Concepts SSH et Interface Virtuelle

L'objectif de cette séance est de comprendre et configurer le protocole SSH pour sécuriser les connexions à distance sur les équipements Cisco, ainsi que de savoir attribuer une adresse IP à un switch via une interface virtuelle.

---

1. Qu'est-ce que SSH ?

- **SSH (Secure Shell) est un protocole de communication chiffré qui permet d'accéder à distance à un équipement en toute sécurité.**
- **Contrairement à Telnet, SSH protège les données échangées (authentification, commandes, mots de passe).**

📌 **SSH fonctionne sur le port 22 par défaut.**

---

2. Conditions d'utilisation de SSH sur un équipement Cisco

Pour utiliser SSH, il faut :

- **Une adresse IP sur l'équipement (souvent via interface vlan 1 sur un switch).**
- **Un nom d'hôte (hostname) et un nom de domaine (ip domain-name) définis.**
- **Un ou plusieurs comptes utilisateur locaux avec mot de passe.**
- **Une clé RSA générée (crypto key generate rsa).**
- **Le transport SSH activé sur les lignes VTY.**

---

3. Interface virtuelle (VLAN 1 sur un switch)

Un switch de couche 2 n’a pas d’interface IP physique. Pour lui attribuer une adresse IP, on utilise une interface VLAN virtuelle :

interface vlan 1

ip address 192.168.1.10 255.255.255.0

no shutdown

Cela permet de gérer le switch à distance (par SSH ou ping).

4. Étapes de configuration SSH

1. **Définir un nom d'hôte :**

hostname SW-SSH

2. **Définir un nom de domaine :**

ip domain-name novatech.local

3. **Créer un utilisateur local avec privilège :**

username admin privilege 15 secret admin123

Le niveau de privilège définit les droits de l'utilisateur. Voir tableau ci-dessous.

4. **Générer la clé RSA :**

crypto key generate rsa

Choisir une taille de clé d'au moins 1024 bits.

5. **Activer SSH sur les lignes VTY :**

line vty 0 4

login local

transport input ssh

6. **Renforcer la sécurité SSH :**

ip ssh version 2 ! Utiliser la version 2 plus sécurisée

ip ssh time-out 60 ! Déconnexion après 60s d'inactivité

ip ssh authentication-retries 3 ! 3 tentatives de connexion maximum

---

5. Niveaux de privilège - Tableau de synthèse

Niveau de privilège	Description	Exemple de commande
0	Accès ultra-limité (ping, logout, etc.)	username user0 privilege 0 secret test
1 (par défaut)	Accès utilisateur classique (show, etc.)	username user1 privilege 1 secret test
15	Accès total (administrateur)	username admin privilege 15 secret admin123

---

6. Texte à trous

1. **Le protocole ___ permet une connexion _____ à distance.**
2. **SSH utilise le port __ par défaut.**
3. **Pour qu'un switch soit accessible en IP, il faut créer une _____ virtuelle.**
4. **La commande crypto key generate RSA permet de _____ la clé SSH.**
5. **Pour activer SSH sur les lignes VTY, il faut utiliser _____ _____ ___.**
6. **La commande ip ssh authentification-retries 3 permet de _____ les tentatives de connexion.**

---

7. Tableau de configuration SSH à compléter

Action	Commande associée Cisco
Définir le nom d'hôte	
Définir un domaine	
Créer un utilisateur local	
Générer les clés RSA	
Activer SSH sur lignes VTY	
Forcer l'utilisation des comptes	
Restreindre les accès à SSH uniquement	
Vérifier si SSH est actif	
Définir le timeout SSH	
Limiter les tentatives SSH	

---

8. Questions de révision

1. **Quelle est la différence entre SSH et Telnet ?**
2. **Pourquoi faut-il générer une clé RSA pour utiliser SSH ?**
3. **À quoi sert la commande login local ?**
4. **Quelle commande permet de vérifier que SSH est activé ?**
5. **Pourquoi définir un nom d'hôte et un nom de domaine pour SSH ?**
6. **Peut-on utiliser SSH sur un switch de couche 2 ? Sous quelles conditions ?**
7. **Quel est l'intérêt de limiter les tentatives d'authentification SSH ?**

line vty 0 4 — Qu'est-ce que c'est ?

🔹 **VTY = Virtual Teletype Lines**

- Ce sont des **lignes logiques** (virtuelles) permettant les connexions **à distance** à un équipement Cisco.
- Ces connexions peuvent se faire via **Telnet ou SSH** (et aujourd'hui, on privilégie **SSH**, car sécurisé).

🔸 **Que veut dire 0 4 ?**

- Les lignes VTY sont **numérotées**.
- line vty 0 4 signifie que tu configures **les lignes 0 à 4**, soit **5 sessions simultanées** possibles à distance.

💡 En résumé :
line vty 0 4 = "Je configure les **5 premières lignes de connexion distante** disponibles sur l'équipement."

🔄 **Peut-on avoir plus de lignes VTY ?**

Oui ! Sur certains équipements Cisco :

- Tu peux avoir line vty 0 15
  → ce qui permet **jusqu'à 16 connexions distantes simultanées**.

- ✅ Résultat :
  Un seul utilisateur pourra se connecter en SSH. Les autres verront un message du type :
- `% Connection refused by remote host`

ip ssh pubkey-chain

username admin

key-string

ssh-rsa AAAAB3... (clé publique générée sur le PC)

exit