# Introduction

Equipment needed: Cisco 851 Router, Cisco serial cable, power brick and cable, Ethernet cables, Debian VM

Four modes usually used in this router:

|  |  |  |
| --- | --- | --- |
| **Mode** | **Access Method** | **Prompt** |
| User Exec | Begin a new session | Router> |
| Privileged Exec | Enter **enable** from user Exec | Router# |
| Global Configuration | Enter **configure** from privileged Exec Mode | Router(config)# |
| Interface Configuration | Enter **interface** *FastEthernet number* from global mode | Router(config-if)# |

These Cisco IOS command modes are hierarchical. When you begin a router session, you start in user EXEC mode. You can see a list of available commands for a particular mode by entering a question mark (?) at the prompt.

# Part 1 –Initialize the Router

## Step 1.1 Setup a serial terminal

Enable minicom on your Debian VM. Check the previous Cisco router lab for details. Use the same configuration of minicom for this lab. Be sure the serial port on the VM is properly enabled to the correct physical port on the workstation.

## Step 1.2 Reset the router

1. Hold the reset button on while turning the router on. This should reset the router to the factory defaults.
2. You should see a bunch of information on your minicom screen as the router starts. Then you will be requested to log in to initialize this router.

## Step 1.3 Create a user account and reset the router’s name

After you see the login information, you will have a ***one-time use*** username "cisco" and password "cisco". These must be changed before restarting the router, otherwise you will need to reinitialize the router and lose all changes. Login to start configuring the router. After you login, you should see the terminal has a prompt similar to: youname#.

Syntax to create a new user account:

***username <myuser> privilege 15 secret 0 <mypassword>***

Replace <myuser> and <mypassword> with the username and password you want to use.

Example for setting a new user with username *user01* and password *pass01*, and set the router’s new name to be myRouter:

youname# config tyourname(config)#username *user01* privilege 15 secret 0 pass*01*

yourname(config)#hostname myRouteryourname(config)#exit

## Step 1.4 Save your running configuration

You need to enter the copy running-config startup-config command to save your configuration changes to nonvolatile RAM (NVRAM) so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

Router# copy running-config startup-config

Destination filename [startup-config]?

Press **Return** to accept the default destination filename *startup-config*

It is suggested to check runnig-config before you save. Run command “show running-config” in the Privileged EXEC mode.

## Step 1.5 Restart your router

You need to use the username and password you just created to login. You should also see the router name has changed.

# Part 2 Configure WAN port and LAN ports

In this step, you will setup the DHCP server in the router so that the router can assign dynamic IP address for the LAN ports. You also need to setup the WAN port to obtain an IP address dynamically. For this lab, we setup the LAN port into 192.168.1.0 network.

## Step 2.1 Setup the WAN port

In the Cisco 850, the WAN port is fastEthernet 4. To configure this port, you need to enter the global configuration mode, and then enter interface configuration mode.

Enter the global configuration mode:

Router#config t

Enter interface configuration mode, specify the WAN port fastEthernet 4:

Router(config)#interface fastEthernet 4

Following are the commands for setting the WAN port to get ip address dynamically.

Router(config-if)#ip address DHCP

Router(config-if)#no shut

Router(config-if)#exit

Check what IP address is obtained for WAN port. Properly document. \*\*

The command *show interfaces* in Privileged Exec mode, shows all interfaces settings. Check the IP address of WAN port which is FE4. The IP address should be in the range of 172.16.X.X. Note that the WAN port must be connected to something to get an address!

## Step 2.2 Setup the LAN ports

Notice that four LAN ports on the Cisco 850 router are default to vlan1. If we want to setup the LAN ports in the 192.168.1.0 network, we actually need to configure a DHCP pool for vlan1 to allow the LAN ports in vlan1 to get IP addresses from the DHCP server in the router.

### Step 2.2.1 Configure a DHCP pool.

Start to run these commands in a configuration mode.

Router(config)#ip DHCP excluded-address 192.168.1.1 192.168.1.100

Router(config)#ip DHCP pool LANPOOL Router(DHCP-config)#network 192.168.1.0 255.255.255.0 Router(DHCP-config)#import all Router(DHCP-config)#default-router 192.168.1.1 Router(DHCP-config)#dns-server 172.16.1.251 Router(DHCP-config)#domain-name hades.lab Router(DHCP-config)#exit

You also need to setup a route from the vlan to the WAN interface

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.0

### Step 2.2.2 Apply the DHCP pool you just created to the VLAN1.

Enter interface configuration mode for vlan1:

Router(config)#interface vlan1

Apply the DHCP pool:

Router(config-if)#ip address pool LANPOOL

Router(config-if)#no shut Router(config-if)#exit

Now connect your computer to LAN port 0, which is FE0. Check what IP address is obtained from the Cisco router. Properly document. \*\*

***Question:*** Try to ping 172.16.1.251from your Debian VM and notice what's happening. Try to ping the WAN port IP address, check what's happening? Document and explain why. \*\*

After you finish the configuration, you should check if your DHCP configuration is right. Think how to do this. Hint: try running-config.

# Part 3 ENABLE NAT for WAN port and LAN ports

Until now, you still cannot ping outside from your Debian VM machine. That is because NAT is not configured on router.

## Step 3.1 Create a NAT permission access-list

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

## Step 3.2 Apply the access-list for the NAT configuration

Note: The first command is to enable dynamic translation of addresses on the inside interface.

Router(config)#ip nat inside source list 1 interface fastEthernet 4 overload

Router(config)#interface vlan1 Router(config-if)#ip nat inside Router(config-if)#no shut Router(config-if)#exit

Router(config)#interface fastEthernet 4 Router(config-if)#ip nat outside Router(config-if)#no shut

Now check the pinging again....Document the results and comment on what is happening. \*\*

If everything goes well, remember to save your currently running configuration as the start-up configuration.

# Part 4 Firewall Configuration

In this step, we wish to allow VM1 to view the Web page on 172.16.1.250, and not allow it to view the Web page on 172.16.1.251. Correspondingly we want VM2 to view 172.16.1.251 but not view 172.16.1.250.

## Step 4.1 Create an access-list for the firewall inspection rules

First we need to setup the firewall rules, that is, create an access-list.

Syntax:

access-list *access-list-number* {deny | permit} *protocol source source-wildcard* [operator [*port*]] *destination*

Let’s assume VM1 has address 192.168.1.101 and VM2 has address 192.168.1.102. Note: substitute your real IP addresses for these sample addresses.

Router(config)#access-list 111 deny tcp host 192.168.1.101 host 172.16.1.251 eq 80

Router(config)#access-list 111 deny tcp host 192.168.1.102 host 172.16.1.250 eq 80

Router(config)#access-list 111 permit tcp any any

Router(config)#access-list 111 permit ip any any

Router(config)#exit

Check the your access-list. Your access-lists should look like this:

Router#show access-lists

Standard IP access list 1

10 permit 192.168.1.0, wildcard bits 0.0.0.255 (75 matches)

Standard IP access list

10 permit 10.10.10.0, wildcard bits 0.0.0.

Extended IP access list 111

10 deny tcp host 192.168.1.101 host 172.16.1.251 eq www

20 deny tcp host 192.168.1.102 host 172.16.1.250 eq www

30 permit tcp any any

40 permit ip any any

## Step 4.2 Create firewall inspection rules and apply these rules

Define an inspection rule for a particular protocol, e.g. call it *tcp*.

### **Syntax**:

ip inspect name *inspection-name protocol*

Router(config)#ip inspect name firewall tcp Router(config)#interface vlan1

Assign the set of firewall inspection rules to the inside interface on the router: Router(config-if)#ip inspect firewall in Router(config-if)#exit

Assigns the defined ACLs to the outside interface on the router: Router(config)#interface vlan1

Router(config-if)#ip access-group 111 in Router(config-if)#exit

Now try to ping 172.16.1.251and 172.16.1.250. Open a browser to try to open the Web pages of 172.16.1.251and 172.16.1.250. Comment what you see. \*\*

You are encouraged to create more firewall rules to check what could happen.

## 2 Bonus Points: Can you allow and disallow pings?

Allow the VM1 to ping 172.16.1.250, and disallow it to ping 172.16.1.251while the VM2 is permitted to ping 172.16.1.251, and not permitted to ping 172.16.1.250. Show results and your access-list in your report.

*Here are some examples for deleting or adding an entry by using sequence number.*

1. If you want delete an entry in one access-list you should use following command:

***no squence-number permit/deny source source-wildcard***

For Example: in this example assuming the sequence number of the rule of “permit ip any any” is 20 and access-list number you want to modify is 111.

Router(config)#ip access-list extended 111 Router(config-ext-nacl)#no 20 permit ip any any Router(config-ext-nacl)#exit Router(config)#exit

Router#show access-lists

1. If you want to add an entry in one access-list, assume the access-list name is 111 and you want to add “deny tcp any host 172.16.1.250 eq 80” and put 15 as sequence number, you should run:

Router(config)#ip access-list extended 111

Router(config-ext-nacl)# 15 deny tcp any host 172.16.1.250 eq 80

Router(config-ext-nacl)#exit Router(config)#exit

Router#show access-lists

# TIPS:

1. If you want to undo a command just type no before the command.
   1. e.g. you want to delete an access-list 111, type no access-list 111.
2. You should always save the configuration once you have a successful configuration.
3. Remember, here as in the Linux CLI, tab is your friend. Use it to help typing.
4. Make sure your vm is using DHCP to obtain ip address. You may need to run ifdown eth0 and ifup eth0 to renew the ip address from the router.
5. You can always use the question mark (?) and arrow keys to help you enter commands. E.g. for a list of command variables, enter the command followed by a space and a question mark:

Router> **show ?**

...

clockDisplay the system clock

dialerDialer parameters and statistics

exceptionexception information

...

# Deliverables:

* Report describing the lab with an intro, body and summary
  + Document the questions
  + Make sure all items with \*\* are properly recorded and documented, as appropriate