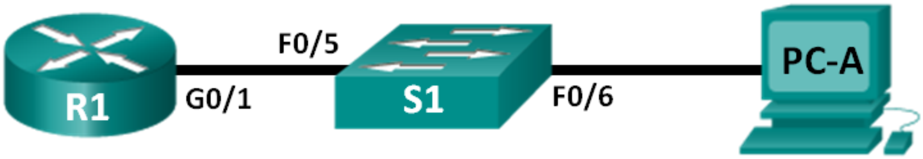
Lab - Accessing Network Devices with SSH (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure the Router for SSH Access

Part 3: Examine a Telnet Session with Wireshark

Part 4: Examine a SSH Session with Wireshark

Part 5: Configure the Switch for SSH Access

Part 6: SSH from the CLI on the Switch

Background / Scenario

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 device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

For SSH to function, the network devices communicating must be configured to support it. In this lab, you will 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.

In this lab, you will configure a router to accept SSH connectivity, and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH. You will also be challenged to configure a switch for SSH connectivity on your own.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used.

Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

a. Console into the router and enable privileged EXEC mode.

b. Enter configuration mode.

c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

d. Assign **class** as the privileged EXEC encrypted password.

e. Assign **cisco** as the console password and enable login.

f. Assign **cisco** as the vty password and enable login.

g. Encrypt the plain text passwords.

h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

i. Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.

j. Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

a. Configure PC-A with an IP address and subnet mask.

b. Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk, because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part in the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

a. Configure device name.

```
Router(config)# hostname R1
```

b. Configure the domain for the device.

```
R1(config)# ip domain-name ccna-lab.com
```

Step 2: Configure the encryption key method.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 3: Configure a local database username.

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

Note: A privilege level of 15 gives the user administrator rights.

Step 4: Enable SSH on the VTY lines.

a. Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

b. Change the login method to use the local database for user verification.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Step 5: Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Part 3: Examine a Telnet Session with Wireshark

In Part 3, you will use Wireshark to capture and view the transmitted data of a Telnet session on the router. You will use Tera Term to telnet to R1, sign in, and then issue the show run command on the router.

Note: If a Telnet/SSH client software package is not installed on your PC, you must install one before continuing. Two popular freeware Telnet/SSH packages are Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) and PuTTy (www.putty.org).

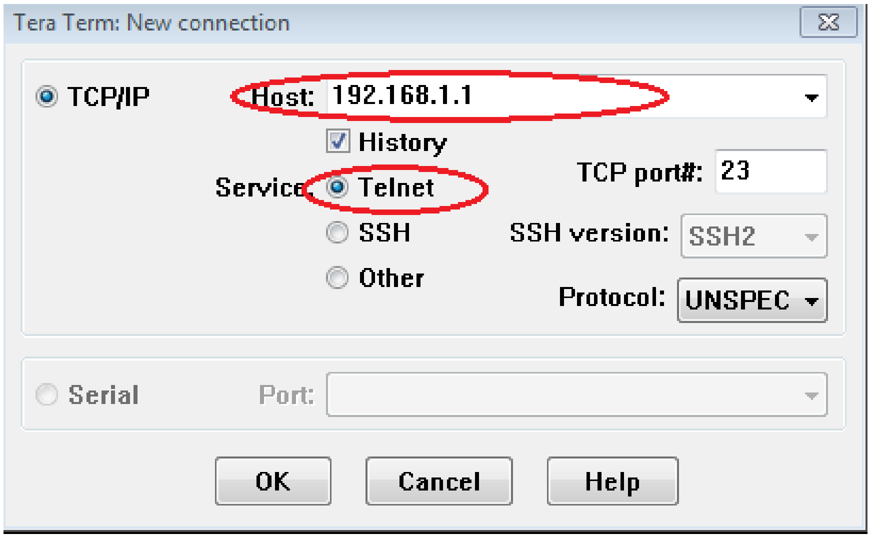
Note: Telnet is not available from the command prompt in Windows 7, by default. To enable Telnet for use in the command prompt window, click **Start** > **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off**. Click the **Telnet Client** check box, and then click **OK**.

Step 1: Open Wireshark and start capturing data on the LAN interface.

Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the **Run as Administrator** option.

Step 2: Start a Telnet session to the router.

a. Open Tera Term and select the **Telnet** Service radio button and in the Host field, enter **192.168.1.1**.



Tera Term: New connection

● TCP/IP Host: 192.168.1.1

☑ History

Service: ● Telnet ○ SSH ○ Other

TCP port#: 23

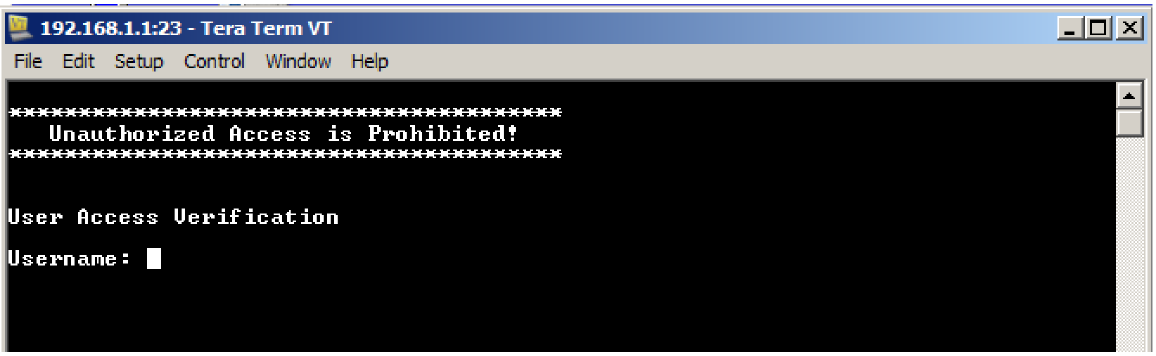
SSH version: SSH2

Protocol: UNSPEC

○ Serial Port:

What is the default TCP port for Telnet sessions? ________________ Port 23

b. At the Username: prompt, enter **admin** and at the Password: prompt, enter **adminpass**. These prompts are generated because you configured the VTY lines to use the local database with the **login local** command.


192.168.1.1:23 - Tera Term VT
File Edit Setup Control Window Help

```
*********************************************
   Unauthorized Access is Prohibited!
*********************************************


User Access Verification

Username:
```

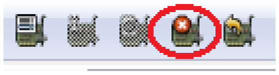
c. Issue the **show run** command.

```
R1# show run
```

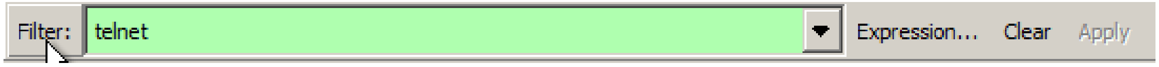
d. Enter **exit** to exit the Telnet session and out of Tera Term.

```
R1# exit
```

Step 3: Stop the Wireshark capture.



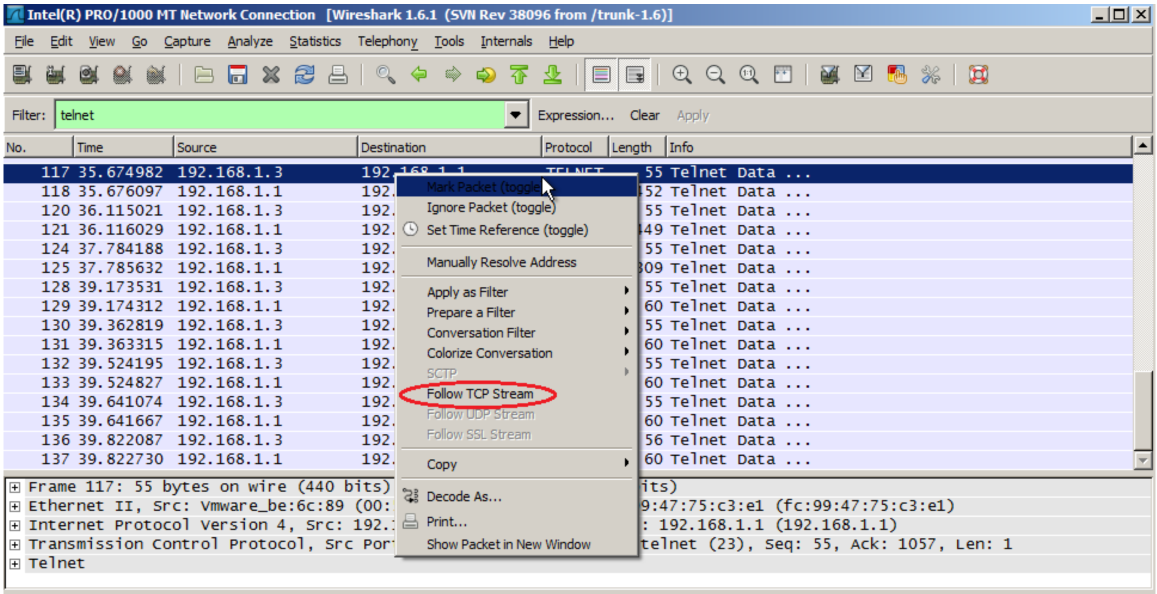
Step 4: Apply a Telnet filter on the Wireshark capture data.



Filter: telnet

Step 5: Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

a. Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and in the drop-down list, select **Follow TCP Stream**.

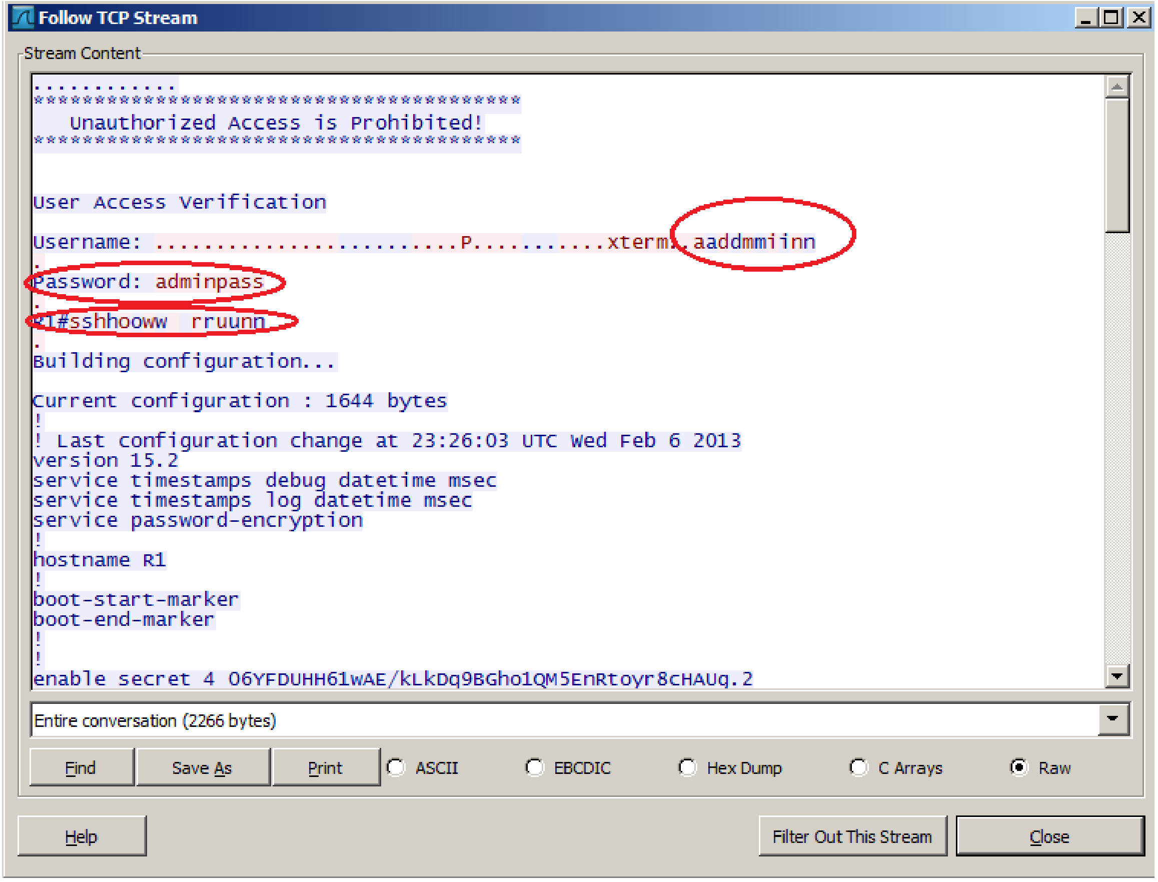


Filter: telnet

```
No.    Time       Source       Destination  Protocol Length Info
  117 35.674982 192.168.1.3   192.168.1.1  TELNET      55 Telnet Data ...
  118 35.676097 192.168.1.1   192.                     152 Telnet Data ...
  120 36.115021 192.168.1.3   192.                      55 Telnet Data ...
  121 36.116029 192.168.1.1   192.                     149 Telnet Data ...
  124 37.784188 192.168.1.3   192.                      55 Telnet Data ...
  125 37.785632 192.168.1.1   192.                     309 Telnet Data ...
  128 39.173531 192.168.1.3   192.                      55 Telnet Data ...
  129 39.174312 192.168.1.1   192.                      60 Telnet Data ...
  130 39.362819 192.168.1.3   192.                      55 Telnet Data ...
  131 39.363315 192.168.1.1   192.                      60 Telnet Data ...
  132 39.524195 192.168.1.3   192.                      55 Telnet Data ...
  133 39.524827 192.168.1.1   192.                      60 Telnet Data ...
  134 39.641074 192.168.1.3   192.                      55 Telnet Data ...
  135 39.641667 192.168.1.1   192.                      60 Telnet Data ...
  136 39.822087 192.168.1.3   192.                      56 Telnet Data ...
  137 39.822730 192.168.1.1   192.                      60 Telnet Data ...

⊞ Frame 117: 55 bytes on wire (440 bits)                its)
⊞ Ethernet II, Src: Vmware_be:6c:89 (00:                9:47:75:c3:e1 (fc:99:47:75:c3:e1)
⊞ Internet Protocol Version 4, Src: 192.                : 192.168.1.1 (192.168.1.1)
⊞ Transmission Control Protocol, Src Por                telnet (23), Seq: 55, Ack: 1057, Len: 1
⊞ Telnet
```

b. The Follow TCP Stream window displays the data for your Telnet session with the router. The entire session is displayed in clear text, including your password. Notice that the username and **show run** command that you entered are displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



```
............
****************************************
   Unauthorized Access is Prohibited!
****************************************


User Access Verification

Username: ........................P..........xterm..aaddmmiinn
.
Password: adminpass
.
R1#sshhooww  rruunn
.
Building configuration...

Current configuration : 1644 bytes
!
! Last configuration change at 23:26:03 UTC Wed Feb 6 2013
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

Entire conversation (2266 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

c. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

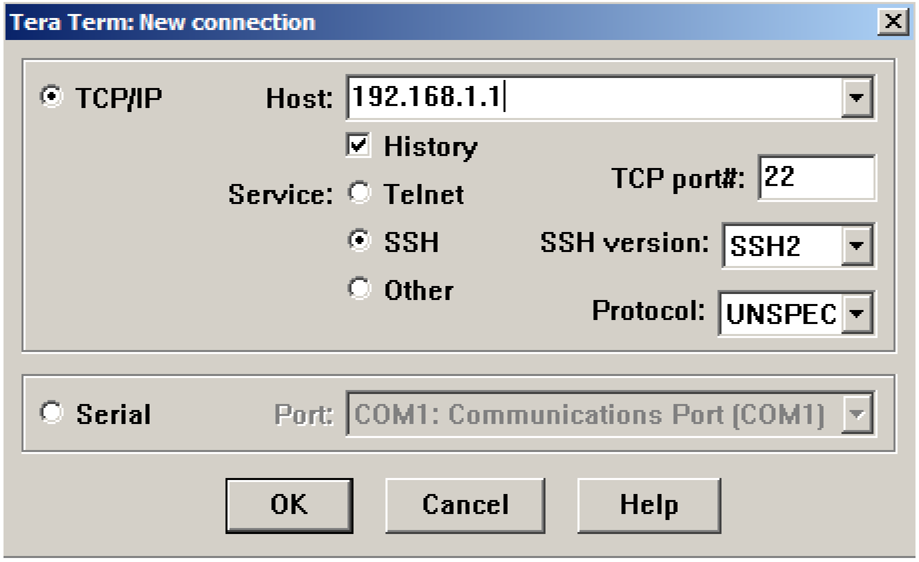
Part 4: Examine an SSH session with Wireshark

In Part 4, you will use the Tera Term software to establish an SSH session with the router. Wireshark will be used to capture and view the data of this SSH session.

Step 1: Open Wireshark and start capturing data on the LAN interface.

Step 2: Start an SSH session on the router.

a. Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.



● TCP/IP Host: 192.168.1.1

☑ History

Service: ○ Telnet

● SSH

○ Other

TCP port#: 22

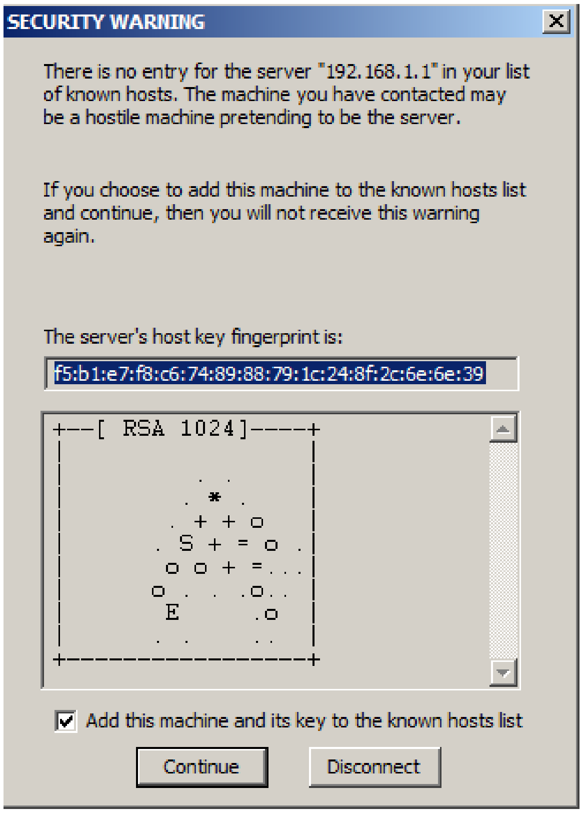
SSH version: SSH2

Protocol: UNSPEC

○ Serial Port: COM1: Communications Port (COM1)

What is the default TCP port used for SSH sessions? ________________ Port 22

b. The first time you establish a SSH session to a device, a **SECURITY WARNING** is generated to let you know that you have not connected to this device before. This message is part of the authentication process. Read the security warning and then click **Continue**.



There is no entry for the server "192.168.1.1" in your list of known hosts. The machine you have contacted may be a hostile machine pretending to be the server.

If you choose to add this machine to the known hosts list and continue, then you will not receive this warning again.

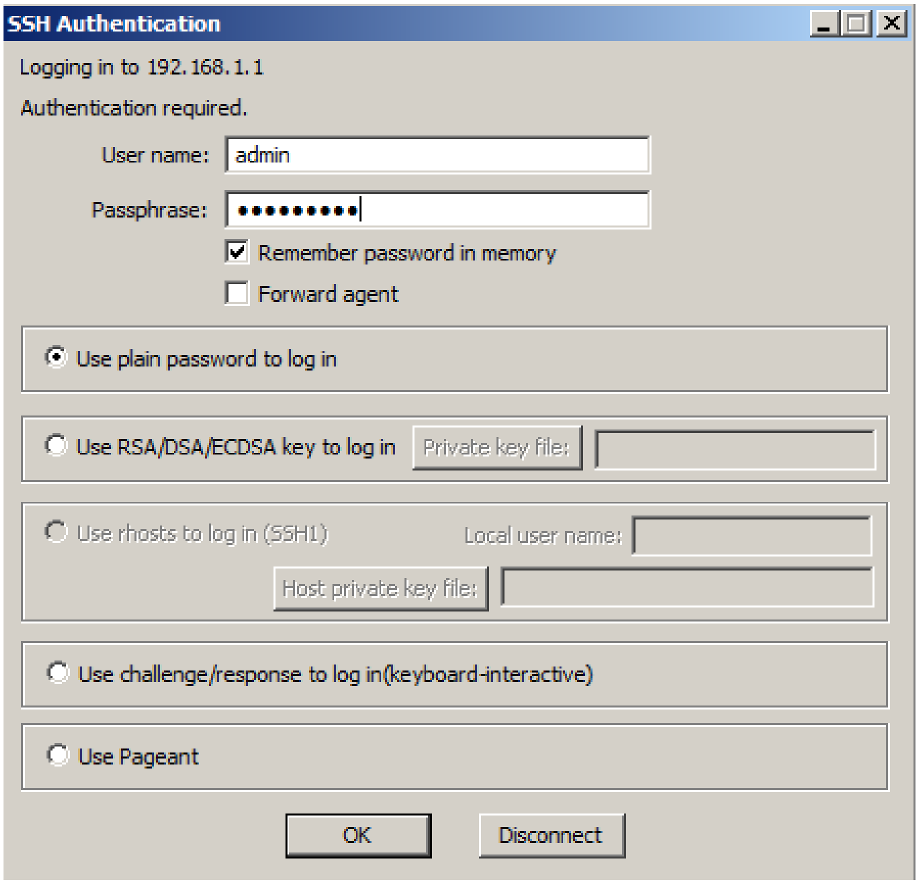
The server's host key fingerprint is:

f5:b1:e7:f8:c6:74:89:88:79:1c:24:8f:2c:6e:6e:39

```
+--[ RSA 1024]----+
|                 |
|         . .     |
|        . * .    |
|       . + + o   |
|      . S + = o .|
|       o o + =...|
|      o . . .o.. |
|       E     .o  |
|      . .    ..  |
+-----------------+
```

☑ Add this machine and its key to the known hosts list

c. In the SSH Authentication window, enter **admin** for the username and **adminpass** for the passphrase. Click **OK** to sign into the router.



SSH Authentication

Logging in to 192.168.1.1

Authentication required.

User name: admin

Passphrase: ●●●●●●●●●●

☑ Remember password in memory

□ Forward agent

● Use plain password to log in

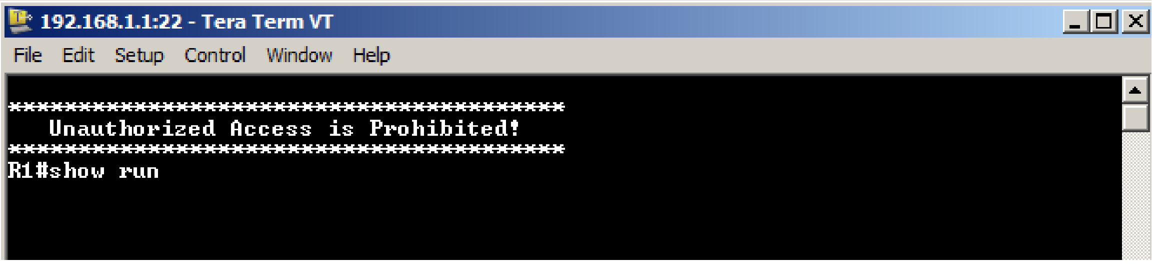
○ Use RSA/DSA/ECDSA key to log in

○ Use rhosts to log in (SSH1)

○ Use challenge/response to log in(keyboard-interactive)

○ Use Pageant

d. You have established a SSH session on the router. The Tera Term software looks very similar to a command window. At the command prompt, issue the **show run** command.

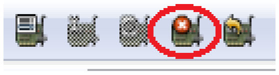


```
*****************************************************
   Unauthorized Access is Prohibited!
*****************************************************
R1#show run
```

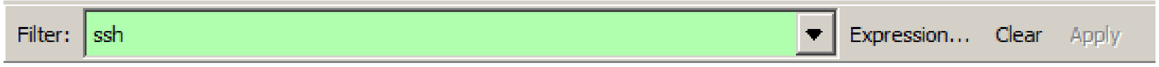
e. Exit the SSH session and out of Tera Term by issuing the **exit** command.

```
R1# exit
```

Step 3: Stop the Wireshark capture.



Step 4: Apply an SSH filter on the Wireshark Capture data.

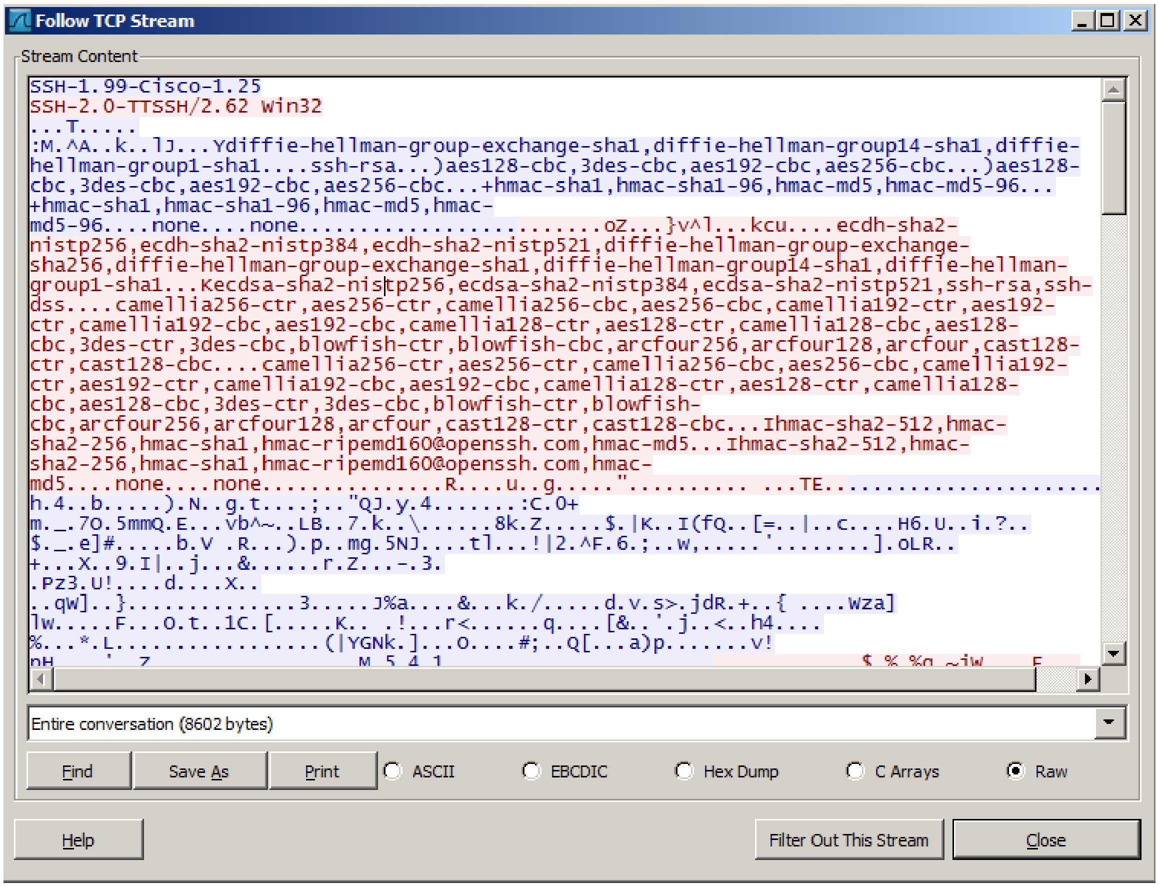


Filter: ssh

Step 5: Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

a. Right-click one of the **SSHv2** lines in the **Packet list** section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.

b. Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



```
SSH-1.99-Cisco-1.25
SSH-2.0-TTSSH/2.62 Win32
...T.....
:M.^A..k..lJ...Ydiffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-
hellman-group1-sha1....ssh-rsa...)aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc...)aes128-
cbc,3des-cbc,aes192-cbc,aes256-cbc...+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96...
+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96....none....none..........................oZ...}v^l...kcu....ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group1-sha1...Kecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-
dss....camellia256-ctr,aes256-ctr,camellia256-cbc,aes256-cbc,camellia192-ctr,aes192-
ctr,camellia192-cbc,aes192-cbc,camellia128-ctr,aes128-ctr,camellia128-cbc,aes128-
cbc,3des-ctr,3des-cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-
ctr,cast128-cbc....camellia256-ctr,aes256-ctr,camellia256-cbc,aes256-cbc,camellia192-
ctr,aes192-ctr,camellia192-cbc,aes192-cbc,camellia128-ctr,aes128-ctr,camellia128-
cbc,aes128-cbc,3des-ctr,3des-cbc,blowfish-ctr,blowfish-
cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128-cbc...Ihmac-sha2-512,hmac-
sha2-256,hmac-sha1,hmac-ripemd160@openssh.com,hmac-md5...Ihmac-sha2-512,hmac-
sha2-256,hmac-sha1,hmac-ripemd160@openssh.com,hmac-
md5....none....none...............R....u..g....."..........  ...TE.......................
h.4..b.....).N..g.t....;.."QJ.y.4.......:C.O+
m._.7O.5mmQ.E...vb^~..LB..7.k..\......8k.Z.....$.|K..I(fQ..[=..|..c....H6.U..i.?..
$._.e]#.....b.V .R...).p..mg.5NJ....tl...!|2.^F.6.;..w,.....'........].oLR..
+...X..9.I|..j...&......r.Z...-.3.
.Pz3.U!....d....X..
..qw]..}..............3.....J%a....&...k./.....d.v.s>.jdR.+..{ ....wza]
lw.....F...O.t..1C.[.....K..  .!...r<......q....[&..'.j..<..h4....
%...*.L.................(|YGNk.]...O....#;..Q[...a)p.......v!
```

Entire conversation (8602 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Why is SSH preferred over Telnet for remote connections?

____

____

Answers may vary. SSH will authenticate with a device and let you know if you are connecting to this device for the first time. It will also secure the session by encrypting all the data.

c. After examining your SSH session, click **Close**.

d. Close Wireshark.

Part 5: Configure the Switch for SSH Access

In Part 5, you are to configure the switch in the topology to accept SSH connections. Once the switch has been configured, establish a SSH session on it using Tera Term.

Step 1: Configure the basic settings on the switch.

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

Step 3: Establish a SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on the S1.

Step 4: Troubleshoot as necessary.

Are you able to establish a SSH session with the switch?

____

Yes. SSH can be configured on a switch using the same commands that were used on the router.

Part 6: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 6, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (**?**) to display the parameter options available with the **ssh** command.

```
S1# 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
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Step 2: SSH to router R1 from S1.

a. You must use the **–l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
***********************************************
  Warning: Unauthorized Access is Prohibited!
***********************************************

R1#
```

b. You can return to S1 without closing your SSH session to R1 by pressing **Ctrl**+**Shift**+**6**. Release the **Ctrl**+**Shift**+**6** keys and press **x**. You should see the switch privilege EXEC prompt display.

```
R1#
```

```
S1#
```

c. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

What versions of SSH are supported from the CLI?

Answers may vary, but this can be determined by using the **ssh –v ?** on the command line. The 2960 switch running IOS version 15.0(2) supports SSH v1 and V2.

```
S1# ssh -v ?
  1  Protocol Version 1
  2  Protocol Version 2
```

Reflection

How would you provide multiple users, each with their own username, access to a network device?

Answers may vary. You would add each user’s username and password to the local database using the username command. It is also possible to use a RADIUS or TACACS server, but this has not been covered yet.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table 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 string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configs - Final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
!
```

```
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Connection to S1-F0/5.
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^C
****************************************
   Unauthorized Access is Prohibited!
****************************************
^C
!
line con 0
 password 7 00071A150754
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0
 password 7 110A1016141D
 login local
 transport input telnet ssh
line vty 1 4
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
```

```
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
!
banner motd ^C
****************************************
  Unauthorized Access is Prohibited!
****************************************
^C
```

```
!
line con 0
 password 7 060506324F41
 login
line vty 0 4
 password 7 060506324F41
 login local
 transport input telnet ssh
line vty 5 15
 password 7 00071A150754
 login local
 transport input telnet ssh
!
end
```