Introduction aux routeurs CISCO

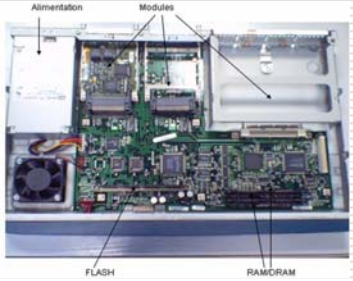
Jean Robert HOUNTOMEY
AFNOG 2006 - NAIROBI - KENYA
hrobert@iservices.tg

Table des Matières

Légende:
En noir les commandes IOS
En bleu le cours

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)

- 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 RAM, 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 (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.

Les composants d'un routeur (5)

- ED "Early Deployment". Early Deployment nouvelles fonctionnalités, supporte de nouvelles plates formes ou interfaces.
- GD "General Deployment". Version majeure devient GD quand CISCO juge que la version de l'IOS peut être utilisée en terme général. Une version deviens majeure lorsque tous les tests de stabilité et de performance ont été concluants
- LD "Limited Deployment". Une version majeure de IOS est déclarée LD entre la première vente de la période de GD.
- DF "Deferred". DF a ne pas utiliser car contient beaucoup de bugs

NB: Il est recommandé une version GD ou ED

- IOS (tm) C2600 Software (C2600-P-M), Version 12.0(21)S6, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

Connexion au routeur

Avant de configurer son routeur il faut se connecter dessus:

- Connexion série par le port console (le mode par défaut)
  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.
- telnet sur les terminaux virtuels
- Connexion par modem sur le port auxiliaire

NB: Paramètres pour la connexion série

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

http://www.cisco.com/warp/public/701/14.html

Connexion au routeur (2)

- Sous Windows: utiliser hyper terminal

Il existe d'autres utilitaires sur Internet 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: **~.**

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

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.

Les facilites de l'IOS

L'IOS de CISCO permet des raccourcis aux commandes

- **Nomination et abréviations des interfaces :**
  - Ethernet0/0, ou e0/0
  - 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 et**<TAB>**
  - Router(config)#interface ethernet 0
  - 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

- **diagnostique des mémoires et des modules**
- **vérification et démarrage de l'IOS**
- **Chargement des fichiers contenus dans la NVRAM (startup config)**

Modes d'Exécution

- Il y a 2 modes d'exécution sur un routeur Cisco :
  1. Le mode utilisateur (prompt : >)
  2. Le mode privilégié (prompt : #)
- Lors de la connexion initiale avec le routeur, vous arrivez dans le mode utilisateur.
- Pour passer au mode privilégié, vous devez introduire la commande enable et ensuite introduire un mot de passe.
- Le mode utilisateur sert uniquement à la visualisation des paramètres (pas de la configuration) et des différents statuts du routeur.
- Par contre, le mode privilégié permet,en plus de la visualisation des paramètres, la configuration du routeur et le changement de paramètres dans la configuration.

Modes d'Exécution (2)

NB: il existe un mode special don't on ne parle pas souvent:

- Mode ROM – nécessaire pour retrouver les mots de passe
  Voir restauration des mots de passe

Les fichiers de configuration

Un routeur a toujours deux configurations:

•La configuration active (*running configuration*)

dans la RAM, il détermine le fonctionnement du routeur

Peut être changée en utilisant la commande de configuration. Pour la voir: show running

•La configuration de démarrage (*startup configuration*)

dans la NVRAM, détermine le fonctionnement du routeur après le prochain démarrage

Est changée par la commande copy

Pour le voir: show startup

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

Procédure de configuration du routeur

Procédure de configuration

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

Procédure de configuration (2)

contexte de configuration

Plusieurs contextes de configuration

- global
  - mode de fonctionnement général
- interface
  - configuration des interfaces
- Router
  - protocole de routage
- line (mode de connexion)
  - line vty 04

Procédure de configuration (3)

Configuration générale

- **Configuration générale (contexte global)**
- Lorsque vous désirez passer en mode configuration, vous devez taper (en mode enable) :
  - conf terminal (Cela signifie que vous configurer le routeur en mode terminal).
  - A ce moment le prompt change en : router(config)#
- Donc vous êtes dans la racine de la configuration du routeur et vous pouvez configurer les paramètres généraux

Procédure de configuration (4)

Configuration des interfaces

- **Configuration des interfaces**
- **Interface Ethernet**
- 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
  - router(config-if)#ip address 196.200.221.124 255.255.255.224
  - router(config-if)#exit
  - router(config)#exit
  - router#copy running-config startup-config

Procédure de configuration (5)

Configuration des interfaces

- **Configuration des interfaces**
- **Interface série**
- 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 serial 0
  - router(config-if)#ip address x.x.x.x y.y.y.y
  - router(config-if)#exit
  - router(config)#exit
  - router#copy running-config startup-config

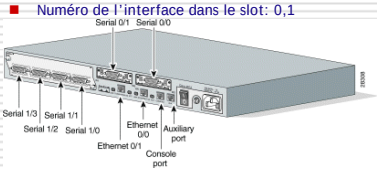
Procédure de configuration (6)

Configuration des interfaces

- **Nomenclature des interfaces**

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/index.htm

- Quand vous avez plusieurs interfaces sur un routeurs:
  - Notion de slot (emplacement): 0,1,2,3
  - Numéro de l'interface dans le slot: 0,1



Procédure de configuration (7)

Configuration des interfaces

- **Interface loopback**
- Pour faciliter les taches de routage, de gestion du routeur on utilise l'interface virtuelle (logicielle) loopback.
  - 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#copy running-config startup-config

Procédure de configuration (8)

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.

Procédure de configuration (9)
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 15 0
  - router(config-line)#exit
  - router(config)#exit
  - router#

Procédure de configuration (10)
Configuration des protocoles de routages

- **Configuration des protocoles de routages**
- La configuration des protocoles de routage est réalisée de la même manière que les interfaces.
  - router leprotocolederoutage

- router>enable
- password :
- router#configure terminal
- router(config)#router ospf 2006
- router(config-router)#network 196.200…
- router(config-router)#exit
- router(config)#exit
- router#

Configuration de base du routeur

Configuration de base du routeur

- Connexion par le port console
  - router>
  - router>enable
  - Password (si il n'en a pas le routeur passe en mode privilège)
  - router#

- Configuration
  - router# configure terminal
  - router(config)#

NB: Pour annuler une commande faire no suivi de la commande

Configuration de base du routeur

- Assignation d'identité
  router(config)# hostname tablex *(x est votre numéro de table)*

- Assignation du mot de passe de privilège:
  - tablex(config)# enable secret afnog06 *(MD5 encryption)*
  - NB: la commande *enable password* n'est plus utilisée car non sécurisée
  - Ce mot de passe apparaît en clair dans la configuration du routeur ce qui est dangereux.

- Assignation d'adresse IP aux interfaces
  - Assignation d'IP a l'interface ethernet
  - tablex(config)# interface ethernet0/0 *(ou 0)*

Configuration de base du routeur

- **Assignation d'une adresses IP**
- router(config-if)# ip address 196.200.221.x 255.255.255.y

Démarrage de l'interface

- router(config-if)# no shutdown
- router(config-if)# ^Z

- Assignation d'IP au loopback
- tablex(config)# interface loopback 0
- *Etc…(voir plus haut)*

NB Arrêt d'une interface

- router(config-if)# shutdown

Configuration de base du routeur

- Paramètres de la liaison console

Router(config)# line con 0
Router(config-line)# exec-timeout 5 0 (déconnecte la console si aucune action après 5 minutes 0 secondes)
Router(config-line)# ^Z

- Paramètres de la liaison auxiliaire

Router(config)# line aux 0
Router(config-line)# exec-timeout 5 0 (déconnecte la console si aucune action après 5 minutes 0 secondes)
Router(config-line)# ^Z

Configuration de base du routeur

- Paramètres des terminaux virtuels

Router(config)# line vty 0 4
Router(config-line)# exec-timeout 5 0 (déconnecte la console si aucune action après 5 minutes 0 secondes)
Router(config-line)# ^Z

Configuration de base du routeur

- Sauvegarde de la configuration sur le routeur

router#copy running-config startup-config

- Sauvegarde de la configuration sur une machine externe

Installer un serveur tftp sur la machine qui doit recevoir le configuration

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

Configuration de base du routeur

Routage statique

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

Les Bonnes pratiques

Les bonnes pratiques (1)

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 a donner aux utilisateurs**
- **Selon les projets d'extension a moyens termes**

Les bonnes pratiques (2)

Mot de passes

- Assignation du mot de passe de privilège:
  - router(config)# enable secret afnog06 *(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

Les bonnes pratiques (3)

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

Les bonnes pratiques (4)

Banner et Contrôle de l'accès au routeur

- Le banner est un message a l'endroit de l'utilisateur qui se connecte.
- Obliger quelqu'un qui veut se connecter au routeur a enter un nom d'utilisateur et un mot de passe.
- Message a la connexion au routeur
  - Router(config)#aaa new-model
  - Router(config)#aaa authentication banner *ROUTEUR D'AFNOGV*
  - Router(config)#aaa authentication login default local

  On peut aussi faire
  - banner login ^C
  - ce routeur est la propriété de AFNOG
  - déconnectez vous si vous n'etes pas des notres.
  - ^C

Les bonnes pratiques(5)

Banner et Contrôle de l'accès au routeur

- Création de username et de password
- NB: il existe des méthodes pour dire au routeur d'aller chercher les users sur un serveur externe RADIUS ou TACACS
  - 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 rouuteur*

Les bonnes pratiques (6)

Description des interfaces

Faire un commentaire sur les interface pour se retrouver
Description de l'interface (utile pour se retrouver)

router(config-if)# description vers backbone

Les bonnes pratiques (7)

Règles de sécurité des interfaces

- no ip redirects *: le routeur n'enverra pas de message de redirection si le IOS est force de renvoyer un paquet sur l'interface ou le paquet a été reçu*
- 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 a déterminer l'adresse Mac d'hôtes sur d'autres réseaux*
- no ip directed-broadcast*: voir attaque SMURF ; un broadcast vers un autre réseau peut être relaye par une interface de votre routeur*

Les bonnes pratiques(8)
Délais de connexion

- Paramètres de la liaison console
  Router(config)# line con 0
  Router(config-line)# exec-timeout 5 0
  (déconnecte la console si aucune action après 5 minutes 0 secondes)
  Router(config-line)# ^Z
- Paramètres de la liaison auxilliaire
  Router(config)# line aux 0
  Router(config-line)# exec-timeout 5 0
  (déconnecte la console si aucune action après 5 minutes 0 secondes)
  Router(config-line)# ^Z

Les bonnes pratiques (9)
Délais de connexion

- Paramètres des terminaux virtuels
  Router(config)# line vty 0 4
  Router(config-line)# exec-timeout 5 0
  (déconnecte la console si aucune action après 5 minutes 0 secondes)
  Router(config-line)# ^Z

Les bonnes pratiques (10)
Access list sur les VTY

- Autoriser seulement mes IP a se connecter par telnet
- Définir l'access list
  - Router(config)#access-list 16 permit 196.200.221.0 0.0.0.255
  - Router(config)#access-list 16 deny any
- Appliquer l'access list
  - Router(config)#line vty 04
  - Router(config-line)#access-class 16 in

Les bonnes pratiques(11)
se prémunir contre certaines attaques

- Contrôle anti spoofing sur les interfaces de bord
- (trafic entrant dans le routeur)
- on interdit les paquets bizarres
- On interdit les adresses prives
- Router(config)#access-list 111 deny ip host 0.0.0.0 any
- Router(config)#access-list 111 deny ip 127.0.0.0 0.255.255.255 any
- Router(config)#access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
- Router(config)#access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
- Router(config)#access-list 111 deny ip 192.168.0.0 0.0.255.255 any log

Les bonnes pratiques(12)
se prémunir contre certaines attaques

- On interdit a quelqu'un de venir de l'extérieur avec notre IP
- Router(config)#access-list 111 deny ip 196.200.221.0 0.0.0.255 any
- On autorise le reste
- Router(config)#access-list 111 pemit ip any any
- on applique l'acl sur l'interface connecte a l'extérieur
- Router(config)#int s0/0
- Router(config-if)#ip access-group 111 in
- Router(config-if)#

Les bonnes pratiques(13)
Autres Options

- La commande bandwidth
- Appliquer la commande bandwidth
- Le routeur pourra alors prendre ses décisions de routages
  - Router(config)#int s0/0
  - Router(config-if)#bandwidth 2048
  - Router(config-if)#
- Options spécifiques a IP:
  - router(config)# ip classless (on est en classless)
  - router(config)# ip subnet-zero

Les bonnes pratiques(14)

Contrôlez vos logs

- Contrôlez les logs de votre routeur en cas de connexion infructueuses.
- Les logs peuvent être déportées sur un autre serveur
  - **Router(config)#logging facility local7**
  - **Router(config)#logging 196.200.221.122**
  - Router(config)#