Configuration d'un commutateur ou d'un routeur CISCO

Ce n'est pas un tutoriel complet de configuration d'un commutateur ou d'un routeur Cisco, mais plutôt un recueil de commandes utilisées fréquemment pour commencer à configurer un commutateur. La validité des commandes présentées varient en fonction du type de commutateur et de la version de l'IOS du matériel.

Connexion en série

Pour la première configuration d'un commutateur, la seule façon de le configurer est par l'intermédiaire d'une liaison Serie RS232 connectée au port console du commutateur.

Sous windows, on peut utiliser l'hyper terminal, sous linux on peut utiliser un émulateur comme kermit. Voici quelques commandes relatives à kermit :

```
set modem type none   ; on utilise une connexion directe (sans modem)
set line /dev/ttyS0       ; Specify device name
set carrier-watch off ; If DTR CD are not cross-connected
set escape-character ^A ; changer le caractere d'echapement
set flow xon/xoff     ; If you can't use RTS/CTS
set speed 57600       ; Or other desired speed
set flow rts/cts      ; If RTS and CTS are cross-connected
set parity even       ; (or "mark" or "space", if necessary)
set stop-bits 2       ; (rarely necessary)
show escape
connect               ; Enter Connect (terminal) state
```

Exemple :

```
$ kermit
C-Kermit 8.0.209, 17 Mar 2003, for Red Hat Linux 8.0
 Copyright (C) 1985, 2003,
  Trustees of Columbia University in the City of New York.
Type ? or HELP for help.
C-Kermit>set modem type none
C-Kermit>set line /dev/ttyS0
C-Kermit>set carrier-watch off
C-Kermit>set escape-character ^A
C-Kermit>connect
```

La sortie de la connexion de kermit se fera par la combinaison de touches :

```
Ctrl-A
q
```

La première fois via une console connectée sur le port console. Au démarrage, on rentre dans le setup permettant de rentrer les paramètres de bases et les adresses IP des différentes interfaces si la mémoire

non volatile est vide.

Identification :

2 modes d'identification :

Mode utilisateur (**user**) : le mot de passe est demandé lors de la connexion via telnet ou à la console. Dans ce mode, nous avons accès à un sous ensemble des commandes : uniquement certaines commandes de visualisation d'informations

Mode administrateur (**privileged** ou **enable**) : C'est dans ce mode que l'on pourra configurer le commutateur.

Visualisation et modification de la configuration :

Liste des commandes disponibles. Attention elle est différente suivant le mode d'identification. Le ? Est aussi utilisable pour connaître les arguments d'une commande :

```
> ?
```

On peut saisir le début de la commande, elle peut être complétée (complétion) comme le bash en utilisant la touche 'TAB'.

Passer en mode privilégié :

```
> enable
```

Le prompt '>' devient '#' pour indiquer que l'on est en mode privilégié.

Pour entrer dans l'éditeur de configuration et la modifier.

```
# configure  terminal
```

pour sortir de l'éditeur :

```
> CTR+Z
```

Assigne un mot de passe encrypté à enable :

```
# enable secret <password>
```

pour visualiser la configuration en mémoire non volatile (celle en mémoire RAM, pas celle sur la mémoire flash) :

```
# write terminal
# show running-config
```

pour visualiser la configuration de démarrage (celle stockée sur la mémoire flash) :

```
# show startup-config
```

Modifier le nom de l'équipement réseau :

```
# hostname <hostname>
```

Pour sauvegarder la nouvelle configuration en mémoire non volatile (FLASH) :

```
# write memory
# copy running-config startup-config
```

Pour effacer la configuration de mémoire non volatile (FLASH) :
ATTENTION : Cela efface la configuration qui est chargée au démarrage, si on re-démarre le commutateur après cette commande, il pert toute sa configuration

```
# erase startup-config
```

Rédémarrage du routeur (reboot) :

```
# reload
```

Toutes les commandes peuvent être rentrées sous forme complète ou sous forme abrégée :

```
# write memory
# wr mem
# conf t
# int fastethernet 0/1
# interface fastethernet 0/1
```

Attribuer une adresse IP à une interface : **ip address <address> <mask>**

```
# write memory
# wr mem
# conf t
# int vlan1
# ip address 192.168.1.20 255.255.255.0
```

Active ou désactive une interface : **shutdown** ou no **shutdown**

```
# write memory
# wr mem
# conf t
# int fastethernet 0/1
# no shutdown
```

Sauvegarde de la configuration du routeur sur un serveur.

On peut sauvegarder la configuration du routeur sur un serveur du réseau via TFTP, RCP ou FTP.
Il faut d'abord mettre en place un serveur TFTP. On suppose que /tftpboot est le

répertoire de chargement du serveur tftp. Passer en mode "enable" sur le Cisco

```
# copy system:/running-config tftp://192.168.1.14/test
Address or name of remote host [192.168.1.14]?
Destination filename [test]?
!!!!!!!!
35761 bytes copied in 1.157 secs (30908 bytes/sec)
#
```

La configuration est sauvegardée dans /tftpboot/test du serveur tftp.

Chargement de la configuration à partir d'un serveur TFTP

De même on peut charger la configuration via un serveur TFTP ou ftp. Cette méthode présente l'avantage de pouvoir écrire tranquillement sa configuration via un éditeur de texte et la charger quand on veut.

```
# copy tftp://192.168.1.14/test system:/running-config
# copy ftp://user:password@192.168.1.14/test system:/running-config
# copy system:/running-config system:/startup-config
# copy ftp://user:password@192.168.1.14/test system:/startup-config
```

Commandes de tests et de visualisation de l'état du routeur :

visualiser l'état des interfaces

```
# show int
```

visualiser la table des routes IP

```
# sh ip route
```

Visualisation de la table arp :

```
# sh ip arp
```

Tester un ping :

```
> ping @IP
```

Compte les trames à destination du routeur (et non toutes celles qui passent).

```
# sh ip traffic
```

interrogation des logs des ACL :

```
# show ip accounting access-violations
```

Réinitialisation des compteurs de l'accounting

```
# clear ip accounting
```

Visualisation de la version de l'IOS et des numéros de série :

```
> sh version
```

Visualisation de l'allocation de la mémoire aux objets de l'IOS

```
> sh mem
```

pour surveiller la charge du routeur (table des processus de l'IOS)

```
> sh process
```

visualisation de la mémoire utilisée et disponible :

```
> sh proc mem
```

Visualisation de la mémoire flash utilisée et disponible :

```
# show flash

Directory of flash:/

    3  -rwx        1216   Feb 29 2008 14:59:32  vlan.dat
    4  -rwx          48   Sep 15 2008 15:44:04  private-config.text
    5  drwx         320   Mar 02 2005 06:44:27  c3750-i9-mz.121.11-AX
   24  -rwx       35761   Sep 15 2008 15:44:03  config.text

15998976 bytes total (6514688 bytes free)
#
```

Commandes par interfaces (sous-commandes)

Elles s'adressent à une partie du commutateur. À 1 ou plusieurs interfaces :

```
#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
routeur(config)#interface fastethernet 1/0/1
routeur(config-if)# ip address x.y.z.y 255.255.255.0
routeur(config)#interface fastethernet 1/0/2
routeur(config-if)# ip address x.y.z.z 255.255.255.0
routeur(config)#interface range fastethernet 1/0/2 - 24
routeur(config-if)# switchport mode acess
routeur(config-if)# switchport acess vlan 3
routeur(config-if)#^Z
```

Les VLAN

Cisco dispose d'un protocole d'échange de la liste des VLAN configurés dans un commutateur, c'est VTP (Vlan Trunking Protocol). C'est un mode client serveur. Un commutateur doit être configuré en mode serveur, les autres commutateurs du réseau local doivent être configurés en mode client :

sur le commutateur « serveur VTP » :

```
Vlan database
  vtp domain <domaine>
  vtp server
  vlan 2 name XXXX
  exit
```

sur le commutateur « client VTP » :

```
Vlan database
  vtp domain <domaine>
  vtp client
  exit
```

Le mode de chaque interface physique :

`switchport mode access` : dans ce mode, on indique au commutateur que le port n'est pas un uplink et que l'on connectera une ou plusieurs machines dans le même VLAN

`switchport access vlan N` : dans ce mode, on indique au commutateur que le port n'est pas un uplink et que l'on connectera une ou plusieurs machines dans le VLAN numéro N

`switchport mode trunk` : dans ce mode, on indique au commutateur que le port va transporter tous les VLAN (sauf prunning)

`switchport trunk encap dot1q` : dans ce mode, on indique au commutateur que le protocole de trunking va utiliser le protocole normalisé 802.1q

`switchport trunk encap isl` : dans ce mode, on indique au commutateur que le protocole de trunking va utiliser le protocole ISL (propriétaire Cisco)

Routage

Ces commandes peuvent uniquement être prises en compte sur les commutateurs de niveau 3 :
Commandes routage statique :
Routage statique : `ip route reseau masque <passerelle>`
Route par défaut : `ip route 0.0.0.0 0.0.0.0 <passerelle>`

```
ip route 0.0.0.0 0.0.0.0 192.168.1.13
ip route 192.168.85.4 255.255.255.252 192.168.84.5
ip route 192.168.85.16 255.255.255.240 192.168.84.5
ip route 192.168.85.32 255.255.255.240 192.168.84.4
```

En fonction des licences disponibles sur le commutateur, il sera capable de faire du routage dynamique interne (RIP, OSPF...) ou externe (BGP...).

Filtrage, access-lists

Filtres sur ICMP
Filtrer icmp est toujours problématique. C'est un protocole à la fois très utile mais aussi potentiellement dangereux. De nombreuse attaques sont basées dessus (« smurf » et autres joyeusetées). Parmis ses différentes fonctions on peut trouver : fragmentation (type 3, message du type "destination unreachable"), PATH MTU Discovery (type 4), drop des paquets, traceroute, ping, controle de flux.

Pour ceux qui veulent filtrer le protocol icmp , voici au moins ce qu'il faut autoriser :

```
access-list 102 permit icmp any any unreachable parameter-problem source-quench
time-exceeded ttl-exceeded packet-too-big administratively-prohibited
access-list 102 deny icmp any any
```

Autrement, pour ceux qui autorisent ping , on peut limiter les excès éventuels en ajoutant ceci sur l'interface d'entrée :

```
rate-limit input access-group 2000 744000 10000 10000 conform-action transmit
exceedaction drop
```

avec :

```
access-list 2000 permit icmp any any echo-reply
access-list 2000 permit icmp any any echo
```

Exemples de configuration presque complète d'une configuration :

```
banner ^

     Ce systeme appartient au Centre National de la Recherche Scientifique

      Une autorisation du service informatique de l'IPNL
           est necessaire pour utiliser ce systeme.

   L'utilisation de ce systeme par une personne non autorisee, est interdite.

^
no service pad
service timestamps debug uptime
service timestamps log datetime localtime
! service password-encryption = chiffrage du password dans les fichiers
! de configuration sauvegardes
service password-encryption
! devalidation de services du cisco (securite)
no service finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
no ip http server
no ip bootp server
! Cisco discovery protocol
no cdp run
! par défaut , émission de requêtes TFTP à l’adresse de broadcast pour
! vérifier que la configuration n’a! pas été modifiée. La commande permet
! d’arrêter ces envois :
no service config
! Le routeur implémente les services
! echo (ports TCP et UDP numéro 7),
! discard (ports TCP et UDP numéro 9),
! chargen (ports TCP et UDP numéro 19).
! Ces 2 commandes permettent de les dévalider.
no service tcp-small-servers
no service udp-small-servers
! le routeur ne doit pas router de paquets IP comportant l'option "Source
! routing". L'option "Source routing" permet à l'émetteur d'un paquet IP de
! spécifier le chemin que doit prendre le paquet pour accéder à sa destination,
! indépendamment des tables de routages des routeurs traversés. Le
! destinataire devra utiliser le chemin inverse pour le retour ( option –g de
! traceroute )
no ip source-route
! permet d'utiliser le mécanisme de syslog pour journaliser sur un serveur
! externe les événements importants recensés ( arrêts, modifications de config,
! trace de tous les paquets ayant satisfait un élément marqué "log" dans une
! ACL ) sur le routeur.
logging facility auth
logging trap debugging
logging 192.168.1.20
! verification si quelqu'un se connecte au routeur
ip accounting
ip accounting access-violations
! permet d’utiliser des masques de réseaux variables
no ip classless
```

```
hostname routeur
!
no logging console
enable secret 5 $1$GUvm$nHdAJdsdffgfd
enable password 7 141E0232323232525
!
clock timezone UTC 2
ip subnet-zero
ip routing
!
! utilise un serveur VMPS qui contient un liste des adresses ethernet a
! utiliser opur le protocole VMPS
vmps server 192.168.1.104 primary
vmps server 192.168.1.26
!
! algorythme utilisé pour le load-balancing pour les etherchannel
port-channel load-balance src-dst-mac
!
! exemples de configurations d'interfaces logiques ou physiques
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
!
interface FastEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 no mdix auto
!
interface FastEthernet1/0/32
 switchport mode access
 no ip address
 no mdix auto
!
interface FastEthernet1/0/37
 switchport access vlan dynamic
 no ip address
 no mdix auto
 spanning-tree portfast
!
interface GigabitEthernet1/0/1
 description inerconnexion
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
!
interface GigabitEthernet1/0/2
 no switchport
 ip address 192.168.69.14 255.255.255.252
!
interface GigabitEthernet1/0/3
 description uplink
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 no mdix auto
 channel-group 1 mode active
!
interface GigabitEthernet1/0/4
```

```
 description uplink
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 no mdix auto
 channel-group 1 mode active
!
interface Vlan1
 description reseau 1 (default)
 ip address 192.168.1.1 255.255.248.0
 ip access-group 171 out
 no ip proxy-arp
 ntp broadcast destination 192.168.143.255
 no ip directed-broadcast
 no ip unreachables
 no cdp enable
 no ip redirects
 no ip proxy-arp
!
interface Vlan2
 description reseau 2
 ip address 192.168.81.1 255.255.255.128
 ip access-group 172 out
 ip helper-address 192.168.1.26
 ntp broadcast destination 192.168.81.127
 no ip directed-broadcast
 no ip unreachables
 no cdp enable
 no ip redirects
 no ip proxy-arp
!
interface Vlan3
 description reseau 3
 ip address 192.168.82.65 255.255.255.224
 ip access-group 173 out
 ip helper-address 192.168.1.26
 ntp broadcast destination 192.168.82.95
 no ip directed-broadcast
 no ip unreachables
 no cdp enable
 no ip redirects
 no ip proxy-arp
!
ip route 0.0.0.0 0.0.0.0 192.70.69.13
ip route 192.168.81.0 255.255.255.0 Null0
ip route 192.168.82.0 255.255.255.0 Null0
ip route 192.168.83.0 255.255.255.0 Null0
ip route 192.168.85.4 255.255.255.252 192.168.84.5
ip route 192.168.85.16 255.255.255.240 192.168.84.5
ip route 192.168.85.32 255.255.255.240 192.168.84.4
!
! Connexion en telnet sur le routeur
access-list 50 permit 192.168.84.0 0.0.1.255
! control d'acces a SNMP (pour la lecture)
access-list 92 permit 192.168.84.20
snmp-server community public RO 92
! control d'acces a SNMP (pour l'ecriture)
access-list 91 permit 192.168.84.19
snmp-server community private RW 91
!
! VLAN 1
```

```
! pour dhcp server
access-list 171 permit udp host 192.168.1.26 eq bootps any
! pour dns
access-list 171 permit tcp any host 192.168.1.50 eq domain
access-list 171 permit udp any host 192.168.1.50 eq domain
access-list 171 permit tcp any any ack
access-list 171 permit icmp any any
access-list 171 deny tcp any any
access-list 171 deny udp any any
! VLAN 2
access-list 172 permit udp host 192.168.1.26 eq bootps any
access-list 172 permit udp host 192.168.1.50 eq domain any
access-list 172 permit icmp any any
access-list 172 permit tcp any any ack
access-list 172 deny tcp any any
access-list 172 deny udp any any
! VLAN 3
access-list 173 permit icmp any any
access-list 173 permit udp host 192.168.1.26 eq bootps any
access-list 173 permit udp host 192.168.1.50 eq domain any
access-list 173 deny ip any any time-range salle-test
access-list 173 permit tcp any any ack
access-list 173 deny tcp any any
access-list 173 deny udp any any
!
line con 0
 exec-timeout 0 0
line vty 0 4
 access-class 50 in
 exec-timeout 60 0
 password 7 11222090B192171F
 ! autorise la banniere
 exec-banner
 login
line vty 5 15
 password 7 022112145505031B
 login
!
ntp clock-period 36029640
ntp server 192.70.69.13
time-range salle-test
 periodic weekdays 0:00 to 7:00
 periodic weekdays 21:00 to 23:59
 periodic Saturday 0:00 to 7:00
 periodic Saturday 14:00 to 23:59
 periodic Sunday 0:00 to 23:59
!
!
end
```