Lab 8.3.3b Configuring a Remote Router Using SSH

Objectives

- Use SDM to configure a router to accept SSH connections.
- Configure SSH client software on a PC.
- Establish a connection to a Cisco ISR using SSH version 2.
- Check the existing running configuration.
- Configure a non-SDM router for SSH using the Cisco IOS CLI.

Background / Preparation

In the past, Telnet was the most common network protocol used to remotely configure network devices. However, protocols such as Telnet do not authenticate or 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 machine and execute commands; however, it can also transfer files using the associated SFTP or SCP protocols.

For SSH to function, the network devices communicating must support it. In this lab, you 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. Network devices connected via other types of links, such as serial, can also be managed using SSH as long as they support IP. Like Telnet, SSH is an in-band, TCP/IP-based Internet protocol.

You can use either Cisco SDM or Cisco IOS CLI commands to configure SSH on the router. The Cisco 1841 ISR supports SSH versions 1 and 2; version 2 is preferred. The SSH client used in this lab is PuTTY, which can be downloaded free of charge. If you are working with a router that does not have SDM installed, use
Cisco IOS CLI commands to configure SSH. Instructions are provided in Step 2 of this lab. To perform the basic router configuration, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI.”

The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS software releases. Many newer Cisco routers come with SDM pre-installed. This lab uses a Cisco 1841 router, which has SDM (and SDM Express) pre-installed. You can use another router model that supports SDM. If the router does not have SDM installed, you can download the latest version free of charge at [http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm](http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm). From this web page, you can also view or download “Downloading and Installing Cisco Router and Security Device Manager.” This document provides instructions and system requirements for installing SDM.

**Note:** If you are using SDM to configure SSH, you must complete Lab 5.2.3, “Configuring an ISR with SDM Express,” on the router to be used before performing this lab. This lab assumes that the router has been previously configured with basic settings.

**Note:** If the startup-config is erased from an SDM router, SDM no longer comes up by default when the router is restarted. In this case, it is necessary to build a basic router configuration using Cisco IOS commands. See the procedure at the end of this lab or contact the instructor.

### Required Resources

The following resources are required:

- Cisco 1841 ISR router with SDM version 2.4 installed and with basic configuration completed
- (Optional) Other Cisco router model with SDM installed
- (Optional) Other Cisco router model without SDM installed (Cisco IOS software version 12.2 or later; must support SSH)
- Windows XP computer with Internet Explorer 5.5 or later and Sun Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810)
- Latest release of putty.exe client installed on the PC and accessible on the desktop
- Straight-through or crossover Category 5 Ethernet cable (for SDM and SSH)
- (Optional) Console cable, if router is to be configured using the CLI
- Access to the PC command prompt
- Access to PC network TCP/IP configuration
Step 1: Use SDM to configure the router to accept SSH connections.

Note: If you are configuring a router that does not have SDM installed, just read through Step 1 to see how SSH is set up as a separate task when using SDM, and then go to Step 2.

a. Connect to the router Fa0/0 interface. Open the web browser and connect to http://192.168.1.1. When prompted, enter admin for the username and cisco123 for the password. Click OK. Cisco SDM loads.
b. Click the **Configure** button on the tool bar. In the Tasks pane, click **Additional Tasks**. In the Additional Tasks pane, expand **Router Access** and click the **SSH** task. Then click the **Generate RSA Key** button.

**Note:** If the **SSH Key Setup** message says: “RSA key exists and SSH is enabled in your router” and the **Status** is “RSA key is set on this router,” you probably completed Lab 5.2.3, “Configuring an ISR with SDM Express.” In that lab, when you configured security, one of the recommended security settings enabled by default is “Enhance security on this router.” If this box is checked, it automatically configures SSH for router access, sets the banner to warn intruders, enforces minimum password length, and restricts the number of unsuccessful login attempts.
c. In the **Key modulus size** dialog box, enter a key size of **1024** bits. Click **OK**.

![Key modulus size dialog box](image)

By entering a key size of 1024 bits, you ensure a higher level of security for your encryption process.

d. In the **Enter SSH Credentials** dialog box, enter **admin** for the username and **cisco123** for the password. Click **OK**.

![Enter SSH Credentials dialog box](image)

By providing the correct username and password, you are able to access the system securely.
e. Notice that the RSA key is now set on the router.
f. In the Additional Tasks pane, click the VTY option. Select **Input Protocols Allowed**, and then click the **Edit** button.
g. Check the **SSH** box for the Input Protocol, and then click **OK**.

h. When the **Commands Delivery Status** window opens, click **OK**.
i. Close the Cisco SDM by clicking the X in the upper right corner of the window.

j. Click Yes to confirm the closing of SDM, and go to Step 3. (Step 2 shows you how to configure SSH on a non-SDM router.)
Step 2: (Optional) Configure SSH on a non-SDM router.

**Note:** If you are configuring a router for SSH that already has SDM installed, you can skip Step 2 and go directly to Step 3.

a. Connect the router console port with a PC and the HyperTerminal program, as described in Lab 5.1.3, "Powering up an Integrated Services Router."

b. Log in to the router. At the privileged EXEC mode prompt, enter the Cisco IOS CLI commands as shown below. These commands do not include all the passwords that need to be set. See Lab 5.3.5, "Configuring Basic Router Settings with the Cisco IOS CLI," for the configuration settings.

**Note:** The router must be running Cisco IOS software release 12.2 or later. In this example, the router is a Cisco 2620XM running Cisco IOS software release 12.2(7r).

c. Configure the basic router and interface information.

```
Router#config terminal
Router(config)#hostname CustomerRouter
CustomerRouter(config)#ip domain-name customer.com
CustomerRouter(config)#username admin privilege 15 password 0 cisco123
CustomerRouter(config)#interface FastEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
```

d. Configure the remote incoming vty terminal lines to accept Telnet and SSH.

```
CustomerRouter(config)#line vty 0 4
CustomerRouter(config-line)#privilege level 15
CustomerRouter(config-line)#login local
CustomerRouter(config-line)#transport input telnet ssh
CustomerRouter(config-line)#exit
```

e. Generate the RSA encryption key pair for the router to use for authentication and encryption of SSH data that is transmitted. Enter 768 for the number of modulus bits. The default is 512.

```
CustomerRouter(config)#crypto key generate rsa

How many bits in the modulus [512] 768
```

```
CustomerRouter(config)#exit
```

f. Verify that SSH is enabled and the version being used.

```
CustomerRouter#show ip ssh
```

g. Fill in the following information based on the output of the `show ip ssh` command.

- SSH version enabled ________________
- Authentication timeout ________________
- Authentication retries ________________

h. Save the running-config to the startup-config.

```
CustomerRouter#copy running-config startup-config
```

Step 3: Configure the SSH client and connect the PC to the ISR.

a. Download putty.exe and place the application on the desktop. Launch PuTTY by double-clicking the putty.exe icon.
b. In the Category pane, click **SSH**. Verify that the preferred SSH protocol version is set to **2**.

**Note:** The Putty client still connects even if the SSH server is running SSH version 1.
c. In the Category pane, click **Session**. Enter the IP address of the router LAN interface, which is 192.168.1.1. Verify that SSH is selected for the connection type. Click **Open**.
d. The first time a connection is made to SSH on the Cisco 1841 ISR using an SSH client, a connection key is cached in the local machine registry. In the PuTTY Security Alert window, click Yes to continue.
e. At the login prompt, type the administrator username admin, and press Enter.
f. At the password prompt, type the administrator password **cisco123**, and press **Enter**.
Step 4: Check the configuration of the Cisco 1841 ISR.

a. To verify the configuration of the router, type `show run` at the privileged mode prompt, and press Enter.

   Note: There is no need to switch from user mode to privileged mode if you are using SDM, because privileged mode is the default mode.

b. Press the Spacebar to scroll through the current configuration of the router.

```
Building configuration...

Current configuration : 2391 bytes

!  version 12.4
  no service pad
  service tcp-keepalives-in
  service tcp-keepalives-out
  service timestamps debug datetime msec localtime show-timezone
  service timestamps log datetime msec localtime show-timezone
  service password-encryption
  service sequence-numbers
  !
  hostname customerrouter
  !
  boot-start-marker
  boot-end-marker
  !
  security authentication failure rate 3 log
  security passwords min-length 6
  logging buffered 51200 debugging
  logging console critical
  enable secret 5 \$1$m30G$4g9lW96YomeTV231pD0X/

--More--
```
Step 5: Log out of the Cisco 1841 ISR.

To log out of the router when you are finished verifying the configuration, type `logout` at the privileged mode prompt, and then press `Enter`.

```
192.168.1.1 - PuTTY

1
control-plane

banner login ^CAuthorized access only!

  Disconnect IMMEDIATELY if you are not an authorized user! ^C

line con 0
  login local
  transport output telnet
line aux 0
  login local
  transport output telnet
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet ssh

! scheduler allocate 4000 1000
end

 luxuryrouter#logout
```
Step 6: Reflection

a. When comparing Telnet and SSH, what are some advantages and disadvantages?
   
   __________________________________________________________
   __________________________________________________________
   __________________________________________________________

b. What is the default port for SSH? _________  What is the default port for Telnet? _________

c. What Cisco IOS software version was displayed in the running-config?
   
   __________________________________________________________
Basic Cisco IOS Configuration to Bring Up SDM

If the startup config is erased in an SDM router, SDM no longer comes up by default when the router is restarted. It is then necessary to build a basic config as follows. Further details regarding the setup and use of SDM can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

1) Set the router Fa0/0 IP address. (This is the interface that a PC connects to using a browser to bring up SDM. The PC IP address should be set to 10.10.10.2 255.255.255.248.)

Note: An SDM router other than the 1841 may require a connection to a different port to access SDM.

```
Router(config)#interface Fa0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.248
Router(config-if)#no shutdown
```

2) Enable the HTTP/HTTPS server of the router.

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

3) Create a user account with privilege level 15 (enable privileges). Replace username and password with the username and password that you want to configure.

```
Router(config)#username <username> privilege 15 password 0 <password>
```

4) Configure SSH and Telnet for local login and privilege level 15.

```
Router(config)#line vty 0 4
Router(config-line)#privilege level 15
Router(config-line)#login local
Router(config-line)#transport input telnet
Router(config-line)#transport input telnet ssh
Router(config-line)#exit
```