Introduction aux routeurs CISCO

Africa Network Operator's Group

Jean Robert HOUNTOMEY
AFNOG VI
MAPUTO 2005
hrobert@iservices.tg

Cisco Systems

Table des Matières

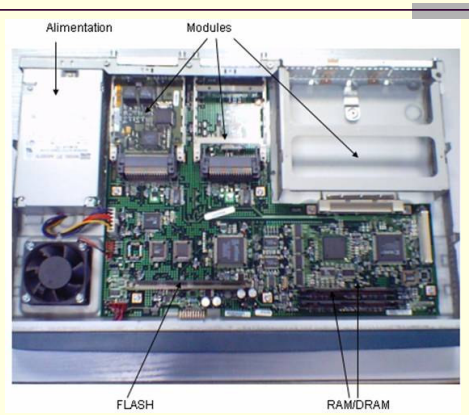
Africa Network Operator's Group

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)

Gère le matériel, les interfaces
Offre l'accès à un vaste éventail d'applications stratégiques de routage, multiservice, de modélisation de trafic, de sécurité/parefeu et de contrôle du trafic etc….

Choisir son Routeur

http://www.cisco.com/global/FR/products/routers/routers_home.shtml

Le Choix matériel

Dépend des applications et des fonctionnalités désirées et à offrir aux utilisateurs.

- Routeurs Ethernet, ADSL, ADSL sur RNIS et G.SHDSL pour petits bureaux et bureaux à domicile.
- Routeurs Ethernet, ADSL, ADSL sur RNIS, G.SHDSL, RNIS et série pour petits bureaux distants et télétravailleurs.
- Routeurs d'accès modulaires souples et sécurisés gamme 1700
- Routeurs à services intégrés de la gamme Cisco 1800

Choisir son Routeur (suite)

-Routeurs de la gamme Cisco 2600

-Routeurs à services intégrés de la gamme Cisco 2800

-Routeurs de la gamme Cisco 3700

-Routeurs à services intégrés de la gamme Cisco 3800

-Routeurs VPN de la gamme Cisco 7100

-Routeurs de la gamme Cisco 7200

Choisir son Routeur (suite)

Choisir son 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.

Choisir son Routeur (suite)

- 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)**

NB: a un moment vous serez peut être amené a changer votre version d'IOS pour des mises a jours de sécurité ou pour ajouter des fonctionnalités.

Choisir son Routeur (suite)

- À un certain stade, les versions GD sont remplacées par de nouvelles versions dotées des technologies de mise en réseau les plus récentes.

- Un processus de retrait de version a été établi avec trois jalons principaux:
  EOS (End of Sales),
  EOE (End of Engineering) et
  EOL (End of Life).

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, fastethernet
  - serial0, ou s0
- Raccourci des commandes:
  - **router#conf t**
  - **router(config)#int e0**
  - **router(config-if)#ip addr 196.200...**
- 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 196.200.221.252 ?**
- 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 10.0.0.1 255.255.255.0**
  - **router(config-if)#exit**
  - **router(config)#exit**
  - **router#copy running-config startup-config**

Procédure de configuration (5)
Configuration des interfaces

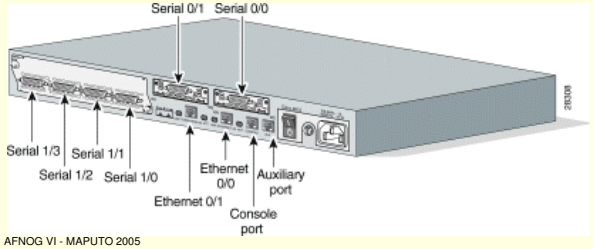
- **Configuration des interfaces**
- **Interface série**
- Pour configurez les interfaces, on passe du mode configuration générale vers la configuration de l'interface.
  - **router> enable**
  - **password :**
  - **router#configure terminal**
  - **router(config)#interface serial 0**
  - **router(config-if)#ip address 10.0.0.1 255.255.255.0**
  - **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 10.0.0.1 255.255.255.255**
  - **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.

  - **Router(config)#interface null 0**

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 routage

- **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 2005**
- **router(config-router)#network 10.0.0.0**
- **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 (2)

- Assignation d'identité
  router(config)# hostname tablex *(x est votre numéro de table)*
- Assignation du mot de passe de privilège:
  - **tablex(config)# enable secret afnog2005 *(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 (3)

Assignation d'une adresses IP
- **router(config-if)# ip address 196.200.221.9 255.255.255.0**

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 (4)

- **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 (5)

- **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 (6)

- 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 la config

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

Configuration de base du routeur (7)

Routage statique

- Route par défaut
  - **router(config)# ip route 0.0.0.0 0.0.0.0 196.200.221.126**
- Route explicite
  - **router(config)# ip route 196.200.220.0. 255.255.254.0 196.200.221.126**

Les Listes de contrôle d'accès

Les Listes de contrôle d'accès

- L'IOS fournit la possibilité de faire du filtrer le trafic: les "accès lists"
- Ils peuvent être configurées pour tous les protocoles routables (IP, IPX, AppleTalk, ...).
- Les "acces lists" permettent de prévenir l'accès sur votre réseau. Les "acces lists" ne sont pas uniquement destinées à la sécurité mais peuvent être utilisées dans le cadre de contrôles de routage, lutte contre les virus (route map) etc.

Les Listes de contrôle d'accès (2)

- Une liste de contrôle d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

  -L'adresse d'origine
  -L'adresse de destination
  -Le numéro de port.
  -Les protocoles
  -D'autres paramètres (horaires par exemple)

Les Listes de contrôle d'accès (3)

- **Création des ACL – Généralités**
- Pour créer une liste de contrôle d'accès, il faut :
  - Créer la liste de contrôle d'accès en mode de configuration globale.
  - Assigner cette ACL à une interface en mode de configuration des interfaces.

  NB: L'un sans l'autre n'a aucun effet.
- Structure générique d'une ACL :
  - **tablex(config)#access-list *numéro d'ACL* {permit | deny} *instructions***

Les Listes de contrôle d'accès (4)

Vérification des paquets

- Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle Cisco IOS examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées.
  - Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiés.
  - Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite deny any à la fin de chaque ACL.
    NB: Il faut faire attention a ce niveau pour savoir ce qu'on fait.

Les Listes de contrôle d'accès (5)

Assignation des ACLs aux interfaces

- Les listes de contrôle d'accès sont affectées à une ou plusieurs interfaces et peuvent filtrer du trafic entrant ou sortant, selon la configuration. Nous verrons plus loin où placer les ACLs de façon optimale selon le type d'ACL créée.
- Une seule liste de contrôle d'accès est permise par port, par protocole et par direction, c'est-à-dire qu'on ne peut pas par exemple définir deux ACLs sur l'interface E0 pour le trafic IP sortant. Par contre, on peut définir deux ACLs pour le trafic IP mais, une pour le trafic entrant et l'autre pour le trafic sortant…

Les Listes de contrôle d'accès (6)

ACL standard et ACL étendus appliques a IP

- Les ACLs standards utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole.
  - Numéroté entre 1 et 99
  - S'appliquent uniquement a l'adresse source
  - Se placent proche de la destination
- Les acl étendus
  - Sont identifies par des nombres de 100 a 199
- Peuvent s'appliquer sur:
  - L'adresse source
  - L'adresse destination
  - Le protocole
  - Le port
  - Se placent proche de la source

Les Listes de contrôle d'accès (7)

- **Le masque générique (inverse mask ou wildcard mask)**
- Un masque générique est jumelé à une adresse IP.
- Le masque générique est l'inverse du Nestmask
- Pour l'obtenir il faut faire 255.255.255.255 – le netmask

TP Définir les masques génériques pour vos plages d'adresses

- /29 sur vos tables
- /26
- /30

Les Listes de contrôle d'accès (8)

- Faire un telnet a partir de votre PC sur votre routeur
- Interdire le telnet de votre PC sur votre routeur
- Quel type d'acl allez vous utiliser?
- Ou allez vous l'appliquer?

Perte du Mot de passe Enable

Perte du mot du mot de passe enable

Comment se connecter au routeur en cas de perte du mot de passe enable et en mettre un nouveau?

tablex>enablePassword:
Password:% Bad secrets

1. Determiner la valeur du registre de configuration

tablex>sh vers
Configuration register is 0x2102

2. Eteindre et allumer le routeur
3. Taper la combinaison de touches ~# ou CTRL+BREAK sous Windows (voir sur le site de cisco pour d'autres touches) dans les 60 secondes qui suivent le démarrage

Perte du mot du mot de passe enable (2)

!--- The router was just powercycled and during bootup a!--- break sequence was sent to the router.! * System received an abort due to Break Key *** signal= 0x3, code= 0x500, context= 0x813ac158PC = 0x802d0b60, Vector = 0x500, SP = 0x80006030**
rommon 1 >

4. Démarrer du Flash sans charger la configuration

rommon 1 > confreg 0x2142
You must reset or power cycle for new config to take effect
rommon 2 > reset

System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)Copyright (c) 1999 by cisco Systems, Inc.TAC:Home:SW:IOS:Specials for infoC2600 platform with 32768 Kbytes of main memory .

NB: le routeur reboot sans charger la configuration de démarrage

Perte du mot du mot de passe enable (3)

5. Ignorer la procédure de configuration interactive en tapant no a chaque question ou CTRL+C
Router>

6. Copier la configuration en flash comme configuration active
***Router>enable* (noter que vous n'avez plus besoin de mot de passe)**
Router#copy startup-config running-config
Destination filename [running-config]?1324 bytes copied in 2.35 secs (662 bytes/sec)
Router# write terminal ou show running-config

NB: Vous ne retrouvez le mot de passe enable que dans le cas ou il n'est pas crypté Si cryptage il y'a il faut le changer.

Perte du mot du mot de passe enable (4)

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret afnog2005
Router(config)#^Z

7. Activer les interfaces (no shutdown sur chaque interface)
Router#copy running-config startup-config
Destination filename [startup-config]? Building configuration... [OK]
Router#show version
Cisco Internetwork Operating System Software ….Configuration register is 0x2142

8. Changer le registre
Router#configure terminal
Router(config)#config-register 0x2102
Router(config)#^Z

Perte du mot du mot de passe enable (5)

Router#

8. Redémarrer le routeur

Quelques liens

- Hardware support
http://www.cisco.com/public/support/tac/hardware.shtml
- Password Recovery Procedures
http://www.cisco.com/warp/public/474/
- Choosing IOS
http://www.cisco.com/warp/public/130/choosing_ios.shtml
- Touches BREAK
http://www.cisco.com/warp/public/701/61.html

Les Bonnes pratiques

Les bonnes pratiques
Mot de passes

- **Assignation du mot de passe de privilège**
  - **router(config)# enable secret afnog2005 *(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
Désactiver les services à 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
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'AFNOGVI***
  - **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
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
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
Règles de sécurité sur les 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
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
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
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
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
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
Autres Options

- La commande bandwidth
- Appliquer la commande bandwidth pour définir la bande passante réelle.
- 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
Contrôlez vos logs

- Contrôlez les logs de votre routeur en cas de connexion infructueuses. (voir slide 71)
- Les logs peuvent être déportées sur un autre serveur
  - **Router(config)#logging facility local7**
  - **Router(config)#logging 196.200.222.122**
  - **Router(config)#**

QUESTIONS????