Lab 2.5.2a Configure SSH

Objective

In this lab, the students will complete the following tasks:

Configuring a router as a Secure Shell (SSH) server Version 1.

Install and configure a SSH client on the Student PC.

Using show and debug commands to troubleshoot SSH

Strengthen SSH by configuring SSHv2.

Scenario

An IT administrator is concerned about using Telnet for remote administration. Therefore, the security policy has been updated and now requires the use of encrypted sessions for remote management sessions. The IT administrator must now configure SSH on the perimeter router.

Topology

This figure illustrates the lab network environment.
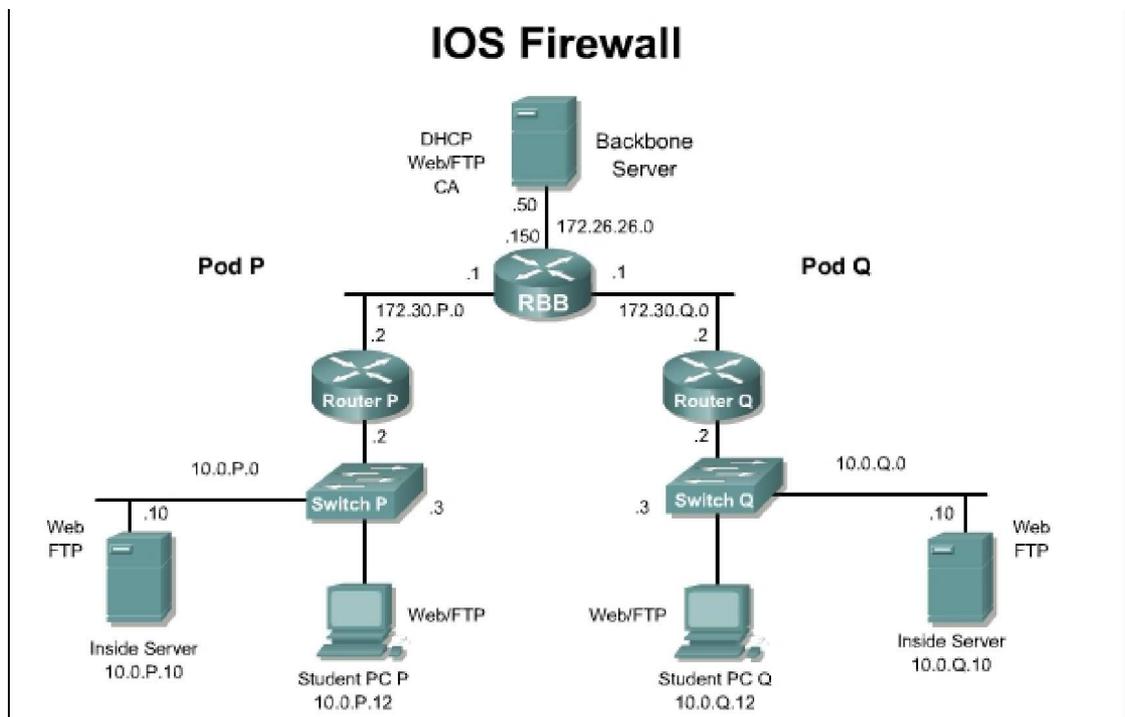
Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal

emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Prior to starting the lab, ensure that each host PC is loaded with a SSH client. There are numerous SSH clients available for free on the Internet. The lab was developed using the PuTTY SSH client.

 http://www.chiark.greenend.org.uk/~sgtatham/putty/

Tools and resources:

In order to complete the lab, the following is required:

Standard IOS Firewall lab topology

Console cable

HyperTerminal

SSH client

Further information about the objectives covered in this lab can be found at the following websites:

 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

 http://www.chiark.greenend.org.uk/~sgtatham/putty/

Command list

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
`crypto key generate rsa`	Generates Rivest, Shamir, and Adleman (RSA) key pairs.
`hostname`	This command changes the hostname of the router.
`ip domain-name`	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names.
`ip ssh`	Use the `ip ssh` command to configure Secure Shell (SSH) control parameters on the router. Use the `version` option to specify the SSH version.
`transport input`	Defines which protocols to use to connect to a specific line of the router.

Step 1 Configuring SSH on a Router

To enable SSH on the router, the following parameters should be configured:

Hostname

Domain-name

Asymmetrical keys

SSH timeouts

Local authentication

Version

b. Set router parameters

Begin by configuring the router hostname and domain-name using the following commands:

To configure the router hostname, use the **hostname** *hostname* command
in configuration mode. In this lab, the hostname has been configured to RouterP,
where P is the pod number. For example, if the team has been assigned to Pod 5 then
the hostname would be Router5.

```
RouterP(config)#hostname  RouterP
```

After the hostname is set, the active CLI will dynamically change.

To configure the router IP domain-name, use the **ip domain-name** *domain*
name command in Configuration Mode.

```
RouterP(config)#ip  domain-name  cisco.com
```

What command can be used to view both the hostname and IP domain name?

_____

Use the **ip ssh version 1** command to configure the router to use SSH version 1.

Step 2 Generate Asymmetric

Keys a. Generate RSA keys

Enter the following command in the configuration mode:

```
RouterP(config)#crypto  key  generate  rsa  ?
```

What are the available help options for this command?

_____

b. Generate RSA keys (continued)

To enable SSH for local and remote authentication on the router enter the command

crypto key generate rsa and press **Enter**. The router will respond with a message
showing the naming convention for the keys.

What is the default size, in bits, of the key modulus?

_____

Press **Enter** to accept the default key size and continue.

Step 3 Configure SSH Timeouts

a. Configuring SSH timeouts and authentication retries is a way of providing additional security
for the connection. Use the command **ip ssh {[time-out** *seconds***]}**
{authentication-retries integer} to enable timeouts and authentication retries.
Set the SSH timeout to 15 seconds and the amount of retries to 2 by entering the following
commands:

```
RouterP(config)#ip  ssh  time-out  15
RouterP(config)#ip  ssh  authentication-retries  2
```

1. What is the maximum timeout value allowed? What is the maximum amount
of authentication retries allowed?

_____

Step 4 Configure Local Authentication and vty

a. Use the following commands to define a local user and assign SSH communication to the
vty lines:

```
RouterP(config)#  username  student  password  cisco
RouterP(config)#  line  vty  0  4
RouterP(config-line)#  transport  input  ssh
RouterP(config-line)#  login  local
```

1. What are the available parameters for the `transport  input` command?

   _____

2. Why would you limit this only to SSH?

   _____

Step 5 Communicating Between a SSH PC (Client) to Router (Server)

The basic settings to allow a PC and a router to establish a SSH session are now configured.
In order to establish a SSH session, launch the SSH client from the student PC.

a. The configurations will vary between the different SSH clients. If PuTTY is being used as the SSH client, following these instructions. Launch the PuTTY.exe file and a pane with various configuration options will open.
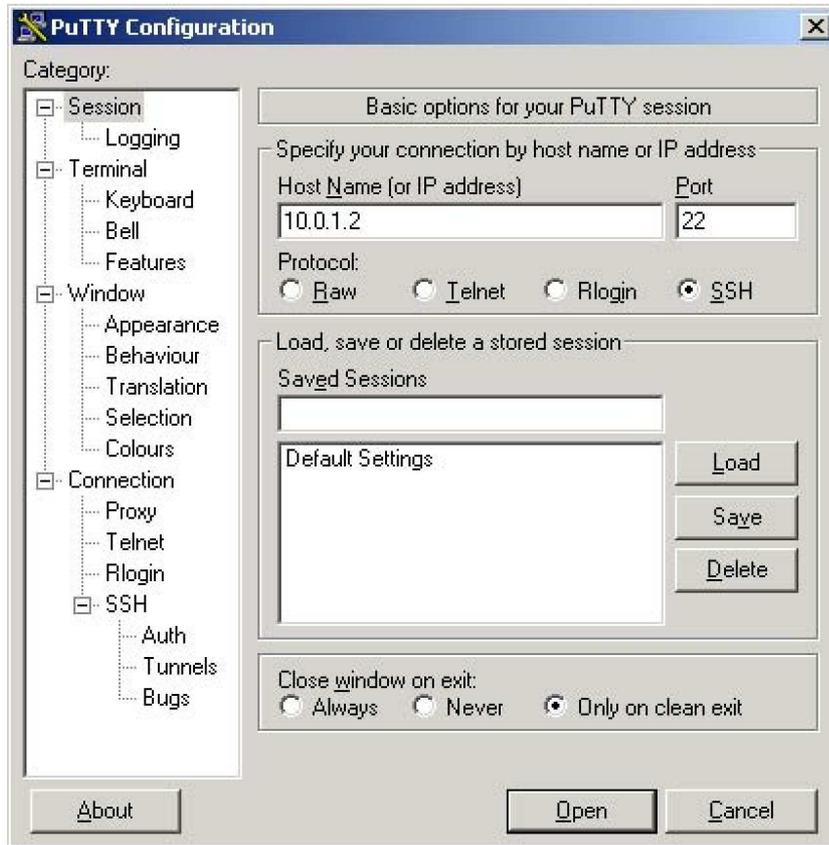
b. In the "Host Name (or IP address)" input box enter the IP address of the pod router. Next, make sure that radio button next to "SSH" is selected under "Protocol:". These two values must be sent to establish the SSH connection. To test the connection, press the **Open** command button at the bottom of the window.

c. The SSH client will prompt for the local username and password that was previously set on the Pod router. Enter the "**student**" for the username and "**cisco**" for the password.
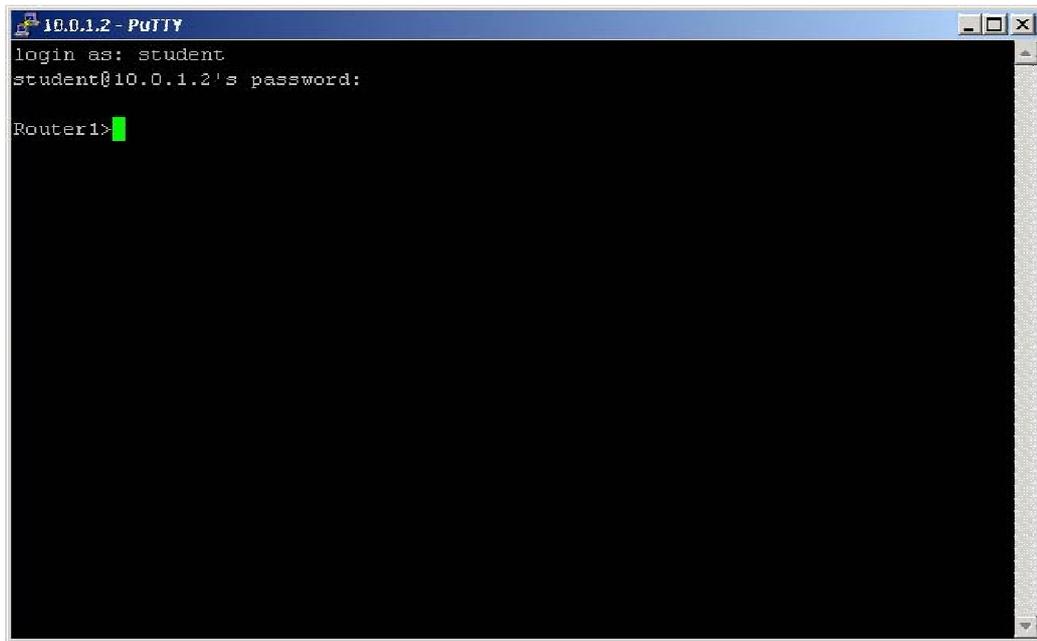
```
10.0.1.2 - PuTTY
login as: student
student@10.0.1.2's password:

Router1>
```

1. Was the SSH connection successful? If so, how is the prompt displayed?

_____

Step 6 Debug and Verify SSH

a. Enable debugging

   i. Enable debugging of SSH by entering the following commands:

```
RouterP(config)#logging on
RouterP(config)#logging console
RouterP#debug  ip  ssh
```

b. SSH debug output

   i. Next, open another instance of the SSH client and connect to the router. Use the correct username and password to log in to the router. The debug output should be similar to the output below.

```
03:45:37:  SSH1:  starting  SSH  control  process

03:45:37: SSH1: sent protocol version id SSH-1.5-Cisco-1.25

03:45:37: SSH1: protocol version id is - SSH-1.5-PuTTY-Release-

0.53b 03:45:37: SSH1: SSH_SMSG_PUBLIC_KEY msg

03:45:38:  SSH1:  SSH_CMSG_SESSION_KEY  msg  -  length  112,  type

0x03 03:45:38: SSH: RSA decrypt started

03:45:39:  SSH:  RSA  decrypt  finished

03:45:39:  SSH:  RSA  decrypt  started

03:45:39: SSH: RSA decrypt finished

03:45:39:  SSH1:  sending  encryption  confirmation

03:45:39:  SSH1:  keys  exchanged  and  encryption  on

03:45:41: SSH1: SSH_CMSG_USER message received

03:45:41:  SSH1:  authentication  request  for  userid  student
```

```
03:45:41:  SSH1:  SSH_SMSG_FAILURE  message  sent

03:45:44:  SSH1:  SSH_CMSG_AUTH_PASSWORD  message  received

03:45:44:  SSH1:  authentication  successful  for  student

03:45:44:  SSH1:  requesting  TTY

03:45:44: SSH1: setting TTY - requested: length 24, width 80;
set: length 24, width 80
03:45:44:  SSH1:  SSH_CMSG_EXEC_SHELL  message  received

03:45:44: SSH1: starting shell for vty03:45:37: SSH1: starting
SSH control process
```

ii. To get an idea of the debugging process and the debugging message, open another instance of the SSH client and intentionally enter the wrong username or password. View the debugging output for failed authentication. When you are done viewing the debugging output, use the **no debug ip ssh** command to stop debugging.

c. Viewing SSH sessions

   i. Use the **show ssh** command to view the active SSH sessions.

   ii. Fill in the appropriate values of the table below, based on the output of the **show ssh** command.

Connection	Version	Encryption	State	Username

   1. Is the SSHv2 server running?

   _____

d. Viewing SSH parameters

   i. To display the version information and SSH parameters, use the **show ip ssh** command.

   1. Is the output displayed exactly as the output below? If not, what are the differences?
```
RouterP#show  ip  ssh

SSH  Enabled  -  version  1.5
Authentication  timeout:  15  secs;  Authentication  retries:  3
```
   _____

   _____

   _____

e. End the SSH connection. From the router console, terminate the SSHv1 session.
```
RouterP#disconnect  ssh  0
```
   0 is the connection # which can be found in the output from the **show ssh** command.

Step 7 Configure SSH Version 2

a. SSH version 1 is more secure than telnet, however there are some cryptopgraphic weaknesses to SSHv1. Many devices now support SSHv2. Configuring SSHv2 is a way of providing additional security for the connection. Use the command **ip ssh version** to enable SSHv2.

> **Note:** If the IOS version in use does not support SSHv2, proceed to Step 7 to communicate between two routers using SSHv1.

```
RouterP(config)#ip ssh version
2 RouterP(config)#exit
RouterP#
```

b. Next, open another instance of the SSH client and connect to the router. Use the correct username and password to log in to the router. Use the **show ssh** command to view the active SSH sessions.

Fill in the appropriate values of the table below, based on the output of the **show   ssh** command.

Connection	Version	Encryption	Hmac	State	Username

1. Is the SSHv2 server running?

_____

c. End the SSH connection. From the router console, terminate the SSHv1 session.

```
RouterP#disconnect  ssh  0
```

0 is the connection # which can be found in the output from the **show   ssh** command.

Step 8 Router to Router SSH Connection

a. Confirm peer SSH configurations

i. Verbally communicate with the peer team to ensure the peer router Q has been configured to accept a SSH connection. Also, confirm the version of SSH. The settings configured in Steps 1 through 7 will be applicable to enable a SSH connection between two routers. Only this time, instead of using a SSH client running on a host computer, the router will be the SSH client and will establish a connection to the peer router. By default, the Cisco IOS will act as both a SSH server and SSH client.

b. Testing Telnet

i. When the peer group is ready, enter the **telnet** command and establish connectivity with the peer router.

```
RouterP#telnet 172.30.Q.2    (where  Q  is  the  peer  team  router)
```

1. Was the Telnet connection successful? Why or why not?

_____

_____

c. SSH parameters

    i. Enter the following commands to establish a SSH connection to the peer router:

      `RouterP(config)#`**`ssh  ?`**

      1. What are the additional arguments of the **`ssh`** command?

            _____

            _____

            _____

            _____

      2. What encryption algorithms are available?

            _____

d. Router to router SSH connection

    i. Enter the following command to establish a SSH connection to the peer router:

      `RouterP>`**`ssh –c  aes128-cbc  –l  student  172.30.Q.2`**

    This command makes a SSH connection to a peer router with an address of 172.30.Q.2, 128 bit AES as the encryption, and "student" as the login username. The password is "cisco".

      1. Was the SSH connection successful?

            _____

e. Verify SSH

    i. Enter the following command to verify the SSH connection:

      `RouterP#`**`show  ip  ssh`**

      `RouterP#`**`show  ssh`**

      1. What other commands could be useful to verify and troubleshoot SSH connections?

            _____

            _____

            _____