

Recuperación de contraseñas para Routers y Switches Cisco.

Por Paulo Colomés – 2010

Este tutorial se basa en los Routers 1700/1800 y los Switches Catalyst 2950/2960

Recuperación de contraseñas de un Router

1. Conectarse vía terminal (consola) al Router
2. Reiniciar el Router con el botón de apagado (Generalmente ubicado en la parte trasera)
3. Mientras el IOS se carga en la RAM (Que es cuando aparecen los hash ####... en pantalla) se debe iniciar la secuencia de detención (Break). Esta secuencia depende del tipo de terminal que se esté utilizando. Para PuTTY, la secuencia por defecto es [CTRL] + [PAUSE]
4. Si todo ha salido bien, cuando termine la carga del IOS se accederá al Monitor de ROM (ROM Monitor) y debería aparecer el prompt “rommon>”
5. Cambiar la configuración de registro a 0x2142 con el comando **confreg 0x2142**.

Rommon> confreg 0x2142

No se olvide que en los Routers Cisco el modo “normal” de funcionamiento se establece cuando el valor de configuración de registro es 0x2102. Al cambiar este valor a 0x2142 le estamos diciendo al dispositivo que iniciaremos el proceso de recuperación.

6. Reinicie con el comando **reload** o **reset**
7. Mientras el sistema arranca ignorará el startup-config, por lo tanto el router se iniciará como si no existiese configuración alguna. Debe responder NO a cualquier pregunta de autoconfiguración.
8. Una vez que haya arrancado el sistema se mostrará el prompt Router>
9. Ir al modo EXEC privilegiado con el comando **enable**. NO debería pedir contraseña
10. En este punto se puede cargar la configuración previa ejecutando el comando **copy startup-config running-config**. Tenga cuidado que NO es running-config startup-config, ya que en este caso queremos cargar la configuración DESDE el startup-config hacia la RAM (running-config)
11. Cambie o elimine cualquier contraseña de la configuración. Revise con **show running-config**. Si desea borrar la contraseña de la consola, ejecute:
Router(Config)# line console 0
Router(Config-line) no password
Router(Config-line) end
Router#copy running-config startup-config

Elimine además la password de enable:

Router(config)# no enable password

Ó

Router(config)# no enable secret

12. Vuelva a establecer el registro de configuración en modo normal. Recuerde que hasta este punto estamos con 0x2142.

Router(config)# config-register 0x2102

13. Reinicie con **reload**

Recuperación de contraseñas para Catalyst 2950 y Catalyst 2960

1. Presione el botón MODE ubicado en el panel delantero del switch y manténgalo así mientras desconecta el cable de poder y lo vuelve a conectar.
2. Suelte el botón MODE después de 15 segundos
3. El LED SYST debería parpadear de color ámbar (Naranja – amarillo)
4. Se ingresará al Monitor ROM y verá el prompt **switch:**
5. Escriba los siguientes comandos en el mismo orden:
flash_init
load_helper
dir flash:
rename config.text config.respaldo
boot
6. El sistema booteará y no encontrará el archivo de arranque en la NVRAM (el config.text) ya que lo hemos renombrado a config.respaldo.
7. Una vez que haya ingresado en el sistema nuevamente ejecute
rename:config.respaldo flash:config.text
copy flash:config.text nvram:startup-config
copy startup-config running-config
8. Cambie o las contraseñas de telnet, consola, líneas VTY, enable
9. Guarde los cambios
Copy running-config startup-config
10. Reinicie
reload