

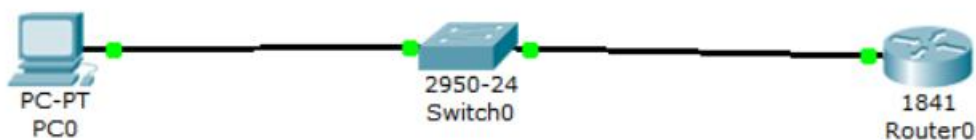
Configuring Telnet on Cisco Router and Switch

This document displays steps to configure telnet on the Cisco routers and Switches.

Configuring SSH access should be strict. As SSH sends traffic in encrypted format, any username and password transmitted over network is not visible for anyone who taps the data.

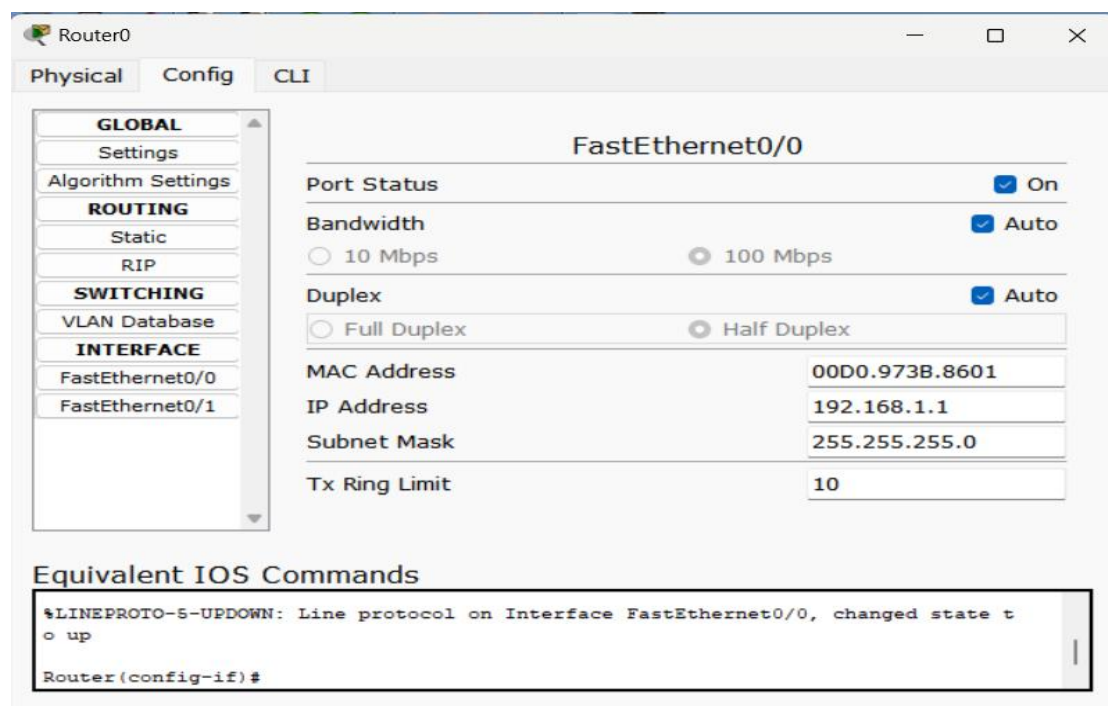
This document displays Telnet configuration so that candidates become aware about Telnet configuration. Also during a router audit they can identify if Telnet access is configured.

Use following devices in the network simulator.



1. Configuring SSH access on Cisco Router.

In the simulator router's FastEthernet 0/0 port is connected to the switch. Thus Click on the router Go to the config menu. Click FastEthernet 0/0 interface. Assign IP address as shown below. Click ON check box.



Now go to the CLI tab.

Type following commands to enable SSH access.

Router> **en**

Router# **conf t**

Set the hostname for the Router. It is required to configure SSH access.

Router(config)# **hostname router1**

Set the domain name. It can be anything. It is also required to configure SSH access.

router1(config)# **ip domain name demo**

Next you need to create private and public key using following command. The command will prompt you to enter the key bit size. Enter 1024 as shown below.

router1(config)# **crypto key generate rsa**

The name for the keys will be: router1.demo

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]

Enter following commands to enable SSH access on the router.

router1(config)# **enable secret abcd@1234**

Create a user on the router and assign password to the user using following command.

router1(config)# **username admin password cisco@123**

Enable ssh version 2 as it is more secure.

router1(config)# **ip ssh version 2**

Now enable 3 lines for SSH connection.

router1(config)# **line vty 0 2**

Now default telnet access is enabled. Enable ssh using following command.

router1(config-line)# **transport input ssh**

Enable login using the username and password that we created above.

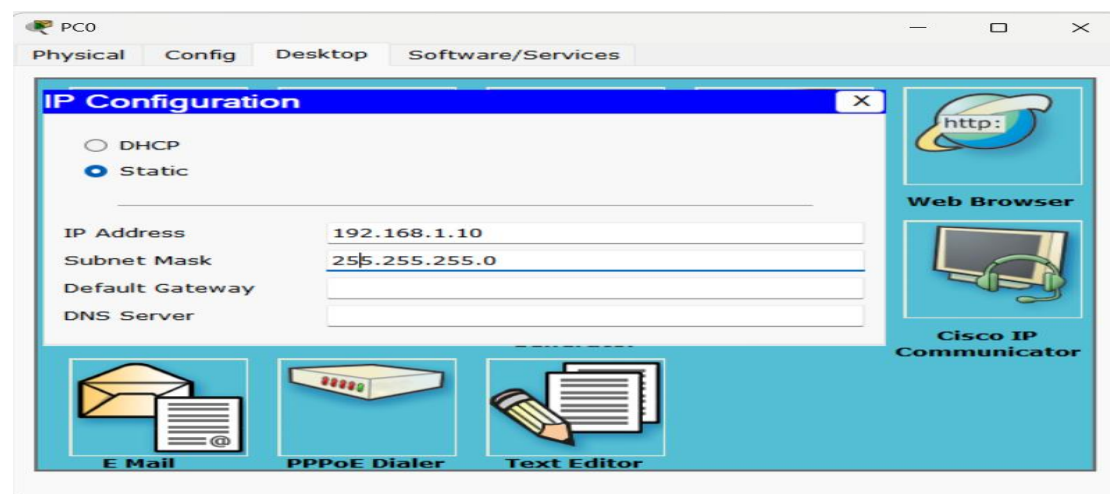
```
router1(config-line)# login local
```

```
router1(config-line)#exit
```

```
router1(config)#
```

Now the SSH access to the router is enabled.

Click on the PC. Click Desktop. Click on the IP configuration. And assign IP address to the PC as shown below.



Close the IP configuration window.

Now open Command Prompt and type following command.

```
ssh -l admin 192.168.1.1
```

Password prompt appears as shown below. You need to enter the user password given. Here it is cisco@123. The router prompt appears. To start configuring router, you need to type enable command. This will ask another password. Here type the password given in enable secret. You will get the prompt as shown below.

```
PC>
PC>ssh
Packet Tracer PC SSH

Usage: SSH -l username target

PC>ssh -l admin 192.168.1.1
Open
Password:

router1>en
Password:
router1#
```

Now you can configure router from any PC within your network. You do not need to go physically to the router.

2. Configure SSH access on Cisco Switch

On Cisco switches, ssh access is configured mostly for VLAN 1. So any PC connected in VLAN 1 can do telnet to the switch and configure the switch remotely.

Here the switch used in the above network configuration is used.

Go to the switch. Click on it. Click CLI.

```
Switch> en
```

Go to the configuration mode.

```
Switch# conf ig t
```

Select the VLAN 1 interface.

```
Switch(config)# interface vlan 1
```

Here we assign the IP address to the VLAN 1 interface.

```
Switch(config-if)# ip address 192.168.1.201 255.255.255.0
```

Turn on the Interface by giving following command.

```
Switch(config-if)# no shutdown
```

Following message will be displayed.

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

Now exit from the interface configuration.

```
Switch(config-if)# exit
```

```
Switch(config)#
```

Now configure SSH access. The commands are same as used on the router.

```
Switch> en
```

```
Switch# conf t
```

```
Switch(config)# hostname switch1
```

Set the domain name. It can be anything. It is also required to configure SSH access.

```
Switch1(config)# ip domain name demo
```

```
Switch1(config)# crypto key generate rsa
```

The name for the keys will be: router1.demo

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]

Enter following commands to enable SSH access on the router.

```
Switch1(config)# enable secret abcd@1234
```

```
Switch1(config)# username admin password cisco@123
```

```
router1(config)# ip ssh version 2
```

```
router1(config)# line vty 0 2
```

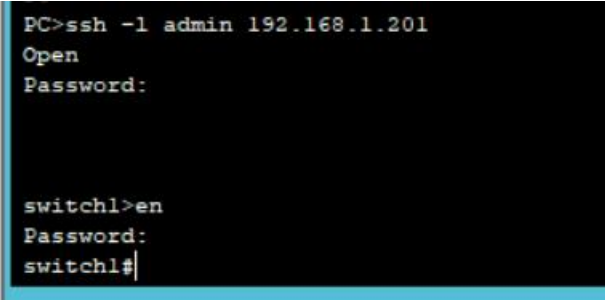
```
router1(config-line)# transport input ssh
```

```
router1(config-line)# login local
```

```
router1(config-line)#exit
```

```
router1(config)#
```

Now go to the PC and type telnet 192.168.1.201.



```
PC>ssh -l admin 192.168.1.201
Open
Password:

switch1>en
Password:
switch1#
```

This is how the SSH access to a Cisco switch configured.