Lab - Configure Network Devices with SSH

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 the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

# Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands. However, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

**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 router.

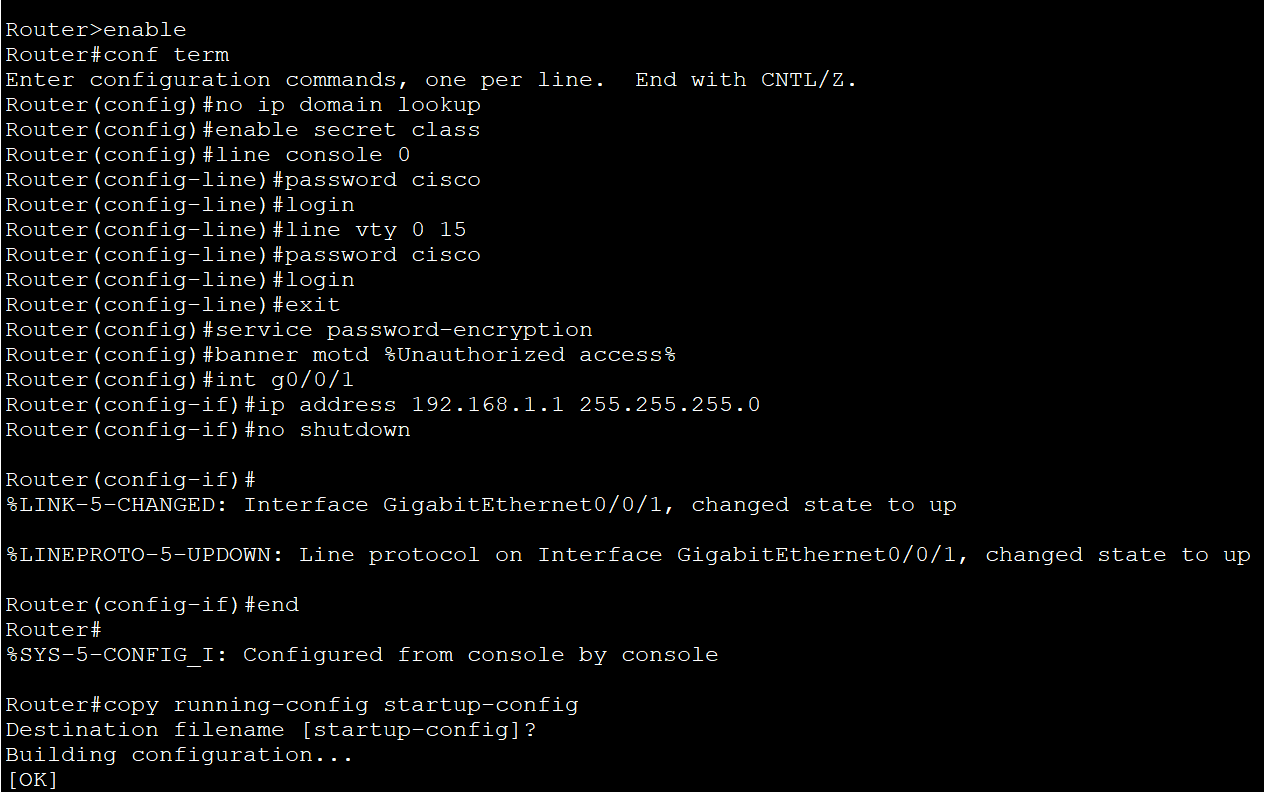
### Cable the network as shown in the topology.

Изображение выглядит как снимок экрана, линия, текст

Автоматически созданное описание

### Initialize and reload the router and switch.

### Configure the router.



### Configure PC-A.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

### Verify network connectivity.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all the information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

### Configure device authentication.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

### Configure the encryption key method.

### Configure a local database username.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

### Enable SSH on the VTY lines.

Изображение выглядит как текст, Шрифт, снимок экрана, типография

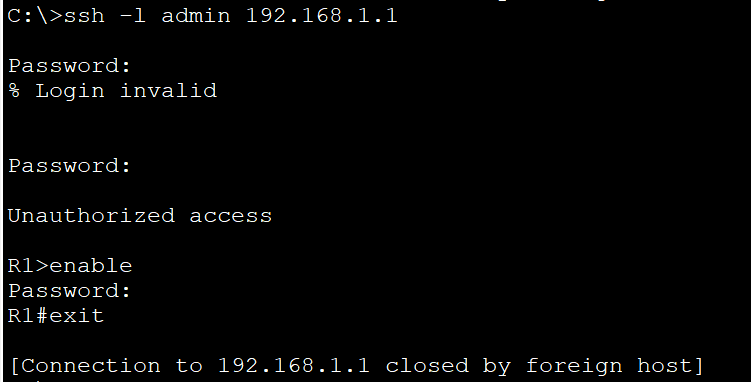
Автоматически созданное описание

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

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

### Establish an SSH connection to the router.



## Configure the Switch for SSH Access

In Part 3, you will configure the switch to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

### Configure the basic settings on the switch.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Open configuration window

### Configure the switch for SSH connectivity.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

### Establish an SSH connection to the switch.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

## SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

### View the parameters available for the Cisco IOS SSH client.

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

### SSH to R1 from S1.

### Изображение выглядит как текст, снимок экрана, Шрифт, дизайн Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, число

Автоматически созданное описание

Close configuration window

# Reflection Question

How would you provide multiple users, each with their own username, access to a network device?

You would add each user’s username and password to the local database using the username command. It is also possible to use a RADIUS or TACACS server, but this has not been covered yet.

Type your answers here.

# 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