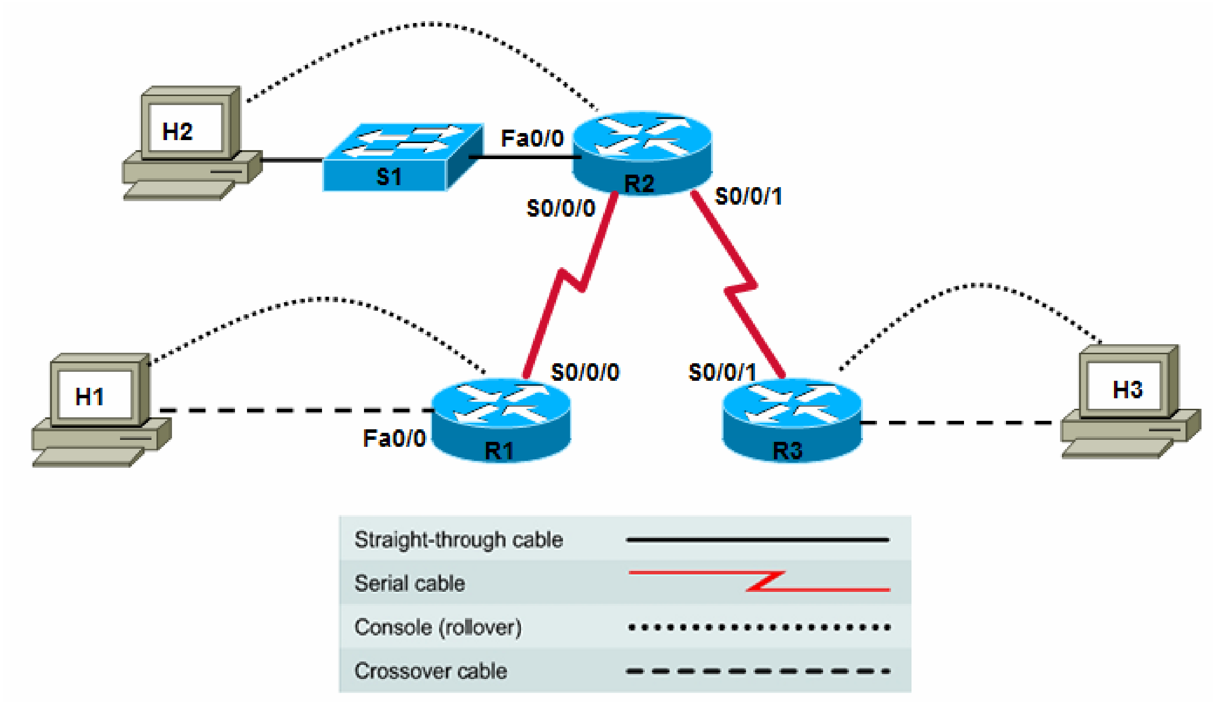
Lab 9.5.3 Using Telnet and SSH to Access Networking Devices



Device	Host Name	Interface	IP Address	Subnet Mask	RIPv2 Network Statements
R1	R1	Serial 0/0/0 (DTE)	10.10.10.1	255.255.255.0	10.0.0.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0	192.168.1.0
R2	R2	Serial 0/0/0 (DCE)	10.10.10.2	255.255.255.0	10.0.0.0
		Serial 0/0/1 (DCE)	172.16.1.1	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.2.1	255.255.255.0	192.168.2.0
R3	R3	Serial 0/0/1 (DTE)	172.16.1.2	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.3.1	255.255.255.0	192.168.3.0
S1	S1	VLAN 1 (mgmt)	192.168.2.99	255.255.255.0	N/A

Objectives

- Establish and manage Telnet connections to a remote router and switch.
- Verify that the Application Layer between the source and destination is working properly.
- Retrieve information about remote routers using **show** commands.
- Configure a router to accept SSH connections using the Cisco IOS CLI.
- Connect from one router using the SSH CLI client to a remote router running the SSH server.

Background / Preparation

Telnet is an excellent tool to use when troubleshooting problems with upper layer functions. Using Telnet to access networking devices enables technicians to enter commands on each device as if they were locally attached. In addition, the ability to reach devices using Telnet indicates that lower layer connectivity exists between the devices. Telnet is widely available on nearly any networking device.

Telnet is an unsecure protocol, which means that all data communicated can be captured and read. SSH is a more secure method for remote device access. Most newer versions of the Cisco IOS software contain an SSH server and an SSH client. In some devices, this service is enabled by default. Other devices require the SSH server to be manually enabled. Similarly, a remote computer with an SSH client installed can be used to start a secure CLI session.

This lab focuses on using Telnet and SSH to access routers remotely to gather information about them and verify upper layer connectivity. In this lab, you telnet from the workstation as a client and from a router into another remote router. In addition, you will configure SSH access on a router and connect using a router-based Cisco IOS CLI client.

Set up a network similar to the one in the topology diagram. Any router that meets the interface requirements displayed in that diagram—such as 800, 1600, 1700, 1800, 2500, or 2600 routers, or a combination of these, can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One router with two serial interfaces and one Fast Ethernet (1841 or other)
- Two routers with one serial interface and one Fast Ethernet (1841 or other)
- One 2960 switch (or comparable) for the R2 LAN
- Three windows XP computers (hosts H2 and H3 are mainly for configuring routers R2 and R3)
- Straight-through and crossover Category 5 Ethernet cables, as required
- Two null serial cables
- Console cable to configure routers
- Access to host H1 command prompt
- Access to host H1 network TCP/IP configuration

On hosts H1, H2, and H3, start a HyperTerminal session to each router.

Note: Make sure that the routers and switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Part 1. Working with Telnet to Verify Device Configurations and Connectivity

Task 1: Build the Network and Verify Network Layer Connectivity

Step 1: Configure the basic information on each router and the switch.

a. Build and configure the network according to the topology diagram and device configuration table. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

b. Configure RIPv2 on each router, and advertise the networks shown in the device configuration table. If necessary, refer to Lab 6.1.5, “Configuring and Verifying RIP”, for instructions on configuring the RIP routing protocol.

c. Configure basic settings on the switch S1 to include host name, passwords and VLAN 1 IP address. If necessary, see Lab 5.5.4, “Configuring the Cisco 2960 Switch.”

Step 2: Configure the hosts.

Configure H1, H2, and H3 with an IP address, subnet mask, and default gateway that is compatible with the IP address of the router default gateway interface address for the LAN to which they are attached.

Step 3: Verify end-to-end Network Layer connectivity.

a. On H1, open a Command Prompt window by choosing **Start > Run** and typing **cmd**. Alternatively, you can choose **Start > All programs > Accessories > Command Prompt**.

b. Use the **ping** command to test end-to-end connectivity. Ping from H1 on the R1 LAN to H3 on the R3 LAN (for example, 192.168.3.2).

```
C:\>ping 192.168.3.2
```

c. If H3 is not attached to R3, ping the R3 serial 0/0/1 interface IP address 172.16.1.2.

```
C:\>ping 172.16.1.2
```

d. If the pings are successful to R3, what does that indicate about the OSI layer connectivity between H1 and R3?

____

Note: If the pings are not successful, troubleshoot the router and host configurations and connections.

Task 2: Establish a Telnet Session from a Host Computer

Step 1: Telnet from H1 to remote router R2.

The Cisco router IOS software has built-in Telnet client and server software. Nearly all computer operating systems have a Telnet client. Many server operating systems also have a Telnet server, although Microsoft Windows desktop operating systems typically do not.

In many cases, you will not have direct access to a router through the console so that you can Telnet to other routers. Usually, you telnet to a router from a host computer. From there, you can Telnet to other routers that are accessible via the network.

a. From the command prompt on H1, telnet to the R2 router Fast Ethernet 0/0 interface.

```
C:\>telnet 192.168.2.1
```

b. Enter the password **cisco** to access the router.

c. What prompt did the router display? _____

d. Issue the **show version** command.

e. What is the Cisco IOS software version for the remote router R2? _______________

f. How many and what type of interfaces does remote router R2 have.? _____

g. If the Telnet from H1 to R2 is successful, what does that indicate about the OSI layer connectivity between the devices?

____

Step 2: End the Telnet session from H1 to remote router R2.

Exit the Telnet session from host H1 to R2 by typing **exit**.

Task 3: Perform Basic Telnet Operations Between the Routers

Step 1: Telnet from R1 to remote router R2.

Note: Telnet uses the vty lines on the remote router to connect. If the vty lines are not configured for login or there is no password set, you cannot connect to the remote router using Telnet.

a. Telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: Look at the interfaces on remote router R2.

a. Issue the **show ip interface brief** command at the remote router prompt.

```
R2>show ip interface brief
```

b. List the interfaces that are up on remote router R2. ___________________________________

Step 3: Display the routing table on the remote router.

Issue the **show ip route** command at the router prompt. Which routes has R2 learned from RIP?

____

```
R2>show ip route
```

Step 4: Display the CDP neighbors for R2.

a. Use the Cisco Discovery Protocol (CDP) to view information about Cisco devices directly attached to R2. Enter the **show cdp neighbors** command at the router prompt.

b. List all device IDs that are connected to the remote router. What is the platform for each device?

____

```
R2>show cdp neighbors
```

Step 5: Suspend the current Telnet session on R2.

a. Press **Ctrl-Shift-6,** and then press the **x** key. This action only suspends the session and returns to the previous router. It does not disconnect from this router.

b. What prompt did the router display? _______

Step 6: Resume the Telnet session to R2.

a. Press the **Enter** key at the router prompt. What does the router respond with?

____

Pressing the **Enter** key resumes the Telnet session that was previously suspended.

b. What prompt did the router display? _______

Step 7: Close the Telnet session to R2.

a. Terminate the Telnet session by typing **exit**..

b. What does the router respond with? ____

c. What prompt did the router display? _______

Note: When the Telnet session is suspended, you can disconnect from that session using the **disconnect** command and the session number.

Task 4: Perform Telnet Operations Between Multiple Routers

Step 1: Telnet from R1 to remote router R2.

a. From R1, telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

b. Use the password **cisco** to enter the router.

Step 2: Establish an additional Telnet session from R2 to R3.

a. From R2, telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

b. Use the password **cisco** to access the router.

c. What prompt did the router display? _______

Step 3: Suspend the Telnet session to R3.

a. Press **Ctrl-Shift-6,** and then press the **x** key.

b. What prompt did the router display? _______

Step 4: View the active Telnet sessions.

Enter the **show sessions** command at the R1 command prompt. How many sessions are in use? _____

Note: The default session is indicated by an asterisk (*). This is the session that resumes when you press **Enter**.

```
R2>show sessions
```

Step 5: Resume the Telnet session to R2.

a. Press **Enter** at the router prompt. What does the router respond with?

____

b. What prompt did the router display? _______

c. Why does the prompt say R3? ____

Step 6: Disconnect the sessions from R1 to R2 and R3.

a. Enter the **exit** command at the R3 prompt, and then press **Enter** to close the connection to R3.

```
R3>exit
[Connection to 172.16.1.2 closed by foreign host]
R2>
```

b. Suspend the R2 session from R1 (session 1 on R1) by pressing **Ctrl-Shift-6,** followed by the **x** key. Use the **disconnect** command to end the connection to R2.

```
R1>disconnect 1
Closing connection to 10.10.10.2 [confirm]
```

Task 4: Remove the vty Password from R3

Step 1: Telnet from R1 to remote router R3.

a. Telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

```
R1>telnet 172.16.1.2
Trying 172.16.1.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: From privileged EXEC mode on R3, remove the vty password.

a. Issue the **enable** command at the R3> command prompt, and enter the password **class**.

b. What prompt did the router display? _______

c. Remove the password for the vty lines on R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#no password
R3(config-line)#end
R3#
```

d. Exit from the Telnet session on R3, and return to R1.

```
R3#exit
[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Step 3: Telnet from R1 to remote router R3 again.

a. Telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

```
R1>telnet 172.16.1.2
```

b. Are you able to telnet to R3? _______

c. What message did you receive and why?

____

____

Step 4: Connect to R3 via the console and reset the vty password.

a. Issue the **enable** command at the R3> command prompt, and enter the password **class**.

b. Reestablish the password for the vty lines on R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#end
```

```
R3#
```

Part 2. Working with SSH to Verify Device Configurations and Connectivity

Secure Shell, or SSH, is an RSA-encrypted version of Telnet. All information, including user IDs, passwords, and data, that passes between an SSH client and SSH server is encrypted. Because SSH is an Application Layer protocol, a successful SSH connection demonstrates that all OSI layers are functioning, including encryption at the Presentation Layer.

Task 1: Configure SSH on Router R2

Step 1: Telnet from R1 to remote router R2.

a. Telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: Configure the SSH server on R2.

a. Create a domain name and a Telnet/SSH user ID and password for remote vty connections.

Note: By creating a user ID and password and specifying local login for the vty lines, any attempt to telnet or SSH to this router requires entry of the username and password created.

Because the admin user has a privilege level of 15 (the highest), and privilege level 15 is configured for the vty lines, the router prompt goes directly into privileged EXEC (enable) mode when connecting to R2 using either Telnet or SSH.

The use of a special user ID and password to secure Telnet and SSH vty access to the router does not affect the console (line con 0) password or the enable secret password.

```
Router#config terminal
R2(config)#ip domain-name customer.com
R2(config)#username admin privilege 15 password 0 cisco123
R2(config)#exit
```

b. Configure the vty terminal lines to accept incoming remote connections from Telnet and SSH clients, and validate the user ID against the local router username database.

```
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input telnet ssh
R2(config-line)#exit
```

Note: If Telnet is not specified in the **transport input** command above, only SSH remote connections will be allowed to this router.

c. 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.

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.customer.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512] 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
*Mar 20 13:17:50.123: %SSH-5-ENABLED: SSH 1.99 has been enabled

R2(config)#exit
```

d. Verify that SSH is enabled and the version used with the **show ip ssh** command.

```
R2#show ip ssh
```

e. Fill in the following information based on the output of the **show ip ssh** command.

SSH version enabled ____________________
Authentication timeout ___________________
Authentication retries ____________________

f. Issue the **show running-config** command. What indication is there that the SSH server has been configured on R2? ____

____

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

```
R2#copy running-config startup-config
```

h. Exit the Telnet session on R2, and return to R1.

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1#
```

Task 2: Log in to R2 Using the R1 CLI SSH Client

Note: You can also log in to an SSH-enabled router or switch using a computer with a GUI client, such as PuTTY. This procedure is described in Lab 8.3.4, “Configuring a Remote Router Using SSH.”

Step 1: Use the Cisco IOS CLI help feature with the ssh command.

From the R1 terminal session, use the Cisco IOS help feature to display the login options for the R1 SSH client.

```
R1#ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system

R1#ssh -l admin ?
  -c    Select encryption algorithm
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system
```

Step 2: Log in to R2 using SSH.

In this step, you log in to the R2 SSH server from the R1 CLI SSH client. You establish a secure remote session with R2 from which you can issue show and configuration commands.

a. Log in to R2 specifying the login username **admin** and password **cisco123,** which were configured earlier, and the IP address of the R2 S0/0/0 interface.

```
R1#ssh -l admin 10.10.10.2

Password:
Unauthorized Use Prohibited
R2#
```

b. Why did you get the privileged EXEC (enable) mode router prompt?

____

c. On R2, issue the **show ssh** command to see the SSH connections to the router.

```
R2#show ssh
Connection Version Mode Encryption   Hmac       State           Username
0          1.99     IN   aes128-cbc  hmac-sha1  Session started  admin
0          1.99     OUT  aes128-cbc  hmac-sha1  Session started  admin
%No SSHv1 server connections running.
```

d. Exit from the SSH session on R2, and return to R1

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1>
```

Note: Ctrl-Shift-6 followed by the **x** key, and the commands used previously with Telnet, are the same for SSH.

Task 3: Reflection

a. **HTTP Connectivity** - You can also verify Application Layer connectivity using the HTTP interface for a router or switch. If the command **ip http server** is present in the device running config, you can open a browser on a computer that has network connectivity to the router or switch IP address (or name, if DNS is enabled) and access the HTTP GUI management application in the device. This can be a basic HTTP interface for non-SDM routers or it can be SDM and SDM Express for SDM-enabled routers. Because HTTP is an Application Layer protocol, a successful HTTP connection demonstrates that all OSI layers are functioning.

b. Compare the advantages and disadvantages of Telnet and SSH.

____

____

____

c. If you can ping to a router interface but cannot connect to it using Telnet or SSH, what could the problem be, and which layers of the OSI model are affected?

____

____

____

Router Interface Summary

Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

Note: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.