Lab – Configuring Basic Router Settings with IOS CLI

Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
|  | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

1. Objectives

Part 1: Set Up the Topology and Initialize Devices

* Cable equipment to match the network topology.
* Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

* Assign static IPv4 information to the PC interfaces.
* Configure basic router settings.
* Verify network connectivity.
* Configure the router for SSH.

Part 3: Display Router Information

* Retrieve hardware and software information from the router.
* Interpret the output from the startup configuration.
* Interpret the output from the routing table.
* Verify the status of the interfaces.

Part 4: Configure IPv6 and Verify Connectivity

1. Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and IPv4 interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and utilize IOS commands to retrieve information from the device to answer questions about the router. In Part 4, you will configure IPv6 on the router so that PC-B can acquire an IP address and then verify connectivity.

For review purposes, this lab provides the commands necessary for specific router configurations.

**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 2960 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 router and switch have been erased and have no startup configurations. Refer to Appendix A for the procedures to initialize and reload devices.

1. 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)
* 2 PCs (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

**Note**: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable can be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

1. Set Up the Topology and Initialize Devices
   1. Cable the network as shown in the topology.
      1. Attach the devices as shown in the topology diagram, and cable as necessary.
      2. Power on all the devices in the topology.
   2. Initialize and reload the router and switch.

**Note**: Appendix A details the steps to initialize and reload the devices.

1. Configure Devices and Verify Connectivity
   1. Configure the PC interfaces.
      1. Configure the IP address, subnet mask, and default gateway settings on PC-A.
      2. Configure the IP address, subnet mask, and default gateway settings on PC-B.
   2. Configure the router.
      1. Console into the router and enable privileged EXEC mode.

Router> **enable**

Router#

* + 1. Enter into global configuration mode.

Router# **config terminal**

Router(config)#

* + 1. Assign a device name to the router.

Router(config)# **hostname R1**

* + 1. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

R1(config)# **no ip domain-lookup**

* + 1. Require that a minimum of 10 characters be used for all passwords.

R1(config)# **security passwords min-length 10**

Besides setting a minimum length, list other ways to strengthen passwords.

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

Use capital letters, numbers, and special characters in passwords.

* + 1. Assign **cisco12345** as the privileged EXEC encrypted password.

R1(config)# **enable secret cisco12345**

* + 1. Assign **ciscoconpass** as the console password, establish a timeout, enable login, and add the **logging synchronous** command. The **logging synchronous** command synchronizes debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

R1(config)# **line con 0**

R1(config-line)# **password ciscoconpass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **login**

R1(config-line)# **logging synchronous**

R1(config-line)# **exit**

R1(config)#

For the **exec-timeout** command, what do the **5** and **0** represent?

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

The session will timeout in 5 minutes and 0 seconds.

* + 1. Assign **ciscovtypass** as the vty password, establish a timeout, enable login, and add the **logging synchronous** command.

R1(config)# **line vty 0 4**

R1(config-line)# **password ciscovtypass**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **transport input telnet**

R1(config-line)# **login**

R1(config-line)# **logging synchronous**

R1(config-line)# **exit**

R1(config)#

* + 1. Encrypt the clear text passwords.

R1(config)# **service password-encryption**

* + 1. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

R1(config)# **banner motd #Unauthorized access prohibited!#**

* + 1. Configure an IP address and interface description. Activate both interfaces on the router.

R1(config)# **int g0/0**

R1(config-if)# **description Connection to PC-B**

R1(config-if)# **ip address 192.168.0.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **int g0/1**

R1(config-if)# **description Connection to S1**

R1(config-if)# **ip address 192.168.1.1 255.255.255.0**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **exit**

R1#

* + 1. Set the clock on the router; for example:

R1# **clock set 17:00:00 18 Feb 2013**

* 1. Verify network connectivity.
     1. Ping PC-B from a command prompt on PC-A.

**Note**: It may be necessary to disable the PCs firewall.

Were the pings successful? \_\_\_\_ Yes

After completing this series of commands, what type of remote access could be used to access R1?

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

Telnet

* + 1. Remotely access R1 from PC-A using the Telnet.

On the command line of PC-A insert the following command: **telnet 192.168.1.1** with

password **ciscovtypass**

Was remote access successful? \_\_\_\_ Yes

Why is the Telnet protocol considered to be a security risk?

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

A Telnet session can be seen in clear text. It is not encrypted. Passwords can easily be seen using a packet sniffer.

* 1. Configure the router for SSH access.
     1. Enable SSH connections and create a user in the local database of the router.

R1# **configure terminal**

R1(config)# **ip domain-name CCNA-lab.com**

R1(config)# **username admin privilege 15 secret adminpass1**

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

R1(config-line)# **exit**

R1(config)# **crypto key generate rsa modulus 1024**

R1(config)# **exit**

* + 1. Remotely access R1 from PC-A using the SSH.

On the command line of PC-A insert the following command: **ssh –l admin 192.168.1.1** with the password **adminpass1**.

Was remote access successful? \_\_\_\_ Yes

1. Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

* 1. Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to R1 at IP address 192.168.0.1 and log in as **admin** with the password **adminpass1**.

* 1. Retrieve important hardware and software information.
     1. Use the **show version** command to answer questions about the router.

R1# **show version**

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thu 26-Jul-12 19:34 by prod\_rel\_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R1 uptime is 10 minutes

System returned to ROM by power-on

System image file is "**flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"**

Last reload type: Normal Reload

Last reload reason: power-on

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 CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.

Processor board ID FTX1636848Z

2 Gigabit Ethernet interfaces

2 Serial(sync/async) interfaces

1 terminal line

DRAM configuration is 64 bits wide with parity disabled.

**255K bytes of non-volatile configuration memory.**

**250880K bytes of ATA System CompactFlash 0 (Read/Write)**

-----------------------------------------------------------------

Technology Technology-package Technology-package

Current Type Next reboot

------------------------------------------------------------------

ipbase ipbasek9 Permanent ipbasek9

security None None None

data None None None

**Configuration register is 0x2142 (will be 0x2102 at next reload)**

What is the name of the IOS image that the router is running?

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

Image version may vary, but answers should be something like c1900-universalk9-mz.SPA.152-4.M3.bin.

How much non-volatile random-access memory (NVRAM) does the router have?

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

Answers may vary, but the output from the **show version** on 1941 router is: 255K bytes of non-volatile configuration memory.

How much Flash memory does the router have?

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

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

Answers may vary, but the default output from the **show version** command on the 1941 router is 250880K bytes of ATA System CompactFlash 0 (Read/Write).

* + 1. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (**|**) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

R1# **show version | include register**

Configuration register is 0x2142

What is the boot process for the router on the next reload?

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

Answers may vary. In most cases (0x2102), the router will undergo a normal boot, load the IOS from the Flash memory, and load the startup configuration from the NVRAM if present. If the config register is 0x2142, the router will bypass the startup config and begin at the user-mode command prompt. If the initial boot fails, the router goes into ROMMON mode.

**(0x2102), el enrutador se someterá a un arranque normal, cargará el IOS desde la memoria Flash y cargará la configuración de inicio desde la NVRAM, si está presente.**

**Si el registro de configuración es 0x2142, el enrutador omitirá la configuración de inicio y comenzará en el símbolo del sistema del modo de usuario.**

**Si el arranque inicial falla, el enrutador entra en modo ROMMON.**

* 1. Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

R1# **show start**

Using 1674 out of 262136 bytes

….

line vty 0 4

exec-timeout 5 0

password 7 060506324F411F0D1C0713181F

logging synchronous

login local

transport input ssh

!

scheduler allocate 20000 1000

end

How are passwords presented in the output?

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

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

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

Passwords are encrypted due to the service password-encryption command. The line con password of ciscoconpass is encrypted as 060506324F410A160B0713181F. The line vty password of ciscovtypass is encrypted as 060506324F411F0D1C0713181F.

Use the **show startup-config | begin vty** command.

line vty 0 4

exec-timeout 5 0

password 7 060506324F411F0D1C0713181F

login local

transport input ssh

!

scheduler allocate 20000 1000

end

What is the result of using this command?

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

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

A user receives the startup configuration output beginning with the line that includes the first instance of the filtering expression.

* 1. Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0

L 192.168.0.1/32 is directly connected, GigabitEthernet0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1

L 192.168.1.1/32 is directly connected, GigabitEthernet0/1

What code is used in the routing table to indicate a directly connected network?

**The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.**

How many route entries are coded with a C code in the routing table? \_\_\_\_\_ 2

* 1. Display a summary list of the interfaces on the router.

Use the **show ip interface brief** command on the router to answer the following question.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 192.168.0.1 YES manual up up

GigabitEthernet0/1 192.168.1.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 unassigned YES unset administratively down down

R1#

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

**no shutdown**

1. Reflection
   1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?

Al investigar un problema de conectividad de red, un técnico sospecha que una interfaz no está habilitada. Qué

¿El comando show podría utilizar el técnico para solucionar este problema?

Answers may vary. However, **show ip interface brief** or **show startup-config** would provide the information.

* 1. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

1. Al investigar un problema de conectividad de red, un técnico sospecha que a una interfaz se le asignó una máscara de subred incorrecta. ¿Qué comando show podría usar el técnico para solucionar este problema?

**show startup-config** or **show running-config**