7.11.1

Setting Up SSH on a Cisco Router

```
SSH-ROUTER#
01:01:42: SSH0: starting SSH control process
01:01:42: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
01:01:42: SSH0: protocol version id is - SSH-1.5-PuTTY-Release-0.54
01:01:42: SSH0: SSH_SMSG_PUBLIC_KEY msg
01:01:51: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
01:01:51: SSH: RSA decrypt started
01:01:57: SSH: RSA decrypt finished
01:01:57: SSH: RSA decrypt started
01:02:00: SSH: RSA decrypt finished
01:02:00: SSH0: sending encryption confirmation
01:02:00: SSH0: keys exchanged and encryption on
01:02:04: SSH0: SSH_CMSG_USER message received
01:02:04: SSH0: authentication request for userid admin
01:02:04: SSH0: SSH_SMSG_FAILURE message sent
01:02:07: SSH0: SSH_CMSG_AUTH_PASSWORD message received
01:02:07: SSH0: authentication successful for admin
01:02:07: SSH0: requesting TTY
01:02:07: SSH0: setting TTY - requested: length 24, width 80; set: length 24
dth 80
01:02:07: SSH0: SSH_CMSG_EXEC_SHELL message received
```

Laboratory Overview

Objective

At the end of this lab students will be able to enable SSH on a Cisco router.

Information for Laboratory

A. Students will utilize Cisco routers running IPSEC cryptography IOS software.
B. Students will utilize PuTTY a SSH client for Windows.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

The routers being used need to have IP PLUS IPSEC 56, IP/FW PLUS IPSEC 56, or an IPSEC 3DES IOS image loaded, and each workstation must have HyperTerminal and PuTTY installed and working.

Warning[s]

Cisco IOS with IPSEC 56 or 3DES is necessary for SSH to run.

Estimated Completion Time

60 Minutes

Secure Shell (SSH)

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a command interface and protocol for securely gaining access to a remote host. It is widely used by network administrators to remotely control servers, routers, and other network equipment. SSH uses RSA public key cryptography for both connection and authentication.

Step 1: Verify cryptographic features on router

Console into the router, and enable Exec mode by issuing the 'enable' command. From the #exec prompt, issue the 'show version' command.

You should see the following within the output…

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

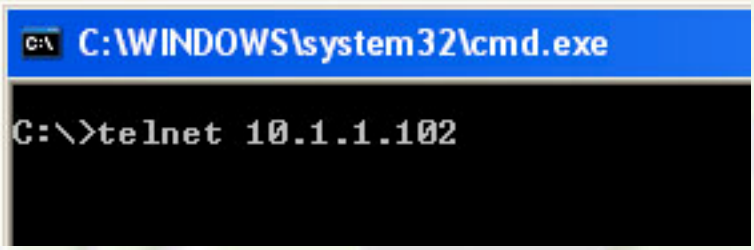
This verifies that the loaded IOS image contains the cryptography capabilities necessary to enable SSH on the router. If the above output is not displayed, an IOS upgrade is needed. Obtain the IP PLUS IPSEC 56 Cisco IOS image and load it on your router, or consult your instructor for further instructions.

Step 2: Testing authentication

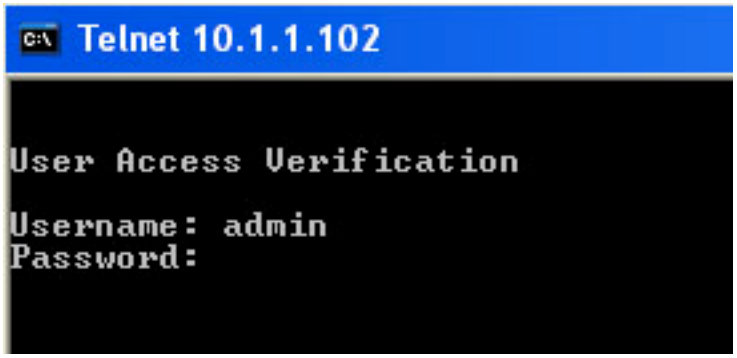
Enable exec mode, and enter config mode. From the Router(config)# prompt**…**

1. Set the Host name
    a. Enter ‘hostname SSH-ROUTER’
2. Set the Domain name
    a. Enter ‘ip domain-name testing.test’
3. Set the Enable secret
    a. Enter ‘enable secret 0 cisco’
4. Setup the User admin
    a. Enter ‘user admin password 0 cisco’
5. Setup the virtual terminals
    a. Enter ‘line vty 0 4’
    b. At the SSH-ROUTER(config-line)# prompt
    c. Enter ‘login local’

From your PC, telnet to your router



You should be prompted with User Access Verification. Enter the username admin and password cisco and press enter.



Step 3: Enabling SSH

From the Console session, enter exec mode, and config mode.
From the SSH-ROUTER(config)# prompt,
Enter ‘crypto key generate rsa’
When asked How many bits? Press enter to use default 512

You should see the following output

```
SSH-ROUTER(config)#crypto key generate rsa
The name for the keys will be: SSH-ROUTER.testing.test
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]:
Generating RSA keys ...
[OK]

SSH-ROUTER(config)#
00:30:11: %SSH-5-ENABLED: SSH 1.5 has been enabled
SSH-ROUTER(config)#
```

Verify that SSH is enabled, Enter ‘show ip ssh’

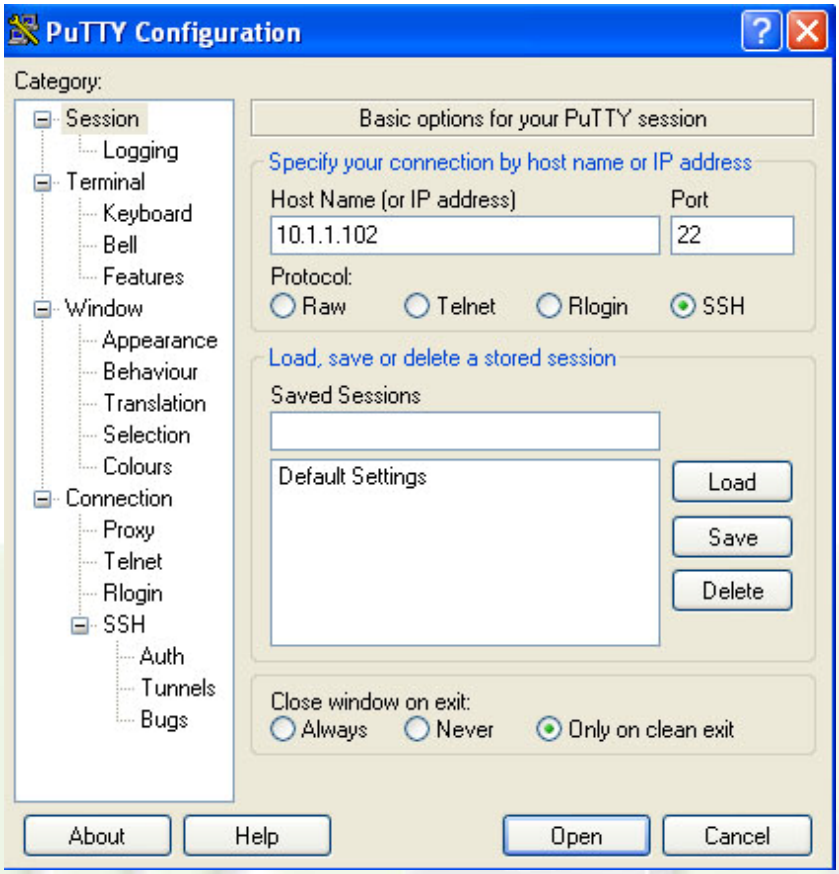
SSH-ROUTER#show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3

Enter ‘show crypto key mypubkey rsa’
You should see something similar to the following…

```
SSH-ROUTER#show cry key mypubkey rsa
% Key pair was generated at: 00:30:11 UTC Mar 1 1993
Key name: SSH-ROUTER.testing.test
 Usage: General Purpose Key
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B2190C E5F22742
  426FFEDD 756D26F0 3F304392 22978AC3 300D6645 F7D4D3DE A54E7B6C 65ABFC7D
  035774D2 3F97A6E8 C2C6EE30 775F9BA5 FAF24461 39F55453 EF020301 0001
% Key pair was generated at: 00:31:45 UTC Mar 1 1993
Key name: SSH-ROUTER.testing.test.server
 Usage: Encryption Key
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00CC7827 0BBEFB61
  2193607A 16CE41AF 3317AB0F EEAE3E0A 9BCB2917 29D4F31C E1FE26AD 4D9B307C
  CAFC90DA E52E20F2 0F1BD3F3 55028C4C 8348A6F8 723079C1 523C1B75 E7498832
  E3E7612C A8CF341F 1F8A5381 16A97263 3D1FE459 23415832 B1020301 0001
SSH-ROUTER#
```

Step 4: Connect via SSH from PC

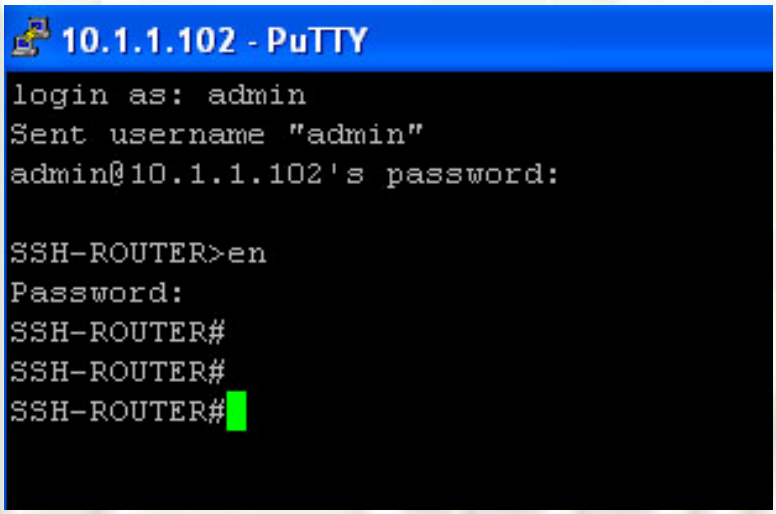
Locate and Launch PuTTY. Enter the IP address of your router, and check the SSH radio button, and click Open.



You will be alerted that the hosts key is not cached, this is because you have never connected via SSH to this host before, and do not have a copy of the key. Click Yes to continue.

Click yes when alerted of single-DES warning

You will then be prompted with login as: prompt. Enter the Username admin and password cisco.



Disconnect by entering ‘exit’ at the #prompt

Step 5: Debug the SSH Process

From the console, exec mode, Enter ‘debug ip ssh’

Slowly, step by step, Reconnect to the Router using PuTTY, as you watch the debug on the routers console.

Keep on eye on the console as you use PuTTY to SSH to the router. As soon as PuTTY makes a connection to the router

there will be some output displayed on the routers console.

Finish the connection and exit.

```
SSH-ROUTER#
01:01:42: SSH0: starting SSH control process
01:01:42: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
01:01:42: SSH0: protocol version id is - SSH-1.5-PuTTY-Release-0.54
01:01:42: SSH0: SSH_SMSG_PUBLIC_KEY msg
01:01:51: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
01:01:51: SSH: RSA decrypt started
01:01:57: SSH: RSA decrypt finished
01:01:57: SSH: RSA decrypt started
01:02:00: SSH: RSA decrypt finished
01:02:00: SSH0: sending encryption confirmation
01:02:00: SSH0: keys exchanged and encryption on
01:02:04: SSH0: SSH_CMSG_USER message received
01:02:04: SSH0: authentication request for userid admin
01:02:04: SSH0: SSH_SMSG_FAILURE message sent
01:02:07: SSH0: SSH_CMSG_AUTH_PASSWORD message received
01:02:07: SSH0: authentication successful for admin
01:02:07: SSH0: requesting TTY
01:02:07: SSH0: setting TTY - requested: length 24, width 80; set: length 24
dth 80
01:02:07: SSH0: SSH_CMSG_EXEC_SHELL message received
```

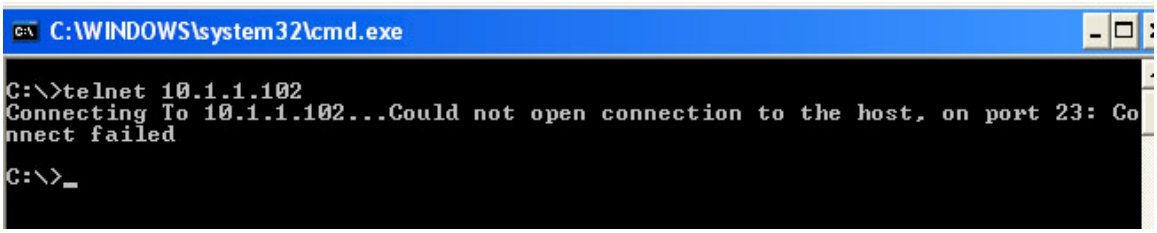
Enter the command ‘un all’ to stop debugging, and exit the console.

Step 6: Disable Telnet access

Once you have enabled SSH, we want to disable Telnet access.

1. Enter config mode for virtural terminals
    a. At the router(config)# prompt Enter ‘line vty 0 4’
2. At the router(config-line)# prompt
   Enter ‘transport input ssh’

Test the configuration by trying to Telnet to the router, your connection should be refused.



Try to SSH to the router, your connection should be accepted.

Analysis

1) For which applications is SSH connections best suited?

2) After working with these utilities, what about SSH do you feel you should study further? Why?

3) Why should you use an SSH connection versus a Telnet connection?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

This lab was developed using PuTTY beta 0.57, which can be obtained from:

www.chiark.greenend.org.uk

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).