Lab 11.2.4.6 Accessing Network Devices with SSH



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| R1 | G0/1 | 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 |

1. Objectives

Part 1: Configure Basic Device Settings

Part 2 and 3: Configure the Router and Switch for SSH Access

Part 4: SSH from the CLI on the Switch

1. 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.

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.

* 1. Cable the network as shown in the topology.
  2. Configure PC-A.
     1. Configure PC-A with an IP address and subnet mask.
     2. Configure a default gateway for PC-A.
  3. Configure the router.
     1. Console into the router and enable privileged EXEC mode.

Router> **enable**

Router#

* + 1. Enter configuration mode.

Router# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

* + 1. Assign the name of the router as R1.

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. Assign **class** as the privileged EXEC encrypted password.

R1(config)# enable secret class

* + 1. Assign **cisco** as the console password and enable login.

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

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

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

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

R1(config)#

* + 1. Assign **cisco** as the vty password and enable login.

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

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

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

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

R1(config)#

* + 1. Encrypt the plain 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 and activate the G0/1 interface on the router using the information contained in the Addressing Table.

R1(config)# **interface 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)# **end**

R1#

* + 1. Save the running configuration to the startup configuration file.

R1# **copy run start**

Destination filename [startup-config]?

Building configuration...

* 1. Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection. (**ping 192.168.1.1**)

1. Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all 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.

* 1. Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

* + 1. Enter configuration mode.

R1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#

* + 1. Configure the domain for the device.

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

* 1. Configure the encryption key method.

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

Modulus[512]: **1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

* 1. Configure a local database username.

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

**Note**: A privilege level of 15 gives the user administrator rights.

The Cisco IOS software CLI has two levels of access to commands.

* User EXEC mode (privilege level 1) - Provides the lowest EXEC mode user privileges and allows only user-level commands available at the router> prompt.
* Privileged EXEC mode (privilege level 15) - Includes all enable-level commands at the router# prompt.
  1. Enable SSH on the VTY lines.
     1. Enable SSH on the inbound VTY lines using the **transport input** command.

**NOTA:** Habilite **SSH** en las líneas VTY entrantes mediante el comando **transport input**.

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

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

* + 1. Change the login method to use the **local database** for user verification.

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

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

R1#

* 1. Save the running configuration to the startup configuration file.

R1# **copy run start**

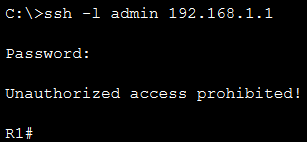
Destination filename [startup-config]?

Building configuration...

[OK]

* 1. Establish an SSH connection to the router.
     1. Start **Comand Prompt** from PC-A.
     2. Establish an SSH connection to the router. Use the username **admin** and password **adminpass**. You should be able to establish an SSH session with R1.

C:\> ssh -l admin 192.168.1.1



1. Configure the Switch for SSH Access

In Part 3, you will configure the switch in the topology to accept SSH connections

* 1. Configure the basic settings on the switch.
     1. Console into the switch and enable privileged EXEC mode.

Switch> **enable**

Switch#

* + 1. Enter configuration mode.

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#

* + 1. Assign the name of the switch as S1.

Switch(config)# **hostname S1**

S1(config)#

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

S1(config)# **no ip domain-lookup**

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

S1(config)# **enable secret class**

* + 1. Assign **cisco** as the console password and enable login.

S1(config)# **line con 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **exit**

S1(config)#

* + 1. Assign **cisco** as the vty password and enable login.

S1(config)# **line vty 0 15**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **end**

S1#

* + 1. Encrypt the plain text passwords.

S1# **configure terminal**

S1(config)# **service password-encryption**

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

S1(config)# **banner motd # Unauthorized access prohibited! #**

* + 1. Configure the default SVI with the IP address information contained in the Addressing Table.

S1#(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0**

S1(config-if)# **no shut**

S1(config-if)# **exit**

S1(config)#

* 1. Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

* + 1. Configure the domain for the device.

S1(config)# **ip domain-name ccna-lab.com**

* + 1. Configure the encryption key method.

S1(config)# **crypto key generate rsa**

modulus[512]**: 1024**

* + 1. Configure a local database username.

S1(config)# **username admin privilege 15 secret adminpass**

* + 1. Enable Telnet and SSH on the VTY lines.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input telnet ssh**

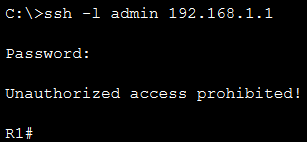
* + 1. Change the login method to use the local database for user verification.

S1(config-line)# **login local**

S1(config-line)# **end**

* 1. Establish an SSH connection to the switch.
     1. Start **Comand Prompt** from PC-A.
     2. Establish an SSH connection to the switch. Use the username **admin** and password **adminpass**. You should be able to establish an SSH session with S1.

C:\> ssh -l admin 192.168.1.11



Are you able to establish an SSH session with the switch? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 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.

* 1. View the parameters available for the Cisco IOS SSH client.

1. Use the question mark (**?**) to display the parameter options available with the **ssh** command.

S1# **ssh ?**

-c Select encryption algorithm

-l Log in using this user name

...

* 1. SSH to R1 from S1.
     1. You must use the **–l** **admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass** for the password.

S1# **ssh -l admin 192.168.1.1**

Password:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Warning: Unauthorized Access is Prohibited!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

R1#

* + 1. You can return to S1 without closing the SSH session to R1 by pressing **Ctrl**+**Shift**+**6**. Release the **Ctrl**+**Shift**+**6** keys and press **x**. The switch privileged EXEC prompt displays.

R1#

S1#

* + 1. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

S1#

[Resuming connection 1 to 192.168.1.1 ... ]

R1#

* + 1. To end the SSH session on R1, type **exit** at the router prompt.

R1# **exit**

[Connection to 192.168.1.1 closed by foreign host]

S1#

Lab 11.2.4.8 Securing Network Devices

1. Topology



1. Objectives

Part 1: Configure Basic Security Measures on the Router

Part 2: Configure Basic Security Measures on the Switch

1. 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.

1. Configure Basic Security Measures on the Router
   1. Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

**Note**: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

* + 1. Configure the router.
    2. Enter configuration mode.

R1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#

* + 1. Change the privileged EXEC encrypted password to meet guidelines.

R1(config)# **enable secret Enablep@55**

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

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

* 1. Secure the console and VTY lines.
     1. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

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

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

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

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

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

R1(config)#

* + 1. The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

R1(config)# **login block-for 30 attempts 2 within 120**

What does the **2 within 120** mean in the above command?

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

What does the **block-for 30** mean in the above command?

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

R1(config)# exit

* 1. 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.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

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

GigabitEthernet0/0 unassigned YES NVRAM administratively down down

GigabitEthernet0/1 192.168.1.1 YES manual up up

Serial0/0/0 unassigned YES NVRAM administratively down down

Serial0/0/1 unassigned YES NVRAM administratively down down

* 1. Verify that your security measures have been implemented correctly.
     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 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

R1# **show login**

A default login delay of 1 second is applied.

No Quiet-Mode access list has been configured.

Router enabled to watch for login Attacks.

If more than 2 login failures occur in 120 seconds or less,

logins will be disabled for 30 seconds.

Router presently in Quiet-Mode.

Will remain in Normal-Mode for 14 seconds.

Denying logins from all sources.

R1#

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

1. Configure Basic Security Measures on the Switch
   1. Strengthen Passwords on the switch.
      1. Configure the switch.
      2. Enter configuration mode.

S1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#

* + 1. Change the privileged EXEC encrypted password to meet strong password guidelines.

S1(config)# **enable secret Enablep@55**

**Note**: The security **password min-length** command is not available on the 2960 switch.

* 1. Secure the console and VTY lines.
     1. Configure the switch to log out a line that has been idle for 10 minutes.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **exit**

S1(config)#

* + 1. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

S1(config)# **login block-for 30 attempts 2 within 120**

S1(config)# **end**

* 1. 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.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.11 YES manual up up

FastEthernet0/1 unassigned YES unset down down

FastEthernet0/2 unassigned YES unset down down

FastEthernet0/3 unassigned YES unset down down

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset up up

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

..

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

* + 1. Use the **interface range** command to shut down multiple interfaces at a time.

S1# config t

S1(config)# **interface range f0/1–4, f0/7-24, g0/1-2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

* + 1. Verify that all inactive interfaces have been administratively shut down.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.11 YES manual up up

FastEthernet0/1 unassigned YES unset administratively down down

FastEthernet0/2 unassigned YES unset administratively down down

FastEthernet0/3 unassigned YES unset administratively down down

FastEthernet0/4 unassigned YES unset administratively down down

FastEthernet0/5 unassigned YES unset up up

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset administratively down down

FastEthernet0/8 unassigned YES unset administratively down down

FastEthernet0/9 unassigned YES unset administratively down down

FastEthernet0/10 unassigned YES unset administratively down down

FastEthernet0/11 unassigned YES unset administratively down down

FastEthernet0/12 unassigned YES unset administratively down down

FastEthernet0/13 unassigned YES unset administratively down down

FastEthernet0/14 unassigned YES unset administratively down down

FastEthernet0/15 unassigned YES unset administratively down down

FastEthernet0/16 unassigned YES unset administratively down down

FastEthernet0/17 unassigned YES unset administratively down down

FastEthernet0/18 unassigned YES unset administratively down down

FastEthernet0/19 unassigned YES unset administratively down down

FastEthernet0/20 unassigned YES unset administratively down down

FastEthernet0/21 unassigned YES unset administratively down down

FastEthernet0/22 unassigned YES unset administratively down down

FastEthernet0/23 unassigned YES unset administratively down down

FastEthernet0/24 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset administratively down down

GigabitEthernet0/2 unassigned YES unset administratively down down

* + 1. Erase NVRAM:

S1# **erase startup-config**