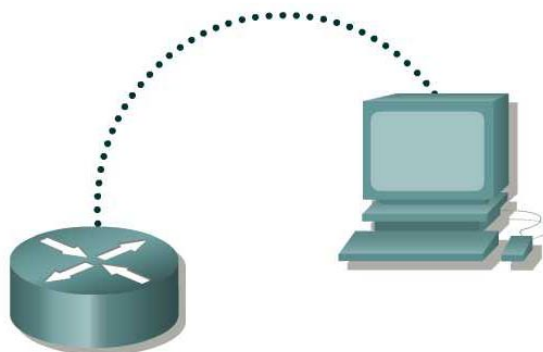


Práctica de laboratorio 5.2.6a Procedimientos de recuperación de la contraseña



Designación del router	Nombre del router	Contraseña enable secret	Contraseñas enable/VTY y de Consola
Router 1	GAD	clase	cisco

Cable de conexión directa	—————
Cable serial	—————  —————
Cable de consola (transpuesto)
Cable de conexión cruzada	- - - - -

Objetivo

- Iniciar una sesión en un router cuya contraseña del modo privilegiado (enable) es desconocida.

Información básica / Preparación

Esta práctica de laboratorio demuestra cómo obtener acceso a un router cuya contraseña del modo privilegiado (enable) es desconocida. Es importante aclarar que cualquiera que conozca este procedimiento y pueda acceder a un puerto de consola de un router puede cambiar la contraseña y asumir el control del router. Por este motivo es de importancia fundamental que los routers también tengan la seguridad física para evitar el acceso no autorizado.

Establezca una red similar a la del diagrama anterior. Se puede usar cualquier router que cumpla con los requisitos de interfaz. Entre las posibles opciones están los routers 800, 1600, 1700, 2500, 2600 o una combinación de los mismos. Consulte la tabla al final de esta práctica de laboratorio para identificar correctamente los identificadores de interfaz que se deben usar según el equipo disponible en el laboratorio. Los resultados de la configuración utilizados en esta práctica se obtuvieron con routers serie 1721. El uso de cualquier otro router puede producir unos resultados ligeramente distintos.

Iniciar una sesión de HyperTerminal tal como se realizó en la práctica de laboratorio Establecer una sesión de HyperTerminal.

Nota: Configure el nombre de usuario y la contraseña en el router. Pida a un instructor, a un asistente de laboratorio o a otro estudiante que configure una configuración básica con una contraseña enable secret. Introduzca `copy running-config startup-config` y vuelva a cargar el router.

Nota: Hilgraeve desarrolló la versión de HyperTerminal proporcionada con Windows 95, 98, NT y 2000 para Microsoft. Es posible que algunas versiones no emitan una secuencia de pausa como se requiere para la técnica de recuperación de la contraseña del router Cisco. Si este es el caso, instale la versión HyperTerminal Private Edition (PE), disponible de forma gratuita para su uso personal y educacional. El programa puede descargarse en <http://www.hilgraeve.com>.

Paso 1 Intentar iniciar una sesión en el router

- Haga las conexiones de consola necesarias y establezca una sesión de HyperTerminal con el router. Intente conectarse al router mediante la contraseña enable **cisco**. El resultado debe ser similar al siguiente:

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

Router>
```

Paso 2 Anote los valores actuales del registro de la configuración

- En la petición de entrada de EXEC del usuario escriba `show version`.
- Anote el valor que aparece para el registro de configuración _____. Por ejemplo 0x2102.

Paso 3 Entrar al modo de Monitor de ROM

- Apague el router, espere unos segundos y vuelva a encenderlo. Cuando el router empieza a mostrar "System Bootstrap, Version ..." en la pantalla de HyperTerminal, presione la tecla **Ctrl** y la tecla **Pausa** al mismo tiempo. El router arranca en el modo de monitor ROM. Según el hardware del router, pueden aparecer una de varias peticiones de entrada, como: "**rommon 1** >" o simplemente ">".

Paso 4 Examinar el modo de ayuda del Monitor de ROM

- Escriba `?` en la petición de entrada. El resultado deberá ser similar a esto:

```
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
tftpdownload  tftp image download
```

Paso 5 Cambiar los valores del registro de configuración para arrancar sin cargar el archivo de configuración

- Desde el modo de Monitor ROM, escriba **confreg 0x2142** para cambiar el registro de configuración (config-register).

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

Paso 6 Reiniciar el router

- Desde el modo Monitor ROM, escriba **reset** o reinicie el router.

```
rommon 2 >reset
```

- Debido a los nuevos valores de registro de configuración, el router no carga el archivo de configuración. El sistema pregunta:

"Would you like to enter the initial configuration dialog? [yes]:"

Introduzca **no** y presione **Intro**.

Paso 7 Entrar al modo EXEC privilegiado y cambiar la contraseña

- Ahora, en la petición de entrada del modo de usuario Router>, escriba **enable** y presione **Intro** para ir al modo privilegiado sin contraseña.
- Use el comando **copy startup-config running-config** para restaurar la configuración existente. Como el usuario ya se encuentra en el modo EXEC privilegiado, no hace falta una contraseña.
- Escriba **configure terminal** para entrar al modo de configuración global.
- En el modo de configuración global escriba **enable secret class** para cambiar la contraseña secret.
- Mientras se encuentra en el modo de configuración global, escriba **config-register xxxxxxxx**. xxxxxxxx es el valor de registro de configuración original que se anotó en el Paso 2. Presione **Intro**.
- Use la combinación de **Ctrl z** para volver al modo EXEC privilegiado.
- Use el comando **copy running-config startup-config** para guardar la nueva configuración.
- Antes de reiniciar el router, verifique los nuevos valores de configuración. Desde el modo EXEC privilegiado, introduzca el comando **show version** y presione **Intro**.
- Verifique que la última línea del resultado diga:
Configuration register is 0x2142 (will be 0x2102 at next reload).
- Use el comando **reload** para rearrancar el router.

Paso 8 Verificar la nueva contraseña y configuración

- Cuando se vuelve a cargar el router la contraseña debe ser **class**.

Al completar los pasos anteriores, desconéctese escribiendo **exit**. Apague el router.

Borrar y recargar el router

Entre al modo EXEC privilegiado escribiendo **enable**.

```
Router>enable
```

Si pide una contraseña, introduzca **class**. Si “class” no funciona, pide ayuda a su instructor.

En el modo EXEC privilegiado, introduzca el comando **erase startup-config**.

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

Como respuesta, aparecerá la siguiente petición de entrada:

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

Presione **Intro** para confirmar.

La respuesta deberá ser:

```
Erase of nvram: complete
```

En el modo EXEC privilegiado, introduzca el comando **reload**.

```
Router#reload
```

Como respuesta, aparecerá la siguiente petición de entrada:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

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

Presione **Intro** para confirmar.

La primera línea de la respuesta será:

```
Reload requested by console.
```

La siguiente petición de entrada aparecerá después de que el router se recargue:

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

Escriba **n** y luego presione **Intro**.

Como respuesta, aparecerá la siguiente petición de entrada:

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

Presione **Intro**.

El router está listo para iniciar la práctica de laboratorio asignada.

Resumen de la interfaz del router					
Modelo de router	Interfaz Ethernet 1	Interfaz Ethernet 2	Interfaz serial 1	Interfaz serial 2	Interfaz 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)	

Para conocer la configuración exacta del router, consulte las interfaces. Esto le permitirá identificar el tipo de router así como cuántas interfaces posee el router. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. Lo que se ha presentado son los identificadores de las posibles combinaciones de interfaces en el dispositivo. Esta tabla de interfaces no incluye ningún otro tipo de interfaz aunque otro tipo pueda existir en un router dado. La interfaz BRI RDSI es un ejemplo de esto. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando IOS para representar la interfaz.