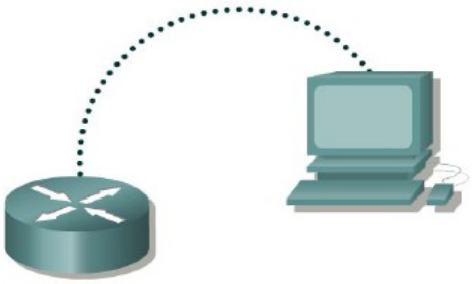
Module R4 – TP1.1 : Récupération d'un mot de passe

Objectif :
Ce TP explique comment accéder à un routeur avec un mot de passe (**enable**) de mode privilégié inconnu. Il est à noter que quiconque connaît cette procédure et a accès à un port console de routeur peut modifier le mot de passe et prendre contrôle d'un routeur. C'est pour cela qu'il est extrêmement important que les routeurs possèdent également une sécurité physique pour empêcher tout accès non autorisé.

Attention: A la fin du TP, il faut supprimer les mots de passe sur tous les routeurs.



Désignation du routeur	Nom du routeur	Mot de passe " enable secret "	Mots de passe enable/VTY/console
Routeur 1	GAD	classe	cisco

Manipulation :

Lancez une session HyperTerminal en mode console. Configurez le nom d'hôte et les mots de passe sur le routeur comme indiqué ci-dessus. Faites une configuration de base avec un mot de passe **enable secret**. Exécutez **copy running-config startupconfig** et rechargez le routeur.

Étape 1 : Tentez de vous connecter au routeur

Tentez de vous connecter au routeur à l'aide du mot de passe enable différent de **classe**. Le résultat doit être similaire à celui-ci :
Router>**enable**
Password:
% Bad secrets

Étape 2 : Documentez la valeur de registre de configuration actuelle

1. Tapez à présent le bon mot de passe.
2. A l'invite du mode utilisateur, tapez **show version**.
3. Consignez la valeur affichée pour le registre de configuration _____ . Par exemple 0x2102.

Étape 3 : Passez en mode moniteur ROM

4. Démarrez le routeur à froid (la commande « reload » permet de réaliser cette procédure).
5. Appuyez sur les touches (**Ctrl**) (**Pause**), cette combinaison doit être effectuée dans les 60 secondes qui suivent le démarrage à froid du routeur.
6. Le mode **rommom** est alors lancé. En fonction du matériel de routeur, l'un des prompt suivants s'affiche : « **rommon 1 >** » ou simplement « **>** ».

Étape 4 : Examinez l'aide du mode moniteur ROM

7. Tapez **?** à l'invite. Indiquez le résultat obtenu ?

Étape 5 : Modifiez la valeur du registre de configuration pour démarrer sans charger le fichier de configuration:

8. À partir du mode rommon, tapez **confreg 0x2142** (voir l'annexe) pour modifier le registre de configuration. rommon 2 > **confreg 0x2142**

   Certains routeurs risquent de ne pas reconnaître la commande **confreg**. Dans ce cas, utilisez la commande suivante : **>o/r 0x2142**

   Cette commande a pour effet d'empêcher le routeur de démarrer sur le fichier de démarrage de la NVRAM.

Étape 6 : Redémarrez le routeur

9. 1. À partir du mode rommon, redémarrez le routeur. La commande **reset (commande i)** relance le routeur. Rommon 3 > **reset (ou i)**
10. À cause de la nouvelle valeur du registre de configuration, le routeur ne charge pas le fichier de configuration. Le système demande :"Would you like to enter the initial configuration dialog? [yes]: Entrez **no** et appuyez sur **Entrée**.

Étape 7 : Passez en mode privilégié et changez de mot de passe

11. À l'invite du mode utilisateur Router>, tapez **enable** et appuyez sur **Entrée** pour passer en mode privilégié sans mot de passe.
12. Passez en mode de configuration globale.
13. Dans le mode de configuration globale, modifiez le mot de passe enable secret.
14. Toujours en mode de configuration globale, tapez **config-register xxxxxxx**. xxxxxxx est la valeur du registre de configuration originale enregistrée à l'étape 2. Appuyez sur **Entrée**.
15. Utilisez la commande **copy running-config startup-config** pour enregistrer la nouvelle configuration.
16. Avant de redémarrer le routeur, vérifiez la nouvelle valeur du registre de configuration. À partir de l'invite du mode privilégié, entrez la commande **show version** et appuyez sur **Entrée**.
17. La dernière ligne qui s'affiche doit être : Configuration register is 0x2142 (will be 0x2102 at next reload).
18. Utilisez la commande **reload** pour redémarrer le routeur.

Étape 8: Enlevez le mot de passe sur le routeur.

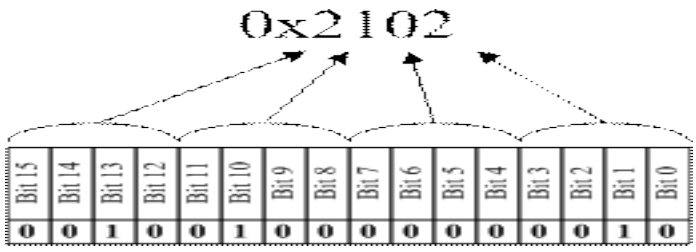
ANNEXE - registre de configuration

1) Généralités

Le registre de configuration a une taille de 16 bits, et s'exprime sous la forme d'une valeur hexadécimale. On peut modifier sa valeur :

- Depuis IOS, en utilisant la commande **config-register {valeur}** dans le mode de configuration globale.
- Depuis le mode RXBoot, accessible en utilisant la combinaison de Break avant les 60 secondes qui suivent le démarrage à froid du routeur (en général **Ctrl-Pause**). La commande permettant de modifier la valeur dépend du type de dispositif sur lequel on se trouve.
- La valeur par défaut du registre de configuration est 0x2102.

Ce registre a pour principal but d'établir le comportement d'un routeur :



- **Bits 0 à 3** : Champ d'amorçage.
- **Bit 4** : Démarrage rapide (sur les routeurs 7000).
- **Bit 5** : Vitesse de la ligne console supérieure à 9600 Bauds.
- **Bit 6** : Ignorer le fichier de configuration de sauvegarde (en NVRAM).
- **Bit 7** : OEM.
- **Bit 8** : Combinaison de Break après chargement d'IOS.
- **Bit 9** : Utilisation du bootstrap secondaire.
- **Bit 10** : Broadcast IP avec tout à zéro.

- **Bits 11 & 12** : Vitesse de la ligne console.
- **Bit 13** : Utiliser l'image par défaut en ROM si échec du démarrage réseau.
- **Bit 14** : Broadcasts IP n'ont pas de numéros de réseau.
- **Bit 15** : Activer les messages de diagnostics et ignorer le contenu de la NVRAM

2) Explication de la valeur de chaque Bit

a) Bits 0 à 3 : Champ d'amorçage.

Ces quatre Bits permettent de spécifier l'ordre de recherche des commandes **boot system** sur le dispositif Cisco :

Valeur du champ d'amorçage	Description
0x---0	Démarrer en mode moniteur de mémoire ROM (invite du bootstrap)
0x---1	Utiliser les commandes **boot system** présentes en mémoire ROM
0x---2 à 0x---F	Utiliser les commandes **boot system** présentes en mémoire NVRAM (fichier de configuration)

b) Bits 5, 11 & 12 : Vitesse de la ligne console.

Ces trois Bits spécifient la vitesse de synchronisation de la ligne console :

Bit 5	Bit 12	Bit 11	Vitesse en Bauds
0	0	0	9600 (par défaut)
0	0	1	4800
0	1	0	1200
0	1	1	2400
1	0	0	19200
1	0	1	38400
1	1	0	57600
1	1	1	115200

c) Bit 6 : Ignorer le fichier de configuration de sauvegarde.

Ce Bit permet de forcer IOS à ignorer le fichier de configuration de sauvegarde, présent en mémoire NVRAM :

- **0** : Utilisation du fichier de configuration.

- **1** : Fichier de configuration ignoré.

La possibilité de pouvoir ignorer ce fichier de configuration est très pratique, principalement pour la procédure de récupération des mots de passe, afin d'outrepasser les mots de passe configurés.

d) Bit 8 : Combinaison de Break après chargement d'IOS.

La possibilité de pouvoir utiliser la combinaison de Break, même après le chargement d'IOS, est indiquée par la valeur du 8ème Bit :

- **0** : Combinaison de Break activée.
- **1** : Combinaison de Break désactivée après le chargement d'IOS (défaut).

e) Bits 10 & 14 : Broadcasts IP.

Ces 2 Bits indiquent comment doivent être formés les broadcasts IP :

Bit 14	Bit 10	Adresse {partie sous-réseau} {partie hôte}
0	0	{uns}{uns}
0	1	{zéros}{zéros}
1	0	{sous-réseau}{zéros}
1	1	{sous-réseau}{uns}

Ceci permet de définir l'adresse de destination des broadcasts IP.

f) Bit 13 : Utiliser l'image par défaut en ROM si échec du démarrage réseau.

Avec ce Bit, on peut modifier le comportement du bootstrap face à un échec de démarrage réseau (TFTP) :

- **0** : Tentatives infinies de chargement du fichier image d'IOS depuis le réseau (TFTP).
- **1** : Maximum 5 tentatives de chargement réseau avant d'utiliser l'image présente en mémoire ROM.

3) Exemples

0x2102 : Valeur par défaut. La combinaison de Break est désactivée après le chargement d'IOS, et la ligne console fonctionnera a une vitesse de 9600 Bauds.

0x2142 : Idem que précédemment, sauf que l'on va ignorer le fichier de configuration de sauvegarde. Cette valeur du registre est généralement utilisée pour la procédure de récupération des mots de passe.

0x6502 : Idem qu'avec la valeur 0x2102, sauf que les broadcasts IP seront émis uniquement sur le sous-réseau local (exemple : 192.168.10.255) et non sur tous les réseaux (255.255.255.255).