

Cisco Router Configuration Tutorial

Cisco Inter-network Operating System:

Cisco IOS Modes of Operation

The Cisco IOS software provides access to several different command modes. Each command mode provides a different group of related commands.

For security purposes, the Cisco IOS software provides two levels of access to commands: user and privileged. The unprivileged user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.

The following table describes some of the most commonly used modes, how to enter the modes, and the resulting prompts. The prompt helps you identify which mode you are in and, therefore, which commands are available to you

Mode of Operation	Usage	How to Enter the Mode	Prompt
User EXEC	Change terminal settings on a temporary basis, perform basic tests, and list system information.	First level accessed.	Router>
Privileged EXEC	System administration, set operating parameters.	From user EXEC mode, enter enable <i>password</i> command	Router#
Global Config	Modify configuration that affect the system as a whole.	From privileged EXEC, enter configure terminal .	Router(config)#
Interface Config	Modify the operation of an interface.	From global mode, enter interface <i>type number</i> .	Router(config-if)#
Setup	Create the initial configuration.	From privileged EXEC mode, enter command setup .	Prompted dialog

User EXEC Mode:

When you are connected to the router, you are started in user EXEC mode. The user EXEC commands are a subset of the privileged EXEC commands.

Privileged EXEC Mode:

Privileged commands include the following:

- Configure – Changes the software configuration.
- Debug – Display process and hardware event messages.
- Setup – Enter configuration information at the prompts.

Enter the command `disable` to exit from the privileged EXEC mode and return to user EXEC mode.

Configuration Mode

Configuration mode has a set of submodes that you use for modifying interface settings, routing protocol settings, line settings, and so forth. Use caution with configuration mode because all changes you enter take effect immediately.

To enter configuration mode, enter the command **configure terminal** and exit by pressing **Ctrl-Z**.

Note:

Almost every configuration command also has a `no` form. In general, use the `no` form to disable a feature or function. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, enter the **no ip routing** command and enter **ip routing** to re-enable it.

Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Router>?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?).

```
Router#co?  
configure connect copy
```

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark.

```
Router#configure ?  
memory      Configure from NV memory  
network     Configure from a TFTP network host  
terminal    Configure from the terminal
```

You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh**.

Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration.

Use the following privileged mode commands to work with configuration files.

- **configure terminal** – modify the running configuration manually from the terminal.
- **show running-config** – display the running configuration.
- **show startup-config** – display the startup configuration.
- **copy running-config startup-config** – copy the running configuration to the startup configuration.
- **copy startup-config running-config** – copy the startup configuration to the running configuration.
- **erase startup-config** – erase the startup-configuration in NVRAM.
- **copy tftp running-config** – load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- **copy running-config tftp** – store the running configuration on a TFTP server.

IP Address Configuration

Take the following steps to configure the IP address of an interface.

Step 1: Enter privileged EXEC mode:

```
Router>enable password
```

Step 2: Enter the **configure terminal** command to enter global configuration mode.

```
Router#config terminal
```

Step 3: Enter the **interface** *type slot/port* (for Cisco 7000 series) or **interface** *type port* (for Cisco 2500 series) to enter the interface configuration mode.

Example:

```
Router (config)#interface ethernet 0/1
```

Step 4: Enter the IP address and subnet mask of the interface using the **ip address** *ipaddress subnetmask* command.

Example,

```
Router (config-if)#ip address 192.168.10.1 255.255.255.0
```

Step 5: Exit the configuration mode by pressing Ctrl-Z

```
Router(config-if)#[Ctrl-Z]
```

Routing Protocol Configuration

Routing Information Protocol (RIP)

Step 1: Enter privileged EXEC mode:

```
Router>enable password
```

Step 2: Enter the **configure terminal** command to enter global configuration mode.

```
Router#config terminal
```

Step 3: Enter the **router rip** command

```
Router(config)#router rip
```

Step 4: Add the network number to use RIP and repeat this step for all the numbers.

```
Router(config-router)#network network-number
```

```
Example: Router(config-router)#network 192.168.10.0
```

Note: To turn off RIP, use the **no router rip** command.

```
Router(config)#no router rip
```

Other useful commands

- Specify a RIP Version

By default, the software receives RIP version 1 and version 2 packets, but sends only version 1 packets. To control which RIP version an interface sends, use one of the following commands in interface configuration mode:

Command	Purpose
ip rip send version 1	Configure an interface to send only RIP version 1 packets.
ip rip send version 2	Configure an interface to send only RIP version 2 packets.
ip rip send version 1 2	Configure an interface to send only RIP version 1 and version 2 packets.

To control how packets received from an interface are processed, use one of the following commands:

Command	Purpose
ip rip receive version 1	Configure an interface to accept only RIP version 1 packets.
ip rip receive version 2	Configure an interface to accept only RIP version 2 packets
ip rip receive version 1 2	Configure an interface to accept only RIP version 1 or 2 packets.

- Enable or Disable Split Horizon

Use one of the following commands in interface configuration mode:

Command	Purpose
ip split-horizon	Enable split horizon.
no ip split-horizon	Disable split horizon.

Open Shortest Path First (OSPF)

Step 1: Enter privileged EXEC mode:

```
Router>enable password
```

Step 2: Enter the **configure terminal** command to enter global configuration mode.

```
Router#config terminal
```

Step 3: Enter the **router ospf** command and follow by the process-id.

```
Router(config)#router ospf process-id
```

Pick the process-id which is not being used. To determine what ids are being used, issue the **show process** command.

```
Router(config)#show process
```

Step 4: Add the network number, mask and area-id

```
Router(config-router)#network network-number mask area area-id
```

The *network-number* identifies the network using OSPF. The *mask* tells which bits to use from the network-number, and the *area-id* is used for determining areas in an OSPF configuration.

Example:

```
Router(config-router)#network 192.168.10.0 255.255.255.0 area  
0.0.0.0
```

Repeat this step for all the network numbers.

To turn off OSPF, use the following command.

```
Router(config)#no router ospf process-id
```

Other useful commands

- Configure OSPF Interface Parameters

You are not required to alter any of these parameters, but some interface parameters must be consistent across all routers in an attached network.

In interface configuration mode, specify any of the following:

Command	Purpose
ip ospf cost <i>cost</i>	Explicitly specify the cost of sending a packet on an OSPF interface.
ip ospf retransmit-interval <i>seconds</i>	Specify the number of seconds between link state advertisement retransmissions for adjacencies belonging to an OSPF interface.
ip ospf transmit-delay <i>seconds</i>	Set the estimated number of seconds it takes to transmit a link state update packet on an OSPF interface.
ip ospf priority <i>number</i>	Set router priority to help determine the OSPF designated router for a network.
ip ospf hello-interval <i>seconds</i>	Specify the length of time, in seconds, between the hello packets that a router sends on an OSPF interface.
ip ospf dead-interval <i>seconds</i>	Set the number of seconds that a router's hello packets must not have been seen before its neighbors declare the OSPF router down.
ip ospf authentication-key <i>password</i>	Assign a specific password to be used by neighboring OSPF routers on a network segment that is using OSPF's simple password authentication.

Interior Gateway Routing Protocol (IGRP)

- Create the IGRP Routing Process

To create the IGRP routing process, use the following required commands starting in global configuration mode.

Step	Command	Purpose
1	router igrp <i>autonomous-system</i>	Enable an IGRP routing process, which place you in router configuration mode.
2	network network-number	Associate networks with an IGRP routing process.

- Disable Holddown

The holddown mechanism is used to help avoid routing loop in the network, but has the effect of increasing the topology convergence time.

To disable holddowns with IGRP, use the following command in router configuration mode. All devices in an IGRP autonomous system must be consistent in their use of holddowns.

Command	Purpose
No metric holddown	Disable the IGRP holddown period.

- Enforce a Maximum Network Diameter

Define a maximum diameter to the IGRP network. Routes whose hop counts exceed this diameter are not advertised. The default maximum diameter is 100 hops. The maximum diameter is 255 hops.

Use the following command in router configuration mode.

Command	Purpose
metric maximum-hops <i>hops</i>	Configure the maximum network diameter.

- To turn off IGRP, use the following command.

Router(config)#**no router igrp** *autonomous-system*

Border Gateway Protocol (BGP)

- Enable BGP Routing

Use the following commands in global configuration mode.

Step	Command	Purpose
1	router bgp <i>autonomous-system</i>	Enable a BGP routing process, which places you in router configuration mode.
2	network network-number [mask network-mask] [route-map route-map-name]	Flag a network as local to this autonomous system and enter it to the BGP table.

- Configure BGP Neighbors

BGP must completely understand the relationships it has with its neighbors.

Command	Purpose
neighbor <i>{ip-address peer-group-name}</i> remote-as <i>number</i>	Specify a BGP neighbor.

- Reset BGP Connections

Use either of the following commands in EXEC mode to reset BGP connections

Command	Purpose
clear ip bgp <i>address</i>	Reset a particular BGP connection.
clear ip bgp *	Reset all BGP connections.

- To turn off BGP, use the following command.

Router(config)#**no router bgp** *autonomous-system*

How to read router/link status

Status of router and links can be easily determined by power LED of router and link LED of each interface (if any). However, you may find a transceiver connected to an AUI port looks like the following:



When this transceiver is correctly connected, the “POWER” LED should light. Similarly, the “LINK” and “POLARITY” LEDs should light when you inserted the cable into the RJ45 socket on the transceiver. (Note that to get this result; the other end of the cable should be connected to some other devices as well.) If these LEDs are not light, you probably have problems with the link (cable).