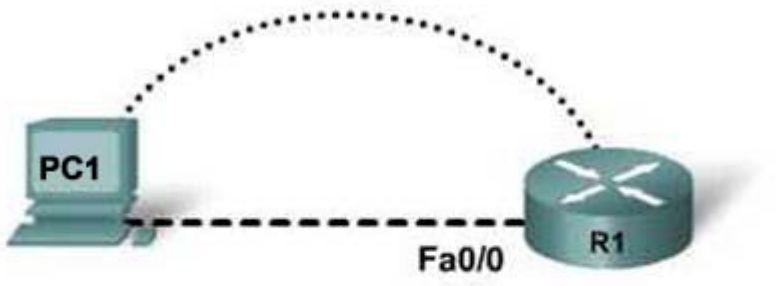
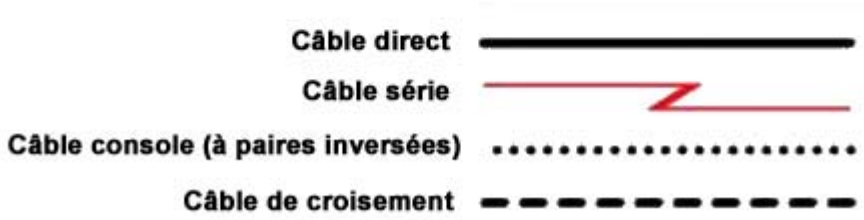
Travaux pratiques 1.4.6A Accès physique au réseau

Topologie 1





Désignation du périphérique	Nom du périphérique	Adresse Fast Ethernet	Masque de sous-réseau
R1	FC-CPE-1	10.0.0.1	255.255.255.0
PC	PC1	10.0.0.254	255.255.255.0

Objectifs

- Accéder à un routeur avec des mots de passe de connexion et de mode privilégié inconnus
- Démontrer la nécessité et l'importance de la sécurité physique pour les périphériques réseau

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques font appel à des compétences qui se rapportent aux objectifs d'examen CCNA suivants :

- Implémenter la sécurité de base d'un routeur
- Décrire les menaces actuelles grandissantes auxquelles est confrontée la sécurité des réseaux et expliquer le besoin d'implémentation d'une politique complète de sécurité afin d'atténuer ces menaces
- Expliquer les méthodes générales de réduction des menaces de sécurité courantes auxquelles les périphériques, hôtes et applications réseau sont confrontés
- Décrire les fonctions des appareils et des applications de sécurité courants
- Décrire les pratiques de sécurité recommandées, notamment les étapes initiales qui sécurisent les périphériques réseau

Résultats attendus et critères de réussite

Avant de commencer ces travaux pratiques, lisez les tâches que vous devez effectuer. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

En quoi est-il utile d'avoir une compréhension de l'accès aux périphériques réseau en administration réseau ?

_____

_____

_____

Comment un administrateur réseau sait-il si l'accès physique au périphérique est correctement configuré ?

_____

_____

_____

Contexte / Préparation

Ces travaux pratiques démontrent qu'un accès physique est nécessaire pour accéder au mot de passe des routeurs et des commutateurs Cisco, et pour le modifier. On tente d'abord d'établir une connexion Telnet en devinant le mot de passe. Lorsque cela ne fonctionne pas, on procède ensuite à l'accès physique au port de la console du routeur afin de permettre la modification des mots de passe et assumer le contrôle de l'appareil. Cela montre qu'il est extrêmement important que les routeurs et les commutateurs possèdent également, en plus d'une haute protection par mot de passe, une sécurité physique pour empêcher tout accès non autorisé.

Lorsqu'une connexion console est établie, les principes suivants s'appliquent au processus d'accès et de modification des mots de passe d'un routeur :

- Les mots de passe se trouvent dans le fichier de configuration de démarrage stocké en mémoire NVRAM. La séquence d'amorçage est modifiée afin qu'elle débute sans charger la configuration. Lorsque le routeur est en fonction sans que la configuration de démarrage ne soit chargée, il peut être reconfiguré à l'aide de nouveaux mots de passe connus.
- Un emplacement mémoire en NVRAM appelé registre de configuration contient une valeur binaire qui détermine la séquence de démarrage du routeur. La valeur du registre doit être modifiée afin que le routeur s'amorce mais ne charge pas la configuration de démarrage. Lorsque les mots de passe ont été changés, le registre de configuration est réinitialisé à une valeur qui charge la configuration de démarrage modifiée la prochaine fois que le routeur est mis sous tension.

Tâche 1 : accès aux mots de passe du routeur et modification

Étape 1 : tentative de connexion au routeur

REMARQUE : si le PC utilisé pour ces travaux pratiques est également connecté au réseau local de votre établissement ou à Internet, assurez-vous de bien noter les raccordements de câbles et les paramètres TCP/IP afin que ceux-ci puissent être rétablis à la fin des travaux pratiques.

a. En vous référant à la topologie 1, connectez le port Ethernet de la carte réseau du PC hôte au port Ethernet Fa0/0 du routeur au moyen d'un câble croisé. Assurez-vous que l'ordinateur hôte et le routeur sont tous les deux sous tension.

b. En utilisant la topologie préconfigurée, essayez d'établir une connexion Telnet au routeur au moyen de la ligne de commande du PC.

Quelle adresse IP utilisez-vous pour établir la connexion Telnet au routeur ? _____

Qu'affiche le message du jour ?

_____

_____

Quel est le nombre de tentatives de connexion autorisées ? _____

Quel message s'affiche pour indiquer l'échec de tentatives de connexion ?

_____

c. Quand la tentative de connexion à distance échoue, établissez une connexion physique directe au routeur en effectuant les raccordements de console nécessaires entre le PC et le routeur. Ouvrez ensuite une session de terminal au moyen de HyperTerminal ou TeraTerm.

Qu'affiche le message du jour ?

_____

_____

Essayez de vous connecter en devinant le mot de passe.

Quel est le nombre de tentatives de connexion autorisées ? _____

Quel message s'affiche pour indiquer l'échec de tentatives de connexion ?

_____

Le registre de configuration doit être modifié de façon à ce que la configuration de démarrage ne soit pas chargée. Cela est généralement effectué dans le mode de configuration globale, mais puisque vous ne pouvez pas du tout vous connecter, le processus d'amorçage doit d'abord être interrompu afin que la modification puisse être faite dans le mode moniteur ROM.

Étape 2 : passage en mode moniteur ROM

Le mode moniteur ROM (ROMmon) est un environnement limité de ligne de commande qui est utilisé dans des conditions particulières, comme le dépannage de niveau inférieur et le débogage. Le mode ROMmon est appelé lorsqu'une séquence de touche Break (Pause Attn) envoyée au port console interrompt le processus d'amorçage du routeur. Cela ne peut être réalisé qu'à partir de la connexion console physique.

La séquence de touche Break (Pause Attn) dépend du programme de terminal utilisé :

- Dans HyperTerminal, la combinaison de touche est Ctrl+Break (Pause Attn).
- Dans TeraTerm, il s'agit de Alt+b.

La liste des séquences de touches Break (Pause Attn) standard est disponible à l'adresse http://www.cisco.com/warp/public/701/61.pdf

a. Pour passer en mode moniteur ROM, éteignez le routeur, attendez quelques secondes, puis rallumez-le.

b. Dès que le routeur affiche « `System Bootstrap, Version …` » sur l'écran du terminal, appuyez simultanément sur les touches **Ctrl** et **Break (Pause Attn)** si vous utilisez HyperTerminal ou sur les touches **Alt** et **b** si vous utilisez TeraTerm.

Le routeur démarre alors en mode moniteur ROM. En fonction du matériel du routeur, l'une des différentes invites telles que « **`rommon 1 >`** » ou tout simplement « **`>`** » peut s'afficher.

Un exemple de résultat pourra ressembler à celui-ci :

```
Router>System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
######################################
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Étape 3 : examen de l'aide du mode moniteur ROM

Saisissez **?** 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 4 : modification du paramètre du registre de configuration pour démarrer sans charger le fichier de configuration

À partir du mode moniteur ROM, saisissez **confreg 0x2142** pour modifier le registre de configuration.

```
rommon 2 > confreg 0x2142
```

REMARQUE : le chiffre situé dans l'invite du mode ROMmon s'incrémente à chaque exécution de commande ; ce comportement est normal. L'incrément n'entraîne pas de changement de mode. Les mêmes commandes du mode ROMmon demeurent à disposition.

« **0x** » (zéro x) indique que 2142 est une valeur hexadécimale. Quelle est cette valeur en binaire ?

_____

Étape 5 : redémarrage du routeur

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

```
rommon 3 > reset
```

À cause de la nouvelle valeur du registre de configuration, le routeur ne charge pas le fichier de configuration. Après redémarrage, le système demande :

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

b. Entrez **no** et appuyez sur **Entrée**.

Étape 6 : passage en mode d'exécution privilégié puis consultation et changement des mots de passe

Le routeur fonctionne sans fichier de configuration.

a. À l'invite du mode utilisateur `Router>`, entrez **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. L'utilisateur étant déjà en mode d'exécution privilégié, aucun mot de passe n'est nécessaire.

c. Saisissez **show running-config** pour afficher les détails de la configuration. Notez que tous les mots de passe sont affichés.

Quelles sont les deux mesures pouvant être prises pour que les mots de passe ne soient pas lisibles ?

_____

_____

d. Si les mots de passe ne sont pas lisibles, ils peuvent être changés. Saisissez **configure terminal** pour passer en mode de configuration globale.

e. Dans ce mode, utilisez ces commandes pour modifier les mots de passe :

```
FC-CPE-1(config)#enable password cisco
FC-CPE-1(config)#line console 0
FC-CPE-1(config-line)#password console
FC-CPE-1(config-line)#login
FC-CPE-1(config-line)#line vty 0 4
FC-CPE-1(config-line)#password telnet
FC-CPE-1(config-line)#login
```

Étape 7 : modification du paramètre du registre de configuration pour démarrer et charger le fichier de configuration

a. Le formateur vous fournit la valeur originale du registre de configuration, qui est vraisemblablement 0x2101. Toujours en mode de configuration globale, saisissez **config-register 0x2101** (ou la valeur donnée par le formateur). Appuyez sur **Entrée**.

```
FC-CPE-1(config)#config-register 0x2101
```

b. Utilisez la combinaison **Ctrl+z** pour retourner en mode d'exécution privilégié.

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

d. Avant de redémarrer le routeur, vérifiez la nouvelle valeur du registre de configuration. À l'invite du mode d'exécution privilégié, entrez la commande **show version** et appuyez sur **Entrée**.

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

```
Configuration register is 0x2142 (will be 0x2101 at next reload).
```

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

Étape 8 : vérification du nouveau mot de passe et de la nouvelle configuration

a. Lors du rechargement du routeur, connectez-vous et changez de mode au moyen des nouveaux mots de passe.

b. Utilisez la commande **no shutdown** dans l'interface fa0/0 pour activer l'interface et lui attribuer l'état « en fonction ».

FC-CPE-1(config-if)# **no shutdown**

c. Enregistrez la configuration active dans la configuration de démarrage.

FC-CPE-1# **copy run start**

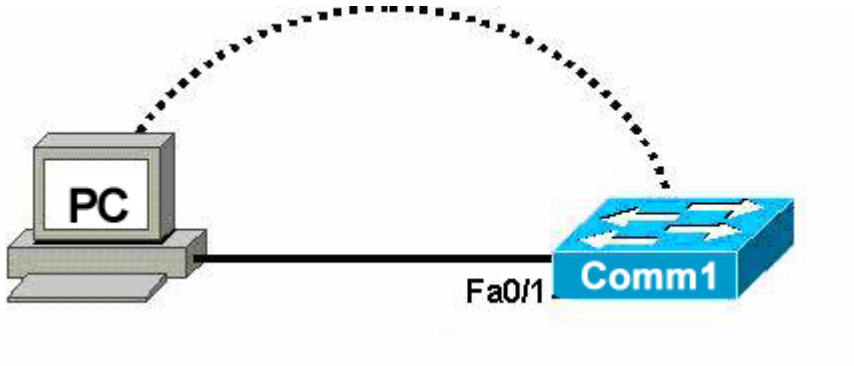
d. Déconnectez le câble console et accédez au routeur au moyen de Telnet en utilisant la ligne de commande du PC.

Les mots de passe nouvellement configurés permettent la connexion.

Étape 9 : remise en état

Effacez les configurations et redémarrez le routeur. Déconnectez et rangez le câblage. Pour les PC hôtes habituellement connectés à d'autres réseaux (comme le réseau local de l'établissement ou Internet), reconnectez le câblage approprié et restaurez les paramètres TCP/IP.

Topologie 2



Désignation du périphérique	Nom du périphérique	Adresse IP	Masque de sous-réseau
Comm1	FC-ASW-1	10.0.0.2	255.255.255.0
PC	PC1	10.0.0.254	255.255.255.0

Contexte / Préparation

Cette tâche démontre qu'un accès physique est nécessaire pour accéder au mot de passe des commutateurs Cisco et pour le modifier, et de nouveau pourquoi il est extrêmement important que les routeurs et les commutateurs possèdent également une sécurité physique pour empêcher tout accès non autorisé.

Après des tentatives de connexion à distance infructueuses, une connexion console est établie et les principes suivants sont appliqués au processus d'accès et de modification des mots de passe d'un commutateur :

- Les mots de passe du commutateur se trouvent dans le fichier de configuration appelé **config.txt** qui est stocké dans la mémoire flash. La séquence d'amorçage est modifiée afin qu'elle débute sans charger la configuration.
- Pendant l'exécution sans que la configuration ne soit chargée, le commutateur peut être reconfiguré à l'aide de nouveaux mots de passe connus.

Tâche 2 : accès aux mots de passe du commutateur et modification

Étape 1 : tentative de connexion au commutateur

REMARQUE : si le PC utilisé pour ces travaux pratiques est également connecté au réseau local de votre établissement ou à Internet, assurez-vous de bien noter les raccordements de câbles et les paramètres TCP/IP afin que ceux-ci puissent être rétablis à la fin des travaux pratiques.

a. En vous référant à la topologie 2, connectez le port Ethernet de la carte réseau du PC hôte au port Ethernet Fa0/1 du commutateur au moyen d'un câble droit. Assurez-vous que l'ordinateur hôte et le commutateur sont tous les deux sous tension.

b. En utilisant la topologie préconfigurée, essayez d'établir une connexion Telnet au routeur au moyen de la ligne de commande du PC.

Quelle adresse IP utilisez-vous pour établir la connexion Telnet au routeur ? _____

Qu'affiche le message du jour ?

_____

_____

Quel est le nombre de tentatives de connexion autorisées ? _____

Quel message s'affiche pour indiquer l'échec de tentatives de connexion ?

_____

c. Quand la tentative de connexion à distance échoue, établissez une connexion physique directe au routeur en effectuant les raccordements de console nécessaires entre le PC et le commutateur. Ouvrez ensuite une session de terminal au moyen de HyperTerminal ou TeraTerm.

Qu'affiche le message du jour ?

_____

_____

Essayez de vous connecter en devinant le mot de passe.

Quel est le nombre de tentatives de connexion autorisées ? _____

Quel message s'affiche pour indiquer l'échec de tentatives de connexion ?

_____

Pour empêcher le chargement de la configuration, le fichier **config.txt** est renommé afin que l'IOS du commutateur ne puisse pas localiser et charger de fichier de configuration valide. Pour renommer le fichier, le processus d'amorçage doit être interrompu pour permettre d'effectuer les modifications dans le mode « **`switch:`** ».

Étape 2 : passage en mode `switch:`

a. Mettez le commutateur hors tension.

b. Localisez le bouton MODE situé sur la face avant du commutateur.

c. Maintenez ce bouton enfoncé pendant que vous mettez le commutateur sous tension. Relâchez le bouton MODE au bout de 10 secondes.

Des informations similaires à celles-ci devraient s'afficher :

```
Base ethernet MAC Address: 00:0a:b7:72:2b:40
Xmodem file system is available.
The password-recovery mechanism is enabled.

The system has been interrupted prior to initializing the
flash files system. The following commands will initialize
the flash files system, and finish loading the operating
system software:

flash_init
load_helper
boot

switch:
```

d. Pour initialiser le système de fichiers et finir de charger le système d'exploitation, saisissez les commandes suivantes à l'invite « `switch:` » :

```
switch: flash_init
switch: load_helper
```

e. Pour afficher le contenu de la mémoire Flash, saisissez **`dir flash:`** à l'invite « `switch:` ».

```
switch: dir flash:
```

REMARQUE : n'oubliez pas de taper les deux points (:) après le mot « flash » dans la commande **`dir flash:`**

Le fichier **`config.txt`** doit apparaître dans la liste.

f. Tapez **`rename flash:config.text flash:config.old`** pour renommer le fichier de configuration. Ce fichier contient les définitions de mots de passe.

g. Saisissez **`dir flash:`** à l'invite « `switch:` » pour afficher le changement de nom.

```
switch: dir flash:
```

Étape 3 : redémarrage du commutateur

a. Entrez **`boot`** pour redémarrer le commutateur.

```
switch: boot
```

Il n'est pas possible de localiser le fichier de configuration **config.txt**. Le commutateur démarre donc en mode Configuration.

b. Voulez-vous terminer autoinstall ? [Yes]: **Y**

c. **`Would you like to enter the initial configuration dialog? [yes/no] N`**

```
Switch>
```

Étape 4 : passage en mode d'exécution privilégié puis consultation et changement des mots de passe

Le commutateur fonctionne sans fichier de configuration.

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

b. Tapez **`rename flash:config.old flash:config.text`** pour redonner son nom d'origine au fichier de configuration.

```
Switch#rename flash:config.old flash:config.text
Destination filename [config.text]?
Press Enter to confirm file name change.
```

c. Copiez le fichier de configuration dans la mémoire RAM.

```
Switch#copy flash:config.text system:running-config
Destination filename [running-config]?
Press Enter to confirm file name.
```

d. Il faut appuyer sur **Entrée** pour accepter les noms de fichier par défaut.

```
Source filename [config.text]?
Destination filename [running-config]
```

Le fichier de configuration est à présent chargé.

e. Saisissez **show running-config** pour afficher les détails de la configuration. Notez que tous les mots de passe sont affichés.

Quelles sont les deux mesures pouvant être prises pour que les mots de passe ne soient pas lisibles ?

_____

_____

f. Si les mots de passe ne sont pas lisibles, ils peuvent être changés. Saisissez **configure terminal** pour passer en mode de configuration globale.

g. Modifier les mots de passe inconnus.

```
FC-ASW-1#configure terminal
FC-ASW-1(config)#enable password cisco
FC-ASW-1(config)#line console 0
FC-ASW-1(config-line)#password console
FC-ASW-1(config-line)#line vty 0 15
FC-ASW-1(config-line)#password telnet
FC-ASW-1(config-line)#exit
FC-ASW-1(config)#exit
```

Étape 5 : enregistrement du fichier de configuration

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

```
FC-ASW-1#copy running-config startup-config
Destination filename [startup-config]?[enter]
Building configuration...
[OK]
FC-ASW-1#
```

Étape 6 : vérification du nouveau mot de passe et de la nouvelle configuration

Mettez le commutateur hors tension puis sous tension et vérifiez que les mots de passe sont maintenant opérationnels.

Étape 7 : remise en état

Effacez les configurations et redémarrez le commutateur. Déconnectez et rangez le câblage. Pour les PC hôtes habituellement connectés à d'autres réseaux (comme le réseau local de l'établissement ou Internet), reconnectez le câblage approprié et restaurez les paramètres TCP/IP.

Tâche 3 : remarques générales

Examinez les différentes méthodes de sécurisation de l'accès physique aux périphériques réseau comme les routeurs et les commutateurs. Expliquez comment seules les personnes qui demandent accès peuvent être identifiées et comment cette sécurité peut être mise en œuvre.

_____

_____

_____

_____

_____

REMARQUE : il est important de se souvenir que les mots de passe utilisés dans ces travaux pratiques (console, cisco, class, Telnet) ne le sont que pour des raisons pratiques. Il ne s'agit *pas* de mots de passe sécurisés qui pourraient être utilisé dans les réseaux de production.