour importer/exporter et sauvegarder des fichiers de configurations et des images d'IOS.
- **Mode de configuration globale** : Ce mode permet d'utiliser toutes les commandes de configuration ayant une portée globale à tout le routeur.
- **Modes de configuration spécifiques** : On ne dispose dans chaque mode spécifique que des commandes ayant une portée localisée au composant du routeur spécifié par ce mode.
- **Mode SETUP** : Mode affichant un dialogue interactif, grâce auquel l'utilisateur néophyte peut créer une configuration élémentaire initiale.
- **Mode RXBoot** : Mode de maintenance permettant notamment de récupérer des mots de passe perdus.

On peut facilement identifier le mode dans lequel on est en repérant l'invite de commande que nous fournit l'interpréteur de commandes EXEC :

Mode	Invite de commande
Utilisateur	Router >
Privilégié	Router #
Configuration globale	Router (config) #
Interface	Router (config-if) #
Ligne	Router (config-line) #
Routage	Router (config-router) #

Nous allons maintenant voir les commandes et les combinaisons de touches permettant de naviguer dans ces différents modes d'IOS :



Les commandes à utiliser pour passer dans un mode de configuration spécifique sont les suivantes :

- **line {type} {numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'une ligne
- **interface {type} {numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface
- **router {protocole} [option]**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration du routeur

Pour les lignes et les interfaces, la numérotation commence à 0.

### 2.3.3. Système d'aide

Le principe d'aide pour les commandes sur la plateforme logicielle Cisco IOS est très simple et est constitué de trois choses :

- **Le caractère ?** : Ce caractère permet d'obtenir les différentes possibilités disponibles. Ce caractère peut être utilisé de 3 façons différentes, à savoir seul, collé à une chaîne de caractères ou après un mot clé. Seul, ce caractère indique au routeur de nous fournir une liste complète des commandes accessibles depuis le mode dans lequel on se trouve. Collé à une chaîne de caractères, il fournit la liste des mots clé commençant par cette chaîne. Enfin, après un mot clé, il fournit la liste des options pour ce dernier.
- **Le caractère ^** : Celui-ci nous indique à quel endroit se trouve une erreur dans une commande erronée. Dans ce cas, il suffit juste de retaper la commande jusqu'à ce caractère, puis d'utiliser le caractère ? pour obtenir la liste des possibilités pour cette commande.
- **La touche de tabulation** : Cette touche est très couramment utilisée en environnement IOS car, à l'instar de certains Shell UNIX, elle effectue une complétion maximale par rapport aux différentes possibilités.

### 2.3.4. Commandes d'édition avancée

L'interface utilisateur offre un mode d'édition avancée nous permettant de modifier une commande au cours de la frappe. Voici un tableau résumant ces combinaisons de touche :

Commande	Description
CTRL+A	Revient au début de la ligne de commande
ECHAP+B	Reculé d'un mot
CTRL+B ou ←	Reculé d'un caractère
CTRL+E	Va à la fin de la ligne de commande
CTRL+F ou →	Avance d'un caractère
ECHAP+F	Avance d'un mot
terminal [no] editing	Active/désactive les commandes d'édition avancée

Il existe un autre point à voir. Il ne s'agit pas d'une commande en lui-même, mais plutôt d'un petit système d'information pratique. Il s'agit du **caractère \$** qui peut apparaître en début ou en fin de ligne d'écran lorsque la commande en elle-même fait plus d'une ligne écran. Ceci indique donc qu'une partie de la ligne de commande est masquée.

### 2.3.5. Historique des commandes

L'interface utilisateur fournit un historique des commandes entrées. Cette fonction est particulièrement utile pour rappeler des commandes ou des entrées longues ou complexes. La fonction d'historique des commandes vous permet d'accomplir les tâches suivantes :

- Réglage de la capacité du tampon d'historique des commandes
- Rappel des commandes
- Désactivation de la fonction d'historique des commandes

Par défaut, la fonction d'historique des commandes est active et le système enregistre 10 lignes de commandes dans son tampon.

Ce tableau nous indique les différentes commandes d'historique que nous avons à notre disposition :

Commande	Description
CTRL+P ou ↑	Rappel de la commande précédente
CTRL+N ou ↓	Rappel de la commande suivante
show history	Affiche la liste des commandes en mémoire
terminal history size {taille}	Définit la taille de la mémoire de commandes (valeur maximale de 256)
terminal [no] history	Active/désactive les fonctions d'historique

Les trois dernières commandes sont utilisables dans les modes utilisateur et privilégié uniquement.

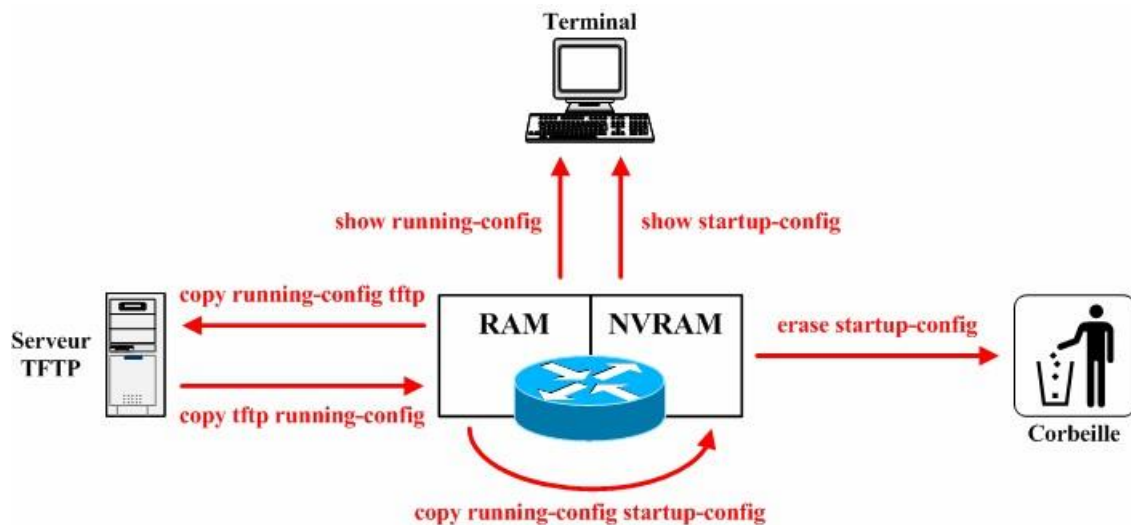
### 2.3.6. Fichiers de configuration

Les deux fichiers de configuration d'un routeur Cisco sont les fichiers de configuration active (dans la RAM) et de sauvegarde (dans la NVRAM). Ils régissent respectivement la configuration en cours d'utilisation par le routeur et la configuration utilisée lors du démarrage du routeur.

Les informations contenues dans un fichier de configuration sont les suivantes :

- Des informations génériques concernant la version d'IOS avec laquelle le fichier de configuration est prévu pour fonctionner
- Le nom du routeur ainsi que le mot de passe du mode privilégié
- Les entrées statiques de résolution de noms
- Chaque interface avec sa configuration spécifique
- Toutes les informations de routage
- Chaque ligne et sa configuration spécifique

Les différentes commandes (IOS >= 11) associées aux fichiers de configuration sont les suivantes :



- **show running-config** : Affiche la configuration courante
- **show startup-config** : Affiche la configuration de sauvegarde
- **copy running-config startup-config** : Sauvegarde la configuration courante dans la NVRAM
- **copy running-config tftp** : Exporte la configuration courante vers un serveur TFTP
- **copy tftp running-config** : Importe une configuration dans la RAM depuis un serveur TFTP
- **copy startup-config tftp** : Exporte la configuration de sauvegarde vers un serveur TFTP
- **copy tftp startup-config** : Importe une configuration dans la NVRAM depuis un serveur TFTP
- **erase startup-config** : Supprime le fichier de configuration de sauvegarde

## **3. Configuration de base d'un routeur**

### **3.1. Commandes de visualisation d'état**

IOS propose une panoplie importante de commandes permettant la visualisation de l'état. Ces commandes commencent toutes par le mot clé **show**. Les commandes de visualisation d'état à connaître en premier lieu sont les suivantes :

- **show running-config** : Affiche le fichier de la configuration active
- **show startup-config** : Affiche le fichier de la configuration de sauvegarde
- **show version** : Affiche la configuration matérielle système, la version d'IOS, le nom et la source de l'image IOS d'amorçage, ainsi que la valeur du registre de configuration
- **show processes** : Affiche des informations sur les processus actifs
- **show memory** : Affiche des statistiques sur la mémoire du routeur, y compris sur la mémoire disponible
- **show stacks** : Contrôle l'utilisation de la pile par les processus et les routines
- **show buffers** : Fournit des statistiques sur les mémoires tampon des interfaces du routeur
- **show arp** : Affiche les entrées ARP connues
- **clear arp** : Vide les entrées dynamiques de la table ARP
- **show hosts** : Affiche la table de résolution de noms
- **show flash** : Affiche des informations sur la mémoire Flash, telles que la quantité d'espace libre et le nom des fichiers présents dans cette mémoire
- **show interfaces [{type} {numéro}]** : Affiche les informations de configuration ainsi que des statistiques de trafic pour chaque interface configurée sur le routeur (couches 2 et 3)
- **show controllers [{type} {numéro}]** : Affiche les informations de couche 1 des interfaces
- **show ip interface [{type} {numéro}] [brief]** : Affiche les informations IP pour les interfaces
- **clear counters [{type} {numéro}]** : Permet de mettre à zéro toutes les statistiques des interfaces du routeur
- **show ip route** : Affiche la table de routage IP
- **show protocols** : Affiche le nom et l'état de tous les protocoles configurés de couche 3
- **show ip protocols** : Affiche les valeurs des compteurs de routage et les informations de réseau associées à l'ensemble du routeur. Cette commande nous indique les différents réseaux avec lesquels le protocole de routage est configuré pour communiquer, ainsi que la distance administrative de ce dernier.
- **show sessions** : Affiche la liste des sessions en cours
- **show users** : Affiche la liste des utilisateurs actuellement connectés au routeur
- **show clock** : Affiche la date et l'heure actuelle
- **show history** : Affiche la liste des commandes en mémoire



### 3.2. Date et heure

Comme pour tout système informatique, la date et l'heure peuvent être configurés. Ceci peut s'avérer utile lorsque l'on utilise les fonctions de log ou de débogage, en fournissant la date et l'heure exacte des événements survenus.

Les commandes utilisées pour le système de date et d'heure sont les suivantes :

- **show clock**
  - Affiche la date et l'heure du système
- **clock set {hh:mm:ss} {jour} {mois} {année}**
  - Mode privilégié
  - Permet de configurer l'heure sur le routeur
  - **hh:mm:ss** correspond à l'heure (de 0 à 23), aux minutes et aux secondes.
  - **jour** est un nombre (de 1 à 31).
  - **mois** est le nom du mois.
  - **année** est l'année avec 4 chiffres.

Cette configuration est manuelle, et est nécessaire à chaque redémarrage du routeur. Il est possible d'utiliser le protocole NTP (Network Time Protocol), afin de maintenir synchronisé le routeur avec un serveur de temps.

### 3.3. Nom d'hôte et résolution de noms

Les noms d'hôtes sont très utiles. En effet, ils permettent d'identifier un hôte avec un nom facile à retenir plutôt que d'utiliser des adresses de couches réseau. Pour pouvoir utiliser ces noms d'hôtes, il faut un système de résolution de noms, sachant que cette résolution de noms a une portée locale.

Les noms d'hôtes et les résolutions de noms ne sont pas transmis de routeur à routeur. Cela signifie qu'il faut configurer la résolution de noms sur tous les dispositifs réseau sur lesquels on souhaite utiliser des noms d'hôtes pour la communication réseau.

Il est possible de configurer :

- Le nom d'hôte du routeur
- La résolution de noms statique
- La résolution de noms dynamique grâce au protocole DNS

Les commandes à utiliser sont les suivantes :

- **hostname {nom}**
  - Mode de configuration globale
  - Attribution du nom d'hôte du routeur
  - Ce nom est affiché par l'invite de commandes.
  - La valeur par défaut est "Router".
- **ip host {nom} [tcp\_port\_number] {IP1} [{IP2}...]**
  - Mode de configuration globale
  - Création d'une entrée statique de résolution de noms dans la table d'hôtes
  - **tcp\_port\_number** permet de spécifier le port TCP à utiliser avec cet hôte pour un accès Telnet.
  - Il est possible de spécifier plusieurs adresses IP pour un seul hôte. Dans ce cas, seule la commande **telnet** utilisera les adresses autres que la première si les précédentes ne répondent pas.
- **[no] ip domain-lookup**
  - Mode de configuration globale
  - Active/désactive la résolution dynamique de noms (DNS)
- **ip name-server {DNS1} [{DNS2}...]**
  - Mode de configuration globale
  - Permet de spécifier le ou les serveurs DNS avec lesquels nous effectuerons les résolutions d'adresses
  - On peut préciser jusqu'à 6 serveurs DNS différents.
- **ip domain-name {préfixe}**
  - Mode de configuration globale
  - Précise le préfixe DNS par défaut à utiliser pour la résolution d'adresses dynamique

La commande **show hosts** permet d'afficher la table des correspondances entre les noms d'hôte et leur(s) adresse(s) de couche 3. Les champs de cette table sont les suivants :

Information	Description
Host	Noms des machines connues
Flag	Description de la méthode utilisée pour apprendre les informations et pour juger de leur pertinence actuelle
perm	Configuré manuellement dans une table d'hôtes
temp	Acquis par le biais d'un serveur DNS
OK	Entrée valide
EX	Entrée obsolète, expirée
Age	Temps (en heures) écoulé depuis que le logiciel a appris l'entrée
Type	Champ identifiant le protocole de couche 3
Address(es)	Adresses logiques associées au nom de machine

### 3.4. Descriptions et bannière de connexion

Les descriptions d'interface et la bannière de connexion sont très utiles pour fournir des informations quant à l'utilité ou la fonction de chaque routeur et de chacune de ces interfaces.

La bannière de connexion s'affiche lors de la connexion d'un terminal à une ligne et permet de transmettre un message aux utilisateurs du routeur. Ceci peut être utile pour les avertir d'un arrêt imminent du routeur ou pour faire passer un message publicitaire.

Pour définir cette bannière, il faut utiliser la commande :

- **banner motd {caractère d'encapsulation} {message} {caractère d'encapsulation}**
  - Mode de configuration globale
  - Le message doit être encapsulé entre un caractère quelconque qui ne doit pas exister dans le message.

Enfin, on peut indiquer une description pour chaque interface du routeur. Ceci est très utile pour ceux qui seraient censés travailler sur ce routeur et qui ne connaissent pas forcément à quoi peut être attribué une interface. Pour cela, il faut utiliser la commande :

- **description {texte}**
  - Mode de configuration d'interface
  - Le texte de description ne peut pas excéder 80 caractères sur les anciens modèles (exemple : Routeur 2500) ou 240 caractères sur les modèles plus récent (exemple : Routeur 2600).
  - Cette description est visible en utilisant la commande **show interfaces**.

### 3.5. Mots de passe

On peut protéger notre système à l'aide de mots de passe pour en restreindre l'accès. Une protection par mot de passe peut être installée pour chaque ligne ainsi que sur l'accès au mode privilégié.

Pour configurer une protection par mot de passe sur une ligne, il faut utiliser les commandes suivantes :

- **line {console | aux | vty} {{numéro} | {premier} {dernier}}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration de la ou des lignes voulues
  - Il est possible d'accéder à plusieurs lignes en même temps. Pour cela, il suffit de préciser non pas le numéro mais la plage de numéros. Par exemple, pour accéder directement dans le mode de configuration des 5 lignes VTY, il suffit d'utiliser la commande **line vty 0 4**.
- **password {mot de passe}**
  - Mode de configuration de ligne
  - Permet de spécifier le mot de passe pour la ligne courante
  - Le mot de passe est écrit par défaut en clair dans le fichier de configuration.
- **login**
  - Mode de configuration de ligne
  - Précise qu'aucun login ne sera demandé lors de la connexion
  - Cette commande ne peut être utilisée que si un mot de passe est déjà configuré sur la ligne.

Les mots de passe pour les lignes console et auxiliaire ne sont pris en compte qu'après le redémarrage du routeur.

Les lignes auxiliaire et VTY ne sont pas opérationnelles si elles n'ont pas de mot de passe configuré. Cela signifie qu'aucun accès autre que par la ligne console n'est faisable sans configuration préalable.

On peut aussi restreindre l'accès au mode privilégié en utilisant au moins une de ces commandes :

- **enable password {mot de passe}**
  - Mode de configuration globale
  - Le mot de passe est écrit en clair dans le fichier de configuration.
- **enable secret {mot de passe}**
  - Mode de configuration globale
  - Le mot de passe est crypté dans le fichier de configuration en utilisant l'algorithme MD5.
  - Cette commande est prioritaire par rapport à **enable password** si elles sont toutes deux configurées.

Malheureusement, tous les mots de passe, à l'exception du **enable secret**, sont écrits en clair dans le fichier de configuration. Ceci implique une plausible faille de sécurité (sauvegarde d'un fichier de configuration sur un serveur TFTP non sécurisé, etc.).

Pour y remédier, il faut utiliser la commande **service password-encryption** depuis le mode de configuration globale. Cette commande permet de crypter tous les mots de passe écrits en clair dans le fichier de configuration en utilisant un algorithme propriétaire Cisco.

### 3.6. Serveur HTTP

IOS fournit un serveur HTTP. Ce serveur fournit un moyen d'accès pour configuration.

La commande à utiliser pour contrôler l'état de ce serveur HTTP est :

- **[no] ip http server**
  - Mode de configuration globale
  - Active/désactive le serveur HTTP interne du routeur
  - Actif par défaut

Pour accéder au service HTTP fourni par le routeur, il faut utiliser un explorateur Web et y accéder en indiquant l'adresse IP d'une interface.

Lors de la connexion, la page Web demande un nom d'utilisateur et un mot de passe. Les valeurs par défaut correspondent à aucun nom d'utilisateur et au mot de passe du mode privilégié.

Ce serveur HTTP faisant l'objet de beaucoup d'exploits et de failles de sécurité, il est recommandé de le désactiver lorsque l'on n'en a plus besoin.

### 3.7. Configuration des interfaces

Les interfaces sont utilisées par les routeurs pour transférer les paquets de données entre différents réseaux de couche 3.

Ces interfaces peuvent être de multiples types. Dans ce cours, nous étudierons uniquement les interfaces suivantes :

- Loopback
- Ethernet
- Serial

La commande **show interfaces** permet l'affichage de l'état des interfaces du routeur. On peut déterminer :

- L'adresse IP et le masque de sous-réseau
- L'adresse de couche 2
- L'encapsulation utilisée
- Les statistiques sur le trafic transitant au travers de chaque interface
- L'état de l'interface, qui correspond à ceci :

Interface (couche 1)	Line protocol (couche 2)
Administratively down (shutdown)	Down (problème de couche 2)
Down (problème de câble)	Up (réception des "keepalive")
Up (média fonctionnel)	

#### 3.7.1. Interfaces Loopback

Les interfaces Loopback sont généralement utilisées pour simuler des interfaces réelles.

Pour leur configuration, on dispose des commandes suivantes :

- **interface loopback {numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface
- **ip address {IP} {masque} [secondary]**
  - Mode de configuration d'interface
  - Permet d'attribuer une adresse IP à cette interface
  - Le paramètre **secondary** précise qu'il s'agit d'une adresse IP secondaire

#### 3.7.2. Interfaces Ethernet/IEEE 802.3

Les interfaces de type Ethernet/IEEE 802.3 peuvent être de type :

- Ethernet (IEEE 802.3)
- Fast Ethernet (IEEE 802.3u)
- Gigabit Ethernet (IEEE 802.3ab ou IEEE 802.3z)
- 10-Gigabit Ethernet (IEEE 802.3ae)

Les interfaces Gigabit ou 10-Gigabit ne seront pas étudiées dans ce cours.

La configuration basique de ces interfaces est très simple, et se résume à ces commandes :

- **interface {Ethernet | FastEthernet} {numéro | slot/numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface
- **ip address {IP} {masque} [secondary]**
  - Mode de configuration d'interface
  - Permet d'attribuer une adresse IP à cette interface
  - Le paramètre **secondary** précise qu'il s'agit d'une adresse IP secondaire
- **[no] keepalive**
  - Mode de configuration d'interface
  - Active/désactive les "keep alive" sur l'interface
  - Utile pour rendre une interface opérationnelle sans avoir à brancher un média
- **[no] shutdown**
  - Mode de configuration d'interface
  - Active/désactive administrativement l'interface

### 3.7.3. Interfaces série

Les interfaces série sont classifiées en fonction de leur mode de transmission qui peut être :

- Synchrone
- Asynchrone
- Synchrone/asynchrone (par défaut en mode synchrone)

Elles sont le plus souvent présentes sous la forme de cartes WIC à insérer dans des slots de routeurs modulaires.

Les commandes utilisées par ces interfaces sont les suivantes :

- **interface {serial | async} {numéro | slot/numéro}**
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface
  - Le mot clé **async** n'est utilisable que pour les interfaces de type asynchrone.
- **clock rate {vitesse}**
  - Mode de configuration d'interface
  - Spécifie la vitesse de fonctionnement de la liaison WAN
  - A faire uniquement sur une interface ETCD
  - Le paramètre **vitesse** est exprimé en bits par seconde.
- **ip address {IP} {masque} [secondary]**
  - Mode de configuration d'interface
  - Permet d'attribuer une adresse IP à cette interface
  - Le paramètre **secondary** précise qu'il s'agit d'une adresse IP secondaire
- **[no] shutdown**
  - Mode de configuration d'interface
  - Active/désactive administrativement l'interface

## **4. Informations et accès aux autres dispositifs**

### **4.1. CDP**

Le protocole CDP (Cisco Discovery Protocol) est un protocole de découverte des voisins propriétaire Cisco.

Il permet d'obtenir des informations sur les dispositifs connectés au routeur local. Ce protocole devient très utile lorsque l'on n'a aucun moyen (visuellement ou par accès de configuration) pour analyser la topologie réseau.

#### **4.1.1. Théorie**

Le protocole CDP permet principalement de connaître les plateformes et les protocoles utilisés par les dispositifs voisins (c'est-à-dire directement connectés).

Voici les différentes caractéristiques du protocole CDP :

- Existe depuis IOS 10.3
- Actif par défaut
- Fonctionne au niveau de la couche 2 (permet donc d'obtenir des informations sur les voisins même si les protocoles de couche 3 sont différents ou non configurés)
- Trames CDP multicast envoyées toutes les 60 secondes

CDP peut fournir ces informations :

<b>Information</b>	<b>Description</b>
ID de dispositif	Nom d'hôte et nom de domaine du voisin
Liste d'adresses	Une adresse pour chaque protocole routé du voisin
Identifiant de port	Interface du voisin utilisée pour se connecter au routeur local
Liste de capacités	Fonction du dispositif voisin (routeur, pont, commutateur, etc.)
Version d'IOS	Version d'IOS du voisin
Plateforme	Type de dispositif (Cisco 2620XM, Catalyst 2950, etc.)

### 4.1.2. Configuration

La configuration de CDP est très simple, et se résume à ces commandes :

- **[no] cdp run**
  - Mode de configuration globale
  - Active/désactive le protocole CDP pour tout le routeur
  - Actif par défaut
- **[no] cdp enable**
  - Mode de configuration d'interface
  - Active/désactive le protocole CDP pour cette interface
  - Actif par défaut sur toutes les interfaces fonctionnelles
- **cdp timer {temps}**
  - Mode de configuration globale
  - Spécifie l'intervalle de temps en secondes pour l'émission des trames CDP
  - Temps par défaut : 60 secondes
- **cdp holdtime {temps}**
  - Mode de configuration globale
  - Spécifie le temps en secondes avant suppression d'une information non rafraîchie
  - Temps par défaut : 180 secondes

### 4.1.3. Visualisation et résolution de problèmes

Voici les commandes utilisées pour afficher les informations obtenues grâce à CDP :

- **show cdp** : Affiche les compteurs de temps pour CDP
- **show cdp interface [{type} {numéro}]** : Affiche les interfaces sur lesquelles CDP est activé
- **show cdp entry {nom | \*}** : Affiche les informations pour un voisin particulier
- **show cdp neighbors [detail]** : Affiche la liste des voisins CDP ainsi que les informations les concernant
- **show cdp traffic** : Affiche les compteurs de trafic CDP
- **clear cdp counters** : Réinitialise les compteurs de trafic CDP
- **clear cdp table** : Vide la table d'informations CDP

## 4.2. Telnet

### 4.2.1. Théorie

Telnet est un protocole faisant partie intégrante de la pile de protocole TCP/IP et fonctionnant au niveau de la couche application du modèle OSI. Il offre un moyen d'accès distant aux dispositifs réseaux sous la forme d'un terminal virtuel (VTY).

La communication réseau s'effectue à l'aide du protocole TCP sur le port 23.

Telnet est utilisé à la fois pour l'accès distant pour configuration ainsi qu'à des fins de tests et de résolution de problèmes. Ce dernier point sera étudié dans le chapitre correspondant.



### 4.2.2. Commandes et utilisation

L'accès Telnet s'effectue au travers d'une ligne VTY. Un tel accès est par conséquent possible que si au moins une ligne VTY est correctement configurée et libre.

Pour rappel, chaque routeur Cisco dispose d'un total de 5 ou 16 lignes VTY (dépend du modèle et de l'IOS).

Les commandes et combinaisons de touches liées à l'utilisation de Telnet sont les suivantes :

<b>telnet {IP   nom} [tcp_port_number]</b>	Etablir une session Telnet avec l'hôte correspondant à l'IP ou au nom précisé ( <b>tcp_port_number</b> permet d'explicitier le numéro de port TCP à utiliser)
<b>connect {IP   nom}</b>	Idem qu'avec <b>telnet</b>
<b>{IP   nom}</b>	Idem qu'avec <b>telnet</b>
<b>exit</b>	Fermeture de la session Telnet avec déconnexion (déconnecté par défaut après 10 minutes d'inactivité)
<b>disconnect</b>	Idem qu'avec <b>exit</b>
<b>CTRL+MAJ+6 puis X</b>	Suspendre la session Telnet en cours et la mettre en tâche de fond (reprise avec la touche <b>Entrée</b> si une seule session est en tâche de fond, sinon utiliser la commande <b>resume</b> )
<b>show sessions</b>	Afficher la liste des sessions en cours
<b>resume {numéro}</b>	Reprend la session Telnet précisée ( <b>numéro</b> correspond à celui fournit par la commande <b>show sessions</b> )

La combinaison de touches **CTRL+MAJ+6** ne fonctionne qu'avec un clavier QWERTY.

On peut observer qu'une erreur dans l'écriture d'une ligne de commande quelconque depuis le mode privilégié pourrait faire croire à IOS que l'on tente d'établir une session Telnet vers un hôte ayant pour nom notre commande erronée. Cela aurait pour impact de lancer une résolution DNS, qui pourrait durer jusqu'à expiration du timeout, pour obtenir l'adresse IP de cet hôte fictif. L'une des solutions pour remédier à ce problème est de désactiver le service DNS sur le routeur si on ne l'utilise pas.

## 5. Gestion d'IOS et processus de démarrage

### 5.1. Processus de démarrage

Le processus de démarrage d'un routeur Cisco est important à connaître, malgré le fait que l'on ne fasse pas de modification sur ce processus à longue durée de temps. Ceci devient par contre indispensable lorsqu'il faut mettre à jour l'image d'IOS actuellement en place ou lorsqu'un problème survient.

Cette partie portera sur :

- **La séquence d'amorçage** : Quelles sont les étapes de l'amorçage d'un routeur Cisco ?
- **Les commandes boot system** : Où le routeur peut trouver une image d'IOS ?
- **Le registre de configuration** : Comment doit démarrer le routeur ?

#### 5.1.1. Séquence d'amorçage

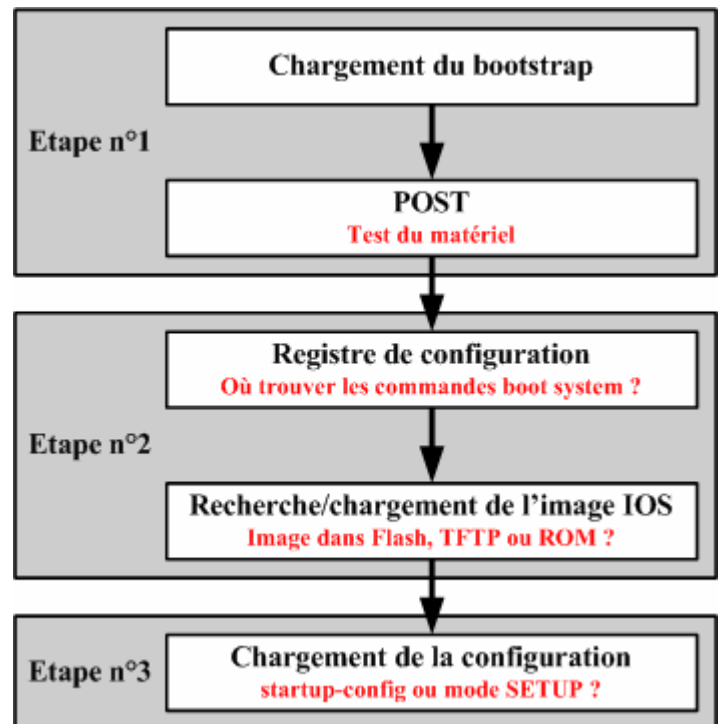
La séquence d'amorçage d'un routeur est découpée en 3 étapes :

- Etape n°1 : POST (Power On Self Test)
- Etape n°2 : Chargement d'IOS
- Etape n°3 : Chargement de la configuration

L'étape n°1 se résume au chargement du bootstrap, microcode contenu dans la ROM du routeur, qui va se charger de tester le matériel.

L'étape n°2 consiste à trouver une image d'IOS fonctionnelle afin de la charger en RAM. Ceci se fait en 2 phases.

La première phase consiste à analyser la valeur du registre de configuration, afin de déterminer si le routeur doit utiliser la séquence de recherche d'image IOS par défaut ou celle précisée dans le fichier de configuration de sauvegarde.



La deuxième phase correspond à la recherche de l'image d'IOS à proprement parler, en utilisant ces séquences de recherche. Si la séquence de recherche d'image IOS précisée dans le fichier de configuration de sauvegarde ne permet pas de trouver une image valide ou si elle est ignorée, le routeur tentera de démarrer en utilisant la première image présente en Flash.

Si aucune image IOS n'a pu être trouvée, le démarrage du routeur s'arrêtera au mode RXBoot.

L'étape n°3 consiste à charger une configuration. Par défaut, le routeur importera le fichier de configuration de sauvegarde dans le fichier de configuration courante.

Si le fichier de configuration de sauvegarde n'est pas chargé, car inexistant ou ignoré, la configuration initiale est chargée et le mode SETUP est automatiquement lancé, afin de procéder à la configuration basique du routeur.

### 5.1.2. Commandes boot system

Les commandes **boot system**, aussi appelées options bootstrap, servent à indiquer au routeur l'emplacement d'une image IOS et peuvent désigner trois types d'emplacements différents :

- **Flash** : C'est l'espace de stockage standard pour les images IOS.
- **TFTP** : Le serveur TFTP permet de stocker de nombreux fichiers. Il est généralement utilisé à des fins de mise à jour du système.
- **ROM** : Sur les anciens routeurs, tels que les Cisco 2500, la ROM contenait une image IOS minimaliste. Celle-ci était utilisée comme solution de secours. Sur les nouveaux routeurs, ceci n'est plus utile car le mode RXBoot est beaucoup plus performant et permet à lui seul de récupérer une image IOS depuis un serveur TFTP.
- **boot system flash {nom du fichier}**
  - Mode de configuration globale
  - Permet de spécifier le nom du fichier dans la Flash contenant l'image IOS
- **boot system tftp {nom du fichier} {IP du serveur TFTP}**
  - Mode de configuration globale
  - Précise le nom du fichier ainsi que l'adresse IP du serveur TFTP stockant l'image IOS
- **boot system rom**
  - Mode de configuration globale

Ces commandes permettent donc de préciser l'emplacement ainsi que l'ordre de recherche de l'image IOS pour la séquence d'amorçage. L'emplacement est explicité par la commande elle-même, alors que l'ordre de recherche est défini par l'ordre dans lequel on a entré les commandes.

### 5.1.3. Registre de configuration

Le registre de configuration est un registre de 16 bits qui se trouve dans la mémoire NVRAM. Sa valeur est exprimée en hexadécimal et sa valeur par défaut est 0x2102. Les 4 bits inférieurs constituent le champ d'amorçage.

Le tableau suivant nous indique les différentes valeurs possibles pour ce champ d'amorçage, ainsi que leur signification :

Valeur	Description
0x---0	Passer par le mode moniteur de mémoire ROM et attendre que l'utilisateur tape la commande <b>b</b> ou <b>boot</b> pour démarrer
0x---1	Démarrer avec la première image présente en Flash ou en utilisant l'image minimaliste présente en ROM (anciens routeurs)
0x---2 à 0x---F	Demander d'utiliser les commandes <b>boot system</b> présentes dans la configuration de sauvegarde. Si aucune commande <b>boot system</b> ne permet d'atteindre une image IOS valide, le routeur tentera de démarrer avec la première image disponible en Flash.

Les 12 autres bits du registre de configuration ont une signification qui ne sera pas étudiée dans ce cours. Il faudra par conséquent toujours garder la valeur par défaut sauf si l'on en connaît l'effet.

Les commandes liées au registre de configuration sont :

- **config-register {valeur}**
  - Mode de configuration globale
  - Permet de modifier la valeur du registre de configuration
  - Le paramètre **valeur** est exprimé en hexadécimal (préfixe 0x).
  - Toute modification de la valeur est prise en compte lors du redémarrage.
- **show version**
  - Affiche la valeur du registre de configuration

### 5.1.4. Mode SETUP

Le mode SETUP, aussi connu sous le nom de dialogue de configuration initiale ou interactive, constitue une des routines de la configuration initiale. L'objectif principal du mode SETUP est de créer rapidement une configuration minimale, à savoir de définir :

- Le nom d'hôte
- Le mot de passe du mode privilégié
- Le mot de passe des lignes VTY
- La configuration basique du protocole SNMP
- L'adresse IP pour une interface

Les options configurables via le mode SETUP peuvent varier en fonction de la version d'IOS utilisée.

Le mode SETUP peut être lancé manuellement grâce à la commande **setup** depuis le mode privilégié ou alors lancé automatiquement si la configuration de sauvegarde n'est pas chargée (car elle n'existe pas ou car elle a été ignorée).

Il se présente sous la forme d'un questionnaire interactif en mode texte, dans lequel il suffit de répondre aux questions posées par le système. Pour la plupart des questions, les réponses par défaut apparaissent entre crochets à la suite de la question. Il suffit d'appuyer sur la touche **Entrée** pour accepter ces valeurs par défaut. Si le système a déjà été configuré, les valeurs par défaut affichées sont celles de la configuration actuelle. Par contre, si on configure le système pour la première fois, il s'agit des valeurs par défaut définies en usine.

Si on ne souhaite plus continuer avec le mode SETUP, on a la possibilité d'utiliser la combinaison de touches **CTRL+C**. Ceci est utile lorsque l'on ne souhaite pas utiliser le mode SETUP pour la configuration basique, ou si l'on s'est trompé sur une réponse. Dans ce dernier cas, il suffit de relancer le mode SETUP pour reprendre le dialogue de configuration au début.

Lorsque l'on a terminé le questionnaire du mode SETUP, la configuration que l'on vient de créer est affichée. Le système nous demande alors si on veut utiliser cette configuration, et par conséquent la sauvegarder dans la NVRAM.

## 5.2. Gestion d'IOS

La gestion des images IOS n'est pas compliquée. Il suffit d'avoir quelques informations utiles, comme la convention de noms utilisée pour nommer les fichiers, ainsi que de connaître les procédures simples de mise à jour du système quelque soit la situation.

### 5.2.1. Informations générales

Avec l'arrivée des IOS 12.x, une interface unique est maintenant utilisée pour les différents systèmes de fichiers, et se nomme IFS (IOS File System). IFS permet d'accéder aux différents systèmes de fichiers avec une syntaxe uniformisée.

Cette syntaxe se présente sous la forme suivante : **{préfixe}:[répertoire(s)]/{nom du fichier}**

Les préfixes peuvent être :

Préfixe	Signification
flash	Mémoire Flash du routeur
nvr	Mémoire NVRAM du routeur
system	Mémoire RAM du routeur
ftp	Serveur réseau utilisant le protocole FTP
tftp	Serveur réseau utilisant le protocole TFTP

Il existe beaucoup d'autres préfixes qui ne seront pas étudiés dans ce cours.

Il n'existe pas un, mais une multitude de versions d'IOS. C'est pourquoi une convention de noms est définie afin de fournir toutes les informations sur l'image concernée.

Cette convention de noms est la suivante : **{Plateforme}-{Feature Set}-{Format}.{Version}.bin**

- **Plateforme** est le matériel, aussi appelée plateforme, sur lequel l'image est prévue pour fonctionner (exemple : **c2600** pour un routeur de la gamme Cisco 2600).
- **Feature Set** correspond à l'ensemble des fonctionnalités incluses dans l'image (exemple : **js** pour une image de type "Entreprise Plus" et **k9** pour un niveau d'encryption).
- **Format** permet de connaître le format de conditionnement de l'image (exemple : **mz** pour une image compressée).
- **Version** est le numéro de version de l'image IOS (exemple : 123-9 pour un IOS version "12.3(9)").

### 5.2.2. Gestion des systèmes de fichiers

La gestion des systèmes de fichiers, et plus particulièrement les images IOS ainsi que les fichiers de configuration, passe par l'utilisation de la commande **copy {source} {destination}**.

La source et la destination peuvent être simplement des mots clés (tftp, running-config, startup-config) ou peuvent être exprimées en utilisant la syntaxe uniformisée d'IFS. On peut regrouper l'utilisation de la commande copy en 2 catégories :

- **Import**
  - Source externe (FTP, TFTP) vers une destination interne au routeur (Flash, NVRAM, RAM)
  - Utilisé pour la mise à jour du système
- **Export**
  - Source interne vers une destination externe
  - Utilisé pour la sauvegarde des données

Au travers de cette commande **copy**, on peut donc effectuer une opération importante, à savoir la mise à jour de l'image IOS. Pour cette opération, il faut prendre quelques précautions préliminaires. Il faut donc procéder ainsi :

- Etape n°1 : Vérifier que l'on dispose de suffisamment de mémoire Flash pour la nouvelle image IOS
- Etape n°2 : Sauvegarder l'image IOS actuelle sur un serveur TFTP ou FTP
- Etape n°3 : Lancer la mise à jour à l'aide de la commande **copy**
- Etape n°4 : Le système effectue une vérification de la validité de l'image IOS (checksum)

### 5.2.3. Mode RXBoot

Le mode RXBoot, aussi connu sous le nom de ROMmon, peut être utilisé pour l'une des deux raisons suivantes :

- Procédure de récupération des mots de passe
- Récupération du système après un problème d'image IOS

Pour accéder au mode RXBoot, il faut utiliser la combinaison de touches **CTRL+Pause** pendant les 60 secondes suivants le redémarrage du routeur. Le mode RXBoot est reconnaissable de part l'invite de commande affichée (exemple : **Rommon 1>** sur un routeur Cisco 2600).

Les commandes utilisées dans le mode RXBoot sont les suivantes :

- **confreg [valeur]**
  - Sans paramètre, cela permet d'afficher/modifier les paramètres de la ligne console (vitesse, etc.).
  - Avec paramètre, **valeur** correspond à la valeur hexadécimale du registre de configuration à attribuer. Ceci est utile lors de la récupération des mots de passe.
- **xmodem -c {nom fichier}**
  - Lance la demande de chargement d'une image IOS au travers de la ligne console
- **dir {système de fichier}**
  - Affiche le contenu d'un système de fichiers
- **boot [{préfixe}:{fichier}]**
  - Démarre le routeur en utilisant une image IOS précise (syntaxe uniformisée d'IFS)
- **set**
  - Permet de visualiser les valeurs des variables d'environnement
- **IP\_ADDRESS={IP}**
  - Variable d'environnement spécifiant l'adresse IP du routeur
- **IP\_SUBNET\_MASK={SM}**
  - Variable d'environnement spécifiant le masque de sous-réseau du routeur
- **DEFAULT\_GATEWAY={IP}**
  - Variable d'environnement spécifiant l'adresse IP de la passerelle par défaut pour le routeur
- **TFTP\_SERVER={IP}**
  - Variable d'environnement spécifiant l'adresse IP du serveur TFTP à utiliser
- **TFTP\_FILE={{répertoire}/{nom fichier}}**
  - Variable d'environnement spécifiant l'emplacement de l'image IOS sur ce serveur TFTP
- **tftpdnld**
  - Lance le téléchargement de l'image IOS en utilisant les valeurs des variables d'environnement
- **reset**
  - Redémarre le routeur
- **i**
  - Quitte le mode RXBoot et continue la séquence d'amorçage du routeur

Les commandes ci-dessus peuvent varier en fonction de la plateforme utilisée. Elles correspondent au mode RXBoot des dernières plateformes Cisco et ne fonctionnent pas sur les anciennes (tel que les routeurs Cisco 2500).

Il est plausible qu'un problème survienne avec IOS. Ceci peut aller de l'utilisation d'une image non prévue pour la plateforme à l'utilisation d'une image n'ayant pas assez de mémoire RAM pour se lancer, en passant par de bien nombreuses autres possibilités.

Dans ce genre de situations, le seul recours est le mode RXBoot. Pour la récupération d'une image IOS, on peut procéder de 2 manières différentes :

- Méthode Xmodem
- Méthode tftpdnld

La première méthode (Xmodem) est utilisée lorsque le routeur n'est branché qu'à un ordinateur via son port console (il faut posséder l'image IOS sur l'ordinateur relié au routeur par le câble console) :

- Etape n°1 : Modifier les paramètres de la ligne console avec la commande **confreg** (vitesse par défaut de 56000 bauds à changer en 115200 bauds)
- Etape n°2 : Redémarrer le routeur avec la commande **reset** puis entrer de nouveau dans le mode RXBoot
- Etape n°3 : Lancer la demande de téléchargement avec la commande **xmodem -c {nom fichier}**
- Etape n°4 : Lancer le téléchargement de l'image grâce au protocole Xmodem depuis le logiciel d'émulation de terminaux
- Etape n°5 : Une fois le téléchargement terminé, effectuer un redémarrage du routeur

La deuxième méthode (tftpdnld) est utilisée lorsqu'un serveur TFTP est disponible sur le réseau :

- Etape n°1 : Configurer toutes les variables d'environnement
- Etape n°2 : Vérifier les variables d'environnement avec la commande **set**
- Etape n°3 : Lancer le téléchargement de l'image IOS avec la commande **tftpdnld**
- Etape n°4 : relancer la séquence d'amorçage du routeur avec la commande **i** ou **reset**



## **6. Routage**

---

### **6.1. Principes fondamentaux**

#### **6.1.1. Fonctions de routage et de commutation**

La couche réseau fournit un acheminement de bout en bout et au mieux des paquets à travers les réseaux interconnectés. Ceci est effectué par 2 fonctions distinctes :

- **Fonction de routage**
- **Fonction de commutation**

La fonction de routage utilise la table de routage du protocole routé utilisé par le paquet à faire transiter pour déterminer le meilleur chemin à emprunter pour atteindre le réseau de destination. La métrique est utilisée pour offrir une mesure de qualité pour les chemins.

La fonction de commutation permet à un routeur d'accepter un paquet d'une file d'attente d'entrée et de le transmettre à une file d'attente de sortie.

Le but de ces deux fonctions est donc complètement différent et entièrement complémentaire.

Il existe plusieurs méthodes permettant d'optimiser la relation entre les fonctions de routage et de commutation. Ces méthodes permettent l'accélération de la transmission des paquets au travers d'un routeur en mettant en mémoire cache les décisions de routage déjà prises. Il existe les méthodes suivantes :

- Fast Switching
- Silicon Switching
- Autonomous Switching
- CEF (Cisco Express Forwarding)

Par défaut, un routeur Cisco utilise le Fast Switching, qui permet de mettre en mémoire cache les décisions de routage pour chaque destination. Pour cela, la première décision est effectuée normalement, en passant successivement par les fonctions de routage et de commutation. A ce moment là, on place en mémoire cache la décision de routage (l'interface de sortie) ainsi que l'en-tête de trame qui fut généré pour la trame de sortie.

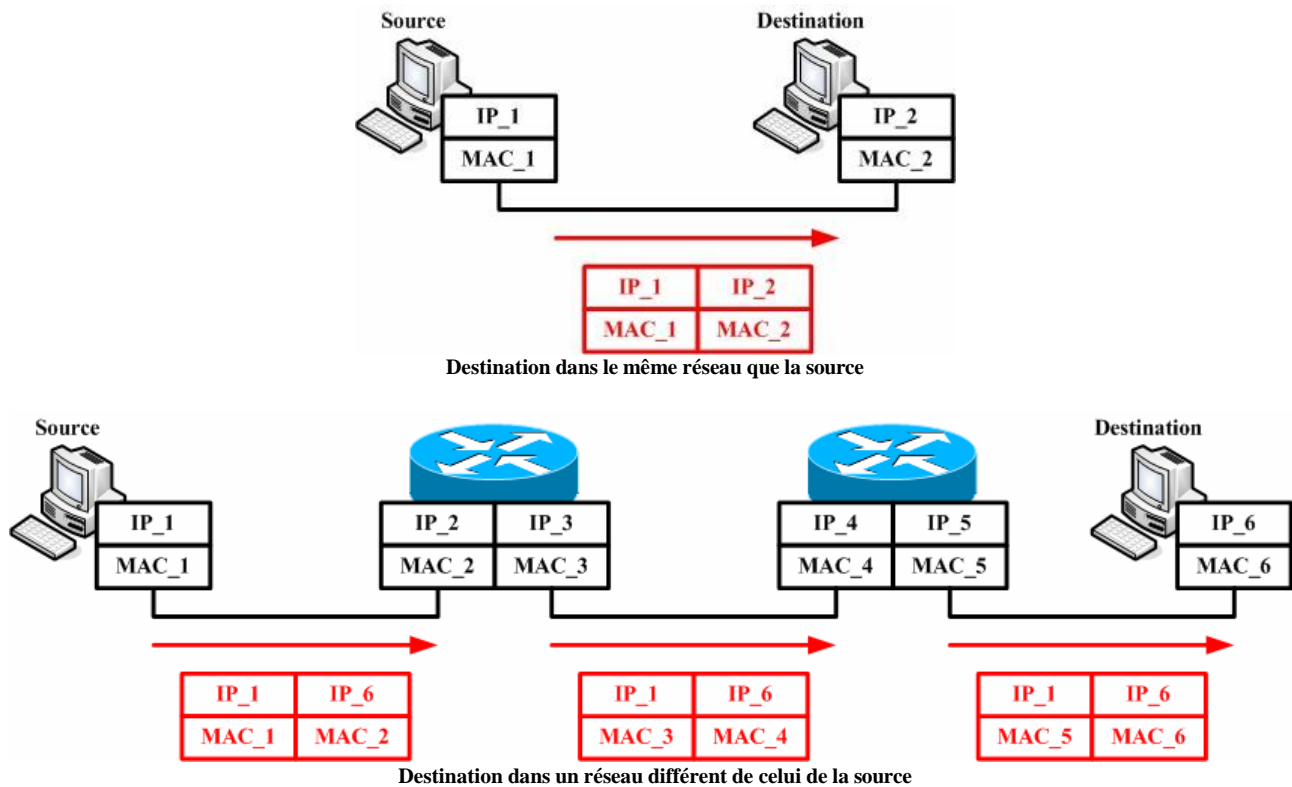
Les paquets suivants pour cette même destination se verront alors automatiquement traités de la même manière que le premier, en utilisant la même interface de sortie ainsi que le même en-tête de trame. Cela permet donc d'économiser le temps de parcours de la table de routage ainsi que le temps de création de l'en-tête pour la nouvelle trame.

La commande suivante peut être utilisée :

- **[no] ip route-cache**
  - Mode de configuration d'interface
  - Active/désactive le Fast Switching sur l'interface courante
  - Actif par défaut

Sauf exceptions, ces méthodes ont un inconvénient majeur, à savoir que seule la première décision de routage est mise en mémoire cache. Cela signifie que le partage de charge entre plusieurs liens pour une même destination devient impossible. Il faut donc choisir entre rapidité de transmission par le routeur et répartition de charge.

### 6.1.2. Processus de transmission



Le processus de transmission des paquets se déroule comme suit :

- L'hôte source détermine si la destination est locale (même réseau ou sous-réseau) ou distante grâce au couple IP/masque de sous-réseau. Elle calcule ainsi l'IP de sous-réseau de la destination ainsi que la sienne.
- Si les IP de sous-réseau sont les mêmes, alors la source émet la trame avec l'adresse de couche 2 de la destination. L'émission est ainsi directe.
- Par contre, si les IP de sous-réseau sont différentes, alors la source encapsule la trame avec l'adresse de couche 2 de sa passerelle par défaut puis l'envoie.
- La passerelle par défaut, à savoir généralement un routeur, reçoit cette trame. Ce routeur va déterminer le chemin à emprunter afin d'atteindre le réseau de destination. Ceci se fait grâce aux informations de couche 3 fournies par le paquet ainsi que par l'analyse d'une table de routage.

Il se pose ensuite deux cas :

- Le routeur actuel est le routeur final, c'est-à-dire qu'il est directement connecté au réseau de destination. Dans ce cas précis, on place les adresses de couche 2 de l'interface du routeur comme adresse source, et celle de la destination dans le champ adresse de destination. La trame est alors envoyée sur le réseau de destination.
- Le routeur actuel est un routeur intermédiaire sur le chemin, c'est-à-dire qu'il va falloir passer obligatoirement par un autre routeur afin d'atteindre le réseau de destination. La trame va donc être encapsulée avec l'adresse de couche 2 de l'interface de ce routeur, et celle du prochain saut dans le champ adresse de destination.

### 6.1.3. Table(s) de routage

La table de routage est l'élément central d'un routeur. C'est cette table qui est utilisée par la fonction de routage pour déterminer le meilleur chemin pour chaque destination connue du routeur.

Il existe une seule table de routage par protocole routé, sachant que cette table de routage peut être complétée manuellement (routage statique) ou dynamiquement (protocoles de routage).

Une table de routage possède les champs suivants :

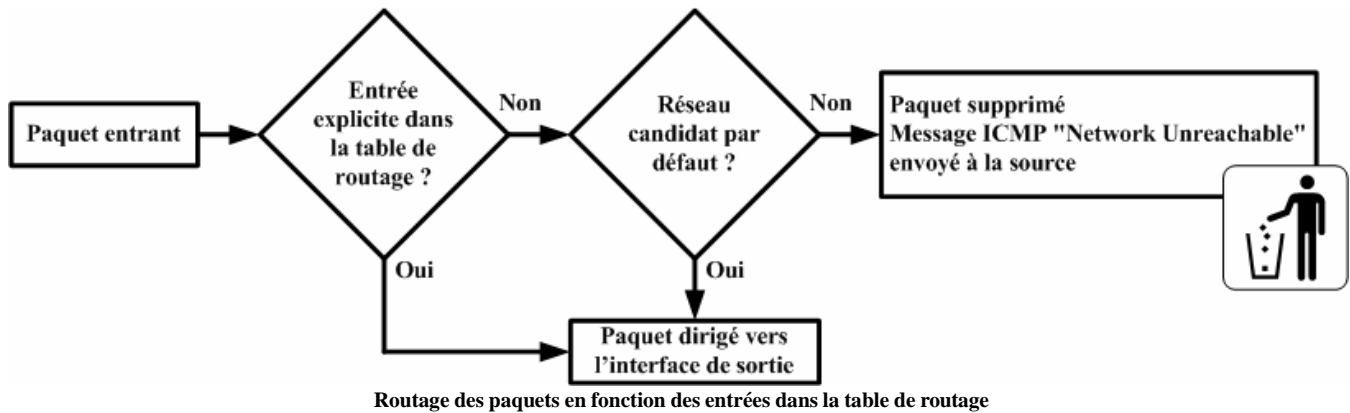
- **Destination**
  - Jusqu'à 6 ou 16 (IOS >= 12.3(2)T) routes différentes pour une même destination peuvent exister dans la table de routage. Ceci permet la répartition de charge sur plusieurs liens (Round Robin).
  - Ces entrées doivent obligatoirement avoir un prochain saut différent.
  - Il ne peut exister qu'une seule entrée dans la table de routage pour une même destination passant par un même prochain saut.
- **Interface de sortie**
  - Interface locale du routeur vers laquelle le paquet sortira
- **Prochain saut**
  - Adresse de couche 3 du prochain routeur sur le chemin pour atteindre le réseau de destination
- **Métrique**
  - Il s'agit d'une valeur numérique, utilisée par les protocoles de routage, qui permet la sélection du meilleur chemin et qui est basée sur des critères propres à chaque protocole de routage.
  - La métrique d'une route pour un réseau directement connecté est égale à 0.
  - Plus la métrique est petite, meilleure est la route.
- **Distance administrative**
  - Cette valeur numérique permet d'indiquer un ordre de préférence entre les différents protocoles lorsque plusieurs d'entre eux concourent pour une même entrée dans la table de routage. En effet, il est presque impossible de comparer objectivement les informations fournies par différents protocoles de routage en utilisant leurs métriques calculées avec des critères différents.
  - Plus la distance administrative est petite, plus le protocole est considéré comme prioritaire.
  - Les différentes valeurs à connaître sont :

Protocole	Distance administrative
Directement connecté	0
Statique	1
RIP	120
IGRP	100

- **Moyen d'apprentissage**
  - Ce champ explicite la méthode d'apprentissage pour chaque entrée dans la table de routage, en nous précisant le protocole de routage qui nous a informé de cette entrée :

Code	Protocole
C	Directement connecté
S	Statique
R	RIP
I	IGRP
*	Candidat par défaut

Un réseau candidat par défaut (aussi appelé route par défaut) est une entrée de table de routage qui dirige les paquets vers un saut suivant défini, lorsqu'il n'y a pas d'entrée explicite pour le réseau de destination. Ce type de route est utilisé par exemple pour rediriger les paquets d'un réseau LAN vers Internet.



Tout paquet qu'un routeur reçoit n'ayant pas d'entrée explicite ou implicite (réseau candidat par défaut) dans la table de routage est détruit. Le message ICMP "Network Unreachable" est alors envoyé par le routeur à la station source du paquet.

La décision prise par la fonction de routage est basée sur le principe de la correspondance la plus longue. Ceci signifie que si plusieurs entrées existent dans la table de routage, la plus précise correspondant à la destination sera choisie.

## 6.2. Routage statique et dynamique

### 6.2.1. Caractéristiques et comparatif

Il existe deux types de routage :

- **Statique** : Tout est géré manuellement par un administrateur réseau qui enregistre toutes les informations dans la configuration d'un routeur. Il doit mettre à jour manuellement les entrées de route statique chaque fois qu'une modification de la topologie le nécessite.
- **Dynamique** : Une fois qu'un administrateur réseau a entré les commandes de configuration pour lancer le routage dynamique, les informations relatives aux routes sont mises à jour automatiquement, par un processus de routage.

Le routage statique offre plusieurs applications utiles :

- Le routage dynamique a tendance à révéler toutes les informations connues d'un réseau, alors que vous souhaiteriez masquer certaines informations pour des raisons de sécurité. Le routage statique vous permet de spécifier les informations que vous souhaitez révéler à propos de réseaux restreints.
- Lorsqu'un réseau n'est accessible que par un seul chemin, une route statique vers ce réseau peut s'avérer suffisante. Ce type de réseau est appelé **réseau d'extrémité**. La configuration d'une route statique vers un réseau d'extrémité permet d'éviter la surcharge liée au routage dynamique.
- Il évite d'avoir une perte en bande passante due aux mises à jour envoyées par les protocoles de routage.

Le routage dynamique possède comme avantage principal de s'adapter automatiquement aux modifications topologiques.

### 6.2.2. Caractéristiques des protocoles de routage

La mise en œuvre du routage dynamique dépend de deux fonctions de base :

- La gestion d'une table de routage
- La distribution opportune des informations aux autres routeurs sous la forme de mises à jour du routage

Le routage dynamique s'appuie sur un protocole de routage pour partager les informations entre les routeurs. Un protocole de routage définit les règles utilisées par un routeur pour communiquer avec les routeurs voisins. Par exemple, un protocole de routage définit les informations suivantes :

- Comment envoyer les mises à jour
- Les informations contenues dans ces mises à jour
- Le moment où les informations doivent être envoyées
- Comment localiser les destinataires des mises à jour

Les protocoles de routage peuvent être classés selon l'algorithme qu'ils utilisent :

- Vecteur de distance
- Etat de liens
- Hybride symétrique

Lorsqu'un algorithme de routage met à jour une table de routage, son principal objectif est de déterminer les meilleures informations à inclure dans cette table. Chaque algorithme de routage interprète à sa façon les meilleures informations.

Un protocole de routage peut calculer les métriques en fonction de critères tels que :

- **Bande passante** : Le débit d'une liaison, mesuré en bits par seconde
- **Délai** : Le temps requis pour acheminer un paquet, pour chaque liaison, de la source à la destination
- **Charge** : La quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison
- **Fiabilité** : Cette notion indique généralement le taux d'erreurs sur chaque liaison du réseau
- **Nombre de sauts** : Le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination
- **Tics** : L'intervalle de temps entre 2 trames pour une liaison de donnée précise (environ 55 millisecondes)
- **Coût** : Généralement basée sur une dépense monétaire attribuée à un lien par un administrateur réseau

## 6.3. Convergence, boucles de routage et solutions

### 6.3.1. Convergence

La convergence est le fait que tous les dispositifs réseau ont la même vue de la topologie réseau. Le temps de convergence est donc le temps pendant lequel les dispositifs réseaux n'ont pas la même vue du réseau.

Lorsque tous les routeurs d'un réseau utilisent les mêmes informations, le réseau est convergent. Une convergence rapide est recommandée pour un réseau, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces.

### 6.3.2. Boucles de routage

Des boucles de routage peuvent se produire si la convergence lente d'un réseau avec une nouvelle configuration entraîne des entrées de routage incohérentes. Les paquets tournent sans cesse sur une boucle bien que le réseau de destination soit en panne.

Pour tenter de contrer les boucles de routages, il existe :

- Métrique de mesure infinie (Finite State Metric)
- Split Horizon
- Route Poisoning
- Mises à jour déclanchées (Triggered Updates)
- Compteurs de retenue (Holddown Timers)

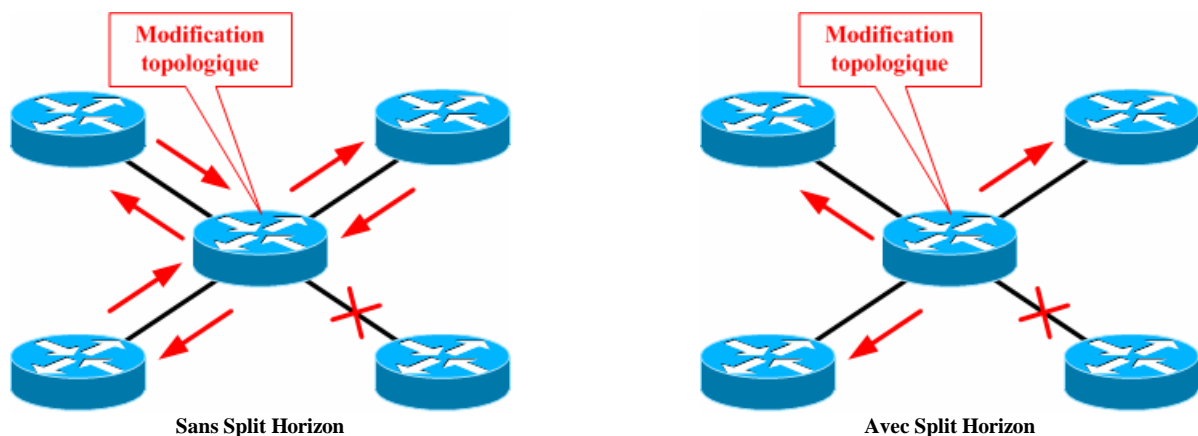
Ces cinq méthodes sont uniquement utilisées par les protocoles de routage à vecteur de distance, afin d'essayer de contrer les plausibles boucles de routage.

On ne se préoccupe que de la table de routage avec ces cinq solutions, car le problème des paquets en eux-mêmes est réglé automatiquement grâce au principe de TTL (Time To Live).

### 6.3.3. Métrique de mesure infinie

Une métrique de mesure infinie peut s'avérer nécessaire. Le principe est de définir l'infini en tant que nombre maximum spécifique. Ce nombre se réfère à une métrique de routage. Grâce à cette méthode, le protocole de routage permet à la boucle de routage d'exister jusqu'à ce que la métrique dépasse la valeur maximale autorisée. Le réseau en panne est considéré comme inaccessible lorsque la valeur métrique atteint la valeur maximale.

### 6.3.4. Split Horizon



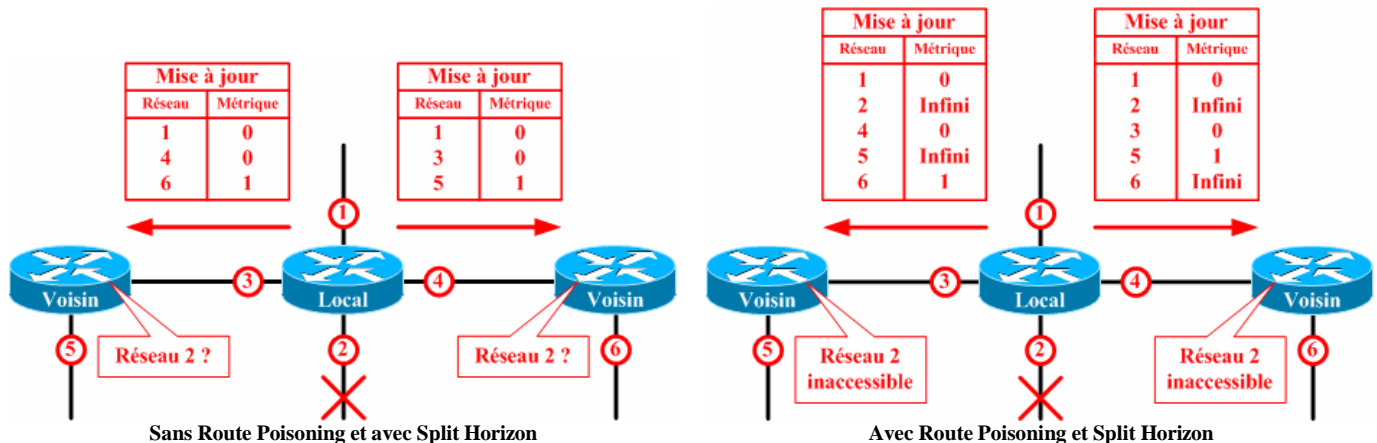
Le principe du Split Horizon est simple. Aucune information de mise à jour ne sera renvoyée par le chemin par lequel on a appris la modification de topologie. Ceci permet d'éviter de renvoyer à la source des informations erronées.

Ceci implique donc que l'information se propage toujours du plus près du réseau de destination au plus éloigné, sans jamais revenir en arrière.

### 6.3.5. Route Poisoning

Le Route Poisoning est utilisé lorsqu'un réseau devient inaccessible. Au lieu de n'avertir que les routes existantes dans la table de routage aux voisins, le Route Poisoning inclut aussi les routes devenues inaccessibles en leur octroyant une métrique infinie.

Ceci permet d'informer directement les voisins qu'un réseau est devenu inaccessible au lieu d'attendre l'expiration de leur compteur d'invalidité (Invalid Timer).



Combiné au Split Horizon, le Route Poisoning n'exclut pas les routes concernées par la règle du Split Horizon mais leur attribue une métrique infinie.

### 6.3.6. Mises à jour déclenchées

Les mises à jour déclenchées servent à informer les voisins d'une modification topologique au moment où elle survient. Cela permet de réduire le temps de convergence en n'attendant pas l'expiration de l'intervalle de temps de transmission des mises à jour périodiques.

### 6.3.7. Compteurs de retenue

On peut aussi utiliser des compteurs de retenue qui permettent d'éviter de changer l'état d'une entrée dans la table de routage impunément. Ils ont pour but de laisser le temps à l'information d'atteindre l'intégralité du réseau avant de modifier de nouveau la même entrée.

Ils fonctionnent de la façon suivante :

- Lorsqu'une modification est effectuée sur une entrée de la table de routage, on lance un compteur de retenue pour cette entrée.
- Si une mise à jour contenant une modification pour cette entrée a eu lieu alors que le temps du compteur de retenue est dépassé, alors la modification est appliquée.
- Si une mise à jour contenant une modification pour cette entrée pendant le temps du compteur de retenue, alors le protocole suivra les règles imposées par le principe des compteurs de retenue.

Les règles imposées par le principe des compteurs de retenue sont les suivantes :

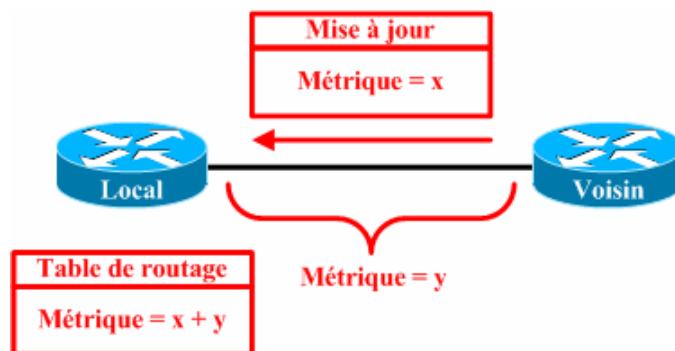
- On autorise l'activation ou l'amélioration de qualité (métrique) pour une entrée.
- On refuse la désactivation ou la dégradation de qualité pour l'entrée concernée.

Pour calculer le temps à utiliser pour la configuration des compteurs de retenue, il faut multiplier le plus petit nombre de sauts à effectuer pour atteindre le routeur le plus éloigné par l'intervalle de temps entre les mises à jour.

### 6.4. Routage à vecteur de distance

L'algorithme de routage à vecteur de distance possède une vision de la topologie du réseau qui est basée sur celle de ses voisins. En effet, les mises à jour de routage envoyées par les protocoles de routage à vecteur de distance contiennent directement la table de routage du routeur émetteur. Le récepteur n'a donc pour seul travail que de récupérer ces informations, de garder les entrées pertinentes et de modifier les métriques.

La métrique locale pour une entrée dans la table de routage a pour valeur le résultat de l'addition entre la métrique incluse dans la mise à jour reçue par un voisin et de la valeur de la métrique vers ce voisin.



De plus, les mises à jour possèdent des caractéristiques précises :

- Elles sont envoyées périodiquement
- Elles contiennent directement toutes les entrées de la table de routage de l'émetteur (sauf les entrées supprimées par Split Horizon)
- Elles sont émises en broadcast (sauf exceptions telles qu'avec RIPv2 et EIGRP)

La sélection du meilleur chemin, qui sera inclus dans la table de routage, se fait en utilisant l'algorithme de Bellman Ford. Ce dernier se base sur le nombre de sauts pour calculer les métriques. Une exception existe pour les protocoles de routage à vecteur de distance propriétaires, tels que IGRP et EIGRP de Cisco.

Les protocoles de routage à vecteur de distance les plus connus sont :

- RIP
- Cisco IGRP
- Cisco EIGRP (vecteur de distance évolué, ou hybride symétrique)



## 6.5. Routage à état de liens

Cet algorithme exploite le principe du plus court chemin d'abord (Shortest Path First). Ce principe est basé sur l'utilisation :

- D'une table de données topologiques
- De l'algorithme de Dijkstra
- D'un arbre du plus court chemin d'abord (SPF Tree)

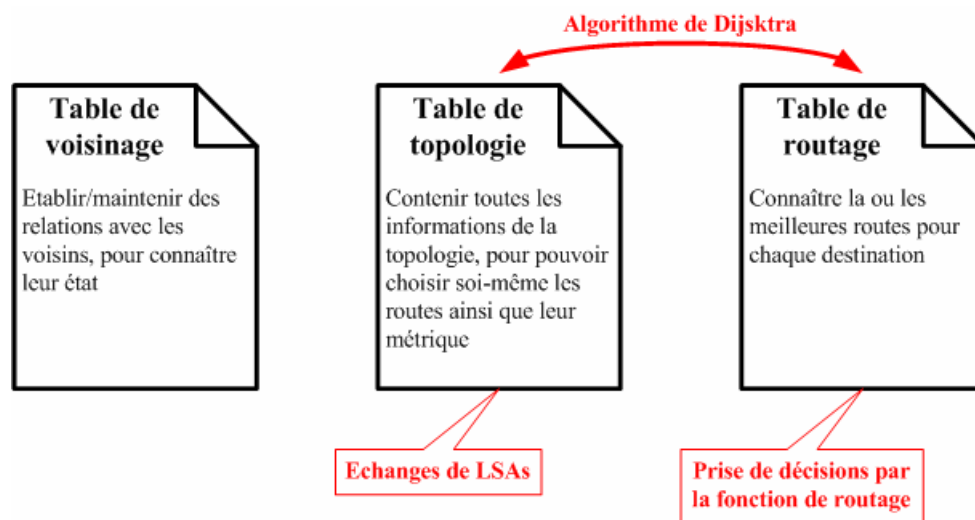
Les mises à jour de routage des protocoles à état des liens possèdent de grandes différences comparées à celles des protocoles à vecteur de distance :

- Elles sont uniquement envoyées lors de modifications topologiques (Triggered Updates).
- Elles contiennent des informations topologiques (Link State Advertisements).
- Elles sont incrémentielles.
- Elles sont émises en multicast sur des adresses spécifiques.

La propagation d'informations topologiques permet de ne pas baser ses décisions de routage sur une vision du réseau donnée par les voisins ainsi que d'être plus efficace au niveau de la pertinence de l'information. En effet, l'état d'un seul lien peut affecter plusieurs routes. Les ressources utilisées sont alors plus orientées processeur que bande passante sur le réseau.

Les protocoles de routage à état de liens développent des relations de voisinage avec les routeurs adjacents. Ces relations sont maintenues en permanence via l'émission réception de messages. L'intérêt principal est de connaître l'existence d'un voisin avec qui converser ainsi que son état et, par conséquent, l'état des routes passant par lui.

Le routage à état de liens se base donc sur l'utilisation de trois tables distinctes (au contraire des protocoles à vecteur de distance qui ne gèrent que la table de routage) :



Tables utilisées par un protocole de routage à état de liens

Le routage à état de liens est lié à deux exigences :

- **Ressource calculatoire** : Un protocole de routage à état de liens requière une puissance CPU importante pour l'algorithme du plus court chemin d'abord, afin de transformer sa base de données topologiques en un arbre du plus court chemin d'abord, puis pour traiter cet arbre pour en déduire la table de routage.
- **Ressource mémoire** : Une grande quantité de mémoire RAM est utilisée par un protocole de routage à état de liens car il faut stocker les tables de voisinage ainsi que de topologie en plus de la classique table de routage.

Les protocoles de routage à état de liens les plus connus sont :

- OSPF
- IS-IS

### 6.6. Systèmes autonomes, protocoles de routage intérieurs et extérieurs

Un système autonome (AS) est, par définition, l'ensemble des dispositifs interconnectés régis par la même administration. Cela permet de délimiter la responsabilité du routage à un ensemble défini.

Ces AS sont identifiés par un numéro qui est chiffré sur 16 bits. Ce numéro est unique dans le monde et permet d'identifier une organisation aux yeux du reste du monde informatique. Il est attribué par le NIC (Network Information Center).

Pour les protocoles de routage imposant l'indication d'un numéro d'AS et se trouvant dans un réseau privé, ce numéro de système autonome peut être choisi arbitrairement dans la plage de valeurs allant de 64512 à 65535.

Cette notion de système autonome crée donc une nouvelle distinction entre les protocoles de routage :

- **Protocoles de routage intérieurs (IGP)** : Protocoles ayant pour mission principale le routage à l'intérieur d'un système autonome
- **Protocoles de routage extérieurs (EGP)** : Protocoles permettant le routage entre les systèmes autonomes

Les protocoles de routage intérieurs voient un système autonome comme un seul et unique protocole de routage. De ce point de vue, si plusieurs protocoles de routage existent dans un même système autonome, chaque protocole considérera le protocole adjacent comme externe.

Les protocoles de routage sont donc classifiés ainsi :

Classification	Protocoles
IGP	RIP, IGRP, EIGRP, OSPF et IS-IS
EGP	EGP et BGP

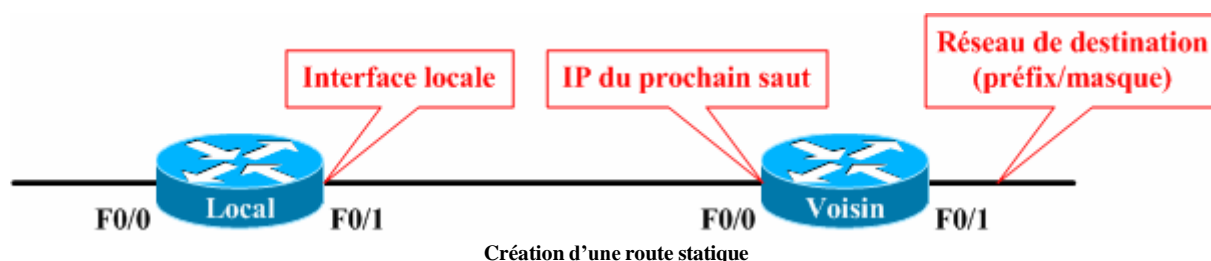
Typiquement, la convergence d'un réseau est restreinte au système autonome. Le temps de convergence dépend donc du protocole utilisé dans le système autonome.

### 6.7. Configuration par défaut, routage statique et visualisation d'état

Par défaut, seul le routage pour le protocole IP est activé sur un routeur Cisco. Le routage s'effectue automatiquement entre les réseaux directement connectés au routeur, sans avoir à utiliser des routes statiques ou un protocole de routage quelconque.

Les commandes permettant de configuration le routage de base sont les suivantes :

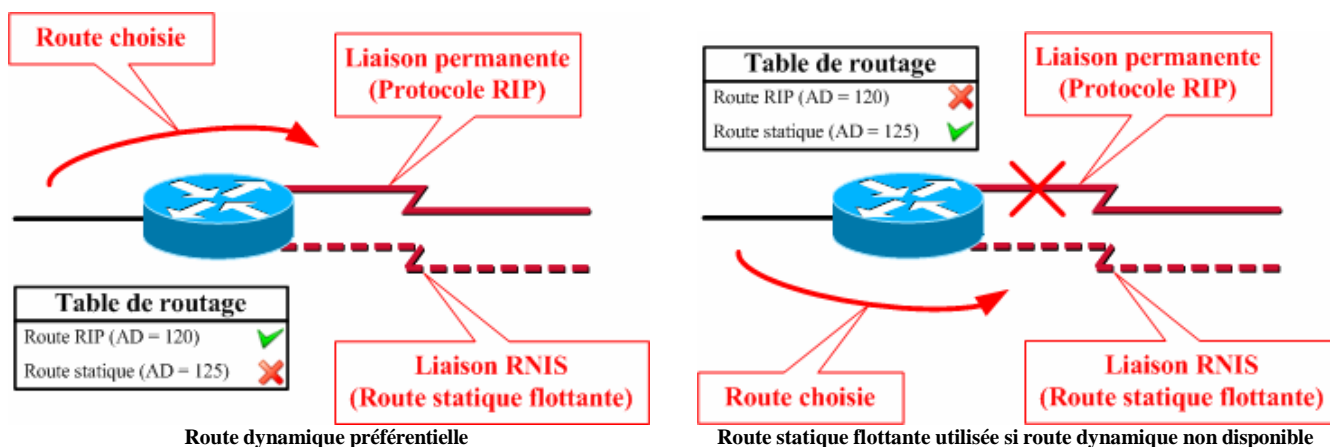
- **{protocole} routing**
  - Mode de configuration globale
  - Permet d'activer/désactiver le routage pour un protocole routé particulier
  - Le paramètre **protocole** correspond au mot clé du protocole voulu (IP, IPX, IPv6, etc.).
- **ip classless**
  - Mode de configuration globale
  - Active le routage Classless sur le routeur
  - Actif par défaut
  - Permet l'utilisation d'information de routage Classless, telles que les routes par défaut
- **ip route {préfixe} {masque} {prochain saut | interface} [distance administrative]**
  - Mode de configuration globale
  - Crée une route statique sur le routeur
  - La distance administrative permet la création d'une route statique flottante (valeur par défaut = 1).



Il est possible de créer une route statique par défaut. Pour cela, il suffit d'utiliser le pseudo réseau ayant pour préfixe 0.0.0.0 et pour masque de sous-réseau 0.0.0.0. Cette route statique sera considérée par le routeur comme un réseau candidat par défaut dans la table de routage.

Les routes statiques sont prioritaires à n'importe quel protocole de routage, à cause de la distance administrative par défaut. Cette distance peut être modifiée afin de rendre une route statique moins préférable à une entrée fournie par un protocole de routage. Pour cela, il faut expliciter pour la route statique une distance administrative plus grande que celle du protocole de routage.

On crée ainsi une route statique flottante, qui est une route alternative à une autre en cas de défaillance de la première. Une route statique flottante doit être pour la même destination qu'une entrée fournie par un protocole de routage.



Cette route statique flottante n'apparaît dans la table de routage que lorsque l'entrée fournie par le protocole de routage n'est plus valide.

Les commandes utilisées pour la visualisation d'état sont :

- **show ip protocols** : Affiche la liste des protocoles de routage configurés sur le routeur ainsi que les informations générales les concernant (interfaces participant à chaque processus de routage, réseaux avertis, compteurs, etc.)
- **show ip route** : Affiche la table de routage IP
- **clear ip route [{préfixe} | \*]** : Supprime une ou plusieurs routes de la table de routage

## 7. Protocole RIP

### 7.1. Théorie

RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance. Il existe en deux versions :

- **RIPv1** (RFC 1058) : Première version du protocole RIP
- **RIPv2** (RFC 1723) : Evolution permettant le routage Classless (en transmettant les masques de sous-réseaux en plus des préfixes dans les mises à jour) et la transmission des mises à jour en multicast

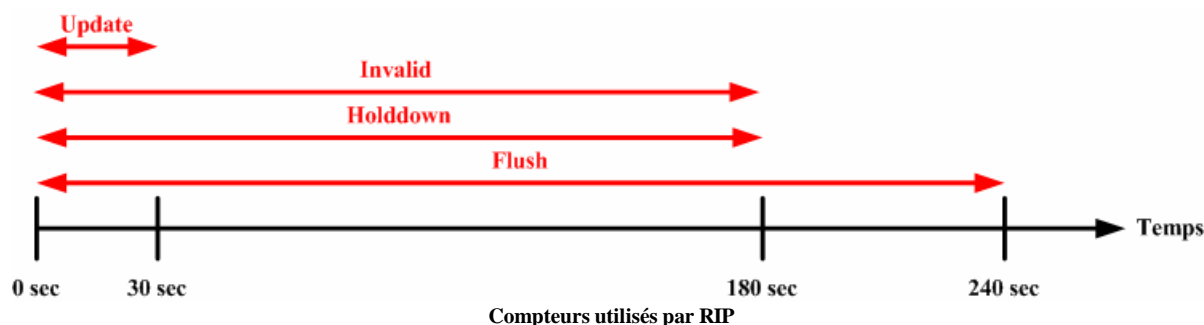
RIPv1	RIPv2
Classful	Classless
Broadcast pour les mises à jour	Multicast (224.0.0.9) pour les mises à jour
Préfixes dans les mises à jour	Préfixes et masques de sous-réseau dans les mises à jour
	Support du VLSM
	Authentification des voisins

Les caractéristiques principales de RIP sont :

- Nombre de sauts (hop count) utilisé pour le calcul des métriques
- Métrique maximale = 15 (métrique de mesure infinie = 16)
- Mises à jour périodiques toutes les 30 secondes

Avantages	Inconvénients
Processus léger	Temps de convergence lent
Implémenté sur tous les systèmes d'exploitation	Nombre de sauts pour calculer les métriques
	Nombre de sauts limité à 15

RIP n'a pas de notion de système autonome. Ceci signifie qu'il ne connaît rien d'autre que lui-même. Le seul moyen de pouvoir sortir du système autonome RIP est par conséquent une route statique par défaut.



En tant que protocole de routage à vecteur de distance, RIP utilise quatre compteurs :

- **Update** : Intervalle de temps entre les mises à jour périodiques (30 secondes par défaut)
- **Invalid** : Intervalle de temps après réception de la dernière mise à jour pour chaque entrée dans la table de routage avant de la considérer comme périmée. Après ce temps, l'entrée concernée ne sera plus analysée lors du parcours de la table de routage (180 secondes par défaut)
- **Holddown** : Intervalle de temps après réception de la dernière mise à jour avant d'autoriser le remplacement de cette route par une autre moins bonne (180 secondes par défaut)
- **Flush** : Intervalle de temps après réception de la dernière mise à jour pour chaque entrée dans la table de routage avant de la supprimer de la table de routage (240 secondes par défaut)

L'implémentation Cisco de RIP supporte les mises à jour déclanchées.

Les caractéristiques de RIP en font le protocole de prédilection pour les réseaux LANs homogènes de petite taille.

## 7.2. Configuration

### 7.2.1. Commandes

Les commandes liées à la configuration du protocole RIP sont :

- **router rip**
  - Mode de configuration globale
  - Active le protocole RIP
  - Passe dans le mode de configuration du routeur
- **network {préfixe}**
  - Mode de configuration du routeur
  - Spécifie le réseau qui sera inclut dans les mises à jour de routage
  - Détermine les interfaces appartenant à ce réseau qui participent au processus de routage
  - Le **préfixe** doit être un réseau directement connecté au routeur.
- **neighbor {IP}**
  - Mode de configuration du routeur
  - Définit l'adresse IP d'un voisin avec lequel RIP échangera des mises à jour de routage
  - Par défaut, aucun voisin n'est définit.
- **passive-interface {type} {numéro}**
  - Mode de configuration du routeur
  - Empêche l'interface indiquée d'envoyer des mises à jour
- **[no] ip split-horizon**
  - Mode de configuration d'interface
  - Active/désactive Split Horizon sur l'interface courante
- **timers basic {update} {invalid} {holddown} {flush}**
  - Mode de configuration du routeur
  - Définit les intervalles de temps, en secondes, utilisés par RIP
- **version {1 | 2}**
  - Mode de configuration du routeur
  - Indique la version de RIP utilisée par le routeur
  - Ceci modifie automatiquement le type (RIPv1 ou RIPv2) de mises à jour envoyées et reçues
  - Par défaut, les mises à jour sont de type RIPv1
- **ip rip {send | receive} version {1 | 2 | 1 2}**
  - Mode de configuration d'interface
  - Spécifie précisément le type (RIPv1 et/ou RIPv2) de mises à jour envoyées ou reçues
- **default-information originate**
  - Mode de configuration du routeur
  - Propage le réseau candidat par défaut aux autres routeurs RIP du système autonome

- **maximum-paths {nombre}**
  - Mode de configuration du routeur
  - Spécifie le nombre maximum de liens ayant la même métrique pouvant être utilisés pour la répartition de charge
  - Par défaut à 4 et maximum à 6 ou 16 (IOS >= 12.3(2)T)
- **redistribute static**
  - Mode de configuration du routeur
  - Injecte les routes statiques locales et les propagent dans les mises à jour RIP
- **rip equal-cost {nombre}**
  - Mode de configuration globale
  - Indique le nombre d'entrées ayant la même métrique pouvant être insérées dans la table de routage
  - De 1 à 15 et par défaut à 1

### 7.2.2. Procédure de configuration

Pour configurer un routeur en utilisant le protocole de routage RIP, il faut procéder comme suit :

- **Etape n°1** : Activer le protocole RIP (commande **router rip**)
- **Etape n°2** : Spécifier les réseaux directement connectés devant participer au processus de routage (commande **network**)
- **Etape n°3 (optionnelle)** : Désactiver l'émission de mises à jour de routage vers les réseaux n'ayant pas de routeur(s) RIP autre(s) que le routeur local (commande **passive-interface**)
- **Etape n°4 (optionnelle)** : Ajuster les différents compteurs de temps (commande **timers basic**)
- **Etape n°5 (optionnelle)** : Choisir la version de RIP à utiliser (commande **version**)
- **Etape n°6 (optionnelle)** : Propager la route par défaut existante sur le routeur local aux autres routeurs RIP du système autonome (commande **default-information originate**)
- **Etape n°7 (optionnelles)** : Activer la répartition de charge entre plusieurs liens de même métrique (commande **maximum-paths**)

Il ne peut y avoir qu'une seule et unique instance du protocole RIP par routeur.

## 7.3. Vérification

IOS fournit une panoplie de commandes permettant de visualiser l'état du protocole RIP ainsi que d'effectuer du débogage. Ces commandes sont les suivantes :

- **show ip protocols** : Affiche les compteurs RIP, les interfaces participant au processus de routage, les réseaux avertis ainsi que la version pour les mises à jour envoyées et reçues
- **show ip rip database** : Affiche la FIB (Forward Information Base) de RIP
- **debug ip rip [events]** : Affiche en temps réel les mises à jour RIP envoyées et reçues

## 8. Protocole IGRP

### 8.1. Théorie

IGRP (Interior Gateway Routing Protocol) est un protocole de routage à vecteur de distance propriétaire Cisco. Il a été conçu au milieu des années 1980 pour remplacer RIP. En effet, des incohérences de routage peuvent survenir avec RIP sur des réseaux hétérogènes.

IGRP est donc capable de fonctionner sur des réseaux hétérogènes de très grande taille, tout en proposant un calcul des métriques basé sur les critères suivants :

- Bande passante
- Délai
- Fiabilité
- Charge

Les métriques IGRP sont des nombres sur 24 bits (de 0 à 16 777 215) calculés à l'aide de cette formule :

$$\text{Métrique} = (\mathbf{K1} \times \mathbf{Bandwidth} + \mathbf{K2} \times \mathbf{Bandwidth} \div (\mathbf{256} - \mathbf{Load}) + \mathbf{K3} \times \mathbf{Delay}) + \mathbf{K5} \div (\mathbf{Reliability} + \mathbf{K4})$$

Les différents paramètres de cette formule sont les suivants :

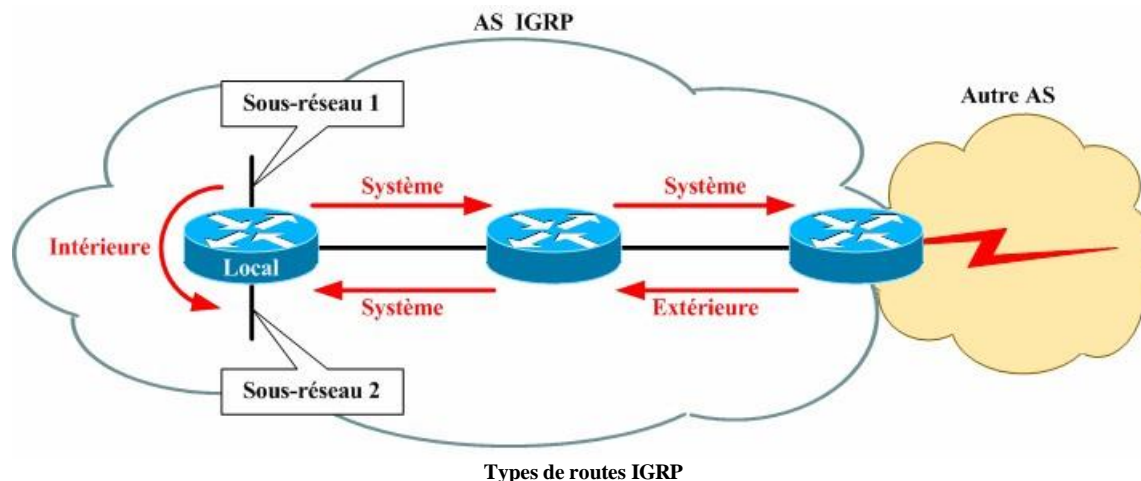
- **K1** : Coefficient rattaché à la bande passante (valeur par défaut = 1)
- **K2** : Coefficient rattaché à la charge (valeur par défaut = 0)
- **K3** : Coefficient rattaché au délai (valeur par défaut = 1)
- **K4** : Coefficient rattaché à la fiabilité (valeur par défaut = 0)
- **K5** : Coefficient rattaché au MTU (valeur par défaut = 0)
- **Bandwidth** : Valeur correspondant à la plus petite bande passante de liaison entre les hôtes source et destination. Cette valeur est calculée avec la formule  $10^7 \div \mathbf{BP}$ , avec BP la bande passante exprimée en Kbps.
- **Load** : Charge sur la liaison. C'est un pourcentage binaire dont la valeur peut aller de 0 à 255.
- **Delay** : Délai de transmission sur le chemin exprimé en microsecondes ( $\mu\text{s}$ ). C'est la somme des délais de toutes les liaisons entre les hôtes source et destination. Cette valeur est calculée via la formule  $\Sigma_{\text{délais}}$ .
- **Reliability** : Fiabilité de la liaison. C'est aussi un pourcentage binaire dont la valeur peut aller de 0 à 255 et qui est déterminée par le ratio entre le nombre de paquets corrects et le nombre de paquets transmis sur le média.

Ainsi, avec les valeurs par défaut, on arrive à la formule simplifiée suivante :

$$\text{Métrique} = \mathbf{Bandwidth} + \mathbf{Delay}$$

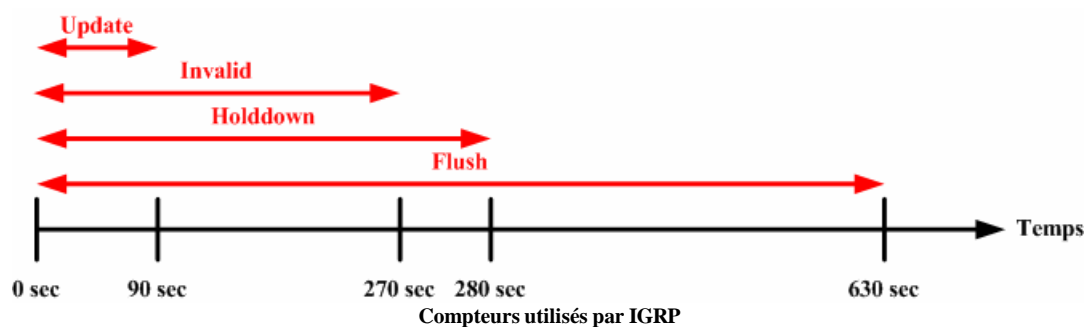
$$\text{Métrique} = (10^7 \div \mathbf{BP} + \Sigma_{\text{délais}})$$





Il peut y avoir jusqu'à 4 routes pour une même destination dans la table de routage. Ces routes peuvent être de 3 types :

- **Intérieure** : Route entre des sous-réseaux directement connectés au routeur local
- **Système** : Route interne au système autonome propagée par un routeur
- **Extérieure** : Route externe à l'AS qui a été redistribuée dans l'AS IGRP (inclus aussi les routes statiques redistribuées)



En tant que protocole de routage à vecteur de distance, IGRP utilise quatre compteurs :

- **Update** : Intervalle de temps entre les mises à jour périodiques (90 secondes par défaut)
- **Invalid** : Intervalle de temps après réception de la dernière mise à jour pour chaque entrée dans la table de routage avant de la considérer comme périmée. Après ce temps, l'entrée concernée ne sera plus analysée lors du parcours de la table de routage (270 secondes par défaut, ou 3 fois l'Update)
- **Holddown** : Intervalle de temps après réception de la dernière mise à jour avant d'autoriser le remplacement de cette route par une autre moins bonne (280 secondes par défaut)
- **Flush** : Intervalle de temps après réception de la dernière mise à jour pour chaque entrée dans la table de routage avant de la supprimer de la table de routage (630 secondes par défaut, ou 7 fois l'Update)

IGRP utilise aussi les mises à jour Poison Reverse. Ceci permet de placer des routes directement à l'état Holddown. Toute route dont la métrique augmentant d'un facteur de 1,1 fera l'objet d'une mise à jour Poison Reverse.

## 8.2. Configuration

### 8.2.1. Commandes

Les commandes pouvant être utilisées pour la configuration du protocole IGRP sont les suivantes :

- **router igrp {AS}**
  - Mode de configuration globale
  - Active le protocole de routage IGRP sur le routeur pour le système autonome indiqué en paramètre
  - Permet de passer dans le mode de configuration du routeur
- **network {préfixe}**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **neighbor {IP}**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **passive-interface {type} {numéro}**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **[no] ip split-horizon**
  - Mode de configuration d'interface
  - Idem qu'avec RIP
- **maximum-paths {nombre}**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **variance {valeur}**
  - Mode de configuration du routeur
  - Permet la répartition de charge entre des liens n'ayant pas la même métrique
  - **valeur** est un entier pouvant aller de 1 à 128 (défaut = 1)
  - La variance est un coefficient multiplicateur permettant de sélectionner les routes ayant des métriques identiques à la variance près pour faire de la répartition de charge pondérée (Weighted Round Robin).
- **metric weights {TOS} {K1} {K2} {K3} {K4} {K5}**
  - Mode de configuration du routeur
  - Spécifie les valeurs pour les coefficients utilisés pour le calcul des métriques.
  - **TOS** doit toujours être à 0.
- **timers basic {update} {invalid} {holddown} {flush}**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **metric maximum-hops {valeur}**
  - Mode de configuration du routeur
  - Indique le nombre maximum de sauts (diamètre du système autonome)
  - **valeur** peut aller de 1 à 255 (défaut = 100)

- **ip default-network {préfixe}**
  - Mode de configuration globale
  - Définit un réseau candidat par défaut à propager dans le système autonome
  - Le réseau indiqué doit être connu des routeurs IGRP et doit être directement connecté.
  - La route propagée sera vue par les autres routeurs IGRP comme une route externe
- **redistribute static**
  - Mode de configuration du routeur
  - Idem qu'avec RIP
- **bandwidth {BP}**
  - Mode de configuration d'interface
  - Définit la bande passante de la liaison
  - Cette valeur est utilisée par IGRP et EIGRP pour le calcul de leurs métriques.
  - Le paramètre BP est exprimé en Kbps

### 8.2.2. Procédure de configuration

Pour configurer un routeur en utilisant le protocole de routage IGRP, il faut procéder comme suis :

- **Etape n°1** : Activer le protocole de routage IGRP (commande **router igrp**)
- **Etape n°2** : Spécifier les réseaux directement connectés devant participer au processus de routage (commande **network**)
- **Etape n°3 (optionnelle)** : Désactiver l'émission de mises à jour de routage vers les réseaux n'ayant pas de routeur(s) IGRP autre(s) que le routeur local (commande **passive-interface**)
- **Etape n°4 (optionnelle)** : Ajuster les différents compteurs de temps (commande **timers basic**)
- **Etape n°5 (optionnelle)** : Propager la route par défaut existante sur le routeur local aux autres routeurs IGRP du système autonome (commande **ip default-network**)
- **Etape n°6 (optionnelle)** : Activer la répartition de charge entre plusieurs liens de même métrique (commandes **maximum-paths** et **variance**)

Il ne peut y avoir qu'une seule instance d'IGRP par numéro de système autonome. Il peut donc y avoir plusieurs instances d'IGRP sur un même routeur.

## 8.3. Vérification

Comme pour RIP, IOS fournit des commandes de visualisation d'état et de débogage pour IGRP :

- **show ip protocols** : Affiche les différentes instances d'IGRP, avec leur numéro d'AS, les compteurs, les coefficients utilisés pour le calcul des métriques, les réseaux avertis ainsi que les interfaces participant au processus de routage
- **debug ip igrp events** : Affiche en temps réel les événements d'IGRP
- **debug ip igrp transactions** : Affiche en temps réel les échanges d'IGRP

## 9. Protocole ICMP

### 9.1. Théorie

ICMP (Internet Control Message Protocol) est un protocole faisant partie de la pile de protocoles TCP/IP et fonctionne au niveau de la couche 3 du modèle OSI.

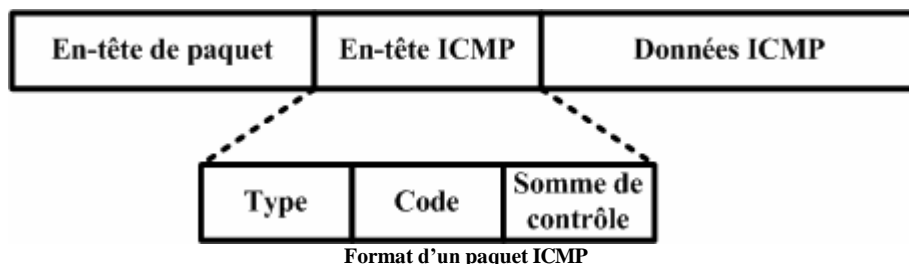
Les messages du protocole ICMP sont classifiés en deux catégories :

- Messages d'erreurs
- Messages de contrôle

Les messages d'erreurs sont présents pour informer les pairs communiquant d'une erreur de transmission, permettant ainsi de contrer la limitation du protocole IP. Ces messages d'erreurs ICMP sont eux-mêmes des paquets IP et sont donc aussi sujets aux erreurs de transmission. Afin d'éviter une boucle de messages d'erreurs, les erreurs survenant à des messages ICMP ne génèrent pas de messages d'erreur ICMP.

Les messages de contrôle servent à informer sur l'état du réseau (dispositif congestionné, meilleure passerelle par défaut existante, etc.).

Les messages ICMP sont encapsulés comme toute autre donnée dans un paquet :



## 9.2. Messages ICMP

### 9.2.1. Types de messages

Il existe plusieurs types de messages ICMP associés à un numéro de code précis :

Code	Message
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/Change Request
8	Echo Request
9	Router Discovery
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

### 9.2.2. Echo Request/Reply

Les messages d'Echo permettent de déterminer si un hôte est joignable ou pas. Ceci s'effectue en utilisant la commande ping qui envoie des messages ICMP Echo Request. L'hôte de destination recevant ces paquets renvoie à son tour des messages ICMP Echo Reply.

L'en-tête ICMP utilisé pour ces messages est le suivant :

8 bits	8 bits	16 bits	16 bits	16 bits	Variable
Type (0 ou 8)	Code (0)	Somme de contrôle	Identificateur	Numéro de séquence	Remplissage

En-tête ICMP Echo Request/Reply

Le numéro de séquence est utilisé pour distinguer les différentes requêtes effectuées.

### 9.2.3. Destination Unreachable

Le message ICMP Destination Unreachable est envoyé par un routeur lorsque ce dernier ne possède pas les informations suffisantes pour transmettre un paquet (typiquement une table de routage n'ayant pas d'entrée pour le réseau de destination).

L'en-tête ICMP utilisé pour les messages ICMP Destination Unreachable est :

8 bits	8 bits	16 bits	16 bits	
Type (3)	Code (de 0 à 12)	Somme de contrôle	Inutilisé (valeur = 0)	En-tête du paquet source + les 64 premiers bits

En-tête ICMP Destination Unreachable

Les différentes valeurs possibles pour le code permettent d'identifier la cause du problème :

Code	Signification
0	Réseau inaccessible
1	Hôte inaccessible
2	Protocole inaccessible
3	Port inaccessible
4	Fragmentation nécessaire mais refusée
5	Echec de la route source
6	Réseau de destination inconnu
7	Hôte de destination inconnu
8	Hôte source isolé
9	Communication avec le réseau de destination administrativement refusée
10	Communication avec l'hôte de destination administrativement refusée
11	Réseau inaccessible pour le ToS utilisé
12	Hôte inaccessible pour le ToS utilisé

### 9.2.4. Parameter Problem

Un message ICMP Parameter Problem est envoyé lorsqu'un paquet n'a pas pu être transmis à cause d'une erreur d'en-tête IP.

L'en-tête d'un message ICMP Parameter Problem est ainsi :

8 bits	8 bits	16 bits	8 bits	8 bits	
Type (12)	Code (de 0 à 2)	Somme de contrôle	Pointeur	Inutilisé (valeur = 0)	En-tête du paquet source + les 64 premiers bits

En-tête ICMP Parameter Problem

Le champ "Pointeur" permet d'indiquer l'octet de l'en-tête IP posant problème.

## 9.2.5. Source Quench

Le message ICMP Source Quench est envoyé par un dispositif réseau subissant une congestion réseau.

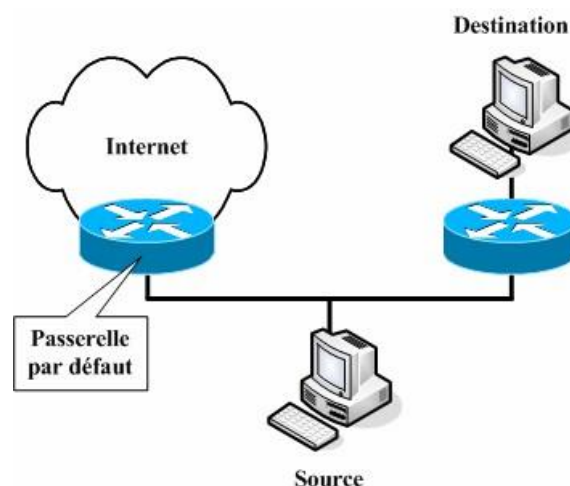
Ne pouvant pas traiter tous les paquets entrant en cas de congestion, il est obligé d'en supprimer. Les sources des paquets supprimés sont avertis par ce message ICMP.

## 9.2.6. Redirect/Change Request

Ce message ICMP permet la notification à la source qu'une meilleure route existe pour une destination précise.

Ce message est envoyé par une passerelle par défaut uniquement si les conditions suivantes sont remplies :

- Interface d'entrée = interface de sortie
- Réseau de la source = réseau du prochain saut
- Route dans la table de routage  $\neq$  route par défaut
- Paquet reçu n'est pas un ICMP Redirect
- Routeur configuré pour envoyer des messages ICMP Redirect



L'en-tête du message ICMP envoyé par la passerelle par défaut est le suivant :

8 bits	8 bits	16 bits	32 bits	
Type (5)	Code (de 0 à 3)	Somme de contrôle	IP d'un routeur	En-tête du paquet source + les 64 premiers bits

En-tête ICMP Redirect

Le champ "IP d'un routeur" fournit à la source l'adresse IP du prochain saut à utiliser pour la destination qu'elle a cherchée à atteindre.

Le code peut avoir ces valeurs :

Code	Signification
0	Redirection pour le réseau de destination
1	Redirection pour l'hôte de destination
2	Redirection pour le ToS pour le réseau de destination
3	Redirection pour le Tos pour l'hôte de destination

Pour configurer le ICMP Redirect sur un routeur Cisco, il faut utiliser cette commande :

- **[no] ip redirects**
  - Mode de configuration d'interface
  - Active/désactive les messages ICMP Redirect
  - Actif par défaut

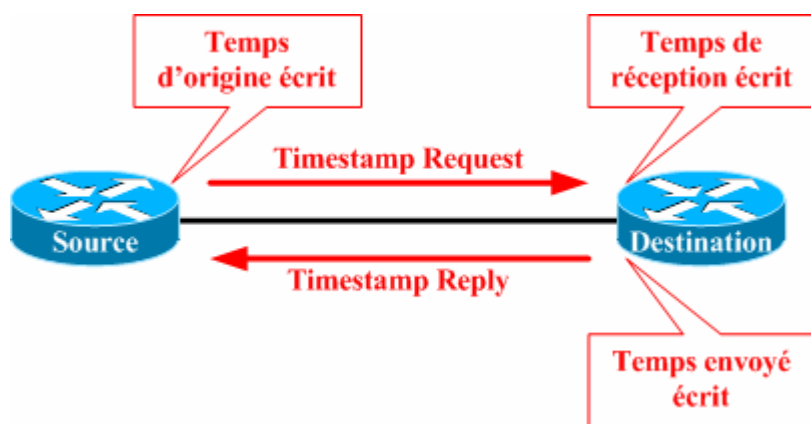
### 9.2.7. Timestamp Request/Reply

Les deux messages ICMP ont été créés afin d'aider à la synchronisation du temps entre des dispositifs. L'en-tête utilisé est ainsi :

8 bits	8 bits	16 bits	16 bits	16 bits	32 bits	32 bits	32 bits
Type (13 ou 14)	Code (0)	Somme de contrôle	Identifica teur	Numéro de séquence	Temps d'origine	Temps reçu	Temps envoyé

En-tête ICMP Timestamp Request/Reply

Les trois temps envoyés, en millisecondes depuis minuit du temps universel (UT), permettent aux deux pairs de vérifier l'heure de l'autre, et sont inscrits suivant cette séquence :



Processus d'échange de messages ICMP Timestamp

Ces messages sont très utiles pour synchroniser les dispositifs entre eux ainsi que pour déterminer le temps de transmission sur la liaison les reliant.

De nos jours, le protocole NTP (Network Time Protocol) est utilisé à la place de ces messages ICMP.



### **9.2.8. Information Request/Reply**

Ces messages étaient utilisés par un hôte pour déterminer son adresse réseau.

Ces messages ICMP sont remplacés par les protocoles BOOTP, RARP et DHCP.

### **9.2.9. Address Mask Request/Reply**

Ces messages permettent à un hôte de demander à sa passerelle par défaut le masque de sous-réseau à utiliser.

### **9.2.10. Router Discovery/Solicitation**

Ces deux messages sont utilisés pour indiquer aux hôtes d'un réseau de l'adresse de leur passerelle par défaut lorsqu'ils ne la connaissent pas.

Le message ICMP Router Solicitation est envoyé par un hôte n'ayant pas de passerelle par défaut.

Le message ICMP Router Discovery est envoyé par le routeur en réponse à un message ICMP Router Solicitation.

## 10. Résolution de problèmes

---

### 10.1. Commandes de vérification

Trois commandes vous permettent de vérifier la configuration des adresses dans votre réseau :

- **telnet {IP ou nom d'hôte} [tcp-port-number]** : Mécanisme de test le plus complet car permet de vérifier toutes les couches du modèle OSI
- **ping [IP ou nom d'hôte]** : Mécanisme de test de base pour la couche 3 permettant de vérifier la connexion matérielle et l'adresse de couche réseau du modèle OSI pour une destination précise
- **trace {IP ou nom d'hôte}** : Génération de messages à partir de chaque routeur situé tout au long du chemin jusqu'à la destination

La commande **telnet** permet, en plus d'offrir un accès à un hôte pour pouvoir l'administrer, de vérifier l'état fonctionnel d'un service. Il nous est possible par conséquent d'explicitier le service, par le biais du port TCP qui lui est rattaché, afin d'en vérifier le bon fonctionnement.

La commande **ping** nous renvoie des informations de la forme suivante :

!	Réception réussie d'une réponse d'écho
.	Délai d'attente dépassé pour la réponse à la requête
U	Erreur due à une destination inaccessible
C	Paquet ayant rencontré une congestion de trafic
I	Vérification ping interrompue (par exemple avec la combinaison CTRL+MAJ+6)
?	Type de paquet inconnu
&	Durée de vie du paquet dépassée

Utilisée sans aucun paramètre depuis le mode privilégié, la commande ping devient ce qui est appelé la commande ping étendue, permettant de modifier les paramètres pour les requêtes.

Lorsqu'on utilise la commande **traceroute**, 3 analyseurs sont lancés sur chaque routeur rencontré sur le chemin menant à la destination, afin d'obtenir les temps de réponse pour chacun d'entre eux. Ceci est très utile pour déterminer l'emplacement d'un plausible problème ou goulet d'étranglement.

Si il y a un problème quelconque, les résultats ne seront pas ces temps, mais seront parmi les suivants :

!H	La sonde d'analyse a été reçue par le routeur, mais elle n'a pas été transmise, probablement en raison d'une liste d'accès
!P	Le protocole était inaccessible
!N	Le réseau était inaccessible
!U	Le port était inaccessible
*	Le délai d'attente a été dépassé

### 10.2. Erreurs courantes et modèle OSI

L'une des méthodes pouvant être utilisée pour la résolution des problèmes est la vérification des différentes couches du modèle OSI en commençant par la plus basse.

Les erreurs courantes au niveau de la couche 1 sont les suivantes :

- Des câbles rompus
- Des câbles déconnectés
- Des câbles raccordés à des ports inappropriés
- Des connexions instables
- Des câbles inappropriés pour la tâche à accomplir (les câbles console, les câbles d'interconnexion et les câbles droits doivent être employés à bon escient)
- Des problèmes d'émetteur-récepteur
- Des problèmes de câblage ETCD
- Des problèmes de câblage ETTD
- Des unités hors tension

Les erreurs courantes au niveau de la couche 2 sont les suivantes :

- Des interfaces série configurées de façon incorrecte
- Des interfaces Ethernet configurées de façon incorrecte
- Un ensemble d'encapsulation inapproprié (HDLC est utilisé par défaut pour les interfaces série)
- Une fréquence d'horloge inappropriée pour les interfaces WAN

Les erreurs courantes au niveau de la couche 3 sont les suivantes :

- Un protocole de routage non activé
- Un protocole de routage activé mais incorrect
- Des adresses IP incorrectes
- Des masques de sous-réseau incorrects
- Des liens DNS/IP incorrects

### 10.3. Déboguage

IOS met à notre disposition toute une panoplie de commandes nous permettant de vérifier en temps réel les interactions et communications. Cela nous permet de vérifier le bon fonctionnement du routeur et, le cas échéant, d'avoir des informations sur les problèmes rencontrés.

Il faut utiliser les commandes de déboguage avec parcimonie car elles exigent un temps processeur important.

Elles sont disponibles depuis le mode privilégié.

En plus des commandes de déboguage déjà étudiées, les commandes suivantes sont disponibles :

- **no debug all** : Permet de stopper tous les déboguages en cours
- **undebug all** : Idem que la précédente
- **debug all** : Affiche l'intégralité des informations de déboguage disponibles

## 10.4. Procédure de récupération des mots de passe d'un routeur

Pour pouvoir accéder à un routeur, sachant que l'on ne dispose pas du ou des mots de passe appropriés, nous avons à notre disposition une procédure de récupération des mots de passe.

Pour cette procédure, il faut avoir impérativement un accès physique au routeur, par le biais du port console.

Cette procédure peut varier en fonction de la plateforme utilisée, et est effectuée en 2 redémarrages :

- **Redémarrage n°1** : Modification du registre de configuration depuis le mode RXBoot
- **Redémarrage n°2** : Modification de la configuration du routeur sous IOS

Pour le redémarrage n°1, il faut faire ainsi :

- Redémarrer le routeur (interrupteur ou avec la commande **reload** sous IOS)
- Utiliser la combinaison de touches **CTRL+Pause** avant expiration des 60 secondes suivant le redémarrage
- On se trouve alors dans le mode RXBoot. Il faut maintenant changer la valeur du registre de configuration afin de forcer le routeur à ignorer le fichier de configuration de sauvegarde lors du démarrage :
  - Commande **o/r 0x2142** (routeurs 2500)
  - Commande **confreg 0x2142** (routeurs 1600, 1700, 2600, 3600, etc.)
- Sortir du mode RXBoot et relancer le routeur :
  - Commande **i** (routeurs 2500)
  - Commande **reset** (routeurs 1600, 1700, 2600, 3600, etc.)

Au redémarrage n°2, nous sommes de nouveaux sous IOS. Il ne nous reste plus qu'à effectuer ces étapes :

- Le mode SETUP nous demande si l'on souhaite effectuer la configuration basique du routeur. Il suffit de refuser en répondant **N** ou en utilisant la combinaison de touche **CTRL+C**.
- On peut ensuite accéder au mode privilégié sans aucun mot de passe. A ce niveau, le routeur a repris sa configuration d'usine.
- Il faut restaurer la valeur initiale du registre de configuration en utilisant la commande **config-register 0x2102** depuis le mode de configuration globale.

Nous avons maintenant la possibilité de restaurer la configuration d'avant, tout en modifiant les mots de passe, ou de laisser le routeur dans sa configuration d'usine.

Pour restaurer la configuration précédente et changer les mots de passe, il faut faire ainsi :

- Importer la configuration précédente (commande **copy start run**)
- Changer les mots de passe des différentes lignes ainsi que pour le mode privilégié
- Sauvegarder l'ancienne configuration avec les nouveaux mots de passe (commande **copy run start**)
- Redémarrer le routeur (commande **reload**)

Il est important de redémarrer le routeur à la fin de cette procédure, car les mots de passe des lignes console et auxiliaire ne sont pris en compte qu'après ce redémarrage.

# 11. ACL

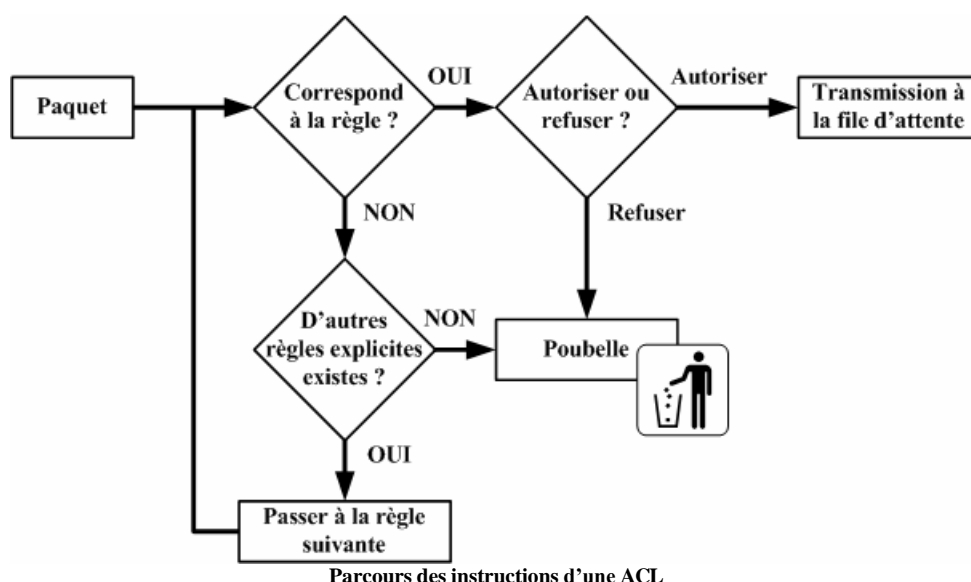
## 11.1. Théorie

### 11.1.1. Principe fondamental

Une ACL (Access Control List) est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie.

Cette liste est parcourue de la première à la dernière instruction jusqu'à trouver une correspondance. Si le paquet répond aux critères d'une instruction, le reste des instructions est ignoré et le paquet est autorisé ou refusé. Si aucune correspondance n'est trouvée dans les critères explicites par l'administrateur, le paquet est implicitement supprimé.

Il ne peut y avoir qu'une seule ACL par protocole, par interface et par direction (entrée/sortie).



Les ACLs permettent ainsi d'autoriser ou d'interdire des trafics en fonctions de critères tels que les adresses sources et destinations, les protocoles utilisés et les numéros de ports.

Une ACL est identifiable par son numéro ou son nom, attribué suivant le protocole et le type :

- ACL standard (numérotée)
- ACL étendue (numérotée)
- ACL nommée (peut être de type standard ou étendue)

Plage de numéros	Type d'ACL associé
1 à 99 et 1300 à 1999	Standard pour IP
100 à 199 et 2000 à 2699	Etendue pour IP
600 à 699	AppleTalk
800 à 899	Standard pour IPX
900 à 999	Etendue pour IPX
1000 à 1099	IPX/SAP

L'avantage principal des ACLs est donc de fournir une base de sécurité réseau en filtrant les trafics traversant un routeur.

Le principal inconvénient est malheureusement un traitement supplémentaire à effectuer pour chaque paquet entrant et/ou sortant du routeur, rallongeant ainsi à la latence réseau et à la surcharge CPU.

La configuration des ACLs se fait en deux parties distinctes, à savoir :

- Création de l'ACL
- Application de l'ACL sur une interface réseau

Quelques précautions sont à prendre en compte lors de la configuration ou de l'utilisation des ACLs :

- Les instructions sont toujours parcourues de la première à la dernière, jusqu'à correspondance des critères.
- Si aucune instruction ne correspond au paquet, la dernière instruction implicite indique alors de supprimer ce paquet.
- Une ACL appliquée sur une interface mais dont les instructions ne sont pas configurées n'a pour seule instruction que la dernière qui bloque tout. Tout trafic serait alors interdit.
- Lors de la création des instructions, il faut toujours procéder du plus précis (exceptions) au plus générique.
- Une ACL IP qui interdit un paquet enverra automatiquement un message ICMP Host Unreachable.
- Une ACL pour un trafic sortant n'affecte pas le trafic originaire du routeur local.

### 11.1.2. Masque générique

Les instructions utilisées dans les ACLs utilisent les masques génériques (Wildcard Mask) conjointement à des préfixes réseaux pour identifier des plages d'adresses.

Un masque générique est une valeur 32 bits noté sous la forme décimale pointée (comme les IP et les masques de sous-réseaux), sachant que :

- **"0" binaire** : Doit correspondre
- **"1" binaire** : Peut varier

On observe donc qu'un masque générique est l'inverse binaire d'un masque de sous-réseaux, ou, du point de vue décimal pointé, est le complément à 255 du masque de sous-réseau correspondant :

Masque de sous-réseau	1111 1111.1111 1111.1110 000.0000 0000
Masque générique	0000 0000.0000 0000.0001 111.1111 1111

$$\begin{array}{rcl} 255 . 255 . 224 . 0 & \text{(Masque de sous-réseau)} \\ + & 0 . 0 . 31 . 255 & \text{(Masque générique)} \\ \hline = & 255 . 255 . 255 . 255 \end{array}$$

Par conséquent, un masque générique ne peut prendre que ces valeurs (pour chaque octet) :

0	1	3	7	15	31	63	127	255
---	---	---	---	----	----	----	-----	-----

Au niveau syntaxique, deux masques génériques précis (les deux extrêmes, à savoir tout ou rien) peuvent s'écrire normalement, sous la forme préfixe/masque générique, ou sous une forme plus conviviale. Ces deux exceptions d'écriture sont les suivantes :

- **{IP} {0.0.0.0} = host {IP}**
- **{IP} {255.255.255.255} = any**

### 11.2. ACL standard

Une ACL standard permet d'autoriser ou d'interdire des adresses spécifiques ou bien un ensemble d'adresses ou de protocoles, sachant que, dans les instructions d'une ACL standard, on ne peut indiquer que des adresses sources.

Ce sont les ACLs les plus simples et, par conséquent, les moins gourmandes en ressources CPU. Elles sont par exemple utilisées pour autoriser ou interdire toute une plage d'adresses réseaux ou encore pour le filtrage des informations contenues dans des mises à jour de routage.

Pour configurer une instruction pour une ACL standard pour IP, il faut utiliser la commande suivante :

- **access-list {numéro} {permit | deny} {préfixe} [masque générique] [log]**
- **access-list {numéro} {remark} {commentaire}**
  - Mode de configuration globale
  - Si le masque générique n'est pas précisé, le masque générique par défaut 0.0.0.0 est utilisé.
  - **log** permet de garder en mémoire le nombre de paquets correspondant à l'instruction en cours.
  - Le mot clé **remark** suivi d'un commentaire permet d'indiquer l'utilité de l'instruction.

L'ordre de parcours des instructions dépend de l'ordre dans lequel on a configuré les instructions. Une nouvelle instruction est donc obligatoirement ajoutée à la fin de la liste, et il est impossible de supprimer une instruction particulière.

Pour toute modification, il est donc conseillé d'utiliser un éditeur de texte, de copier la liste des instructions de l'ACL devant être modifiée, de supprimer cette ACL sur le routeur, d'éditer les instructions pour faire les modifications voulues puis de les insérer dans le routeur.

### 11.3. ACL étendue

Une ACL étendue permet de faire un filtrage plus précis qu'une ACL standard. En effet, une ACL étendue permet de filtrer en fonction de :

- Protocole utilisé (couche 3 et 4)
- Adresse source
- Adresse de destination
- Numéro de port

La commande permettant de configurer une ACL étendue pour IP est :

- **access-list {numéro} {permit | deny} {protocole} {préfixe source} {masque source} [{opérateur} {opérande}] {préfixe destination} {masque destination} [{opérateur} {opérande}] [icmp-type] [log] [established]**
- **access-list {numéro} {remark} {commentaire}**
  - Mode de configuration globale
  - **protocole** peut être soit le nom (IP, TCP, UDP, ICMP, IGRP, etc.) soit le numéro du protocole (de 0 à 255).
  - Le couple **opérateur/opérande** est pour les numéros de ports TCP ou UDP uniquement, et peut être spécifié pour la source et/ou pour la destination :

Opérateur	Signification
eq	Egal à
neq	Différent de
lt	Inférieur à
gt	Supérieur à
range	Entre (nécessite 2 numéros de port)

- Le paramètre **icmp-type** ne peut être utilisé que pour le protocole ICMP, et correspond au nom ou au numéro du type de message ICM devant être vérifié.
- Le paramètre **established** ne peut être utilisé que pour le protocole TCP et permet de faire correspondre uniquement les sessions TCP déjà établies (drapeaux ACK, FIN, PSH, RST, SYN ou URG).

Pour l'ordre de parcours ou la modification, les règles sont les mêmes qu'avec une ACL standard.

## 11.4. ACL nommée

Depuis la version 11.2 d'IOS, il est possible d'utiliser les ACLs nommées. Les ACLs nommées permettent l'identification par des chaînes alphanumériques plutôt que par la représentation numérique actuelle.

Une ACL nommée peut être de type standard ou étendue.

Deux nouveaux modes de configuration sont donc étudiés :

Mode de configuration	Invite de commande associée
ACL nommée standard	(config-std-nacl)#
ACL nommée étendue	(config-ext-nacl)#

Les ACLs nommées permettent :

- D'identifier intuitivement les listes de contrôle d'accès à l'aide d'un code alphanumérique
- De supprimer une instruction particulière sans avoir à tout supprimer et réécrire



Les commandes suivantes permettent de configurer une ACL nommée :

- **ip access-list {standard | extended} {nom}**
  - Mode de configuration globale
  - Permet de créer une ACL nommée standard ou étendue
  - Permet de passer dans le mode de configuration de l'ACL nommée
- **{permit | deny} {préfixe} [masque] [log]**
  - Mode de configuration d'ACL nommé standard
  - Les paramètres sont identiques que pour une ACL standard numérotée.
- **{permit | deny} {protocole} {préfixe source} {masque source} [{opérateur} {opérande}] {préfixe destination} {masque destination} [{opérateur} {opérande}] [icmp-type] [log] [established]**
  - Mode de configuration d'ACL nommée étendue
  - Les paramètres sont identiques que pour une ACL étendue numérotée
- **remark {commentaire}**
  - Mode de configuration d'ACL nommée (standard ou étendue)
  - Fournit un commentaire pour indiquer l'utilité de l'ACL

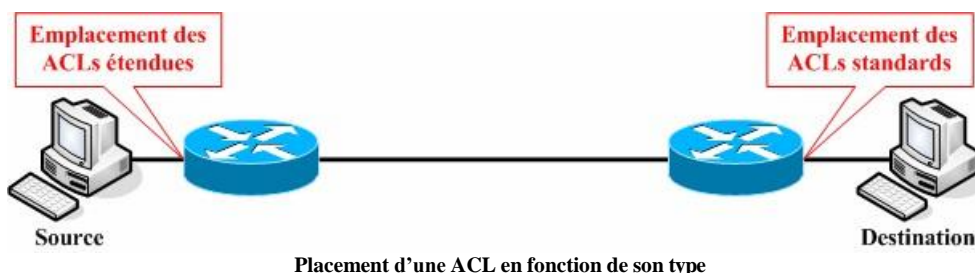
### 11.5. Mise en place et vérification des ACLs

La création des ACLs étant faite, il faut maintenant les appliquer en utilisant les commandes suivantes :

- **ip access-group {numéro | nom} {in | out}**
  - Mode de configuration d'interface
  - Applique une ACL (standard, étendue ou nommée) sur l'interface pour filtrer le trafic entrant ou sortant
- **ip access-class {numéro | nom} {in | out}**
  - Mode de configuration de ligne
  - Applique une ACL sur la ligne pour filtrer les accès à cette dernière
- **no access-list {numéro}**
  - Mode de configuration globale
  - Supprime complètement une ACL numérotée

Les commandes suivantes servent à vérifier le placement des ACLs, ainsi que leurs instructions :

- **show access-lists [numéro | nom]** : Affiche la liste des ACLs créées sur le routeur, leurs instructions ainsi que le nombre de correspondance pour chaque instruction
- **show ip interface [{type} {numéro}]** : Permet entre autres de voir quelles sont les ACLs appliquées sur les interfaces et pour quelle direction



Parce que les ACLs standards ne permettent que de filtrer en fonction d'adresses sources, il faut les placer au plus près de la destination, et inversement pour les ACLs étendues qui doivent toujours être placées au plus près de la source.

De plus, les ACLs standards, interdisant intégralement un trafic pour une source donnée, bloquent implicitement le trafic dans le sens opposé (explicitement bloqué de la source vers la destination et implicitement bloqué de la destination à la source).