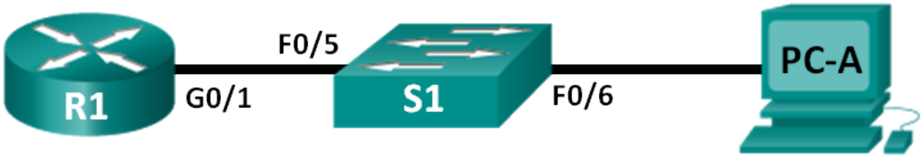
BOLIMA, DIMERO, GO, LIM, TALABAN Lab 6.4 – Device Remote Backup and Password Recovery - PT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.1.1	255.255.255.0	N/A
S1	VLAN 1	172.16.1.2	255.255.255.0	172.16.1.1
PCA	NIC	172.16.1.10	255.255.255.0	172.16.1.1

Objectives

Part 1: Configure Initial Device Settings

Part 2: Use TFTP to Restore and Backup the Router Running Configuration

Part 3: Use TFTP to Backup the Switch IOS

Part 4: Perform Password Recovery on a Router

Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup and load device configuration files and OS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

The enable password protects access to privileged EXEC and configuration mode on Cisco devices. In case of forgotten passwords, the enable password can be recovered, but the enable secret password is encrypted and will need to be replaced with a new password. Recovering from a forgotten device password requires familiarity with device ROMMON mode and the password recovery procedure of the device.

In this lab, you will use TFTP server software to perform backup and load device configuration as well as IOS images. You will also be practicing password recovery on a router to be familiar with the procedure.

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 with terminal emulation program and TFTP server software (such as TFTPd32)

- 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: Configure the router.

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

b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configure and activate the G0/0 interface on the router using the information contained in the Addressing Table.

Step 4: Configure the switch.

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

b. Configure the hostname of S1.

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

Part 2: Use TFTP to Backup and Restore Router Configuration

In Part 2, you will backup a configuration and later use it to restore device settings. Due to an equipment failure, a new router has been put in place. Fortunately, backup configuration files have been saved to a Trivial File Transfer Protocol (TFTP) Server. You are required to restore the files from the TFTP Server to get the router back online as quickly as possible.

Step 1: Establish Connectivity to the TFTP Server

Test connectivity to PC-A. Troubleshoot, if necessary.

Step 2: (Optional) Install TFTP server.

If a TFTP server is not already installed on the PC, download and install the latest version of a syslog server, such as Tftpd32, on PC-A. The latest version of Tftpd32 can be found at the following link:

http://tftpd32.jounin.net/

Step 3: Start the syslog service on the PC-A.

a. After starting the Tftpd32 application, click the **TFTP server** tab.

b. Set the server interface to 172.16.1.10

c. Examine the "Current Directory" setting of the service. This folder serves as the file repository of the TFTP service. All files uploaded to the server will be stored here; and all files stored here may also be downloaded from the server.

Step 4: Backup the Configuration File to the TFTP Server

a. Save the current configuration of R1 to its startup configuration.

```
R1# copy running-config startup-config
Destination filename [startup-config]? <cr>
Building configuration...
[OK]
```

b. Create a backup copy of the R1 startup config on the TFTP server. From privileged EXEC mode, issue the following command:

```
R1# copy startup-config tftp:
Source filename [startup-config]? <cr>
Address or name of remote host []? 172.16.1.10
Destination filename [startup-confg]? R1-backup
```

c. Verify that the backup file exists on PC-A by navigating to the Current Directory folder of its TFTP service and checking if a file named "R1-backup" is present. Open the file in notepad to confirm that it contains the configuration saved on R1 earlier.

Step 5: Restore Router Configuration from the TFTP Server.

a. Erase the startup configuration of R1. This mimics a scenario where the saved configuration of a device is accidentally deleted.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] <cr>
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

b. Verify that the router startup config is now empty.

```
R1# show startup-config
startup-config is not present
```

c. Copy the configuration to the TFTP Server using the copy command:

```
R1# copy tftp startup-config
Address or name of remote host []? 172.16.1.10
Source filename []? R1-backup
```

```
Destination filename [startup-config]? <cr>
```

The router should return the following:

```
Accessing tftp://172.16.1.10/R1-backup...
Loading R1-backup from 172.16.1.10: !
[OK - 785 bytes]
785 bytes copied in 0.001 secs
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
```

d. When the transfer completes, verify that the startup configuration is again present on the router (show startup-config).

Does R1 now have saved configurations again?	Yes

Part 3: Use TFTP to Backup the Switch IOS

A TFTP server can also help manage the storage of IOS images and revisions to IOS images. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image A TFTP server can also be used to store new upgrades to the IOS and then deployed throughout the network where it is needed.

In Part 3, you will backup the current IOS image of a switch with the use of a TFTP server.

Step 1: Verify Switch IOS version

Issue the **show version** command on **SW1** to check the current IOS version running on the switch.

```
SW1> show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Switch uptime is 39 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbasek9-mz.150-2.SE4.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K bytes of
memory.
```

The output will indicate the IOS version and boot image used by the device.

What is the filename of the IOS image on SW1?	c2960-lanbasek9-mz.150-2.SE4.bin

Step 2: Backup the Switch IOS to the TFTP Server

a. Backup the IOS in flash to the TFTP Server on PC-A using the following command:

```
SW1> enable
SW1# copy flash tftp:
Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin
Address or name of remote host []? 172.16.1.10
Destination filename [c2960-lanbasek9-mz.150-2.SE4.bin]? <cr>
```

*Note: Not all switch models use the same image file name. Use the filename acquired in Step 1

What special character repeatedly displays indicating that the IOS file is being copied to the TFTP server successfully?

The special character indicating that the IOS file is being copied by the TFTP server successfully is “!” respectively. When performing the command successfully, the screen is inputted with multiple “!”s such as “!!’.

b. Open the current directory of the TFTP server on PC-A

Has the IOS file been copied to PC-A?	yes

Part 4: Perform Password Recovery on a Router

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In Part 4, you will change the configuration register in order to reset the enable password on a Cisco router.

Step 5: Change router password settings.

a. Copy the following basic configuration and paste it to the running-configuration on **R1**.

```
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyML15/
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
end
write
```

```
exit
```

b. Press **Enter** and try to enable Privileged Exec mode.

As you can see, access to a Cisco IOS device is very limited if the enable password is unknown. It is important for a network engineer to be able to recover from an unknown enable password issue on a Cisco IOS device.

Step 2: Establish a Console Connection to the Router

Connect a console cable between PC-A and R1. Use PuTTY to open a console session with the R1 CLI.

Step 3: Reboot Router and Enter ROMMON

a. While still consoled into R1, reboot the router using its power switch to turn it off then on again.

b. Quickly return to the console session on PC-A and issue the keyboard break sequence (CTRL+Break) to interrupt the router's normal boot process and enter ROMMON mode.

```
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#######################
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Step 4: Reset the configuration register.

a. From the ROMMON prompt, type a **?**, then press **Enter**. This will display a list of available ROMMON commands. Look for the **confreg** command in this list.

```
rommon 1 > ?
boot                    boot up an external process
confreg                 configuration register utility
dir                     list files in file system
help                    monitor builtin command help
reset                   system reset
set                     display the monitor variables
tftpdnld                tftp image download
unset                   unset a monitor variablerommon 2 >
```

Note: The number at the end of the ROMMON prompt will increment by one each time a command is entered.

b. Type **confreg 0x2142** and press **Enter**. Changing the register to Hex 2142 tells the router not to automatically load the startup configuration when booting. The router will need to be rebooted for the configuration register change to take effect.

```
rommon 2 > confreg 0x2142

You must reset or power cycle for new config to take effect
rommon 3 >
```

c. Issue the **reset** ROMON command to reboot the router.

```
rommon 3 > reset
```

d. When asked if you would like to enter the initial configuration dialog, type **no** and press **Enter**.

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

e. The router will complete its boot process and display the User Exec prompt. Enter Privileged Exec mode.

```
Router> enable
```

Are you still prompted to enter a password?	Yes

Step 5: Reset Password and Save New Configuration

a. While in Privileged Exec mode, copy the startup configuration to the running configuration.

```
Router# copy startup-config running-config
Destination filename [running-config]?
1478 bytes copied in 0.272 secs (5434 bytes/sec)

R1 #
```

b. Enter global configuration mode.

c. Reset the enable secret password to **cisco**.

```
R1 (config)# enable secret cisco
```

d. Reset the configuration register back to 0x2102 to allow the startup configuration to automatically load the next time the router is rebooted.

```
R1(config)# config-register 0x2102
```

e. Exit global configuration mode.

f. Copy the running configuration to the startup configuration.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

You have successfully reset the enable password on a router.

Step 6: Verify the Router is Loading Correctly

a. Reboot R1 and wait for it to come back online.

Did it automatically load its saved configuration?	Yes

b. Enter Privileged Exec mode.

The new enable secret password should be cisco. If you are able to enter Privileged Exec mode, then you have successfully completed the password recovery process.

Reflection Questions

1. Why is it a recommended practice to keep backups of device configuration and OS images on a remote server?

   It is an ideal practice to keep backups of device configurations and OS images on a remote server to ensure data integrity, availability, and prevention due to natural causes such as natural disasters, acts of god, security breaches, and other unexpected notions aforementioned above.

2. After performing this lab activity, you were able to see that a password reset can be easily done on a device even if a very secure password was configured on it. What concrete preventive measures can you do so that unauthorized persons cannot easily perform a password reset procedure on a device?

   A concrete preventive measure is to enable 2FA or two-factor authentication to prevent and restrict physical access to the devices by implementing specific secure physical controls.