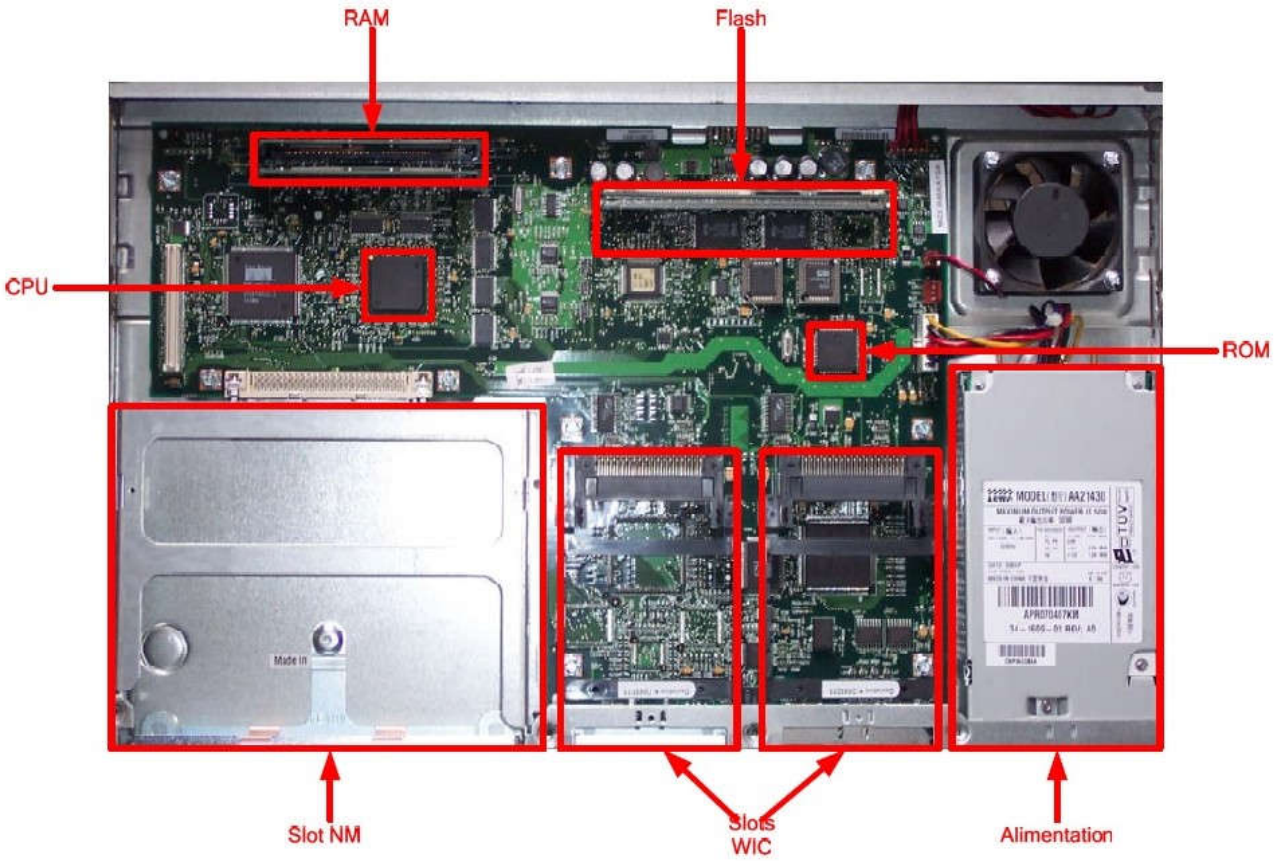
2. Introduction aux routeurs

2.1. Présentation d'un routeur Cisco

2.1.1. Composants internes



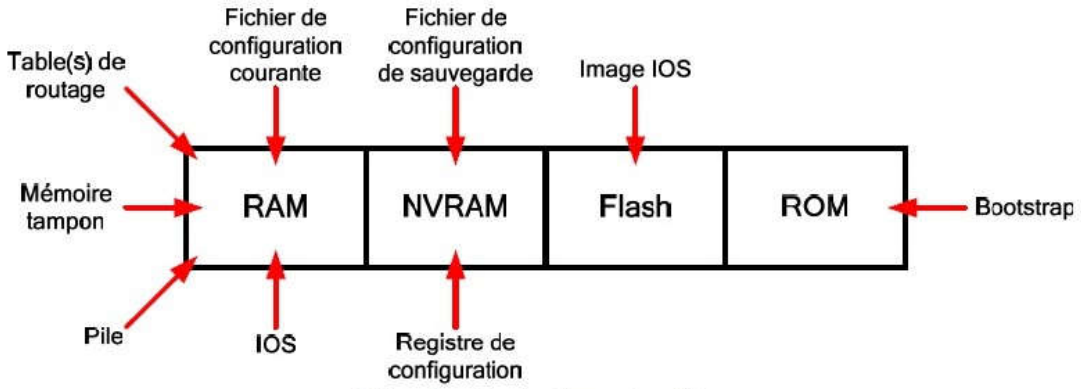


Schéma des mémoires d'un routeur Cisco

Schématiquement, les composants internes qui nous intéressent principalement sont les différentes mémoires utilisées :

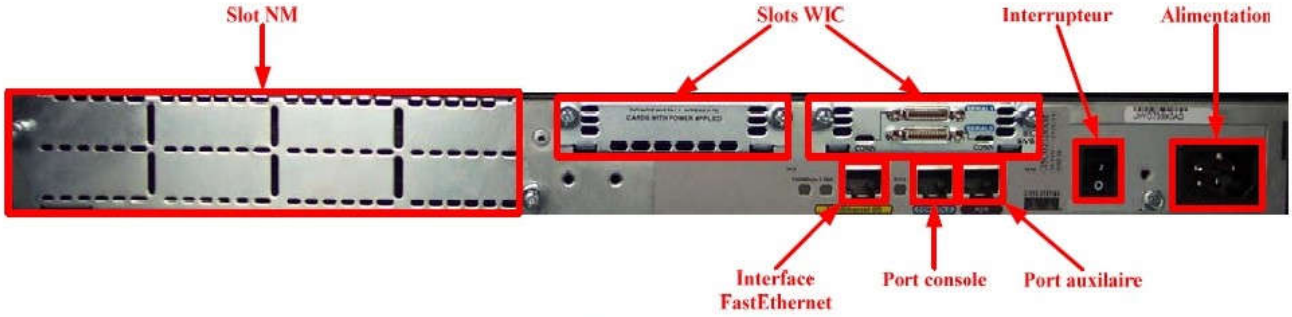
- **RAM** : C'est la mémoire principale de travail du routeur. Elle contient entre autres le système d'exploitation une fois chargé, le fichier de configuration active, la ou les tables de routage, ainsi que les mémoires tampon utilisées par les interfaces et la pile utilisée par les processus logiciels. Sa taille varie en fonction du modèle de routeur (64 ou 96 Mo sur un 2620XM). Le contenu de cette mémoire est effacé 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 effacé 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. Celle-ci est donc uniquement utilisée au démarrage du routeur.

2.1.2. Composants externes



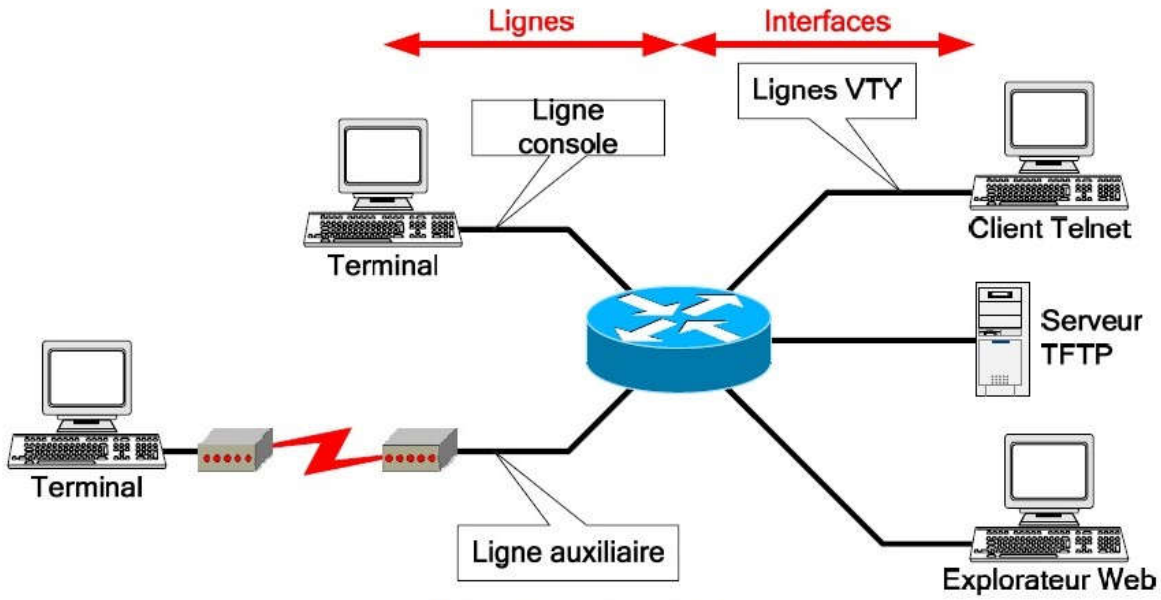
Vue arrière d'un routeur Cisco 2620XM

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)

2.2.2. Accès pour configuration

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



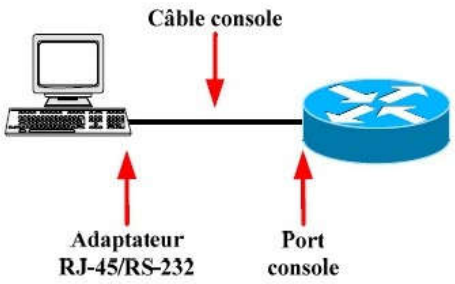
Moyens d'accès pour configuration

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** : Import/export de fichiers de configuration.

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).

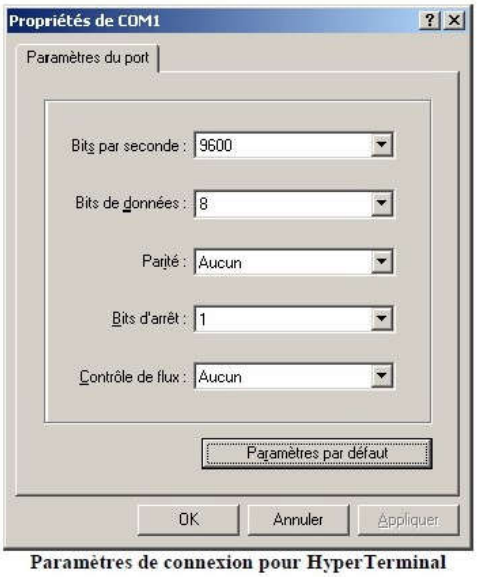


Un émulateur de terminaux (exemple : HyperTerminal sous Windows) permet l'accès à l'interface de configuration du routeur.

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 dispositifs 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 la 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 **terminal [no] 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 ne dispose que de commandes de visualisation d'état sur le 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 que dans chaque mode spécifique 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.

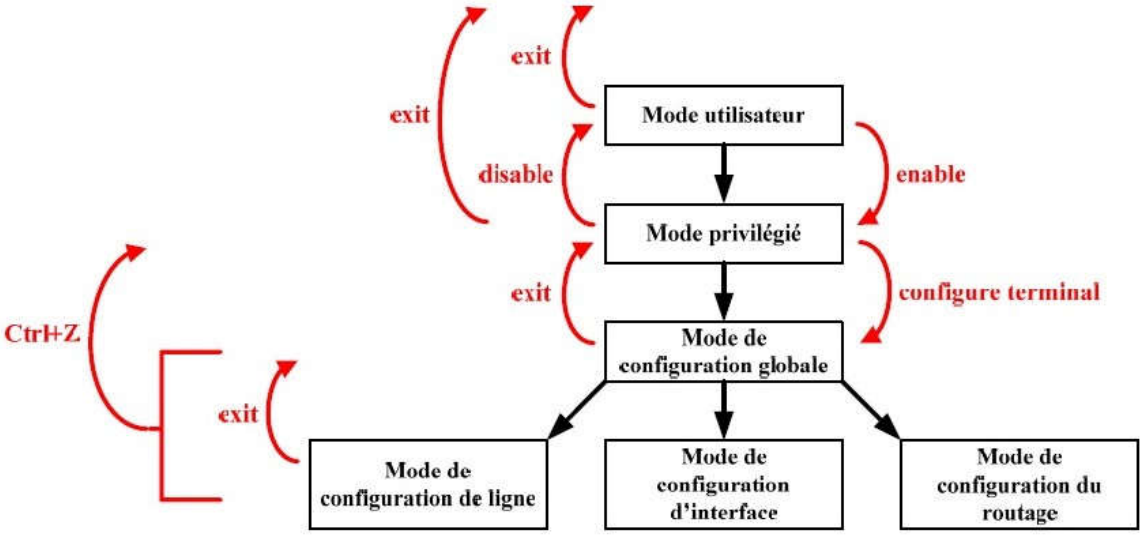
On peut facilement identifier le mode dans lequel on est en repérant l'invite de commande que nous fournit l'interpréteur de commandes EXEC :

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

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

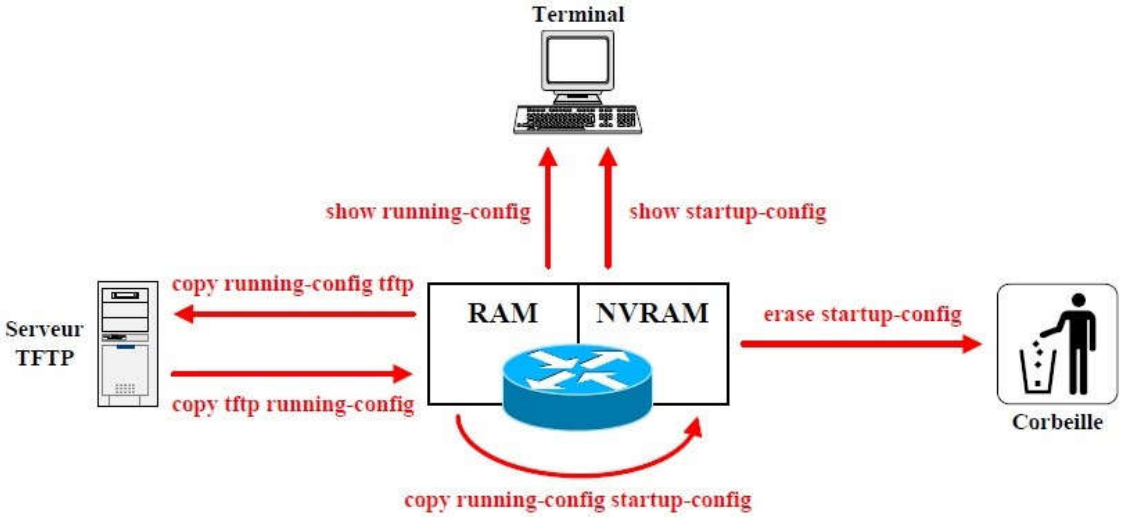
Mode	Invite de commande
Utilisateur	Router >
Privilégié	Router #
Configuration globale	Router (config) #
Interface	Router (config-if) #
Ligne	Router (config-line) #
Routage	Router (config-router) #

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



Hiérarchie et navigation dans les modes d'IOS

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

3.1. 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.

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

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

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 fournit 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 ne 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/pas besoin.

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 modifications sur ce processus à longueur de temps. Cela devient en revanche primordial lorsqu'il faut mettre à jour l'image d'IOS actuellement en place sur le routeur 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

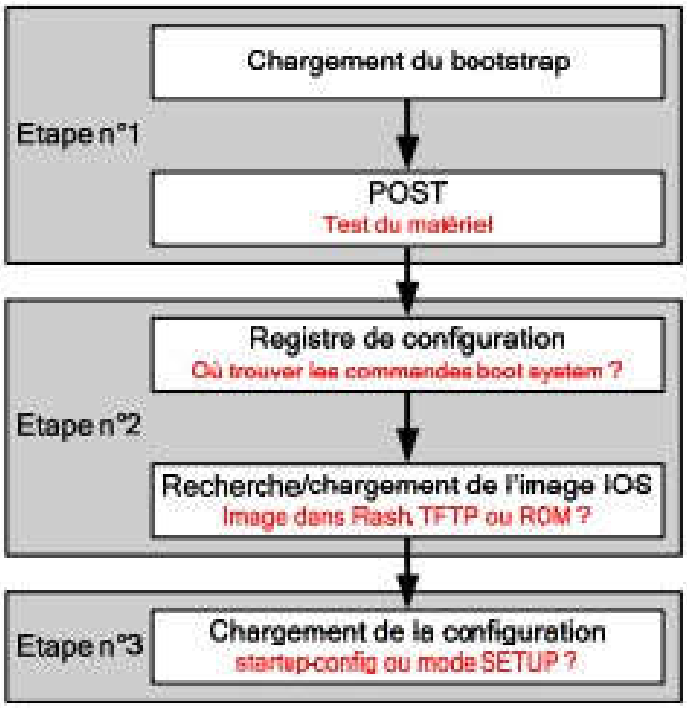
La séquence d'amorçage d'un routeur est découpée en 3 étapes :

- 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.

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.
  - 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

6.2. Commutateurs

6.2.1. Présentation

Un commutateur est un équipement réseau de couche 2. Il en existe une grande variété avec des caractéristiques différentes :

- Nombre de ports
- Type de port (10/100 Mbits, gigabit)
- Type de commutation (Strore and Forward, Cut Through)
- Facilité d'installation en armoire etc…

Les différents types de commutation :

- **Store and forward**: Le commutateur attend d'avoir reçu toute la trame avant de la transmettre. Cette méthode offre une grande vérification d'erreur car le commutateur a le temps de vérifier la valeur FCS. Cependant ce traitement augmente la latence réseau.

- **Cut Through**: Dès que l'adresse de destination est connue, la trame commence à être commutée. Ce mode est plus rapide que le précédent. Il existe différentes variantes de ce type de commutation:

    - **Fragment Free**: Filtrage des fragments de collision (inférieur à 64 octets). Le commutateur attend d'avoir reçu les 64 premiers octets avant de commencer à transmettre la trame. La détection des collisions subies doit être détectée au niveau des 64 premiers octets.

    - **Fast Forward**: Pas de vérification d'erreurs. La trame est transmise dès que l'adresse de destination est identifiée.

6.2.4. Voyants d'un commutateur

Voyant	Etat et signification	
Système	Voyant éteint : le système est hors tension.	
	Voyant vert : le système est sous-tension.	
	Voyant ambre : problème suite au POST.	
RPS (Remote Power Supply)	Ce voyant indique si l'alimentation de sécurité est utilisée.	
Port	Chaque port a son voyant qui donne des indications sur l'état du port selon le mode choisi.	
Bouton mode	Permet de choisir entre les 4 modes: Stat, Util, Duplex et Speed.	
Bouton mode	Stat	Donne des informations sur l'état des ports. Une lumière verte indique que le port est opérationnel. Quand elle clignote elle témoigne d'une activité. Si la lumière est éteinte le port est non opérationnel.
	Util	Ce mode utilise l'ensemble des voyants de ports pour donner des informations sur l'utilisation générale du commutateur.
	Duplex	Quand le voyant est allumé le port fonctionne en mode full duplex. Eteint, c'est le mode half duplex qui est employé.
	Speed	Un voyant allumé indique un débit de 100 Mbits, un voyant éteint un débit de 10Mbits.

Face avant et arrière d'un commutateur Cisco Catalyst 2950

6.3. Protocole Spanning-Tree

Les topologies redondantes sont mises en place pour palier à des liaisons interrompues. En effet, plusieurs chemins peuvent permettre d'accéder au même lien.

Mais si ces chemins redondants ne sont pas correctement gérés, les trames peuvent boucler indéfiniment. Le protocole Spanning-Tree permet d'y remédier.

6.3.1. Théorie concernant Spanning-Tree

Les commutateurs implémentent le protocole **IEEE 802.1D Spanning-Tree**. Il apporte une réponse au problème de bouclage. Pour ce faire, **STP** (Spanning-Tree Protocol) empêche certains ports de transmettre en mettant les ports dans un état de blocage ou dans un état de transmission, afin qu'il n'y ait qu'un seul chemin possible entre deux segments de LAN.

Un port bloqué ne peut ni recevoir ni émettre et inversement en mode de transmission. En premier lieu, des **BPDUs (Bridge Protocol Data Unit)** sont envoyés toutes les 2 secondes sur tous les ports.

Le commutateur qui détient l'identifiant de pont le plus bas (Bridge ID) est élu racine. Le Bridge ID de 8 octets est composé d'une priorité sur 2 octets (32768 par défaut), suivi par l'adresse MAC du port émetteur. Tous les ports du commutateur racine sont placés en état de transmission par le protocole STP.

Le commutateur racine transmet par tous ses ports des BPDUs. Ces messages sont transmis par les commutateurs non racine. A chaque réception de BPDU, le champ du coût est incrémenté, ce qui permet aux commutateurs non racine de connaître la valeur de l'itinéraire jusqu'à la racine.

Le port de chaque commutateur qui reçoit le BPDU comportant le coût le plus bas (donc le plus proche du commutateur racine) est élu port racine pour le segment de LAN auquel il est connecté.

Le calcul de la route se base sur la vitesse. Plus elle est grande, plus le coût est bas. Le port par lequel arrivent les BPDU portant le moindre coût vers la racine est mis en état de transmission. Les autres ports sont mis en état de blocage, pour éliminer toute route redondante et ainsi éviter qu'il y ait des boucles actives.

Les ports prennent d'autres états. Voici un tableau récapitulatif des états appliqués aux ports :

Etat	Description
Transmission	Le port émet et reçoit les trames.
Ecoute	Le port écoute les BPDU pour s'assurer qu'il n'y ait pas de boucle. Ce processus a une durée de vie de 15 secondes.
Apprentissage	Le port écoute les BPDU pour découvrir les adresses MAC. Ce processus a une durée de vie de 15 secondes également.
Désactivé	Le port n'est pas utilisé pour des raisons administratives.
Blocage	Le port ne peut ni émettre ni recevoir les trames.

6.3.2. Théorie concernant Rapid Spanning-Tree

Le protocole RSTP (Rapid Spanning Tree Protocol) est défini par le standard IEEE 802.1w. Il diffère principalement de STP de part sa convergence plus rapide. En effet, RSTP offre une convergence au minimum 5 fois plus rapide que STP. RSTP prend moins de 10 secondes pour converger.

RSTP et STP partagent certaines similitudes:

- Election d'un commutateur racine suivant le même processus.
- Ils élisent le port racine des commutateurs non racine de la même manière.
- Ils élisent le port désigné pour un segment de LAN de la même façon.
- Ils placent tous les ports dans un état de blocage ou de transmission, à la différence que RSTP utilise l'appellation discarding pour l'état de blocage.

RSTP définit aussi des types de liaisons et de bordures. Les liaisons sont les connections physique entre les commutateurs et les bordures les connections physiques entre un commutateur et un hôte ou un concentrateur. On distingue:

- Les liaisons point-à-point, c'est-à-dire entre deux commutateurs.
- Les liaisons partagées, c'est-à-dire entre un et plusieurs commutateurs.
- Les bordures point-à-point, entre un hôte et un commutateur.
- Les bordures partagées, entre un concentrateur et un commutateur.

Les ports des liaisons point-à-point et des bordures point-à-point sont immédiatement placés dans l'état de transmission. Ce qui permet d'améliorer la vitesse de convergence des commutateurs.