Laboratory_19: Configure Network Devices with SSH.

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	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

- Configure Basic Device Settings
- Configure the Router for SSH Access
- Configure the Switch for SSH Access
- SSH from the CLI on the Switch

Background / Scenario

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.

The network devices that are communicating must be configured to support SSH in order for SSH to function. 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.

Initialize and reload the router and switch.

Instructions for Packet Tracer:

On Switch:

```
switch# delete flash:vlan.dat
switch# erase startup-config
switch# reload
```

On Router:

```
router# erase startup-config
router# reload
```

Configure the router

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

```
router> enable
router# configure terminal
```

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

```
router(config)# no ip domain-lookup
```

c. Assign class as the privileged EXEC encrypted password.

```
router(config)# enable secret class
```

d. Assign cisco as the console password and enable login.

```
router(config)# line console 0
router(config-line)# password cisco
router(config-line)# login
```

e. Assign cisco as the VTY password and enable login.

```
router(config)# line vty 0 4
router(config-line)# password cisco
router(config-line)# login
```

f. Encrypt the plaintext passwords.

```
router(config)# service password-encryption
```

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

```
router(config)# banner motd $ Authorized Users Only! $
```

h. Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.

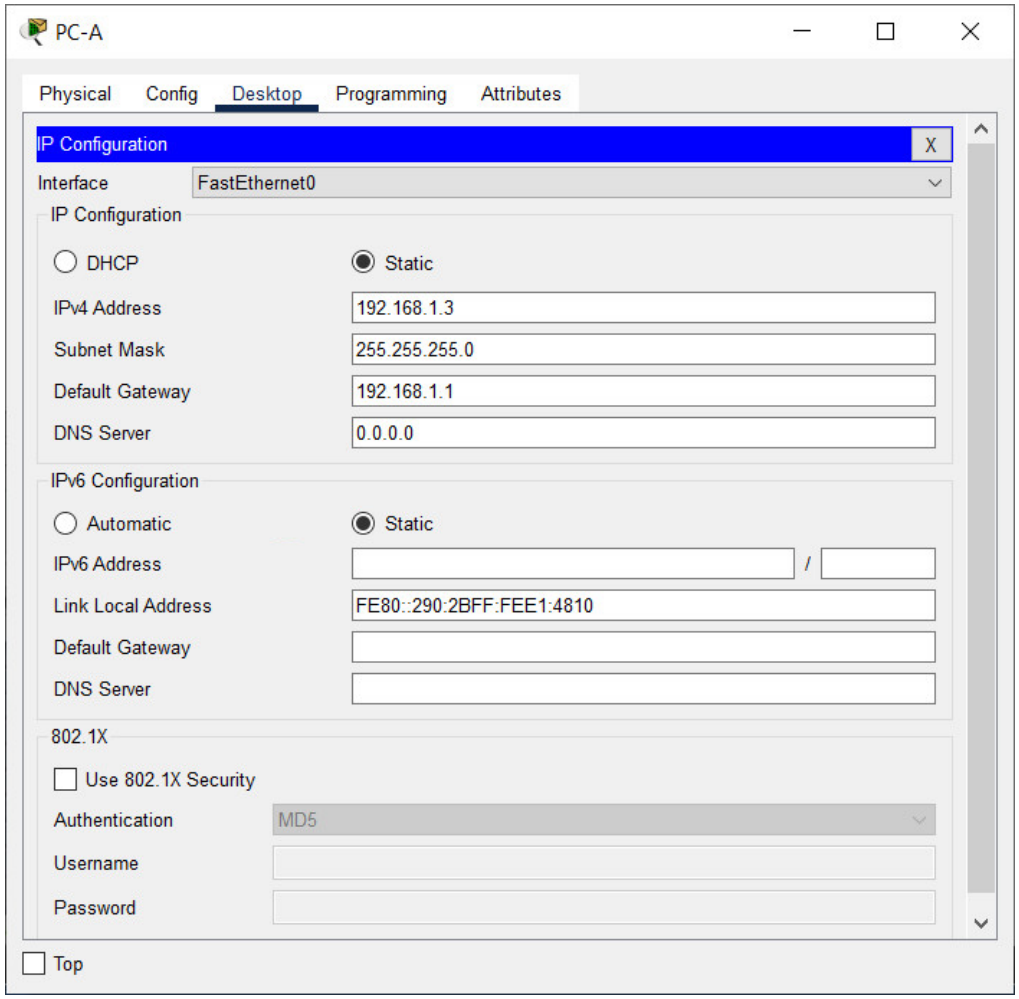
```
router(config)# interface g0/0/1
router(config-if)# ip address 192.168.1.1 255.255.255.0
router(config-if)# no shutdown
```

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

```
router# copy running-config startup-config
```

Configure PC-A.

a. Configure PC-A with an IP address and subnet mask.
b. Configure a default gateway for PC-A.



Configure the Router for SSH Access

a. Configure device name.

router(config)# hostname R1

b. Configure the domain for the device

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

c. Configure the encryption key method.

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
```

d. Configure a local database username.

```
R1(config)# username admin secret Adm1nP@55
```

e. Enable SSH on the VTY lines.

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

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

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

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

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

h. Establish an SSH connection to the router.

- Start Tera Term from PC-A.
- Establish an SSH session to R1. Use the username admin and password Adm1nP@55. You should be able to establish an SSH session with R1.

Configure the Switch for SSH Access

a. Configure the basic settings on the switch. Console into the switch and enable privileged EXEC mode.

```
switch> enable
```

b. Enter configuration mode.

```
switch# configure terminal
```

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

```
switch(config)# no ip domain-lookup
```

d. Assign class as the privileged EXEC encrypted password.

```
switch(config)# enable secret class
```

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

```
switch(config)# line console 0
switch(config-line)# password cisco
switch(config-line)# login
```

f. Assign cisco as the VTY password and enable login.

```
switch(config)# line vty 0 15
switch(config-line)# password cisco
switch(config-line)# login
```

g. Encrypt the plain text passwords.

   switch(config)# service password-encryption

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

   switch(config)# banner motd $ Authorized Users Only! $

i. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.

   switch(config)# interface vlan 1
   switch(config-if)# ip address 192.168.1.11 255.255.255.0
   switch(config-if)# no shutdown

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

   Switch# copy running-config startup-config

k. Configure the switch for SSH connectivity. Configure the device name as listed in the Addressing Table.

   switch(config)# hostname S1

l. Configure the domain for the device.

   S1(config)# ip domain-name ccna-lab.com

m. Configure the encryption key method.

   S1(config)#crypto key generate rsa
   The name for the keys will be: S1.ccna-lab.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#

n. Configure a local database username.

S1(config)# username admin secret Adm1nP@55

o. Enable Telnet and SSH on the VTY lines.

S1(config)# line vty 0 15
S1(config-line)# transport input ssh

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

S1(config-line)# login local
S1(config-line)# end

q. Establish an SSH connection to the switch.

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

SSH From the CLI on the Switch

a. View the parameters available for the Cisco IOS SSH client.

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

b. SSH to R1 from S1.

You must use the –l admin option when you SSH to R1. This allows you to log in as user admin. When prompted, enter Adm1nP@55 for the password.

S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>

Device Configs – Final

- **Router R1**

```
enable
configure terminal
no ip domain-lookup
enable secret class

line console 0
password cisco
login
exit

line vty 0 4
password cisco
login
exit

service password-encryption
banner motd $ Authorized Users Only! $
interface g0/0/1
```

```
ip address 192.168.1.1 255.255.255.0
no shutdown
exit

hostname R1
ip domain name ccna-lab.com
crypto key generate rsa
1024

username admin secret Adm1nP@55

line vty 0 4
transport input ssh
login local
end

copy running-config startup-config
```

- **Switch S1**

```
en
conf t
no ip domain-lookup
enable secret class
line con 0
pass cisco
login
exit

line vty 0 15
pass cisco
login
exit

service password-encryption
banner motd $ Authorized Users Only! $
```

```
interface vlan 1
ip address 192.168.1.11 255.255.255.0
no sh
exit

hostname S1
ip domain-name ccna-lab.com

crypto key generate rsa
1024

username admin secret Adm1nP@55

line vty 0 15
transport input ssh
login local
end

copy running-config startup-config
```