Lab – Managing Router Configuration Files with Terminal Emulation Software (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
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

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: This lab uses Tera Term 4.75. Tera Term should be installed on the PC prior to starting the lab. You can download the latest version from a number of Internet sites. Simply search for a tera term download.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology and cable as necessary.

Step 2: Configure the PC-A network settings according to the Addressing Table.

Step 3: Initialize and reload the router and switch.

Step 4: Configure the router.

a. Console into the router and enter global configuration mode.

b. Set the router name to R1.

c. Disable DNS lookup.

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the vty password and enable login.

g. Encrypt the plain text passwords.

h. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

i. Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.

j. Save the running configuration to the startup configuration file.

Step 5: Configure the switch.

a. Console into the switch and enter into global configuration mode.

b. Set the switch name to S1.

c. Disable DNS lookup.

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the vty password and enable login.

g. Encrypt the plain text passwords.

h. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

i. Configure the default SVI management interface with the IP address information contained in the Addressing Table.

j. Configure the switch default gateway.

k. Save the running configuration to the startup configuration file.

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

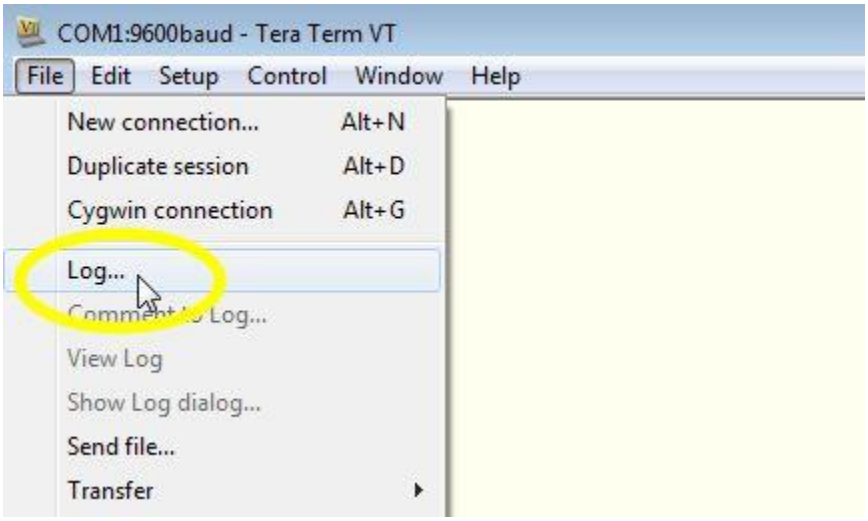
Step 1: Establish a Tera Term console session to the router.

Launch the Tera Term Program, and in the New Connection window, select the **Serial** radio button and the appropriate communications port for your PC (i.e., COM1).

Note: If Tera Term is not installed, you can download the latest version from a number of Internet sites. Simply search for a Tera Term download.

a. In Tera Term, press Enter to connect to the router.

b. From the **File** menu, choose **Log…**, and save the **teraterm.log** file to the Desktop. Ensure that the **Append** and **Plain text** check boxes are enabled (checked).



c. The Tera Term log file will create a record of every command issued and every output displayed.

Note: You can use this feature to capture the output from several commands in sequence and use it for network documentation purposes. For example, you could issue the **show version**, **show ip interface brief**, and **show running-config** commands to capture information about the router.

Step 2: Display the router running-configuration.

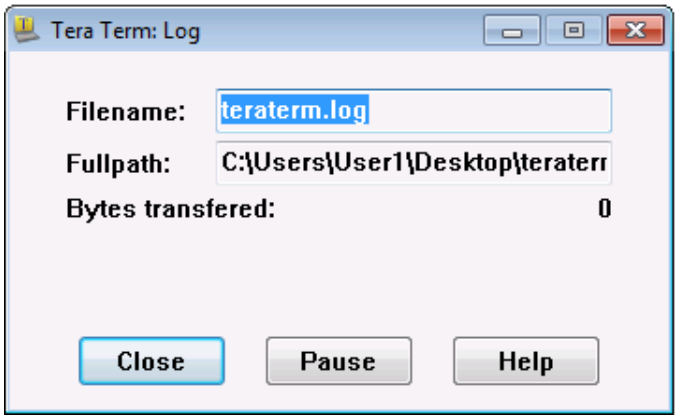
a. Use the console password to log in to the router.

b. Enter privileged EXEC mode.

c. Enter the **show running-config** command.

d. Continue pressing the space bar when **--More--** is displayed until you see the router R1# prompt return.

e. Click the **Tera Term: Log** icon on the Task bar. Click **Close** to end log session.



Note: You can also copy and paste the text from the Tera Term window directly into a text editor.

Part 3: Use a Backup Configuration File to Restore a Router

Step 1: Erase the router startup-configuration and reload.

a. From privileged EXEC mode erase the startup configuration.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

b. Reload the router.

```
R1# reload
Proceed with reload? [confirm]
```

c. At the System Configuration Dialog prompt, type **no**; a router prompt displays, indicating an unconfigured router.

```
         --- System Configuration Dialog ---

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

Press RETURN to get started!
<output omitted>
Router>
```

d. Enter privileged EXEC mode and enter a **show running-config** command to verify that all of the previous configurations were erased.

Step 2: Edit the saved configuration backup file to prepare it for restoring the router configuration.

To restore the router configuration from a saved running configuration backup file, you must edit the text.

a. Open the **teraterm.log** text file.

b. Remove each instance of **--More--** in the text file.

Note: The **--More--** was generated by pressing the Spacebar when displaying the running configuration.

c. Delete the initial lines of the backup configuration file, so that the first line starts with the first configuration command as shown below.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

d. Replace the encrypted secret password.

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

Change to:

```
enable secret class
```

e. In the lines for interface GigabitEthernet0/1, insert a new line to enable the interface.

```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

Change to:

```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
```

f. Change the message-of-the-day (MOTD) banner configuration to insert the delimiting characters as if you were entering the command at the command line.

```
banner motd ^C Unauthorized Access is Prohibited! ^C
```

Change to:

```
banner motd " Unauthorized Access is Prohibited! "
```

g. In line con 0 and vty 0 4 sections, replace the encrypted password.

```
line con 0
 password 7 104D000A0618
line vty 0 4
 password 7 104D000A0618
```

Change to:

```
line con 0
 password cisco
line vty 0 4
 password cisco
```

h. After you have made all of the edits to the backup configuration file, save your changes to filename, **R1-config-backup**.

Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

Step 3: Restore the router configuration.

You can restore the edited running configuration directly to the console terminal in router global configuration mode, and the configurations are entered as if they were commands entered individually at the command prompt.

a. From the Tera Term console connection to the router, enter global configuration mode.

b. From the **File** menu, select **Send file…**.

c. Locate **R1-config-backup** and select **Open**.

d. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
```

e. Verify the new running configuration.

Step 4: Back up and restore the switch.

Go back to the beginning of Part 2 and follow the same steps to backup and restore the switch configuration.

Reflection

Why do you think it is important to use a text editor instead of a word processor to copy and save your command configurations?

_____

_____

_____

A word processor could possibly add special control characters to the text making it difficult to use to restore the router.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #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)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs – Final

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
```

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
```