

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

Étape 4 : Attribuer un nom au commutateur S1

1. Expliquez et exécuter les étapes permettant de définir le nom S1 au 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
3. Expliquez l'intérêt de cette démarche.
4. Afficher à nouveau la configuration courante avec la commande : `show running-config`
5. Que constatez-vous ?

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

1. Quelle commande permet de chiffrer le mot de passe ?
2. Indiquez le type de chiffrement employés ?
3. Exécutez la commande suivante et commentez là.
`show running-config | include enable secret`
4. Expliquez l'intérêt de cette fonctionnalité de chiffrement ?
5. Sortez du mode configuration.
6. Quelle commande permet de sauvegarder votre nouvelle configuration.

Étape 7 : Chiffrer les mots de passe d'activation

1. Quelle commande permet de chiffrer tous les mots de passe d'activation.
2. Citez les différences entre configurer un mot de passe chiffré pour le mode privilégié et chiffrer les mots de passe d'activation.

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

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.**
2. **Quelle commande permet d'attribuer l'adresse ip 192.168.1.201 au vlan1.**
3. **Activez l'interface**
4. **Exécutez la commande pour vérifier votre configuration.**

`Show ip interface brief`

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 ?
3. Accédez à la configuration de l'ensemble des lignes VTY.
4. Configurez le mot de passe suivant Cisco2024.
5. Activez l'authentification par mot de passe.
6. Affichez les sections de configuration relatives aux lignes 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.
2. Configurez le mot de passe suivant Cisco2024.
3. Activez l'authentification par mot de passe.
4. Chiffrez tous les mots de passe les fichiers de configuration.
5. Exécutez la commande suivante :
`show running-config | section line console`
6. Expliquez la commande ci-dessus.

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.

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.
3. Configurer une connexion en Telnet.

Étape 13 : Configurer les ordinateurs

1. Configurez sur chaque PC, les paramètres IP manuellement ou via DHCP.
2. Utiliser Telnet pour accéder à R1 et S1

Étape 14 : Telnet vs SSH

1. Décrire les différences, les risques entre ces deux moyens d'accès à distance.
2. Reconfigurer votre switch et votre routeur en mode SSH.
3. Testez la connexion SSH sur le routeur et sur le switch.
4. Commentez l'ensemble des étapes.

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