# Télécommunication et réseaux Travaux pratique

Comment accéder aux différents modes du terminal :

Utilisateur : >

Privilégié (actif) : #

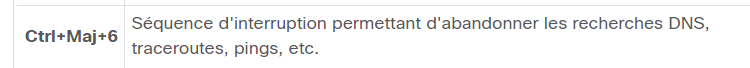
Configuration globale : (config) #

Configuration spécifique :(config-if) exemple.

Une image contenant texte, capture d’écran, Police, noir

Description générée automatiquement

Raccourci pour annuler une action :



Mètre **?** pour nous aider à trouver la bonne syntaxe et les attributs de nos commandes.

**Modifier le nom de l’appareil :**





Choisir un mot de passe approprier :

Une image contenant texte, Police, algèbre, capture d’écran

Description générée automatiquement

Configurer les mots de passe :

**Mot de passe du port console :**

Passer en mode configuration globale : **configure terminal .**

Puis accéder à l’entrer que vous voulez sécuriser **line console 0** (le port console) .

Utiliser la commande **password** ……(mot de passe).

Terminer par **login** pour activer le mot de passe.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Mot de passe du mode privilégier :**

Pour sécuriser l’accès au mode privilégier on utilise la commande **enable secret** suivie du mot de passe.



**Sécuriser les lignes Vty (terminal virtuel):**

Les lignes Vty sont des lignes qui permettent aux responsables IT de se connecter à distance aux périphériques.

Pour les sécuriser il faut accéder au mode de configuration globale puis a la ligne Vty. **Line vty 0 15**

Ensuite utiliser la commande **password** suivie du mot de passe

Et puis activer **l’acces Vty** avec la commande **login.**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

**Chiffrer les mots de passe :**

Pour éviter l’affichage des mots de passe quand on exécute la commande **show running config**

On utilise : **service password-encryption**

Qui va les encrypter.



**Message de bannière :**

Il est important de mètre un message qui restreint l’accès aux personnes non autoriser pour des thèmes juridiques.

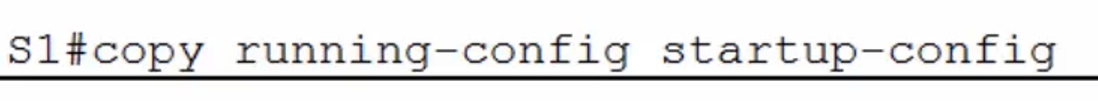
Pour cela on se rend dans le mode de **configuration globale**

Et on utilise la commande **banner motd # du message du jour #**

****

**Enregistrer la configuration du périphérique :**

Pour afficher le fichier de configuration initiale, lancez la commande **show startup-config** du **mode d'exécution privilégié.**

Pour enregistrer les modifications apportées à la configuration en cours dans le fichier de configuration initiale, utilisez la commande **copy running-config startup-config** du **mode d'exécution privilégié.** 

**Reload** permet d’effacer les modifications faites qui ne sont pas enregistrer

La commande **erase startup-config** du **mode d'exécution privilégié** permet de supprimer la configuration initiale. Quand vous entrez cette commande, le commutateur vous demande de la confirmer. Appuyez sur Enter pour accepter la connexion.

Configuration d’une interface virtuelle :

Pour pouvoir accéder a un commutateur a distance il faut configurer le SVI

Pour cela on utilise la commande **interface Vlan 1** depuis le mode de configuration globale

Puis la commande **ip address** suivie de l’adresse ip que l’on veut lui attribuer

Enfin pour activer l’interface virtuelle il faut mettre la commande **no shutdown**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

La commande ping permet de voir s’il y a pas de problèmes de communication entre périphériques finaux.

Pour configurer un GUA IPV6 sur un router

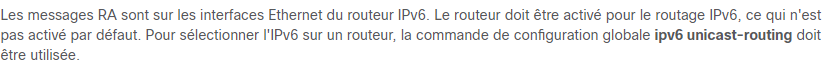
Une image contenant texte, capture d’écran

Description générée automatiquement

Une image contenant texte, capture d’écran

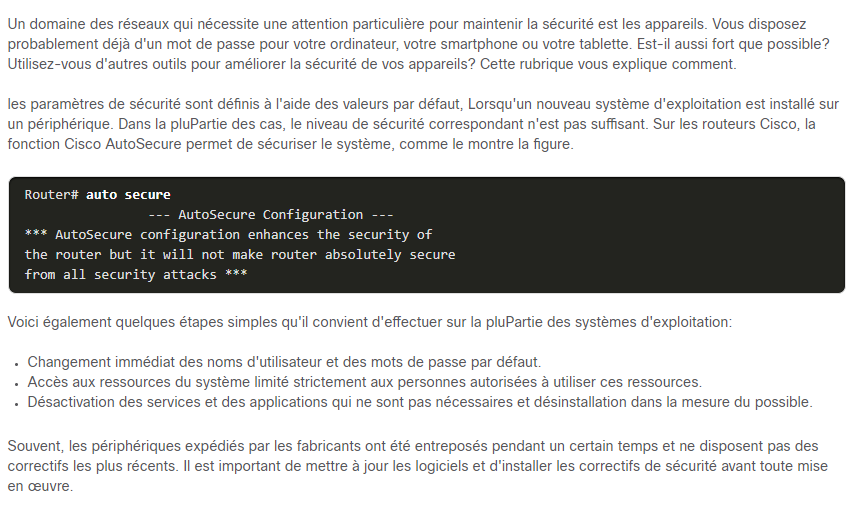
Description générée automatiquement

Demander un RA :



Une image contenant texte, Police, capture d’écran, algèbre

Description générée automatiquement



Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Activation de SSH :

Pour sécuriser un périphérique il faut activer le SSH pour éviter que les données soient compromises pour ce faire il faut suivre 6 étapes :

1 Configurer un Nom d’hôte unique a ce périphérique : (config)# hostname [nom de votre choix]

2 Configurer le nom de Domaine ip : (config)# ip-domain name [nom de domaine de votre choix]

3 Générer une clé pour chiffrer le trafic SSH : crypto key generate rsa general-keys modulus [bits] il est recommandé d’utiliser un module de au moins 1024

4 Vérifiez ou créer une entrée dans la base de données locale pour cela on crée un nom d’utilisateur dans la base locale avec la commande username et un mot de passe pour celui-ci avec le paramètre secret suivi du mot de passe :  (config)# username …… secret ……..

5 Authentification par rapport à la base de données locale. Utilisez la commande login local de configuration de ligne pour authentifier la ligne vty par rapport à la base de données locale.

:

6. Activez les sessions SSH entrantes de vty. Par défaut, aucune session d'entrée n'est autorisée sur les lignes vty. Vous pouvez spécifier plusieurs protocoles d'entrée, y compris Telnet et SSH à l'aide de la commande transport input [ssh | telnet] :

R1(config)# line vty 0 4

R1(config-line)# login local

R1(config-line)# transport input ssh

R1(config-line)# exit

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement