NetSim®
NETWORK SIMULATOR®

Lab ID: 9.9K614A031.SAI1.1

NetSim® NETWORK SIMULATOR®

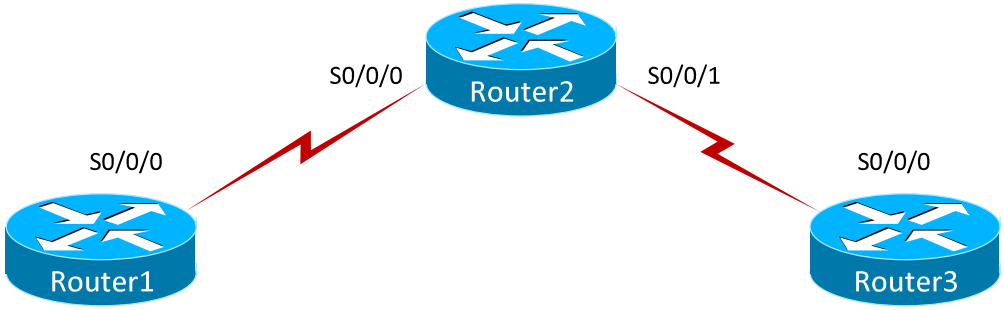
Stand-Alone Lab: Router Basics Part II

Objective

Learn how to properly configure a router. You would typically perform these types of tasks when setting up the local area network (LAN) for a new office. Configure all three routers with basic settings: set the routers' host names, configure basic security, and configure a login banner.

Lab Topology

The topology diagram below represents the NetMap in the Simulator.



Command Summary

Command	Description
banner login [*delimiting-character message delimiting-character*]	configures a message that is displayed at user login attempts
banner motd [*delimiting-character message delimiting-character*]	configures a message-of-the-day (MOTD) banner that can be used to display a message at user login attempts
configure terminal	enters global configuration mode from privileged EXEC mode
enable	enters privileged EXEC mode
enable password *password*	sets the enable password
enable secret *password*	sets the enable secret password
end	ends and exits configuration mode
exit	exits one level in the menu structure
hostname *host-name*	sets the device name
line console 0	accesses console line configuration mode
line vty 0 4	enters configuration mode for virtual terminal (Telnet) lines
login	enables password checking at login
login local	changes a login user name
password *password*	specifies the password that is required for a user to log in
service password-encryption	applies encryption to all current and future passwords configured on the device
show running-config	displays the active configuration file

Lab Tasks

Task 1: Perform Initial Router Configuration on Router1

Configure basic security for Router1.

1. Configure a host name of **Router1** for the router.

2. Configure an enable password of **boson** and an enable secret password of **cisco** on Router1.

3. Test the passwords you configured by exiting, or logging out of, the router and then typing **enable** at the user EXEC mode prompt. Try to use **boson** as the password to access privileged EXEC mode on Router1. Authentication will fail because the enable secret password overrides the enable password. Therefore, if both passwords are set, you must use the enable secret password to enter privileged EXEC mode. Enter **cisco** to access Router1.

4. Configure a password of **cisco** for Router1's console port.

5. Test the passwords currently configured on Router1 by logging out of the router and then pressing the Enter key.

6. On Router1, view the passwords that are configured

7. On Router1, encrypt all current and future passwords stored on the router.

8. Verify that the passwords configured on Router1 are not stored in plain-text format.

9. A Cisco device has the ability to be configured remotely. Configure a password of cisco for Router1's remote access lines.

10. On Router1, view the password you configured for remote access. Note that the password is stored in an encrypted form.

Task 2: Configure Banner Messages on Router1

Configure an MOTD banner and a login banner on Router1. Banners are used to display information about devices or to display security messages.

1. On Router1, create an MOTD banner; use **This device is used to route traffic between departments** as the text of the message. Use **#** as a delimiting character.

2. On Router1, display the banner you created in the previous step.

3. Configure the text **You must be an authorized user to access this device** as the login banner on Router1. Use **$** as a delimiting character.

4. Create a user named **MyName** that has a password of **cisco** so you can verify your configuration.

5. On Router1, view the banners configured on Router1.

Task 3: Perform Initial Router Configuration on Router2 and Router3

In this task, you will configure basic security and banners for Router2 and Router3.

1. Configure Router2 with a host name of **Router2** and Router3 with a host name of **Router3**. Then configure **boson** as an enable password and **cisco** as an enable secret password on both routers.

2. On Router2 and Router3, will the enable password or the enable secret password be required the next time you issue the enable command to access privileged EXEC mode? _____

3. On Router2 and Router3, configure **cisco** as a password for the console port.

4. On Router2, view the configured passwords. How are the passwords displayed in the running configuration? _____

5. Configure Router2 and Router3 to store all current and future passwords in an encrypted form.

6. On Router2 and Router3, enable remote access. Use **cisco** as the password where appropriate. How many simultaneous remote access sessions using Telnet can Router2 support? _____ In what form will the password you configured in this step be stored in the running configuration? _____

Task 4: Configure Banner Messages on Router2 and Router3

Configure an MOTD banner and a login banner on Router2 and Router3. Banners are used to display information about devices or to display security messages.

1. Configure **This device is used to route traffic between departments** as a message that will be displayed when a user accesses Router2 and Router3. Use **#** as a delimiting character.

2. Configure Router2 and Router3 to require a user name of **MyName** and a password of **cisco** to log in to the console port.

3. Configure **You must be an authorized user to access this device** as a login banner on Router2 and Router3. Use **$** as a delimiting character.

Lab Solutions

Task 1: Perform Initial Router Configuration on Router 1

1. From user EXEC mode, issue the following commands to configure a host name on Router1:

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#
```

2. Issue the following commands to configure an enable password and an enable secret password:

```
Router1(config)#enable password boson
Router1(config)#enable secret cisco
```

3. Test the passwords you configured by logging out of the router and then typing **enable** at the user EXEC mode prompt. Try to use **boson** as the password to access privileged EXEC mode on Router1. Authentication will fail because the enable secret password overrides the enable password. Therefore, if both passwords are set, you must use the enable secret password to enter privileged EXEC mode. Enter **cisco** to access Router1.

```
Router1(config)#exit
Router1#exit
Router1>enable
Password:boson
% Authentication failed
Password:cisco
Router1#
```

4. Configure a password for Router1's console port by issuing the following commands:

```
Router1#configure terminal
Router1(config)#line console 0
Router1(config-line)#login
login disabled on line 0 until password is set.
Router1(config-line)#password cisco
```

5. Test the passwords currently configured on Router1 by logging out of the router and then pressing the Enter key.

```
Router1(config-line)#end
Router1#disable
Router1>exit
Router1 con0 is now available
Press RETURN to get started.
Password:cisco
Router1>enable
Password:boson
% Authentication failed
Password:cisco
Router1#
```

6. Issue the **show running-config** command to view the passwords configured on Router1. The following sample output shows that the enable password and console password are stored in plain text. Conversely, the enable secret password is stored in an encrypted form.

```
Router1#show running-config
Building configuration...
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
enable secret 5 $sdf$6978yhg$jnb76sd
enable password boson
!
<output omitted>
!
line con 0
 login
 password cisco
<output omitted>
```

7. Router1 can be configured to store current and future passwords in an encrypted form by using the **service password-encryption** command. Issue the following commands to encrypt all current and future passwords stored on Router1:

```
Router1#configure terminal
Router1(config)#service password-encryption
```

8. Verify that the passwords configured on Router1 are not stored in plain-text format.

```
Router1(config)#end Router1#show running-config
Building configuration...
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router1
enable secret 5 $sdf$6978yhg$jnb76sd
enable password SE#C#cd$@VDS#$
!
<output omitted>
!
line con 0
 login
 password 68436986578330754
<output omitted>
```

9. A Cisco device has the ability to be configured remotely by using a virtual terminal (vty) line. The **line vty 0 4** command enables you to enter the configuration mode necessary to enable remote access to the device and set remote access passwords. By default, the line vty password is stored as plain text. Configure a password for Router1's vty lines by issuing the following commands:

```
Router1#configure terminal
Router1(config)#line vty 0 4
Router1(config-line)#login
Router1(config-line)#password cisco
```

10. Issue the **show running-config** command to view the password you configured for remote access. Note that the vty password is stored in an encrypted form.

```
Router1(config-line)#end
Router1#show running-config
Building configuration...
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router1
enable secret 5 $sdf$6978yhg$jnb76sd
enable password SE#C#cd$@VDS#$
!
<output omitted>
!
line con 0
 login
 password 68436986578330754
line aux 0
line vty 0 4
 login
 password 687533686576944232
!
no scheduler allocate
end
```

If service password encryption had not been configured on Router1, the password configured on the vty lines would be displayed as shown below:

```
Router1#show running-config
<output omitted>
line vty 0 4
 login
 password cisco
!
no scheduler allocate
end
```

Task 2: Configure Banner Messages on Router1

1. The following commands configure the appropriate MOTD banner on Router1:

```
Router1#configure terminal
Router1(config)#banner motd #This device is used to route traffic between
departments #
```

The **banner motd** command is used to configure a message that is displayed when a user accesses a device. The delimiting character used at the beginning and end of the message should not be a character you are going to use within the message. Type the text of the message you want to display, and then type the delimiting character so the router knows when you are finished entering text for the banner.

2. To view the banner, exit global configuration mode and exit the router. Press Enter to display the banner.

```
Router1(config#)exit
Router1#exit
Router1 con0 is now available
Press RETURN to get started.

This device is used to route traffic between departments
Password:cisco
Router1>enable
Password:cisco
```

3. On Router1, issue the following commands to configure a login banner:

```
Router1#configure terminal
Router1(config)#banner login $You must be an authorized user to access this
device $
```

4. On Router1, issue the following commands to create a user name and password combination that will allow you to view the login banner you configured:

```
Router1(config)#line console 0
Router1(config-line)#login local
Router1(config-line)#exit
Router1(config)#username MyName password cisco
```

5. Enter the following commands to view the banners configured on Router1. Note that when the login banner and the MOTD banner are both configured, the MOTD banner is displayed first, followed by the login banner.

```
Router1(config#)exit
Router1#exit

Press RETURN to get started.

This device is used to route traffic between departments
You must be an authorized user to access this device

Username:MyName
Password:cisco
Router1>
```

Task 3: Perform Initial Router Configuration on Router2 and Router3

1. You should issue the following commands to configure Router2 and Router3 with the appropriate host names and passwords.

```
Router>enable
Router#configure terminal
Router(config)#hostname Router2
Router2(config)#enable password boson
Router2(config)#enable secret cisco

Router>enable
Router#configure terminal
Router(config)#hostname Router3
Router3(config)#enable password boson
Router3(config)#enable secret cisco
```

2. The enable secret password will be required the next time you issue the enable command to access privileged EXEC mode on Router2 or Router3.

3. You should issue the following commands to configure **cisco** as a password for the console port of Router2 and Router3:

```
Router2(config)#line console 0
Router2(config-line)#login
Router2(config-line)#password cisco

Router3(config)#line console 0
Router3(config-line)#login
Router3(config-line)#password cisco
```

4. When you issue the **show running-config** command to view the passwords, you should verify that the enable password and console password are stored in plain text. Sample output from Router2 is shown below:

```
Router2(config-line)#end
Router2#show running-config
Building configuration...
!
Version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
enable secret 5 $sdf$6978yhg$jnb76sd
enable password boson
!
<output omitted>
!
line con 0
 login
 password cisco
<output omitted>
```

5. You should issue the **service password-encryption** command to store all current and future passwords on Router2 and Router3 in an encrypted form.

```
Router2#configure terminal
Router2(config)#service password-encryption

Router3(config-line)#exit
Router3(config)#service password-encryption
```

6. Issue the following commands to enable remote access on both routers:

```
Router2(config)#line vty 0 4
Router2(config-line)#login
Router2(config-line)#password cisco

Router3(config)#line vty 0 4
Router3(config-line)#login
Router3(config-line)#password cisco
```

A Cisco device has the ability to be configured remotely using a virtual terminal line. The **line vty 0 4** command enables you to enter the configuration mode necessary to enable remote access to the device and set the remote access password. By default, the line vty password is stored as plain text. However, the password configured on the vty lines in this step will be stored in an encrypted form because service password encryption has been enabled. Router2 and Router3 can support five simultaneous remote access sessions using Telnet.

Task 4: Configure Banner Messages on Router2 and Router3

1. On Router2 and Router3, you should issue the following commands to configure the MOTD banner:

```
Router2(config-line)#exit
Router2(config)#banner motd #This device is used to route traffic between
departments #

Router3(config-line)#exit
Router3(config)#banner motd #This device is used to route traffic between
departments #
```

   The MOTD banner is displayed when a user accesses a device.

2. You should issue the following commands to configure Router2 and Router3 to require a user name and password to log in to the console port:

```
Router2(config)#line console 0
Router2(config-line)#login local
Router2(config-line)#exit
Router2(config)#username MyName password cisco

Router3(config)#line console 0
Router3(config-line)#login local
Router3(config-line)#exit
Router3(config)#username MyName password cisco
```

3. On Router2 and Router3, you should issue the following commands to configure the login banner:

```
Router2(config)#banner login $You must be an authorized user to access this
device $

Router3(config)#banner login $You must be an authorized user to access this
device $
```

Sample Configuration Script

Router1	Router1 (continued)
Router1#show running-config Building configuration... ! Version 12.3 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname Router1 enable secret 5 sdf6978yhg$jnb76sd enable password SE#C#cd$@VDS#$! username MyName password 6843698657529 ! ip subnet-zero ! ip cef no ip domain lookup ! interface Serial0/0/0 no ip address no ip directed-broadcast shutdown ! interface Serial0/0/1 no ip address no ip directed-broadcast shutdown !	interface FastEthernet0/0 no ip address no ip directed-broadcast shutdown ! interface FastEthernet0/1 no ip address no ip directed-broadcast shutdown ! ip classless no ip http server ! banner login ^C You must be an authorized user to access this device ^C banner motd ^C This device is used to route traffic between departments ^C line con 0 login local password 6843698657529 line aux 0 line vty 0 4 login password 68753368657529 ! no scheduler allocate end