TP– Découverte et préparation d'un switch

Contextualisation :

Lors d'un stage de votre BTS SIO, vous êtes au service informatique d'un Centre hospitalier. On vous demande de préparer un switch de type Cisco 2950 / 2960 / 3560. Vous devrez en faire la prise en main et la préparation basique du switch. Pour cela, votre tuteur vous donne un document qui vous permettra de réaliser cette tâche. Dans un premier temps, vous réaliserez cette activité sur Packet Tracer avant de le faire sur un actif réseau.

But : découverte de l'administration d'un switch

- atteindre la CLI par liaison console. Cette démarche est réalisée par le prof devant les élèves pour montrer la faisabilité d'une connexion par console. Puis tour à tour, chaque étudiant passe manipuler.
- Ce TP est destiné à privilégier la prise en main par essai-erreur d'un commutateur de LAN (en d'autres termes, vous devrez configurer les switch d'un réseau local).
- On y lira 3 articles. Le premier explique la connexion à la console d'administration. Le deuxième explique la nécessité de définir un VLAN d'administration. Le troisième montre la procédure à suivre pour configurer un switch.

Ce TP est à réaliser sous Packet Tracer dans un premier temps. Vous devez, à l'aide des articles ci-dessous, définir un VLAN d'administration pour gérer un switch.

Le quatrième article ira bien à ceux qui veulent approfondir, il s'agit d'établir une connexion sécurisée entre un PC et un switch.

Article 1 – première connexion à la CLI

La méthode de base pour configurer un switch Cisco est de se connecter via le port console de l'appareil. C'est en tout logique nécessaire pour une première configuration, mais ensuite, il est tout de même plus aisé de pouvoir accéder au CLI via un machine distante connectée au réseau. Voici les quelques paramètres à configurer pour rendre celà possible…

Pré-requis
Il faut bien entendu, lors d'une première configuration pouvoir se connecter au port console d'une manière ou d'une autre. Dans la majorité des cas, il faut disposer d'un port série sur le PC utilisé, d'un adaptateur RJ45-DB9 et d'un cable Rollover. Et enfin disposer d'un programme qui permet de gérer une communication sur port série comme Hyperterminal, PuTTY (pour les utilisateurs Windows).

- Brancher le câble Rollover au port console du switch.
- Placer l'adaptateur USB-DB9 sur le port USB du PC.
- Connecter le câble rollover sur l'adaptateur.

Il existe en outre un câble de connexion RJ45-DB9 complet qui ne demande donc plus d'adaptateur.

Il faut maintenant initialiser la connexion au port console via un programme terminal comme « Hyperterminal » ou PuTTY. Il faut en outre s'assurer que les paramètres suivants sont bien définis:

- Bits par seconde: 9600
- Data Bits: 8
- Parité: aucune
- Stop Bits: 1
- Contrôle de flux: aucun

Vu que chaque programme est différent, je ne vais pas détailler l'utilisation de ceux-ci.
Une fois la connexion établie, on accède à l'interface de configuration du switch.

```
Switch con0 is now available
Press RETURN to get started.
Switch>
```

Article 2 - Configurer l'interface VLAN d'administration du switch

Dans cet article nous allons voir comment configurer une adresse IP sur l'**interface VLAN d'administration** d'un switch.

Mais pourquoi définir une adresse IP à un switch? En soi, on n'en a pas besoin car ce qu'on demande au switch c'est principalement de **commuter les trames** des ordinateurs entre eux et vers le routeur de sortie Internet.

Si vous êtes chez vous que vous avez besoin de brancher plusieurs ordinateurs entre eux + votre imprimante + votre borne Wifi… alors vous pouvez acheter un petit switch 4 ou 8 ports dans une grande surface. Certains ne sont pas administrable, impossible de les configurer et pourtant ça fonctionne.

Le fait de configurer une adresse IP à un switch (qui est configurable) nous permet de prendre **la main à distance** et de le **configurer à distance**. La majorité des switchs d'entreprises sont configurés pour être joignables à distance par les administrateurs.

Ceux qui travaillent dans le support réseau ont régulièrement besoin d'accéder aux Switch pour ouvrir un port, le mettre dans un VLAN particulier, configurer la vitesse et le duplex de l'interface, analyser les statistiques du switch pour comprendre pourquoi un utilisateur se plaint de lenteur… et j'en passe…

Configuration de l'interface VLAN d'administration.

Nous verrons cela plus tard, mais le switch contient des VLAN qui servent à **isoler** des interfaces physiques entre elles.
Nous avons donc la nécessité de configurer une adresse IP sauf que le switch ne dispose pas du protocole IP. Par contre, dans les VLAN, il est possible de définir une interface virtuelle (donc avec une IP mais qui ne correspond à aucune interface physique). Il sera possible par la suite de se connecter à cette interface.

L'exemple ci-dessous doit être adapté à votre configuration ! Vous pouvez utiliser un réseau 172.16.4.253/24 par exemple.

- identifier une interface VLAN logique du switch (par exemple VLAN 1 qui est par défaut sur les Cisco)
- entrer dans le mode privilégié (**enable**)
- entrer dans le mode de configuration globale du switch (**configure terminal**)
- entrer dans le mode de configuration de l'interface VLAN en question (**interface Vlan 1**)
- définir l'adresse IP et son masque (**ip address x.x.x.x 255.255.255.0**)
- activer **logiquement** l'interface VLAN (**no shutdown**)
- sortir du mode de l'interface VLAN (**exit**)
- option : définir une passerelle pour pouvoir sortir du réseau 172.16.4.0/24 (**ip default-gateway 172.16.4.254**)

(cela devrait être la même que celle des stations connectée au switch).

- sortir du mode de configuration global (**exit**)

Exemple :

```
Switch>
Switch>
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#ip address 10.1.1.8 255.255.255.0
Switch(config-if)#
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#
Switch(config)#ip default-gateway 10.1.1.254
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Conclusion

Il faut identifier quelle interface VLAN va servir pour **administrer** le switch à distance et lui assigner une adresse IP.

Dans un réseau, on dédit un VLAN pour l'administration et la prise à distance de tous les équipements réseaux pour que seuls les administrateurs puissent y accéder. On évite ainsi que les élèves et les stagiaires s'amusent avec le réseau…

Question : pourquoi défini-t-on une passerelle dans le cadre du switch ?

Article 3 - Activer l’accès d’administration d’un switch via Telnet

La méthode de base pour configurer un switch Cisco est de se connecter via le port console de l’appareil. C’est en tout nécessaire pour une première configuration, mais ensuite, il est tout de même plus aisé de pouvoir accéder au CLI via une machine distante connectée au réseau. Voici les quelques paramètres à configurer pour rendre cela possible…

Pour pouvoir accéder au CLI via Telnet, il faut pouvoir établir une connexion entre le PC et le switch. Ce qui implique:

- Le PC et le Switch disposent d’une adresse IP.
- Si le PC et le Switch sont sous le même sous-réseau, il faut bien sur que les adresses IP y correspondent.
- Si le PC et le Switch ne sont pas sur le même sous réseau, il faut que les tables de routages des différentes passerelles soient correctement configurées.
- Les connexions Telnet sur le switch sont autorisées.

Pour attribuer une adresse IP à un switch, on en configure une sur une ou plusieurs interfaces « vlan ». Par défaut, le VLAN 1 existe, nous allons donc utiliser celle-là.

Dans le cas présent, nous supposons que le PC est directement connecté sur un des ports du switch. On attribuera l’adresse 192.168.1.100 / 255.255.255.0 au switch et 192.168.1.101 / 255.255.255.0 au pc. On configurera également une passerelle par défaut pour les deux qui sera 192.168.1.1. Elle ne sera pas ici nécessaire, mais ça montrera comment la configurer dans le cas d’un réseau complexe.

Commencez par configurer l’adresse IP du switch sur le VLAN 1.

Quelles sont les commandes que vous avez utilisées?

On vérifie que tout est en ordre:

Comment vérifier que votre interface virtuelle est bien configurée ?

On configure également l'adresse IP du PC en 192.168.1.101 / 255.255.255.0. Une fois cela fait, si tout fonctionne comme prévu, les deux machines devraient pouvoir communiquer...

Comment vérifiez-vous la bonne communication des deux machines à partir du switch? Observez bien la forme du prompt qui vous donne une indication sur le mode où se placer :

```
Switch#
```

Ok tout est en ordre! Il reste maintenant à vérifier que le switch est bien configuré pour autoriser les connexions Telnet.
Les connexions Telnet se font via les « lignes » VTY. Leur nombre varie selon les modèles, on peut les retrouver en jetant un œil sur la configuration active:

```
Switch#sh running-config
Building configuration...
Current configuration : 979 bytes
!
version 12.2
no service password-encryption
!
hostname Switch
!
!
!
interface FastEthernet0/1
!
……
!
interface FastEthernet0/24
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
ip address 192.168.1.100 255.255.255.0
!
ip default-gateway 192.168.1.1
!
line con 0
!
line vty 0 4
no login
line vty 5 15
no login
!
!
end
Switch#
```

Combien y-a-t-il de lignes VTY possibles ?

Afin de pouvoir se connecter en Telnet, on va définir un mot de passe, activer l'encryption des mots de passe et également définir un mot de passe pour le mode privilégié (enable).

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#service password-encryption
Switch(config)#line vty 0 15
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable password cisco
Switch(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

On vérifie que tout est en place:

```
Switch#sh run
```

A quoi correspond cette commande ?

Comment voyez vous que la ligne pour le Telnet est ouverte ?

Voilà, il ne reste plus qu'à se connecter en Telnet depuis un PC branché sur le switch. Pour ce faire, utilisez PuTTY installé sur votre poste et renseignez le champ « host name » avec l'IP du switch. Une fois la connexion établie, vous pouvez continuer l'administration de votre switch.

Article 4 - Configuration du protocole ssh pour le switch

- Vérification de la prise en compte du protocole ssh par l'IOS

Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l'IOS.
La commande pour vérifier la version de l'IOS est:

```
2960-RG#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
12.2(55)SE, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 07-Aug-10 23:04 by prod_rel_team
```

- Configuration du nom d'hôte et du nom de domaine.

Le nom du switch ainsi que le nom de domaine doivent avoir été configurés.

- Création de la clé

```
2960-RG(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: 2960-RG.mondomaine.fr
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

2960-RG(config)#
*Mar 1 00:42:43.625: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Activation de ssh

```
RG-2960(config)#ip ssh version 2
```

- Options ajoutées au service ssh

- les évènements associés aux connexions ssh sont enregistrés.
- Un timeout de 60 secondes est ajouté pour les sessions ssh en cas d'inactivité.
- Nous laissons trois essais pour la connexion au switch.

```
clem(config)#ip ssh logging events
clem(config)#ip ssh time-out 60
clem(config)#ip ssh authentication-retries 3
```

- Ajout d'un compte administrateur

```
clem(config)#username admin secret P@55w0rd
```

- Désactivation de telnet pour l'accès au switch

```
clem(config)#line vty 0 15
clem(config-line)#login local
clem(config-line)#transport input ssh
```

- Vérification de la configuration

```
2960-RG#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
```

SSH est maintenant activé. nous pouvons accéder au switch avec un client ssh (par exemple putty pour windows).

Suppression de ssh

La suppression de la clé entraine la désactivation de ssh.

```
2960-RG(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
2960-RG(config)#
```

Vérification:

```
2960-RG#sh ip ssh
SSH Disabled - version 2.0
%Please create RSA keys to enable SSH (of atleast 768 bits size) to
enable SSH v2.
Authentication timeout: 60 secs; Authentication retries: 3
```