

Configuration et Administration d'un switch

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 ;

Le ? permet de voir les commandes disponibles et leurs différentes options.

Manipulation des configurations

Switch#**show running-config**

Switch#**show startup-config**

Switch#**Copy running-config startup-config** //ou le contraire

Switch(config)#**hostname RI-Switch** //attribue un nom au switch

Switch#**Show interfaces** // afficher les interfaces du switch

Switch#**Show interfaces identifiant_interface** // affiche les informations de l'interface mentionnée

Configuration d'une interface

Après passage en mode configuration d'interface, vous pouvez faire plusieurs manipulations :

Switch(config)#**interface nom_interface** // passer en mode configuration de l'interface donnée

Switch(config-if)#**duplex {auto|full|half}** // modifie le mode duplex

Switch(config-if)#**speed {auto|10|100|...}** // modifie la vitesse du port

Switch(config-if)#**shutdown** //désactive l'interface

Switch(config-if)#**no shutdown** // active l'interface

Définition des mots de passes

Switch(config)#**enable password** *mot-passe*

Switch(config)#**enable secret** *mot-passe*

Configuration du mot de passe console	Configuration du mot de passe terminal
Switch(config)# Line console 0 Switch(config)# Password mot-passe Switch(config)# Login	Switch(config)# Line vty 0 4 Switch(config)# Password mot-passe Switch(config)# Login

Switch(config)#**Service password-encryption** // crypter les mots de passes

A partir d'une poste, vous pouvez ouvrir une session sur le switch :

- terminal console sur le port série et à l'aide du logiciel terminal. Cet outil est équivalent à l'outil HyperTerminal de Windows (Programmes > Accessoires > Communications> HyperTerminal) ;

- terminal telnet, à l'aide de la commande DOS **telnet @IP_switch** ;

Manipulation de la table MAC et ARP

Switch#**show mac-address-table** // affichage table des adresses MAC

Switch#**clear mac-address-table dynamic** //effacer la table des adresses MAC

Switch(config)#**mac-address-table static adresse-mac vlan 1 interface identifiant-interface** // ajout d'une adresse mac statique

Switch#**show arp** //afficher la table arp

Définition d'une adresse ip du switch

Switch(config)#**interface VLAN 1**

Switch(config-if)#**ip address** *adresse_IP* *masque_réseau*

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

Switch(config-if)#**exit**

Les commandes de contrôle d'accès

✚ Pour éviter que n'importe qui se connecte sur les ports d'un switch, il est possible de faire un contrôle sur les adresses MAC des machines qui ont le droit de se connecter sur chaque port. Pour activer cette sécurité sur l'interface concernée :

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

- ✚ La définition des adresses MAC autorisées sur un port peut se faire de deux manières différentes soit :

- **Adresse MAC fixée manuellement:**

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

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

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

- ✚ Nous pouvons Limiter le nombre d'hôtes (adresses MAC) qui peuvent accéder sur chaque port

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

- ✚ Pour visualiser la politique de sécurité d'une interface, utiliser la commande suivante.

RI-Switch # **show port-security interface *nom_interface***

- ✚ Cette commande efface la table des adresses MAC, déverrouille la sécurité des adresses MAC et permet l'enregistrement d'une nouvelle adresse.

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

- ✚ Pour modifier les paramètres de sécurité, vous pouvez utiliser les commandes suivantes.

- **Désactivation de la sécurité sur le port**

RI-Switch(config-if)#**no switchport port-security**

- **Désactivation de l'apprentissage automatique d'adresse MAC**

RI-Switch(config-if)#**no switchport port-security mac-address sticky**

- **Suppression d'une adresse MAC de la liste des MAC autorisées**

RI-Switch(config-if)#**no switchport port-security mac-address 0008.744d.8ee2**

- ✚ En cas d'usurpation d'adresse MAC (accès d'une MAC non autorisées à l'interface), plusieurs politiques de sécurité peuvent être envisagées.

- **Blocage du port**

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

- **On bloque toutes les trames avec des adresses MAC non connu et on laisse passer les autres. Le port ne se bloque pas suite à un accès non autorisé.**

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

- **Soit un message dans le syslog et via SNMP sont envoyés. De plus le compteur du nombre de violation est incrémenté.**

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