

*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

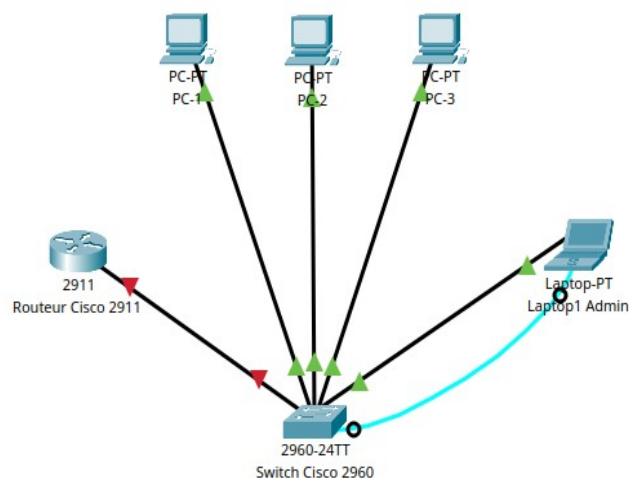
L'objectif de ce TP est d'apprendre à configurer les paramètres initiaux des périphériques Cisco, à sécuriser l'accès et à assurer la connectivité de base dans un réseau local.

### Étape par Étape avec Explications Détaillées

#### Étape 1 : Réaliser la topologie sur Cisco Packet Tracer

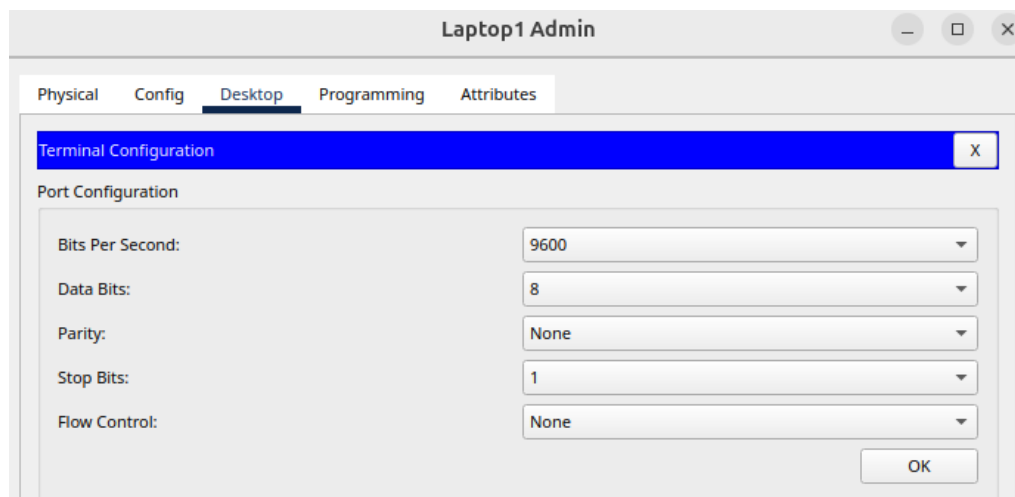
##### 1. Créer la topologie réseau :

- 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 ?  
**Show running-config**
2. Exécuter la commande et expliquer les grands paramétrages déjà définis

***no service timestamps log datetime msec --- no service timestamps debug datetime msec*** : Cela simplifie la sortie de log en évitant d'afficher les informations de date/heure pour chaque message.

***no service password-encryption*** --- Indique que les mots de passe ne seront pas cryptés dans le fichier de configuration.

***hostname Switch*** --- Le nom de l'appareil est défini comme "Switch".

***spanning-tree mode pvst*** --- PVST (Per-VLAN Spanning Tree). Cela permet de gérer un arbre couvrant indépendant pour chaque VLAN, ce qui améliore la gestion du trafic dans les réseaux basés sur des VLANs.

*spanning-tree extend system-id* --- Ajoute l'ID système dans les messages BPDUs (Bridge Protocol Data Units), ce qui permet à plusieurs switchs dans un réseau d'avoir un identifiant unique même s'ils partagent la même priorité.

*Interfaces FastEthernet0/1 à FastEthernet0/24 et GigabitEthernet0/1 à GigabitEthernet0/2* --- Aucun paramètre spécifique n'a été configuré sur ces interfaces.

*interface Vlan1* --- Le vlan1 sert en générale pour gérer le switch dans sa globalité. Ici, il est configurée sans adresse IP et est désactivée (shutdown), ce qui signifie que le switch n'est pas encore accessible via une interface de gestion réseau.

*line con 0* --- Il s'agit de la ligne console, utilisée pour accéder au switch via une connexion console (physique). Aucun mot de passe n'est défini pour cette ligne.

*line vty 0 4* --- *line vty 5 15* --- Ces lignes définissent les connexions à distance via Telnet ou SSH (ligne virtuelle). Les commandes `login` indiquent qu'un mécanisme de login (mot de passe, par exemple) est requis, mais aucun mot de passe n'a encore été configuré pour ces sessions.

#### Étape 4 : Attribuer un nom au commutateur S1

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

```
Switch>en
Switch#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

---

*en* → passer en mode privilégié

*conf* → passer en mode configuration globale

*hostname* → permet de renommer le switch

#### Étape 5 : Sécuriser l'accès au mode privilégié

1. Exécuter la commande suivante en mode configuration globale.

*enable password cisco*

2. Définir un mot de passe compliqué

Un mot de passe compliqué est un mot de passe ayant minimum 12 caractères comportant au minimum 1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial. Il ne doit pas comporter d'éléments facile à deviner et de répétitions.

3. Expliquez l'intérêt de cette démarche.

L'intérêt de définir un mot de passe compliqué est d'améliorer la sécurité en protégeant l'accès aux systèmes contre les attaques non autorisées. Un mot de passe complexe est difficile à deviner ou à casser par des méthodes automatisées telles que les attaques par force brute ou par dictionnaire. Cela renforce la protection des données sensibles et réduit les risques d'intrusion.

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

5. Que constatez-vous ?

On constate que la ligne « *enable password cisco* » est rajoutée

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

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

`service password-encryption`

2. Indiquez le type de chiffrement employés ?

La commande utilise un chiffrement simple et réversible, appelé Vigenère.

3. Exécutez la commande suivante et commentez là.

`show running-config | include enable secret`

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

Cette commande permet de cacher le mot de passe défini lorsqu'on regarde la configuration avec la commande « *show running-config* »

5. Sortez du mode configuration.

6. Quelle commande permet de sauvegarder votre nouvelle configuration.

`write memory`

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.

- Configurer un mot de passe chiffré pour le mode privilégié : La commande `enable secret` permet de définir un mot de passe chiffré

- Chiffrer les mots de passe d'activation : La commande `service password-encryption` chiffre tous les mots de passe existants avec un chiffrement simple et réversible

## 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.

3. Exécuter l'une des deux commandes :

`write memory`

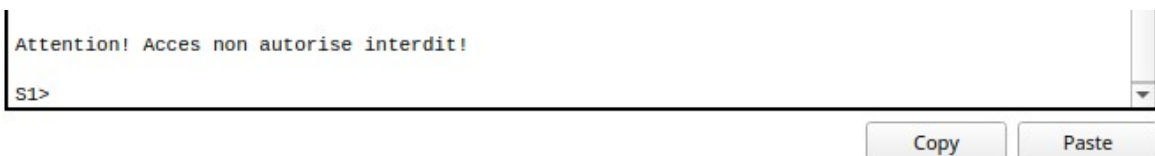
**ou**

`copy running-config startup-config`

4. Quelle commande permet de se déconnecter ?

`exit`

5. Déconnectez et reconnectez-vous.



```
Attention! Accès non autorise interdit!
S1>
```

The screenshot shows a terminal window with a black background and white text. The first line displays the configured MOTD banner: "Attention! Accès non autorise interdit!". The second line shows the prompt "S1>". Below the terminal window, there are two buttons: "Copy" and "Paste".

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

La commande « *banner* » permet d'afficher un message personnalisé à chaque connexion au switch ou au routeur.

## 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.**

```
S1(config)#vlan 1
S1(config-vlan)#
```

Copy

Paste

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

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

Copy

Paste

**Activez l'interface**

**no shutdown**

3. **Exécutez la commande pour vérifier votre configuration.**

**Show ip interface brief**

```
Vlan1          192.168.1.201  YES manual up
```

**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

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
line vty 5 15
```

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

```
S1(config)#line vty 0 4
```

4. Configurez le mot de passe suivant Cisco2024.

```
S1(config-line)#password cisco2024
S1(config-line)#
```

5. Activez l'authentification par mot de passe.

login

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

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

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

```
S1(config)#line console 0
S1(config-line)#password cisco2024
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
S1#show runn
S1#show running-config | section line console
^C
```

6. Expliquez la commande ci-dessus.

**La commande `show running-config` | section `line console` affiche la section de la configuration en cours qui concerne 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.

`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.

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.202 255.255.255.0
Router(config-if)#no shutdown
```

3. Configurer une connexion en Telnet.

```
Router(config)#line vty 0 4
Router(config-line)#password cisco2024
Router(config-line)#login
```

## Étape 13 : Configurer les ordinateurs

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

IPv4 Address	192.168.1.203
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.201
DNS Server	192.168.1.202

IPv4 Address	192.168.1.204
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.201
DNS Server	192.168.1.202

IPv4 Address	192.168.1.205
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.201
DNS Server	192.168.1.202

2. Utiliser Telnet pour accéder à R1 et S1

```
C:\>telnet 192.168.1.202
Trying 192.168.1.202 ...Open

User Access Verification

Password:
Router>|
```

```
C:\>telnet 192.168.1.201
Trying 192.168.1.201 ...OpenAttention! Acces non autorise interdit!

User Access Verification

Password:
S1>|
```



## Étape 14 : Telnet vs SSH

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

- **Sécurité** : Telnet ne chiffre pas les données, exposant les mots de passe ; SSH chiffre tout, offrant une connexion sécurisée.
- **Authentification** : Telnet utilise une authentification simple; SSH propose des méthodes plus robustes, y compris par clés publiques.
- **Ports** : Telnet utilise le port « 23 », tandis que le SSH utilise le port « 22 ».
- **Risques de Telnet** : Interception des mots de passe et vulnérabilités aux attaques de type "man-in-the-middle".

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

### ROUTEUR

```
Router(config)#hostname R1
R1(config)#ip domain-name
R1(config)#ip domain-name TP
R1(config)#crypto key generate rsa
The name for the keys will be: R1.TP
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local

R1(config-line)#username admin secret cisco2024
R1(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1#
```

### SWITCH

```

S1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip domain-name TP
S1(config)#crypto key generate rsa
The name for the keys will be: S1.TP
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#line vty 0 4
*Mar 1 1:59:3.981: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#username admin secret cisco2024
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
S1#

```

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

```

[Connection to 192.168.1.202 closed by foreign host]
C:\>ssh -l admin 192.168.1.202

Password:

R1>

```

```

C:\>ssh -l admin 192.168.1.201

Password:

Attention! Acces non autorise interdit!

S1>

```

### 4. Commentez l'ensemble des étapes.

- **Sécurité** : La transition de Telnet à SSH renforce considérablement la sécurité des connexions à distance, ce qui est essentiel pour protéger les données et les configurations sensibles.
- **Configuration** : Les étapes de configuration pour SSH sont simples et suivent une structure standard, ce qui facilite leur mise en œuvre.
- **Authentification** : La création d'utilisateurs avec des mots de passe sécurisés améliore la sécurité des accès réseau.
- **Tests** : Tester les connexions SSH garantit que tout est correctement configuré et que les accès sont sécurisés.

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