Lab - Secure Network Devices

# Topology



# 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)
* 1 PC (Windows with a 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

# Instructions

## 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.

### Cable the network as shown in the topology.

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

### Initialize and reload the router and switch.

### Configure the router and switch.

Open configuration window

* + - 1. Console into the device and enable privileged EXEC mode.
      2. Assign the device name according to the Addressing Table.
      3. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
      4. Assign class as the privileged EXEC encrypted password.
      5. Assign cisco as the console password and enable login.
      6. Assign cisco as the VTY password and enable login.
      7. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
      8. Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.
      9. Configure the default SVI on the switch with the IP address information according to the Addressing Table.
      10. Save the running configuration to the startup configuration file.

Close configuration window

### Configure PC-A.

Open command prompt

* + - 1. Configure PC-A with an IP address and subnet mask.
      2. Configure a default gateway for PC-A.

Close command prompt

### Verify network connectivity.

Open configuration window

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

Close configuration window

## Configure Basic Security Measures on the Router

### Configure security measures.

Open configuration window

* + - 1. Encrypt all clear-text passwords.
      2. Configure the system to require a minimum 12-character password.
      3. Change the passwords (privileged exec, console, and vty) to meet the new length requirement.
         1. Set the privileged exec password to **$cisco!PRIV\***
         2. Set the console password to **$cisco!!CON\***
         3. Set the vty line password to **$cisco!!VTY\***
      4. Configure the router to accept only SSH connections from remote locations
         1. Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020**
         2. The router’s domain name should be set to ccna-lab.com
         3. The key modulus should be 1024 bits.
      5. Set security and best-practice configurations on the console and vty lines.
         1. Users should be disconnected after 5 minutes of inactivity.
         2. The router should not allow vty logins for 2 minutes if 3 failed login attempts occur within 1 minute.

Close configuration window

## Configure security measures.

### Verify that all unused ports are disabled.

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.

Open configuration window

Close configuration window

### Verify that your security measures have been implemented correctly.

Open configuration window

* + - 1. Use Tera Term on PC-A to telnet to R1.

#### Question:

Does R1 accept the Telnet connection? Explain.

Không, kết nối bị từ chối. Telnet đã bị vô hiệu hóa với lệnh input SSH.

* + - 1. Use Tera Term on PC-A to SSH to R1.

#### Question:

Does R1 accept the SSH connection?

Có.

* + - 1. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

#### Question:

What happened after you failed to login the second time?

Kết nối với R1 đã bị ngắt kết nối. Kể cả có cố gắng kết nối lại vẫn sẽ bị từ chối trong vòng 30 giây.

* + - 1. 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.
      2. After the 120 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **55HAdm!n2020** for the password.

#### Question:

After you successfully logged in, what was displayed?

R1 –MOTD.

* + - 1. Enter privileged EXEC mode and use **$cisco!PRIV\*** for the password.

#### Question:

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

Không. Nếu nhập sai 3 lần trong 60 giây sẽ chỉ giám sát các lần đăng nhập phiên trên các dòng VTY, chứ không ngắt kết nối truy cập SSH.

* + - 1. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Close configuration window

## Configure Basic Security Measures on the Switch

### Configure security measures.

Open configuration window

* + - 1. Encrypt all clear-text passwords.
      2. Change the passwords (privileged EXEC, console, and vty).
         1. Set the privileged exec password to **$cisco!PRIV\***
         2. Set the console password to **$cisco!!CON\***
         3. Set the vty line password to **$cisco!!VTY\***
      3. Configure the switch to accept only SSH connections from remote locations.
         1. Configure the username **SSHadmin** with an encrypted password of **55HAdm!n2020**
         2. The switches domain name should be set to ccna-lab.com
         3. The key modulus should be 1024 bits.
      4. Set security and best-practice configurations on the console and vty lines.
         1. Users should be disconnected after 5 minutes of inactivity.
         2. The switch should not allow logins for 2 minutes if 3 failed login attempts occur within 1 minute.
      5. Disable all of the unused ports.

### Verify all unused ports are disabled.

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

* + - 1. You can verify the switch port status using the **show ip interface brief** command.
      2. Use the **interface range** command to shut down multiple interfaces at a time.
      3. Verify that all inactive interfaces have been administratively shut down.

Close configuration window

### Verify that your security measures have been implemented correctly.

* + - 1. Verify that Telnet has been disabled on the switch.
      2. SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.
      3. After the 30 seconds has expired, SSH to S1 again and log in using the **SSHadmin** username and **55HAdm!n2020** for the password.

#### Question:

Did the banner appear after you successfully logged in?

Sau khi đăng nhập thành công, nó có xuất hiện.

* + - 1. Enter privileged EXEC mode using **$cisco!PRIV\*** as the password.
      2. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Close configuration window

# 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?

Mật khẩu này chỉ được sử dụng một lần và không được sử dụng thêm. Bởi vì lệnh này đã bị vô hiệu hóa ngay khi lệnh đăng nhập cục bộ được nhập cho các dòng đó.

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

Không. Độ dài tối thiểu của lệnh mật khẩu bảo mật chỉ ảnh hưởng đến các mật khẩu được nhập sau khi lệnh này được sử dụng. Mọi mật khẩu đã tồn tại trước đó vẫn còn có tính khả thi. Nếu những mật khẩu đó được thay đổi thì độ dài mỗi mật khẩu sẽ có ít nhất 12 ký tự.

# 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.

End of document