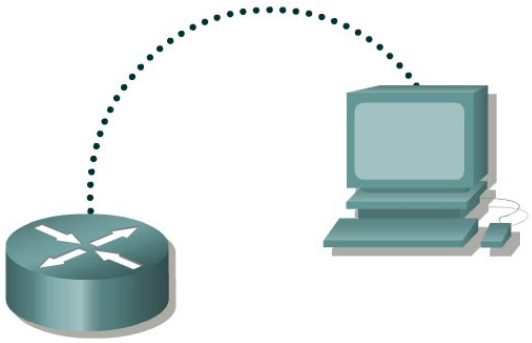
TP 5.2.6a Procédures de récupération de mot de passe



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

Objectif

- Accéder à un routeur avec un mot de passe (enable) de mode privilégié inconnu.

Prérequis/Préparation

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.

Installez un réseau similaire à celui du schéma précédent. Tout routeur doté de l'interface appropriée peut être utilisé. Vous pouvez utiliser les routeurs 800, 1600, 1700, 2500, 2600 ou une combinaison de ces routeurs. Reportez-vous au tableau qui se trouve à la fin du TP pour repérer les identifiants d'interfaces à utiliser en fonction de l'équipement disponible. Dans ce TP, les informations affichées par le routeur lors de sa configuration ont été obtenues avec un routeur de la gamme 1721. Celles-ci peuvent varier légèrement avec un autre routeur.

Lancez une session HyperTerminal comme indiqué dans le TP intitulé Établissement d'une session en mode console avec HyperTerminal.

Remarque : Configurez le nom d'hôte et les mots de passe sur le routeur. Demandez à un professeur, à un assistant de laboratoire ou à un autre étudiant de configurer une configuration

de base avec un mot de passe enable secret. Exécutez **copy running-config startup-config** et rechargez le routeur.

Remarque : La version du programme HyperTerminal fournie avec Windows 95, 98, NT et 2000 a été développée pour Microsoft par Hilgraeve. Certaines versions peuvent ne pas exécuter de séquence d'« interruption » comme l'exige la technique de récupération des mots de passe sur les routeurs Cisco. Dans ce cas, une mise à niveau, appelée HyperTerminal Private Edition (PE), est disponible gratuitement à des fins personnelles ou de formation. Vous pouvez télécharger ce programme à l'adresse http://www.hilgraeve.com.

Étape 1 Tentez de vous connecter au routeur

a. Réalisez les connexions de console nécessaires et établissez une session HyperTerminal avec le routeur. Tentez de vous connecter au routeur à l'aide du mot de passe enable **cisco**. Le résultat doit être similaire à celui-ci :

```
Router>enable
Password:
Password:
Password:
% Bad secrets

Router>
```

Étape 2 Documentez la valeur de registre de configuration actuelle

a. A l'invite du mode utilisateur, tapez **show version**.

b. Consignez la valeur affichée pour le registre de configuration _____ . Par exemple 0x2102.

Étape 3 Passez en mode moniteur ROM

a. Mettez le routeur hors tension, attentez quelques secondes, puis remettez-le sous tension. Dès que le routeur affiche « System Bootstrap, Version … » sur l'écran HyperTerminal, appuyez simultanément sur la touche **Ctrl** et sur la touche **Attn**. Le routeur démarre alors en mode moniteur ROM. En fonction du matériel de routeur, l'une des différentes invites telles que : « **rommon 1 >** » ou simplement « **>** » peut s'afficher.

Étape 4 Examinez l'aide du mode moniteur ROM

a. Tapez **?** à l'invite. Le résultat doit être similaire à celui-ci :

```
rommon 1 >?
alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
context             display the context of a loaded image
dev                 list the device table
dir                 list files in file system
dis                 display instruction stream
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
sysret              print out info from last system return
tftpdnld            tftp image download
xmodem              x/ymodem image download
```


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

a. À partir du mode moniteur ROM, tapez **confreg 0x2142** 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
```

Étape 6 Redémarrez le routeur

a. À partir du mode moniteur ROM, tapez **reset** ou mettez le routeur hors tension puis sous tension.

```
rommon 2 >reset
```

b. 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

a. Maintenant, à l'invite du mode utilisateur Router>, tapez **enable** et appuyez sur **Entrée** pour passer en mode privilégié sans mot de passe.

b. Utilisez la commande **copy startup-config running-config** pour restaurer la configuration de routeur existante. Puisque l'utilisateur est déjà en mode privilégié, aucun mot de passe n'est nécessaire.

c. Tapez **configure terminal** pour passer en mode de configuration globale.

d. Dans le mode de configuration globale, tapez **enable secret class** pour modifier le mot de passe enable secret.

e. 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**.

f. Utilisez la combinaison **Ctrl z** pour retourner en mode privilégié.

g. Utilisez la commande **copy running-config startup-config** pour enregistrer la nouvelle configuration.

h. 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**.

i. La dernière ligne qui s'affiche doit être :

Configuration register is 0x2142 (will be 0x2102 at next reload).

j. Utilisez la commande **reload** pour redémarrer le routeur.

Étape 8 Vérifiez le nouveau mot de passe et la nouvelle configuration

a. Lors du rechargement du routeur, le mot de passe doit être **class**.

Après avoir réalisé les étapes précédentes, déconnectez-vous en tapant **exit**. Mettez le routeur hors tension.

Effacement et rechargement du routeur

Passez en mode privilégié à l'aide de la commande **enable**.

```
Router>enable
```

Si un mot de passe vous est demandé, entrez class. Si "class" ne fonctionne pas, demandez au professeur de vous aider.

À l'invite du mode privilégié, entrez la commande **erase startup-config**.

```
Router#erase startup-config
```

Vous obtenez le message suivant :

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

Appuyez sur **Entrée** pour confirmer.

La réponse suivante devrait s'afficher :

```
Erase of nvram: complete
```

Ensuite, à l'invite du mode privilégié, entrez la commande **reload**.

```
Router#reload
```

Vous obtenez le message suivant :

```
System configuration has been modified. Save? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Proceed with reload? [confirm]
```

Appuyez sur **Entrée** pour confirmer.

La première ligne de la réponse est la suivante :

```
Reload requested by console.
```

Après le rechargement du routeur, la ligne suivante s'affiche :

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

Tapez **n**, puis appuyez sur **Entrée**.

Vous obtenez le message suivant :

```
Press RETURN to get started!
```

Appuyez sur **Entrée**.

Le routeur est prêt et le TP peut commencer.

Relevé des interfaces de routeur					
Modèle du routeur	Interface Ethernet 1	Interface Ethernet 2	Interface série 1	Interface série 2	Interface 5
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)			
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)	
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)	
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)	
Pour connaître la configuration exacte du routeur, observez les interfaces. Vous pourrez ainsi identifier le type du routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. En revanche, le tableau fournit les identifiants des combinaisons d'interfaces possibles pour chaque appareil. Ce tableau d'interfaces ne comporte aucun autre type d'interface même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI pourrait illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans une commande IOS.					

