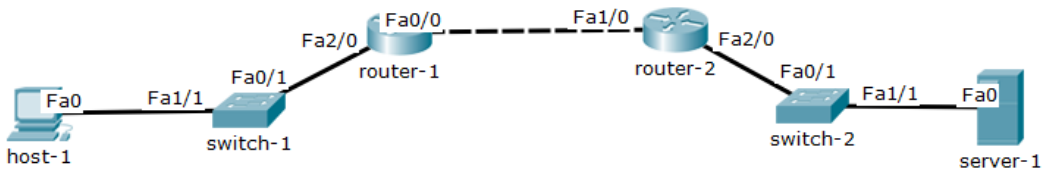
Secure Shell (SSHv2)

Lab Summary

Configure and verify SSHv2 remote management access on router-2.

Figure 1 Lab Topology



Lab Configuration

Start Packet Tracer File: **SSHv2**

Step 1: Click *Router-2* icon and select the *CLI* folder. Press <enter> key for user mode prompt.

Step 2: Enter global configuration mode.

router-2 > **enable**
router-2# **configure terminal**

Step 3: Enable password encryption so that passwords are not readable from the configuration script.

router-2(config)# **service password-encryption**

Step 4: Configure username account cisco with privilege level 15 and secret password ccnalabs for SSH remote authentication.

router-2(config)# **username cisco privilege 15 secret ccnalabs**

Step 5: Enable SSH (encrypted) remote management access to router-2.

router-2(config)# **ip domain-name lab.cisconet.com**
router-2(config)# **crypto key generate rsa**
[type ***yes*** *to create key*]
bits? [***768***]
router-2(config)# **ip ssh version 2**
router-2(config)# **ip ssh time-out 60**

Step 6: Allow SSH protocol access only to router-2 for security purposes.

router-2#(config)# **line vty 0 4**
router-2#(config-line)# **login local**
router-2#(config-line)# **transport input ssh**
router-2(config-line)# **end**
router-# **copy running-config startup-config**

Step 7: Verify Lab

Start an SSHv2 session from host-1 to router-2 and confirm there is remote access. Attempt to access router-2 with Telnet and verify that it is denied to that router.

SSH from host-1 to router-2 with the following commands.

c:\> **ssh –l cisco 192.168.2.2**
Open
Password: **ccnalabs**
router-2# **exit**

Telnet from host-1 to router-2 and verify that access is denied.

c:\> **telnet 192.168.2.2**

Trying 192.168.2.2 ...Open

[Connection to 192.168.2.2 closed by foreign host]