Administration de routeurs CISCO

Pr. M. AIT HEMAD
ait.hemad.m@gmail.com

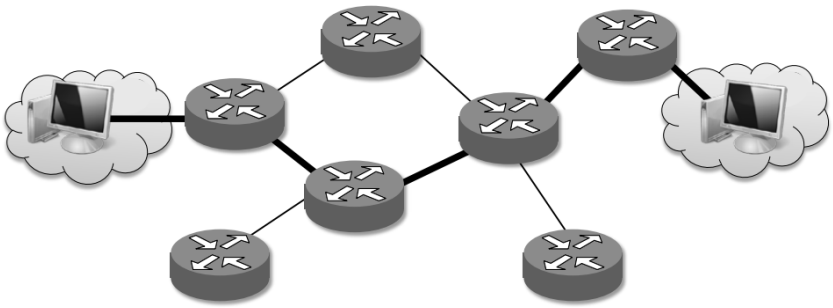
Rappel : Routage IP

Routage

- On appelle "*routage*" toute technique basée sur des adresses de niveau 3 réseau permettant d'aiguiller une trame quelconque émise par un nœud d'un sous-réseau vers un nœud de destination pouvant être situé sur un autre sous-réseau.
- Des dispositifs matériels (comportant des logiciels) permettant d'effectuer cette tâche s'appellent des *Routeurs*.

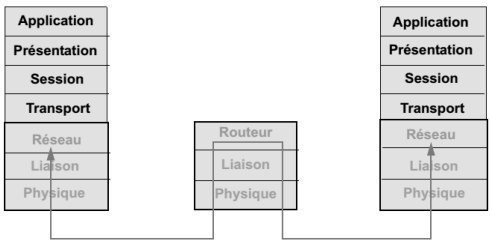
Routage

- Routeurs



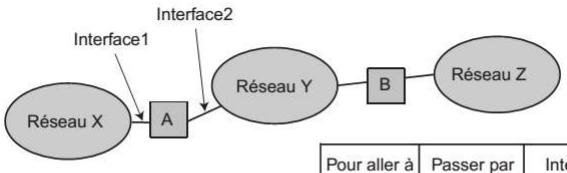
Routage

- C'est quoi un routeur : c'est un élément d'interconnexion de niveau 3 qui achemine (route) les données vers un destinataire identifié par son adresse de niveau 3



Routage

- les routeurs acheminent les paquets selon des informations contenues dans des tables dites *tables de routage*



Pour aller à	Passer par	Interface
X	–	1
Y	–	2
Z	B	2

Routage : Tables de routage

- Les informations contenues dans cette table sont:

Destination	Passerelle	Interface
Au réseau de destination	Adresse du prochain routeur	Interface utilisée pour envoyer les paquets

- Elle est composée de plusieurs lignes.
  - Chaque ligne correspond à une route vers un réseau

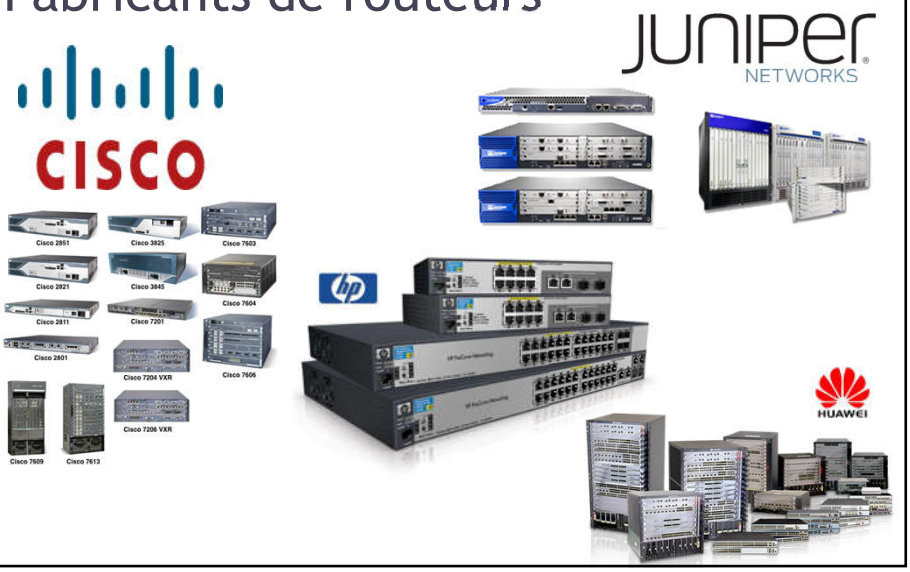
Routage

- Machines et routeurs participent au routage :
  - Ils possèdent tous deux une table de routage,
  - les machines doivent déterminer si le datagramme doit être délivré sur le réseau physique sur lequel elles sont connectées ou bien si le datagramme doit être acheminé vers un routeur, elle doit identifier le routeur appropriée.
  - les routeurs effectuent le choix de routage vers d'autres routeurs afin d'acheminer le datagramme vers sa destination finale.

Routage

- La table de routage est présente dans les hôtes comme dans les routeurs.
  - La différence entre la table de routage d'un hôte et celle d'un routeur, réside dans le fait qu'un hôte ne route que des datagrammes émis par lui-même, alors que le routeur transmet les datagrammes provenant d'autres nœuds IP.

Fabricants de routeurs



Routeur Cisco

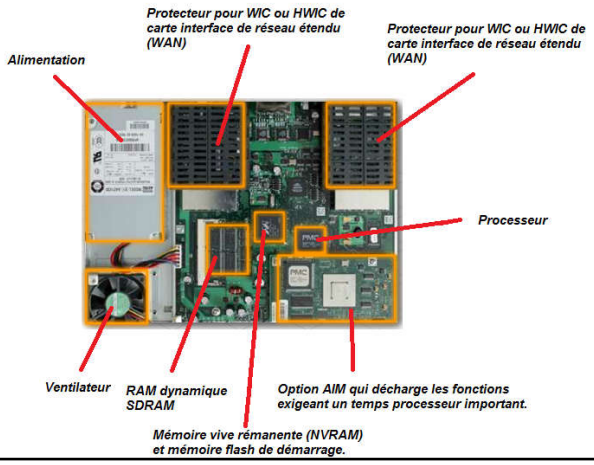
Présentation d'un routeur Cisco

Présentation d'un routeur Cisco

- En fonction des modèles, un routeur possède (au minimum) les composants matériels et logiciels suivants :
  - Carte mère
  - CPU
  - Mémoire
  - Bus
  - Interface E/S
  - Système d'exploitation

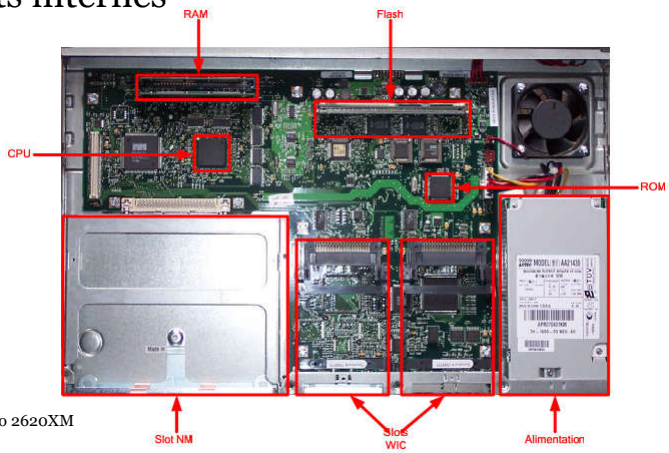
Présentation d'un routeur Cisco

- Composants internes



Présentation d'un routeur Cisco

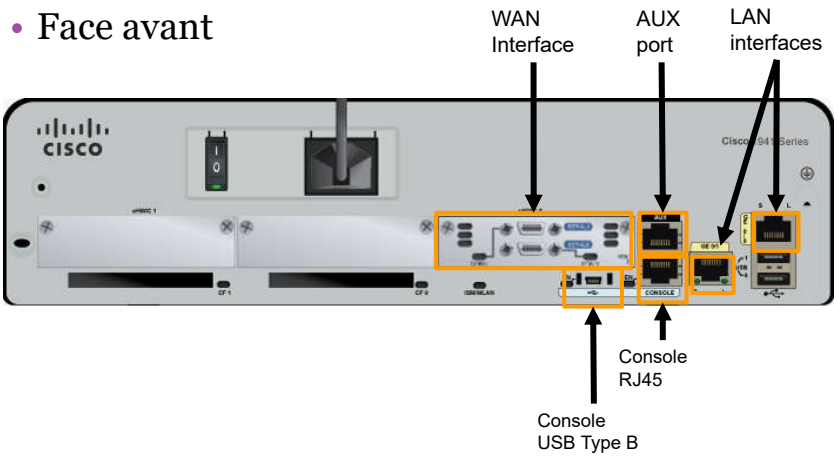
- Composants internes



Vue interne d'un routeur Cisco 2620XM

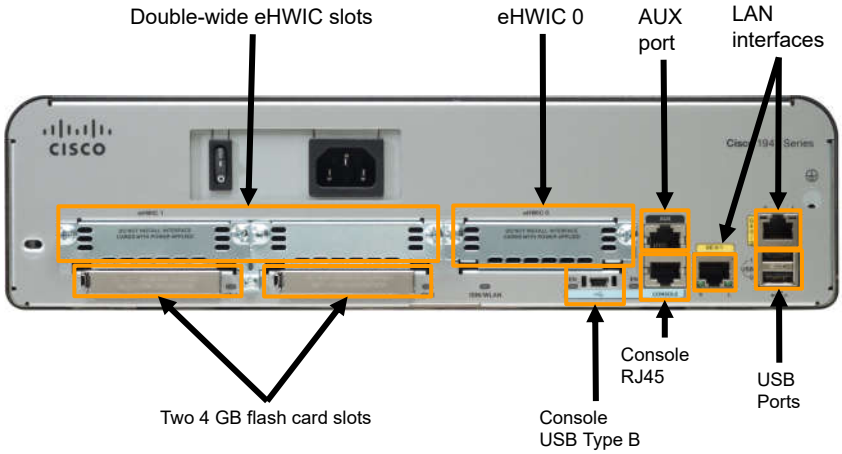
Présentation d'un routeur Cisco

- Face avant



Présentation d'un routeur Cisco

- Face avant



CPU (Central Processing Unit)

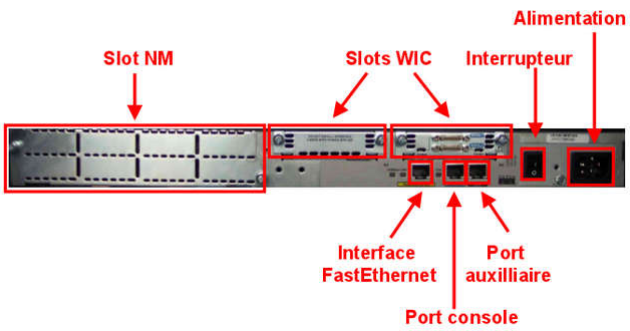
- le microprocesseur est responsable de l'exécution du système d'exploitation du routeur.
- De la puissance du CPU dépend la capacité de traitement du routeur.
- Historiquement, les processeurs des routeurs Cisco sont des processeurs RISC (Reduced Instruction Set Computing).
  - Exemple :
    - pour les séries 1700 et 2600 : Motorola MPC860 cadencés à au plus 80 MHz

Interface E/S

- 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)
  - …etc.

Présentation d'un routeur Cisco

- Interfaces d'E/S



Présentation d'un routeur Cisco

- Interfaces d'E/S

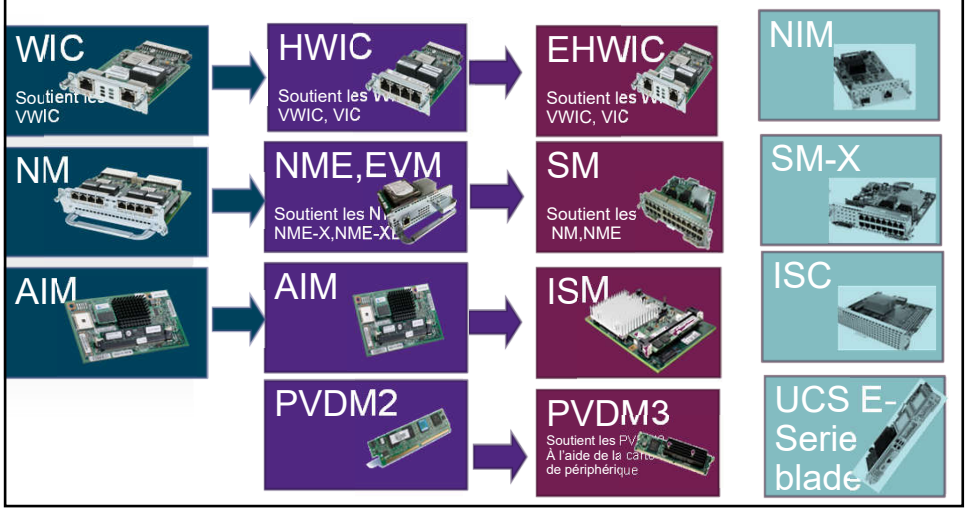
Cartes WIC

- Les cartes WIC (WAN Interface Card) s'enfichent dans les slots WIC du routeur et lui ajoutent une ou plusieurs interfaces d'un certain type.
- Voici quelques cartes WIC possibles :
  - WIC-1T (One-port serial, asynchronous and synchronous (T1/E1))
  - WIC-2T (Two-port serial, asynchronous and synchronous (T1/E1))
  - WIC-1B-S/T (One-port ISDN Basic Rate Interface (BRI) S/T)
  - WIC-1ADSL (One-port ADSL interface)
  - WIC-1SHDSL (One-port G.shdsl interface)
  - . . .et il y en a beaucoup d'autres

Cartes NM

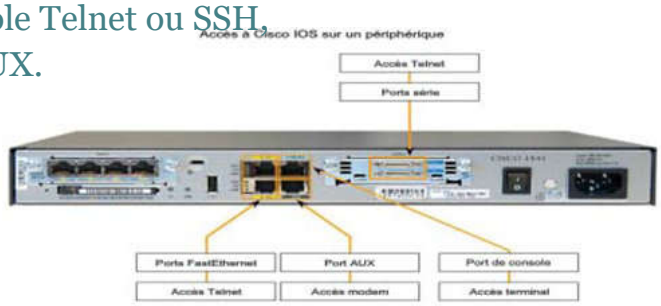
- Les cartes NM (Network Module) sont des modules réseau plus grands que les WIC et peuvent doter le routeur de nombreuses interfaces
- Il existe de nombreuses cartes NM, voici quelques exemples :
  - NM-1E : One-port 10BASE-T Ethernet interface
  - NM-ESW16 : Switch 16 ports Ethernet
  - NM-4E : 4-port 10BASE-T Ethernet interface

Autres cartes



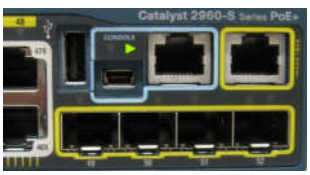
Méthodes d'accès au routeur Cisco

- Il y a plusieurs moyens d'accéder à l'environnement CLI.
- Les méthodes les plus répandues utilisent :
  - le port de console
  - le protocole Telnet ou SSH,
  - le port AUX.



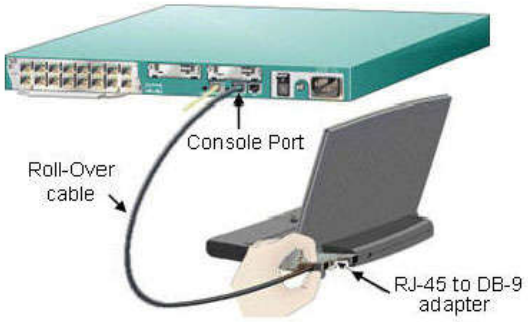
Port console

- La console s'utilise en particulier dans les circonstances suivantes :
  - configuration initiale du périphérique réseau
  - procédures de reprise après sinistre et dépannage lorsque l'accès distant est impossible
  - procédures de récupération des mots de passe.



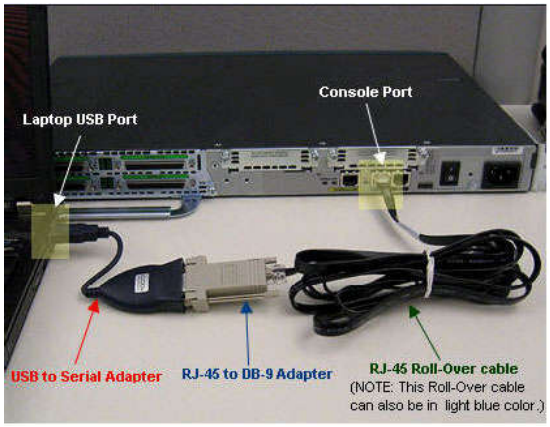
Port console

- Illustration



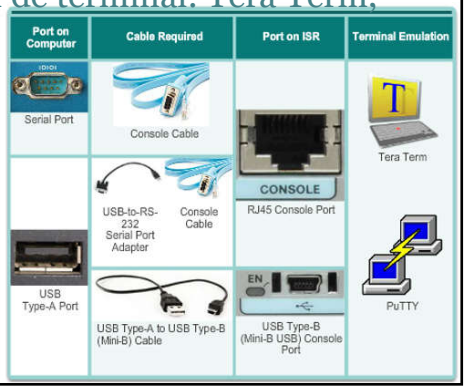
Port console

- Illustration



Port console

- Éléments requises :
  - câble console RJ-45-to-DB-9
  - Programme d'émulation de terminal: Tera Term, PuTTY, HyperTerminal



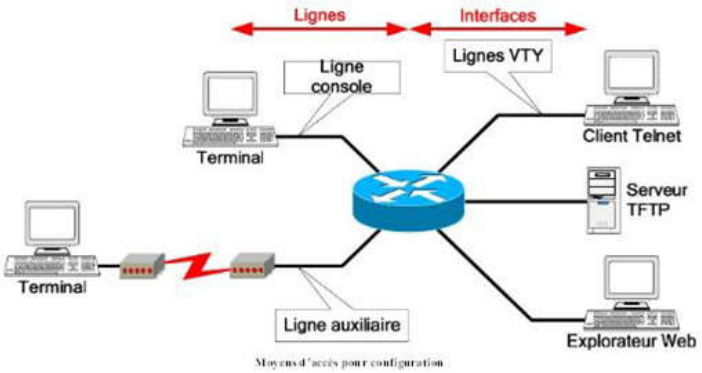
Port AUX

- Une autre façon d'ouvrir une session CLI à distance consiste à établir une connexion téléphonique commutée à travers un modem connecté au port AUX du routeur.
- À l'instar de la connexion console, cette méthode ne requiert pas la disponibilité de services réseau sur le périphérique.

Telnet ou SSH

- À la différence des connexions console, les sessions Telnet/SSH requièrent des services réseau actifs sur le périphérique.
  - Le périphérique réseau doit avoir au moins une interface active configurée avec une adresse de couche 3, par exemple une adresse IPv4.

Méthodes d'accès au routeur Cisco



Moyens d'accès pour configuration

Mémoires

- Un routeur dispose de plusieurs types de mémoires :
  - RAM
  - NVRAM
  - FLASH
  - ROM

RAM

- C'est la mémoire principale de travail du routeur.
- Le contenu de cette mémoire est effacé lors de la mise hors tension ou du redémarrage.
- Elle contient entre autres :
  - le système d'exploitation une fois chargé
  - le fichier de configuration active
  - les tables de routage
  - La table ARP
  - Les mémoires tampon utilisées par les interfaces
- Sa taille varie en fonction du modèle de routeur
  - exemple :
    - 128 Mo sur un routeur Cisco 2801
    - 256 Mo sur un routeur Cisco 2811.

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 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 représente une sorte de ROM effaçable et programmable
- Elle contient l'image du système d'exploitation de Cisco.
- Son contenu est conservé lors de la mise hors tension et du redémarrage

ROM

- Utilisée uniquement au démarrage du routeur
- C'est une mémoire permanente contenant :
  - le code pour réaliser les diagnostics de démarrage du matériel (POST, Power On Self Test)
  - le code pour le chargement (System Bootstrap) de l'image de l'IOS vers la RAM et la mise en route du système.
  - Elle contient aussi un système minimal (ROMMON)
    - une interface de commandes simplifiée permettant de réaliser des opérations de secours :
      - modification de la phase de boot
      - téléchargement par TFTP d'une image suite à une corruption de la flash
      - etc.

Mémoires

- Résumé

RAM	NVRAM	Flash	ROM
Table de routage	Fichier de configurationde sauvegardé	Image IOS	Bootstrap
Fichier de configuration courante	Registre de configuration		
Mémoire tampon			
Pile			
IOS			

Système d'exploitation Cisco IOS

- L'IOS prend en charge les protocoles et fournit l'interface de commandes CLI (Command Line Interface) accessible via une liaison série ou une session terminal Telnet ou SSH.
  - IOS : Internetwork Operating System
  - IOS-XE
  - NX-OS (les plateformes Nexus)
  - IOS-XR

Noms des fichiers IOS

- Le fichier d'image Cisco IOS est basé sur une convention d'attribution de noms spéciale :

{Plateforme}-{Feature Set}-{Format}.{Version}.bin

  - Plateforme: est le matériel sur lequel l'image est prévue pour fonctionner
  - Feature Set: correspond à l'ensemble des fonctionnalités incluses dans l'image
  - Format: permet de connaître le format de conditionnement de l'image
  - Version: est le numéro de version de l'image IOS

Noms des fichiers IOS

- Exemple 1 :

  c2600-ik9s-mz.122-40a.bin

  - c2600 : pour un routeur de la gamme Cisco 2600
  - i : IP
  - k9: cryptographie forte (3DES, AES)
  - s : fonctionnalités plus
  - m : l'image s'exécute en RAM
  - z : l'image est compressée selon le format zip
  - 122-40a : pour le numéro de version de l'image IOS
  - bin : extension de fichier

Noms des fichiers IOS

- Exemple 2:

  c1900- universalk9-mz.SPA. 152-4.M3 .bin

  - c1900 : pour un routeur de la gamme Cisco 1900
  - universalk9 : indique la désignation de l'image.
    - Les deux désignations d'un routeur ISR G2 sont universalk9 et universalk9_npe.
      - Universalk9_npe ne contient pas de chiffrement fort
  - m : l'image s'exécute en RAM
  - z : l'image est compressée selon le format zip
  - SPA : le fichier est signé numériquement par Cisco.
  - 152-4.M3 : pour le numéro de version de l'image IOS
  - bin : extension de fichier

Fichiers de configuration

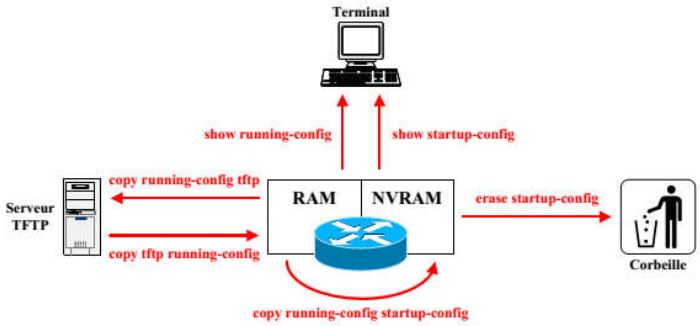
- Dans un routeur Cisco (en général), il existe différents fichiers de configuration
  - Il y a un fichier de configuration dans la NVRAM (startup-config), qui est lu au démarrage du routeur
  - startup-config est copié dans la mémoire vive (et devient la “running-config”)
- La “startup-config” est conservée dans la NVRAM sous forme ASCII.
- La “running-config” est conservée dans la RAM sous forme binaire

Fichiers de configuration

- 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.
  - Chaque interface avec sa configuration spécifique.
  - Toutes les informations de routage.
  - Chaque ligne et sa configuration spécifique.

Fichiers de configuration

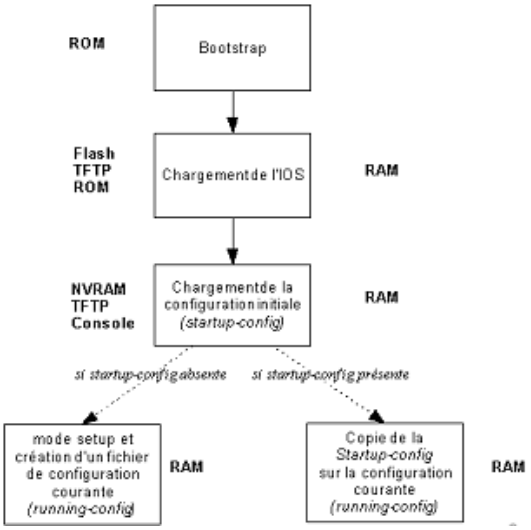
- Commandes (IOS >= 11) associées aux fichiers de configuration



Boot du routeur

- Le boot du routeur est constitue des phases suivantes :
  - POST
  - chargement du bootstrap
  - recherche et chargement de l'IOS
  - recherche et chargement du fichier de configuration ou accès en mode Setup

Séquence de démarrage



Processus de démarrage d'un routeur Cisco

Atelier

GNS3

- GNS3 se définit comme un simulateur de réseau graphique.
- Mais en réalité, il s'agit plutôt d'une interface qui facilite la mise en œuvre de Dynamips

GNS3

GNS3

- GNS3 signifie Graphical Network Simulator et est composé entre autre des outils suivants :
  - Dynamips : Emulateur de routeur physique.
  - Dynagen : Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.

Command Line Interface (CLI)

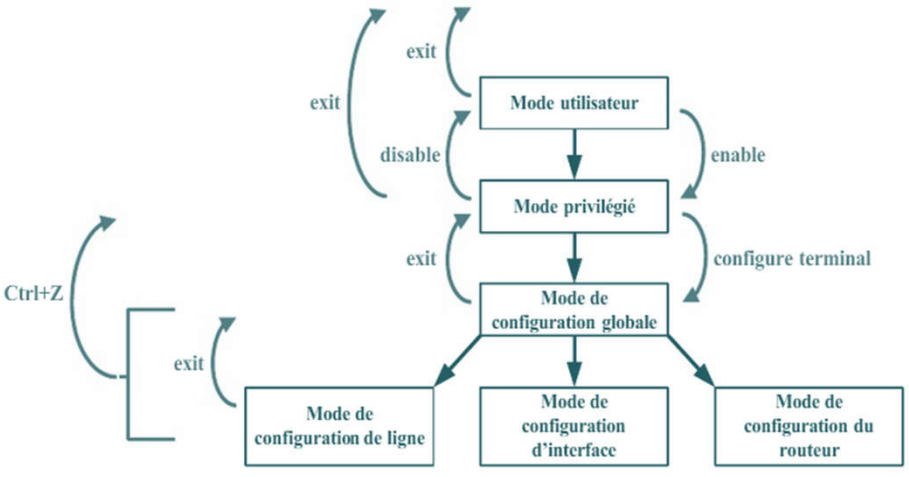
- La CLI (Command Line Interface) est l'interface entre l'utilisateur ou l'administrateur et l'IOS (Internetwork Operating System).
  - Par analogie aux systèmes Unix, la CLI est un shell (assez basique), alors que l'IOS est le système d'exploitation.
- La CLI lit des commandes utilisateur et demande à l'IOS de réaliser les actions correspondantes.

Command Line Interface (CLI) : Hiérarchie

- Modes du routeur : C'est une façon de protéger l'équipement

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

Modes du routeur



Command Line Interface (CLI) : Hiérarchie

- Mode Utilisateur

I. Mode utilisateur (User EXEC mode)	
Invite	Router>
Accès	Mode par défaut au démarrage
Description	Informations très limitées sur le routeur

Command Line Interface (CLI) : Hiérarchie

- Mode Privilégié

II. Mode privilège (Privileged EXEC mode)	
Invite	Router#
Accès	Router>**enable**
Description	Informations détaillées et toutes commandes qui ne configurent pas le routeur

Command Line Interface (CLI) : Hiérarchie

- Mode Configuration globale

III. Mode configuration globale (Global Configuration mode)	
Invite	Router(config)#
Accès	Router#**configure terminal**
Description	Configuration générale et globale du routeur

- Le mode configuration global possède des niveaux spécifiques dont, entre-autres :
  - Mode Configuration des interfaces
  - Mode Configuration des lignes
  - Mode Configuration du routage

Command Line Interface (CLI) : Hiérarchie

- Mode Configuration des interfaces

III. 1. Configuration des interfaces	
Invite	Router(config-if)#
Accès	Router(config)#**interface FastEthernet 0/0**, par exemple ou Router(config)#**interface serial 0/3/0**
Description	Configuration spécifique des interfaces

Command Line Interface (CLI) : Hiérarchie

- Mode Configuration des lignes

III. 2. Configuration des lignes (ports)	
Invite	Router(config-line)#
Accès	Router(config)#**line console** , par exemple ou Router(config)#**line aux**
Description	Configuration spécifique des lignes (ports)

Command Line Interface (CLI) : Hiérarchie

- Mode Configuration du routage

III. 3. Configuration du routage	
Invite	Router(config-router)#
Accès	Router(config)#**router rip** , par exemple ou Router(config)#**router igrp 100**
Description	Configuration spécifique du routage

- NB:
  - *exit* permet de sortir d'un mode et de revenir au précédent
  - *ctrl+z* ramène au mode privilège

Attribution d'un nom d'hôte

- Pour donner un nom à un routeur visible dans l'invite :
  - Router(config)#*hostname* name
- Par exemple :
  - Router(config)#hostname R1
  - R1(config)#

Configurer la bannière d'accueil

- Pour ajouter une bannière :
  - Router(config)# banner motd [delimited char] <message> [delimited char]
- Exemple :
  - Routeur(config)#banner motd #
  - Enter TEXT message. End with the character '#'.
  - **********
  - * ATTENTION *
  - * Acces reserve aux personnes autorisees *
  - * Toute activite illicite fera l'objet d'un recours en justice*
  - **********#

Historique de commande

- L'IOS maintient un historique des dernières commandes entrées.
- Par défaut, les dix dernières commandes. Pour changer ce nombre :
  - Router#*terminal history size* nombre
- Par exemple :
  - Router#*terminal history size* 30

Command Line Interface: système d'aide

- La commande ? donne la liste des commandes disponibles dans un mode.
- Par exemple :
  - Router>?
- Une commande incomplète suivie de ? donne les disponibilités
- Par exemple :
  - Router#co?
  - configure connect copy

Command Line Interface: système d'aide

- Une commande entière suivie de ? donne la liste des paramètres suivants immédiats
- Par exemple :
  - Router#configure ?

```
memory  Configure from NV memory
network Configure from a TFTP network host
overwrite-network Overwrite NV memory from TFTP
          network host
replace     Replace the runnin-config with a new config file
terminal    Configure from the terminal
```

- Une commande erronée est renseignée :
  - Router#shaw running-config

```
          ^% Invalid input detected at '^' marker.
```

Commandes abrégées

- On peut abréger certaines commandes.
- Quelques exemples:
  - Router# sh ip int br
    - à la place de Router# show ip interface brief
  - Router# copy run start
    - à la place de Router# copy running-config startup-config

Obtenir des informations

- La commande show
  - show running-config: la configuration courante
  - show startup-config: la configuration en mémoire
  - show interface nomInterface: la configuration de l'interface
  - show ip interface brief: vue d'ensemble des interfaces
  - show ip protocols: les protocoles de routage
  - show ip route: les tables de routage
  - show ip access-lists: les ACLs
  - show ip nat translations: le NAT
  - show ip dhcp binding: les réservations DHCP
  - show version: version d'IOS

Obtenir des informations : Show version

- La commande show version donne :
  - version de l'IOS
  - version du bootstrap
  - emplacement de l'IOS
  - CPU
  - quantité de RAM
  - interfaces
  - quantité de NVRAM
  - quantité de Flash
  - registre de configuration

Configuration des interfaces

- En mode configuration :
  - sélection
    - *interface nomInterface*
  - adresse IP
    - ip address adresseIP masqueSousReseau
  - Commentaire
    - description
  - Activation
    - no shutdown

Configuration des interfaces : Exemple

- Interface LAN
  - Router(config)# interface Fastethernet 0/0
  - Router(config-if)# ip address 192.168.1.1 255.255.255.0
  - Router(config-if)# description “mon reseau local"
  - Router(config-if)# no shutdown
- Interface WAN
  - Router(config)# interface s0/0
  - Router(config-if)# ip address 192.168.1.1 255.255.255.0
  - Router(config-if)# no shutdown
  - Router(config-if)# description “lien loue 64k“
  - Router(config-if)# bandwidth 64

Mots de passe

- Pour configurer une protection par mot de passe sur une ligne, il faut utiliser les commandes suivantes :
  - line {console | aux | vty} {{numéro} | {premier} {dernier}}
  - password {mot de passe}
  - login
- Exemple : Mot de passe de console
  - Router(config)# line con 0
  - Router(config-line)# password Pa$$wordConsole
  - Router(config-line)# login
- Exemple : Mot de passe du port auxiliaire
  - Router(config)# line aux 0
  - Router(config-line)# password Pa$$wordAux
  - Router(config-line)# login

Mots de passe

- Exemple : Mot de passe du terminal virtuel
  - Router(config)# line vty 0 4
  - Router(config-line)# password Pa$$wordTelnet
  - Router(config-line)# login

Mots de passe

- On peut aussi restreindre l'accès au mode privilégié en utilisant au moins une de ces commandes :
  - enable password {mot de passe}
    - Le mot de passe sera écrit en clair dans le fichier de configuration
  - enable secret {mot de passe}
    - Le mot de passe sera crypté dans le fichier de configuration en utilisant l'algorithme MD5.

Mots de passe

- Malheureusement, tous les mots de passe, à l'exception du *enable secret*, sont écrits en clair dans le fichier de configuration.
- la commande service password-encryption permet de crypter tous les mots de passe écrits en clair dans le fichier de configuration en utilisant un algorithme propriétaire Cisco.

Configuration d'une route statique

- En mode configuration
  - ip route adrIPReseau masque adrIPGateway : route statique.
- Par exemple : (route par défaut)
  - Router(config)# ip route 0.0.0.0 0.0.0.0 10.10.15.1