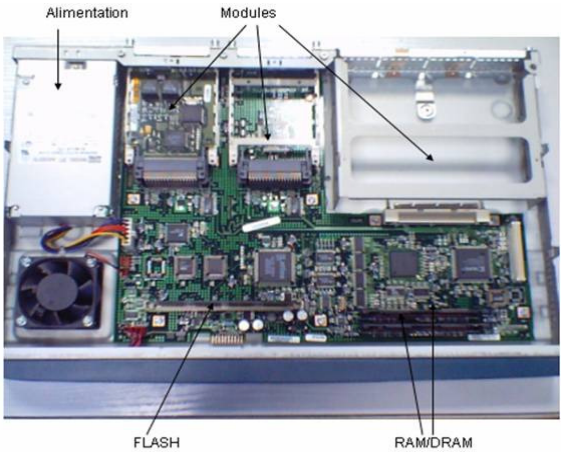
Introduction aux routeurs CISCO

Jean Robert HOUNTOMEY

Table des Matières

Les composants d'un routeur

Les composants d'un routeur



Les composants d'un routeur (2)

Comme un ordinateur un routeur est composé du:
materiel (hard)

- **Le Microprocesseur (CPU)** L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation du routeur.
- **Mémoire Flash:** La flash représente une sorte de ROM effaçable et programmable. Sur beaucoup de routeurs, la flash est utilisé pour maintenir une image d'un ou plusieurs systèmes d'exploitation.
- **ROM:** La ROM contient le code pour réaliser les diagnostics de démarrage (POST : PowerOn Self Test). En plus, la ROM permet le démarrage et le chargement du système d'exploitation contenu sur la flash.

Les composants d'un routeur (3)

- **Bootstrap** – stocké dans le microcode du ROM – boot le routeur durant l'initialisation et démarre l'IOS.
- **POST** – Power On Self Test – dans le microcode du ROM microcode il vérifie les fonctionnalités basique du matériel et détermine les interfaces présentes.
- **ROM Monitor** – utilisé pour le manufacturing, les tests et le troubleshooting
- **Mini-IOS** – a.k.a RXBOOT/boot loader par Cisco – c'est une petite version d'IOS (small IOS ROM) utilisée pour activer les interfaces et pour charger le IOS CISCO en mémoire flash à partir d'un serveur TFTP. Est aussi utilisé pour des taches de maintenance.

Les composants d'un routeur (4)

- **RAM** La RAM est utilisé par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir la configuration qui s'exécute (running) , les tables de routage, la table ARP, etc. Et comme c'est de la mémoire volatile, lors de la coupure de l'alimentation, elle est effacée.
- **NVRAM** (RAM non volatile) Le problème de la RAM est la non conservation des données après la coupure de l'alimentation. La NVRAM solutionne le problème, puisque les données sont conservées même après la coupure de l'alimentation.

  La configuration est maintenue dans la NVRAM.
- **Modules (Portes I/O):** L'essence même d'un routeur est l'interfaçage vers le monde extérieur. Il existe un nombre impressionnant d'interfaces possibles pour un routeur

  (Liaison série asynchrone, synchrone, Ethernet, tokenring, ATM,FO, ...).

Les composants d'un routeur (5)

- **Le Registre de configuration:** invoqué par **Config-Register**
  - Controle comment le routeur démarre;
  - Valeur affichée par **"show version"** ;
  - 0x2102, indique au routeur de charger l'IOS de la mémoire flash et le startup-config de la NVRAM
- Modifier le **config-register** pour:
  - Forcer le routeur à demarrer en ROM Monitor
  - Booter sur une autre source et charger un ficher de démarrage par défault
  - Activer/désactiver la fonction **BREAK**
  - Controler les adresses de broadcast
  - Fixer le baud rate de la console terminal
  - Charger le IOS de la ROM
  - Activer le boot par serveur TFTP

Les composants d'un routeur (4)

logiciel (SOFT): Système d'exploitation appelé IOS (Internetworking Operating System)

Éléments essentiels de l'IOS

IOS Software releases utilise le format **A.B(C)D** ou :

* A, B, et C sont des nombres
* D (si présent) est une lettre
* A.B sont des nombres importants par rapport a la version.
* C est la version de mise a jour.(maintenance version).
* D si présent indique que ce n'est pas une version majeure mais une extension d'une version majeure. Ces extensions apportent de nouvelles fonctionnalités et gèrent de nouveaux matériels.

L'interpréteur de commande

- L'interpréteur de commande, comme son nom l'indique, est responsable de l'interprétation des commandes que vous tapez.

- La commande interprétée, si elle est correcte, réalise
  l'opération demandée. Si incorrecte renvoie un message d'erreur

Les facilités de l'IOS

L'IOS de CISCO permet des raccourcis aux commandes

- **Nomination et abréviations des interfaces :**
  - **ethernet0/0, ou e0/0, fastethernet0 ou fa0**
  - **serial0, ou s0**

- Raccourci des commandes:
  - **router#conf t**
  - **router(config)#int e0**
  - **router(config-if)#ip addr 81.199...**

- TAB pour Compléter une commande
  - **Router(config)#int<TAB>**
  - **Router(config)#interface fa <TAB>**
  - **Router(config)#interface fastEthernet**
  - **Router(config-if)#ip add<TAB>**
  - **Router(config-if)#ip address**

L'aide de l'IOS

IOS aide en cas d'oubli des commandes en les affichant ou les complétant

- "?" après le prompt pour une liste des commandes possibles

  - **router#?**

- "<commande partielle> ?" liste les options et les commandes complémentaires; ex:

  - **router#show ?**
  - **router#show ip ?**

L'aide de l'IOS (2)

- **router(config)#ip a?**
- **accounting-list accounting-threshold accounting-transits address-pool alias as-path**

- **router(config)#int e0**
- **router(config-if)#ip a?**
- **access-group accounting address**

- **router(config-if)#ip addr ?**
- A.B.C.D IP address

- **router(config-if)#ip addr 196.200.221.0 ?**
- A.B.C.D IP subnet mask

Le fonctionnement du routeur

Processus de démarrage du routeur

- **POST chargé à partir de la ROM effectue le diagnostique des mémoires, des modules et des composants hard du routeur**
- **Bootstrap – vérifie et démarre l'IOS; par défault l'IOS est chargé de la FLASH**
- **Startup-config si trouvé dans la RAM est chargé sinon le routeur démarre en mode setup.**

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]:
```

Procédure de configuration du routeur

Configurer son routeur c'est agir sur le fonctionnement de ce dernier et le contrôler.

Procédure de configuration

- Assignation d'identité (nom) au routeur (*hostname*)
- Mots de passe d'accès
- Configuration des interfaces
- Bonnes pratiques – Sécurité
- Connexion du routeur au réseau
- Configuration des protocoles de routage (static – dynamique ou défault)
- Sauvegarde dans la NVRAM
- Sauvegarde sur un serveur externe (facultatif mais utile)

contexte de configuration

Plusieurs contextes de configuration

NB: Tous les contextes de configurations sont effectués en mode privilégié.

- **global**
  - **mode de fonctionnement général**
- **interface**
  - **configuration des interfaces**
- **Router**
  - **protocole de routage**
- **line (mode de connexion)**
  - **line vty 0 4**

Mode de Configuration générale

- Configuration générale (contexte global)

router>
router>enable
password
router#

- Lorsque vous désirez passer en mode configuration, vous devez taper (en mode enable) :

router# configure terminal
router(config)#

(Vous êtes dans la racine de la configuration du routeur et vous pouvez configurer les paramètres Généraux)

Mode de Configuration des interfaces

- **Configuration des interfaces**

- **Interface Ethernet ou fastethernet**

- Pour configurez les interfaces, on passe du mode configuration générale vers la configuration de l'interface.
  - **router> enable**
  - **password :**
  - **router#configure terminal**
  - **router(config)#interface ethernet 0 (ou fa0/0…)**
  - **router(config-if)#ip address 196.200.221.125 255.255.255.192**
  - **router(config-if)#exit**
  - **router(config)#exit**
  - **router#**

Configuration des interfaces

- **Interface loopback**
- Pour faciliter les tâches de routage, de gestion du routeur on utilise l'interface virtuelle (logicielle) loopback. **Ne change jamais d'état.**
- **router> enable**
- **password :**
- **router#configure terminal**
- **router(config)#interface loopback 0**
- **router(config-if)#ip address x.x.x.x 255.255.255.255**
- **router(config-if)#exit**
- **router(config)#exit**
- **router#**

Configuration des interfaces

- **Interface loopback**
- Pour faciliter les tâches de routage, de gestion du routeur on utilise l'interface virtuelle (logicielle) loopback. **Ne change jamais d'état.**
- **router> enable**
- **password :**
- **router#configure terminal**
- **router(config)#interface loopback 0**
- **router(config-if)#ip address x.x.x.x 255.255.255.255**
- **router(config-if)#exit**
- **router(config)#exit**
- **router#**

Configuration des interfaces

- **Interface null 0**

  Associée a **/dev/null** cette interface poubelle vous permet par exemple:

  - de désactiver un client en envoyant le block du client vers null0

- de router tout ce que vous ne voulez pas accepter vers null0
- De bloquer vos annonces bgp surtout si vous recevez un grand bloc dont une partie n'est pas utilisée.

contexte de configuration

- Configuration des lignes VTY
- Il existe aussi différent types d'interfaces à configurer. Par exemple, la configuration des interfaces virtuelles (pour l'accès via telnet) se fait de la même manière que les interfaces.

```
router>enable
password :
router#configure terminal
router(config)#line vty 0 4
router(config-line)#exec-timeout 5 0
router(config-line)#exit
router(config)#exit
router#
```

Dans quel contexte suis-je ?

- **Router(config-route-map)#** - route-map configuration prompt
- **Router(config-router)#** - routage configuration prompt
- **Router(config-line)#** - line configuration prompt
- **rommon 1>** - ROM Monitor mode

Configuration de base du routeur

- Sauvegarde de la configuration sur le routeur

tablex #copy running-config startup-config

Ou

Write memory

- Sauvegarde de la configuration sur une machine externe - Installer un serveur tftp sur la machine qui doit recevoir le configuration

```
tablex #copy running-config tftp
Address or name of remote host []?
Destination filename [router-confg]?
```

Configuration de base du routeur

Routage statique

- Route par défaut
  - **tablex(config)# ip route 0.0.0.0 0.0.0.0 196.200.221.124**
- Route explicite
  - **tablex(config)# ip route 196.200.221.216 255.255.255.248 196.200.221.68**

Suppression de la configuration

Pour effacer la configuration du routeur

tablex#erase startup-config
ou
tablex#write erase
tablex#reload

- Le routeur démarre à nouveau en mode setup

Procédure de configuration

1. Entrer en mode privilege

```
Router>en
Router#
```

2. Entrer en mode config

```
Router#conf t
Enter configuration commands, one per line.  End with
    CNTL/Z.
Router(config)#
```

3. Assignation d'identité (nom) au routeur (*hostname*)

```
Router(config)#hostname brd-afnog
brd-afnog(config)# (noter le prompt)
```

4- Mots de passe secret

```
brd-afnog(config)#enable secret goraf
brd-afnog(config)#
```

Procédure de configuration

5.Mot de passe sur la console

```
brd-afnog(config)#line cons 0
brd-afnog(config-line)# default login local
brd-afnog(config-line)#password afnog
```

Notes: le routeur va demander le mot de passe a la prochaine connexion console Press RETURN to get started.

```
User Access Verification

Password:
Router>
```

Procédure de configuration

6. Configuration des interfaces.

```
brd-afnog(config)#interface fa0/1
brd-afnog(config-if)#description lien-vers-bb
brd-afnog(config-if)#ip address 196.200.221.80 255.255.255.192
brd-afnog(config-if)#no shutdown
brd-afnog(config-if)#
```

7. Sauvegarde de la config

```
brd-afnog(config-if)#
brd-afnog(config-if)#^Z
brd-afnog#
brd-afnog#copy run startup-config
Destination filename [startup-config]
Building configuration...
[OK]
brd-afnog#
```

Procédure de configuration

- Sauvegarde sur un serveur externe (facultatif mais utile)

```
brd-afnog#copy running-config tftp
Address or name of remote host []? 196.200.216.78
Destination filename [brd-afnog-confg]?
!!
1763 bytes copied in 1.108 secs (1591 bytes/sec)
brd-afnog#
```

Brd-afnog-confg etant le fichier de config

196.200.216.78 etant le serveur tftp

Les fichiers de configuration

Un routeur a toujours deux configurations:

- La configuration active (*running configuration*)
  - dans la RAM, il détermine le fonctionnement du routeur
  - changée en utilisant la commande configure
  - pour la voir: show running-config
- La configuration de démarrage (*startup configuration*)
  - dans la NVRAM, détermine le fonctionnement du routeur après le prochain démarrage
  - modifiée par la commande copy
  - pour la voir: show startup-config

Ou se trouve la configuration ?

La configuration du routeur peut aussi être sauvegarde dans différents endroits:

`Machines externes (tftp)`

`En mémoire flash`

Les commandes de copy

```
copy run start
copy run tftp
copy start tftp
copy tftp start
copy flash start
copy start flash
```

Modes d'Exécution ou d'Accès

1. Le mode utilisateur ou **User EXEC Mode (Router>)**

Le mode utilisateur sert uniquement à la visualisation des paramètres (pas de la configuration) et des différents statuts du routeur.
Lors de la connexion initiale avec le routeur, vous arrivez dans le mode utilisateur.

2. Le mode privilégié ou **Privileged EXEC mode (Router#)**

Le mode privilégié permet,en plus de la visualisation des paramètres, la configuration du routeur et le changement de paramètres dans la configuration.Mais aussi des tests et debugging.

3. Le mode **ROM Monitor** – Utile pour retrouver les mots de passe d'accès et pour le chargement de nouveaux IOS

4. Le mode **Setup** – retrouvé sur les routeurs n'ayant pas de configuration

Source de configuration

- Console
  - Accès à partir d'un PC via port série
- Port Aux / Auxiliary port
  - Acces par Modem
- Terminaux virtuels / Virtual terminals
  - Acces Telnet/SSH
- Serveur TFTP
  - Copie de la configuration file dans RAM/NVRAM
- Logiciels de Gestion réseau
  - e.g. CiscoWorks

Changer la Configuration

- Immédiatement en entrant les commandes manuellement (Attention aux commandes car changement immédiat de la running config mais pas de la startup config) ceci en se connectant par SSH/TELENET ou Console.

- En éditant un fichier texte sur un serveur TFTP et en le chargeant sur le router par tftp – copy tftp start

Connexion au routeur

Avant de configurer son routeur il faut se connecter dessus:

- Connexion série par le port console (le mode par défaut exécuté la première fois que le routeur est déballé)

  Se fait grâce a un câble dit console fourni par CISCO avec

  le routeur. Le câble console a un connecteur série d'un bout et RJ45 a l'autre.

NB: Paramètres pour la connexion série

9600 baud – 8 bits de données – sans parité – 1 bit stop – pas de contrôle d'erreur

Connexion au routeur (2)

-Sous Windows: utiliser hyper terminal

Il existe d'autres utilitaires comme secureCRT
http://www.vandyke.com/products/securecrt/index.html

-Sous FREEBSD

la commande **tip com1** (com1 étant le port sur lequel est connecte le routeur)

Pour sortir de la console du routeur: **~.**

TP: Connecter vous sur vos routeurs via la console

Dans quel contexte suis-je ?

Pour savoir dans quel contexte de config on se trouve, se référer au prompt.

- **Router>** – USER prompt mode
- **Router#** – PRIVILEGED EXEC prompt mode
- **Router(config)** – terminal configuration prompt
- **Router(config-if)** – interface configuration prompt

Mieux connaître son routeur

- La commande show version

```
Router>show version
Processeur:cisco 2611 (MPC860) processor (revision 0x202) with
    26624K/6144K bytes of memory
```

- Mémoire RAM. Ajouter les deux chiffres pour avoir la mémoire totale : RAM= 26624+6144=32768
- Interface Ethernet: 2 Ethernet/IEEE 802.3 interface(s)
- Interface série: 2 Serial network interface(s)
- Mémoire FLASH: 8192K bytes of processor board System flash partition
- Registre de configuration: Configuration register is 0x2102

Mieux connaître son routeur

- La commande show version
- **Router>show version**

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(21a)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 29-Sep-08 16:02 by prod_rel_team ……

Cisco 2811 (revision 53.51) with 249856K/12288K bytes of memory.
Processor board ID FTX1320A22H
2 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
62720K bytes of ATA CompactFlash (Read/Write)
Configuration register is 0x2102
sif-rtr>
```

Les Bonnes pratiques

Comment choisir son routeur

Le choix d'un routeur se base aussi bien sur le matériel que l'IOS

- **Selon le type d'activités**
- **Selon les fonctionnalités à donner aux utilisateurs**
- **Selon les projets d'extension à moyens termes**

Mot de passes

- Assignation du mot de passe de privilège:
  - **router(config)# enable secret afnog *(MD5 encryption)***
  - NB: l'ancienne commande **enable password** n'est plus utilisée.
- Cryptage des mots de passe: les Mots de passe apparaissent en clair dans la configuration du routeur ce qui est dangereux
  - **router(config)# service password-encryption**

Désactiver les services a risques

- **Router(config)#no ip finger**
  Désactive l'écoute des requêtes finger d'hôtes distants
- **Router(config)#no service udp-small-servers**
- **Router(config)#no service tcp-small-servers**
  Désactive les serveurs TCP et UDP dont les ports sont inférieurs a 20
- **Router(config)#no ip bootp server**
- **Router(config)#no cdp run**
  Si CDP est nécessaire en interne, on peut l'activer et dans ce cas on le désactive sur les interfaces externes
- **Router(config)#cdp run**
- **Router(config)#int serial 0/0**
- **Router(config-if)#no cdp enable**

Désactiver les services a risques

- **Router(config)#no ip source-route**

Source route autorise un paquet à spécifier comment il doit être routé dans un réseau plutôt que passer par les routeurs désignés par le routage interne. A utiliser sauf si considérations particulières et si vous savez ce que vous faites

Règles de sécurité des interfaces

- **no ip redirects** : *ICMP REDIRECT autorisent la modification de la manière dont les paquets transitent dans le réseau. Via ICMP redirects un hacker peut rediriger le traffic vers un routeur de son choix et donc monitorer ou enregistrer ou faire des attaques.*
- **no ip proxy-arp**: *Proxy ARP est défini dans le RFC 1027 et est utilisé par le routeur pour permettre aux machines n'ayant pas de fonctionnalité de routage ou de routeur par défaut. La machine envoie un ARP sur le réseau et le routeur répond en lui envoyant son adresse mac comme adresse à utiliser .*

Règles de sécurité des interfaces

- **no ip directed-broadcast**: *empêcher ICMP Directed broadcast c'est empecher votre routeur de relayer un ping envoyé à l'adresse broadcast. voir attaque SMURF.*

Banner et Contrôle de l'accès au routeur

- Il est indispensable de contrôler qui accède au routeur. Plusieurs méthodes sont possibles: RADIUS; TACACS+ où les utilisateurs sont crées sur des serveurs externes.
- Utiliser AAA pour créer des utilisateurs locaux si pas besoin de serveurs externes. AAA = Authentication, authorization, accounting.

- Création de username et de password
  - **Router(config)#username f2 password afnog**

- Message a afficher pour un utilisateur qui se trompe

  - **aaa authentication fail-message *vous n'etes probablement pas autorise a vous connecter a ce routeur***

Banner et Contrôle de l'accès au routeur

- **Router(config)#aaa new-model**
- **Router(config)#aaa authentication login default local**
- **Router(config)#line vty 0 4**
- **Router(config-line)#login authentication default**
- **Router(config-line)#exit**
- **Router(config)#line con 0**
- **Router(config-line)#login authentication default**
- **Router(config-line)#exit**
- **Router(config)#**

Banner et Contrôle de l'accès au routeur

- Le banner est un message a l'endroit de l'utilisateur qui se connecte. Tous vos routeurs doivent en avoir.
- Un bon banner doit avoir 4 objectifs:
  - Être suffisamment légal pour poursuivre les utilisateurs non autorisés
  - Informer que les sessions sont monitorées et enregistrées
  - Ne pas transporter des informations qui pourraient être utilisées par un utilisateurs malveillant
  - Protéger les administrateurs, situer les responsabilités