CISCO Router Configuration

There are three methods to configure a Cisco router

1. Console
2. Telnet
3. Auxiliary

Above these **Console** used for **initial configuration** only, rest we can do via **Telnet**.

How Configuration of Cisco router

Cisco IOS supports various command modes, among those followings are the main command modes.

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Sub Interface Configuration Mode
- Setup Mode

- ROM Monitor Mode

Mode	Prompt	Command to enter	Command to exit
User EXEC	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Router(config)#	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Router(config-if)#	Use **interface type *number*** command from global configuration mode	Use **exit** command to return in global configuration mode
Sub-Interface Configuration	Router(config-subif)	Use **interface type *sub interface number*** command from global configuration mode or interface configure mode	Use **exit** to return previous mode. Use **end** command to return in privileged exec mode.

SOME RULES:

- ✓ IOS commands are not case sensitive; you can enter them in uppercase, lowercase, or mixed case.
- ✓ Password is case sensitive. Make sure you type it in correct case.
- ✓ In any mode, you can obtain a list of commands available on that mode by entering a question mark (?).

- ✓ Standard order of accessing mode is
  User Exec mode => Privileged Exec mode => Global Configuration mode => Interface Configuration mode => Sub Interface Configuration mode

Change default router name

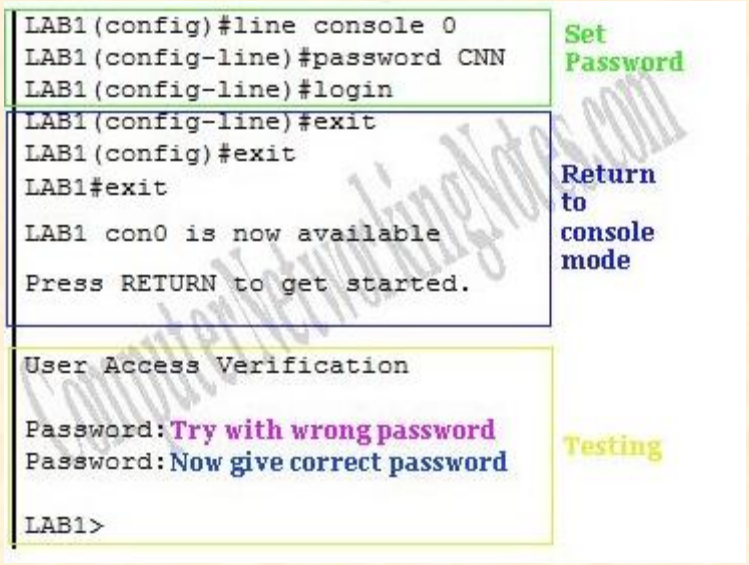
By default *Router* name is configured on routers. We can configure any desired name on router. ***hostname*** command will change the name of router. For example following command will assign **LAB1** name to the router.

```
Router(config)#hostname LAB1
LAB1(config)#
```

Configure password on cisco router

Router is a critical device of network. It supports multiple lines for connection. We need to secure each line [port].

Secure console port



Command	Description
Router(config)#line console 0	Move in console line mode
Router(config-line)#password console	Set console line password to CNN
Router(config-line)#login	Enable password authentication for console line

Secure auxiliary port

Auxiliary port provides remote access to router. You can attach modem in this port. Not all devices support this port. If your router supports this port use following commands to secure it.

Set auxiliary line password

Command	Description
Router(config)#line aux 0	Move into auxiliary line mode
Router(config-line)#password AUXCNN	Set auxiliary line mode password to AUXCNN
Router(config-line)#login	Enable auxiliary line mode password

Enable telnet access on cisco router

Depending on the model number and IOS software version router may supports various number of VTY connections range from 5 to 1000. VTY is the standard name for telnet and SSH connection. By default only first five VTYs connections are enabled. But you cannot connect them. When you try to connect them remotely you will get following message.

Password required but none set

This message indicates that password is not set on VTY lines. Password is required to connect VTYs. Following commands set password to TELCNN on VTYs line.

```
LAB1(config)#line vty 0 4
LAB1(config-line)#password TELCNN
LAB1(config-line)#login
LAB1(config-line)#exit
LAB1(config)#
```

Command	Description
Router(config)#line vty 0 4	Move into all five VTYs line
Router(config-line)#password TELCNN	Set password to TELCNN on all five lines
Router(config-line)#login	Configure VTYs to accept telnet connection

Configure serial interface in router

Serial interface is used to connect wan network. Following command will configure serial 0/0/0 interface.

```
LAB1(config)#interface serial 0/0/0
LAB1(config-if)#description Connected to bhilwara
LAB1(config-if)#ip address 10.0.0.1 255.0.0.0
LAB1(config-if)#clock rate 64000
LAB1(config-if)#bandwidth 64
LAB1(config-if)#no shutdown
LAB1(config-if)#exit
LAB1(config)#
```

Serial cable is used to connect serial interfaces. One end of serial cable is DCE while other end is DTE. You only need to provide clock rate and bandwidth in DCE side.

Command	Description
Router(config)#interface serial 0/0/0	Enter into serial interface 0/0/0 configuration mode
Router(config-if)#description Connected to bhilwara	Optional command. It set description on interface that is locally significant
Router(config-if)#ip address 10.0.0.1 255.0.0.0	Assigns address and subnet mask to interface
Router(config-if)#clock rate 64000	DCE side only command. Assigns a clock rate for the interface
Router(config-if)#bandwidth 64	DCE side only command. Set bandwidth for the interface.
Router(config-if)#no shutdown	Turns interface on

Configure FastEthernet Interface in router

Usually FastEthernet connects local network with router. Following commands will configure FastEthernet 0/0 interface.

```
LAB1(config)#interface fastethernet 0/0
LAB1(config-if)#description Development deparment
LAB1(config-if)#ip address 192.168.0.1 255.255.255.0
LAB1(config-if)#no shutdown
LAB1(config-if)#exit
LAB1(config)#
```


Command	Description
Router(config)#interface fastethernet 0/0	Enter into the FastEthernet 0/0 interface.
Router(config-if)#description Development department	This command is optional. It will set description on interface.
Router(config-if)#ip address 192.168.0.1 255.255.255.0	Assigns address and subnet mask to interface
Router(config-if)#no shutdown	Turns interface on. All interfaces are set to off on startup.

Securing Administration Using SSH

- ✓ **Secure Shell (SSH) is recommended to connect to your router to monitor, configure, and troubleshoot. Although Telnet is still available as an option, its use is discouraged because the session is not encrypted and usernames and passwords can be seen in clear text.**

- ✓ **SSH uses a client-server model. Your Cisco router is both an SSH server and an SSH client.**

- ✓ **You can use SSH on a desktop client to connect to a router, then the router itself can be a client, allowing you to jump from one router to another securely.**

- ✓ **SSH can be configured using either the command line or the SDM tool.**

Let's examine the steps necessary to configure it by command line first:

Before you can configure SSH, a domain name must be defined. Use the following syntax in global configuration mode:

Router1(config) # ip domain-name myrouter.com

If this is a new router (or recently reset to default), you may not have any crypto keys configured on it. You can display any keys configured by using the following command in privileged EXEC mode.

Router1# show crypto key mypubkey rsa

If you have keys displayed after doing this command, you will need to zeroize them by performing the following command in privileged EXEC mode:

Router1# crypto key zeroize rsa

The zeroize command deletes all keys. Make sure that’s what you want to do.

Once you've reset the keys, you need to generate new ones. Enter the following command:

Router1(config)# crypto key generate rsa general-keys modulus 1024

Next we want to limit the amount of time that it takes for the SSH connection to time out. Specify the amount of time in seconds. The following example sets the time-out limit to 120 seconds, or 2 minutes:

Router1(config)# ip ssh timeout 120

Last, you want to allow SSH as an option to be used inbound on the VTY lines. Use the following to allow only SSH:

Router1(config-line)# transport input *ssh*