Práctica de laboratorio: Administración de los archivos de configuración del router con software de emulación de terminal (versión para el instructor)

**Nota para el instructor**: El color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

1. Topología



1. Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/D |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

1. Objetivos

Parte 1: Configurar los parámetros básicos de los dispositivos

Parte 2: Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

Parte 3: Utilizar un archivo de configuración de respaldo para restaurar un router

1. Aspectos básicos/situación

Se recomienda mantener archivos de configuración de respaldo de routers y switches en caso de que sea necesario restaurar una configuración anterior. El software de emulación de terminal puede utilizarse para realizar una copia de respaldo o para restaurar fácilmente un archivo de configuración de router o switch.

En esta práctica de laboratorio, utilizará Tera Term para hacer una copia de respaldo de un archivo de configuración en ejecución del router, eliminar el archivo de configuración de inicio del router, volver a cargar el router y, luego, restaurar la configuración del router faltante a partir del archivo de configuración de respaldo.

**Nota**: Los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces de router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

**Nota para el instructor**: Consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

**Nota para el instructor**: En esta práctica de laboratorio, se utiliza Tera Term 4.75. Se debe instalar Tera Term en la PC antes de comenzar la práctica de laboratorio. Puede descargar la versión más reciente de diversos sitios de Internet. Simplemente, busque una descarga de Tera Term.

1. Recursos necesarios

* 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
* 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
* 1 PC (Windows 7 u 8 con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet, como se muestra en la topología

1. Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de las interfaces, el acceso de los dispositivos y las contraseñas del router.

* 1. Realizar el cableado de red tal como se muestra en la topología.

Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.

* 1. Configurar los parámetros de red de la PC-A según la tabla de direccionamiento.
  2. Iniciar y volver a cargar el router y el switch.
  3. Configurar el router.
     1. Acceda al router e ingrese al modo de configuración global.
     2. Establezca R1 como nombre del router.
     3. Desactive la búsqueda DNS.
     4. Use **class** como la contraseña cifrada de EXEC privilegiado.
     5. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
     6. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
     7. Cifre las contraseñas de texto sin formato.
     8. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.
     9. Configure y active la interfaz G0/1 en el router utilizando la información de la tabla de direccionamiento.
     10. Guarde la configuración en ejecución en el archivo de configuración de inicio.

1. Utilizar software de emulación de terminal para crear un archivo de configuración de respaldo

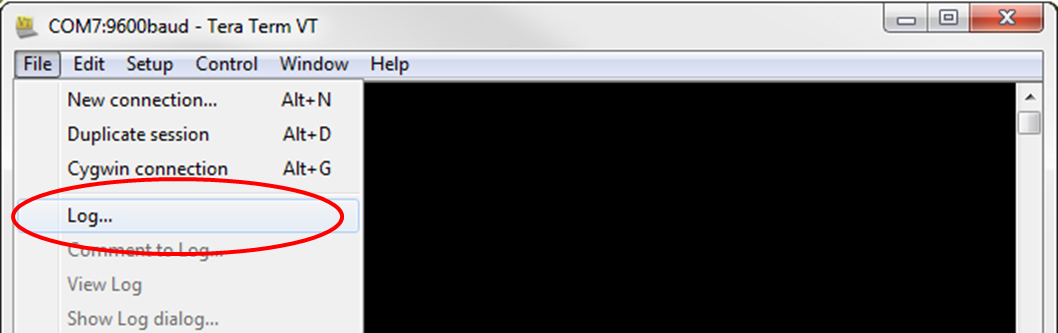
En la parte 2, utilizará Tera Term como software de emulación de terminal. Si usa otros programas de emulación de terminal, el procedimiento será diferente.

* 1. Establecer una sesión de consola de Tera Term con el router.
     1. Inicie el programa Tera Term y, en la ventana New Connection (Conexión nueva), seleccione el botón de opción **Serial** y el puerto de comunicaciones apropiado para su PC (es decir, COM7).

**Nota**: Si no está instalado en la PC, Tera Term se puede descargar del siguiente enlace seleccionando **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

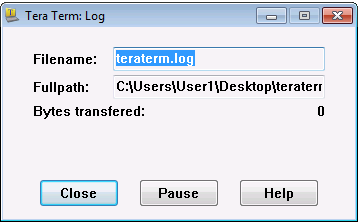
* + 1. En Tera Term, presione Intro para conectarse al router.
    2. En el menú **File** (Archivo), seleccione **Log...** (Registro...) y guarde el archivo **teraterm.log** en el escritorio. Asegúrese de que las casillas de verificación **Append** (Anexar) y **Plain text** (Texto sin formato) estén activadas (marcadas).



* + 1. El archivo de registro de Tera Term creará un registro de cada comando emitido y de cada resultado que se muestra.

**Nota**: Puede utilizar esta característica para capturar el resultado de varios comandos en secuencia y utilizarlo para fines de registro de la red. Por ejemplo, podría emitir los comandos **show version**, **show ip interface brief** y **show running-config** para capturar información sobre el router.

* 1. Mostrar la configuración en ejecución del router.
     1. Ejecute el comando **show running-config**.
     2. Continúe presionando la barra espaciadora cuando se muestre **--More--** (Más), hasta que vuelva a ver el símbolo del sistema R1# del router.
     3. Haga clic en el ícono **Tera Term: Log** (Tera Term: registro) en la barra de tareas. Haga clic en **Close** (Cerrar) para finalizar la sesión de registro.



**Nota**: También puede copiar el texto de la ventana de Tera Term y pegarlo directamente en un editor de texto.

1. Utilizar un archivo de configuración de respaldo para restaurar un router
   1. Borrar la configuración inicial y volver a cargar el router.
      1. En el modo EXEC privilegiado, elimine la configuración de inicio.

R1# **erase startup-config**

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

[OK]

Erase of nvram: complete

* + 1. Recargue el router.

R1# **reload**

Proceed with reload? [confirm]

* + 1. En el mensaje System Configuration Dialog (Cuadro de diálogo de configuración del sistema), escriba **no**. Aparecerá un aviso del router, que indica que hay un router sin configurar.

--- System Configuration Dialog ---

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

Press RETURN to get started!

<resultado omitido>

Router>

* + 1. Ingrese al modo EXEC privilegiado e introduzca el comando **show running-config** para verificar que todas las configuraciones anteriores se hayan borrado.
  1. Editar la copia de respaldo de la configuración guardada.

Para restaurar la configuración del router desde un archivo de configuración en ejecución de respaldo guardado, debe editar el texto.

* + 1. Abra el archivo de texto **teraterm.log**.
    2. Elimine cada instancia de **--More--** en el archivo de texto.

**Nota**: **--More--** se genera al presionar la barra espaciadora mientras se muestra la configuración en ejecución.

* + 1. Elimine las líneas iniciales del archivo de configuración de respaldo, de modo que la primera línea comience con el primer comando de configuración.

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

* + 1. Reemplace la contraseña secreta cifrada.

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

Cambiar a:

enable secret class

* + 1. En las líneas para la interfaz GigabitEthernet0/1, inserte una línea nueva para habilitar la interfaz.

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

Cambiar a:

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

**no shutdown**

* + 1. Cambie la configuración del anuncio del mensaje del día (MOTD) de modo que se inserten caracteres delimitadores como si introdujera el comando en la línea de comandos.

banner motd ^C Unauthorized Access is Prohibited! ^C

Cambiar a:

banner motd “ Unauthorized Access is Prohibited! “

* + 1. En las secciones line con 0 y vty 0 4, reemplace la contraseña cifrada.

line con 0

password 7 104D000A0618

line vty 0 4

password 7 104D000A0618

Cambiar a:

line con 0

password cisco

line vty 0 4

password cisco

* + 1. Después de realizar todas las ediciones al archivo de configuración de respaldo, guarde los cambios con el nombre de archivo **R1-config-backup**.

**Nota**: Cuando guarde el archivo, puede agregarse automáticamente una extensión, como **.txt**, al nombre del archivo.

* 1. Restaurar la configuración del router.

Puede restaurar la configuración en ejecución editada directamente en el terminal de consola en el modo de configuración global del router. Las configuraciones se introducen como si fueran comandos introducidos individualmente en el símbolo del sistema.

* + 1. Ingrese al modo de configuración global desde la conexión de consola de Tera Term al router.
    2. En el menú **File** (Archivo), seleccione **Send file...** (Enviar archivo).
    3. Localice **R1-config-backup** y seleccione **Open** (Abrir).
    4. Guarde la configuración en ejecución en el archivo de configuración de inicio.

R1# **copy running-config startup-config**

* + 1. Verifique la nueva configuración en ejecución.

1. Hacer una copia de respaldo y restaurar el switch (opcional)

En la parte 4, practicará el procedimiento para realizar una copia de respaldo y restaurar un switch mediante el mismo procedimiento que se usa para un router. Creará un archivo de configuración básica del switch. Realizará una copia de respaldo y restaurará el archivo de configuración para el switch mediante un software de emulación de terminal.

* 1. Configurar los parámetros básicos del switch.
     1. Acceda al switch e ingrese al modo de configuración global.
     2. Establezca S1 como nombre del switch.
     3. Desactive la búsqueda DNS.
     4. Use **class** como la contraseña cifrada de EXEC privilegiado.
     5. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
     6. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
     7. Cifre las contraseñas de texto sin formato.
     8. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.
     9. Configure la interfaz de administración predeterminada SVI con la información de dirección IP incluida en la tabla de direccionamiento.
     10. Configure el gateway predeterminado del switch.
     11. Guarde la configuración en ejecución en el archivo de configuración de inicio.
  2. Hacer una copia de respaldo del switch.
     1. Establezca una sesión de consola de Tera Term con el switch, según sea necesario.
     2. Inicie un archivo de registro con Tera Term y guárdelo en el escritorio.
     3. Ingrese al modo EXEC privilegiado del switch e introduzca el comando **show running-config**.
     4. Cuando aparezca la configuración en ejecución completa, finalice la sesión de registro.
  3. Borrar y volver a cargar el switch.
     1. En el modo EXEC privilegiado, elimine la configuración de inicio.

S1# **erase startup-config**

* + 1. Vuelva a cargar el switch.
    2. En el mensaje System Configuration Dialog, escriba **no** para salir del diálogo de configuración inicial.
    3. Verifique que se hayan eliminado todas las configuraciones anteriores.
  1. Editar el archivo de copia de respaldo de la configuración guardado.
     1. Abra el archivo de texto de copia de respaldo de la configuración guardado.
     2. Reemplace la contraseña secreta cifrada por una contraseña no cifrada.
     3. Active los puertos de switch adecuados para establecer la conectividad en la red.
     4. Elimine cada instancia de **--More--** en el archivo de texto.
     5. Elimine las líneas iniciales del archivo de configuración de respaldo, de modo que la primera línea comience con el primer comando de configuración.
     6. Reemplace los caracteres delimitadores en la configuración del aviso del mensaje del día (MOTD).
     7. Después de realizar todas las ediciones al archivo de configuración de respaldo, guarde los cambios con el nombre de archivo **S1-config-backup**.

**Nota**: Cuando guarde el archivo, puede agregarse automáticamente una extensión, como **.txt**, al nombre del archivo.

* 1. Restaurar la configuración del switch.
     1. Ingrese al modo de configuración global desde la conexión de consola de Tera Term al router.
     2. En el menú **File** (Archivo), seleccione **Send file...** (Enviar archivo).
     3. Localice **S1-config-backup** y seleccione **Open** (Abrir).
     4. Guarde la configuración en ejecución en el archivo de configuración de inicio.

R1# **copy running-config startup-config**

* + 1. Verifique la nueva configuración en ejecución.

1. Reflexión

¿Por qué cree que es importante utilizar un editor de texto en lugar de un procesador de textos para copiar y guardar las configuraciones de los comandos?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Un procesador de textos posiblemente añada caracteres de control especiales al texto, lo que dificultaría su uso para restaurar el router.

1. Tabla de resumen de interfaces de router

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resumen de interfaces de router | | | | |
| Modelo de router | Interfaz Ethernet 1 | Interfaz Ethernet 2 | Interfaz serial 1 | Interfaz serial 2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Nota**: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS Cisco para representar la interfaz. | | | | |

1. Configuración de dispositivos: final
2. Router R1

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

!

no ipv6 cef

!

no ip domain lookup

ip cef

multilink bundle-name authenticated

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

no ip address

shutdown

clock rate 2000000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!

banner motd ^C Unauthorized Access is Prohibited! ^C

!

line con 0

password 7 104D000A0618

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 104D000A0618

login

transport input all

!

scheduler allocate 20000 1000

!

end

1. Switch S1

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.11 255.255.255.0

!

ip default-gateway 192.168.1.1

ip http server

ip http secure-server

banner motd ^C Unauthorized access is prohibited! ^C

!

line con 0

password 7 070C285F4D06

login

line vty 0 4

password 7 070C285F4D06

login

line vty 5 15

login

!

end