

Configuration of SSH on a Cisco Switch or Router

Verify the Switch Supports SSH

Screenshots are taken in Packet Tracer using Catalyst 2960

To enable SSH on a Catalyst 2960 switch, the switch must be using a version of the IOS software including cryptographic (encrypted) features and capabilities. Use the **show version** command on the switch to see which IOS the switch is currently running. An IOS filename that includes the combination “k9” supports cryptographic (encrypted) features and capabilities. The example shows the output of the **show version** command.

```
3 Switch>show version
4 Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
5 Technical Support: http://www.cisco.com/techsupport
```

Step 1

Configure SSH

Before configuring SSH, the switch must be minimally configured with a unique hostname and the correct network connectivity settings.

```
66 Switch>show ip ssh
67 SSH Disabled - version 1.99
68 %Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
69 Authentication timeout: 120 secs; Authentication retries: 3
```

Step 2

Configure the IP domain.

Configure the IP domain name of the network using the **ip domain-name domain-name** global configuration mode command. In the figure, the *domain-name* value is **myname.org**.

```
70 Switch>enable
71 Switch#configure terminal
72 Enter configuration commands, one per line. End with CNTL/Z.
73 Switch(config)#ip domain name mydomain
```

Step 3

Generate RSA key pairs.

Not all versions of the IOS default to SSH version 2, and SSH version 1 has known security flaws. To configure SSH version 2, issue the **ip ssh version 2** global configuration mode command. Generating an RSA key pair automatically enables SSH. Use the **crypto key generate rsa** global configuration mode command to enable the SSH server on the switch and generate an RSA key pair. When generating RSA keys, the administrator is prompted to enter a modulus length. The sample configuration in the figure uses a modulus size of 1,024 bits. A longer modulus length is more secure, but it takes longer to generate and to use.

Note: To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration mode command. After the RSA key pair is deleted, the SSH server is automatically disabled.

```
Switch(config)#hostname mySwitch1
mySwitch1(config)#crypto key generate rsa
The name for the keys will be: mySwitch1.mydomain
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]
```

Step 4

Configure user authentication.

The SSH server can authenticate users locally or using an authentication server. To use the local authentication method, create a username and password pair using the **username *secret password*** global configuration mode command. In the example, the user admin is assigned the password **mysecret**.

```
84 mySwitch1(config)#username admin secret mysecret
85 *Mar 1 0:11:42.933: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 5

Configure the vty lines.

Enable the SSH protocol on the vty lines by using the **transport input ssh** line configuration mode command. The Catalyst 2960 has vty lines ranging from 0 to 15. This configuration prevents non-SSH (such as Telnet) connections and limits the switch to accept only SSH connections. Use the **line vty** global configuration mode command and then the **login local** line configuration mode command to require local authentication for SSH connections from the local username database.

```
86 mySwitch1(config)#enable secret class
87 mySwitch1(config)#line vty 0 15
88 mySwitch1(config-line)#transport input ssh
89 mySwitch1(config-line)#login local
90 mySwitch1(config-line)#exit
```

Step 6

Enable SSH version 2.

By default, SSH supports both versions 1 and 2. When supporting both versions, this is shown in the **show ip ssh** output as supporting version 2. Enable SSH version using the **ip ssh version 2** global configuration command.

```
mySwitch1(config)#ip ssh version 2
mySwitch1(config)#
```

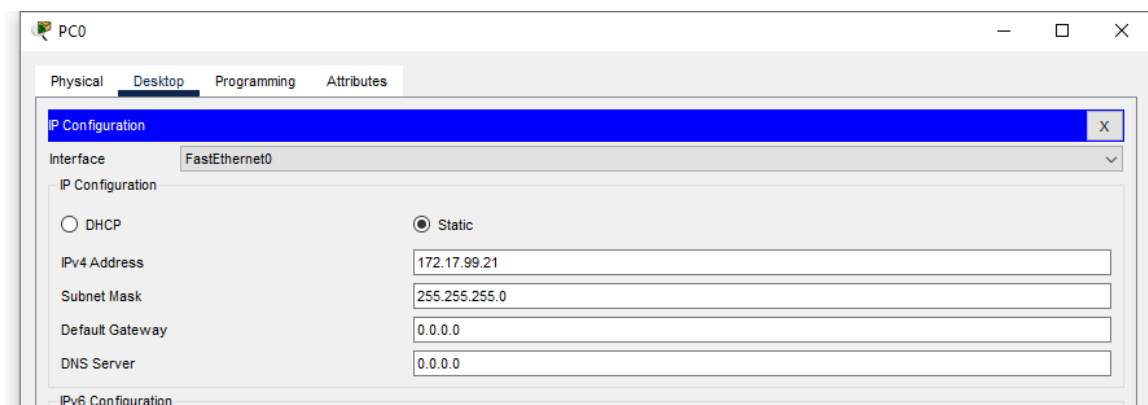
Verify SSH is Operational Switch

On a PC, an SSH client such as PuTTY, is used to connect to an SSH server. For example, assume the following is configured:

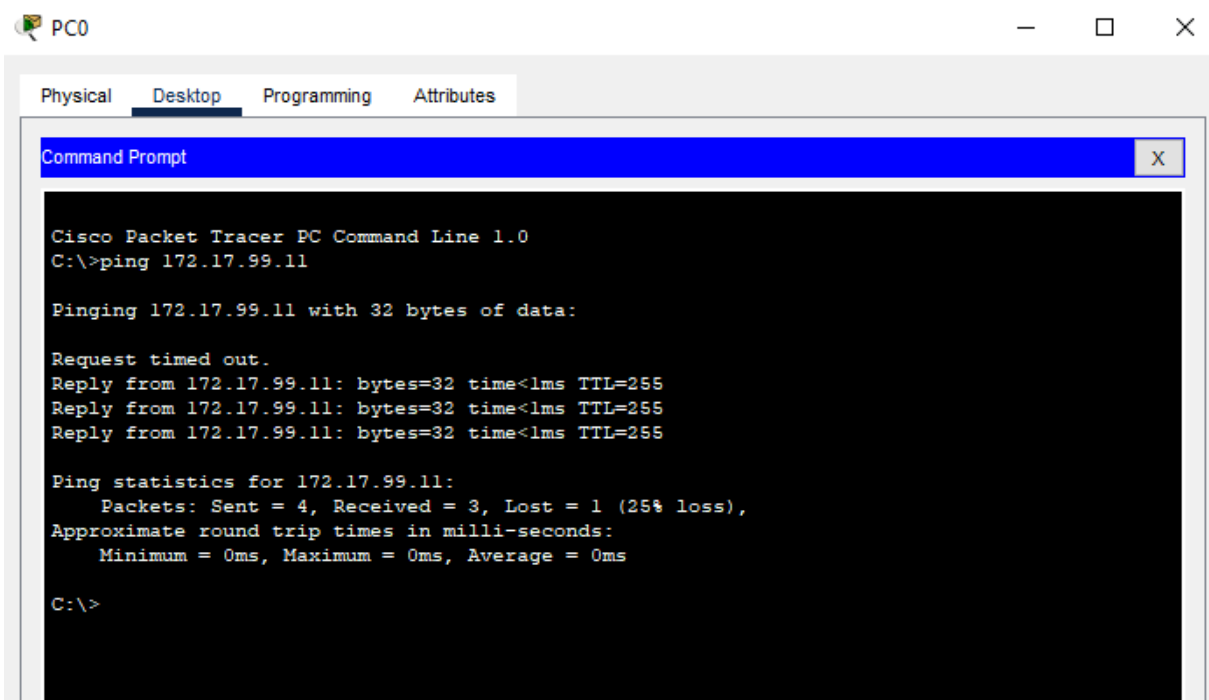
- SSH is enabled on switch mySwitch1
- Interface VLAN 1 (SVI) with IPv4 address 172.17.99.11 on switch mySwitch1
- PC1 with IPv4 address 172.17.99.21

The figure shows the PuTTY settings for PC1 to initiate an SSH connection to the SVI VLAN IPv4 address of S1.

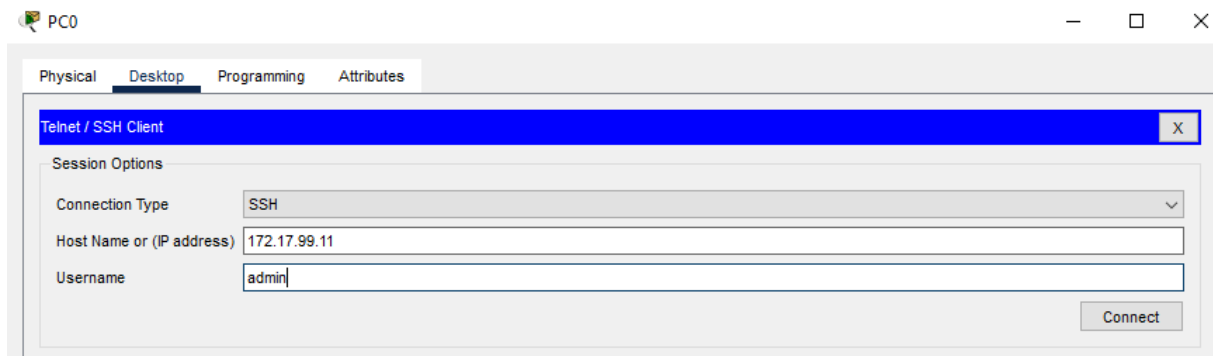
```
mySwitch1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
mySwitch1(config)#interface vlan 1
mySwitch1(config-if)#ip address 172.17.99.11 255.255.255.0
mySwitch1(config-if)#no shutdown
mySwitch1(config-if)#
```



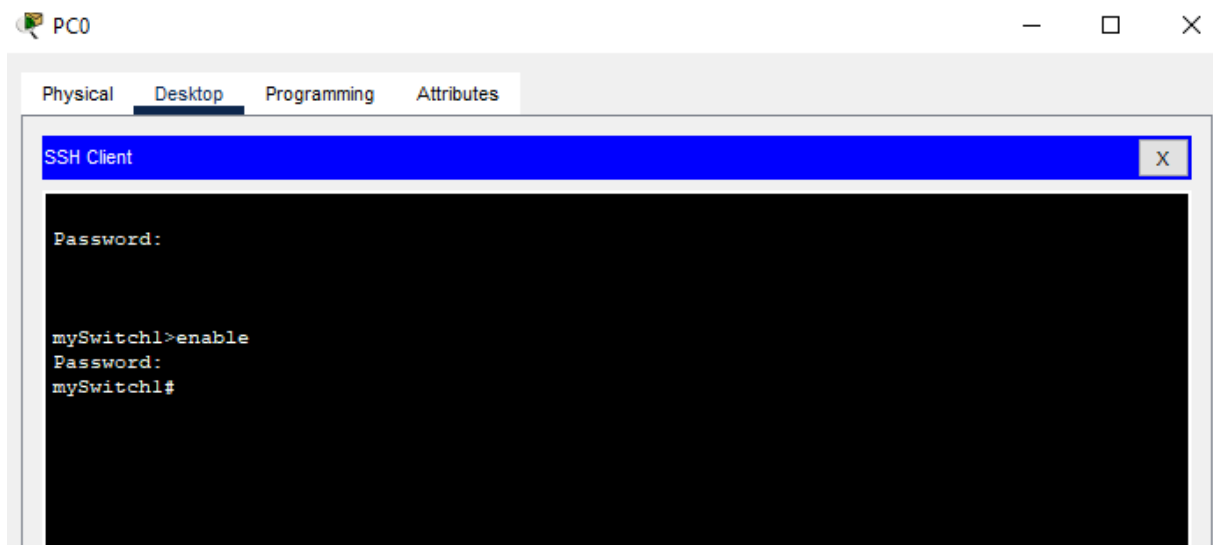
Check connection!



When connected, the user is prompted for a username and password as shown in the example. Using the configuration from the previous example, the username **admin** and password **mysecret** are entered. After entering the correct combination, the user is connected via SSH to the command line interface (CLI) on the Catalyst 2960 switch.



Result expected:

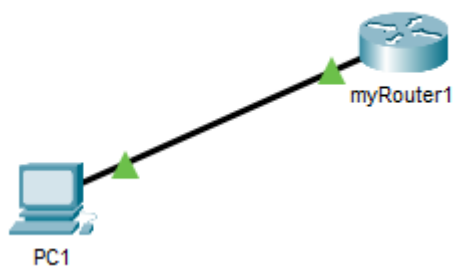


Verify SSH is Operational Router

On a PC, an SSH client such as PuTTY, is used to connect to an SSH server. For example, assume the following is configured:

- SSH is enabled on router myRouter1
- Interface GigabitEthernet 0/0 with IPv4 address 10.1.1.2 on myRouter1
- PC1 with IPv4 address 10.1.1.1

The figure shows the PuTTY settings for PC1 to initiate an SSH connection to the GigabitEthernet 0/0 IPv4 address of myRouter1.



```
myRouter1>
myRouter1>enable
Password:
myRouter1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
myRouter1(config)#interface Gig
myRouter1(config)#interface GigabitEthernet 0/0
myRouter1(config-if)#ip address 10.1.1.2 255.255.255.0
myRouter1(config-if)#no shutdown

myRouter1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

PC1

Physical Config Desktop Programming

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 10.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

PC1

Physical Config Desktop Programming

Telnet / SSH Client

Session Options

Connection Type: SSH

Host Name or (IP address): 10.1.1.2

Username: admin

Connect