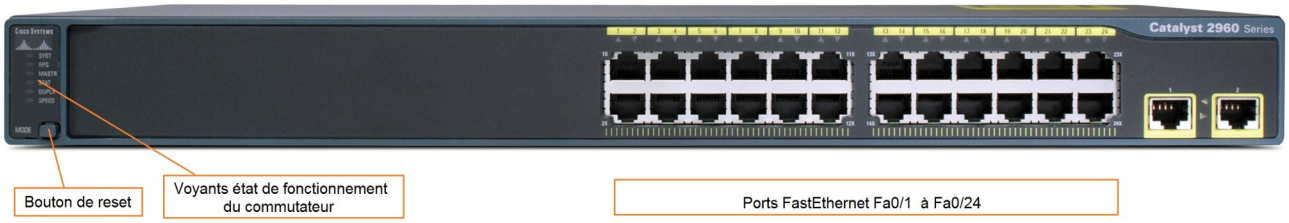
TP1
Configuration de VLAN statique - Sécurité

Il sera largement tenu compte du soin apporté à la rédaction: évitez le style SMS, numérotez soigneusement les réponses,évitez les fautes, faites des schémas précis contenant toutes les informations réseau de configuration...

Objectifs :

- Créer une configuration de base d'un commutateur et la vérifier ;
- Créer plusieurs VLANs, les nommer et leur affecter des ports membres ;
- Tester la fonctionnalité en transférant une station de travail d'un LAN virtuel à un autre ;
- Enlever une interface d'un VLAN et supprimer un VLAN ;
- Analyser un fichier de configuration d'un commutateur et en déduire toute la configuration VLAN statiques créée.



En début et fin de séance :

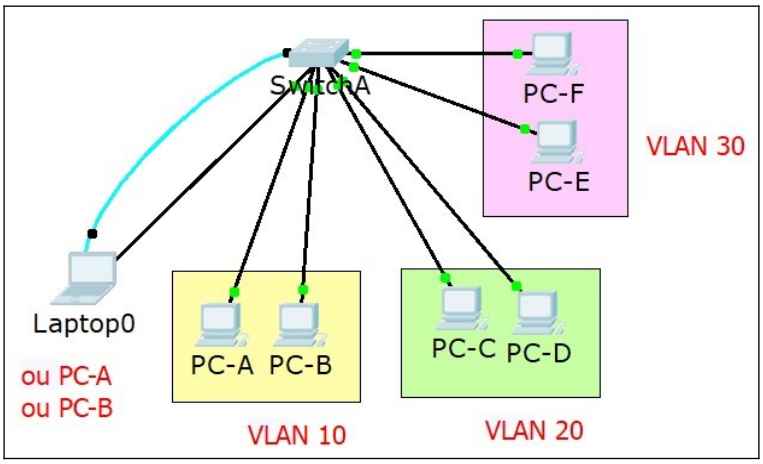
Le commutateur est normalement dans son état standard.

Vérifier malgré tout que tout qu'il a bien été réinitialisé par show vlan (demander à votre professeur si besoin).

Sinon, voir la rubrique « Réinitialiser la configuration » dans l'annexe. Re-vérifier que tout a bien été réinitialisé par show vlan.

Schéma réseau du TP : seuls 2 PC seront utilisés (PC-A et PC-B).

Note : Le schéma réellement utilisé sera à reporter dans votre compte-rendu et à compléter avec les adresses IP / masque réseau de chaque élément.



1) Préparation *(ceci est un rappel : à effectuer en début et en fin de séance).*

La station près de la baie étant connectée sur le port console du commutateur , démarrer un terminal en ligne de commande et suivez les consignes ci-contre pour accéder à distance à la configuration du commutateur.

Fenêtre console sur commutateur :

- *ouvrit une fenêtre Terminal*
- *saisir minicom -s*
- *choisir menu "sortir"*
- *répondre no aux questions posées au démarrage du commutateur*

Démarrez le commutateur :

n'entrez pas dans le mode de configuration rapide en répondant **no** (voir copie écran ci-dessous)

```
         --- System Configuration Dialog ---

Enable secret warning
---------------------------------
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the intial configuration dialog, or if you exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
----------------;----------------
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

En suite, effacez la configuration du commutateur :

```
Switch> enable
Switch# delete flash:vlan.dat
Delete filename [vlan.dat]? [Entrée]
Delete flash:vlan.dat? [confirm][Entrée]
S'il n'y a pas de fichier VLAN, un message d'erreur apparaît.
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files ! [confirm][Entrée]
Switch# reload
```

Note : Au redémarrage, n'entrez pas dans le mode de configuration rapide (no)

2) Configuration usine d'un commutateur.

Sur le commutateur, tapez la commande « **show vlan** » à l'invite de commande privilégié :

1) Quels ports appartiennent au VLAN par défaut ?

2) Combien de VLAN sont configurés par défaut sur le commutateur ?

3) Comment s'appelle le VLAN 1003 ?

4) Combien de ports comporte le VLAN 1 ?

5) Quelles sont les deux commandes permettant d'obtenir les informations sur un VLAN précis ? Saisir la commande « **show vlan ?** » pour obtenir les options de cette commande.

6) Saisir la commande « **show running-config** » pour obtenir le contenu de base de la mémoire running-configuration (voir annexe 1). Copier / coller cette configuration initiale dans votre compte-rendu.

3) Configuration de base du commutateur.

1) Configurez les paramètres généraux du commutateur :

- Nom du commutateur: Switch_A

2) Vérifier le statut de l'interface **vlan1**. Qu'est-il indiqué si l'interface n'est pas démarrée ? Et si elle est démarrée ?

3) Configurez les paramètres réseau des stations (hôtes) reliées au commutateur.

Toute la configuration sera faite en ligne de commande (voir annexe). Visualisez les interfaces réseau de votre machine (**ip a**) et configurez l'interface réseau non utilisée (en général la carte fille Ethernet).

- Relier les PC-A et PC-B respectivement aux ports 1 et 2 du switch.
- Demander une adresse réseau à votre enseignant.
- Configurez les paramètres IP des PC-A et PC-B pour qu'ils soient dans le même réseau que le commutateur.

4) Vérifiez la connectivité du réseau.

4) Création des VLAN.

Numéro du VLAN	Nom du VLAN	Affectation des ports du commutateur
VLAN 10	Comptabilité	Fa0/5 à Fa0/8
VLAN 20	Marketing	Fa0/9 à Fa0/12
VLAN 30	Ingénierie	Fa0/13 à Fa0/16

1) Créez et nommez les VLAN comme indiqué sur le tableau ci-dessus (sans les accents !).

2) Affichez les informations sur les VLAN. Quels changements pouvez-vous remarquer lorsque l'on exécute la commande d'information générale sur les vlans (« **show vlan** ») ?

5) Affectation des ports aux VLAN.

1) Suivant le tableau des VLAN ci-dessus, affectez les ports du commutateur à leur VLAN respectif.

2) Quels nouveaux changements pouvez-vous remarquer lorsque l'on exécute la commande d'information générale sur les vlans (« **show vlan** ») ?

3) Tapez la commande « **show running-config** » pour obtenir le contenu de base de la mémoire running-configuration (voir annexe 1). Copier / coller cette configuration modifiée dans votre compte-rendu. Comparez là avec la configuration obtenue à la question 6. Surligner les changements et indiquer à quoi correspondent ces lignes supplémentaires.

6) Vérification de la configuration des VLAN.

Pour les besoins de cette question, nous allons ajouter une adresse IP sur le vlan 1.

1) Configurez une adresse IP au VLAN 1

Attention : après avoir attribué une IP au switch, ne pas oublier de démarrer l'interface !

2) Vérifier le statut de l'interface. Qu'est-il indiqué si l'interface n'est pas démarrée ? Et si elle est démarrée ?

Ouvrir deux fenêtres de terminaux linux sur le PC-B. Dans la première, pinguer le VLAN1 du switch et dans la seconde, pinguer PC-A. On laissera ces commandes tourner en continu, ce qui permettra de surveiller les connexions.

: le fait de débrancher le câble réseau risque de faire perdre l'adresse IP configurée sur l'hôte. A chaque branchement, revérifiez si l'interface réseau est bien configurée (**ip a**). Sinon rappeler la ligne de configuration de l'adresse IP et du masque et vérifiez toujours le résultat (**ip a**) avant de pinguer

3) De quelles couleurs sont les DELs des deux ports ? Les requêtes « ping » (sur le switch ET sur PC-A) aboutissent-elles ? Dans les questions suivantes, vous expliquerez pourquoi cela fonctionne ou pas ou seulement après un certain temps. Ces questions constituent le cœur du TP !

4) Passer PC-B sur le port 5 du switch: qu'observez-vous (mêmes questions)

5) Passer PC-A sur le port 6 : qu'observez-vous ?

6) Passer PC-B sur le port 9 : idem

7) Passer le port 6 dans le VLAN Marketing: mêmes questions.

7) Suppression de la configuration des VLAN.

1) Supprimez le port Fa0/6 du VLAN 20. Quels nouveaux changements pouvez-vous remarquer lorsque l'on exécute la commande d'information générale sur les vlans ?

2) Supprimez intégralement le VLAN Marketing. Que pouvez vous remarquer à propos des ports précédemment configurés dans le VLAN Marketing ?

3) Supprimez intégralement le VLAN 1 (VLAN de gestion). Conclusion ?

4) Tout en continuant à pinguer le switch et PC-A depuis PC-B, réinitialiser le switch. Décrire ce qui se passe pendant et après. Chronométrez le temps mis pour retrouver la connectivité réseau.

5) Faire un « **show vlan** » et vérifier que tout est en ordre.

8) Sécurisation de l'accès aux ports Fa0/x.

Dans une entreprise, il ne faut pas que les utilisateurs puisse connecter leur ordinateur sur le réseau filaire de celle-ci.

1) Pour les interfaces du vlan 10 configurez chaque interface avec l'adresse MAC de la station normalement branchée sur celle-ci. En cas de branchement d'un autre équipement, la communication doit être bloquée. Mais si l'on rebranche la station initiale, la communication doit reprendre sans intervention des responsables informatiques. Réalisez la configuration demandée.

2) Testez la sécurisation des ports du vlan 10. Décrivez le procédé de test pour valider le bon fonctionnement de la sécurisation des ports. Visualiser la configuration réalisée.

3) Configurer l'adresse MAC sur chaque port peut être fastidieux. Que faudrait-il modifier dans la configuration ci-dessus pour que chaque port apprenne automatiquement l'adresse MAC de la station qui lui est normalement connectée. Réalisez cette configuration sur le vlan 20.

4) Testez la sécurisation des ports du vlan 20. Décrivez le procédé de test pour valider le bon fonctionnement de la sécurisation des ports. Où sont stockées les adresses MAC apprises automatiquement par les ports ?

Visualiser la configuration réalisée.

9) Sécurisation de l'accès physique (via le port console).

Même si tous les périphériques intermédiaires sont regroupés dans une pièce fermée à clefs, il faut protéger l'accès physique permettant d'accéder aux paramétrages des commutateurs.

1) Configurez le mot de passe ***cisco1*** pour accéder en mode utilisateur via le port console.

2) Configurez un message d'avertissement "***Accès aux personnes autorisées seulement***".

3) Configurez le mot de passe ***class*** pour accéder en mode privilégié.. Ce mot de passe devra être crypté.

4) Saisissez la commande « **show running-config** » pour obtenir le contenu de base de la mémoire running-configuration. Comment sont stockés les mot de passe ?

5) Déconnectez vous du commutateur. Puis reconnectez vous pour arriver en mode privilégié. Testez l'apparition du message d'alerte et de la validité des mots de passe configurés.

10) Sécurisation des accès à distance : Telnet.

Expérimentez l'accès à distance via Telnet. On en profitera pour regarder ce qui se passe sur la liaison Ethernet via WireShark.

1) Configurez les lignes vty pour accéder à distance au commutateur :

- Créez le vlan 89 et y affecter l'interface Fa0/24.
- Mettez une adresse IP sur la vlan 89 (gestion). L'adresse réseau à utiliser : 192.168.89.0 /24
- Configurez la ligne **`vty 0`** pour un accès distant. Mot de passe à utiliser : ***cisco2*** (tout en minuscule). Le mot de passe devra être crypté.
- Configurez les autres lignes `vty 1 à 5` pour interdire tout accès distant.

2) Saisissez la commande « **show running-config** » pour obtenir le contenu de base de la mémoire running-configuration. Comment sont stockés les mot de passe ?

3) Sur la station qui fera la gestion à distance *(utiliser la station non reliée par le câble console Cisco)* :

- Reliez le câble Ethernet sur le port du vlan 89 (à préciser).
- Configurez l'adresse IP de la station (même réseau que le vlan 89).
- Testez la connectivité de la station avec le vlan 89.

4) Réalisez un accès à distance au commutateur via **`telnet`** tout en capturant ce qui se passe sur le réseau avec Wireshark :

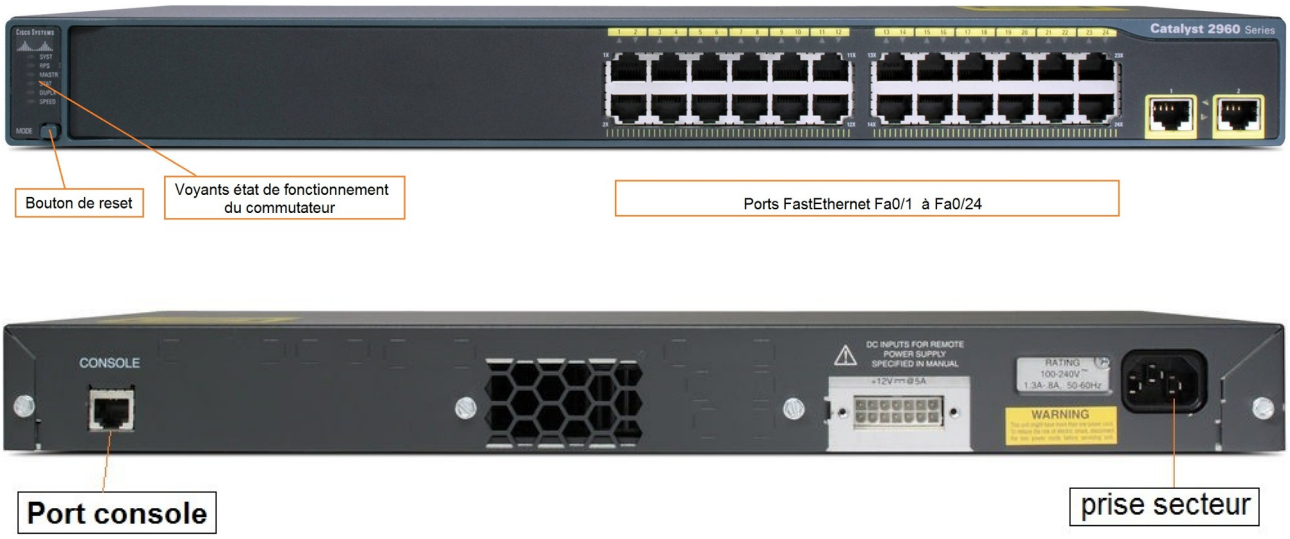
- Démarrer Wireshark.
- Depuis le terminal `minicom` et se connecter au commutateur en mode privilégié. Créer un vlan et y affecter 2 ou 3 interfaces. Saisir la commande « **show vlan ?** » pour vérifier le résultat.
- Déconnectez vous puis arrêtez le logiciel Wireshark.

5) Analyser le contenu des trames (filtre **telnet**). Que constate-t-on au niveau du mot de passe et des commandes Cisco ? Afficher le diagramme des flux de trames entre la station et le commutateur.

6) Réinitialiser la configuration du commutateur (voir annexe ou éteindre le commutateur). Vérifiez en saisissant la commande « **show running-config** ».

A faire vérifier impérativement par à votre enseignant !

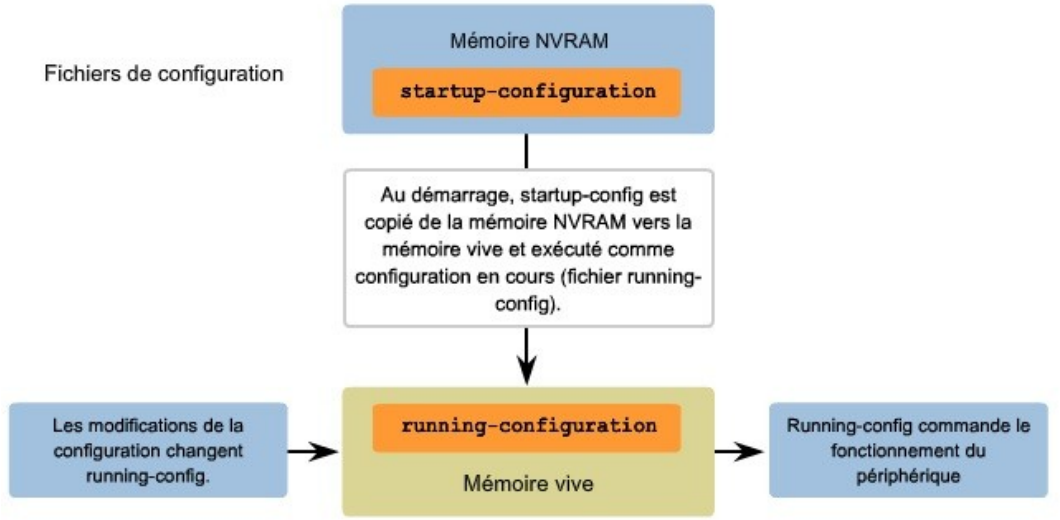
Annexe 1 : Le commutateur CISCO



A la mise sous tension, le contenu de la mémoire ***startup-configuration*** est recopié dans la mémoire ***running-configuration***.

Toutes les modifications de configuration sont faites dans la mémoire ***running-configuration***.

Une fois la configuration du commutateur mise au point, il faudra recopier le contenu de la mémoire running-configuration dans la mémoire startup-configuration. Sinon toute la configuration sera perdue en cas d'arrêt du commutateur.



Enfin, à la fin de la séance, il faudra impérativement réinitialiser le commutateur à son état standard. Pour cela, voir la rubrique « Réinitialiser la configuration » dans l'annexe2. Vérifier que tout a bien été réinitialisé par show vlan. Cette manoeuvre sera exécutée en début de séance si le switch n'a pas été correctement réinitialisé.

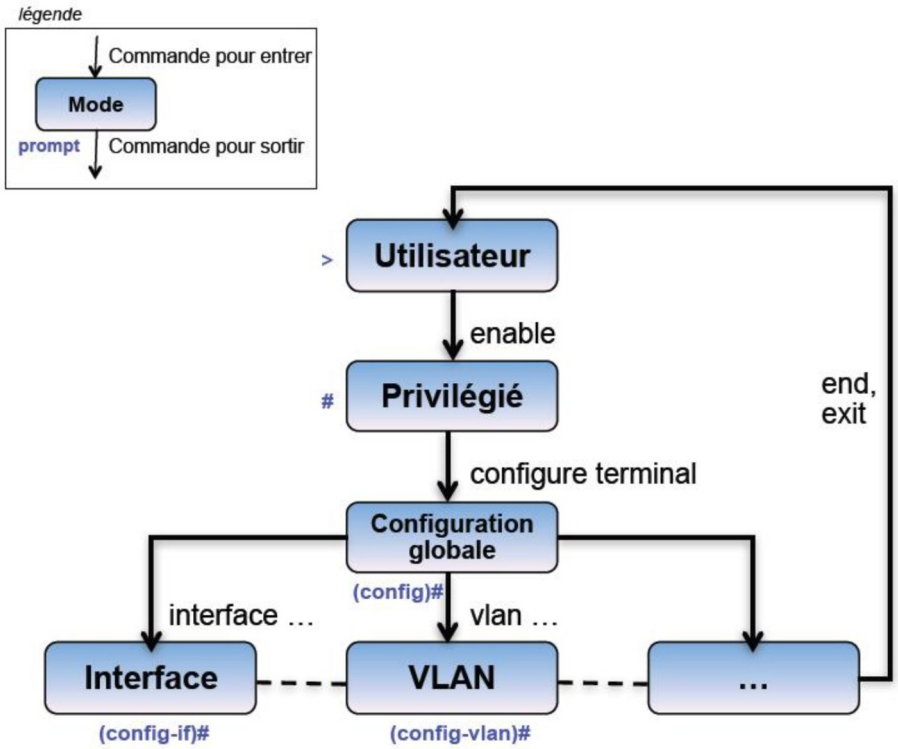
Annexe 1 (suite) : Le commutateur CISCO

Les principales commandes sont données en annexe2.

Le langage du commutateur Cisco est structuré en classes de commandes. Certaines commandes peuvent être utilisées en mode utilisateur, d'autres en mode privilégié, d'autres en mode de configuration, ...

Le mode courant est matérialisé par un prompt: >, #, (config#), ...

Le schéma ci-contre montre la façon dont les modes sont structurés, ainsi que la commande qui permet de passer de l'un à l'autre.



Les niveaux d'accès

Par mesure de sécurité, l'IOS sépare les sessions d'exécution en trois niveaux d'accès :

- **Mode exec ou utilisateur :** mode avec droits restreints (>) ;
- **Mode privilégié ou enable :** mode de consultation de la configuration (#) ;
- **Mode configuration (conf) :** mode de modification de la configuration ;

- **enable** : bascule en mode privilégié avec mot de passe ;
- **configure terminal ou conf t** : passer à la configuration globale en indiquant que celle-ci se fera à partir du terminal ;
- **exit** : pour descendre d'un niveau de commande ;
- **CTRL-Z ou end** : pour sortir du mode configuration ;

La commande la plus importante est la commande « point d'interrogation » ? : elle permet de voir les commandes disponibles et leurs différentes options.
Éventuellement, si elle est précédée de quelques lettres, elle liste les commandes commençant par ces lettres. Si elle est précédée d'une commande, elle liste les options qui peuvent suivre cette commande. Essayez !

La commande **no** est elle aussi importante: elle exprime l'annulation d'une commande précédente.
Dans ce TP, il faudra taper de nombreuses commandes, éventuellement plusieurs fois les mêmes. C'est ainsi que vous vous familiariserez avec le langage IOS de Cisco (qui sert pour les commutateurs **et** les routeurs Cisco)..

Les commandes peuvent être abrégées s'il n'y a pas ambiguïté. Par exemple, quelle commande la plus abrégée permet de passer du mode ***Privilégié*** au mode ***Configuration globale*** ? (utiliser ? Pour vous aider)

Annexe 2 : commandes pour commutateur CISCO

Nommer le commutateur
Switch(config)# hostname <*nom*>

Diagnostique VLAN
Switch# show vlan
Switch# show vlan ?
Switch# show interface <*port*> switchport
Switch# show vtp ?

Créer et nommer un VLAN
Switch(config)# vlan <*numéro_vlan*>
Switch(config-vlan)# name <*nom_vlan*>

Attribuer une IP à un VLAN
Switch(config)# interface vlan 1 *(1 ou autre numéro de vlan)*
Switch(config-if)# ip address <IP> <Mask>

Arrêter/démarrer une interface
Switch(config-if)# shutdown
Switch(config-if)# no shutdown

Vérifier le statut d'une interface (vis à vis de son adresse IP)
Switch# show ip interface brief vlan <*numéro_vlan*> *(« brief » est optionnel)*

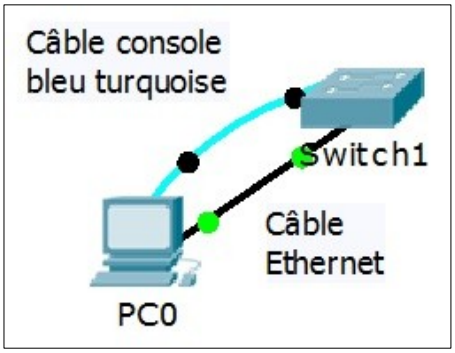
Affecter un port à un VLAN
Switch(config)# interface <*port*> *(<port> est le nom d'un port, par exemple Fa0/5)*
ou Switch(config)# interface range <*port_début*>-<*port_fin*> *(ex : interface range Fa0/5-10 ports de 5 à 10)*
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <*numéro_vlan*>

Supprimer un port d'un VLAN
Switch(config)# interface <*port*>
Switch(config-if)# no switchport access vlan

Supprimer un VLAN
Switch(config)# no vlan <*numéro_vlan*>

Visualiser la configuration actuelle
Switch# show running-config

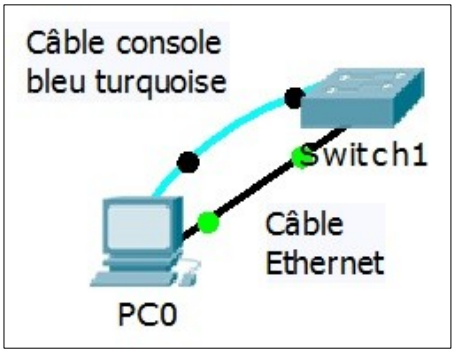
Réinitialiser la configuration
Switch# erase startup-config
Switch# delete flash:vlan.dat
Switch# reload *(A la question: configuration has been modified: Save ? Répondre « no »)*



Paramètres de la liaison série :
- *9600 bit/s,*
- *8 bits de données,*
- *pas de parité,*
- *1 bit d'arrêt,*
- *pas de contrôle de flux*

Fenêtre console sur commutateur :
- *ouvrit une fenêtre Terminal*
- *saisir minicom -s*
- *choisir menu "sortir"*
- *répondre no aux questions posées au démarrage du commutateur*

Annexe 2 : commandes pour commutateur CISCO (suite)



Nommer le commutateur

Switch(config)# hostname <*nom*>

Créer un vlan de gestion à distance

- *créer le vlan*
- *lui attribuer une adresse IP*
- *affecter un port Ethernet*

Configurer un mot de passe de user simple à user privilégié

Switch(config)# enable password <*mot_de_passe*>

ou

Switch(config)# enable secret <*mot_de_passe*>

========== *Pour configurer les lignes vty (Virtual TelTYpe text) pour Telnet* ==========

Configurer les lignes vty pour telnet

Switch(config)# line vty 0 15 *(selon nombre de connexions simultanées)*

Switch(config-line)# transport input telnet

Switch(config-line)# password <*mot_de_passe*>

Switch(config-line)# service password-encryption

Switch(config-line)# login

Switch(config-line)# exit

Démarrer un client Telnet sur une station Linux, avec Minicom :

- ***telnet @IP du vlan de gestion***

Sous Windows, démarrer un client Telnet avec Putty.

Désactiver les lignes vty

Switch(config)# line vty 5 (ex sur ligne 5)

Switch(config-line)# no login

========== *Pour sécuriser les interfaces Fa0/x* ==========

Configurer la sécurité des ports Fa0/i

Switch(config)# interface <*Fa0/i*> ou Switch(config)# interface FastEthernet <*0/i*>

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 1 *// activer l'apprentissage d'une adresse MAC sur ce port*

Switch(config-if)# switchport port-security mac-address *00 :01 :42 :99 :E0 :10* *// Adresse MAC à adapter*

Switch(config-if)# switchport port-security violation <*methode*>

Lorsqu'un hôte non autorisé se connecte sur un port sécurisé, le switch se doit de réagir a cette violation de la sécurité. Pour cela la commande `switchport port-security violation` avec 3 options différentes, qui sont :

- La méthode `shutdown` : elle désactive l'interface lorsque qu'il y a violation. L'administrateur réseau devra saisir successivement `shutdown` puis no `shutdown` pour réactiver l'interface.
- La méthode `protect` : toutes les trames ayant des adresses MAC sources inconnues sont bloquées et les autres autorisées.
- La méthode `restrict` : Alerte SNMP envoyée et le compteur de violation est incrémenté.

Il est possible de remplacer : Switch(config)# switchport port-security mac-address *0001.4299.E010*

par : Switch(configif)# switchport port-security mac-address sticky *// activer l'apprentissage rémanent*

Visualiser la configuartion des ports fa0/x

Switch# show port-security

Annexe 3 : commandes pour configurer une interface réseau sous Linux sous DEBIAN 9

 # Initialisation eno1 (ancien nom : eth0)
 # Pas obligatoire (car cela coupera l'accès à Internet)
ip link set eno1 down
ip addr flush eno1

 # Initialisation enp2s0 (ancien nom : eth1)
ip link set enp2s0 down
ip addr flush enp2s0

 # Activation de l'interface
ip link set enp2s0 up

 # Configuration de l'adresse
ip addr add <adresse>/<masque> dev <interface> (ici : enp2s0)

#Suppression d'une adresse IP
ip addr del <adresse>/<masque> dev <interface>

#Suppression de toutes les adresses d'une interface
ip addr flush <interface>

 # Configuration d'une route statique
ip route add <adresse>/<masque> via <adresse_passerelle>

 # Configuration de la route par défaut
ip route add default via <adresse_passerelle>

 # Suppression d'une route statique
ip route del <adresse>/<masque> via <adresse_passerelle>

 # Connexion Internet (client DHCP)
dhclient eno1

Autres commandes usuelles :

#Visualiser les paramètres d'une interface (↔ ifconfig)
ip addr ou **ip a** ou **ip addr show**

#Tester la connectivité entre 2 interfaces
ping <adresse IP dest.>