

# Travaux pratiques : configuration et vérification de la récupération de mot de passe

## Topologie



## Objectifs

**Partie 1 : Configurer les paramètres de base des périphériques**

**Partie 2 : Redémarrer le routeur et passer au mode ROMMON**

**Partie 3 : Réinitialiser le mot de passe et enregistrer la nouvelle configuration**

**Partie 4 : Vérifier que le routeur charge correctement**

## Contexte/scénario

L'objectif de ces travaux pratiques consiste à réinitialiser le mot de passe actif sur un routeur Cisco spécifique. Le mot de passe enable protège l'accès au mode d'exécution privilégié et au mode de configuration sur les périphériques Cisco. Le mot de passe actif peut être récupéré, mais le mot de passe secret actif est chiffré et devra être remplacé par un nouveau mot de passe.

Afin de contourner un mot de passe, un utilisateur doit être familiarisé avec le mode du moniteur ROM (ROMMON), ainsi qu'avec les paramètres du registre de configuration des routeurs Cisco. ROMMON est un logiciel simplifié d'interface de ligne de commande stocké dans la mémoire morte. Il peut être utilisé pour résoudre les erreurs de démarrage et récupérer un routeur lorsqu'un IOS est introuvable.

Dans ces travaux pratiques, vous changerez le registre de configuration afin de réinitialiser le mot de passe actif sur un routeur Cisco.

## Ressources requises

- 1 routeur (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 1 PC (Windows 7, Vista ou XP, équipé d'un programme d'émulation du terminal tel que Tera Term)
- Câble de console pour connecter le PC au périphérique Cisco IOS par le port de console

## Partie 1 : Configurer les paramètres de base des périphériques

Dans la partie 1, vous configurerez la topologie du réseau et copierez la configuration de base vers le routeur R1. Le mot de passe est chiffré afin de configurer le scénario du besoin de récupération à partir d'un mot de passe actif inconnu.

**Étape 1 : Câblez le réseau conformément à la topologie indiquée.**

**Étape 2 : Initialisez et redémarrez les routeurs, le cas échéant.**

**Étape 3 : Configurez les paramètres de base sur le routeur.**

- Accédez au routeur par la console et passez en mode de configuration globale.

- b. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le routeur.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyMLl5/
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
line con 0
logging sync
end
Écrire
exit
```

- c. Appuyez sur **Entrée** et essayez de passer en mode d'exécution privilégié.

Comme vous pouvez le voir, l'accès à un périphérique IOS Cisco est très limité si le mot de passe actif est inconnu. Il est important pour un ingénieur réseau de sortir d'un problème de mot de passe actif inconnu sur un périphérique IOS Cisco.

## Partie 2 : Redémarrer le routeur et passer au mode ROMMON

### Étape 1 : Redémarrer le routeur

- a. Tout en étant toujours en console dans le routeur R1, enlevez le cordon d'alimentation à l'arrière de R1.

**Remarque** : si vous travaillez dans un pod NETLAB, demandez à votre instructeur comment éteindre, puis rallumer le routeur.

- b. À partir de la session de console sur le PC-A, effectuez une coupure franche pour interrompre le processus de démarrage normal des routeurs, puis passez au mode ROMMON.

**Remarque** : pour effectuer une coupure franche dans Tera Term, appuyez simultanément sur les touches **Alt** et **B**.

### Étape 2 : Réinitialisez le registre de configuration.

- a. À partir de l'invite ROMMON, entrez un point d'interrogation (?), puis appuyez sur **Entrée**. Cela permettra d'afficher une liste des commandes ROMMON disponibles. Recherchez la commande **confreg** dans cette liste.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
break                set/show/clear the breakpoint
confreg             configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of motherboard cookie PROM in hex
dev                  list the device table
dir                  list files in file system
frame                print out a selected stack frame
help                 monitor builtin command help
history              monitor command history
```

iomemset	set IO memory percent
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
rommon-pref	Select ROMMON
set	display the monitor variables
showmon	display currently selected ROM monitor
stack	produce a stack trace
sync	write monitor environment to NVRAM
sysret	print out info from last system return
tftpdnld	tftp image download
unalias	unset an alias
unset	unset a monitor variable
hwpart	Read HW resources partition

rommon 2 >

**Remarque :** le nombre à la fin de l'invite ROMMON sera incrémenté de 1 à chaque fois qu'une commande est entrée.

- b. Entrez **confreg 0x2142**, puis appuyez sur **Entrée**. Changer le registre en Hex 2142 ordonne au routeur de ne pas charger automatiquement la configuration de démarrage pendant le démarrage. Il faudra redémarrer le routeur pour que le remplacement du registre de configuration soit appliqué.

rommon 2 > **confreg 0x2142**

You must reset or power cycle for new config to take effect

rommon 3 >

- c. Lancez la commande ROMMON **reset** pour redémarrer le routeur.

rommon 3 > **reset**

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)  
Technical Support: <http://www.cisco.com/techsupport>  
Copyright (c) 2011 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB  
CISCO1941/K9 platform with 524288 Kbytes of main memory  
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized  
program load complete, entry point: 0x80803000, size: 0x1b340  
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software  
program load complete, entry point: 0x81000000, size: 0x480ce0c  
Self decompressing the image :  
#####

```
#####
#####
#####
#####
#####
#####
##### [OK]
```

<résultat omis>

- d. Lorsqu'il vous est demandé si vous voulez entrer dans la boîte de dialogue de la configuration initiale, entrez **no**, puis appuyez sur **Entrée**.

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

- e. Le routeur achèvera son processus de démarrage et affichera l'invite d'exécution utilisateur. Passez en mode d'exécution privilégié.

```
Router> enable
Router#
```

### Partie 3 : Réinitialiser le mot de passe et enregistrer la nouvelle configuration

- a. En mode d'exécution privilégié, copiez la configuration de démarrage dans la configuration en cours.

```
Router# copy startup-config running-config
Destination filename [running-config]?
1478 bytes copied in 0.272 secs (5434 bytes/sec)
```

```
R1#
```

- b. Passez en mode de configuration globale.  
c. Réinitialisez le mot de passe secret actif en **cisco**.

```
R1(config)# enable secret cisco
```

- d. Remettez le registre de configuration en 0x2102 pour permettre à la configuration de démarrage de charger au prochain redémarrage du routeur.

```
R1(config)# config-register 0x2102
```

- e. Quittez le mode de configuration globale.  
f. Copier la configuration en cours en tant que configuration de démarrage

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Vous avez réussi à réinitialiser le mot de passe actif sur un routeur.

## Partie 4 : Vérifier que le routeur charge correctement

**Étape 1 :** Redémarrez le routeur R1.

**Étape 2 :** Vérifiez que la configuration de démarrage est chargée automatiquement.

**Étape 3 :** Passez en mode d'exécution privilégié.

Le nouveau mot de passe secret actif doit être cisco. Si vous arrivez à passer en mode d'exécution privilégié, c'est que vous avez réussi ces travaux pratiques.

### Remarques générales

Pourquoi est-il important qu'un routeur soit physiquement sécurisé pour empêcher les accès non autorisés ?

---

---

---