

Lab 1: Network Device Simulation with ENVL

1.1 Details

Aim: The aim of this lab is to begin using the ENVL (Edinburgh Napier Virtual Lab) and configure Cisco devices. And performing basic networking and security configurations.

The ENVL Lab manual will provide you with more details on how to setup a network using a Web-based Emulated Virtual Environment.

1.2 Activities

1.2.1 What is ENVL?

ENVL is a Web-based Emulated Virtual Environment which provides simulation/emulation of entire networks, containing a number of Cisco network devices, other vendors and host machines. It can be used for studying all kinds of technologies. You can learn about general technologies or vendor specific topics. You can test new technologies like network automation, SDN, etc.

It can be used to recreate corporate networks and test changes before putting them into production. You can create proof of concepts for clients. You can troubleshoot network issues by recreating them and e.g. use Wireshark to inspect packets.

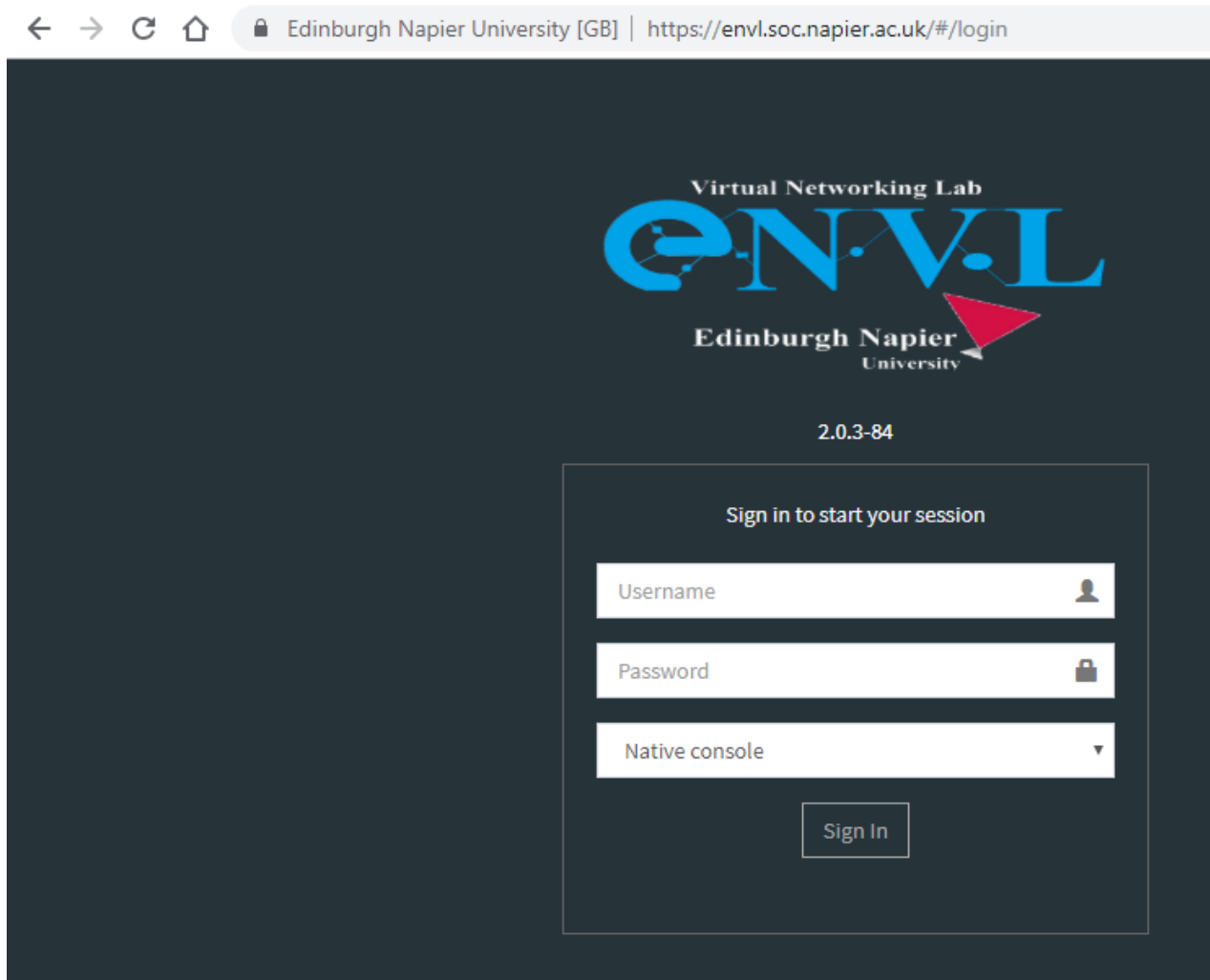
It is most definitely not just for networking, it can be used to test software in simulated networks, test out security vulnerabilities of any kind, system engineering like LDAP and AD servers and many, many more areas.

ENVL gives you tools to use around virtual devices and interconnect them with other virtual or physical devices. Many of its features greatly simplify the usability, re-usability, manageability, interconnectivity, distribution and therefore the ability to understand and share topologies, work, ideas, concepts or simply “labs”. This can simply mean it will reduce the cost and time to set up what you need or it might enable you to do tasks you would not have thought could be done this simple.

1.2.2 Using ENVL

To start working with **ENVL** first you need to login to the web link below using you login details provided by the lecturer.

Insert your Username and your password. Leave the third option to be the Native Console.

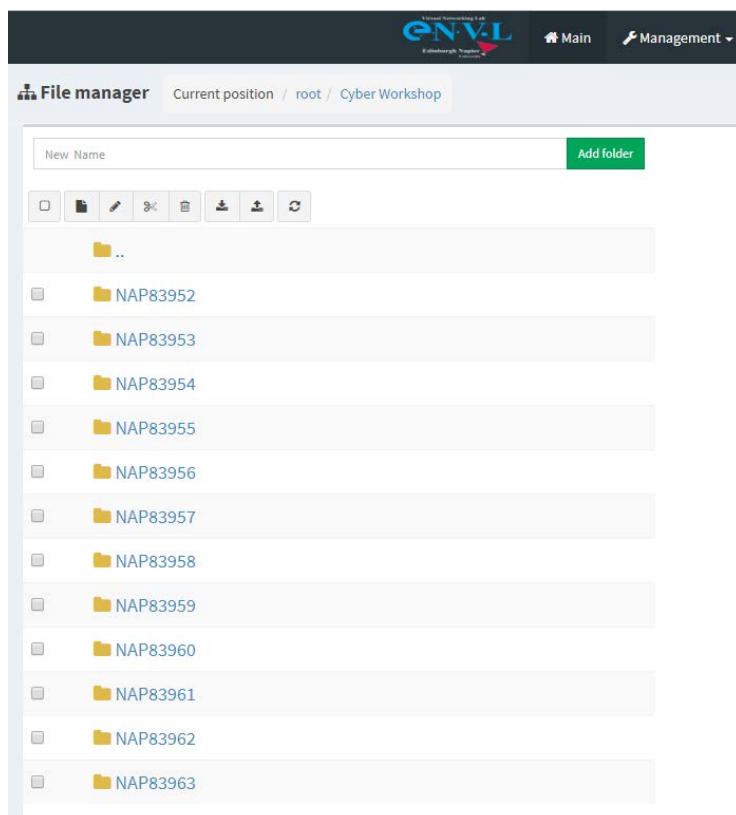
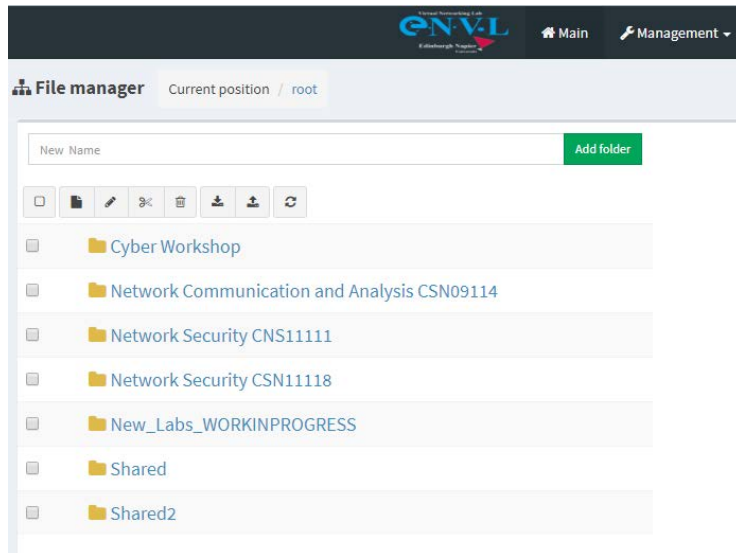


The screenshot shows a web browser window with the address bar displaying "Edinburgh Napier University [GB] | https://envl.soc.napier.ac.uk/#/login". The main content area has a dark blue background. At the top center, it says "Virtual Networking Lab" above a large, stylized blue "ENVL" logo. Below the logo is the "Edinburgh Napier University" logo, which includes a red triangle. Underneath the university logo, the version number "2.0.3-84" is displayed. In the center-right, there is a white-bordered box containing the text "Sign in to start your session". Below this text are three input fields: "Username" with a user icon, "Password" with a lock icon, and "Native console" with a dropdown arrow. A "Sign In" button is located at the bottom of this box.

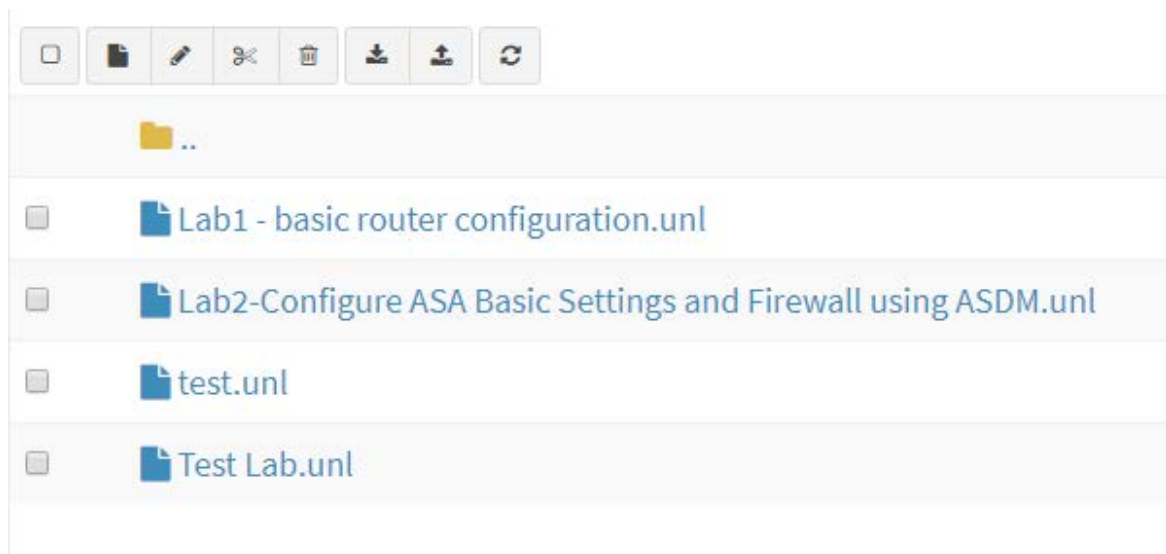
1.2.3 UNVL Main Page

After successful login, you will be able to see the main folder related to your course “Cyber Workshop”. Inside the main folder you will find a sub-folder with your username.

Each student has his own folder, which can be seen as the rack, which contains the labs with different devices. Having separate folders will allow each student to configure his own lab without interfering with other students running the same lab. So please make sure you are using the folder assigned to you.



Open your folder. At this stage the folders should contain labs for router configuration.



Next click on the “Lab1 – basic router configuration” and press “open” button in the middle of the screen. This should take you to the lab configuration tab.

Add folder

..

Lab1 - basic router configuration.unl

Lab2-Configure ASA Basic Settings and Firewall using ASDM.unl

test.unl

Test Lab.unl

Lab1 - basic router configuration

Scale

Lab Path: /Cyber
Workshop/NAP83952/Lab1 - basic router configuration.unl
Version: 1
UUID: d42c6307-ae5b-499b-8a2d-6c71baf5c7ee
Author: Isam Wadhaj

Description:
The aim of this lab is to get familiar with EVNL and perform basic router configuration and Basic Router Security/Device Hardening .

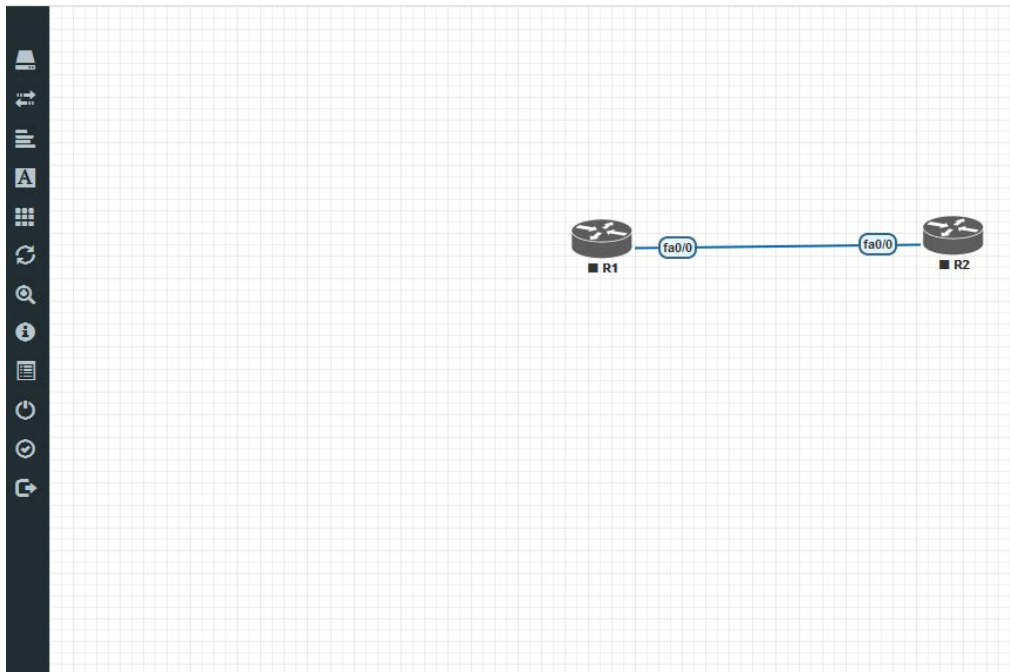
Open

Edit

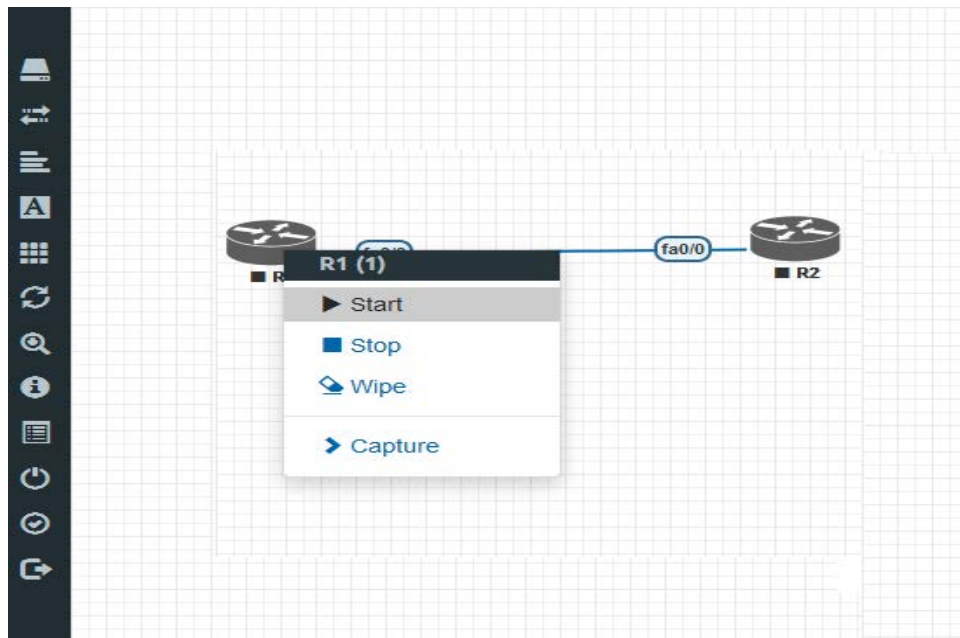
Delete

1.2.4 Lab Configuration Tab

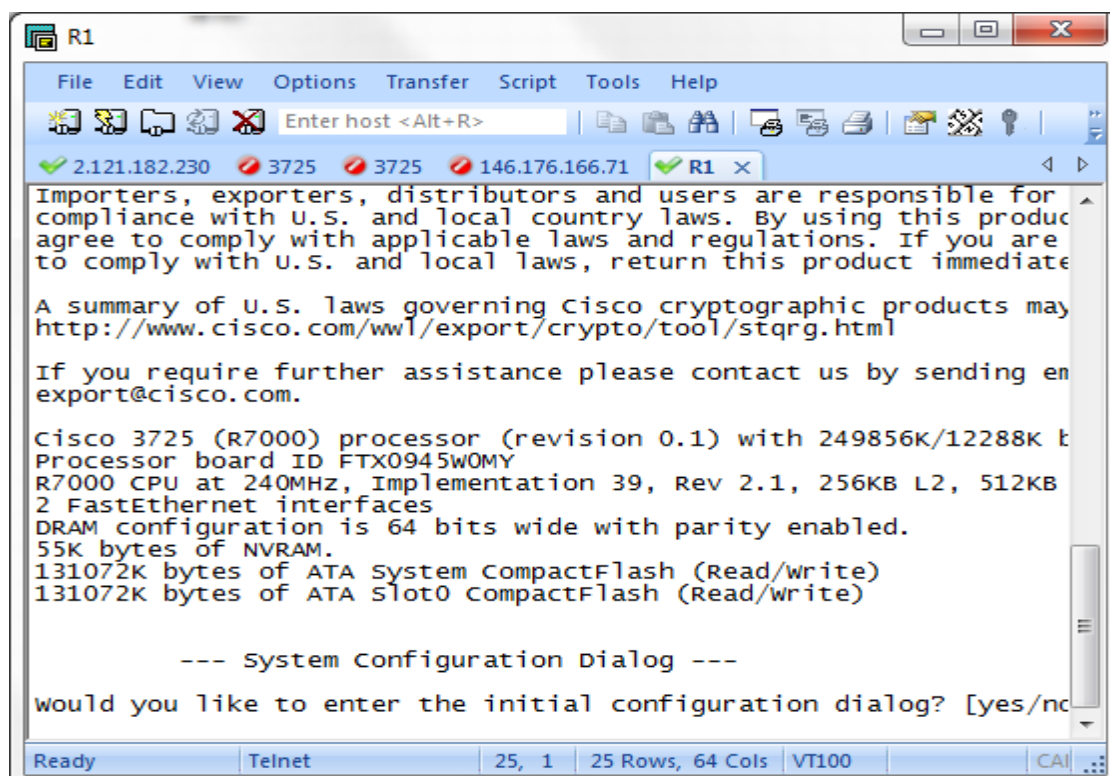
The lab configuration tab is where you are going to start configuring the network as it can be seen that Lab1 consists of two cisco routers version 3725. The routers are connected through FastEthernet interfaces f0/0.



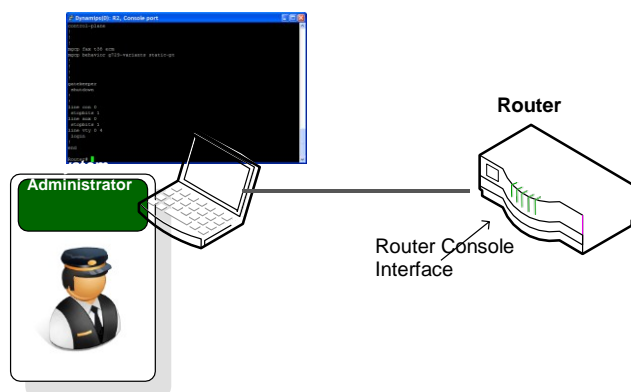
To start configuring the router they have to be started first. To do so right mouse click and then start. Right Click>start



Next step is to console to the router to start the configuration, this can be done by clicking on the router. A console session will start as shown in the figure below.
If the router terminal is in the configuration mode, as shown in the figure below, exit by typing **no**



This console window simulates an administrator physically connecting to the router with a laptop, via the routers console port, and using a command line to configure, as illustrated below. This Command Line Interface (CLI) allows the configuration of the router using the Cisco IOS Command language.



1.2.5 Basic Cisco Router Configuration

The router can now be configured using the console, the Command Line Interface (CLI). It is important to gain a good understanding of the basics of Cisco device configuration via the CLI, as this will be the foundation for most of the labs in the module.



To assist with the cisco router configuration commands the following can be used:
<http://www.cisco.com/en/US/docs/ios/preface/usingios.html>

Cisco router CLI has many different **Command Modes**, each giving access to a range of commands. When the router boots, the command line is in **User Exec Command Mode**, with the **Router>** prompt.

If the router prompt is **Router#** and not **Router>**, use the **disable** command until the prompt is **Router>**.

Only a limited set of commands are available in this mode. Type **“?”** to see the available commands for the current command mode. The figure below shows the commands being listed for user exec mode.

```
R1
File Edit View Options Transfer Script Tools Help
Enter host <Alt+R>
2.121.182.230 3725 3725 146.176.166.71 R1 x
Router>?
Exec commands:
access-enable      Create a temporary Access-List entry
access-profile     Apply user-profile to interface
clear              Reset functions
connect            Open a terminal connection
credential          load the credential info from file system
crypto             Encryption related commands.
disable            Turn off privileged commands
disconnect         Disconnect an existing network connection
enable             Turn on privileged commands
exit               Exit from the EXEC
help               Description of the interactive help system
m
lat                Open a lat connection
lock               Lock the terminal
login              Log in as a particular user
logout             Exit from the EXEC
modemui            Start a modem-like user interface
mrinfo             Request neighbor and version information
from a
multicast router
```

Try the `show running-config` command. An error should be generated, as this mode does not have permissions for the command.

Privileged Exec Command Mode

From the user exec mode, enter Enable Command Mode, more commonly known as Privileged **Exec Command Mode** using the `enable` command as shown below. A `Router#` prompt is now shown, and more privileged commands are now available.

```
Router> enable
Router#
```

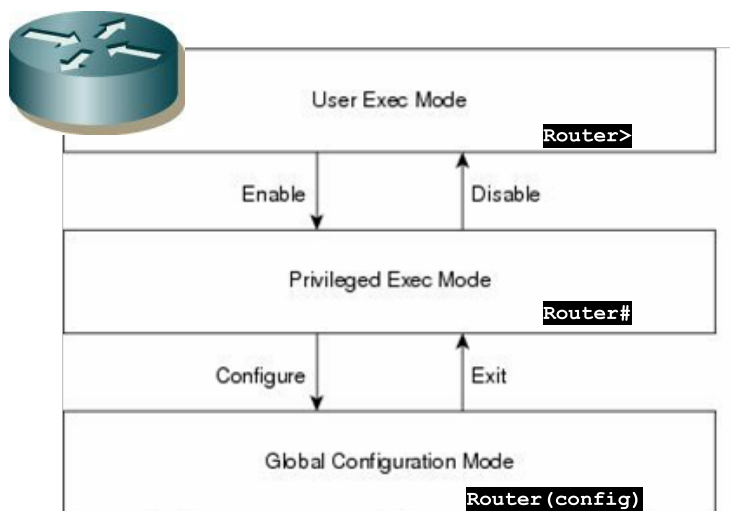
View the available commands using “?” and scroll back up the console window to compare the command sets.

Questions

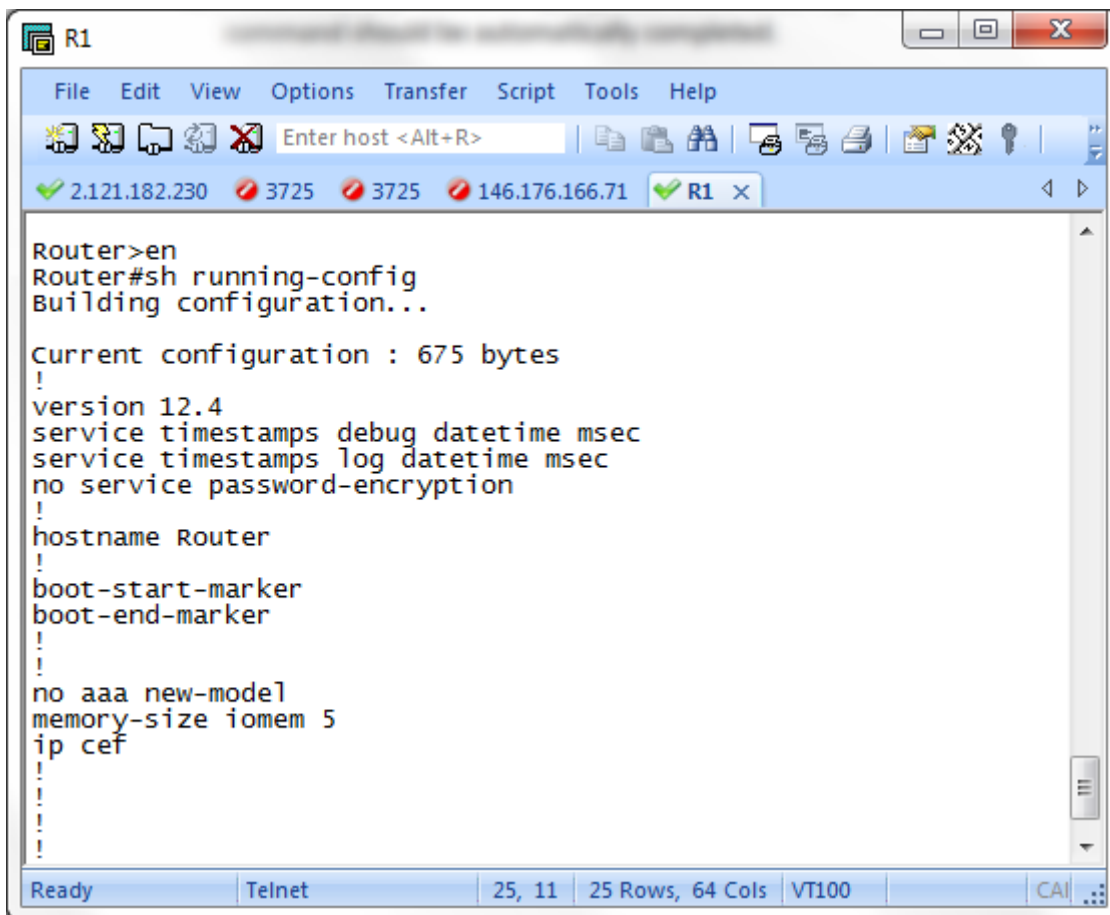
Q. Are there more or less commands available in **Privileged Exec Command Mode**?

View the routers configuration file with the command `show running-config`. It should be similar to the figure below with no IP Addresses or Passwords set up. <SPACE> and <RETURN> can be used to scroll page or line at a time. A full default configuration for a Cisco router is shown in **Appendix 1**.

The following shows Router Command modes with the commands to navigate between them. The associated prompts are shown on the bottom right.



Completing Partial Commands Parts of commands can be completed, as in Linux, using the TAB key with a unique partial command. Try the command `show run <TAB>`. The command should be automatically completed.



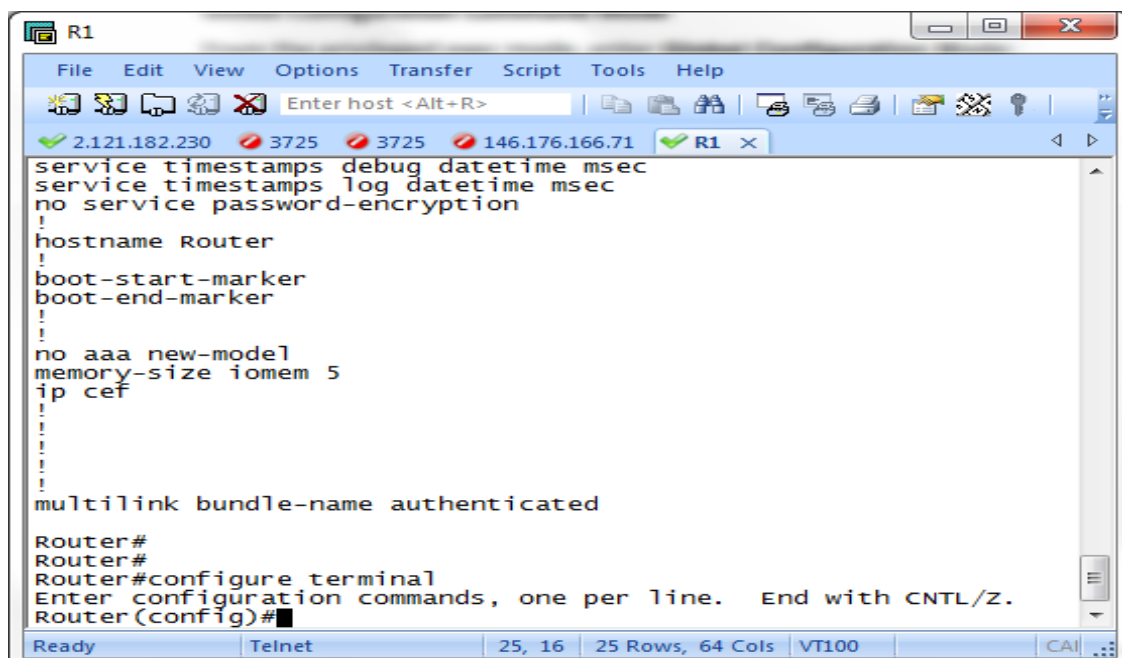
```
R1
File Edit View Options Transfer Script Tools Help
2.121.182.230 3725 3725 146.176.166.71 R1 x
Router>en
Router#sh running-config
Building configuration...

Current configuration : 675 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
```

Global Configuration Command Mode

From the privileged exec mode, enter **Global Configuration Mode**:

```
Router# configure terminal
Router(config)#
```



```
R1
File Edit View Options Transfer Script Tools Help
2.121.182.230 3725 3725 146.176.166.71 R1 x
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
multilink bundle-name authenticated

Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

From this command mode, Router configuration changes can be made. Change the device hostname to Router1:

```
Router(config)# hostname R1
R1(config)#
```

Note the prompt has now changed to show the new router name.

If you want to remove a configuration command from the router, simply negate the command by using the **no** command in from of any command. For example:

```
R1(config)# no hostname R1
Router(config)#
```

To move from a higher command mode to a lower mode, use the **exit** command or CTRL+C, and to move from Privileged Exec to User Exec use **disable**:

```
Router# config terminal
Router(config)# exit
Router# disable
Router>
```

1.2.6 Basic Router Security/Device Hardening

Configure a Password for access to Privileged Exec Command Mode

Cisco IOS supports two commands that set access to the privileged exec mode. The historical command, **enable password**, uses weak cryptography to secure the password, and should never be used if a more secure method is available.

The **enable secret** command uses a one way MD5 cryptographic hash algorithm to store the password. Hash algorithms will be discussed in more detail in a later Cryptography unit.

Password security relies not only on the cryptographic algorithm used, but also the password selected. Weak, easy to remember password will be used in the labs, but longer, more complex passwords should always be used in production environments.

Set the privileged exec password to **cisco**.

```
Router1#config t
Router1(config)# enable secret cisco
```

The enable password is now set to **cisco**. The result of this can be seen by doing the following:

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

```
Router1> enable
Password: cisco
```

Router1#

Questions

Q: Why would setting a password on the privileged mode be a good idea?

View the routers configuration file again, using the **show run** command, from the appropriate command mode.

Questions

Q: What are the last 5 characters of the privileged command mode password?

Try setting the privileged exec password a second time to the same value: **cisco**.

```
R1# config t
R1(config)# enable secret cisco
```

View the routers configuration file again, using the **show run** command, from the appropriate command mode.

Questions

Q: What security are the last 5 characters of the privileged command mode password?

Q: Is this the same encrypted password?

```
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$U230$UQF9XGgP2rvGGMPk8qww0.
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
!
--More--
```

The encrypted password is shown in the configuration details for the router which can be a problem if configurations are printed. The **secret 5** shows it is a MD5 hash of the plaintext password.

To make things more secure the MD5 hash is salted. This means the same password gives a different hash output every time, and is harder to crack. The salt value is shown between the 2nd and 3rd \$ character.

1.2.7 Configure Banner Message

Banners can be displayed to users trying to gain administrative access to a network device. The Cisco Message of the Day (MOTD) banner, which is displayed at login, is commonly used to greet the user. This can have legal and security implications for an organization. For example, a welcome message should never be displayed, as this could be seen as an invitation to unauthorized users to try access the device.

A banner should include information about authorization, penalties for unauthorized access, connection logging, and applicable local laws. An organizations **security policy** should provide policy on banner messages.

To configure a banner use the following command in **Global Configuration Mode**:

```
Router(config)# banner motd [delimited char] <message> [delimited char]
```

Try something similar to the following:

```
Router> enable
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)# banner motd #
Enter TEXT message. End with the character '#'
*****
*                                     *
*                WARNING                *
*    YOU HAVE ACCESSED A RESTRICTED DEVICE    *
*    USE OF THIS DEVICE WHITHOUT PRIOR AUTHORISATION *
*            IS PROHIBITED, AND WILL BE PROSECUTED *
*            ALL CONNECTIONS ARE LOGGED *
*                                     *
*****
#
Router1(config)# exit
Router1#
```

Questions

Q: Why would details about the organization, the network, or the device being logged into be a bad idea in a banner message?

Q: What would be the global configuration command to *remove* the MOTD banner?

1.2.8 Router Network Interface Configuration

Configure the Routers Fast Ethernet Network Adapter

To view the routers network interfaces and their current states, use the `show ip interface` command, from Priv Exec command mode, as shown below.

```
R1# show ip interface brief
```

Questions

- Q: What are the routers interface names?
- Q: What are the assigned IP Address?
- Q: What is its current status of the interfaces?

Each router interface that interconnect two devices has to be assigned a network layer address, or **IP Address**, to be able to communicate with other devices.

```
R1(config)# interface fa0/0
R1(config-if)# description TO THE LAN 192.168.100.x NETWORK
R1(config-if)# ip address 192.168.100.1 255.255.255.0
```

The no shutdown command, is needed to enable the interface for communication

```
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

To save your configurations issue.

```
R1#copy running-config startup-config
Destination filename [startup-config]?
```

Watch as the interface becomes active:

```
*Sep 14 10:41:13.843: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
```

Check the devices network interfaces and their current states again.

Questions

- Q: Does the interface have an IP Address, and what is the current state now?
- Q: Why did we configure the administration security before the interfaces?

1.2.9 Optional Challenge – Extend Topology

Start R2 the router, and start a CLI terminal.

Set the hostname **R2**. Assign its interface the IP Address **192.168.100.2**

```
Router2(config)# interface fa0/0
Router2(config-if)# description LAN TO THE 192.168.100.x NETWORK
Router2(config-if)# ip address 192.168.100.2 255.255.255.0
```

Test Connectivity

From the first Router use the **ping** command to test connectivity between the interfaces. The ping command uses ICMP packets and can be used to check if a device/interface exists, and is responding.

```
R1(config)# ping 192.168.100.2
```

Router2 should be able to ping Router1s interface

```
Router2(config-if)#do ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!.!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/49/72 ms
Router2(config-if)#
```

Questions

Q. How might the ping command be misused?

Q. Try to ping google.com, and then amazon.com

1.3 Appendix 1 - default Cisco IOS router configuration

Current configuration: 824 bytes

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Router  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
ip cef  
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface Serial0/1/0  
no ip address  
shutdown  
no fair-queue  
!  
interface Serial0/1/1  
no ip address  
shutdown  
clock rate 2000000  
!  
interface Vlan1  
no ip address  
!  
ip http server  
no ip http secure-server  
!  
control-plane  
!  
line con 0  
line aux 0  
line vty 0 4  
login  
!  
scheduler allocate 20000 1000  
end
```