

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

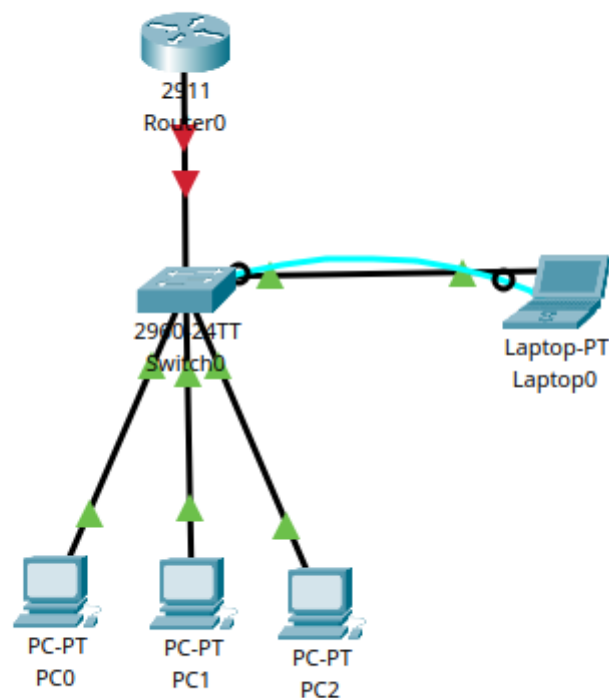
L'objectif de ce TP est d'apprendre à configurer les paramètres initiaux des périphériques Cisco, à sécuriser l'accès et à assurer la connectivité de base dans un réseau local.

Étape par Étape avec Explications Détaillées

Étape 1 : Réaliser la topologie sur Cisco Packet Tracer

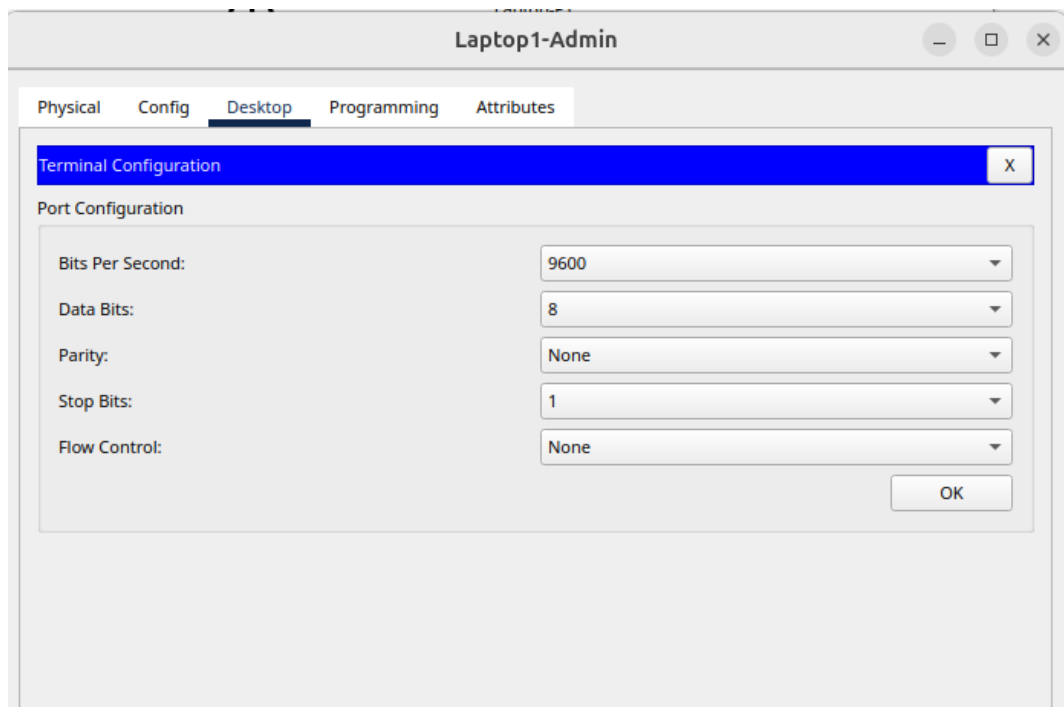
1. Créer la topologie réseau :

- 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

1. **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

1. Quelle

commande permet l'affichage de la configuration courante ?

Enable puis show running-config

```
% Invalid input detected at '^' marker.  
Switch>show running-config  
^  
% Invalid input detected at '^' marker.  
  
Switch>enable  
Switch#sho  
Switch#show run  
Switch#show running-config  
Building configuration...  
  
Current configuration : 1080 bytes  
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Switch  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
--More--
```

2. Exécuter la commande et expliquer les grands paramètres déjà définis

- Version
- Horodatage des services
- Chiffrement des mots de passe
- Nom d'hôte
- Spanning Tree
- Interfaces

Étape 4 : Attribuer un nom au commutateur S1

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

- enable
- configure terminal
- hostname S1
- exit
- show running-config

```

!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1

Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

```

Étape 5 : Sécuriser
l'accès au mode

privilegié

1. Exécuter la commande suivante en mode configuration globale.

enable password cisco

2. Définir un mot de passe compliqué

- enable password Corantin07&*

```

S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#enable password cisco
S1(config)#
S1(config)#
S1(config)#enable password Corantin07&*
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
sho
S1#show rui
S1#show ru
S1#show running-config
Building configuration...

Current configuration : 1107 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable password Corantin07&*
!
!

```

3. Expliquez l'intérêt de cette démarche.

- **Sécurité** : Un mot de passe complexe est essentiel pour protéger l'accès à la configuration de l'appareil.
- **Prévention des accès non autorisés** : En sécurisant l'accès au mode privilégié, tu limites les risques d'accès non autorisé à la configuration du switch
- **Conformité** : De nombreuses organisations doivent respecter des politiques de sécurité strictes. Avoir un mot de passe complexe peut être une exigence de conformité.

4. Afficher à nouveau la configuration courante avec la commande : `show running-config`

5. Que constatez-vous ?

- **Le mot de passe apparaît en clair**

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

1. Quelle commande permet de chiffrer le mot de passe ?

- `enable secret <mot_de_passe>`
- `service password-encryption`

2. Indiquez le type de chiffrement employés ?

- Le mot de passe défini avec la commande `enable secret` est chiffré à l'aide de l'algorithme de hachage MD5. Cela signifie qu'il ne sera pas stocké en clair dans la configuration.

3. Exécutez la commande suivante et commentez là.

`show running-config | include enable secret`

```
%SYS-5-CONFIG_I: Configured from console by console
show running-config | include enable secret
enable secret 5 $1$mERr$XYQ0.kVi7r3cGvjRLgHZH/
S1#
```

- Cette commande filtre la sortie de la configuration en n'affichant que la ligne contenant "enable secret". Cela te permettra de vérifier si le mot de passe chiffré a été correctement configuré.

- Le "5" indique que le mot de passe est chiffré en utilisant un algorithme de type MD5.

4. Expliquez l'intérêt de cette fonctionnalité de chiffrement ?

- **Sécurité renforcée**
- **Protection contre le piratage**
- **Conformité aux politiques de sécurité**

5. Sortez du mode configuration.

- `exit`

6. **Quelle commande permet de sauvegarder votre nouvelle configuration.**

- write memory
- copy running-config startup-config

Étape 7 : Chiffrer les mots de passe d'activation

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

- service password-encryption

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

- Niveau de sécurité : enable secret : Il offre une sécurité renforcée car il utilise un algorithme de hachage, ce qui le rend plus difficile à déchiffrer.
- Usage spécifique : enable secret : Utilisé exclusivement pour le mode privilégié.

Étape 8 : Configurer une bannière MOTD

1. **Exécuter la commande suivante en configuration :**

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

2. **Quitter le mode configuration.**

- Exit

3. **Exécuter l'une des deux commandes :**

write memory

ou

copy running-config startup-config

4. **Quelle commande permet de se déconnecter ?**

- Logout

5. **Déconnectez et reconnectez-vous.**

- Logout
- Enable password

6. **Quel est l'intérêt de la commande banner.**

- Avertissement
- Information

- Responsabilité

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.

1. Comment entrer dans le mode configuration de l'interface vlan1.
- interface vlan 1
2. Quelle commande permet d'attribuer l'adresse ip 192.168.1.201 au vlan1.
- ip address 192.168.1.201 255.255.255.0
3. Activez l'interface
- no shutdown
4. Exécutez la commande pour vérifier votre configuration.

Show ip interface brief

```
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
show ip interface brief
Interface                IP-Address      OK? Method Status  Protocol
FastEthernet0/1          unassigned      YES manual up       up
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 down   down
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
FastEthernet0/22         unassigned      YES manual down   down
FastEthernet0/23         unassigned      YES manual down   down
FastEthernet0/24         unassigned      YES manual down   down
GigabitEthernet0/1       unassigned      YES manual down   down
GigabitEthernet0/2       unassigned      YES manual down   down
Vlan1                    192.168.1.201   YES manual up       up
S1#
S1#
S1#
S1#
```

Info :
L'interface VLAN1 est l'interface de gestion par défaut sur les commutateurs Cisco. Ass

igner 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

1. Exécutez la commande suivante

`show running-config | include line vty`

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

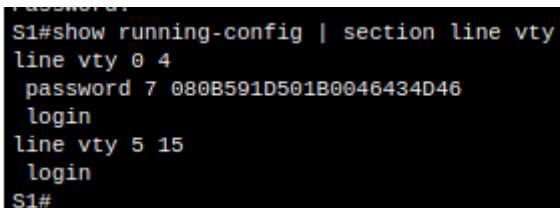
- line vty 0 4, il y a 5 lignes de 0 à 4.

- line vty 5 15, il y a 11 lignes

- total 16 lignes

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

- `show running-config | include line vty`



```
S1#show running-config | section line vty
line vty 0 4
 password 7 080B591D501B0046434D46
 login
line vty 5 15
 login
S1#
```

4. Configurez le mot de passe suivant Cisco2024.

- `password *****`

5. Activez l'authentification par mot de passe.

- `login`

6. Affichez les sections de configuration relatives aux lignes VTY.

- `show running-config | section line vty`

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

1. Quelle commande permet d'accéder à la configuration de la ligne console.

- `line console 0`

2. Configurez le mot de passe suivant Cisco2024.

- `password Cisco2024`

3. Activez l'authentification par mot de passe.

- `login`

4. **Chiffrez tous les mots de passe les fichiers de configuration.**

- service password-encryption

5. **Exécutez la commande suivante :**

show running-config | section line console

6. **Expliquez la commande ci-dessus.**

- la commande permet de filtrer et de visualiser rapidement la configuration spécifique à 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.

1. **Exécuter la commande suivante :**

running-config startup-config.

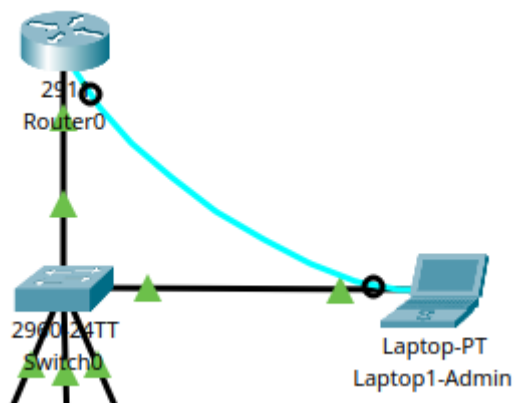
2. **Quelle autre commande permet de réaliser la même chose.**

- copy running-config startup-config

- write memory

Étape 12 : Configurer R1 de manière similaire.

1. **Connectez-vous à R1 via le câble console.**



2. **Attribuez l'adresse IP 192.168.1.202/24 à l'interface G0/0.**

- interface GigabitEthernet 0/0

- ip address 192.168.1.202 255.255.255.0

3. **Configurer une connexion en Telnet.**

- configure terminal

- line vty 0 4

- password Cisco2024

- login
- transport input telnet
- exit

Étape 13 : Configurer les ordinateurs

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

- PC1 : 192.168.1.10
- PC2 : 192.168.1.11
- PC3 : 192.168.1.12

2. Utiliser Telnet pour accéder à R1 et S1

- telnet 192.168.1.202

Étape 14 : Telnet vs SSH

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

- Telnet est risqué en raison de son absence de chiffrement et ne doit pas être utilisé dans des environnements sensibles. SSH est fortement recommandé pour toutes les connexions à distance en raison de sa sécurité accrue.

2. Reconfigurer votre switch et votre routeur en mode SSH.

- configure terminal
- hostname S1
- ip domain-name example.com
- crypto key generate rsa
- 1024
- username admin privilege 15 secret Cisco2024
- line vty 0 4
- transport input ssh
- login local
- exit

(les commandes pour le routeur sont identiques à peu de chose près) ,

```

R1>ena
R1>enable
R1#conf
R1#configure t
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
R1(config)#copy running-config startup-config
      ^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

```

3. Testez la connexion SSH sur le routeur et sur le switch.

Telnet / SSH Client

Session Options

Connection Type	SSH
Host Name or (IP address)	192.168.1.201
Username	admin

SSH Client

Password:

Attention! Acces non autorise interdit!

S1#

4. Commentez l'ensemble

des étapes.

- PC
- SSH Client
- Renseigner les informations
- mettre votre mot de passe
- Bravo, vous êtes connecté

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