

Lab - Secure Network Devices Topology

16.5.2



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	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: Configure Basic Security Measures on the Router

Part 3: Configure Basic Security Measures on the Switch

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the 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.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable) 15.0(2) X
- 1 PC (Windows with a terminal emulation program, such as Tera Term) →
- Console cables to configure the Cisco IOS devices via the console ports *Show flash*
- Ethernet cables as shown in the topology

Instructions

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 devices.

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

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

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router and switch.

- Console into the device and enable privileged EXEC mode. *> enable*
- Assign the device name according to the Addressing Table. *(.)# hostname R1*
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames. *(.)# no ip domain-lookup*
- Assign class as the privileged EXEC encrypted password. *(.)# enable secret class*
- Assign cisco as the console password and enable login. *R1(.)# line con 0 → password cisco → login*
- Assign cisco as the VTY password and enable login. *R1(.)# line vty 0 4 → password cisco → login*
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited. *(.)# banner motd #Unauthorized access is prohibited#*
- Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table. *R1(.)# int G0/0/1 → ip address 192.168.1.1 255.255.255.0 → no shutdown*
- Configure the default SVI on the switch with the IP address information according to the Addressing Table. *S1(.)# int VLAN 1 → ip address 192.168.1.1 255.255.255.0 → no shutdown*
- Save the running configuration to the startup configuration file. *write memory*

Step 4: Configure PC-A.

- Configure PC-A with an IP address and subnet mask. *192.168.1.3/24*
- Configure a default gateway for PC-A. *192.168.1.1*

Step 5: Verify network connectivity.

Ping R1 and S1 from PC-A. If any of the pings fail, troubleshoot the connection.

Part 2: Configure Basic Security Measures on the Router

Step 1: Configure security measures.

- Encrypt all clear-text passwords. *(.)# service password-encryption*
- Configure the system to require a minimum 12-character password. *security passwords min-length 12*
- Change the passwords (privileged exec, console, and vty) to meet the new length requirement.
 - Set the privileged exec password to **\$cisco!PRIV***. *(.)# enable secret \$cisco!PRIV**
 - Set the console password to **\$cisco!!CON***. *(.)# line con 0 → password \$cisco!!CON* → login*
 - Set the vty line password to **\$cisco!!VTY***. *(.)# line vty 0 4 → password \$cisco!!VTY* → login*
- Configure the router to accept only SSH connections from remote locations
 - Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020**. *R1(.)# user name SSHadmin secret 55HAdm!n2020*

Lab - Secure Network Devices

- 2) The router's domain name should be set to ccna-lab.com *R1()# ip domain-name ccna-lab.com*
- 3) The key modulus should be 1024 bits. *R1()# crypto key generate RSA → 1024*
- e. Set security and best-practice configurations on the console and vty lines.
line vty 0 4 → transport input ssh → login local.
line con 0 / line vty 0 4 →
 - 1) Users should be disconnected after 5 minutes of inactivity. *exec-timeout 5 0*
 - 2) The router should not allow vty logins for 2 minutes if 3 failed login attempts occur within 1 minute. *R1()# login block-for 120 attempts 3 within 60*

Part 3: Configure security measures.

Step 1: Verify that all unused ports are disabled. ✓ *R1()# show ip int brief*

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command. Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

Step 2: Verify that your security measures have been implemented correctly.

- a. Use Tera Term on PC-A to telnet to R1. ✓

Does R1 accept the Telnet connection? Explain. ✓

No, the connection because when I configured the transport at vty 0 4, I used SSH

- b. Use Tera Term on PC-A to SSH to R1. ✓

Does R1 accept the SSH connection? ✓

Yes

- c. Intentionally mistype the user and password information to see if login access is blocked after two attempts. ✓

What happened after you failed to login the second time?

the connection after R1 was disconnected. If I try to connect between the time that I have less (60 seconds or less), the connection will be block

- d. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 120 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 111 more seconds.

- e. After the 120 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **55HAdm!n2020** for the password.

After you successfully logged in, what was displayed?

R1 banner motd that I configured before

- f. Enter privileged EXEC mode and use **\$cisco!PRIV*** for the password.

If you mistype this password, are you disconnected from your SSH session after three failed attempts within 60 seconds? Explain.

No, the access will block for 120 attempts 3 within 60 on vty lines

- g. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Part 4: Configure Basic Security Measures on the Switch

Step 1: Configure security measures.

- a. Encrypt all clear-text passwords. *(S1) # service password-encryption*
- b. Configure the system to require a minimum 12 character password *security passwords min-length 12*
- c. Change the passwords (privileged exec, console, and vty) to meet the new length requirement.
 - 1) Set the privileged exec password to **\$cisco!PRIV*** *(S1) # enable secret \$cisco! PRIV**
 - 2) Set the console password to **\$cisco!!CON*** *(S1) # line con 0
password \$cisco!!CON* login*
 - 3) Set the vty line password to **\$cisco!!VTY*** *(S1) # line vty 0 15
password \$cisco!! VTY* → login*
- d. Configure the switch to accept **only** SSH connections from remote locations.
 - 1) Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020** *(S1) # username SSHadmin secret 55HAdm!n2020*
 - 2) The switches domain name should be set to **ccna-lab.com** *(S1) # ip domain-name ccna-lab.com*
 - 3) The key modulus should be 1024 bits. *(S1) # crypto key generate RSA → 1024*
- e. Set security and best-practice configurations on the console and vty lines. *(line con 0 line vty 0 15)*
 - 1) Users should be disconnected after 5 minutes of inactivity. *exec-timeout 5 0 exit*
 - 2) The switch should not allow logins for 2 minutes if 3 failed login attempts occur within 1 minute. *login block-for 120 attempts 3 within 60*
 - f. Disable all of the unused ports. *→ int range F0/1-4, F0/7-24, G0/1-2 → shutdown*

Step 2: Verify all unused ports are disabled.

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

- a. You can verify the switch port status using the **show ip interface brief** command. ✓
- b. Use the **interface range** command to shut down multiple interfaces at a time. *int range F0/1-4, F0/7-24, G0/1-2 → shutdown*
- c. Verify that all inactive interfaces have been administratively shut down. ✓

Step 3: Verify that your security measures have been implemented correctly.

- a. Verify that Telnet has been disabled on the switch. ✓
- b. SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.
- c. After the 30 seconds has expired, SSH to S1 again and log in using the **SSHadmin** username and **55HAdm!n2020** for the password. *No because I can't update the IOS of the switch.*

Did the banner appear after you successfully logged in?

Yes

- d. Enter privileged EXEC mode using **\$cisco!PRIV*** as the password.
- e. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Reflection Questions

1. The **password cisco** command was entered for the console and VTY lines in your basic configuration in Part 1. When is this password used after the best practice security measures have been applied?

This password won't be used because I can figure a new password with the length requirement.

2. Are preconfigured passwords shorter than 10 characters affected by the **security passwords min-length 12** command?

No, all password that I configured before this command is not affected. All password that I will set after this command, it will affect.

Router Interface Summary Table

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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

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.