Cours sur le paramétrage d'un switch CISCO

I. SOURCES DE CONFIGURATION :

Les commutateurs CISCO peuvent être configurés, simultanément et/ou indépendamment, à partir

de plusieurs sources. On peut classer ces différentes sources en deux catégories : les sources locales

et les sources distantes.

A. Sources locales :

- Le **port "Console"** : il s'agit d'un port série qui sera relié par un câble série (en général de quelques décimètres), soit à un **Terminal Asynchrone**, soit à un micro-ordinateur utilisant un **émulateur** de Terminal Asynchrone comme Hyper Terminal de Microsoft, T-Term Pro, etc. La configuration par défaut est 9600 bits/s, 8 bits/caractère, 1 bit de départ, 1 bit d'arrêt, pas de bit de parité, pas de contrôle de flux. Le port console est indispensable si le commutateur n'a pas de protocole IP configuré.

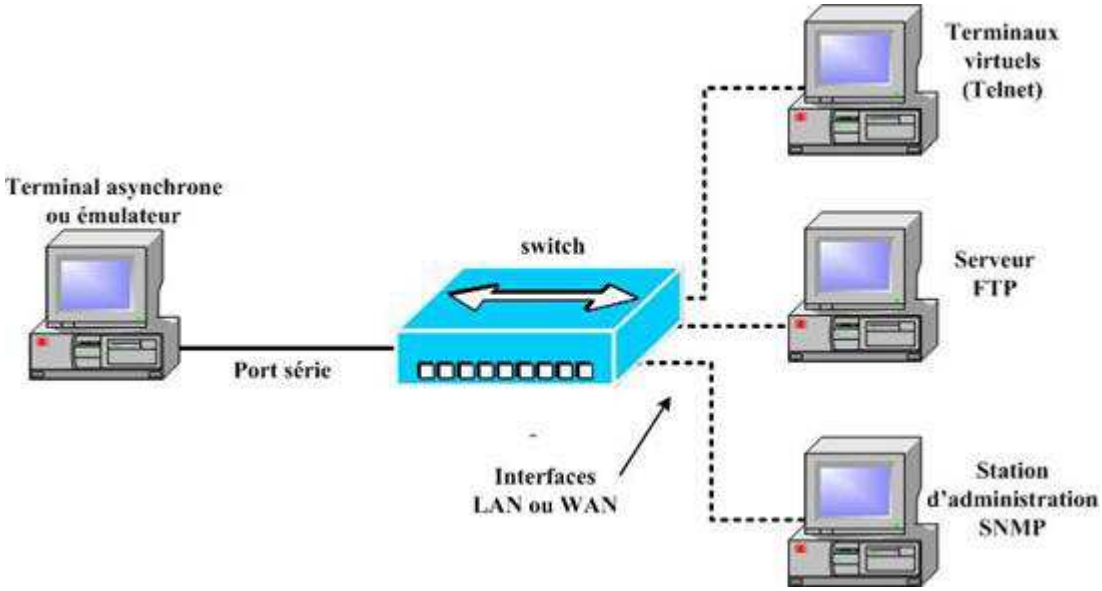
B. Sources distantes :

Dès que le protocole IP a été configuré sur le commutateur, il est possible de le configurer à distance à partir d'une station de réseau local. La communication utilise alors l'une des interfaces de réseau du commutateur.

- Les terminaux virtuels (VTY) : au moyen d'un émulateur de Terminal Asynchrone comme un client Telnet par exemple.

- Les serveurs TFTP : qui permettront de télécharger un fichier de configuration sur le commutateur.

- Les stations d'administration de réseau : au moyen d'une station SNMP comme CiscoWorks ou HP Open View.



II. MODES DE CONFIGURATION :

En dehors de l'utilisation d'un serveur TFTP pour télécharger une configuration existante, les principales sources de configuration des commutateurs sont soit un terminal asynchrone (ou un émulateur) par le port console, soit un client Telnet sur un PC, par l'une des interfaces LAN ou WAN.

Les commutateurs CISCO peuvent utiliser plusieurs modes différents parmi lesquels :

- Mode **EXEC** : mode permettant d'accéder à un interpréteur de commandes appelé EXEC. Le mode EXEC dispose de deux niveaux d'accès :

  - Mode **EXEC utilisateur** : ne permet qu'un examen limité de la configuration du commutateur. L'invite est "**Switch>**".

  - Mode **EXEC privilégié** : obtenu en tapant la commande "**enable**" à partir du mode EXEC utilisateur. Il permet l'examen total et la configuration du commutateur, ainsi que l'accès à des mécanismes de tests et de dépannage. L'invite est "**Switch#**". Pour quitter le mode EXEC privilégié, taper "**exit**", "**end**" ou "**CTRL+Z**".

- Mode de **configuration globale** : obtenu en tapant la commande "configure" à partir du mode EXEC privilégié. L'invite est "**Switch(config)**#". Ce mode donne accès à des commandes qui concernent l'ensemble du commutateur comme par exemple la commande "**hostname**" qui affecte un nom au commutateur. Ce nom sera repris par la plupart des invites des différents modes.

    - Mode de **configuration d'interface** : ….

    - Mode de **configuration de protocole** : …

III. PRINCIPALES OPERATIONS :

A. Ouverture/fermeture de session :

En fonctionnement normal, après sa phase d'initialisation, le commutateur affiche le message "Press RETURN to get started.". Actionner alors la touche "Entrée" pour passer en mode EXEC utilisateur (invite "Switch>"). Taper "**exit**" ou "**logout**" pour terminer une session

A partir du mode EXEC utilisateur, passer en mode EXEC privilégié par la commande "**enable**".

Revenir au mode EXEC utilisateur par la commande "**disable**" ou "**exit**".

Press RETURN to get started

Switch>**enable**

Switch#**exit**

Switch>**logout**

B. Sauvegarde/Restauration de configuration :

- Copie de la configuration de démarrage dans la configuration en cours : "**copy start run**".
- Copie de la configuration en cours dans la configuration de démarrage: "**copy run start**".
- Copie de la configuration de démarrage sur un serveur TFTP : "**copy start tftp**".
- Copie de la configuration en cours sur un serveur TFTP : "**copy run tftp**".
- Copie de la configuration de démarrage à partir d'un serveur TFTP : "**copy tftp start**".

IV. AIDES A LA CONFIGURATION :

A. Liste des commandes disponibles :

Dans les modes EXEC, la commande "**?**" affiche la liste des commandes disponibles dans le mode actif :

- L'écran affiche 22 lignes. Le message **"--more--**" en bas indique que la liste n'est pas terminée.
- Actionner la barre d'espacement pour afficher les 22 lignes suivantes.
- Actionner la touche "**Entrée**" pour n'afficher que la ligne suivante.
- Actionner n'importe quelle autre touche pour revenir à l'écran du mode EXEC actif.

B. Commandes et mots clés abrégés :

Il suffit de taper le nombre de caractères suffisants pour que l'interpréteur de commandes reconnaisse la commande exacte. Par exemple: **Switch>ena** suffit pour que l'interpréteur reconnaisse la commande "**enable**". Il est alors possible, mais pas obligatoire, d'actionner la touche de tabulation pour que l'interpréteur complète la commande automatiquement.

C. Liste des commandes commençant par une séquence de caractères particuliers :

Taper ces premiers caractères identiques à plusieurs commandes puis, **SANS espace**, taper un point d'interrogation. Par exemple :

Switch>lo?

D. Liste des arguments d'une commande :

Taper le nom de la commande puis **un espace**, puis un point d'interrogation. Par exemple :

Switch#conf ?

E. Commandes d'édition :

- **CTRL+A** : retour au début de la ligne
- **CTRL+E** : positionnement à la fin de la ligne
- **ECHAP+B** : début du mot précédent
- **CTRL+F** : déplacement à droite d'un caractère
- **CTRL+B** : déplacement à gauche d'un caractère
- **ECHAP+F** : déplacement à droite d'un mot

Si une ligne dépasse la largeur de l'écran, l'éditeur la décale de 10 caractères vers la gauche et introduit un caractère "$" au début de la ligne pour indiquer que ce n'est pas le début de la commande.

F. Historique des commandes :

- La touche ↑ rappelle la commande précédente.
- Actionner plusieurs fois la touche ↑ pour rechercher les commandes plus anciennes.
- Actionner plusieurs fois la touche ↓ pour rechercher les commandes moins anciennes.
- La commande "**show history**" affiche la liste des commandes utilisées précédemment.

G.Copier-Coller des commandes :

Les émulateurs de terminaux asynchrones permettent pour la plupart, d'effectuer des copier-coller afin de ne pas avoir à retaper des commandes ou des ensembles de lignes de commandes.

V. CONSULTATION DE L'ÉTAT DU COMMUTATEUR :

- **Show version** : affiche la configuration matérielle ainsi que la version et les noms des fichiers de configuration et d'IOS.
- **Show flash** : affiche des informations sur la mémoire flash.
- **Show running-config** : affiche la configuration en cours.
- **Show startup-config** : affiche la configuration de démarrage.
- **Show interfaces** : affiche les paramètres des interfaces ainsi que des statistiques.

VI. MOTS DE PASSE :

Si aucun mot de passe n'a été configuré, le mode EXEC privilégié ne peut être accessible qu'à partir du port console du commutateur, et donc pas par une session Telnet à partir d'une station.

Les commandes de configuration de mot de passe sont à mettre dans le mode de configuration globale (invite "**Switch(config)#**").

A. Mot de passe de console :

La commande "**line console 0**" obligera à taper un mot de passe pour accéder au mode EXEC à partir du port console.

B. Mot de passe de Terminal Virtuel :

La commande "**line vty 0 4**" puis "**password[mot_de_passe]**" obligera à taper le mot de passe [mot_de_passe] pour accéder au mode EXEC à partir d'une session Telnet.

C. Mot de passe du mode EXEC privilégié :

La commande "**enable password**" ou "**enable secret**" obligera à taper un mot de passe pour accéder au mode EXEC privilégié, tant à partir du port console qu'à partir d'une session Telnet.

Ces deux commandes utilisent un système de cryptage des mots de passe lors de leur transmission sur le réseau. La commande "**enable secret**" utilise un cryptage plus performant que la commande "**enable password**" et sera donc préférée à cette dernière, sauf si la version d'IOS est trop ancienne.

D. Cryptage supplémentaire :

La commande "**service password-encryption**" permet de crypter les mots de passe lors de l'affichage d'une configuration.

E. Désactivation des mots de passe :

Pour désactiver une commande de mot de passe, précéder la commande correspondante du mot "**no**".

VII. CREATION DE VLANS :

Par défaut, lors de la réception d'un commutateur, tous les ports sont affectés dans le Vlan 1. Ce Vlan nommé "**DEFAULT**" est le Vlan permettant l'administration du commutateur à partir d'une interface LAN ou WAN. Il n'est pas possible de le renommer.

A. Création des Vlans :

La création des Vlans se fait à partir du mode **EXEC privilégié**.

```
Switch#vlan database
Switch(vlan)#vlan 2 name nom-vlan2
Switch(vlan)#vlan 3 name nom-vlan3
Switch(vlan)#exit
Switch#show vlan
```

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

2 nom-vlan2 active

3 nom-vlan3 active

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

1 enet 100001 1500 - - - - - 0 0

2 enet 100002 1500 - - - - - 0 0

3 enet 100003 1500 - - - - - 0 0

1002 fddi 101002 1500 - - - - - 0 0

1003 tr 101003 1500 - - - - - 0 0

1004 fdnet 101004 1500 - - - ieee - 0 0

1005 trnet 101005 1500 - - - ibm - 0 0

B. Affectation des ports aux différents Vlans :

Pour affecter les différents ports, il faut être en mode **configuration globale.** L'invite est alors : **Switch(config)#** et il faut passer en mode configuration d'interface à l'aide de la commande **"FastEthernet** *N°port***"**.

```
Switch#configure terminal
Switch(config)#interface fastEthernet 0/2
```

Il faut ensuite affecter le port au vlan souhaité.

Switch(config-if)#switchport mode access

```
Switch(config-if)#switchport access vlan 2
```

L'opération est à répéter pour tous les ports dont on veut modifier le vlan d'appartenance.

La commande "**Show Vlan**" en mode **EXEC privilégié** permet de vérifier l'affectation des ports.

VIII. CONFIGURATION DES VLANS SUR PLUSIEURS COMMUTATEURS :

Lorsque les Vlans sont répartis sur plusieurs commutateurs, un lien particulier est mis en place entre les commutateurs. Ce lien configuré en **mode Trunk**, transmet la trame en ajoutant 4 octets indiquant le vlan d'appartenance.

La configuration de l'interface se fait à partir du mode de **configuration globale**.

```
Switch#conf t

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport mode trunk
```

IX. AFFECTATION D'UNE ADRESSE IP A UN VLAN :

Si on veut pouvoir administrer un commutateur à partir d'un client Telnet sur un PC, ou par l'une des interfaces LAN ou WAN, il faut affecter une adresse IP au vlan d'administration qui est souvent le vlan par défaut. La configuration de l'interface se fait à partir du mode de **configuration globale**.

```
Switch(config)#interface vlan 1

Switch(config-if)#ip address ip-address ip-mask

Switch(config-if)#no shutdown
```

Il faut ensuite tester le fonctionnement de l'interface en mode **EXEC privilégié**.

```
Switch#ping ip-address

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to ip-address, timeout is 2
seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max =
1/2/4 ms

Switch#
```

X. SECURITE

A. Port inactif

```
Switch(config)# interface fastethernet0/12


Switch(config-if)# shutdown


Switch(config)# interface range fastethernet0/1 - 5


Switch(config-if-range)# shutdown
```

B. Réservation statique

```
Cet exemple montre comment configurer une "MAC ADDRESS" bloquée statique et
une "MAC ADDRESS" bloquée collant sur le port FastEthernet 1


Switch(config)# interface fastethernet0/12


Switch(config-if)# switchport mode access


Soit

        Switch(config-if)# switchport port-security


        Switch(config-if)# switchport port-security mac-address
0000.02000.0004


Ou bien

        Switch(config-if)# switchport port-security mac-address sticky


        Switch(config-if)# switchport port-security mac-address sticky
0008.a343.b581
```

```
Switch(config-if)# end

Switch# show port-security address

=          Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0000.0000.000a    SecureDynamic       Fa0/1      -
   1    0000.0002.0300    SecureDynamic       Fa0/1      -
   1    0000.0200.0003    SecureConfigured    Fa0/1      -
   1    0000.0200.0004    SecureConfigured    Fa0/12     -
   1    0003.fd62.1d40    SecureConfigured    Fa0/5      -
   1    0003.fd62.1d45    SecureConfigured    Fa0/5      -
   1    0003.fd62.21d3    SecureSticky        Fa0/5      -
   1    0005.7428.1a45    SecureSticky        Fa0/8      -
   1    0005.7428.1a46    SecureSticky        Fa0/8      -
   1    0006.1218.2436    SecureSticky        Fa0/8      -
   1    0008.a343.b581    SecureSticky        Fa0/12     -
----------------------------------------------------------------------
```

C. Réservation dynamique

```
Cet exemple montre comment activer la sécurité sur le port FastEthernet 1
et comment fixer le nombre maximum d'adresses apprises.

Switch(config)# interface fastethernet0/1
```

```
Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 50

Switch(config-if)# switchport port-security mac-address sticky

Switch(config-if)# end

Switch# show port-security interface fastethernet0/1
 Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses :50
Total MAC Addresses: 11
Configured MAC Addresses: 0
Sticky MAC Addresses :11
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

XI. OPTIMISATION DES LIAISONS ENTRE SWITCHs

A. Agrégation de liens

```
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if)# channel-group 5 mode on
Switch(config-if)# end
```

B. STP (Spanning Tree)