Rappel de cours
Learning Tree 466
Introduction aux routeurs Cisco

Présentation du routeur

Le fonctionnement du routeur nécessite :
- un système d'exploitation : IOS, qui contrôle le routeur
- une configuration, qui adapte le fonctionnement du routeur à nos besoins

Lorsque le routeur est démarré et en phase d'exploitation, l'IOS et la configuration (running-config) sont en RAM (en mémoire vive) --> accès plus rapide aux données.

Lorsque le routeur est éteint, ces deux éléments sont stockés en FLASH et NVRAM et chargés au démarrage,
- l'IOS est chargé à partir (=depuis) la mémoire FLASH
- et la configuration est chargée à partir de la NVRAM
  - en NVRAM, la configuration s'appelle **startup-config** (configuration de démarrage)
  - en RAM, la configuration s'appelle **running-config** (configuration courante)

Lorsqu'on modifie la configuration courante du routeur, on modifie la running-config en RAM et les effets sont pris en compte immédiatement.
- Pour modifier la configuration courante : configure terminal
- Pour sauvegarder la configuration courante (running-config) vers la NVRAM (startup-config) : copy running-config startup-config

Ces opérations ne sont possibles qu'en mode privilégié (mode enable).

Prise en main de l'IOS

On dispose de trois mode :
- Mode user : accès de base au routeur, éventuellement après un mot de passe
  Accès restreint en lecture, pas de lecture de la config possible
  Caractérisé par l'invite **>**
- Mode privilégié, mode Enable : accès en tapant **enable**, éventuellement après un mot de passe
  Accès total en lecture, lecture de la config possible, réinitialisation ou rafraîchissement de valeurs (routes dynamiques, cache arp, NAT, etc.), permet d'accéder au mode de configuration
  Caractérisé par l'invite **#**
- Mode configuration : accès en tapant configure terminal
  Accès total à la modification de la configuration
  Caractérisé par l'invite **(config)#**

Dans tous les modes, l'IOS complète automatiquement les commandes.

On peut se contenter des taper les premières lettres et non pas le mot entier --> PLUS RAPIDE !!!
La touche TAB permet de compléter une commande. Si plusieurs mots commencent par les mêmes lettres, l'IOS renvoit un bip ou un message d'erreur.

Pour connaître les possibilités derrière un début de mot, taper le début du mot suivi immédiatement

du **?** (sans espace).
Pour connaître les autres commandes possibles derrière un commande, taper la commande + espace + **?**

Pour aller en début de ligne : CTRL – A
Pour aller en fin de ligne : CTRL – E
Pour répéter la ligne en cours d'écriture : CTRL – R
Flèche Haut : Rappel des commandes tapées

Configuration du routeur

Accès à partir du mode enable en tapant : **configure terminal** (configuration à partir du terminal sur lequel on est connecté)

Plusieurs niveaux de configurations :
- configuration globale : paramètres qui concernent l'ensemble du routeur (nom du routeur, routes, SNMP, etc.)
- configuration des interfaces : ensemble des paramètres des interfaces
  interface nom_interface numero_interface
  interface serial 0/0
- configuration des protocoles des routages
  router nom_protocole [paramètres éventuels]
- configuration des lignes d'accès au routeur :
  - Port Console : accès physique au routeur à partir d'un terminal DTE type PC
    line con 0
  - Port Auxiliaire : accès « physique » à distance via une ligne (branchement d'un DCE)
    line aux 0
  - Port Virtuel : accès distant supporté par un protocole réseau (TELNET)
    line vty première_ligne dernière _ligne
    line vty 0 4 = 5 lignes Telnet définies

Tous les paramètres concernant une section sont décalés d'un caractère.

Pour sortir du mode de configuration, **end** ou CTRL – Z. Pour sortir d'un niveau, **exit**

Routage

Généralités

Accéder à un réseau signifie pouvoir envoyer des messages (paquets) à toutes les interfaces de ce réseau.

Pour désigner un réseau, on donne :
- l'identifiant du réseau : la première adresse du réseau (par exemple : 192.168.1.0)
- le masque du réseau : qui va indiquer la dernière adresse du réseau (par exemple : 255.255.255.0)

Un réseau peut faire n'importe quelle taille :

- 254 adresses IP : exemple : 192.168.1.0 masque 255.255.255.0
- encore plus grand : exemple 171.14.0.0 masque 255.255.0.0
- encore plus grand : exemple : 10.0.0.0 masque 255.0.0.0

- encore plus grand !!! exemple 0.0.0.0 masque 0.0.0.0 (= tout Internet)

Dans l'absolu et pour pousser le raisonnement à l'extrême, un réseau peut faire *une seule adresse* IP, et je peux indiquer une route pour ce réseau (route très spécifique donc).

Exemple : 194.51.3.65 masque 255.255.255.255

Mise en oeuvre du routage

Pour résumer, trois moyens d'accéder à un réseau :
- **Directly connected** : le réseau est directement connecté à un interface, l'interface appartient à ce réseau
- **Route statique** : l'administrateur indique localement au routeur par quel point il doit passer pour atteindre le réseau (= à quel routeur il doit envoyer les paquets pour qu'ils atteignent le réseau destination)
- **Route dynamique** : ce sont les autres routeurs qui indiquent au routeur le chemin ; le routeur écoute donc les annonces de routage des autres routeurs.

Directly connected : configurer le routeur pour qu'il accède au réseau = sur l'interface connectée physiquement à ce réseau, mettre une adresse IP qui fait partie du même réseau IP que toutes les autres machines.

interface nom_interface numero_interface
ip address adresse_IP masque_reseau
no shut (active l'interface)

Route statique : indiquer au routeur à quel point *extérieur* à lui-même envoyer des paquets pour qu'ils atteignent le réseau destination. Il faut que ce point soit **connu** du routeur ; il s'agit d'un autre routeur présent sur le même réseau que lui, donc accessible en **Directly Connected** : c'est un **Next-Hop** (Prochain Saut)

NB : Si l'on indique un routeur éloigné, c'est-à-dire sur un réseau distant inconnu, la route ne marchera pas.

Configuration :

ip route identifiant_de_réseau masque_réseau next-hop_connu

Attention : on donne le chemin pour un réseau distant, il faut donner l'identifiant de ce réseau (la première adresse de ce réseau) et non pas l'adresse d'une machine !!! (pour résumer : 192.168.1.0 et non pas 192.168.1.45 par exemple)

Route dynamique : Route apprise par d'autres routeurs. Il faut configurer un **protocole de routage** qui permettra au routeur d'échanger des **annonces de routages** avec d'autres routeurs

Dans une seule commande, on va définir quels réseaux annoncer et sur quelles interfaces échanger des annonces de routuages :

router rip
network 172.16.0.0

La commande network 172.16.0.0 fait trois choses :

- annoncer le réseau 172.16.0.0 (en réalité, les réseaux présents sur le routeur appartenant à 172.16.0.0, c'est-à-dire 172.16.1.0, 172.16.2.0, ..., 172.16.13.0, etc...)
  = annoncer au autres routeurs qu'ils peuvent m'envoyer leurs paquets pour atteindre ces réseaux
- envoyer des annonces de routages sur les interfaces appartenant à 172.16.0.0
  Par exemple, j'envoie des messages RIP sur **interface FastEthernet 0/0** dont l'adresse est **172.16.100.1**
- écouter les annonces de routages provenant des autres routeurs, sur les interfaces appartenant à 172.16.0.0
  Par exemple, j'écoute les messages RIP arrivants sur **interface FastEthernet 0/0** dont l'adresse est **172.16.100.1**

Si l'on veut désactiver l'envoi d'annonces sur une interface (et donc *simplement annoncer le réseau* connecté à cette interface) :

router rip
passive-interface nom_interface numero_interface

Exemple :

router rip
network 172.16.0.0
network 10.0.0.0
passive-interface FastEthernet 0/0

J'annonce les réseaux 10.0.0.0 et 172.16.0.0 et j'active l'émission et la réception des annonces sur les interfaces appartenant à 10.0.0.0 et 172.16.0.0.

Mais je désactive l'émission d'annonces sur l'interface FastEthernet 0/0 (qui appartient accessoirement au réseau 172.16.0.0). Donc pas d'annonce RIP du réseau 10.0.0.0 sur cette interface. Donc les routeurs présents sur le réseau connecté à cette interface ne connaîtront pas l'existence de 10.0.0.0.

Filtrage de paquets IP

Les routeurs permettent de filtrer les trames (niveau 2) et les paquets (niveaux 3 et 4). On se concentre sur le filtrage de paquets IP.

On examine les flux entrants ou sortant sur une interface en les comparant dans l'ordre à une liste de critères. Chaque ligne de la liste contient un critère (par exemple : d'où vient le paquet), ainsi qu'une action associée (par exemple : détruire ou autoriser le paquet).

1) Il faut donc définir les critères et les actions pour chaque critères dans une liste (une Access-List)
   En Mode Global de configuration
2) Activer cette Access-List aux flux entrants ou sortants d'une interface
   Dans la configuration de l'interface, définir si l'on examine les flux entrants ou sortants en faisant référence aux critères contenus dans une Access-List

1) Définition de l'Access-List

Deux types :

- 1 à 99 : Standard
  Critère : origine du paquet = adresse IP source du paquet
- 100 à 199 : Etendue
  Beaucoup plus de critères : adresse IP source, port source, adresse IP destination, port destination, etc.

Configuration

access-list numéro action critère [critères étendus]

où action = **deny** ou **permit**

Access-List Standard : critère : Adresse IP source de machine ou de réseau
Le paquet vient-il de telle machine ? Vient-il de tel réseau ?
Attention : pour une adresse de réseau, le masque du réseau est inversé !

Exemple :
- détruire les paquets provenant de la machine 192.168.1.45
  access-list 1 deny host 192.168.1.45
- autoriser les paquets provenant du réseau 172.16.1.0 masque 255.255.255.0
  access-list 1 permit 172.16.1.0 0.0.0.255

2) Appliquer l'Access-List à une (ou plusieurs) interface

Dans la configuration de l'interface :

interface nom_interface numero_interface
ip access-group numéro sens

où sens = **in** ou **out**

Exemple :
- J'examine les flux entrant sur l'interface FastEthernet 0/0 et je les compare avec l'ACL 21

interface FastEthernet 0/0
ip access-group 21 in

Attention : Par défaut, une ACL détruit tous les paquets (**deny any** ajouté à la fin de l'ACL). Si l'on veut *autoriser tout le trafic restant* (après l'examen des divers critères), rajouter un **deny any.**

Rappel de commandes utiles

show version
Affiche les caractistiques matérielles et logicielles du routeur : type de routeur, nom et nombre d'interface, quantité de mémoire, nom de version d'IOS, état du registre de configuration, etc.

show interface nom_interface numero_interface
Affiche l'état de l'interface, ses caractéristiques de niveau 2 et 3, les compteurs.

show ip interface brief

Résumé de l'état des interfaces et de leurs adresses IP

show ip route
Affiche la table de routage du routeur

clear ip route *
Supprime toutes les routers dynamiques du routeur (le routeur demande alors de nouvelles routes)

show ip protocols
Affiche les protocoles de routage configurés sur le routeur (RIP, EIGRP, etc.)

show arp ou **show ip arp**
Affiche la table de correspondance entre adresses MAC et adresses IP

clear arp-cache
Demande à nouveau les adresses MAC correspondantes aux adresses IP dans le cache ARP

debug ?
Affiche en temps réel un examen des trames ou des paquets transitant sur le routeur

undebug all ou no debug all
Stop tous les debug en cours

show controllers serial 0/0
Affiche entre autre le type de câble connecté sur l'interface (Norme + horloge)

clockate vitesse_horloge
En mode de configuration d'interface, **sur le routeur DCE**, définit la vitesse d'horloge d'une interface Série

enable secret mot_de_passe
En mode global de configuration, définit le mot de passe d'accès au mode privilégié

enable password mot_de_passe
Cette commande est **obsolète** rappelez-vous !

password mot_de_passe
Dans la configuration des lignes d'accès au routeur, définit le mot de passe d'accès au mode User spécifique à chaque ligne

login
Dans la configuration des lignes d'accès au routeur, active la demande du mot de passe par le routeur

no ip domain-lookup
Désactive la résolution DNS sur le routeur

?
Votre meilleur ami.