

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.

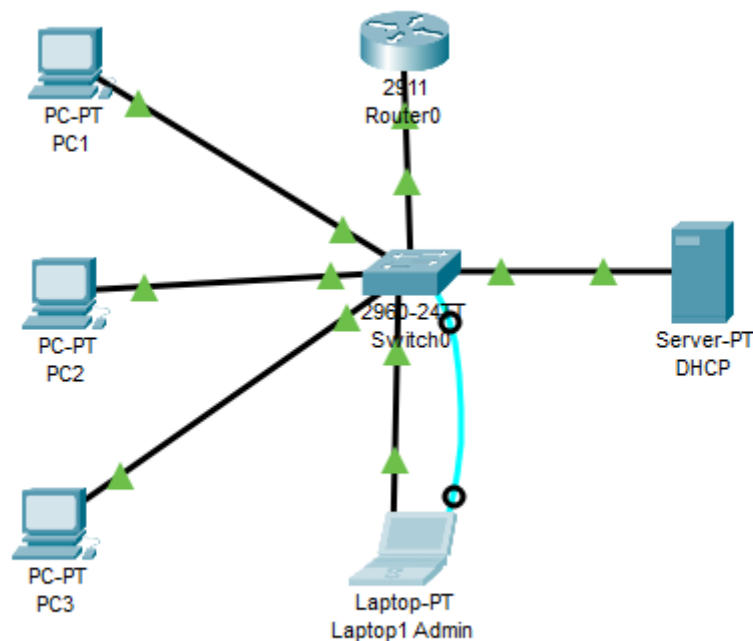
Étape par Étape avec Explications Détaillées

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.

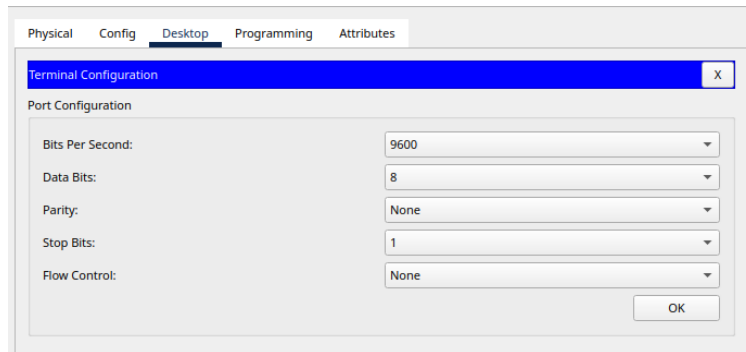
Étape 2 :
Laptop
pour
S1 via le
console



Utiliser le
Admin
configurer
câble

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 ru

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

1080 du

```
Switch>enable
Switch#show ru
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
```

bytes, pas de sécurité par mot de passe, nom Switch

Étape 4 : Attribuer un nom au commutateur S1

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

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

Enable pour accéder au mode admin

Conf t pour accéder au paramétrage du Terminal

hostname pour changer le nom

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 comporte des chiffres des majuscules, des caractères spéciaux, une certaine longueur (~12 caractères), il faut également éviter de mettre des informations personnelles telles que le prénom le nom, la date d'anniversaire, le nom d'un animal de compagnie...

```
S1(config)#enable password P@$$word2024
```

3. Expliquez l'intérêt de cette démarche.

C'est plus sécurisé car cela limite l'accès au mode administration du commutateur (le mot de passe est demandé à chaque utilisation)

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

```
S1#show ru
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 P@$$w0rd2024|
!
```

5. Que constatez-vous ?

On remarque que mon mot de passe est affiché en clair dans la nouvelle configuration (ce n'est pas très sécurisé)

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

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

En mode config : service enable secret

2. Indiquez le type de chiffrement employés ?

Il s'agit du codage en MD5

3. Exécutez la commande suivante et commentez là.

show running-config | include enable secret

Cela affiche le mot de passe chiffré.

```
service password-encryption
!
hostname S1
!
enable password 7 08116C0A4D0E550516595C567E
!
```

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

Le mot de passe n'est plus en clair, ce qui signifie qu'on ne peut pas le trouver facilement.

5. Sortez du mode configuration.

6. Quelle commande permet de sauvegarder votre nouvelle configuration.

Write terminal (wr)

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.

enable secret ne chiffre que le mot de passe du mode privilégié, mais il s'agit d'un chiffrement fort en MD5

password-encryption chiffre tous les mots de passe d'activation, mais il s'agit d'un chiffrement plus faible, en type 7, cependant réversible (on peut le déchiffrer pour revenir en clair)

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.

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

Cela affiche un message à chaque connexion au mode admin du switch, ici « Attention! Accès non autorisé interdit! »

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.

enable

conf t

int 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

```
S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int VLAN 1
S1(config-if)#ip
S1(config-if)#ip a
S1(config-if)#ip address 192.168.1.201 255.255.255.0
S1(config-if)#^Z
```

4. Exécutez la commande pour vérifier votre configuration.

Show ip interface brief

```
GigabitEthernet0/2    unassigned    YES manual down    down
Vlan1                192.168.1.201 YES manual administratively down down
S1# |
```

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 ?

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

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

line vty 0 15

4. Configurez le mot de passe suivant Cisco2024.

password Cisco2024

5. Activez l'authentification par mot de passe.

login

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

```
S1#show ru | section line vty
line vty 0 4
password 7 0802455D0A165747405F
login
line vty 5 15
password 7 0802455D0A165747405F
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

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

```
S1(config)#line console 0
S1(config-line)#password Cisco2024
S1(config-line)#login
S1(config-line)#exit
S1(config)#service pass
S1(config)#service password-encryption
S1(config)#exit
S1#
```

5. Exécutez la commande suivante :

show running-config | section line console

6. Expliquez la commande ci-dessus.

Cela affiche uniquement la configuration de la console effectuée plus haut.

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 :

copy 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>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int G0/0
Router(config-if)#ip address 192.168.1.202 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#line vty 0 15
Router(config-line)#password Cisco2024
Router(config-line)#login
Router(config-line)#tran
Router(config-line)#transport input tel
Router(config-line)#transport input telnet
Router(config-line)#exit
Router(config)#end
```

3. Configurer une connexion en Telnet.

```
Router#show ip interface brief
Interface                IP-Address      OK? Method Status              Protocol
GigabitEthernet0/0       192.168.1.202   YES manual up                  up
GigabitEthernet0/1       unassigned      YES unset  administratively down down
```

Étape 13 : Configurer les ordinateurs

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

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.168.1.10	255.255.255.0	100	0.0.0.0	0.0.0.0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

IP Configuration

☒ DHCP ☐ Static

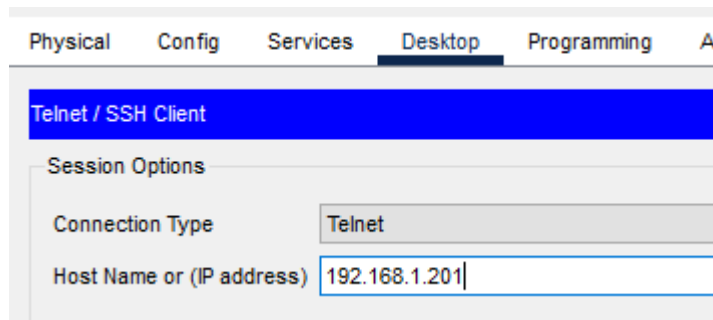
IPv4 Address: 192.168.1.11

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

2. Utiliser Telnet pour accéder à R1 et S1



Physical Config Services Desktop Programming A

Telnet / SSH Client

Session Options

Connection Type Telnet

Host Name or (IP address) 192.168.1.201

Étape 14 : Telnet vs SSH

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

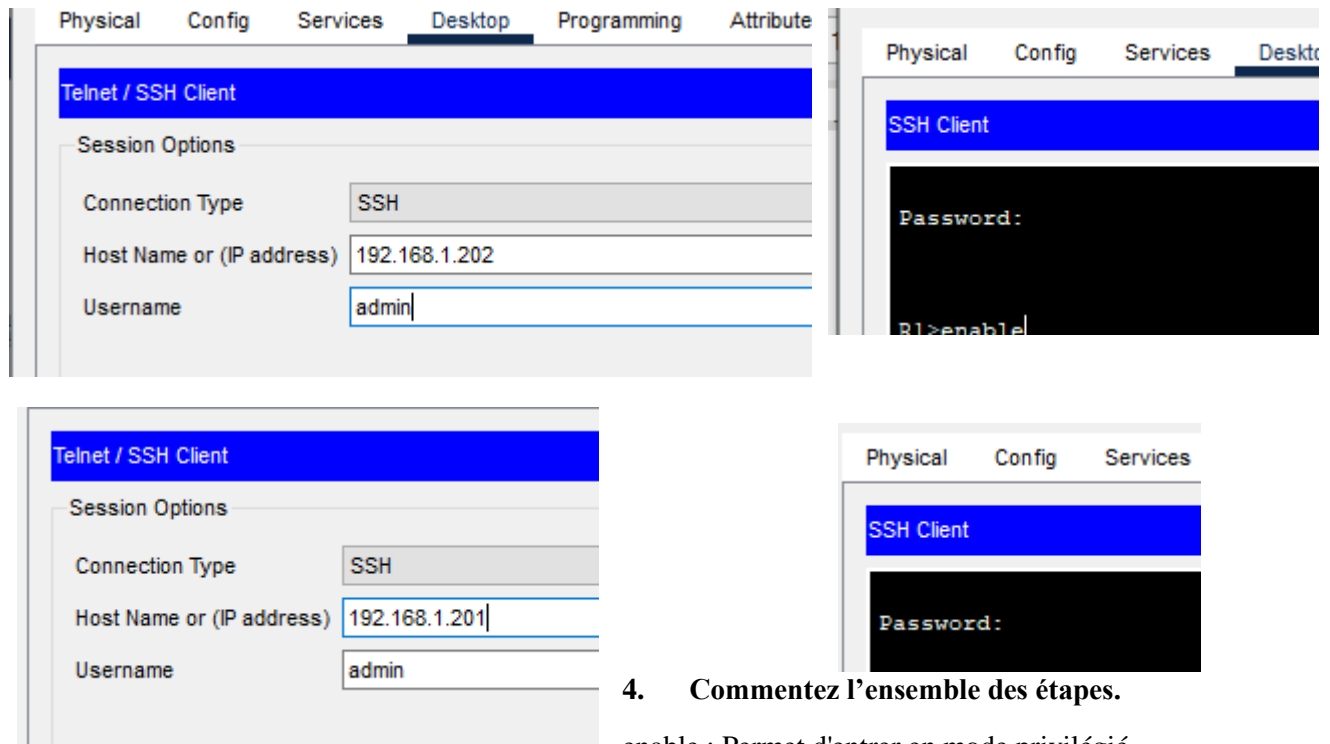
Telnet envoie les communications en clair, et SSH les chiffre, SSH est donc préféré dans les environnements partageant des données sensibles, car Telnet comporte le risque de des attaquants interceptent les communications

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

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1 S1(config)#username admin password cisco
R1 S1(config)#ip domain-name cisco.com
R1 S1(config)#crypto key generate rsa
R1 The name for the keys will be: S1.cisco.com
R1 Choose the size of the key modulus in the range of 360 to 4096 for your
R1 General Purpose Keys. Choosing a key modulus greater than 512 may take
R1 a few minutes.
R1 %
R1 How many bits in the modulus [512]: 1024
R1 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1 T
R1 C S1(config)#line vty 0 15
R1 *Mar 1 0:3:12.152: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1 S1(config-line)#transport input ssh
R1 S1(config-line)#login local
R1 H S1(config-line)#exit
R1 % S1(config)#end

R1 R1(config)#line vty 0 15
R1 *Mar 1 2:48:12.935: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1 R1(config-line)#transport input ssh
R1 R1(config-line)#login local
R1 R1(config-line)#exit
```

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



4. Commentez l'ensemble des étapes.

enable : Permet d'entrer en mode privilégié

conf t : (config terminal) Entrer en mode de configuration du routeur / switch

username admin password cisco : Crée un utilisateur nommé "admin" avec le mot de passe "cisco"

ip domain-name cisco.com : Définit le nom de domaine pour l'appareil

crypto key generate rsa : Commence le processus de génération de clés RSA pour plus de sécurité

How many bits in the modulus : 1024 : Spécifie la taille de la clé RSA en bits (1024 bits)

line vty 0 15 : Sélectionne les lignes virtuelles 0 à 15

transport input ssh : Limite les protocoles de connexion à SSH (plus sécurisé que Telnet)

login local : Indique que l'authentification des utilisateurs doit se faire localement (avec l'user et le mdp donné avant)

exit : Sort du mode de configuration (conf t)

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