

# TP Réseaux : Configuration et Sécurisation d'un Switch

## Partie 1 : Découverte et Connexion Initiale (Câble Console)

Pour configurer un switch sorti d'usine, il faut d'abord s'y connecter physiquement via son port console.

1. **Câblage** : Connectez le câble console entre le port série/USB de votre PC et le port "Console" situé à l'arrière ou à l'avant du switch.
2. **Logiciel** : Ouvrez un émulateur de terminal sur votre PC (ex: PuTTY ou TeraTerm).
3. **Paramètres** : Configurez la connexion en mode "Serial" avec les paramètres standards (Vitesse : 9600 bauds, Bits de données : 8, Parité : Aucune, Bits d'arrêt : 1, Contrôle de flux : Aucun).
4. **Démarrage** : Allumez le switch. Observez la séquence de démarrage (POST) sur votre écran.
5. Une fois le switch démarré, appuyez sur *Entrée*. Quel est le symbole qui s'affiche à côté du nom du switch ? Que signifie-t-il ?

## Partie 2 : Configuration de Base et Sécurisation Locale

Vous allez maintenant donner une identité au switch et le protéger contre les accès physiques non autorisés.

1. Passez en mode d'exécution privilégié, puis en mode de configuration globale.
2. **Nom d'hôte** : Renommez le switch en SW-GroupeX (remplacez X par votre numéro de groupe).
3. **Mot de passe privilégié** : Configurez un mot de passe chiffré (cisco123) pour protéger le passage en mode privilégié.
4. **Sécurisation du port console** : Protégez l'accès console avec le mot de passe compass. Faites en sorte qu'il soit demandé à chaque connexion.
5. **Chiffrement** : Activez le service qui permet de chiffrer tous les mots de passe en clair dans le fichier de configuration.
6. **Vérification** : Quittez complètement la session et essayez de vous reconnecter pour tester vos mots de passe.

## Partie 3 : Administration à Distance (Management IP et SSH)

Un administrateur réseau ne se déplace pas toujours avec son câble console. Vous allez configurer le switch pour qu'il soit accessible via le réseau (câble RJ45).

1. **Interface de Management (SVI)** : Allez dans la configuration de l'interface virtuelle VLAN 1.
2. Attribuez-lui l'adresse IP 192.168.10.254 avec le masque 255.255.255.0. N'oubliez pas d'activer l'interface.

3. **Préparation SSH :**
  - Configurez un nom de domaine IP : `tp-reseau.local`
  - Générez des clés de chiffrement RSA (choisissez une taille de 1024 bits).
  - Créez un utilisateur local : Nom d'utilisateur `admin`, mot de passe secret `admin123`.
4. **Activation SSH :** Allez dans la configuration des lignes virtuelles (VTY 0 à 4). Paramétrez-les pour qu'elles utilisent la base de données locale pour l'authentification et qu'elles n'acceptent **que** le protocole SSH.

## Partie 4 : Test de Connectivité (Câble RJ45)

Il est temps de tester l'accès réseau.

1. **Câblage :** Connectez le câble RJ45 entre la carte réseau de votre PC et le port FastEthernet 0/1 (ou GigabitEthernet 1/0/1) du switch.
2. **Configuration PC :** Configurez l'adresse IP de votre PC de manière statique : IP `192.168.10.10`, Masque `255.255.255.0`.
3. **Ping :** Ouvrez l'invite de commande du PC (`cmd`) et lancez un ping vers l'adresse IP du switch (`192.168.10.254`). Le ping fonctionne-t-il ? (Note: le premier paquet peut être perdu à cause d'ARP).
4. **Accès SSH :** Ouvrez PuTTY, choisissez le protocole SSH, entrez l'adresse IP du switch. Connectez-vous avec l'utilisateur `admin`. Vous devriez maintenant configurer le switch via le réseau !

## Partie 5 : Sécurisation du Port d'Accès (Port Security)

Pour éviter qu'une personne non autorisée ne branche son propre ordinateur sur votre switch, vous allez verrouiller le port FastEthernet 0/1 sur l'adresse MAC de *votre* PC.

1. Sur le switch (en SSH ou console), repérez l'adresse MAC de votre PC.
2. Entrez dans la configuration de l'interface Fa0/1 (ou Gi1/0/1).
3. Passez le port en mode accès (Access).
4. Activez le "Port Security".
5. Configurez-le pour qu'il n'accepte qu'une seule adresse MAC (maximum 1).
6. Configurez-le pour qu'il apprenne automatiquement (sticky) l'adresse MAC du premier PC qui y envoie des données (le vôtre).
7. En cas de violation (si une autre adresse MAC est détectée), le port doit s'éteindre automatiquement (shutdown).
8. *Optionnel pour tester :* Si vous aviez un autre PC sous la main, que se passerait-il si vous le branchiez à la place du vôtre ?

## Partie 6 : Sauvegarde et Nettoyage

1. **Sauvegarde :** Enregistrez votre configuration courante (Running-config) dans la mémoire non volatile (Startup-config) pour qu'elle survive à un redémarrage.
2. Faites valider votre travail par le professeur.
3. **Nettoyage :** Effacez la configuration de démarrage.

