

# Commandes des commutateurs Cisco

## Table des matières

|       |  |   |
|-------|--|---|
| I     | Présentation du commutateur.....                                 | 1 |
| I.1   | Modes de configuration.....                                      | 1 |
| I.2   | Mémoires du commutateur.....                                     | 2 |
| I.3   | Procédure de démarrage.....                                      | 2 |
| II    | Commandes de base d'un commutateur Cisco.....                    | 3 |
| II.1  | Connexion au commutateur.....                                    | 3 |
| II.2  | Particularités des commandes.....                                | 3 |
| II.3  | Visualisation des informations générales sur le commutateur..... | 3 |
| II.4  | Changement du nom d'hôte du commutateur.....                     | 3 |
| II.5  | Mise en place de mots de passe.....                              | 4 |
| II.6  | Gestion de la configuration.....                                 | 4 |
| II.7  | Gestion des interfaces.....                                      | 4 |
| II.8  | Les commandes pour la table des adresses MAC.....                | 5 |
| II.9  | Les commandes de contrôle d'accès.....                           | 5 |
| II.10 | Connexion au commutateur par réseau.....                         | 6 |
| III   | Commandes pour les réseaux virtuels.....                         | 6 |
| III.1 | Création d'un VLAN.....  | 7 |
| III.2 | Configuration des ports.....                                     | 7 |
| III.3 | Visualisation des informations d'un VLAN.....                    | 8 |
| IV    | Mise en place du protocole SNMP.....                             | 8 |

## I Présentation du commutateur

Un commutateur réseau (ou switch en l'anglais) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs (entre 4 et 100) ports Ethernet permettant de relier des systèmes réseau (ordinateurs, imprimantes, serveurs, ...) entre eux.



En schématisant, un commutateur est un ordinateur possédant des nombreuses interfaces ou port Ethernet. Il permet d'établir une connexion entre un système et un autre après avoir analysé les adresses MAC du destinataire de la trame, systèmes connectés aux ports du commutateur.

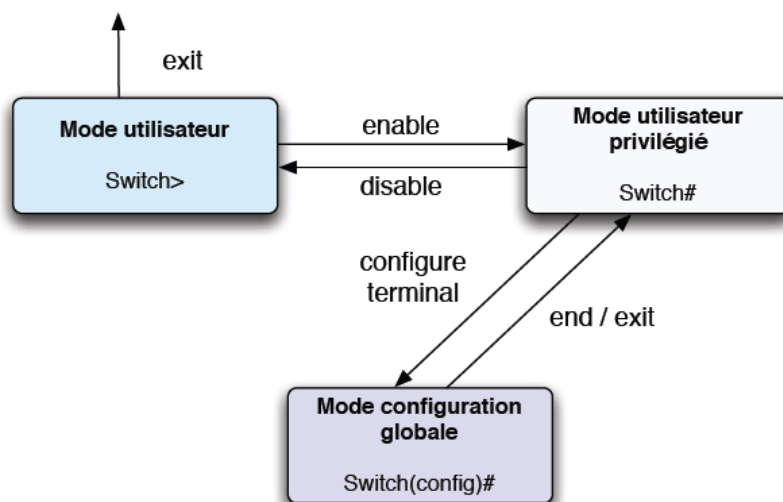
Comme tout ordinateur, les commutateurs Cisco exécutent un système d'exploitation. Cet OS embarqué est appelé IOS pour Internetworking Operating System. L'interaction à distance avec ce système permet notamment la modification de la configuration du commutateur, autrement dit sa programmation. La gestion (visualisation/modification) de la configuration du commutateur peut s'effectuer à travers plusieurs canaux (pouvant être activés indépendamment les uns des autres et actifs simultanément).

Pour configurer le commutateur, nous allons utiliser l'interpréteur de commande appelé CLI (Command Line Interface), accessible depuis un terminal série.

### I.1 Modes de configuration

Les modes de configuration déterminent les commandes autorisées. Trois modes de configuration existent :

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

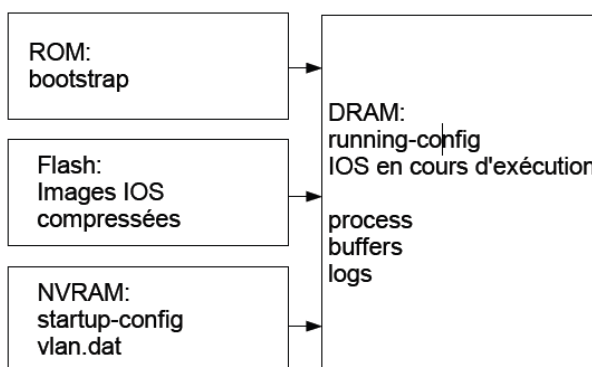


- x **Mode utilisateur** : quelques commandes d'affichage sont disponibles, pas de modification permanente de la configuration possible à ce niveau. Il est symbolisé par > .
- x **Mode privilégié** : C'est l'équivalent d'un accès root sous Linux. Symbole : #. Pour quitter le mode privilégié et revenir au mode utilisateur, tapez la commande disable.
- x **Mode de configuration** : Mode permettant l'accès à la configuration globale du matériel.

## I.2 Mémoires du commutateur

Chaque commutateur possède différents types de mémoire : la DRAM, la NVRAM, la mémoire Flash, et la ROM.

1. Mémoire ROM (non volatile) : elle contient le logiciel minimum utilisable en cas de problème (bootstrap).
2. Mémoire DRAM (volatile), mémoire de travail : elle contient l'IOS en cours d'exécution, la configuration en cours d'exécution/modification (running-config), les logs, statistiques, buffers réseaux, les processus, etc.
3. Mémoire Flash (non volatile) : elle contient les images IOS (IOS : système d'exploitation) compressées.
4. NVRAM (non volatile) : elle contient le configuration de démarrage (startup-config).



## I.3 Procédure de démarrage

Au démarrage la séquence d'initialisation est la suivante :

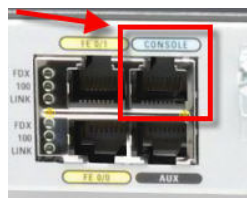
1. Chargement du bootstrap de la ROM vers la DRAM (programme qui va être exécuté ensuite) ;
2. Test de la plate-forme pour vérifier qu'aucune erreur dans la mémoire par exemple ;
3. Chargement de l'IOS de Flash vers DRAM (la mémoire flash contient une image compressée de l'IOS qui sera donc décompressée avant d'être chargée) ;
4. Chargement du fichier de configuration du commutateur de la NVRAM (fichier startup-config) vers la DRAM (fichier running-config).

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

## II Commandes de base d'un commutateur Cisco

### II.1 Connexion au commutateur

Pour configurer le commutateur, il faut connecter son port console grâce à un câble console (câble bleu), au port série de votre ordinateur.



Les paramètres de configuration du port série sont les suivants :

|                  |               |
|------------------|---------------|
| Vitesse          | 9600 bps      |
| Bits de Données  | 8             |
| Bits de Stop     | 1             |
| Parité           | Pas de parité |
| Contrôle de flux | Aucun         |

Nous supposons dans la suite que vous vous êtes connecté via le port série au port console du commutateur.

### II.2 Particularités des commandes

Vous pouvez à tout moment connaître toutes les commandes possibles en tapant « ? ». De plus, la commande peut être terminée automatiquement grâce à la touche **TAB**.

Avec les touches flèches vers le haut ou vers le bas, vous pouvez remonter dans l'historique.

Toute commande peut être inversée en la précédant du mot **no**.

**Exemple** : *shutdown* désactive une interface réseau, *no shutdown* l'active.

### II.3 Visualisation des informations générales sur le commutateur

Vous pouvez avoir toutes les informations sur le matériel constituant le commutateur ainsi que sur l'IOS :

```
Switch>show version
```

**Exemple partiel :**

```
Switch>show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (
fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000

ROM: Bootstrap program is is C2950 boot loader

Switch uptime is 1 minutes, 17 seconds
System returned to ROM by power-on

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.

Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)
```

### II.4 Changement du nom d'hôte du commutateur

Vous pouvez modifier le nom du commutateur selon sa position géographique, son utilisation par exemple, afin de pouvoir le différencier des autres lors d'une connexion.

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

Pour configurer le nom d'hôte du commutateur, vous devez utiliser la commande **hostname** en mode de configuration générale.

**Exemple** : Configuration avec le nom d'hôte CustomerSwitch

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname CustomerSwitch      Nom du commutateur : CustomerSwitch
CustomerSwitch(config)#exit
```

## II.5 Mise en place de mots de passe

L'accès la configuration du commutateur peut être protégé par des mots de passe afin d'éviter les piratages.

Le premier est pour empêcher tout accès au commutateur (aucune commande autorisée). Le second interdit la commande enable qui permet de passer dans le mode privilégié. Les exemples ci-dessous montrent leur mise en œuvre.

x Définition du mot de passe de console cisco123 :

```
Switch#configure terminal
Switch(config)#line console 0              Le mot de passe via le port console
Switch(config-line)#password cisco123      est cisco123
Switch(config-line)#login
Switch(config-line)#exit
```

x Définition du mot de passe secret du mode d'exécution privilégié sur cisco123 :

```
Switch(config)#enable password cisco123
```

Dans ce cas le mot est stocké dans le fichier running-config en clair. Si vous voulez qu'il soit stocké crypté, vous devez utiliser la commande suivante :

```
Switch(config)#enable secret cisco123
```

Si vous accédez au commutateur via le réseau, il faut également protéger son accès grâce aux commandes « line vty » et « password » :

```
Switch#configure terminal
Switch(config)#line vty 0 15
Switch(config-line)#password cisco123
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#exit
```

## II.6 Sauvegarde de la configuration

Deux configurations sont dans votre commutateur :

- x La configuration actuelle (celle en cours) ;
- x La configuration au démarrage.

Lors du démarrage du commutateur, la configuration au démarrage est celle appliquée. En cas de modification de la configuration, seule la configuration en cours est modifiée. Donc si vous ne copiez pas la configuration en cours dans celle au démarrage, vos modifications ne seront pas prises en compte.

Remarque : un commutateur n'est jamais éteint mais il peut y avoir tout de même une coupure de courant donc la sauvegarde est importante.

x Visualisation de la configuration en cours :

```
Switch#show running-config
```

x Visualisation de la configuration au démarrage :

```
Switch#show startup-config
```

x Enregistrement de la configuration :

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

```
Switch#copy running-config startup-config
```

## II.7 Gestion des interfaces

Vous pouvez visualiser les interfaces, les désactiver ou les activer (elles sont activées par défaut).

- x Affichage des interfaces du commutateur :

```
Switch#show interfaces
```

- x Affichage des informations de l'interface mentionnée :

```
Switch#show interfaces FastEthernet0/2
```

- x Désactivation de l'interface :

```
Switch(config)#interface FastEthernet0/2
```

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

- x Activation de l'interface :

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

## II.8 Les commandes pour la table des adresses MAC

Au fur et à mesure que des connexions sont réalisées entre les différents ports, le commutateur apprend quels sont les adresses MAC des équipements connectés sur ces ports. Ces informations sont stockées dans la table des adresses MAC.

- x Affichage de la table des adresses MAC :

```
Switch#show mac-address-table
```

Mac Address Table

```
-----
```

| Vlan | Mac Address    | Type    | Ports  |
|------|----------------|---------|--------|
| ---- | -----          | -----   | -----  |
| 1    | 0001.430b.6418 | DYNAMIC | Fa0/24 |
| 1    | 0006.2a92.ac98 | DYNAMIC | Fa0/8  |
| 1    | 0090.2104.d99d | DYNAMIC | Fa0/1  |

- x Effacement de la table des adresses MAC

```
clear mac-address-table dynamic
```

- x Ajout d'une adresse mac statique

Dans de rares cas, vous pourriez souhaiter ajouter manuellement une adresse MAC dans la table.

```
mac-address-table static <adresse-mac> vlan <vlan-id> interface <identifiant-interface>
```

## II.9 Les commandes de contrôle d'accès

L'objectif de cette partie est de limiter l'accès à un port à une machine spécifique grâce à son adresse MAC. Ainsi un autre ordinateur ne pourra pas se connecter à la prise réseau correspondante.

Avec les commutateurs Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option « Port-security ».

Il y a deux méthodes, la première consiste à enregistrer manuellement l'adresse MAC autorisée et la seconde consiste à prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer une trame en premier à ce port du commutateur Cisco.

- x Pour visualiser la politique de sécurité d'une interface (fa0/1 dans l'exemple) :

```
Switch#show port-security interface fa0/1
```

- x Pour visualiser les adresses MAC connues sur les ports

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

Switch#**show port-security address**

- x Pour faire un contrôle sur les adresses MAC des machines qui ont le droit de se connecter sur un port :

switchport mode access

switchport port-security

- x Pour définir les adresses MAC autorisées sur un port :
  - ✓ Adresse MAC fixée manuellement:

switchport port-security mac-address <@MAC\_autorisée>

- ✓ Adresse MAC (source) apprise automatiquement à partir de la première trame qui traversera le port :

switchport port-security mac-address sticky

**Exemple :**

Switch#**configure terminal**

Switch(config)#**int fa 0/3**

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

Switch(config-if)#**switchport port-security**

Switch(config-if)#**switchport port-security mac-address 0050.5611.06b1**

**ou**

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

- x Pour autoriser plus d'une seule adresse MAC par port (10 dans l'exemple) :

Switch(config-if)#**switchport port-security maximum 10**

- x Pour effacer la table des adresses MAC, déverrouiller la sécurité des adresses MAC et permettre l'enregistrement d'une nouvelle adresse :

Switch#**clear mac-address-table dynamic**

- x Pour bloquer le port en cas d'usurpation :

Switch(config-if)#**switchport port-security violation shutdown**

- x Pour ne bloquer que les trames d'adresses MAC inconnues :

Switch(config-if)#**switchport port-security violation protect**

- x Pour émettre un message dans le syslog et via SNMP :

Switch(config-if)#**switchport port-security violation restrict**

- x Pour réactiver un port désactivé automatiquement, suite à un problème de sécurité, faire un **shutdown** suivi d'un **no shutdown**.

## II.10 Connexion au commutateur par réseau

Si vous voulez configurer par exemple, le commutateur via le réseau sans utiliser le câble console, il faut lui attribuer une adresse IP. Dans ce cas, il faut configurer le vlan correspondant à la connexion. Si vous n'avez pas configuré de vlan, il faut choisir **le vlan par défaut, le 1**.

- x Choix du VLAN en mode configuration :

interface vlan <vlan-id>

- x Définition de l'adresse IP et du masque réseau en mode de configuration de l'interface :

ip address <ip-address> <subnet-mask>

- x Définition de la passerelle par défaut en mode configuration :

ip default-gateway <ip-address>

**Exemple :**

Switch#**configure terminal**

Switch(config)#**int vlan 1**

Switch(config-if)#**ip address 192.168.0.253 255.255.255.0** L'adresse sur le vlan 1 est 192.168.0.253/24

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

|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

```
Switch(config-if)#ip default-gateway 192.168.0.254 La passerelle par défaut est 192.168.0.254
Switch(config-if)#end
```

### III Commandes pour les réseaux virtuels

Les commutateurs permettent généralement de gérer plusieurs VLAN (Virtual Local Area Network) dans un même commutateur. La configuration type dans ce cas comprend :

- x La création des VLANs sur le commutateur ;
- x L'attribution des interfaces désirées dans les différents VLANs ;
- x La définition de la liaison entre les commutateurs ou le commutateur et le routeur comme un « trunk ».

Il faut ensuite configurer le routeur pour qu'il réalise le routage entre les différents VLANs.

#### III.1 Création d'un VLAN

Les commandes pour la création d'un VLAN sont :

```
vlan <vlan_id>
name <nom_du_vlan>
```

**Exemple :**

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Technique
Switch(config-vlan)#exit
Switch(config)#exit
```

Le VLAN 10 est créé  
et a pour nom Technique

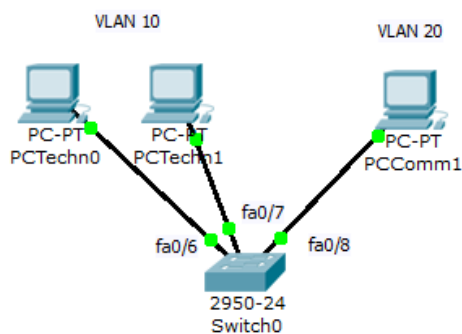
#### III.2 Configuration des ports

##### a Mise d'une interface dans un VLAN

La commande est la suivante :

```
switchport access vlan <vlan_id>
```

**Exemple :**



```
Switch#configure terminal
Switch(config)#interface fastEthernet0/6
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastEthernet0/8
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastEthernet0/8
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
```

Le port fa0/6  
est dans le vlan 10  
Le port fa0/7  
est aussi dans le vlan 10  
Le port fa0/8  
est dans le vlan 20

Pour affecter plusieurs ports à un vlan, on peut sélectionner les ports grâce à la commande :

```
interface range fastEthernet [port – port]
```

Switch: les ports 5 à 8 dans le vlan 4

```
Switch(config)#interface range fastEthernet 0/6 – 7 Les ports fa0/6 à fa0/7
```



|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

```
Switch(config-if-range)#switchport access vlan 10      sont dans le vlan 10
Switch(config-if-range)#end
Switch(config)#exit
```

## b Configuration du port en mode trunk

Le mode **trunk** est utilisé dans le cas où plusieurs VLANs doivent circuler sur un même lien donc la liaison entre les commutateurs est en mode trunk. Les autres ports des commutateurs sont en mode **access**.

Ce mode trunk est aussi utilisé pour communiquer avec le routeur en charge d'effectuer le routage entre les VLANs.

La commande pour définir le mode est :

```
switchport mode {access | dynamic {auto | desirable} | trunk}
```

Les liaisons entre les commutateurs et le routeur sont en mode trunk et doivent donc être configurées en le précisant.

**Exemple** : le port fa0/1 sert à laisser passer tous les VLANs vers un autre commutateur ou un routeur

```
Switch#configure terminal
Switch(config)#interface fastethernet0/1      Le port fa0/1 est configuré en trunk
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch(config)#exit
```

## III.3 Visualisation des informations d'un VLAN

Voici quelques commandes pour visualiser les informations sur les VLANs :

- x Visualisation de l'ensemble des VLANs et des ports (version courte) :

```
show vlan brief
```

- x Visualisation des ports d'un vlan :

```
show vlan id <vlan_id>
```

- x Visualisation des agrégations de VLAN pour les communications entre commutateurs :

```
show interface trunk
```

**Exemple :**

```
Switch-1#sh interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    99
Fa0/3     on        802.1q         trunking    99

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99
```

## IV Mise en place du protocole SNMP

Pour superviser les commutateurs Cisco, il faut activer le protocole SNMP sur ceux-ci. En effet, le protocole SNMP permet notamment de récupérer des informations statistiques sur les équipements réseaux.

La commande de base est :

```
snmp-server community string [view view-name] [ro | rw] [access-list-number]
```

- x Elle configure la communauté string.



|                               |                                  |
|-------------------------------|----------------------------------|
| BTS SNIR                      | Document ressource               |
| Lycée Jean Rostand Villepinte | Commandes des commutateurs Cisco |

x ro | rw : lecture seule ou lecture/écriture

**Exemple** : 2 communautés essai en lecture simple et essaiRoot en lecture/écriture

```
Switch#conf t
Switch(config)#snmp-server community essai R0
Switch(config)#snmp-server community essaiRoot RW
Switch(config)#end
```

Pour activer chaque trap SNMP, il faut utiliser la commande suivante :

```
snmp-server enable traps type
```