Important : Réalisez l'ensemble des tâches en capturant les étapes et en commentant toutes les étapes. (Pensez à alimenter votre portfolio à partir de ce TP)

TP2 : Configuration des paramètres initiaux d'un périphérique Cisco

Objectif

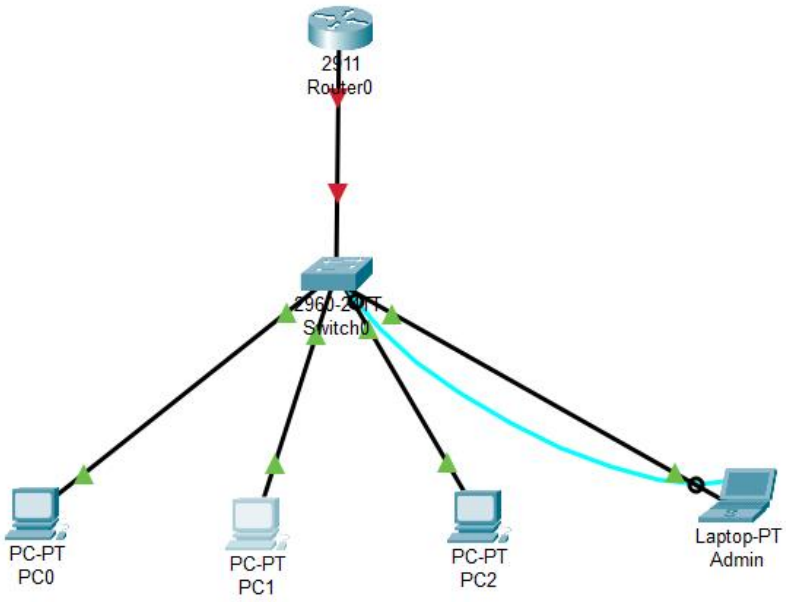
L'objectif de ce TP est d'apprendre à configurer les paramètres initiaux des périphériques Cisco, à sécuriser l'accès et à assurer la connectivité de base dans un réseau local.

Étape par Étape avec Explications Détaillées

Étape 1 : Réaliser la topologie sur Cisco Packet Tracer

- **Créer la topologie réseau :**
    - Ouvrez Cisco Packet Tracer.
    - Placez un routeur Cisco 2911 et un switch Cisco 2960 sur la zone de travail.
    - Ajoutez trois PC (PC1, PC2, PC3) et un Laptop (Laptop1 Admin).
    - Connectez les PC et le Laptop au switch 2960 en utilisant des câbles Ethernet.

- Connectez le routeur au switch avec un câble Ethernet.
- Pour la connexion console, utilisez un câble console entre le Laptop1 Admin et le port console du switch.



Étape 2 : Utiliser le Laptop Admin pour configurer S1 via le câble console

- **Connexion à la console** : La connexion console est souvent utilisée pour la configuration initiale d'un périphérique avant de l'ajouter au réseau.
  - Cliquez sur Laptop1 Admin, puis sur l'onglet "Desktop" et choisissez "Terminal".

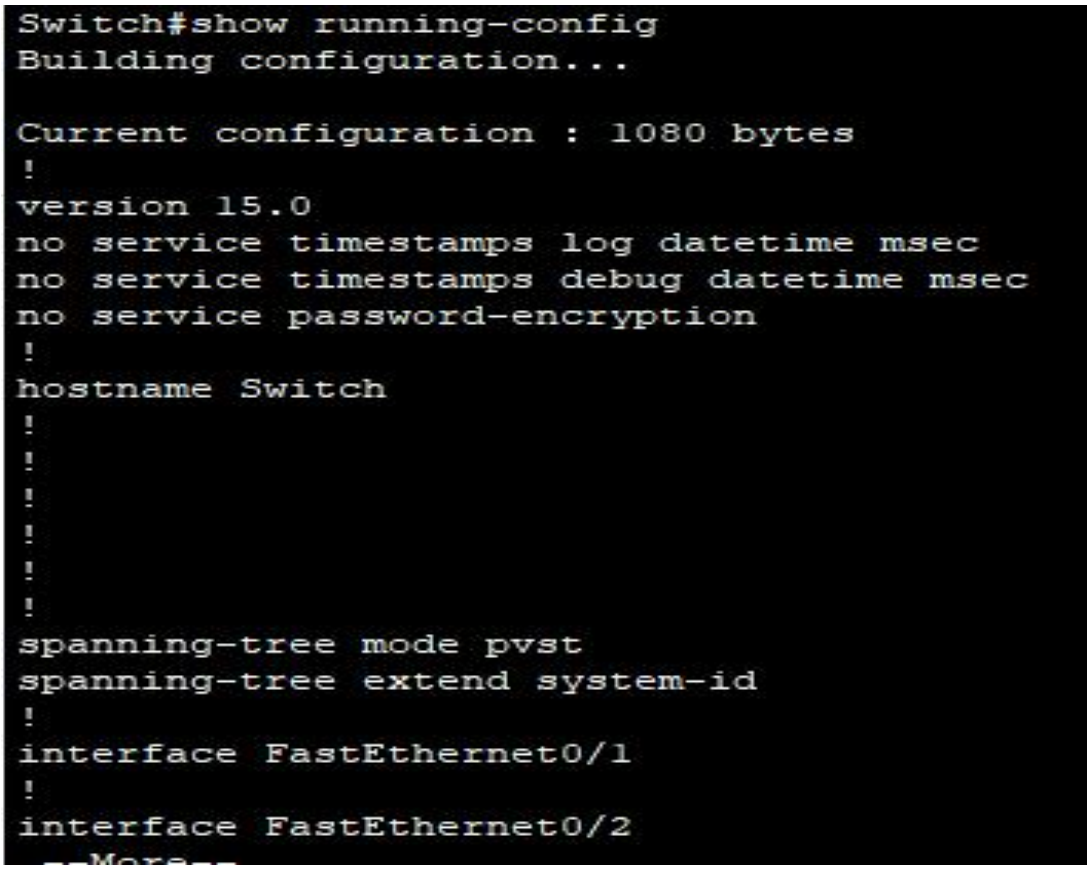
- Configurez les paramètres de terminal par défaut (Bits par seconde : 9600, Bits de données : 8, Parité : Aucun, Bits d'arrêt : 1, Contrôle de flux : Aucun) et cliquez sur "OK".

Étape 3 : Vérifier la configuration par défaut du commutateur S1

- **Quelle commande permet l'affichage de la configuration courante ?**

  show running-config

- **Exécuter la commande et expliquer les grands paramétrages déjà définis**



Étape 4 : Attribuer un nom au commutateur S1

- Expliquez et exécuter les étapes permettant de définir le nom S1 au switch.

enable (pour passer en mode super user) > conf t (pour passer en mode configuration > hostname s1 (changer le nom du switch pour S1)

Étape 5 : Sécuriser l'accès au mode privilégié

- Exécuter la commande suivante en mode configuration globale.

  enable password cisco

```
S1(config)#enable password  cisco
```

- Définir un mot de passe compliqué
-
```
S1(config)#enable password clsc0
```

- Expliquez l'intérêt de cette démarche.

  cette commande permet de securiser le materielle face au pirate

- Afficher à nouveau la configuration courante avec la commande :

  show running-config

- Que constatez-vous ?

  le mot de passe apparait en claire

```
S1#show running-config
Building configuration...

Current configuration : 1100 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable password c1sc0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
```

Étape 6 : Configurer un mot de passe chiffré pour le mode privilégié

- Quelle commande permet de chiffrer le mot de passe ?
- `S1(config)#service Password-encryption`
- Indiquez le type de chiffrement employés ?

  Chiffre Vigenère et MD5

- Exécutez la commande suivante et commentez là.

  show running-config | include enable secret

  aficcher la configuration en cours et chiffrer l'affichage du mots de passe

- Expliquez l'intérêt de cette fonctionnalité de chiffrement ?

  elle permet de ne pas montrer le mot de passe est donc eviter que quelqu'un de non autoriser le recupere (via shoulder surfing par exemple)

- Sortez du mode configuration.
- Quelle commande permet de sauvegarder votre nouvelle configuration.
- wr ou write

Étape 7 : Chiffrer les mots de passe d'activation

- Quelle commande permet de chiffrer tous les mots de passe d'activation.

```
S1(config)#service Password-encryption
```

- Citez les différences entre configurer un mot de passe chiffré pour le mode privilégié et chiffrer les mots de passe d'activation.

chiffrer pour le mode privilégier permet de s'assurer que personne ne puisse modifier la cofiguration et le mot de passe d'activation permet d'eviter que quelqun puisse acceder au switch tout court

Étape 8 : Configurer une bannière MOTD

- Exécuter la commande suivante en configuration :

  banner motd #Attention! Accès non autorisé interdit!#.

- Quitter le mode configuration.

  exit

- Exécuter l'une des deux commandes :

  write memory

  ou

  copy running-config startup-config

```
S1#write memory
Building configuration...
[OK]
```

- Quelle commande permet de se déconnecter ?

```
S1#logout



S1 con0 is now available



Press RETURN to get started.
```

- **Déconnectez et reconnectez-vous.**
- **Quel est l'intérêt de la commande banner.**

```
Attention! Accs non autoris interdit!

S1>
```

cette commande permet d'afficher un message de banniere au demarage du switch afin de faire passer un message

Étape 9 : administration à distance d'un commutateur réseau

Étape 9.1 : Attribuer une adresse IP à l'interface VLAN1 du S1

Faire en sorte que le switch soit joignable sur le réseau.

- **Comment entrer dans le mode configuration de l'interface**

vlan1.

```
S1>en
Password:
S1#int
S1#con
S1#conf t
Enter configuration commands, one per line.
S1(config)# int vlan1
S1(config-if)#
```

- Quelle commande permet d'attribuer l'adresse ip 192.168.1.201 au vlan1.

```
S1(config-if)#ip address 192.168.1.201 255.255.255.0
```

- Activez l'interface

```
S1(config-if)#no shutdown
```

- Exécutez la commande pour vérifier votre configuration.

Show ip interface brief

```
S1#Show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual down                  down
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
FastEthernet0/5        unassigned      YES manual up                    up
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
```

Info : L'interface VLAN1 est l'interface de gestion par défaut sur les commutateurs Cisco. Assigner une IP permet au commutateur d'être **joignable sur le réseau.**

Étape 9.2 : Configurez la ligne de terminal virtuel (VTY) pour Telnet

Autoriser et sécuriser l'accès via Telnet/SSH

- **Exécutez la commande suivante**

  show running-config | include line vty

```
S1#show running-config | include line vty
line vty 0 4
line vty 5 15
S1#
```

- Quel est le nombre de ligne VTY disponible sur votre switch ?

  15 ?

- Accédez à la configuration de l'ensemble des lignes VTY.

- Configurez le mot de passe suivant Cisco2024.

```
S1(config)#line vty 0 15
S1(config-line)#password Cisco2024
S1(config-line)#login
```

- Affichez les sections de configuration relatives aux lignes VTY.

```
line con 0
 password 7 0802455D0A165747405F
!
line vty 0 4
 login
line vty 5 15
 login
```

Info : La configuration des lignes VTY est nécessaire pour gérer le **control** d'accès à distance au périphérique via Telnet ou SSH.

Étape 10 : Sécuriser et chiffrer l'accès console

- Quelle commande permet d'accéder à la configuration de la ligne console.
- line con0
- Configurez le mot de passe suivant Cisco2024.

  password Cisco2024
- Activez l'authentification par mot de passe.

  login
- Chiffrez tous les mots de passe les fichiers de configuration.
- Exécutez la commande suivante :

  show running-config | section line console
- Expliquez la commande ci-dessus.

  cette commande permet de voire la configuration de la ligne console

  Intérêt : Protéger l'accès console avec un mot de passe est essentiel pour empêcher un accès non autorisé physique au périphérique.

Étape 11 : Sauvegarder la configuration

Sauvegarder la configuration garantit que tous les paramètres sont conservés après un redémarrage.

- **Exécuter la commande suivante :**

  running-config startup-config.

- **Quelle autre commande permet de réaliser la même chose.**

  wr ou write

Étape 12 : Configurer R1 de manière similaire.

- Connectez-vous à R1 via le câble console.
- Attribuez l'adresse IP 192.168.1.202/24 à l'interface G0/0.
- ```
  Router(config-if)#ip address 192.168.1.202 255.255.255.0
  ```
- Configurer une connexion en Telnet.
- ```
  Router(config-line)#password Cisco2024
  ```

Étape 13 : Configurer les ordinateurs

- Configurez sur chaque PC, les paramètres IP manuellement ou via DHCP.

- Utiliser Telnet pour accéder à R1 et S1

```
Trying 192.168.1.201 ...OpenAttention! Accs non autoris interdit!


User Access Verification

Password:
Password: Password:
S1>en
Password:
Password:
S1#
```

Étape 14 : Telnet vs SSH

- Décrire les différences, les risques entre ces deux moyens d'accès à distance

un ssh permet de parametrer des profil selon les utilisateur et peut donc étre plus sécuriser en geranr les permisson , telnet est plus simple mias seule le mot de passe protege la connexion

- Reconfigurer votre switch et votre routeur en mode SSH.
- Testez la connexion SSH sur le routeur et sur le switch.

-
- Commentez l'ensemble des étapes.
-

Étape 15 : Rendez votre travail sur Ecole directe (Cahier de texte).