GraceStOne
ProfessiOnals

ICND1 Lab Exercises

Lesson Companion

Joe Rinehart

MBA, CCIE #14256

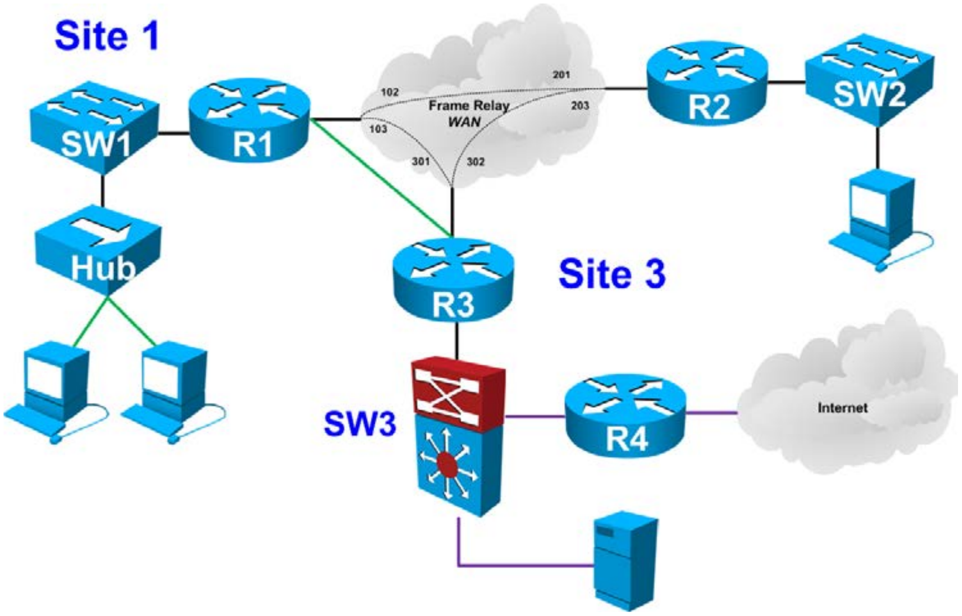
CCNP/DP/VP

May 2, 2014

Table of Contents

Introduction

The Overall Topology



The CCENT/ICND1 Project is designed to reinforce networking concepts as well as build critical job-related work skills in Cisco environments. Utilizing Cisco Packet Tracer (version 6.0.1), the simulated lab environment consists of the following elements:

- Four (4) Cisco 2800 class routers
- Three (3) Cisco Catalyst switches
- Three (3) computer workstations
- One (1) networking hub
- One (1) server
- Wide Area Network connectivity
- Simulated Internet connection

Purpose of the Lab Project

A thorough understanding of networking concepts is the foundation upon which understanding is essentially built. While theoretical knowledge is important, the application of that knowledge is equally important, and forms the basis for effective performance in real-world environments. Early versions of the original CCNA-level certification exams concentrated on factual knowledge, while current exams utilize realistic scenarios that reflect more “hands on” experiences. To satisfy these types of requirements, CCENT students need practical, experience-based exercises.

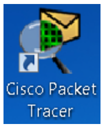
Lesson 1 Lab Exercises

Packet Tracer Exploration

If you have not already done so, locate and download Cisco Packet Tracer, version 6.0.1 or later. Numerous sites exist that host this software, which is designed for Cisco certification studies.

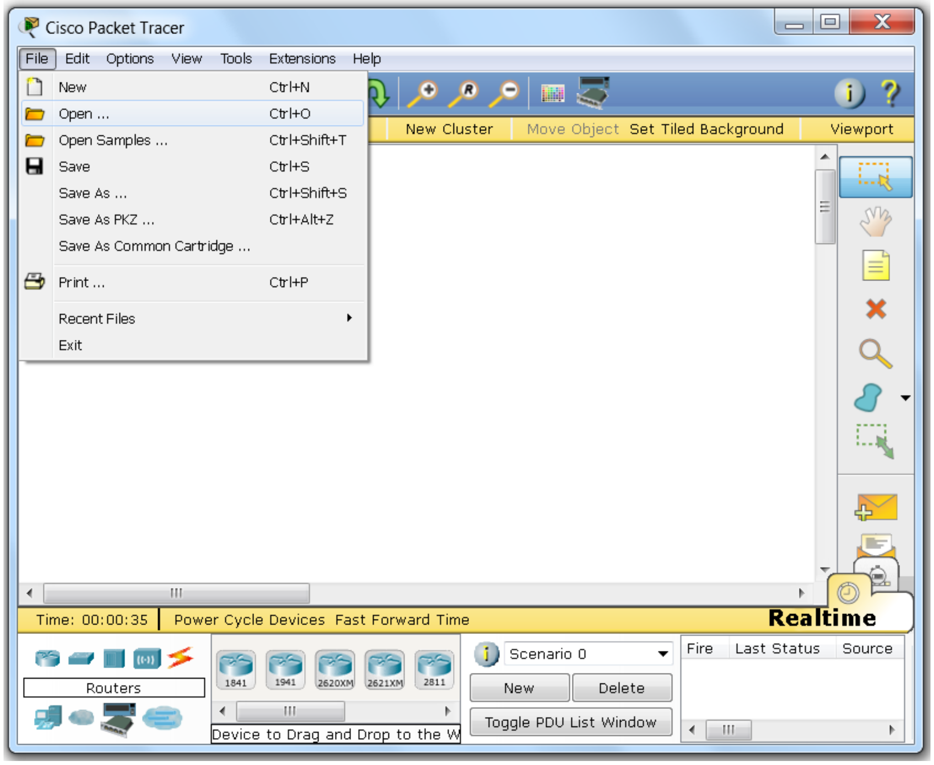
1.1.1. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:

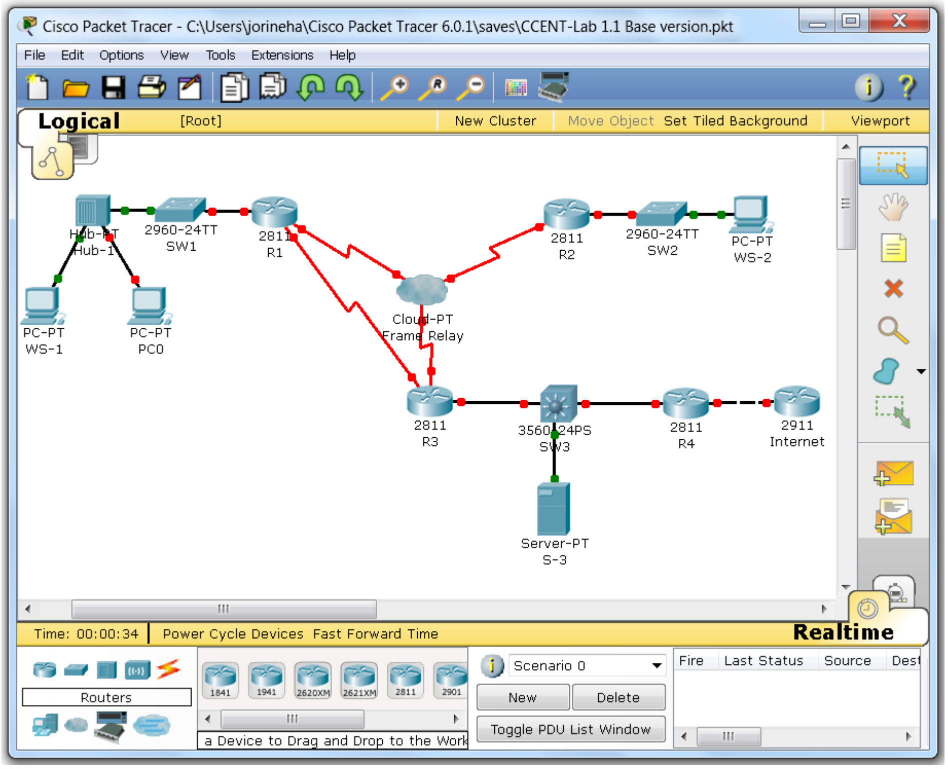


1.1.2. Load the Basic Lab Topology

Locate the configuration file provided to you by the instructor (should be named **CCENT-Lab-Startup.pkt**):



Once the topology is loaded, it should look nearly identical to the image shown below:

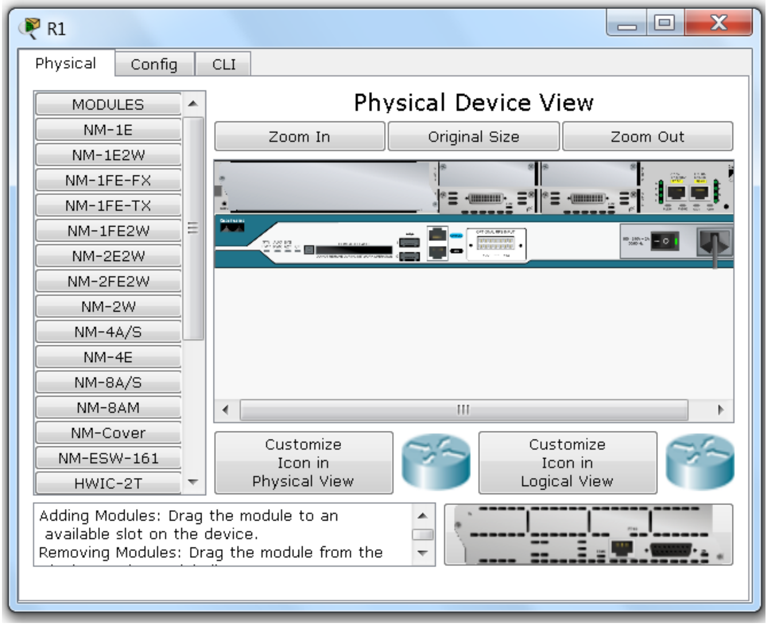


1.1.3. Getting Familiar with the User Interface

Because Packet Tracer might seem strange and unfamiliar, keep in mind that human nature generally is resistant to change; discomfort with something new is to be expected. All connections, interfaces, and device hardware configuration is already defined in the file that you loaded, which will allow you to perform the various lab exercises with ease. To assist with you getting familiar with the program, here are some steps to common tasks:

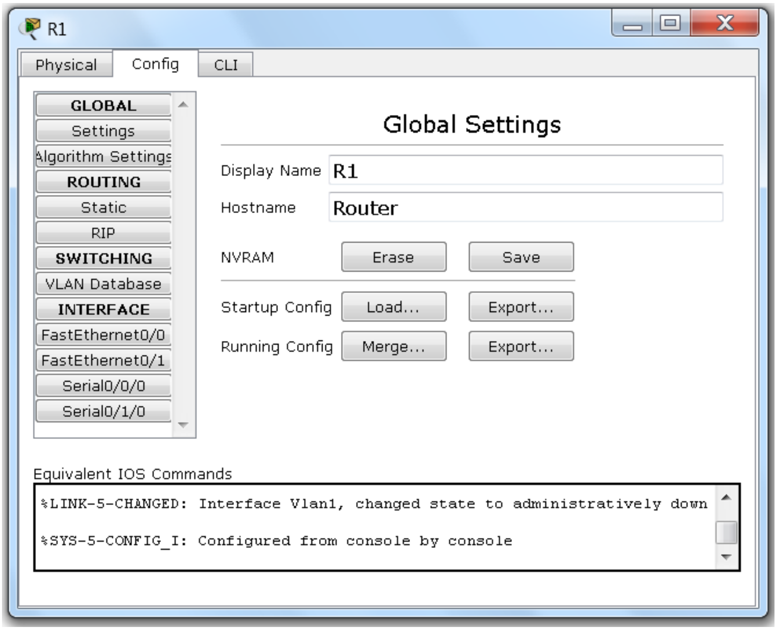
- **Saving configurations**: This is critical, because if you fail to save the changes that you have made to devices in the lab, then all your work will be lost. You have several options for saving your work:
  - On the top menu bay, click **File>Save**
  - Using the keyboard shortcut **Ctrl+S**
  - When exiting Packet Tracer, you will be prompted to save your work
- **Interacting with devices**: As part of the lessons, you will perform various configuration and verification tasks that require you to log into the devices directly. The simplest and easiest way to do that is to double click the image of the device you want to access, and the following window will display, with three tabs:

- **Physical** Tab: This displays the physical configuration of the device as if it were in use, and by which you can alter the layout of the hardware. While you can certainly change this later as you advance in your studies, you will not interact directly with this tab very often.



Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the

- **Config** Tab: While you can make some changes here, your learning process will be best spent on the third tab



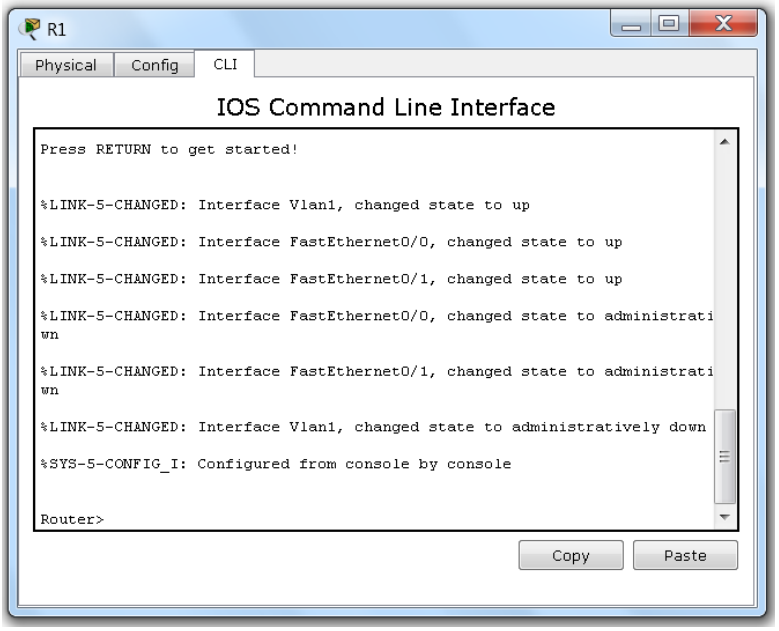
Display Name R1

Hostname Router

Equivalent IOS Commands

```
%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down

%SYS-5-CONFIG_I: Configured from console by console
```

- **CLI** Tab: This screen/window is where you will spend most of your time, specifically the **Command Line Interface** or **CLI**. While some graphical tools exist for configuration, nearly every Cisco network engineer/technician works directly in the CLI. Once this window is open, you can press **<enter>** and then interact directly with the equipment.



```
Press RETURN to get started!


%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administrati
wn

%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down

%SYS-5-CONFIG_I: Configured from console by console


Router>
```

**** NOTE that the topology referenced in the videos of the lessons is different due to changes that were made to the CCENT exam itself. While all the concepts are still valid, some of the topics have been moved around. When in doubt, pay attention to this lab guide. ****

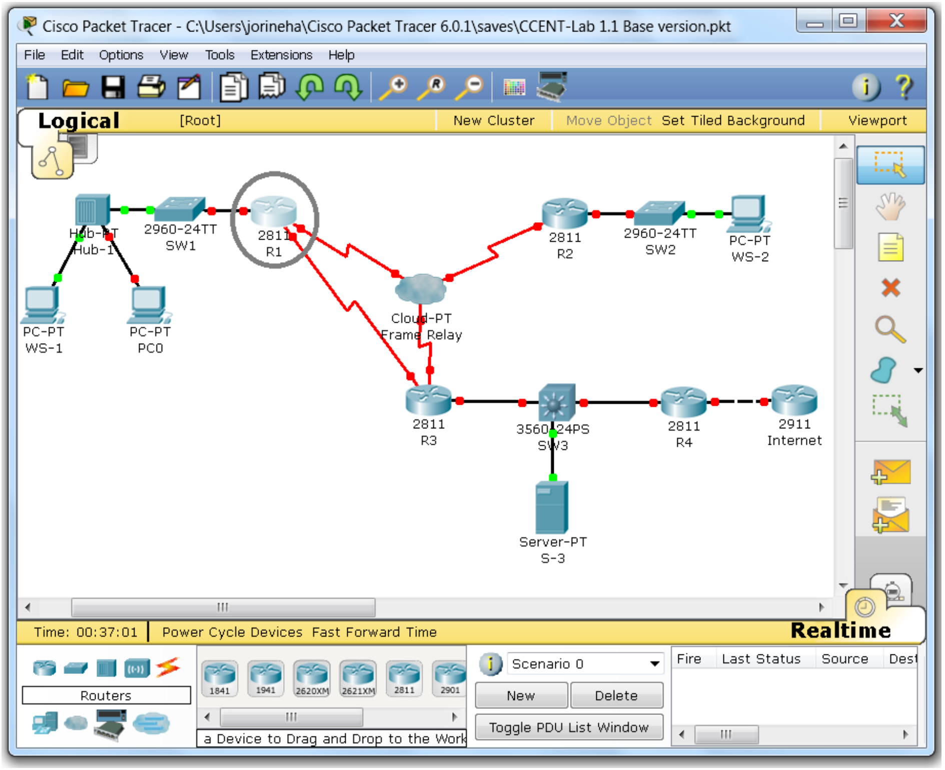
Lesson 2 Lab Exercises

Router Exploration

One of the most basic networking devices is a router, so named because it routes traffic. Just as you would start out from your home to drive to work, so a router directs **packets** (the basic network unit of data) from one location in a network to another. Cisco has manufactured these types of devices since the early 1980's when they pioneered the technology. Today this equipment comes in many different sizes and capabilities, which we will review in a future lesson. The purpose of this lab exercise is just to start getting familiar with routers and the CLI.

1.1.4. Select R1 by double clicking the image

In the topology, you have probably noticed that there are five routers, labeled R1, R2, R3, R4 & Internet. In these lab exercises, you will interact with the first four devices, as the Internet router is already configured to support your efforts. Simply double click the image of R1 to bring up the three tabbed device window and then click the CLI tab.

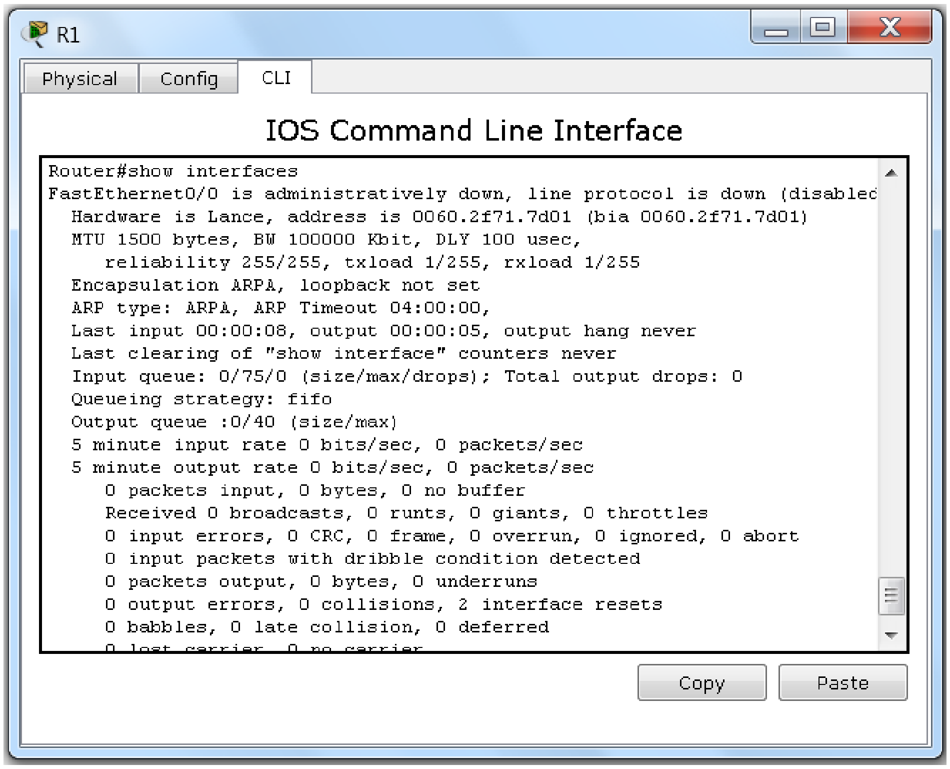


1.1.5. Explore the CLI

In many ways, a router is a compact, purpose-built computer equipped with specialized hardware. Like a desktop computer, a router cannot do anything without being given instructions about what to do, even though ***the Matrix*** may claim otherwise. Cisco engineers use a very specialized set of instructions to direct the activities of routers in a way that helps it direct network traffic.

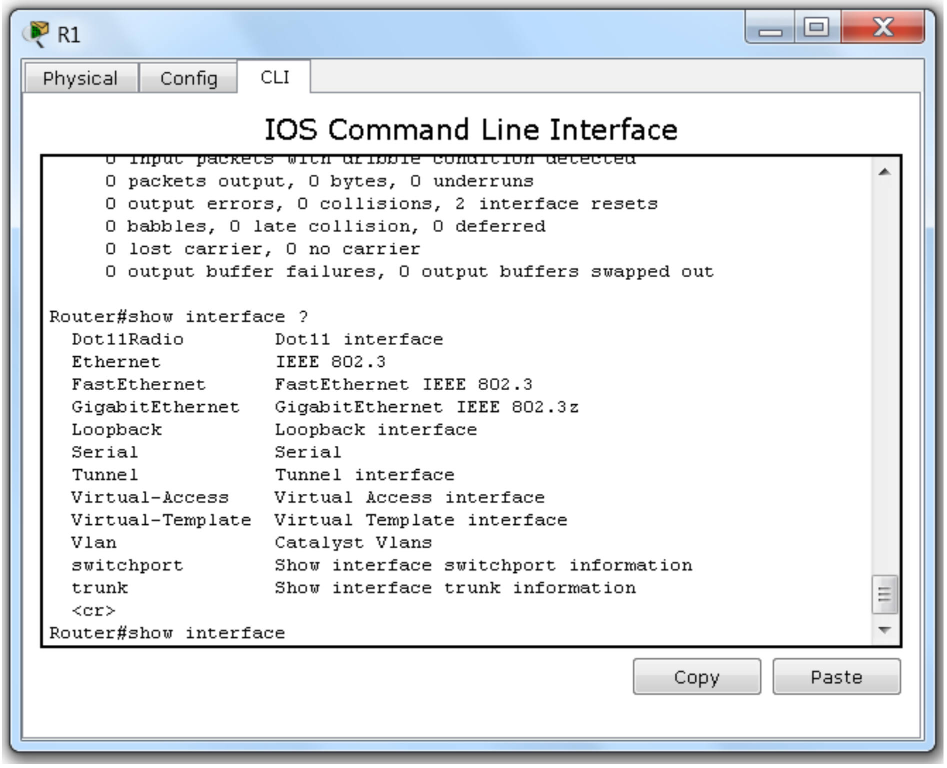
Just as your personal computer uses Microsoft Windows as its operating system, Cisco routers use an operating system as well. This software is referred to as **IOS**, or **Internetwork Operating System**, and different versions are introduced periodically. As a technician, you enter a series of configuration commands to tell the router what to do, and the IOS software then instructs the router to carry out those commands. **Configuration** commands are entered and stored in memory, even when the router is turned off, and perform various tasks. Other commands, such as **diagnostic** commands, are entered at the command line to tell the technician what the device happens to be doing. The purpose of this lab exercise is to familiarize you with some of these commands.

Press <enter> in the CLI screen to access the interface directly. If you want to display the interfaces on the router, type **show interface** and press **<enter>** and watch the output.



```
Router#show interfaces
FastEthernet0/0 is administratively down, line protocol is down (disabled
  Hardware is Lance, address is 0060.2f71.7d01 (bia 0060.2f71.7d01)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

One of the most helpful features in the Cisco IOS CLI is referred to as context-sensitive help, in which a user can use the **?** to get guidance on what commands are available for use. Going back to the previous command, type **show interface**, but instead of pressing <enter>, use the question mark (?) instead.



```
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Router#show interface ?
  Dot11Radio        Dot11 interface
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Loopback          Loopback interface
  Serial            Serial
  Tunnel            Tunnel interface
  Virtual-Access    Virtual Access interface
  Virtual-Template  Virtual Template interface
  Vlan              Catalyst Vlans
  switchport        Show interface switchport information
  trunk             Show interface trunk information
  <cr>
Router#show interface
```

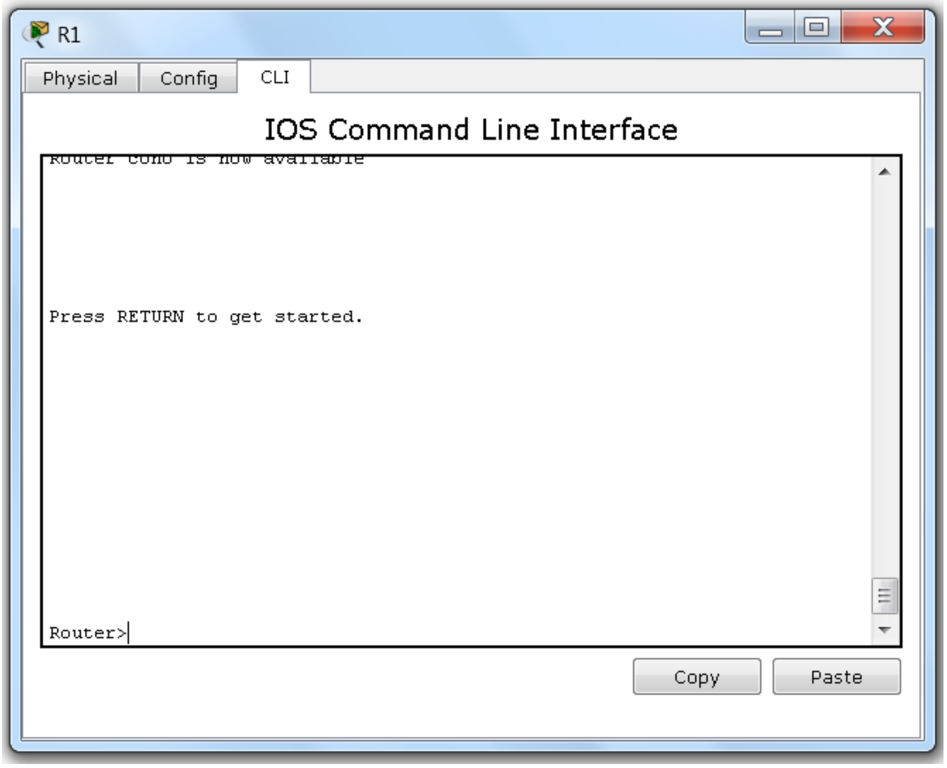
Notice the list of commands that are available just with this command alone. Don't worry about what all of them mean at this point, you will learn about many of them throughout upcoming lessons.

1.1.6. CLI Mode/Hierarchy

You probably understand levels of authority and responsibility from school, work, family, and other areas of life. Young children, for example, do not have the freedom to make life-altering choices, mostly for safety concerns. At work, you may have the latitude to do certain things on your own authority, while others you have to consult a supervisor or manager. The CLI has the same concept, with several levels of privileges and capabilities.

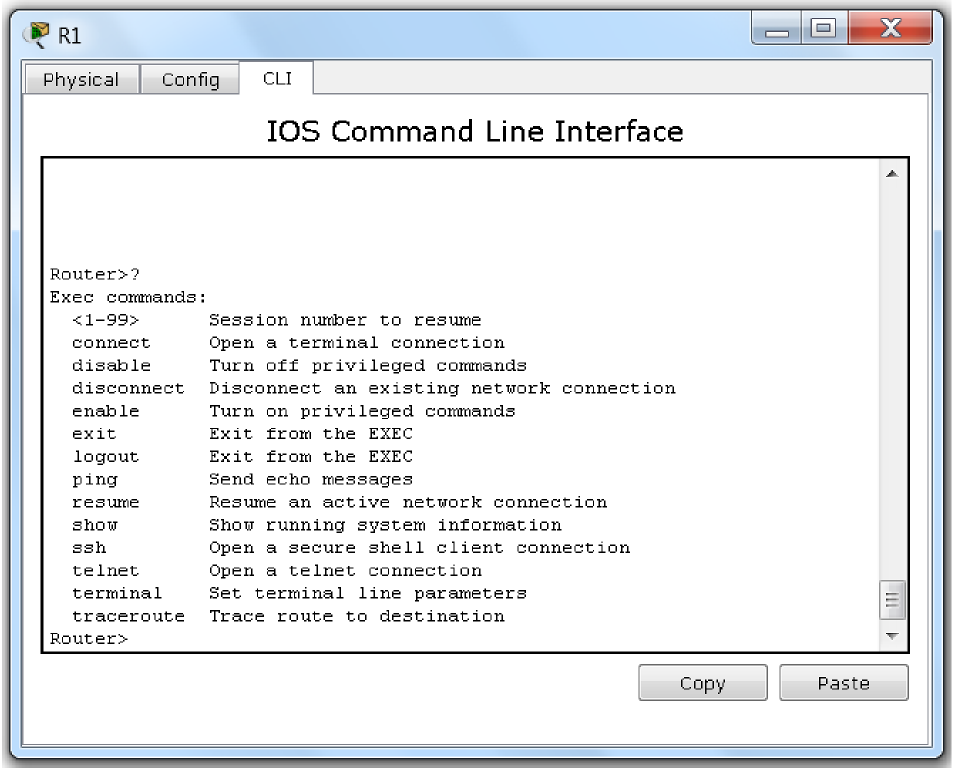
When you first log into a Cisco switch or router, you will notice right away that the device name is displayed (helpful for knowing which one you are accessing), as well as a character called a **prompt**. The prompt is your clue as to which level (more correctly referred to as **mode**) you are in. The first mode is called **user**

mode, or **exec mode** (exec = execution, or able to enter commands). The associated prompt is the **>** symbol, as you see here:



```
Router con0 is now available




Press RETURN to get started.













Router>
```

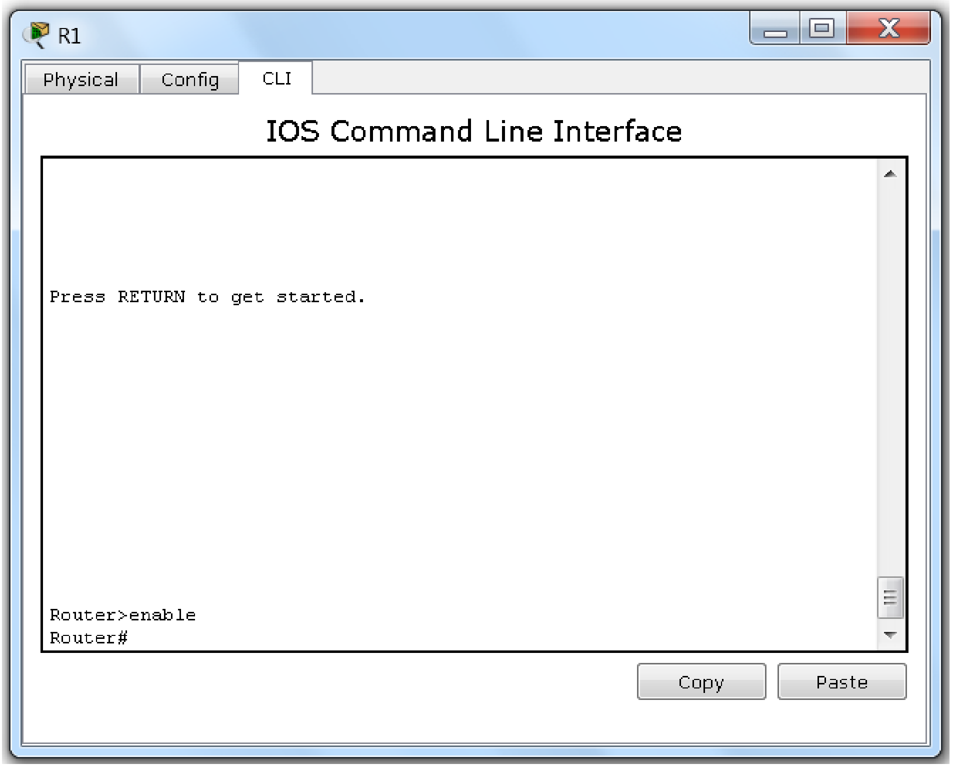
User mode is the lowest possible level in a Cisco device, and has restrictions in the commands allowed. If you use the **?** symbol at the command line, you will see a rather small list of diagnostic commands that are available.



```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Router>
```

In addition, you cannot view or make changes to the configuration of the device from this mode.

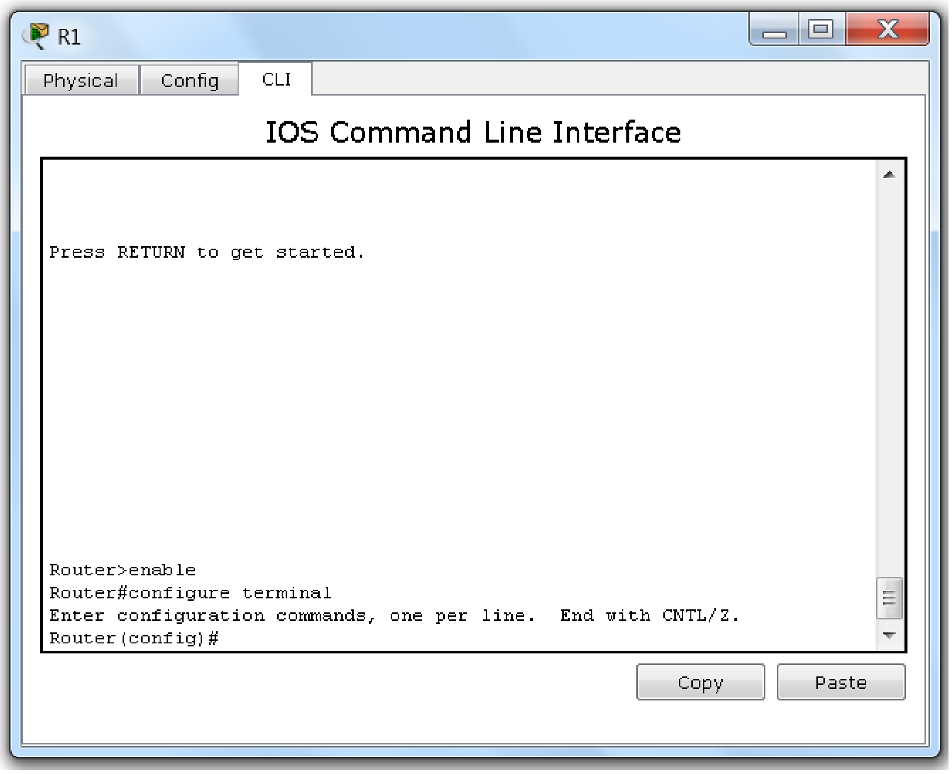
The second mode is called **privileged mode**, and allows the user to do anything they want with regard to the device (full privileges). To access, you simply enter the command **enable**, and to leave you use the **disable** command. Note the change in the prompt from the **>** symbol to the **#** symbol.



```
Press RETURN to get started.


Router>enable
Router#
```

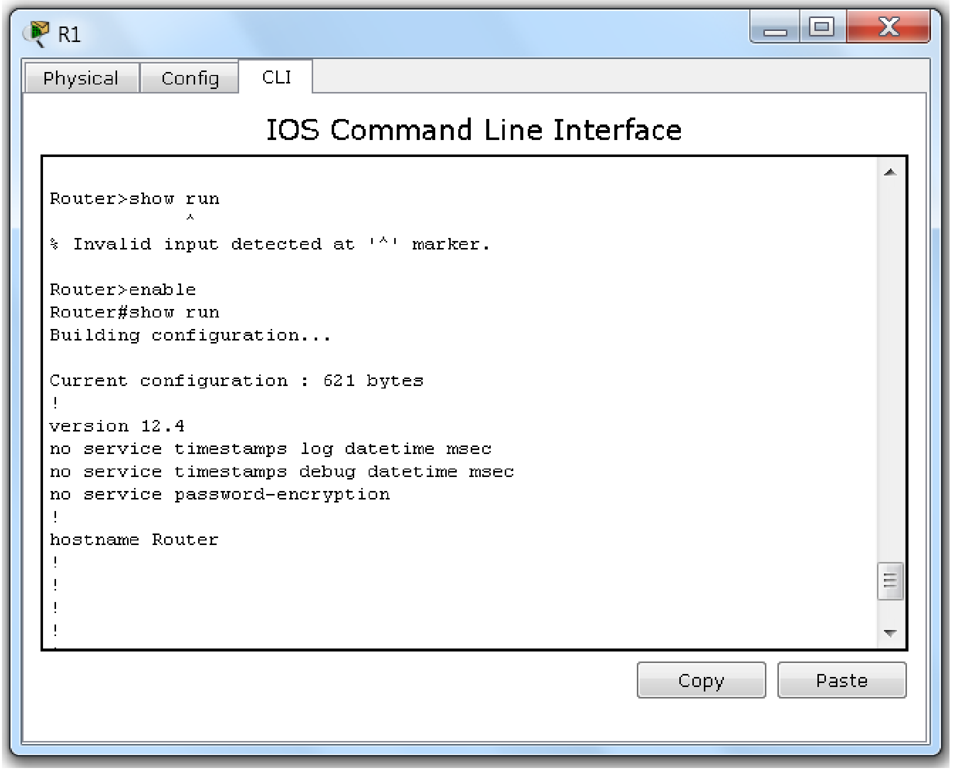
The final mode to consider is **configuration** mode, which also has a number of submodes that you will learn about later. As the name suggests, this is the mode in which network technicians enter configuration commands, which are stored in memory and executed. At this point it is a good idea to learn about the two types of configurations on a Cisco device:

- **running-configuration**: This is the active configuration running in memory on the device, and the configuration to which changes are applied when commands are entered from the CLI. When the device is switched off, this configuration is lost unless it is written to memory (and becomes the startup-configuration, as described below).
- **startup-configuration**: This is the configuration stored in long-term memory and remains on the device when powered off. When the device boots up, this configuration is loaded into active memory and becomes the running configuration.



```
Press RETURN to get started.









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

To display the (active) running-configuration, enter the command **show running-configuration** (may be abbreviated to **sh run**). To display the startup-configuration, use the command show **startup-configuration** (may be abbreviated **sh start**). Remember that these are only available in **privileged mode** (# prompt).



```
Router>show run
            ^
% Invalid input detected at '^' marker.

Router>enable
Router#show run
Building configuration...

Current configuration : 621 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
```

Lesson 3 Lab Exercises

Importance of Binary

As you learned in the video presentation, computers do not use the same method of calculation as human beings do; they count using two possible states of a circuit, on (**1**) or off (**0**). Binary truly is the key to understanding anything computer-related, including networking. If there truly is any secret to mastering computer networking, binary would win that contest handily. IP addressing and subnetting are topics that are much simpler with a grasp of binary.

Binary to Decimal Conversion Practice

Convert the following binary numbers to their decimal equivalents (answers to follow):

1.1.7. 00101010

1.1.8. 11110111

1.1.9. 11010101

1.1.10. 00001100

1.1.11. 00000100

1.1.12. 01000011

1.1.13. 10100010

1.1.14. 00000011

1.1.15. 00010101

1.1.16. 00010000

1.1.17. 11000001

1.1.18. 11110011

1.1.19. 01001001

1.1.20. 00101001

1.1.21. 00001001

1.1.22. 01111001

1.1.23. 00111110

1.1.24. 01100011

Decimal to Binary Conversion Practice

Convert the following decimal numbers to their binary equivalents (answers to follow):

1.1.25. 22

1.1.26. 9

1.1.27. 108

1.1.28. 101

1.1.29. 129

1.1.30. 42

1.1.31. 204

1.1.32. 73

1.1.33. 30

1.1.34. 204

1.1.35. 128

1.1.36. 192

1.1.37. 89

1.1.38. 12

1.1.39. 118

1.1.40. 67

1.1.41. 57

1.1.42. 252

Binary to Decimal Answer Key

1.1.43. 42

1.1.44. 247

1.1.45. 213

1.1.46. 12

1.1.47. 4

1.1.48. 67

1.1.49. 162

1.1.50. 3

1.1.51. 21

1.1.52. 16

1.1.53. 193

1.1.54. 243

1.1.55. 73

1.1.56. 41

1.1.57. 9

1.1.58. 121

1.1.59. 62

1.1.60. 99

Decimal to Binary Conversion Answer Key

1.1.61. 00010110

1.1.62. 00001001

1.1.63. 01101100

1.1.64. 00000101

1.1.65. 10000001

1.1.66. 00101010

1.1.67. 11001100

1.1.68. 01001001

1.1.69. 00011110

1.1.70. 11001100

1.1.71. 10000000

1.1.72. 11000000

1.1.73. 01011001

1.1.74. 00001100

1.1.75. 01110110

1.1.76. 01000011

1.1.77. 0111001

1.1.78. 011111100

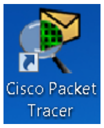
Lesson 4 Lab Exerci ses

Initial Device Configuration on R1

Now that you have started learning some of the principles of Cisco devices, it's time to start configuring devices. The layout of these lab exercises is progressive; each one builds upon the previous. When you have completed these tasks, you will have a fully functional network. Your tasks in this lab will be to perform initial configuration tasks on all devices.

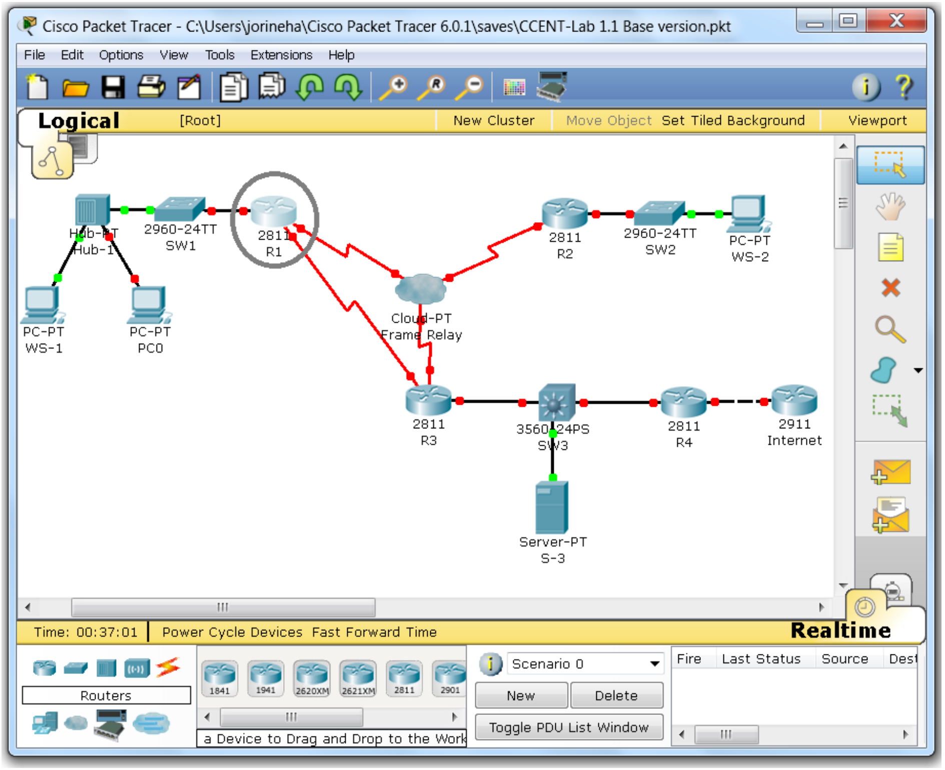
1.1.79. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



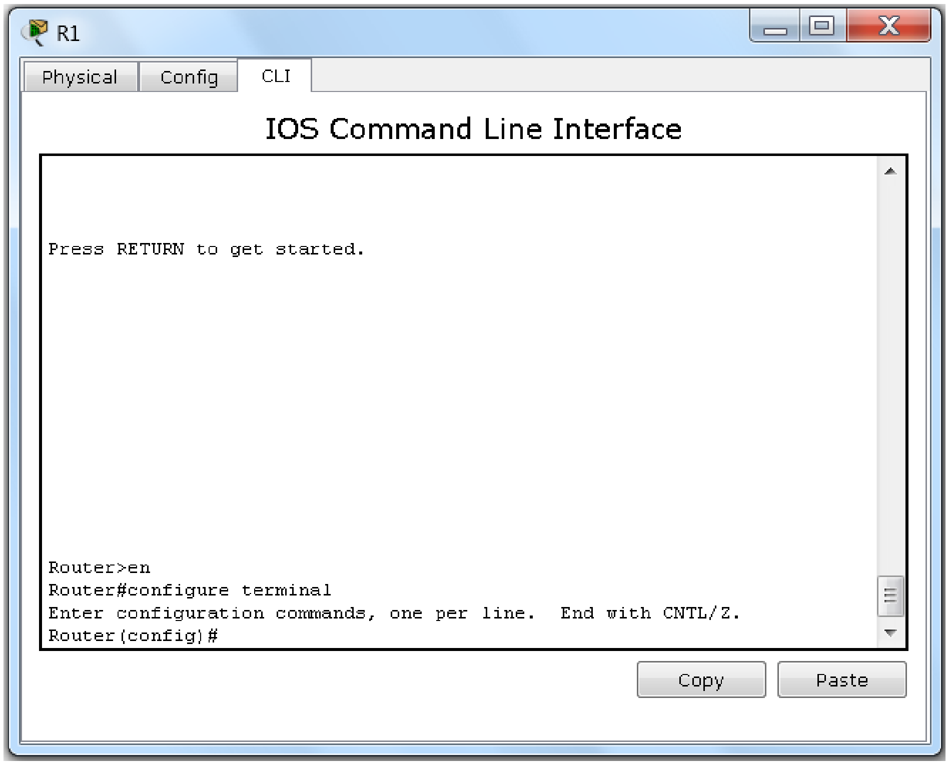
1.1.80. Select R1 by double clicking the image

Begin by accessing R1 by double clicking the image (as you did in the first lab exercise) to bring up the three tabbed device window and then click the CLI tab.


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCENT-Lab 1.1 Base version.pkt

1.1.81. Enter Configuration Mode

Once you the CLI screen, press **<enter>** to begin a terminal session to R1, and then issue the **enable** command to enter privileged mode. Remember, you cannot enter configuration mode from user exec mode (the **>** prompt); you must be in privileged mode (**#**) to do that. Finally, enter configuration mode with the **configure terminal** command (you are using a ***terminal session*** when accessing the CLI):



```
Press RETURN to get started.



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

1.1.82. Review Keyboard Shortcuts

Cisco IOS has a variety of line editing features that can assist you when you are configuring devices from the command line, especially for saving time. The following lists some of the more common ones:

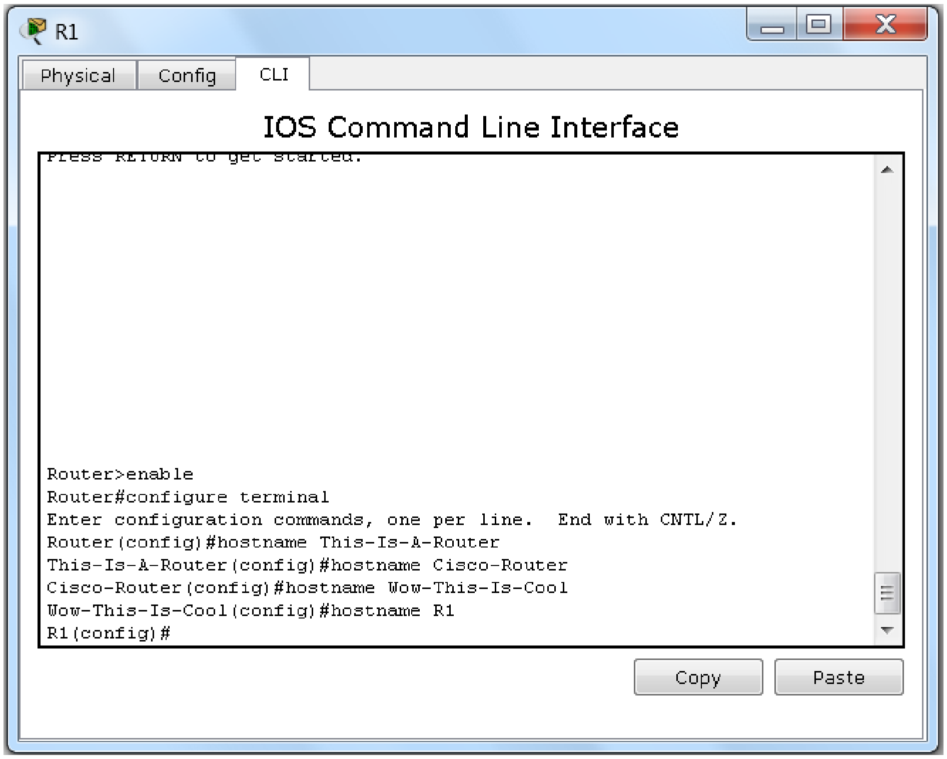
- **<Tab>**: One of the most valuable shortcuts, it automatically completes whatever command you are entering. If more than one command matches what you have typed (for example, typing the letter **c** from privileged mode), then you may need to enter more of the command for it to work. In this example, the letter c by itself is used in the commands **clear**, **clock**, **configure**, **connect** and **copy**.
- **Up Arrow:** This repeats the commands previously entered. If you press the key one time, the command just entered will be displayed. If you press it twice, the command before that will show, and so on.

- **<Ctrl>+a**: Moves the cursor to the beginning of the line being typed.
- **<Ctrl>+e**: Moves the cursor to the end of the line being typed.
- **<Ctrl>+w**: Deletes the previous word in the line.
- **<Ctrl>+u**: Deletes the entire line of text.

Try these shortcuts as you enter configuration commands. For a more complete list, perform a web search for ***cisco ios keyboard shortcuts***.

Configure the Hostname of the Device

One of the first configuration items entered on a Cisco device is the **hostname**, a term used in the networking world for the name of a device on the network. In most cases this name is just local to the device (in other words, only that device knows/controls what it is called). As an example of this principle, you may notice that ***all*** of the routers and switches in the lab topology have the default name of ***Router*** and ***Switch***. To change the existing name of a device, execute the command hostname command, followed by the desired name, as follows:

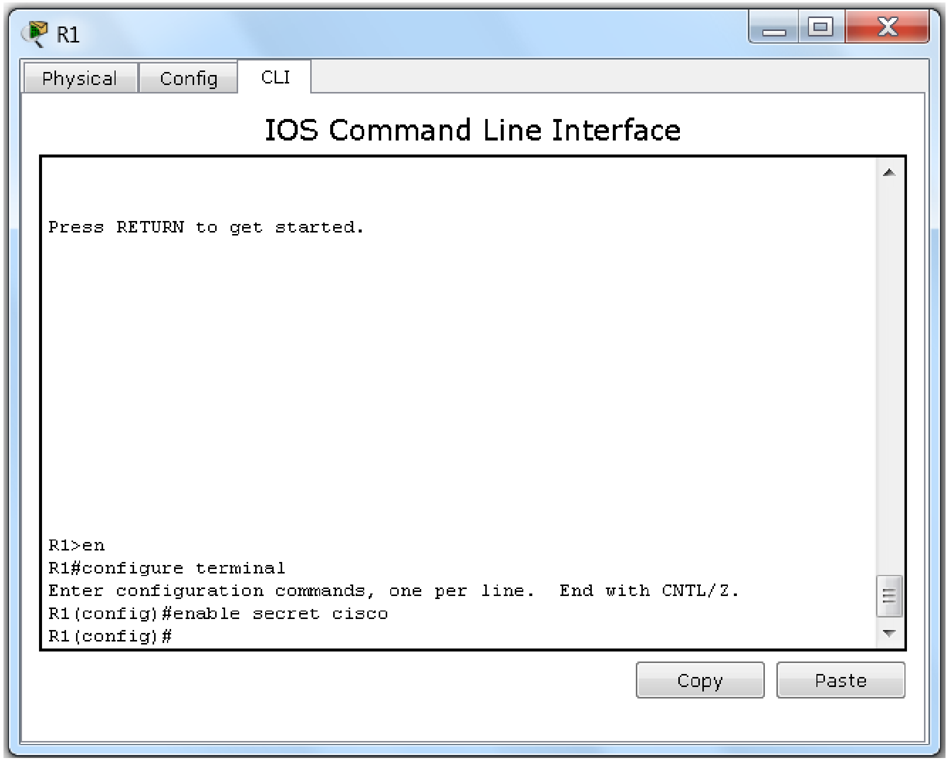


```
Press RETURN to get started.




Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname This-Is-A-Router
This-Is-A-Router(config)#hostname Cisco-Router
Cisco-Router(config)#hostname Wow-This-Is-Cool
Wow-This-Is-Cool(config)#hostname R1
R1(config)#
```

One thing to notice right away is that the hostname changes in the command line display, to whatever set of characters you enter. In most networks, the hostname reflects the function, location, or significance. In our network, the name of the device is ***R1***, meaning ***Router 1***. Repeat this same process for the rest of the following devices:

Configure the Enable/Enable Secret Password

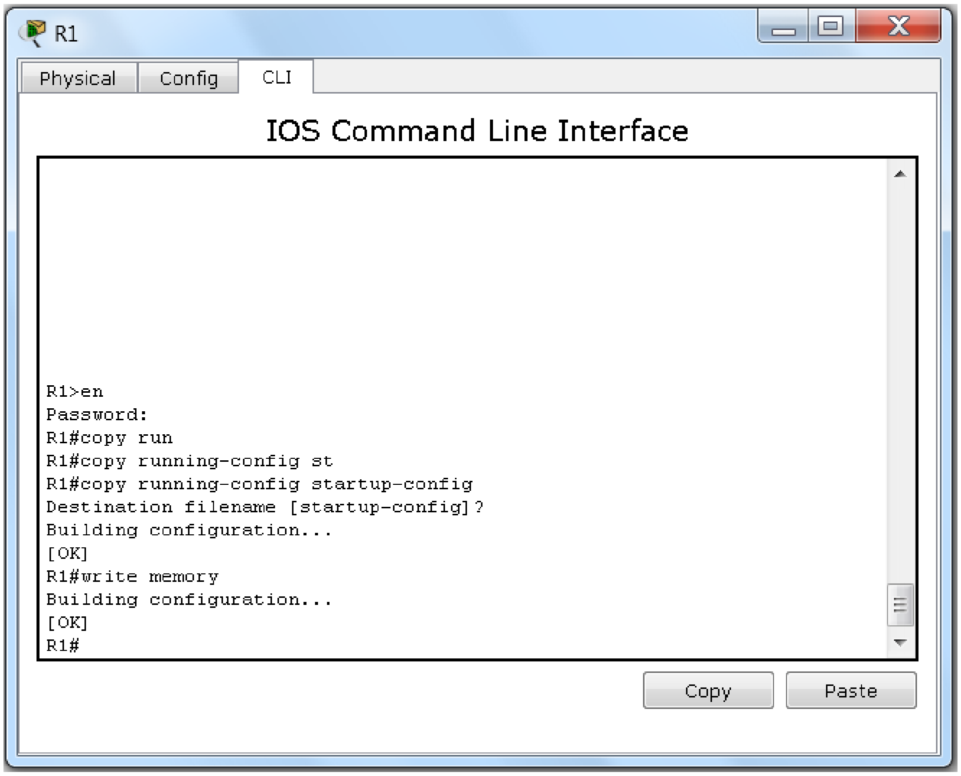
Up to this point, you have been able to get into privileged mode on the devices in the lab simply by pressing the **<enter>** key. In production networks, this would leave critical devices open to anyone and allow unauthorized personnel to make changes (a thoroughly undesirable situation). This points out the obvious need to protect these higher modes, which is accomplished through the use of the **enable password** or **enable secret** password commands. These both accomplish the same thing, but **enable secret** encrypts the stored password, while **enable password** does not. Use the command **enable secret cisco** to configure this security feature with ***cisco*** as the password:



```
Press RETURN to get started.







R1>en
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret cisco
R1(config)#
```

Write the Changes to Memory

When you make changes on a Cisco IOS device, you alter the configuration held in active memory (***RAM***, or ***Random Access Memory***). If you are familiar with computers, you may remember that once you shut the device down, everything in RAM is lost. This is the reason for the two configuration files referred to earlier, the ***running-configuration*** (running in RAM), and startup-configuration (stored in more permanent memory, called ***nonvolatile RAM*** or ***NVRAM***). In order to save the changes that you made to the **running-configuration**, you need to copy it to the **startup-configuration**, as follows:



```
R1>en
Password:
R1#copy run
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#write memory
Building configuration...
[OK]
R1#
```

Initial Device Configuration on Remaining Cisco Devices

Perform the previous steps on the following lab devices. Make certain that you save your configuration. You may do so with the **copy running-config startup-config** or the **write memory** commands.

- **R2**
- **R3**
- **R4**
- **SW1**
- **SW2**
- **SW3**

**** NOTE: Do not configure the Internet router, which is already configured, nor the workstations, servers, or the hub ****

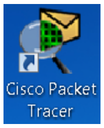
Lesson 5 Lab Exercises

SW1 Interface Discovery

To reinforce the concepts from Local Area Network Fundamentals

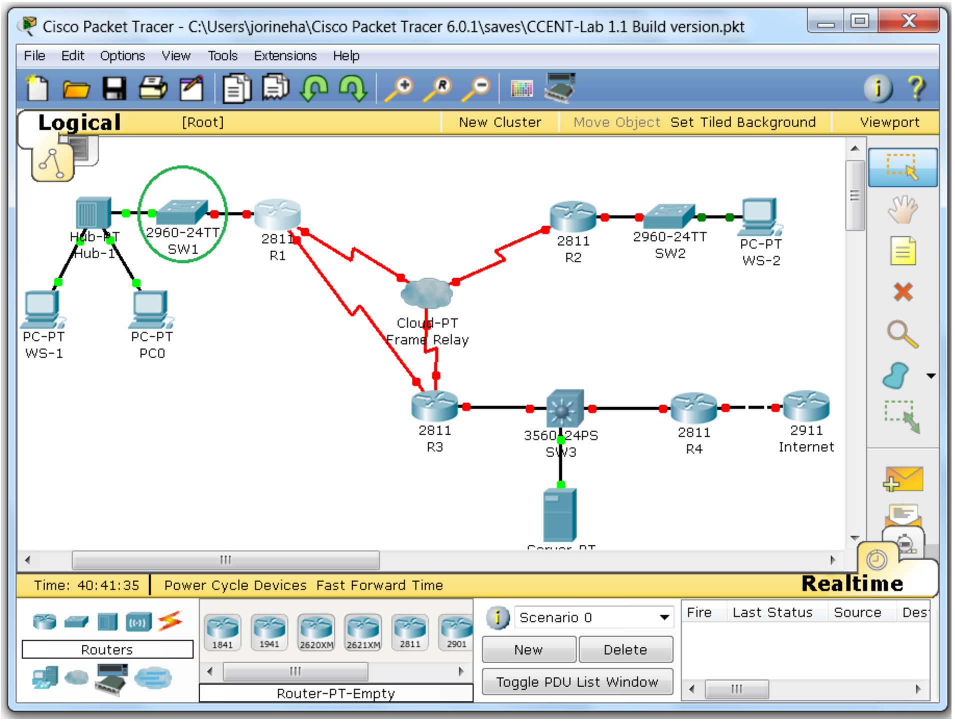
1.1.83. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



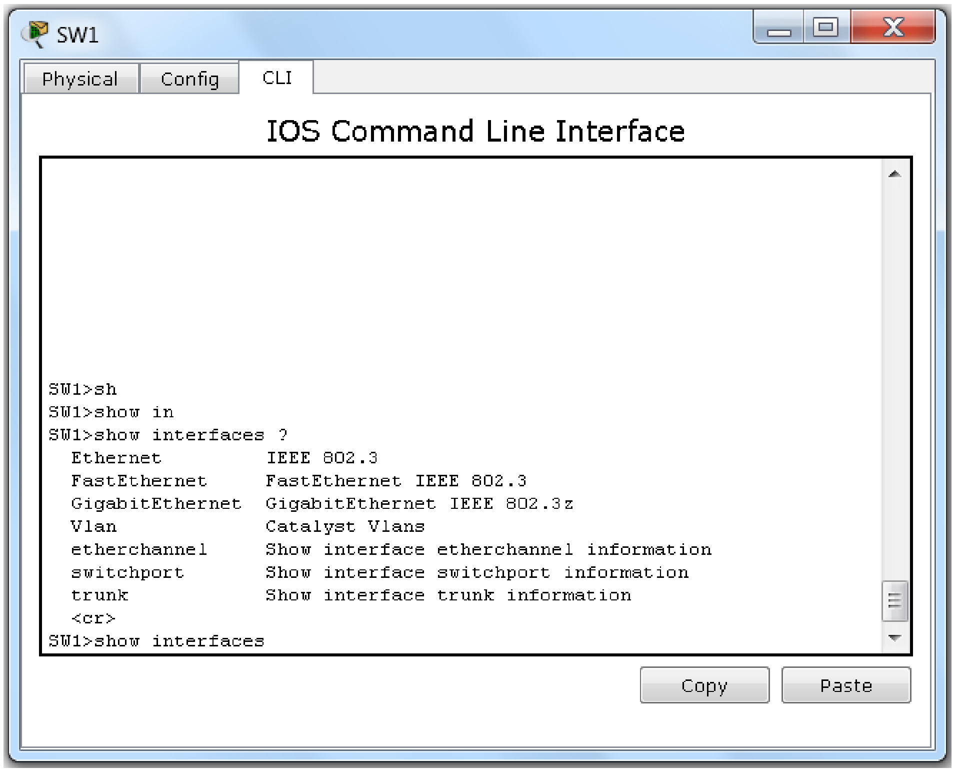
1.1.84. Select SW1 by double clicking the image

Begin by accessing SW1 by double clicking the image (as you did in the first lab exercise) to bring up the three tabbed device window and then click the CLI tab.



1.1.85. Review Cisco Interface Naming Conventions

Once inside the command line interface of SW1, type the command **show interface ?** in order to see the interface types available on a Cisco LAN switch. The output should be as follows:



```
SW1>sh
SW1>show in
SW1>show interfaces ?
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Vlan              Catalyst Vlans
  etherchannel      Show interface etherchannel information
  switchport        Show interface switchport information
  trunk             Show interface trunk information
  <cr>
SW1>show interfaces
```

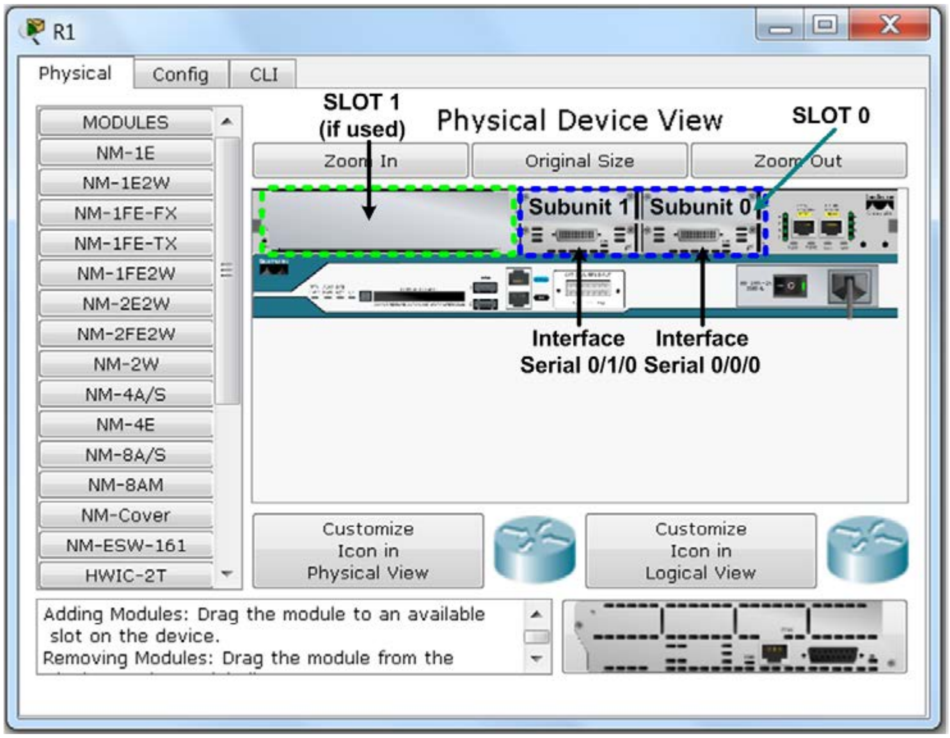
As mentioned before, in a Cisco Local Area Network switch only supports LAN (that is, Ethernet) interfaces, all of which are displayed here. The interpretation of this output is below:

- **Ethernet:** 10 Mbps (megabits per second), IEEE 802.3/10BASE-T
- **FastEthernet:** 100 Mbps, IEEE 802.3u/100BASE-TX
- **GigabitEthernet:** 1000 Mbps, 1 Gbps (gigabits per second):
  - IEEE 802.3z/1000BASE-LX/SX
  - IEEE 802.3ab/1000BASE-TX
- **VLAN**: Virtual LAN (covered in subsequent lessons/labs)
- **Etherchannel:** Link bonding mechanism (covered in subsequent lessons/labs)
- **Switchport:** Ethernet Port/VLAN information (covered in subsequent lessons/labs)
- **Trunk:** Switch-to-Switch/Some Switch-to-Router connections (covered in subsequent lessons/labs)

1.1.86. Understand Cisco Port/Slot Interface References.

In addition to the Ethernet interface speed naming, you need to understand the way in which Cisco devices (both routers and switches) refer to the various ports. Most interfaces are references using the format **interface <*type*> <*slot*>/<*port*>** or **interface <*type*> <*slot*>/<subunit>/<*port*>,** which refer to the where that specific is port is located on the device, as follows:

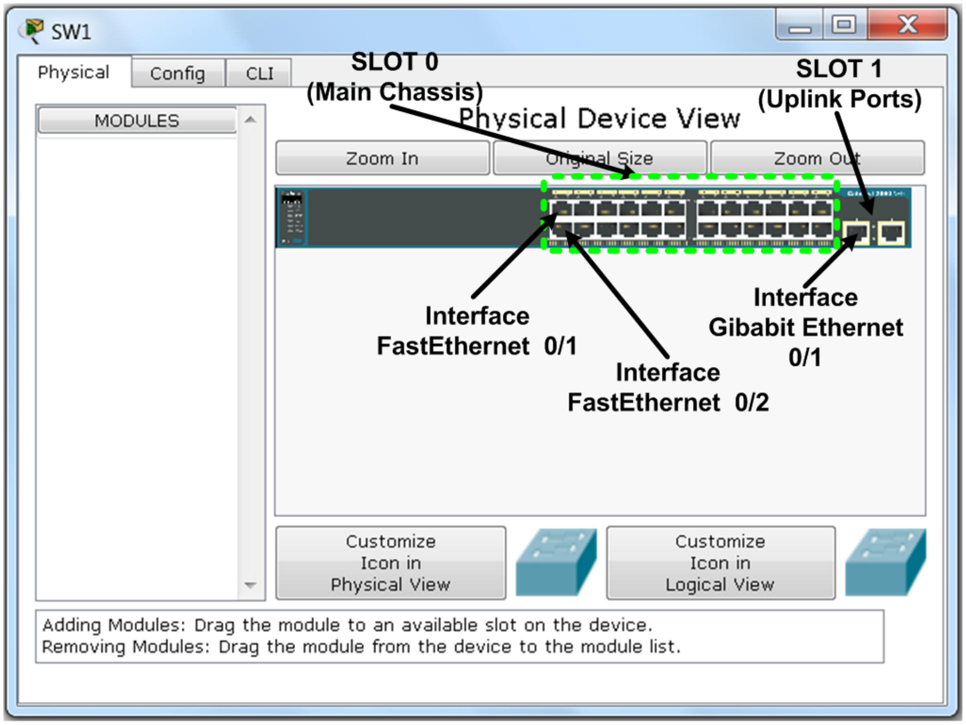
- **Routers:** Several Interface types, naming as follows:



Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the

  - **Slot:** On routers there are usually 2 slots, numbered 0 and 1. On the 2811 model pictured in Packet Tracer, Slot 0 includes the onboard FastEthernet interfaces as well as expansion slots. Slot 1 is for a larger class of expansion device called a ***Network Module***. Interfaces on a Network Module would be **<type> 1/**X, with X=the port number on the module. Some routers, such as the 2811, also have a subunit number.
  - **Port:** Within a slot, the ports are numbered starting with 0, and ending with whatever physical port is present. Using the 2811 onboard FastEthernet interfaces as an example, these belong to Slot 0, with the first port being 0 and the second being one. Thus they would be referred to ***FastEthernet 0/0*** and ***0/1***, respectively. The smaller expansion interface adapters are referred to as ***WAN Interface Cards***, or ***WICs*** for short. The references for these are slightly different for these; these specific cards contain ***Serial*** interfaces (more on these later). The first adapter is in ***slot 0*** (main chassis), in ***subunit 0***) on the right), and ***port 0*** of that subunit (***port 1*** would be above it if installed). Thus, the reference for these interfaces would be ***Serial 0/0/0*** and ***Serial 0/1/0*** respectively.

- **Switches:** Ethernet interface types, simpler naming as follows:



Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the device to the module list.

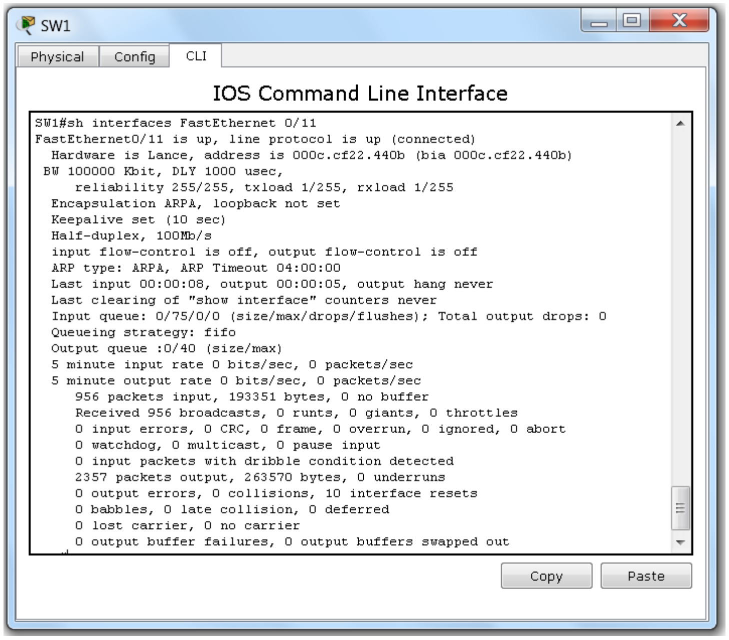
  - **Slot**: An important distinction exists on switches, in that the designation for the slot for chassis-based switches (that is, those with multiple adapter cards) and the smaller stacking type switches, as pictured above. Typically, ***Slot 0*** is either the entire chassis, or the main chassis. Using the Cisco Catalyst 2960 switch above, ***Slot 0*** is the main chassis, which commonly houses between 24-48 Ethernet ports, and ***Slot 1*** houses the uplinks. Understanding this explains how to identify the interfaces assignments, some of which are labeled above for reference.

SW1 Media Access Control (MAC) Addressing

Devices on a Local Area Network (LAN) have addresses to enable communication between themselves and others. **Unicast** addresses enable messaging between a pair of devices alone, much like when you might carry on a personal conversation. There is only one broadcast address, which makes announcements to every device on a local area network (address ***FFFF.FFFF.FFFF***, the highest mathematically possible MAC address). Final, there is the multicast LAN address, which uses the format ***0100.5eXX.XXXX***, which enables communication between a specific set of devices. You will examine some LAN addresses on SW1 in the lab environment, as outlined below:

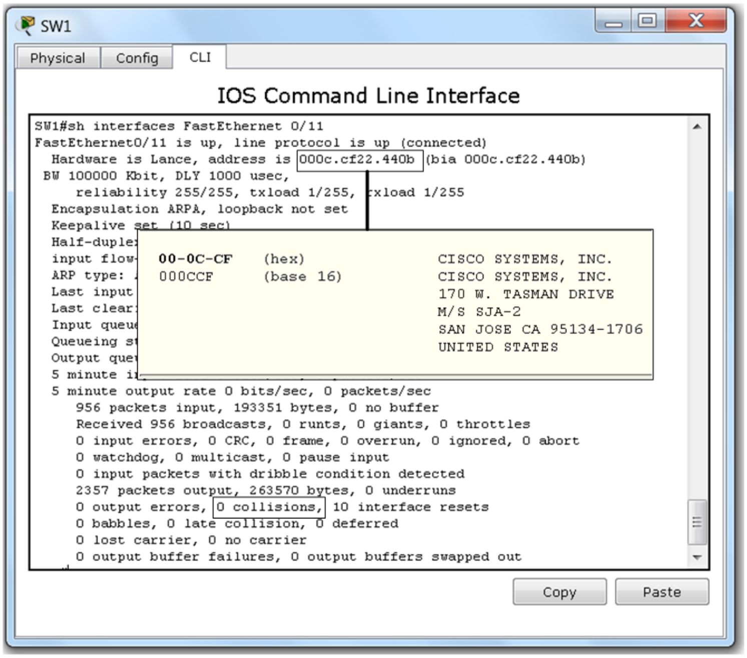
1.1.87. Examine LAN Addresses on an Ethernet Interface.

Return to the SW1 CLI and log back in if your terminal session has timed out. Once back in privileged mode, issue the command show interface Fa0/11, which will display the following output:



```
SW1#sh interfaces FastEthernet 0/11
FastEthernet0/11 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.cf22.440b (bia 000c.cf22.440b)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

While this might look a little overwhelming at first glance, you will probably not need to reference a number of items on this page. Since the subject of the accompanying lesson is ***LAN Fundamentals***, there are only two items to pay attention to:



```
SW1#sh interfaces FastEthernet 0/11
FastEthernet0/11 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.cf22.440b (bia 000c.cf22.440b)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, xload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duple
  input flow-
  ARP type: 
  Last input
  Last clear
  Input queu
  Queueing st
  Output que
  5 minute i
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

```
00-0C-CF     (hex)                CISCO SYSTEMS, INC.
000CCF       (base 16)            CISCO SYSTEMS, INC.
                                  170 W. TASMAN DRIVE
                                  M/S SJA-2
                                  SAN JOSE CA 95134-1706
                                  UNITED STATES
```

- **Address is 000c.cf22.440b:** This is the hardware or ***Media Access Control/LAN Address***, used by Layer 2 devices for LAN communication. Remember that the first half of the address is the ***OUI*** (vendor code), and you can see that this one belongs to Cisco. Since the address does not contain ***FFFF*** or ***0100.5e,*** you can safely conclude that this is a unicast address.
- **0 (zero) Collisions:** This refers to the number of frames that have collided on the LAN, which is a direct result of the operation of the ***Carrier Sense Multiple Access with Collision Detect*** mechanism used by Ethernet.

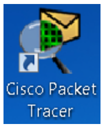
Lesson 6 Lab Exercises

R1 Interface Configurations

To reinforce the concepts from LAN Hubs, Repeaters & Switches

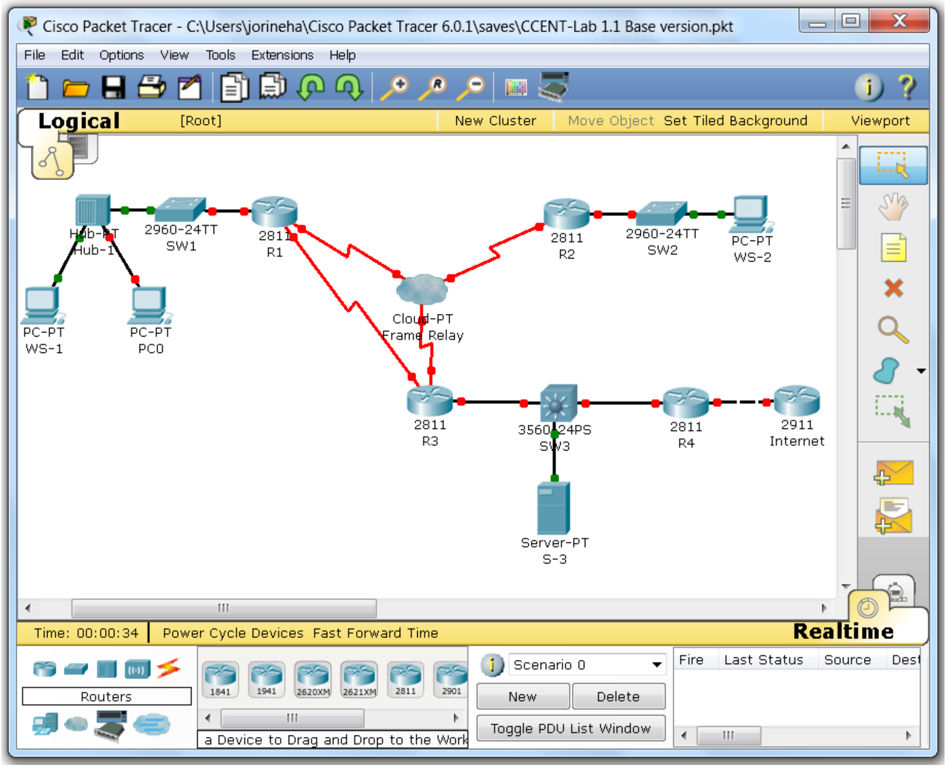
1.1.88. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



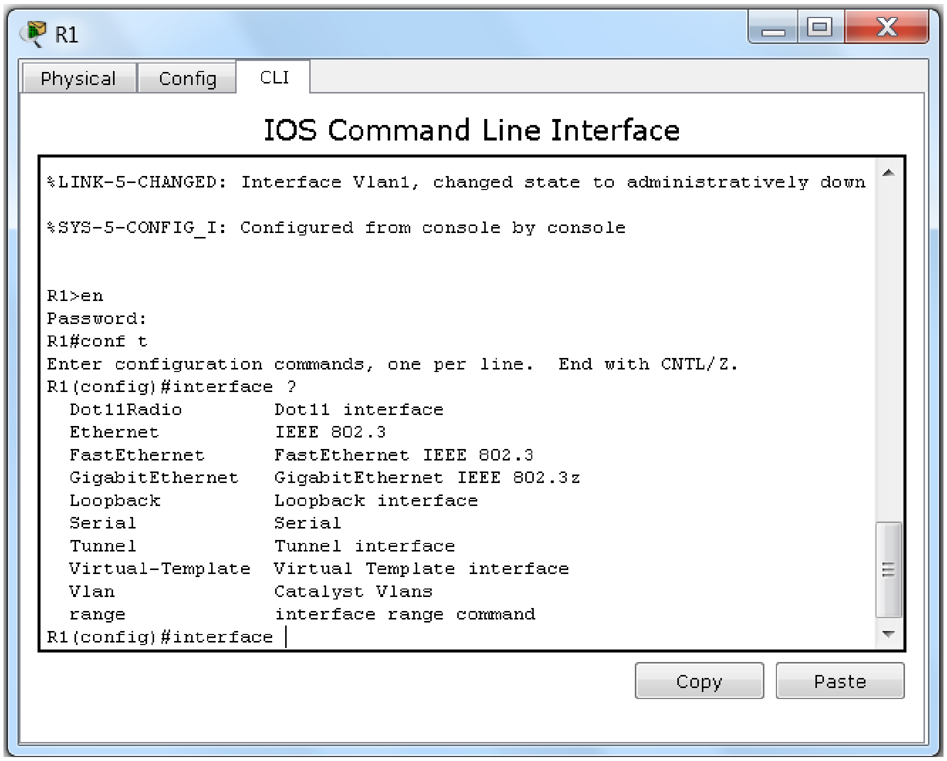
1.1.89. Select R1 by double clicking the image

Begin by accessing R1 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCENT-Lab 1.1 Base version.pkt

1.1.90. Review Available Interface Types on R1

Once inside the command line interface of R1, type the command **show interface ?** in order to see the interface types available on a Cisco router. The output should be as follows:



```
%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down

%SYS-5-CONFIG_I: Configured from console by console


R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface ?
  Dot11Radio        Dot11 interface
  Ethernet          IEEE 802.3
  FastEthernet      FastEthernet IEEE 802.3
  GigabitEthernet   GigabitEthernet IEEE 802.3z
  Loopback          Loopback interface
  Serial            Serial
  Tunnel            Tunnel interface
  Virtual-Template  Virtual Template interface
  Vlan              Catalyst Vlans
  range             interface range command
R1(config)#interface
```

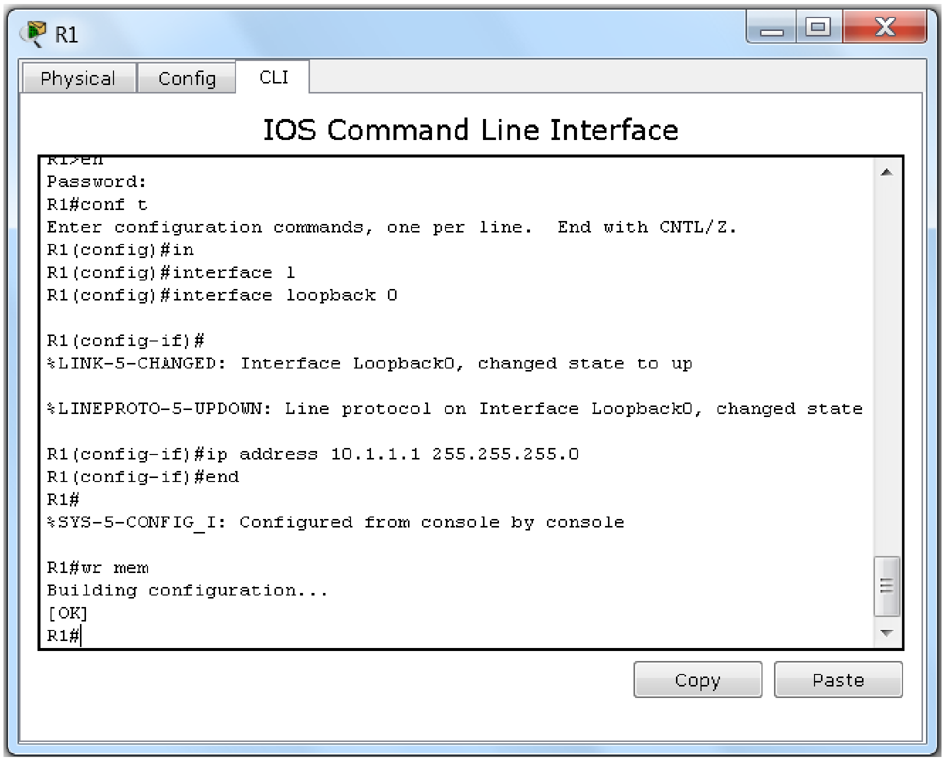
As mentioned before, Cisco routers support multiple interfaces types, depending on the installed cards, some of which are displayed here. The interpretation of this output is below:

- **Dot11Radio:** 802.11 wireless interfaces (2.4 or 5 GHz)
- **Ethernet:** 10 Mbps (megabits per second), IEEE 802.3/10BASE-T
- **FastEthernet:** 100 Mbps, IEEE 802.3u/100BASE-TX
- **GigabitEthernet:** 1000 Mbps, 1 Gbps (gigabits per second):
  - IEEE 802.3z/1000BASE-LX/SX
  - IEEE 802.3ab/1000BASE-TX
- **Loopback**: A virtual interface that exists only on the router. These are used for a variety of purposes which is a topic covered later
- **Serial:** So named due to the fact that data is sent in a stream (***series***, hence the name ***seri-al***), and usually used for Wide Area Network (WAN) connection types.
- **Tunnel:** A logical interface used to create a virtual IP-based connection across a network. Often utilized with Virtual Private Networks (VPN’s) and other special purposes

- **Virtual-Template:** Used for forming dynamically created interfaces (beyond ICND1/2 subject matter)
- **VLAN:** Logical LAN interface, more often used in LAN switching environments
- **range:** Not an interface type per-se, but a macro (process) that can be used to configure groups of the same interface types at one time

1.1.91. Create a Loopback Interface

As mentioned above, loopback interfaces do not exist physically on the router, as is the case with actual ports on the router (e.g., FastEthernet, Serial, etc.). Instead, they exist ***virtually*** in software, and only on the device they exist on. Since the interface cannot go down unless the device is shut off, it can serve as a control point for all types of router processes. Configuration of a loopback interface is a simple process, as outlined here:



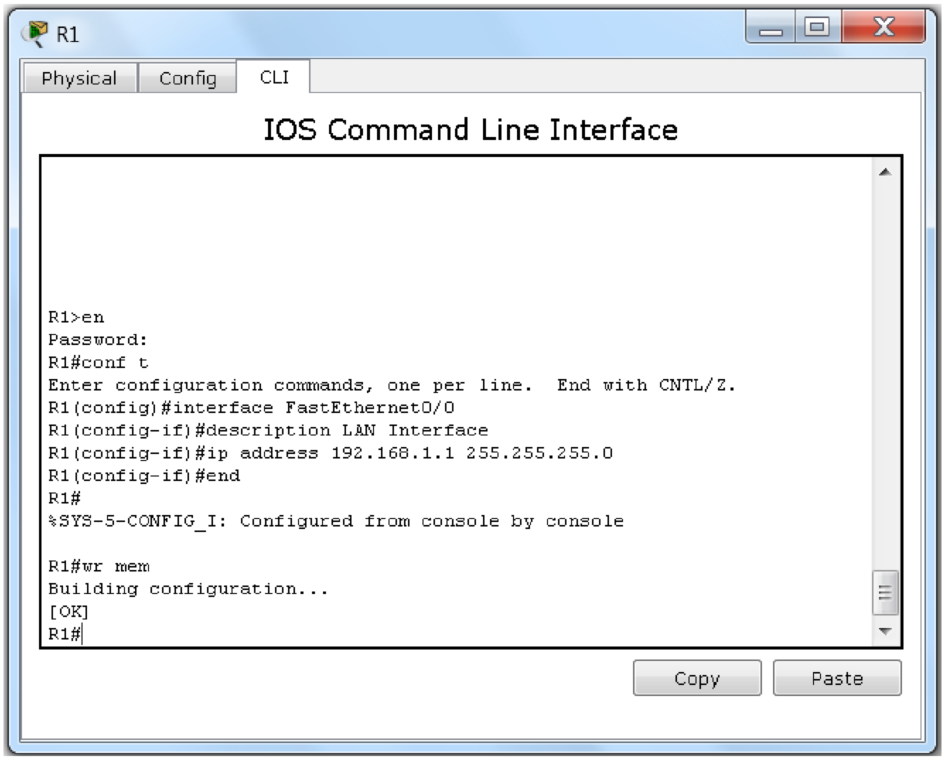
```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#in
R1(config)#interface l
R1(config)#interface loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state

R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr mem
Building configuration...
[OK]
R1#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface loopback 0** (you can use any number available if you like).

- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 10.1.1.1 255.255.255.255** without worrying about what the numbers mean at this point.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.92. Configure the LAN Interface

Configuring the physical Local Area Network interface is identical to that of the loopback interface, as follows:



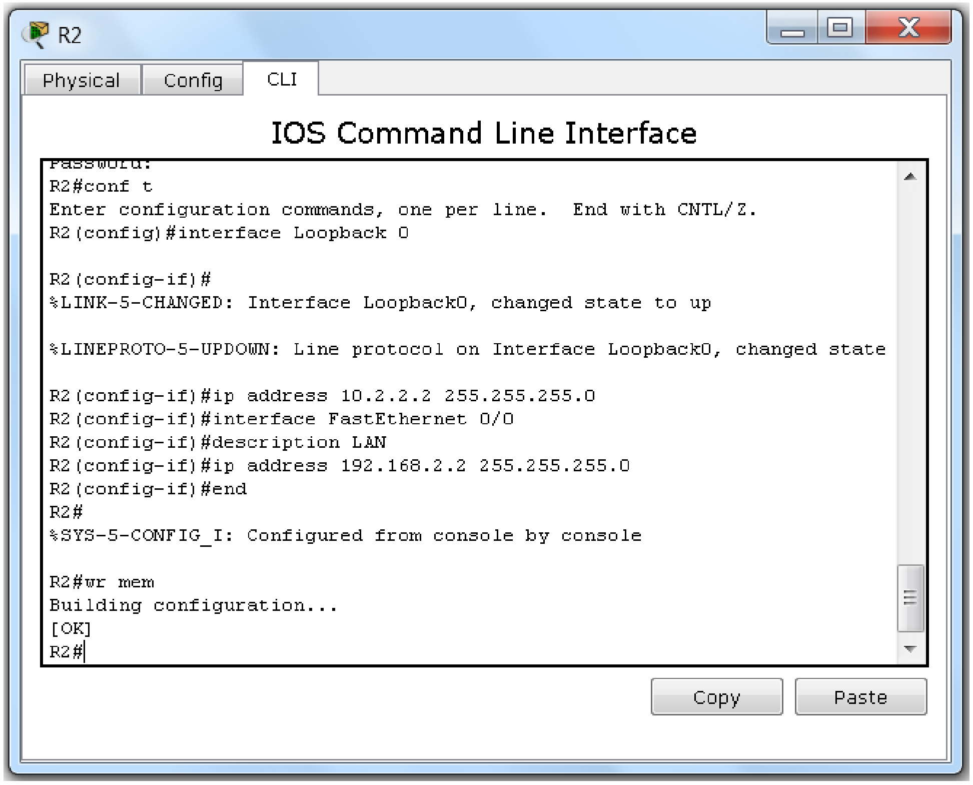
```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#description LAN Interface
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr mem
Building configuration...
[OK]
R1#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)

- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface FastEthernet 0/0** (remember the slot/port format discussed earlier?).
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.1.1 255.255.255.0** without worrying about what the numbers mean at this point.
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

R2 Interface Configurations

These steps are identical to the previous ones you have already performed, with the exception of IPv4 addressing information. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface Loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state

R2(config-if)#ip address 10.2.2.2 255.255.255.0
R2(config-if)#interface FastEthernet 0/0
R2(config-if)#description LAN
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr mem
Building configuration...
[OK]
R2#
```

1.1.93. Create a Loopback Interface

As mentioned above, loopback interfaces do not exist physically on the router, as is the case with actual ports on the router (e.g., FastEthernet, Serial, etc.). Instead, they exist ***virtually*** in software, and only on the device they exist on. Since the interface cannot go down unless the device is shut off, it can serve as a control point for all types of router processes. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface loopback 0** (you can use the shorter version ***Lo0*** if you like).
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 10.2.2.2 255.255.255.255** without worrying about what the numbers mean at this point.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.94. Configure the LAN Interface

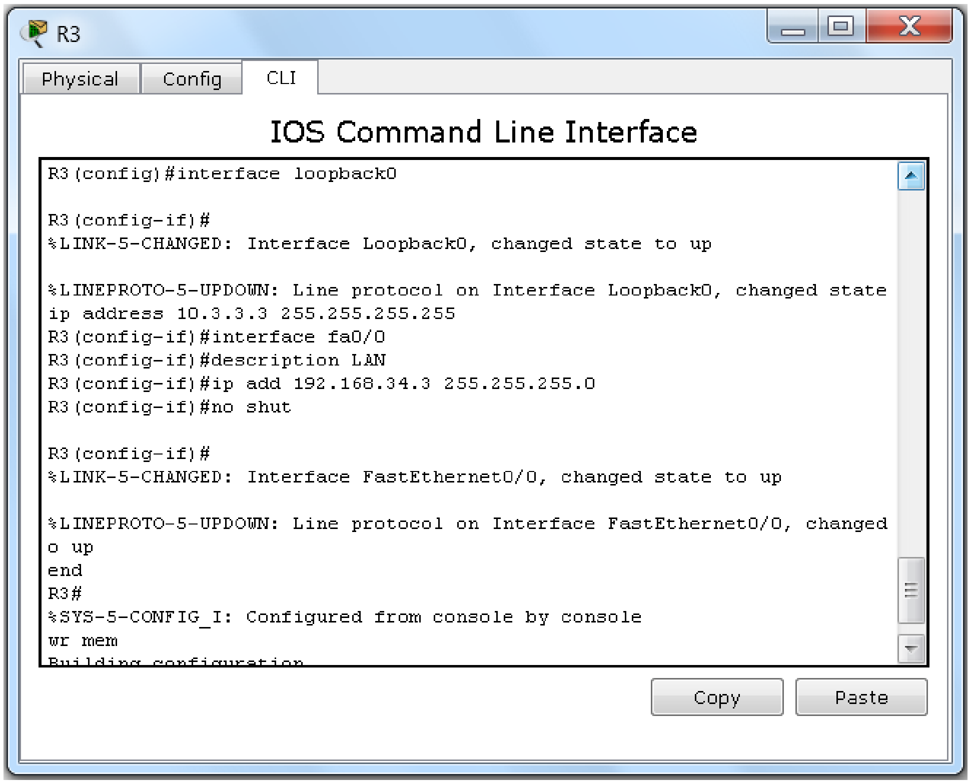
Configuring the physical Local Area Network interface is identical to that of the loopback interface, as follows:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface FastEthernet 0/0** you can also use the shorter ***Fa0/0***).

- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.2.2 255.255.255.0** without worrying about what the numbers mean at this point.
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

R3 Interface Configurations

These steps are identical to the previous ones you have already performed, with the exception of IPv4 addressing information. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
R3(config)#interface loopback0

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
ip address 10.3.3.3 255.255.255.255
R3(config-if)#interface fa0/0
R3(config-if)#description LAN
R3(config-if)#ip add 192.168.34.3 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
o up
end
R3#
%SYS-5-CONFIG_I: Configured from console by console
wr mem
Building configuration
```

1.1.95. Create a Loopback Interface

As mentioned above, loopback interfaces do not exist physically on the router, as is the case with actual ports on the router (e.g., FastEthernet, Serial, etc.). Instead, they exist ***virtually*** in software, and only on the device they exist on. Since the interface cannot go down unless the device is shut off, it can serve as a control point for all types of router processes. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface loopback 0** (you can use the shorter version ***Lo0*** if you like).
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 10.3.3.3 255.255.255.255** without worrying about what the numbers mean at this point.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.96. Configure the LAN Interface

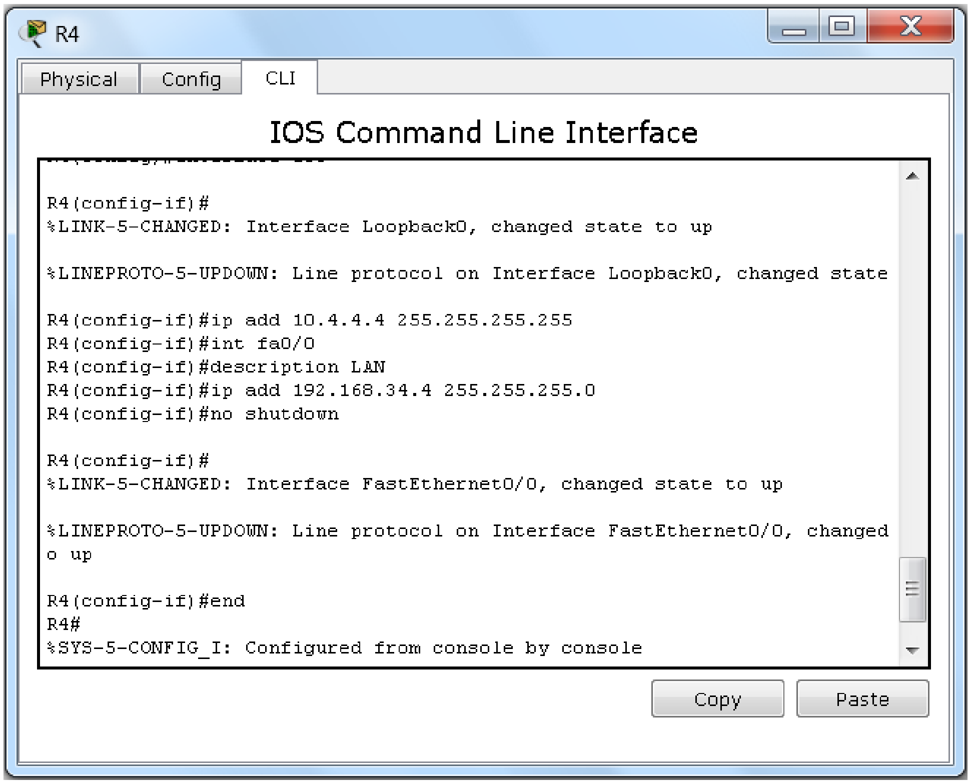
Configuring the physical Local Area Network interface is identical to that of the loopback interface, as follows:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface FastEthernet 0/0** you can also use the shorter ***Fa0/0***).

- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.34.3 255.255.255.0** without worrying about what the numbers mean at this point.
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

R4 Interface Configurations

These steps are identical to the previous ones you have already performed, with the exception of IPv4 addressing information. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state

R4(config-if)#ip add 10.4.4.4 255.255.255.255
R4(config-if)#int fa0/0
R4(config-if)#description LAN
R4(config-if)#ip add 192.168.34.4 255.255.255.0
R4(config-if)#no shutdown

R4(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
o up

R4(config-if)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console
```

1.1.97. Create a Loopback Interface

As mentioned above, loopback interfaces do not exist physically on the router, as is the case with actual ports on the router (e.g., FastEthernet, Serial, etc.). Instead, they exist ***virtually*** in software, and only on the device they exist on. Since the interface cannot go down unless the device is shut off, it can serve as a control point for all types of router processes. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface loopback 0** (you can use the shorter version ***Lo0*** if you like).
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 10.4.4.4 255.255.255.255** without worrying about what the numbers mean at this point.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.98. Configure the LAN Interface

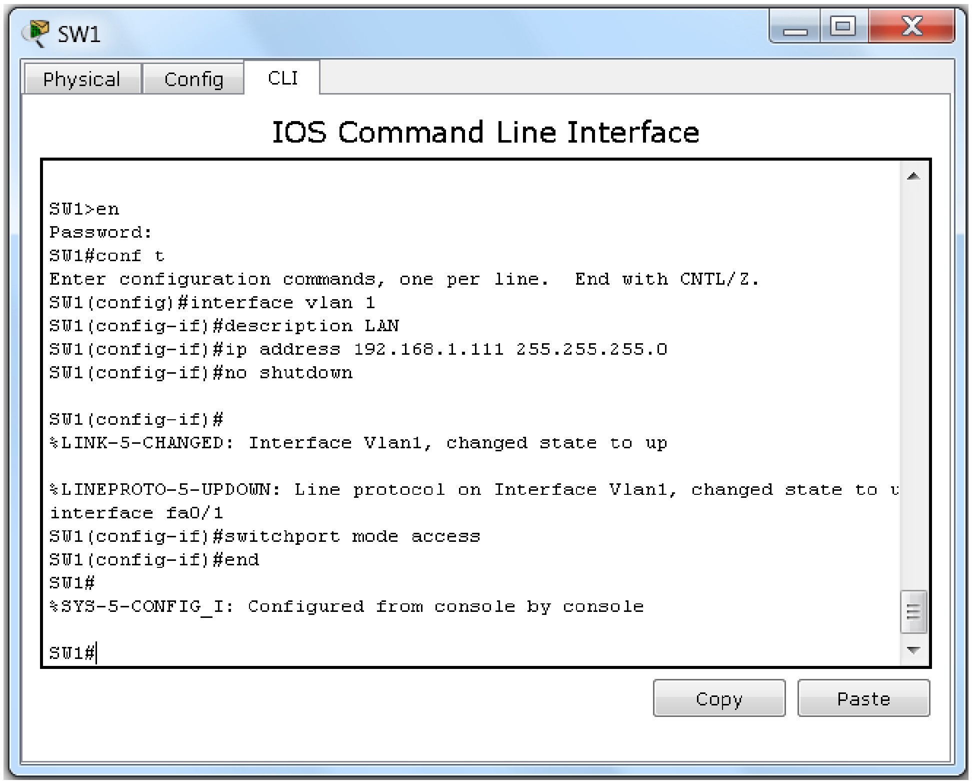
Configuring the physical Local Area Network interface is identical to that of the loopback interface, as follows:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface FastEthernet 0/0** you can also use the shorter ***Fa0/0***).

- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.34.4 255.255.255.0** without worrying about what the numbers mean at this point.
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

SW1 Interface Configurations

The interface configuration processes on Cisco switches have many similarities to those of their router counterparts, but differences as well. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
SW1>en
Password:
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface vlan 1
SW1(config-if)#description LAN
SW1(config-if)#ip address 192.168.1.111 255.255.255.0
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to u
interface fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#
```

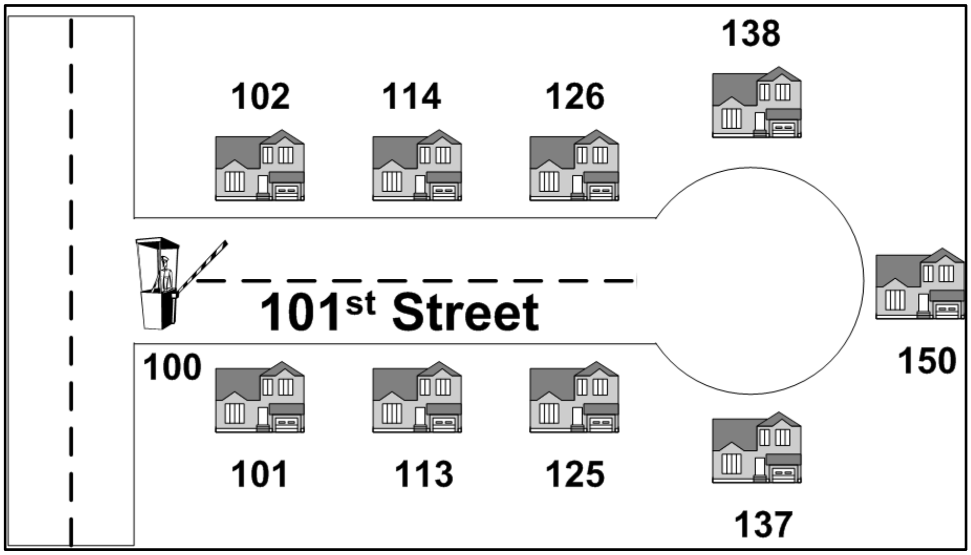
1.1.99. Configure the VLAN Interface

As mentioned previously, switches operate at the Data Link layer of the OSI model (by contrast, routers and Layer 3 switches operate at the network layer). As such, LAN ports on the switch operate differently than those on routers, some of which you will discover during this lab exercise. One significant difference is the concept of a ***VLAN interface***, which is a logical interface that may seem similar to a loopback interface on a router. One important difference is that VLAN interface is tied to the physical ports on the switch itself, while a loopback is not. Some documentation will also call this a ***Switch Virtual Interface***, or ***SVI***. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter VLAN interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface vlan 1** (this interface exists by default on all switches, as does VLAN 1; a VLAN is a ***virtual*** LAN). On Layer 2 switches, you can only have ***one*** of these interfaces active at any given time.
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.1.111 255.255.255.0** without worrying about what the numbers mean at this point. You may notice that this address looks similar to the one configured on the LAN interface of R1.
- **Enable the interface:** As with LAN interfaces on routers, VLAN interfaces are shut down by default, so you must activate them with the command **no shutdown**.
- **Configure the port mode:** Ports on Cisco switches operate in Layer 2 mode (sometimes referred to ***switchport*** mode). Since most of the relevant topics occur in the CCNA course, just understand that these ports will need to be in ***access*** mode, with the interface-level configuration command **switchport mode access**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual switch nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.100. Configure the Default Gateway

While you will understand the concept of a default gateway more fully in later lessons, you need a little background now for it to make sense here. Think of most Local Area Networks (LANs) as ***cul de sacs***, meaning roads with only one way in or out. In the image below, to get in or out of this gated community, you have to pass through the guard station. A ***default gateway*** is the address of the device through which any traffic has to pass through to get in or out of that network. Configuring a default gateway is very simple, as described here:

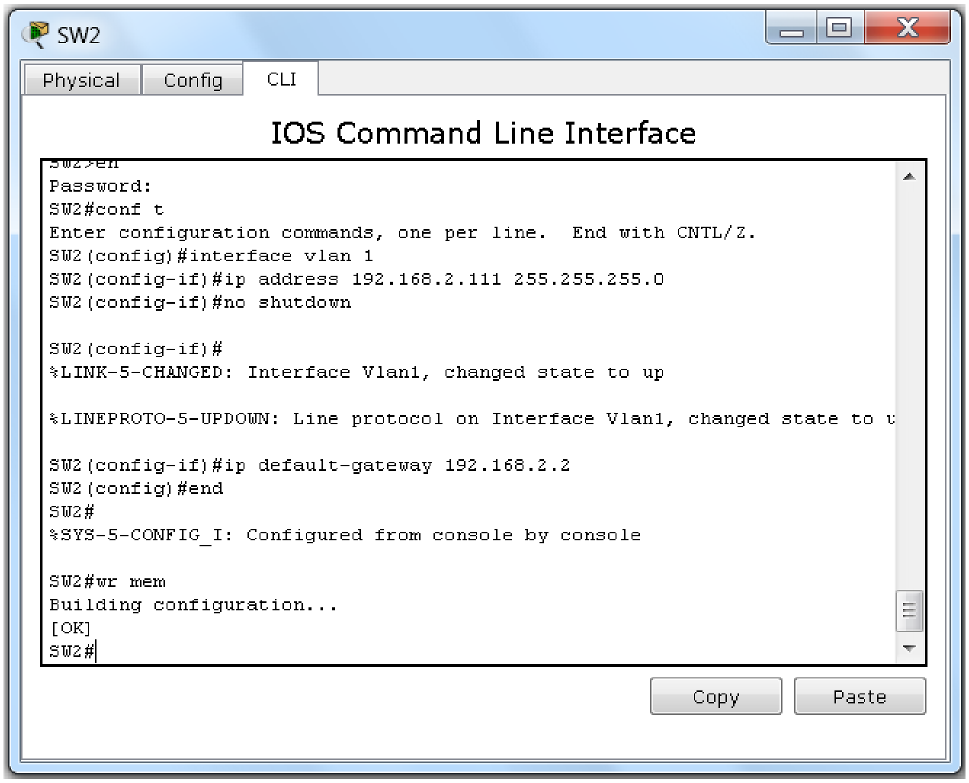


- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Specify the default gateway:** As explained earlier, this is instructing a device to send any traffic it doesn't specifically know about to a designated device for processing. On this switch, this is anything not on the 192.168.1.0 network. Use the command **ip default-gateway 192.168.1.1** (the address of R1's LAN interface)
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual switch nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well.

To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

SW2 Interface Configurations

The interface configuration processes on Cisco switches have many similarities to those of their router counterparts, but differences as well. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
SW2>en
Password:
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#interface vlan 1
SW2(config-if)#ip address 192.168.2.111 255.255.255.0
SW2(config-if)#no shutdown

SW2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to u

SW2(config-if)#ip default-gateway 192.168.2.2
SW2(config)#end
SW2#
%SYS-5-CONFIG_I: Configured from console by console

SW2#wr mem
Building configuration...
[OK]
SW2#
```

1.1.101. Configure the VLAN Interface

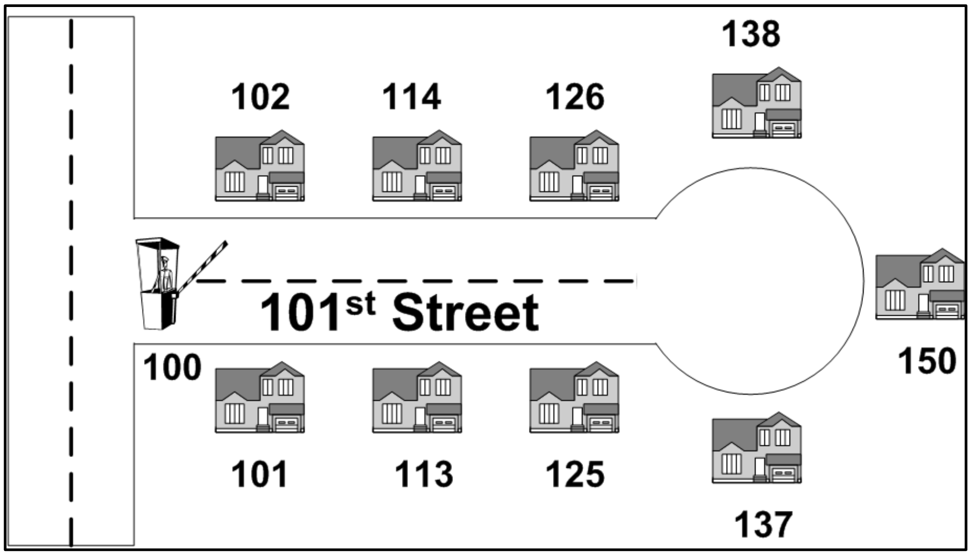
As mentioned previously, switches operate at the Data Link layer of the OSI model (by contrast, routers and Layer 3 switches operate at the network layer). As such, LAN ports on the switch operate differently than those on routers, some of which you will discover during this lab exercise. One significant difference is the concept of a ***VLAN interface***, which is a logical interface that may seem similar to a loopback interface on a router. One important difference is that VLAN interface is tied to the physical ports on the switch itself, while a loopback is not. Some documentation will also call this a ***Switch Virtual Interface***, or ***SVI***. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)

- **Enter VLAN interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface vlan 1** (this interface exists by default on all switches, as does VLAN 1; a VLAN is a ***virtual*** LAN). On Layer 2 switches, you can only have ***one*** of these interfaces active at any given time.
- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.2.111 255.255.255.0** without worrying about what the numbers mean at this point. You may notice that this address looks similar to the one configured on the LAN interface of R2.
- **Enable the interface:** As with LAN interfaces on routers, VLAN interfaces are shut down by default, so you must activate them with the command **no shutdown**.
- **Configure the port mode:** Ports on Cisco switches operate in Layer 2 mode (sometimes referred to ***switchport*** mode). Since most of the relevant topics occur in the CCNA course, just understand that these ports will need to be in ***access*** mode, with the interface-level configuration command **switchport mode access**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual switch nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.102. Configure the Default Gateway

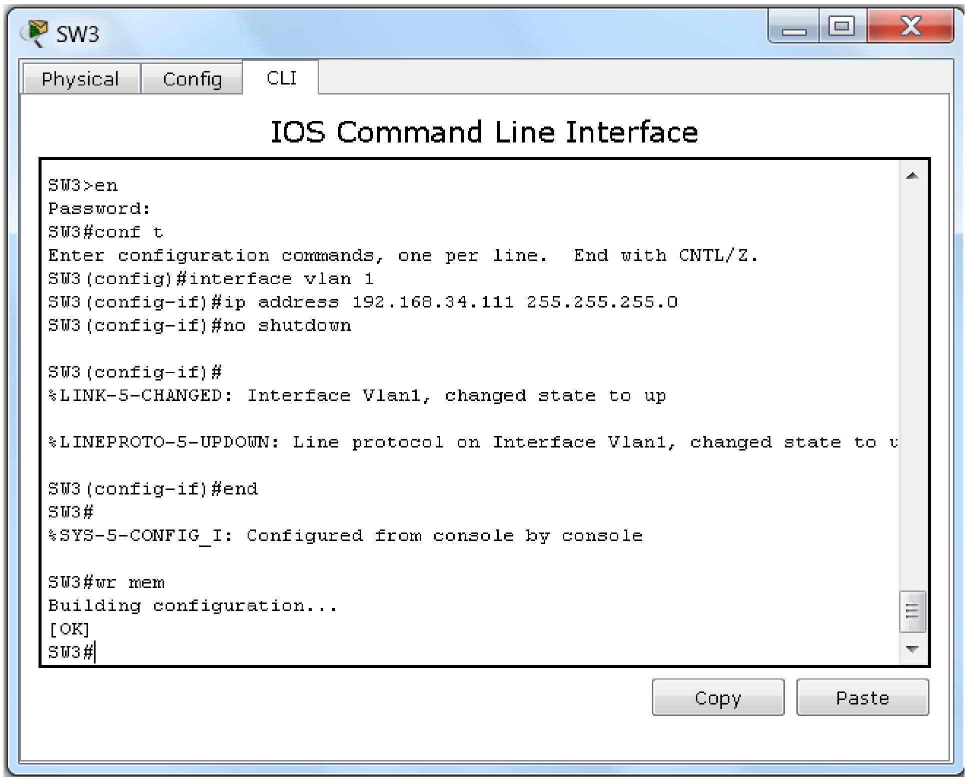
While you will understand the concept of a default gateway more fully in later lessons, you need a little background now for it to make sense here. Think of most Local Area Networks (LANs) as ***cul de sacs***, meaning roads with only one way in or out. In the image below, to get in or out of this gated community, you have to pass through the guard station. A ***default gateway*** is the address of the device through which any traffic has to pass through to get in or out of that network. Configuring a default gateway is very simple, as described here:



- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Specify the default gateway:** As explained earlier, this is instructing a device to send any traffic it doesn't specifically know about to a designated device for processing. On this switch, this is anything not on the 192.168.2.0 network. Use the command **ip default-gateway 192.168.2.2** (the address of R2's LAN interface)
- **Enable the interface:** LAN interfaces on routers are shut down by default, so you must activate them with the command **no shutdown**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual switch nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

SW3 Interface Configurations

The interface configuration processes on Cisco switches have many similarities to those of their router counterparts, but differences as well. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:



```
SW3>en
Password:
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#interface vlan 1
SW3(config-if)#ip address 192.168.34.111 255.255.255.0
SW3(config-if)#no shutdown

SW3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to u

SW3(config-if)#end
SW3#
%SYS-5-CONFIG_I: Configured from console by console

SW3#wr mem
Building configuration...
[OK]
SW3#
```

1.1.103. Configure the VLAN Interface

As mentioned previously, switches operate at the Data Link layer of the OSI model (by contrast, routers and Layer 3 switches operate at the network layer). As such, LAN ports on the switch operate differently than those on routers, some of which you will discover during this lab exercise. One significant difference is the concept of a ***VLAN interface***, which is a logical interface that may seem similar to a loopback interface on a router. One important difference is that VLAN interface is tied to the physical ports on the switch itself, while a loopback is not. Some documentation will also call this a ***Switch Virtual Interface***, or ***SVI***. Configuration of a loopback interface is a simple process, as outlined here:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter VLAN interface configuration mode:** In order to create an interface, you need to enact interface configuration submode. In this case, you will use the command **interface vlan 1** (this interface exists by default on all switches, as does VLAN 1; a VLAN is a ***virtual*** LAN). Unlike Layer 2 switches, you can only have ***many*** of these interfaces active at any given time, since this is a Layer 3 switch (able to perform networking, similar to a router)

- **Enter IPv4 addressing information:** Since IP addressing is a later topic, you will have specific instructions for entering the correct information. Explanations will appear in later lessons. Use the command **ip address 192.168.34.111 255.255.255.0** without worrying about what the numbers mean at this point. You may notice that this address looks similar to the one configured on the LAN interfaces of R3 & R4.
- **Enable the interface:** As with LAN interfaces on routers, VLAN interfaces are shut down by default, so you must activate them with the command **no shutdown**.
- **Configure the port mode:** Ports on Cisco switches operate in Layer 2 mode (sometimes referred to ***switchport*** mode). Since most of the relevant topics occur in the CCNA course, just understand that these ports will need to be in ***access*** mode, with the interface-level configuration command **switchport mode access**.
- **Exit configuration mode:** Two ways exist for this, the first is to use the ***exit*** command multiple times, since command modes have a distinct hierarchy. The second (and simpler) method is the ***end*** command, which takes you back to privileged mode.
- **Save the configuration:** At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual switch nothing else would be necessary, but with Packet Tracer, you need to save changes in the program as well. To accomplish this, either use the **File>Save option** or the **Ctrl+S** keyboard shortcut.

1.1.104. Configure the Default Gateway

Because SW3 had Layer 3 capabilities, configuration of the default gateway is not a requirement.

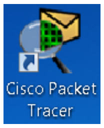
Lesson 7 Lab Exercises

Switch Types (Layer 2 & Layer 3)

The purpose of this lab exercise is to reinforce the concepts from the Cisco Switch Operations and Configuration lesson.

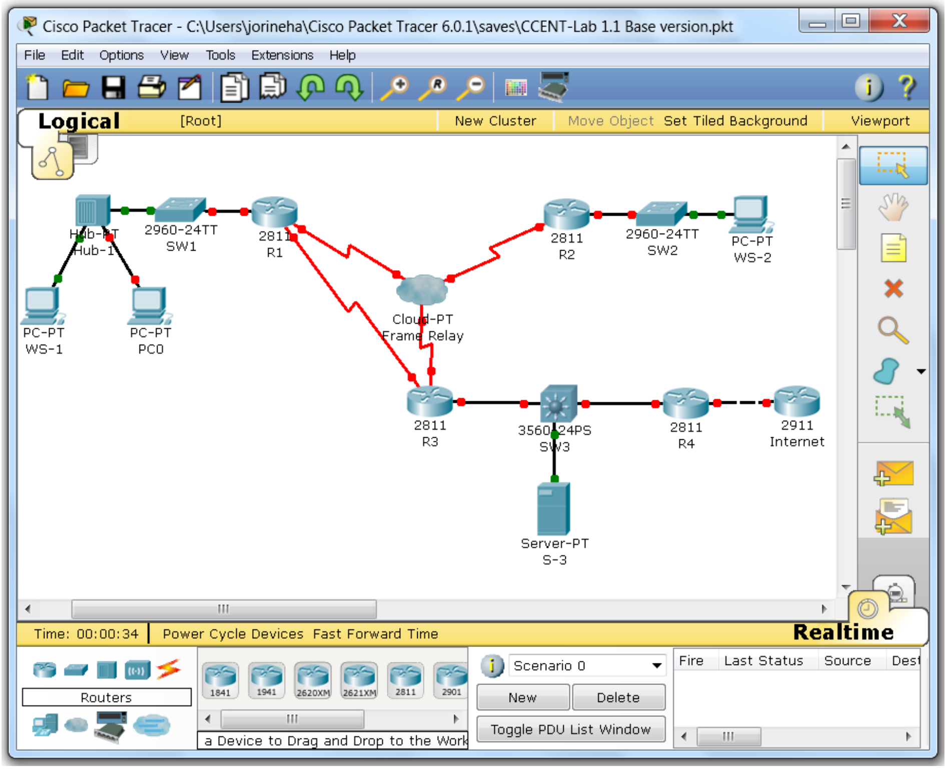
1.1.105. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



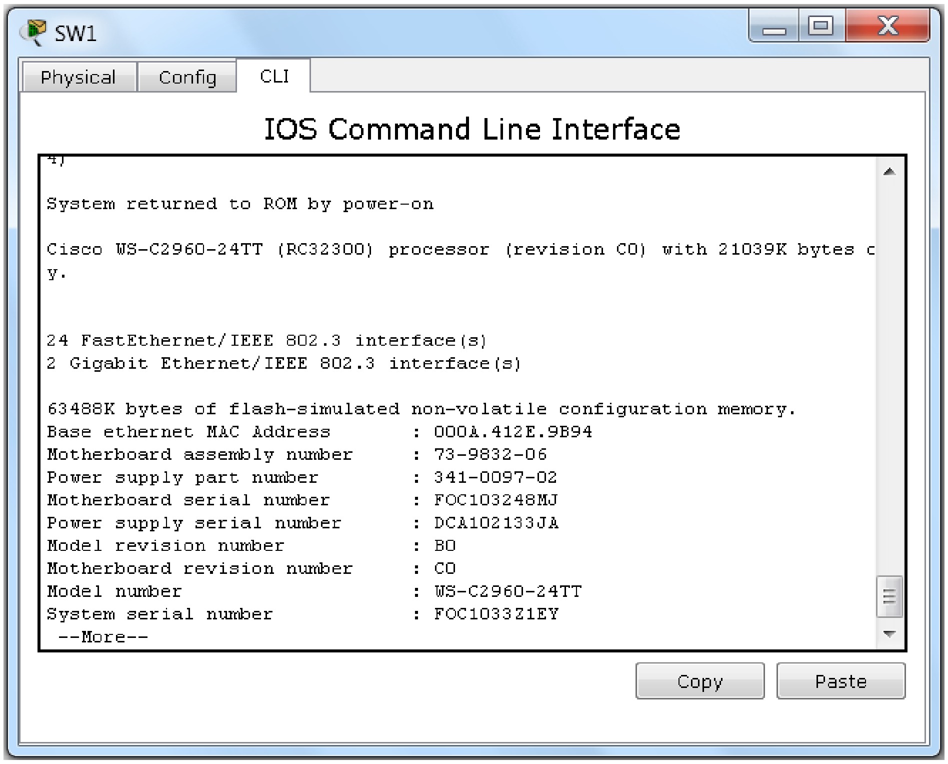
1.1.106. Select SW1 by double clicking the image

Begin by accessing SW1 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



1.1.107. Review device hardware information on SW1

Once inside the command line interface of SW1, type the command **show version**; this will display detailed hardware information on the device in question, as follows:



```
4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes c
y.


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address        : 000A.412E.9B94
Motherboard assembly number      : 73-9832-06
Power supply part number         : 341-0097-02
Motherboard serial number        : FOC103248MJ
Power supply serial number       : DCA102133JA
Model revision number            : B0
Motherboard revision number      : C0
Model number                     : WS-C2960-24TT
System serial number             : FOC1033Z1EY
 --More--
```

Note some of the important details on SW1, which indicates extensive information which you will gain the ability to interpret:

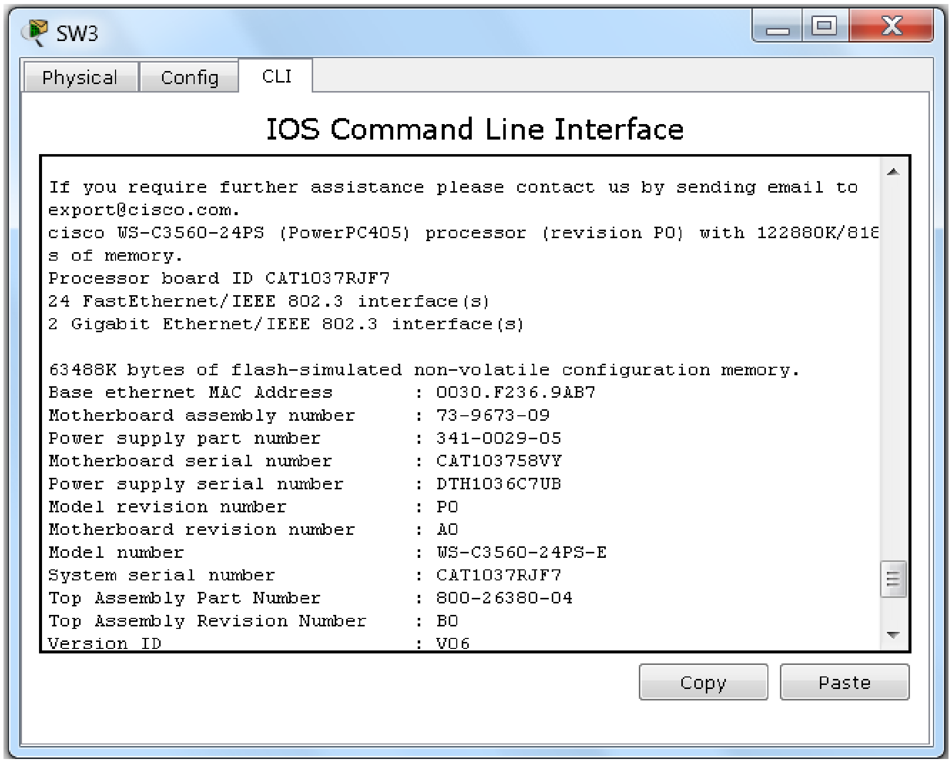
- **Model Number**: To begin with, notice the model number WS-C2960-24TT which indicates several things:
  - o **C**: Catalyst (the official name of this family of switches).
  - o **2960:** The model of switch (2960), note that the **2** at the beginning .signifies that this is a ***Layer 2*** switch (no routing capabilities)
  - o **24:** Indicates the number of Ethernet ports on the chassis.
  - o **T:** Indicates that these are RJ-45 copper connections
- **Interfaces**: Aside from the model number, the number and type of interfaces are clearly identified:
  - o 24 Fast Ethernet
  - o 2 Gigabit Ethernet
- **Available Memory**: Helpful when deciding what software images are supported.
- **Software Version/Image**: Though not displayed in the image above, the **show version** command also indicates what software is stored on the device, and what version is in use.

1.1.108. Select SW3 by double clicking the image

Leave the terminal window for SW1, but return to the Packet Tracer interface and click on the icon for SW3 to open a session to the command line interface of SW3.

1.1.109. Review device hardware information on SW3

Once inside the command line interface of SW3, type the command **show version**; this will display detailed hardware information on the device in question, as follows:



```
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/818
s of memory.
Processor board ID CAT1037RJF7
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0030.F236.9AB7
Motherboard assembly number     : 73-9673-09
Power supply part number        : 341-0029-05
Motherboard serial number       : CAT103758VY
Power supply serial number      : DTH1036C7UB
Model revision number           : P0
Motherboard revision number     : A0
Model number                    : WS-C3560-24PS-E
System serial number            : CAT1037RJF7
Top Assembly Part Number        : 800-26380-04
Top Assembly Revision Number    : B0
Version ID                      : V06
```

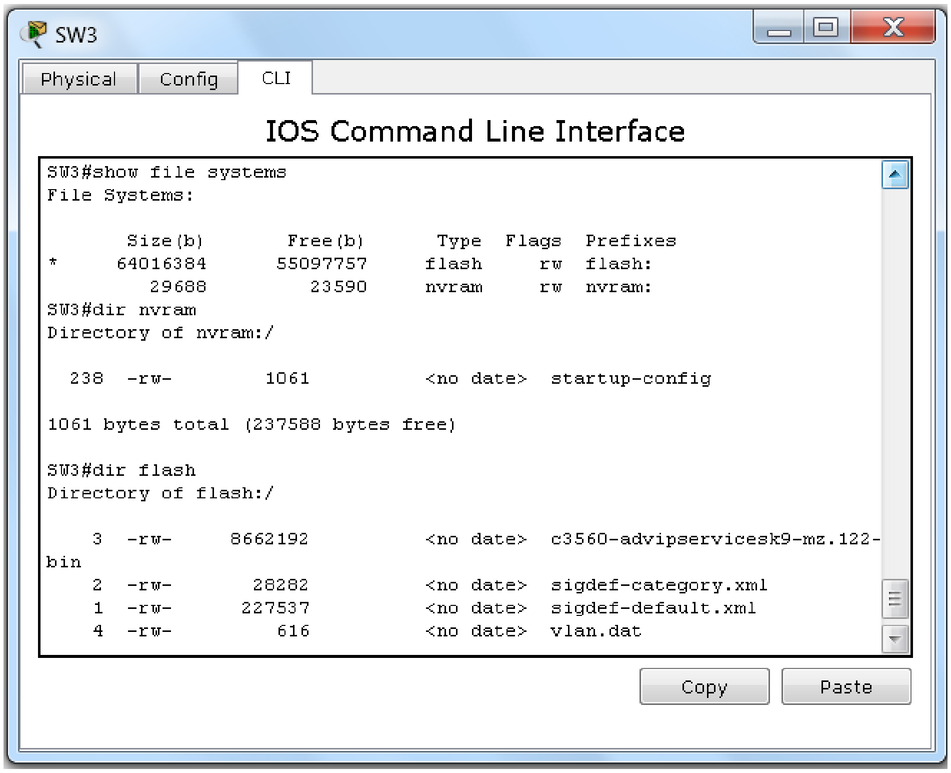
Notice that while some of the details appear similar to SW1, that others are different:

- **Model Number**: To begin with, notice the model number WS-C3560-24PS which indicates several things:
  - **C**: Catalyst (the official name of this family of switches).
  - **3560:** The model of switch (2960), note that the **3** at the beginning .signifies that this is a ***Layer 3*** switch (has routing capabilities)
  - **24:** Indicates the number of Ethernet ports on the chassis.
  - **PS:** Indicates that these ports have the ability to supply DC power to attached devices (referred to as ***Power over Etherne***t, or ***POE***)
- **Interfaces**: Aside from the model number, the number and type of interfaces are clearly identified:
  - 24 Fast Ethernet
  - 2 Gigabit Ethernet

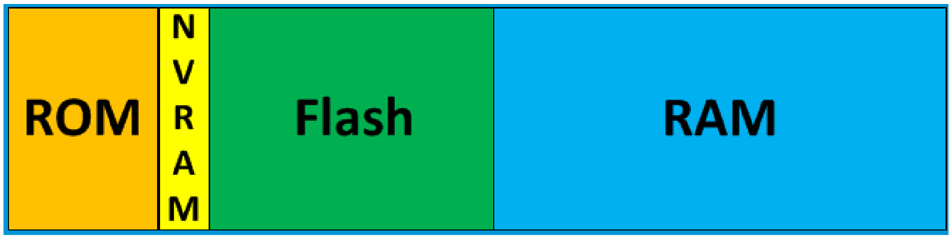
- **Available Memory**: Helpful when deciding what software images are supported.
- **Software Version/Image**: Though not displayed in the image above, the show version command also indicates what software is stored on the device, and what version is in use.

Switch Memory Types

As explained in the accompanying lesson, Cisco switches employ several types of memory, each of which has a special function in the operation of the device. Return to the terminal window of SW3 in order to explore these types of memory, as shown here:



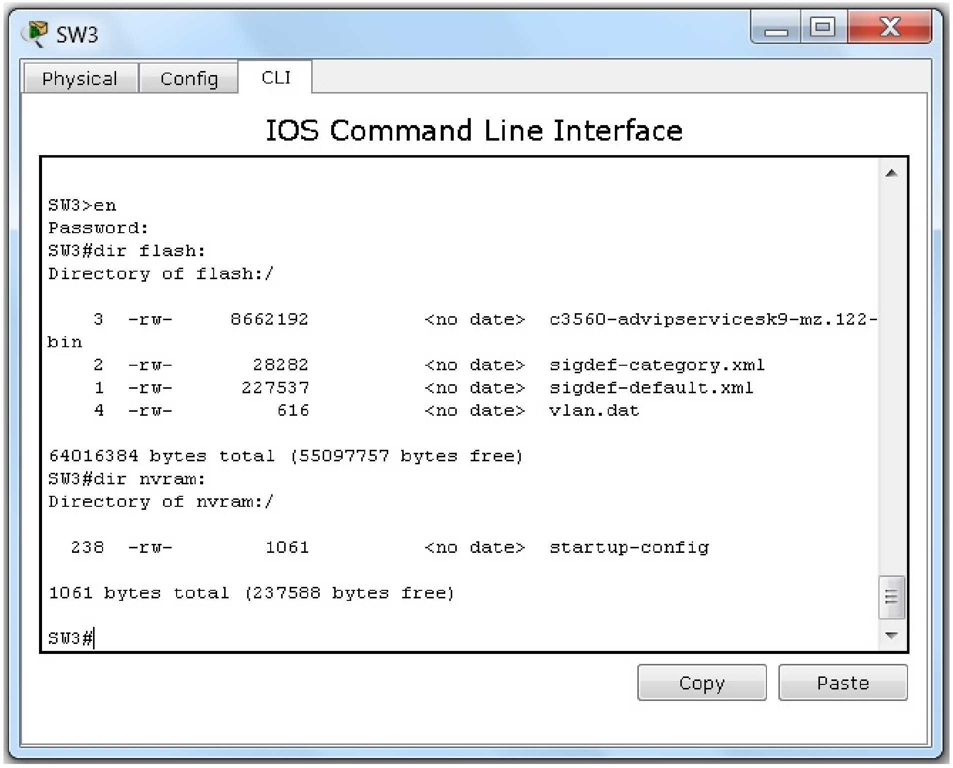
```
SW3#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
*     64016384      55097757     flash     rw   flash:
         29688         23590     nvram     rw   nvram:
SW3#dir nvram
Directory of nvram:/

  238  -rw-        1061          <no date>  startup-config

1061 bytes total (237588 bytes free)

SW3#dir flash
Directory of flash:/

    3  -rw-     8662192          <no date>  c3560-advipservicesk9-mz.122-
bin
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml
    4  -rw-         616          <no date>  vlan.dat
```



Enter the command **show file systems** in order to display information on two of the memory types referenced in the previous lesson. You will notice these listed as follows:

- **flash**: Storage of IOS code and other operations
- **nvram**: Storage of the startup-configuration

You can display the contents of each of these types of memory using the **dir** (short for directory) command. This will produce an itemized list of all files contained within the memory device that you specify. To explore the contents of flash memory, enter the command **dir flash:**, followed by **dir nvram**:



```
SW3>en
Password:
SW3#dir flash:
Directory of flash:/

    3  -rw-     8662192          <no date>  c3560-advipservicesk9-mz.122-
bin
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml
    4  -rw-         616          <no date>  vlan.dat

64016384 bytes total (55097757 bytes free)
SW3#dir nvram:
Directory of nvram:/

  238  -rw-        1061          <no date>  startup-config

1061 bytes total (237588 bytes free)

SW3#
```

Note first that several files are stored in flash memory, several of which are not relevant to the ICND1/ICND2 course of study. The two items to take note of are listed here:

- **vlan.dat**: Locally stored database containing the names and identifiers for virtual local area networks (VLANs, an ICND2 topic).
- **c3560-advipservicesk9-mz.122-37.SE1.bin**: The file containing the IOS code that is running on the switch. This is the file that would be changed if you were to upgrade to a newer version of code.

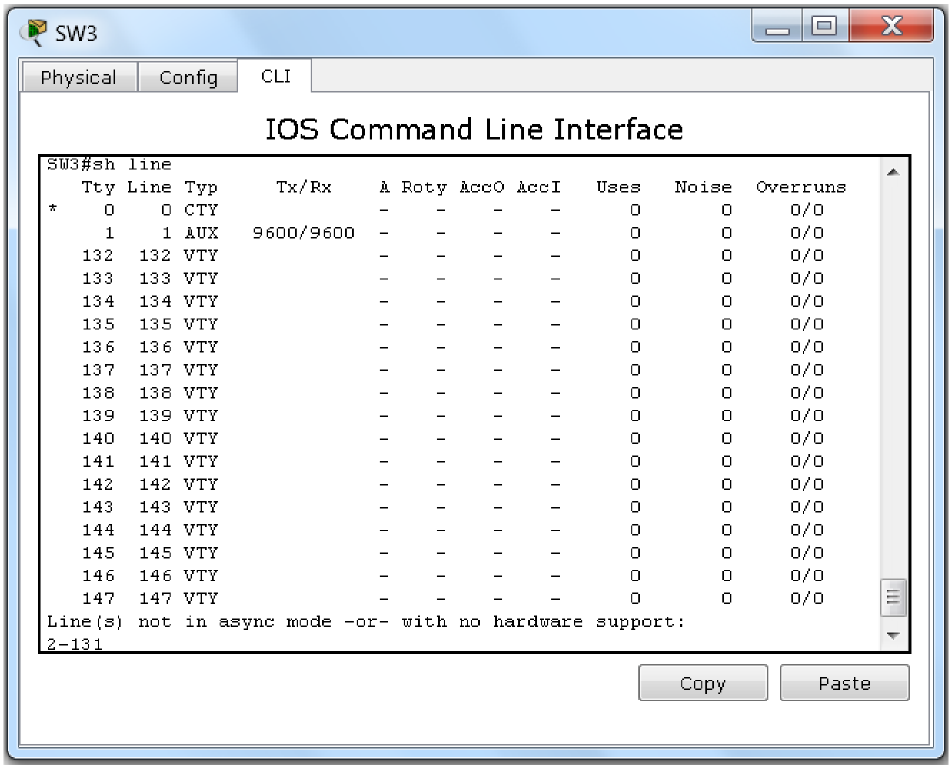
When you execute the second command, notice the name of the ***only*** file listed---the ***startup configuration***. As previously discussed, this is the stored configuration that is loaded into ***RAM*** at system startup.

Switch Access (Console/Telnet)

One of many critical technical skills that you need to demonstrate is the ability to configure access to Cisco devices, in this case, switches. Note that these access methods also apply to routers, which you will encounter in a later lesson. In addition, you will perform some configuration functions that will help you in real-world settings.

1.1.110. Console Access

The device access screen that you have used thus far is in fact console access, achieved in production settings through the use of a special cabled connection to the CON port of the switch. In this exercise you will verify that through the use of specific **show** commands. It is assumed that you are already in the Packet Tracer Interface. These steps are as follows:

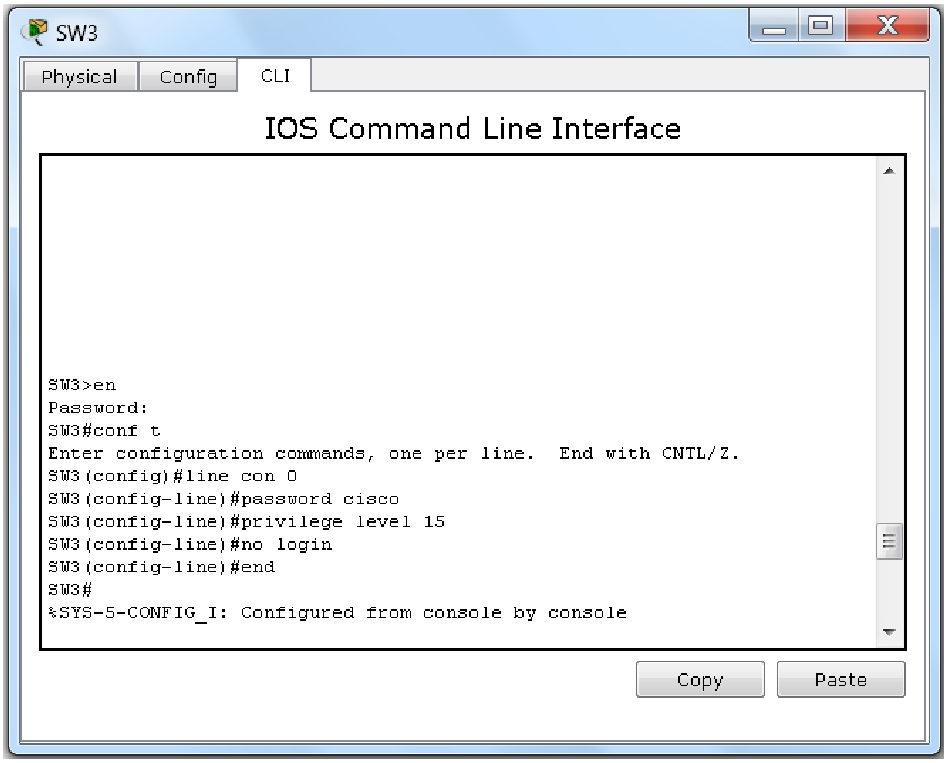


```
SW3#sh line
   Tty Line Typ     Tx/Rx    A Roty AccO AccI   Uses   Noise  Overruns
*    0    0 CTY              -    -    -    -      0       0     0/0
     1    1 AUX   9600/9600  -    -    -    -      0       0     0/0
   132  132 VTY              -    -    -    -      0       0     0/0
   133  133 VTY              -    -    -    -      0       0     0/0
   134  134 VTY              -    -    -    -      0       0     0/0
   135  135 VTY              -    -    -    -      0       0     0/0
   136  136 VTY              -    -    -    -      0       0     0/0
   137  137 VTY              -    -    -    -      0       0     0/0
   138  138 VTY              -    -    -    -      0       0     0/0
   139  139 VTY              -    -    -    -      0       0     0/0
   140  140 VTY              -    -    -    -      0       0     0/0
   141  141 VTY              -    -    -    -      0       0     0/0
   142  142 VTY              -    -    -    -      0       0     0/0
   143  143 VTY              -    -    -    -      0       0     0/0
   144  144 VTY              -    -    -    -      0       0     0/0
   145  145 VTY              -    -    -    -      0       0     0/0
   146  146 VTY              -    -    -    -      0       0     0/0
   147  147 VTY              -    -    -    -      0       0     0/0
Line(s) not in async mode -or- with no hardware support:
2-131
```

- Execute the **show line** command on SW3 in privileged mode in order to list all currently open terminal sessions (the term ***line*** refers to ***terminal lines***). Note the following terms in the output:

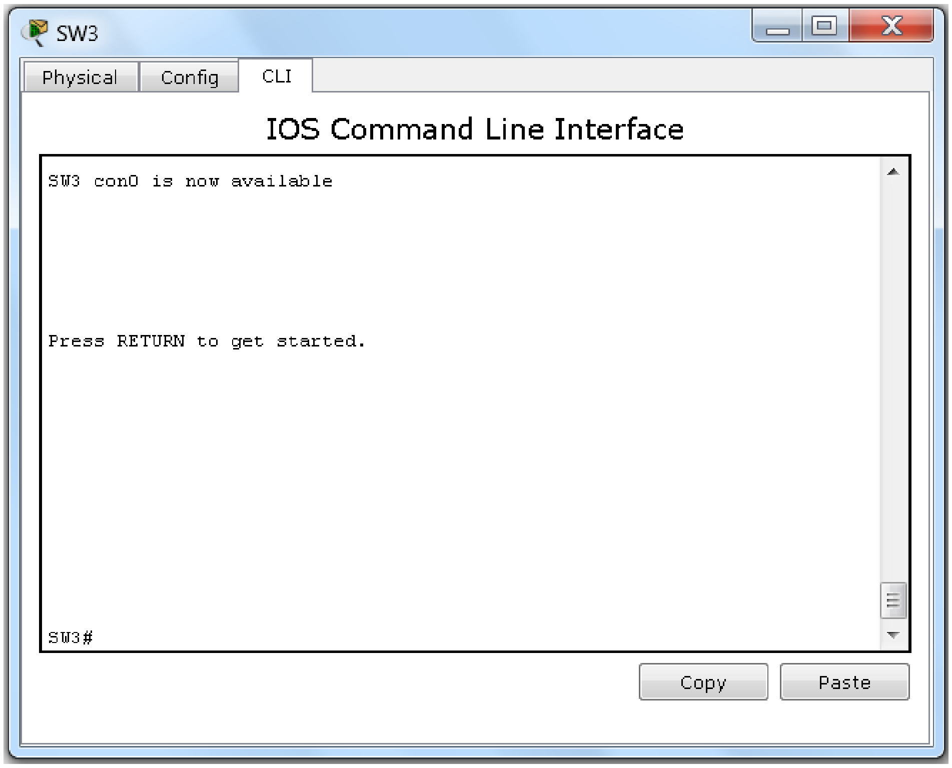
    - **TTY/Line**: The logical number of the connection type, used to refer to a specific connection.
    - **Typ(e)**: The type of connection. CTY is the console, AUX is the auxiliary port (typically used for modem connections), and VTY is for virtual terminal, remote telnet/ssh connections.
    - *****: Designates which lines are active (note that the only active line is the ***console line*** that you are using)
    - **The remaining output is largely beyond the scope of ICND1/2.**

- For lab purposes, to avoid having to go through the login process on the console port, you can configure a simple shortcut. ***Note that this is not recommended for use in a production network, as it poses a critical security risk.*** Execute the following steps to create this:



```
SW3>en
Password:
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#line con 0
SW3(config-line)#password cisco
SW3(config-line)#privilege level 15
SW3(config-line)#no login
SW3(config-line)#end
SW3#
%SYS-5-CONFIG_I: Configured from console by console
```

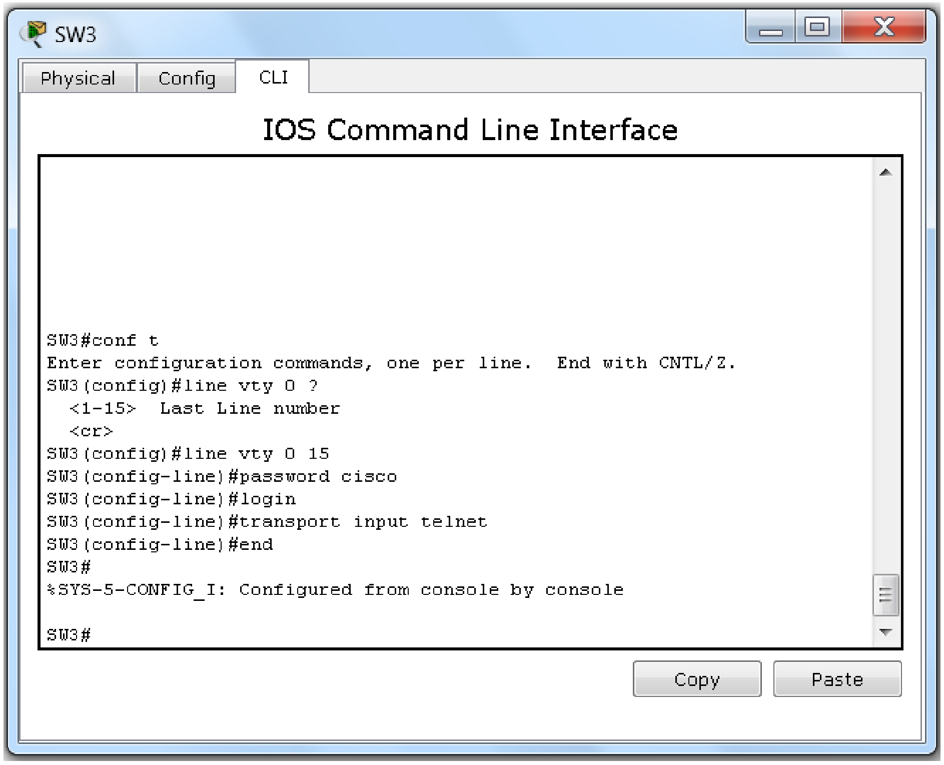
- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Since you set en ***enable secret*** password in previous steps, you will have to enter it again at the password prompt (remember, the password is ***cisco***)
- **Enter console line configuration mode**: Use the command **line con 0** to specify settings for the console access line.
- **Specify a login password**: Set the password to access the console line to ***cisco*** with the command **password cisco**.
- **Bypass the enable secret process**: To prevent having to enter the enable command altogether, enter the command **privilege level 15**. To understand the contrast, ***privilege level 0*** is equivalent to user exec mode. ** **Do not use this in a production network. ****
- Disable the login process: To avoid any login process on the console line, enter the command **no login**. ** **Do not use this in a production network. ****
- Now if you log out and back into the console line, and you should enter into privileged mode at the CLI by simply pressing the **<enter>** key.
- Repeat this configuration process on all the remaining switches and routers in the lab topology.



```
SW3 con0 is now available




Press RETURN to get started.










SW3#
```

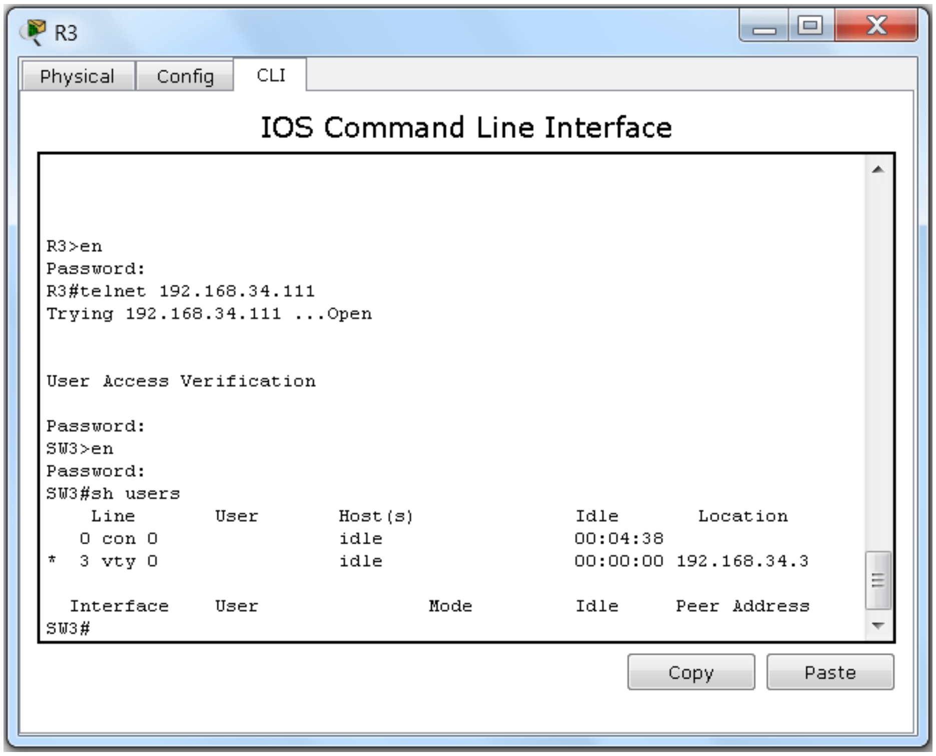
1.1.111. Telnet Access

As mentioned previously, ***telnet*** access (or its more secure cousin ***secure shell/ssh***) allows technicians to log into devices from remote locations. It is assumed that you are already in the Packet Tracer Interface. The required configuration steps are as follows:



```
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#line vty 0 ?
  <1-15>  Last Line number
  <cr>
SW3(config)#line vty 0 15
SW3(config-line)#password cisco
SW3(config-line)#login
SW3(config-line)#transport input telnet
SW3(config-line)#end
SW3#
%SYS-5-CONFIG_I: Configured from console by console

SW3#
```

- To use a telnet connection, open a terminal session to R3 by double clicking on the image. Go to the command line in privileged mode and enter the command **telnet 192.168.34.111** (the VLAN port of SW3)
- When the password prompt on SW3's VTY line, enter the password **cisco**
- Enter privileged mode using the command **enable**, followed by the enable secret command of **cisco** as well.
- At the command line, enter the command show users to display login sessions to the device. You should see CON and VTY entries as shown below.



```
R3>en
Password:
R3#telnet 192.168.34.111
Trying 192.168.34.111 ...Open


User Access Verification

Password:
SW3>en
Password:
SW3#sh users
    Line       User       Host(s)              Idle       Location
   0 con 0                idle                 00:04:38
*  3 vty 0                idle                 00:00:00 192.168.34.3

  Interface    User               Mode         Idle     Peer Address
SW3#
```

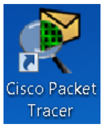
Lesson 8 Lab Exercises

Using Show Commands for Diagnosis Purposes

In addition to using a troubleshooting process, as a network technician/engineer you also will need to have great familiarity with the use of Cisco IOS diagnostic commands. While this includes both the **show** and **debug** commands, you will start with the former.

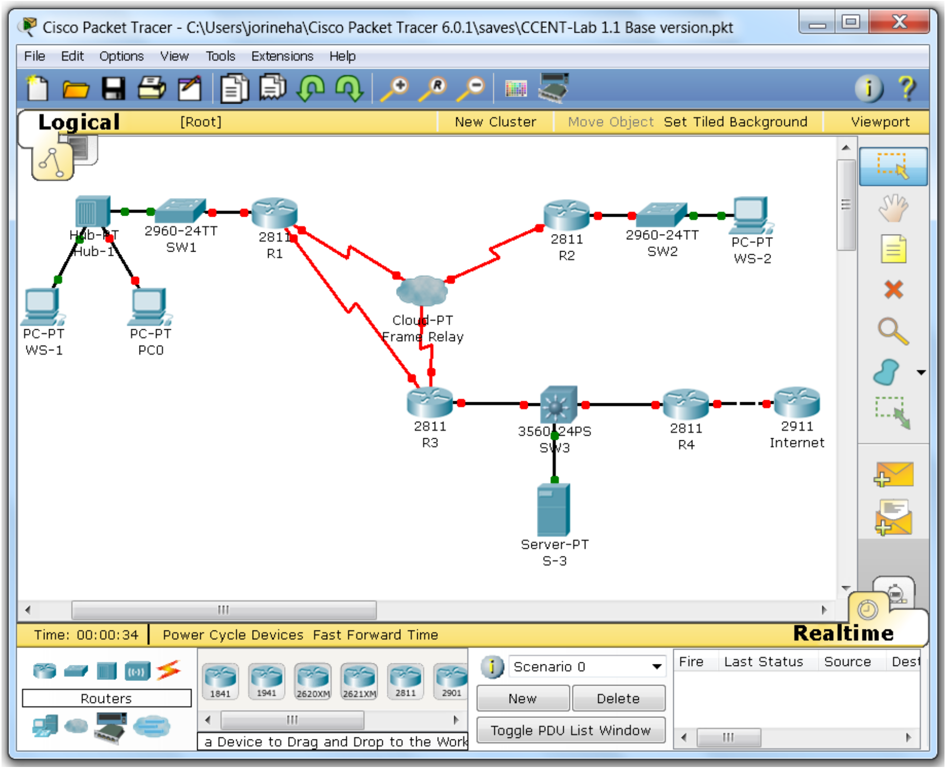
1.1.112. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



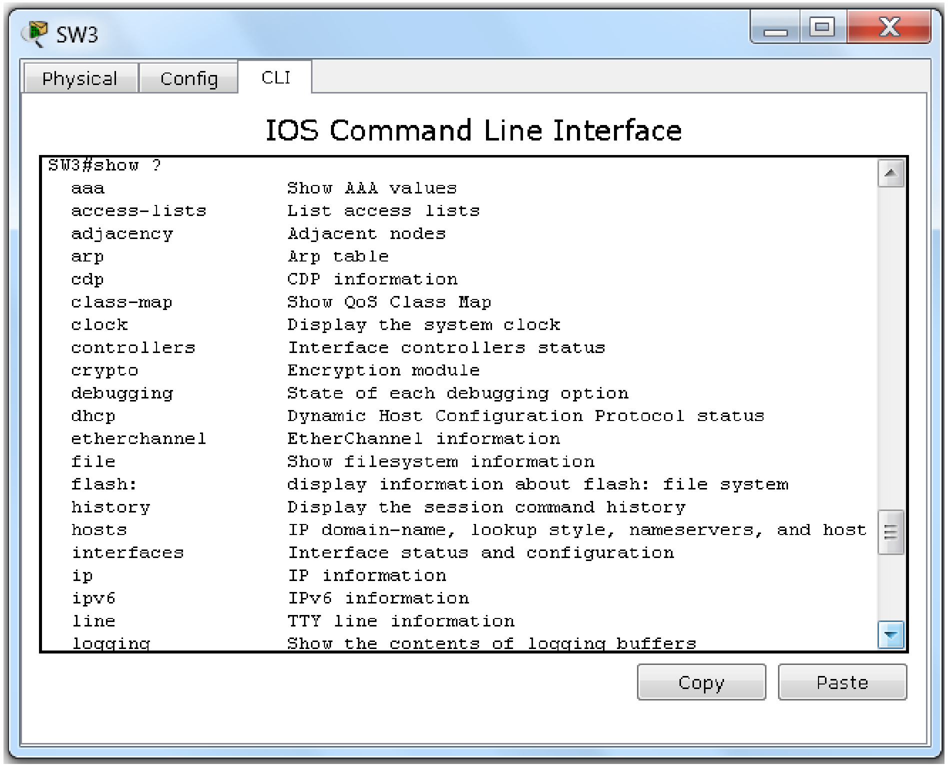
1.1.113. Select SW3 by double clicking the image

Begin by accessing SW3 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



1.1.114. Review available show commands on SW3

Some of the most useful and powerful diagnostic tools on a Cisco IOS switch are **show** commands, and the name suggests, they display specific information on the device. To display an available list, type the **show ?** command in privileged mode, as shown here:



```
SW3#show ?
  aaa                 Show AAA values
  access-lists        List access lists
  adjacency           Adjacent nodes
  arp                 Arp table
  cdp                 CDP information
  class-map           Show QoS Class Map
  clock               Display the system clock
  controllers         Interface controllers status
  crypto              Encryption module
  debugging           State of each debugging option
  dhcp                Dynamic Host Configuration Protocol status
  etherchannel        EtherChannel information
  file                Show filesystem information
  flash:              display information about flash: file system
  history             Display the session command history
  hosts               IP domain-name, lookup style, nameservers, and host
  interfaces          Interface status and configuration
  ip                  IP information
  ipv6                IPv6 information
  line                TTY line information
  logging             Show the contents of logging buffers
```

One important factor to keep in mind is that there are differences between Packet Tracer (which is a network simulator) and a physical Cisco Catalyst IOS-based switch. The accompanying handout, entitled ICND1 Relevant Commands, may contain some commands that work on an actual switch but are not supported in Packet Tracker.

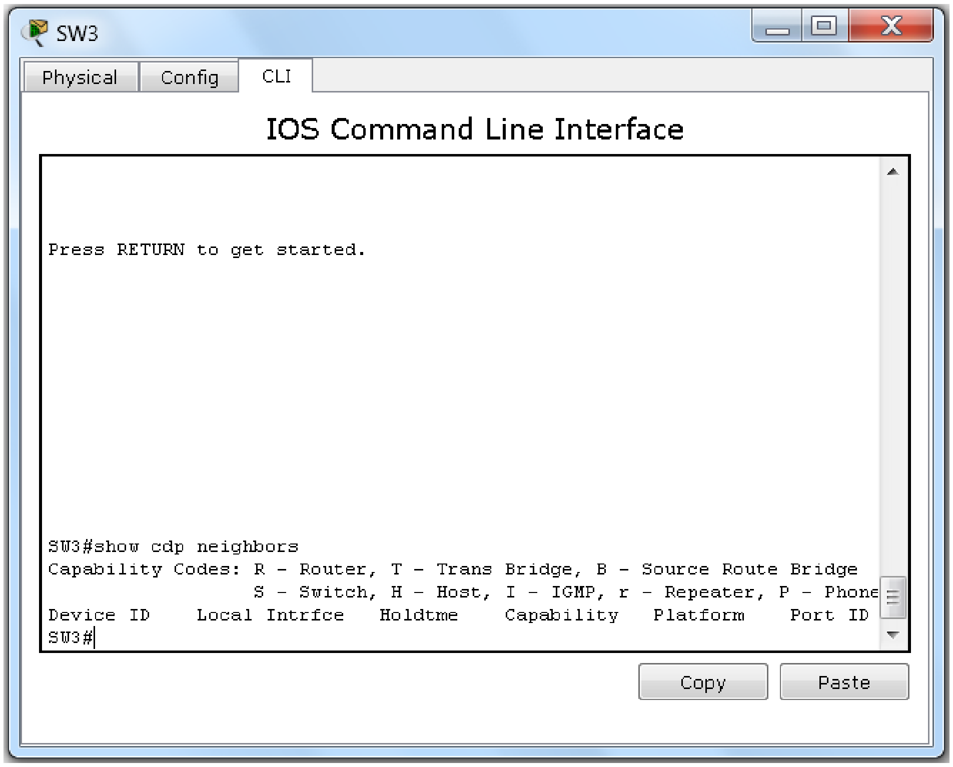
Scroll through the list and note several of the more common and frequently used commands, such as:

- **show interface <slot/port>**: Displays a large amount of statistics on the specified interface, which on a switch will almost always be an Ethernet interface.
- **show ip interface brief**: Very helpful, in that this will display an abbreviated list of interfaces, their operational state, and IP addressing information.
- **show cdp neighbors**: If you remember the OSI model discussion, you may recall that switches operate at Layer 2, the Data Link Layer. Use of the Cisco Discovery Protocol can indicate whether Layer 2 (Ethernet) connectivity to other devices is intact.

- **show mac address-table [dynamic]**: In order to build the internal switching table (often referred to as the ***Content Addressable Memory***, or ***CAM***), switches read the source MAC addresses and the ports they were received on. In order to examine the CAM table, you can use this show command to display the contents.
- **show controllers <slot/port>**: When you encounter issues that you think may be related to failed device hardware, you can examine this with the **show controllers** command.
- **show running-config**: If you need to examine the current configuration, this command will allow you to read the output.
- **show startup-config**: If you need to examine the stored configuration, this command will allow you to read the output. This can be helpful if you are comparing configurations, including the current **running-config**.
- **show version**: Used to identify the current IOS version of the switch.

Enable Cisco Discovery Protocol on R3 & R4

In general, Cisco Discovery Protocol (CDP) is enabled on Cisco devices, but occasionally you may find it has been disabled. This can be unintentional, but may also be for security reasons. On devices facing the Internet, this makes perfect sense, though internally it may not pose a threat. First, execute the **show cdp neighbors** command on the CLI of SW3:

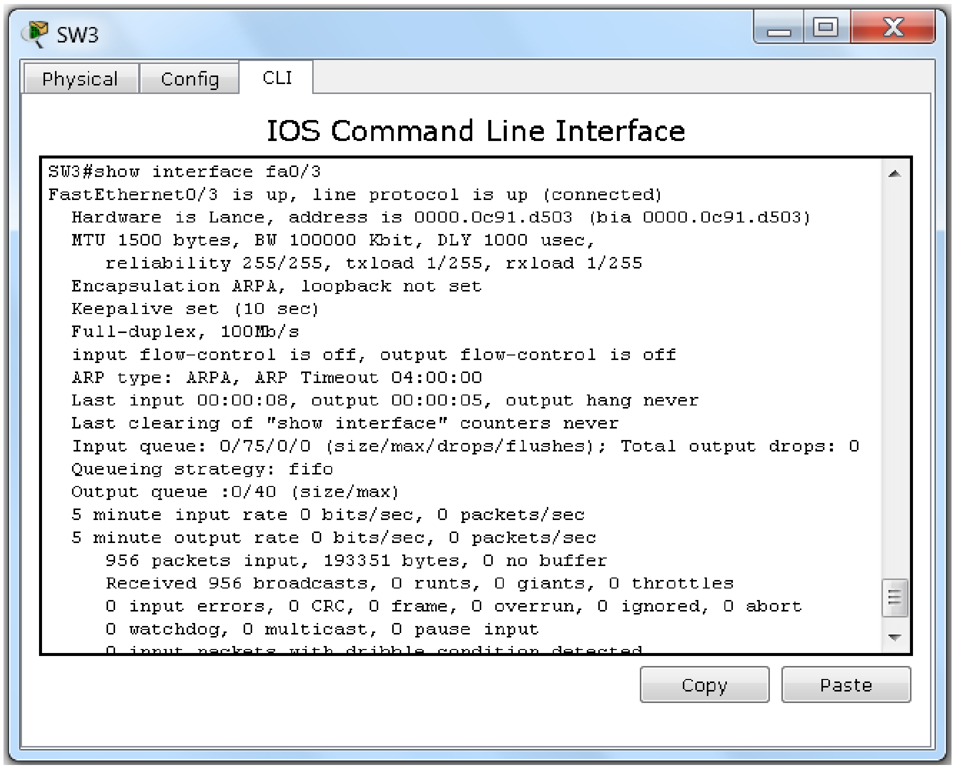


```
Press RETURN to get started.









SW3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability    Platform    Port ID
SW3#
```

You should notice that the results indicate that SW3 has not indicated the presence of other Cisco devices. In production networks, this can happen for the following reasons:

- The interface connected to the neighboring devices is shut down
- The interface to the neighboring device is not connected
- CDP has been disabled on one or both devices
- The device is not directly connected
- The other device does not support CDP

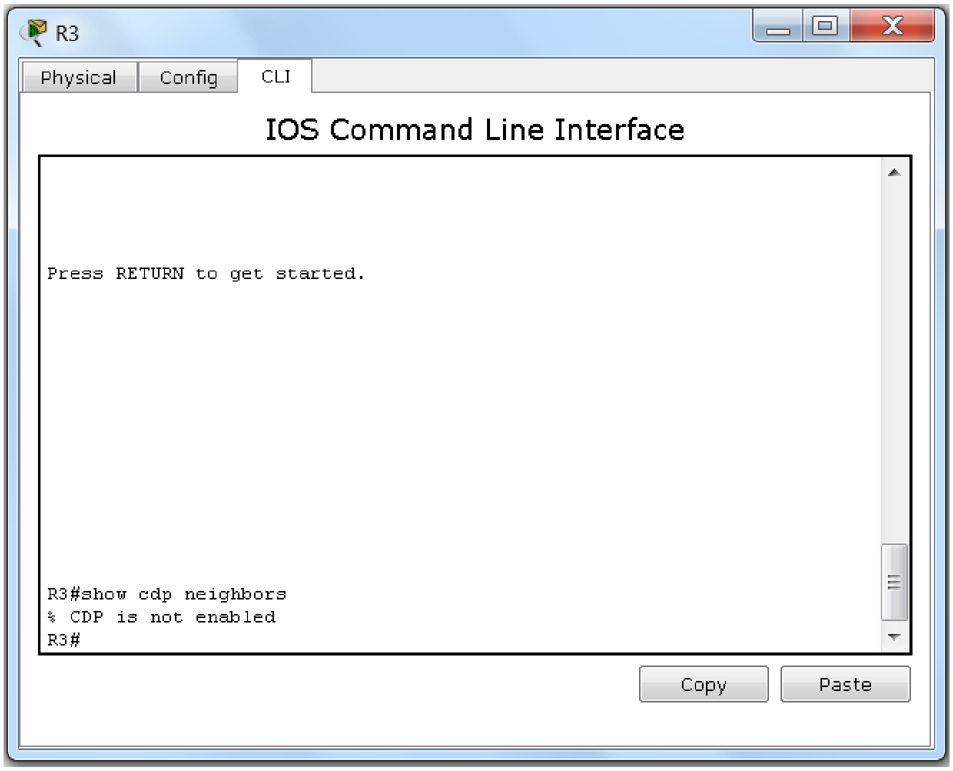
First, rule out some of the more obvious causes, such as device support. All Cisco devices in the Packet Tracer environment support CDP, with the exception of Hub-1. Next, examine the lab topology to see whether or not the devices are directly connected; you will notice that R3 & R4 are connected by Ethernet, and you can use the **show interface** command to determine the state of the interfaces (Fa0/3 & Fa0/4) to those devices:



```
SW3#show interface fa0/3
FastEthernet0/3 is up, line protocol is up (connected)
  Hardware is Lance, address is 0000.0c91.d503 (bia 0000.0c91.d503)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
```

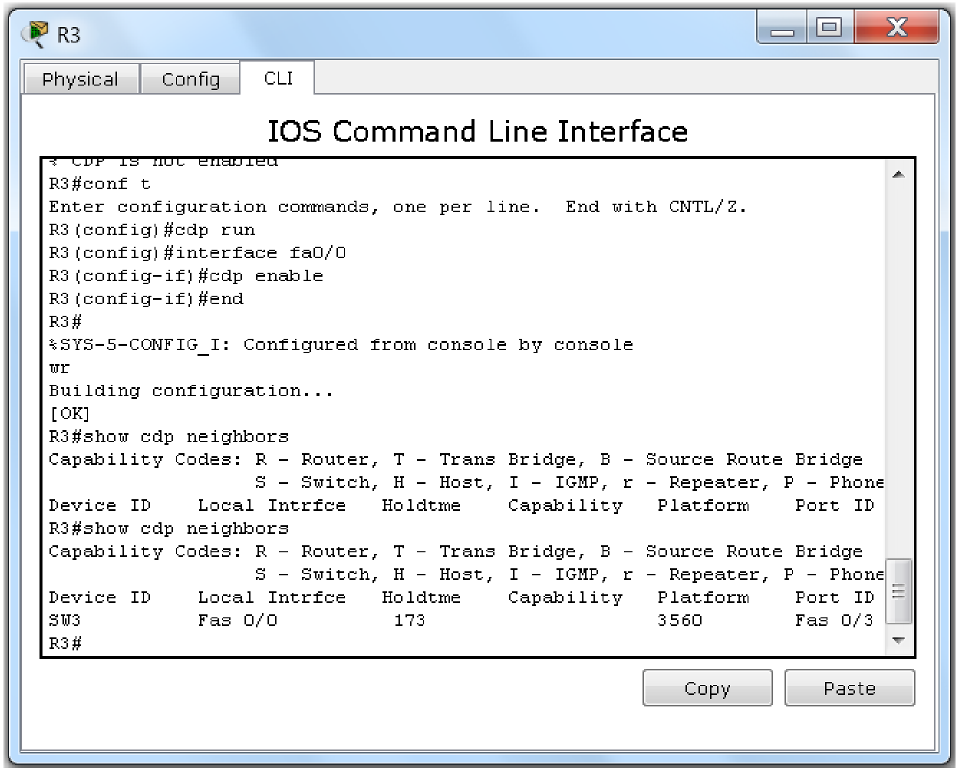
Use the commands show **interface Fa0/3** and **show interface Fa0/4** as shown above, and you will notice the phrases “**is up**” (remember, that indicates the physical layer status) and “**line protocol is up**” (Layer 2 is up), which demonstrates that there is no interface issue in this case.

To complete the diagnostic process, click on R3 in the Packet Tracer topology window, and execute the command **show cdp neighbors** to determine if the protocol is running correctly on R3 (and R4, if you want to log in there as well). The resulting message should read as shown below:



```
Press RETURN to get started.




R3#show cdp neighbors
% CDP is not enabled
R3#
```

Remember the list of possible causes? If CDP is not enabled on both devices, then it will not function for neighbor detection. Fortunately, enabling CDP is a simple process, consisting of two steps (not always necessary, but advisable), enabling CDP globally, and enabling CDP on an interface:



```
% CDP is not enabled
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#cdp run
R3(config)#interface fa0/0
R3(config-if)#cdp enable
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
SW3          Fas 0/0          173                    3560        Fas 0/3
R3#
```

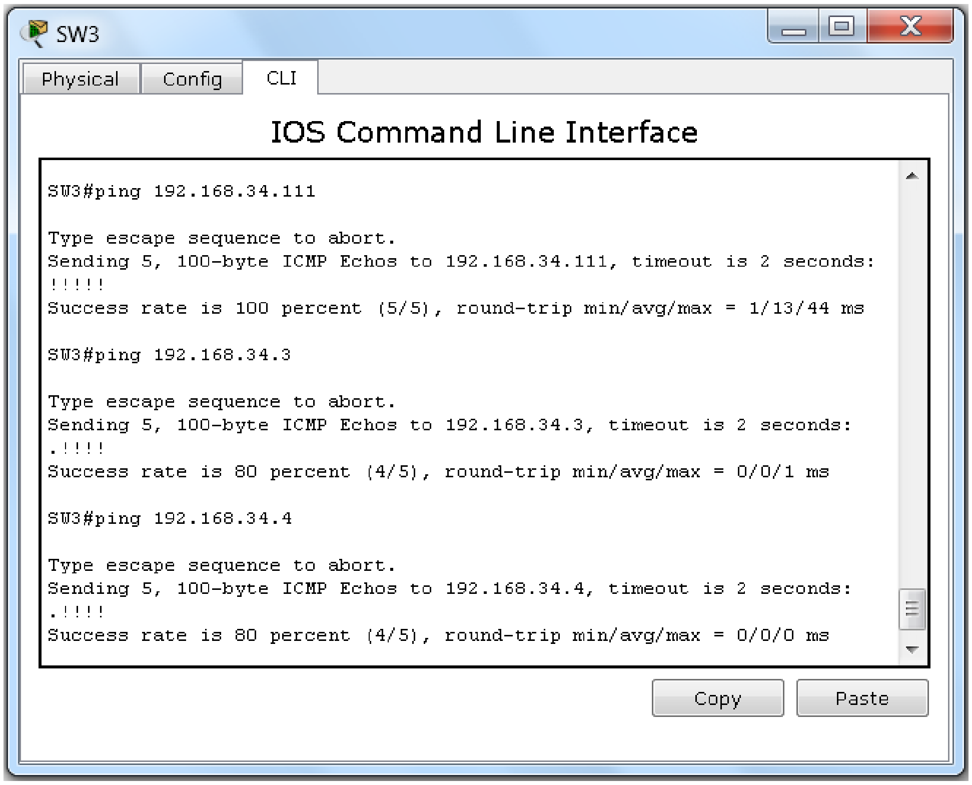
When enabling CDP globally on the switch, use the command **cdp run** in global configuration mode, and use **cdp enable** in interface command mode. Now when you use the **show cdp neighbors command**, you will see SW3 listed as a directly connected neighbor. Repeat these steps on R4 to complete the process.

Use IP Utilities to Test for Connectivity & Reachability

When troubleshooting a network, two important things you need to verify are connectivity (that is, is the interface and/or device attached to the network) and reachability (whether you can get to that device across the network). You have already used CDP as a tool for verifying Layer 2 connectivity, so now you need to get acquainted with tools that test at Layer 3. These tools are **ping** and **traceroute**, and you will use them on SW3. It is assumed that you are already in the Packet Tracer Interface. The instructions for using these commands are as follows:

1.1.115. Testing for network connectivity using ping

Ping is rumored to be an acronym for the phrase Packet Internet Groper (the author of the utility, Mike Muuss, denies this), and acts in the same way as sonar, in which a signal is transmitted and returns back to the point of origin. If you have ever shouted across a canyon and heard your voice reflected back, then you have an idea of how this operates. The network utility ping sends an electronic signal (called an ICMP **echo**), and when it reaches a network device, that device sends another signal back (called an ICMP **echo-reply**). There are two types of pings you can send from the CLI of a Cisco device, simple ping and extended ping, which you will use on SW3 as follows:



```
SW3#ping 192.168.34.111

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/44 ms

SW3#ping 192.168.34.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

SW3#ping 192.168.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

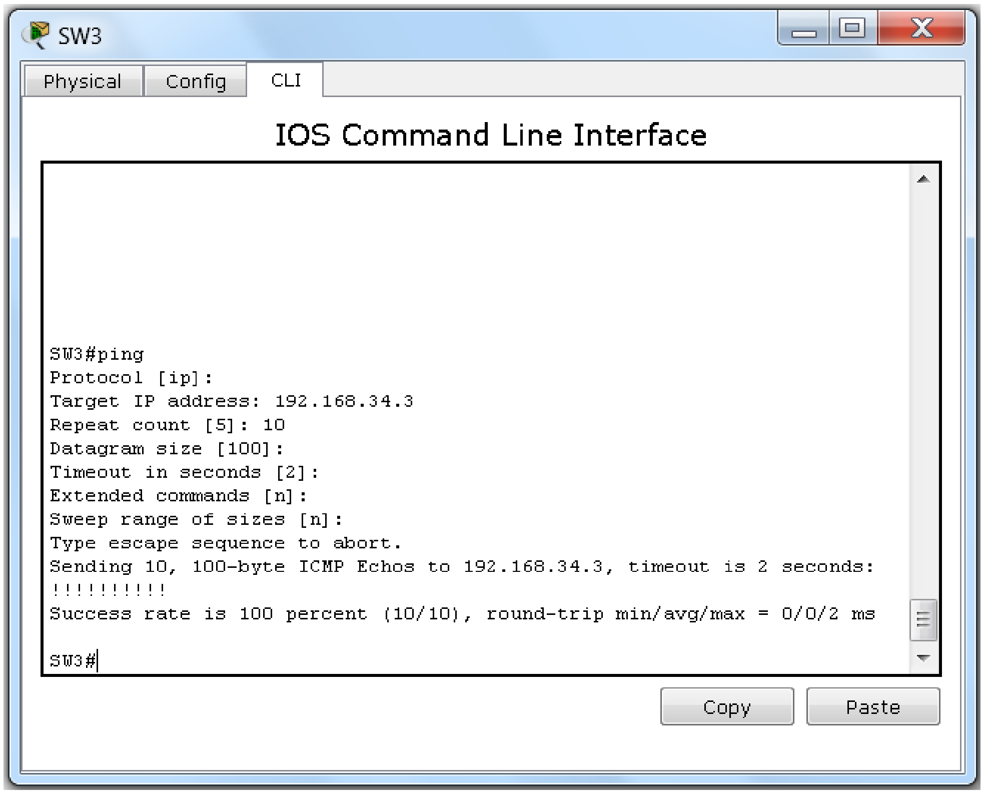
- Go to the command line interface of SW3 in user exec or privileged exec mode, and issue the command **ping <ip-address>**, as follows:

  - **ping 192.168.34.111** (the address of the VLAN 1 interface on SW3)
  - **ping 192.168.34.3** (the address of the LAN interface on R3)
  - **ping 192.168.34.111** (the address of the LAN interface on R4)

  You should receive replies from the addresses/devices as shows above. If you lose a packet or two at the beginning of the process, don't worry, you will get an explanation in one of the next lessons.

- Perform an extended ping by entering the command ping at the command line of SW3, with no specified address. You will see several questions regarding input, as follows:

  - **Protocol**: Typically IP (IP version 4, or IPv4), press enter for default
  - **Target IP Address**: The address of the device to send the signal to (use 192.168.34.3)
  - **Repeat Count**: How many packets to send (use 10)
  - **Datagram Size**: How large the packets should be (in bytes, leave at 100)
  - **Timeout in Seconds:** Interval in seconds between packets (leave at 2)
  - **Extended Commands:** Additional options to use (leave at no)
  - **Sweep Range of Sizes:** Increment the sizes of the packets (leave at no)

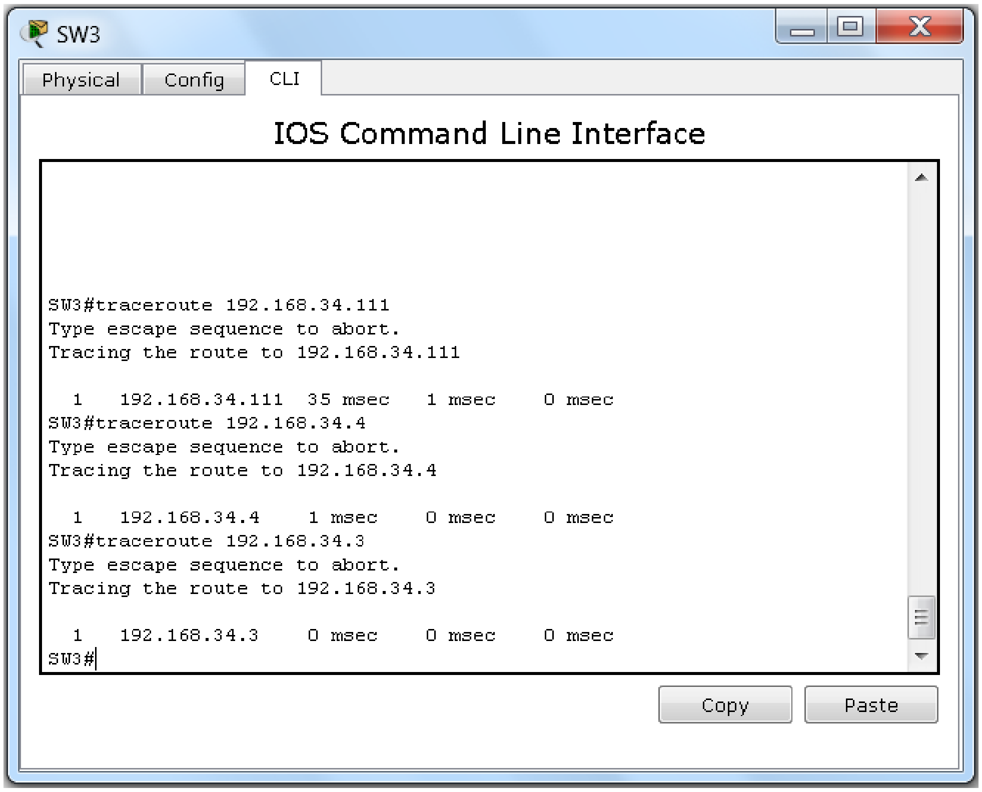


```
SW3#ping
Protocol [ip]:
Target IP address: 192.168.34.3
Repeat count [5]: 10
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.34.3, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 0/0/2 ms

SW3#
```

As you can see, ten ping packets with matching replies have been sent and received. In most cases you will use the simple **ping** command, but in order to generate traffic or choose a specific source address, you can use extended **ping**.

1.1.116. Testing for network connectivity using traceroute

Using **ping**, you can easily determine whether connectivity exists between addresses/interfaces/devices on the network, but you cannot determine the path that the packets have taken. Using ping's cousin, the **traceroute** utility, you can determine reachability and path of the packets. As with **ping**, you have the option of using a simple traceroute or an extended traceroute. Perform a simple traceroute on SW3 using the same addresses used before, as follows:



```
SW3#traceroute 192.168.34.111
Type escape sequence to abort.
Tracing the route to 192.168.34.111

  1   192.168.34.111  35 msec    1 msec    0 msec
SW3#traceroute 192.168.34.4
Type escape sequence to abort.
Tracing the route to 192.168.34.4

  1   192.168.34.4     1 msec    0 msec    0 msec
SW3#traceroute 192.168.34.3
Type escape sequence to abort.
Tracing the route to 192.168.34.3

  1   192.168.34.3     0 msec    0 msec    0 msec
SW3#
```

Since each of the IP addresses used are directly connected on the same LAN, you will observe only a single **hop** (the term for the number of IP networks that the packet crossed in reaching the destination). If a ping is sent to a network and fails, you can use the **traceroute** command to narrow down where the network path has been compromised. **Traceroute** is also helpful in determining the path that packets may travel.

Lesson 9 Lab Exercises

**** Cisco has removed 802.11 wireless topics and questions on the 100-101 and 200-101 exams for the CCNA/CCENT ****

Lesson 10 Lab Exercises

Internet Protocol version 4 Addressing

As explained in the lesson, the primary type of IP addressing is based on version 4 of the Internet Protocol. Most of the time you will see this referenced simply as IP, though this is increasingly referred to as IPv4. Since IP addressing is a complex topic that you need to thoroughly understand, this set of lab exercises will focus on these specifics.

1.1.117. Identifying IP (IPv4) address classes

In the early days of IP, addresses were organized into groups with specific characteristics. While five such classes exist, you will only have to focus on the first three for these lab exercises. For each IP address below, indicate whether it represents an A, B, of C address class (answers to follow):

- **192.168.1.0**
- **10.47.12.6**
- **1.1.1.1**
- **128.150.6.200**
- **1.2.3.4**
- **135.14.16.44**
- **12.34.56.78**
- **7.6.5.4**
- **200.200.200.200**
- **172.16.200.10**
- **216.145.1.2**
- **198.230.12.111**
- **223.200.187.30**
- **191.1.88.76**
- **50.40.30.20**
- **100.100.100.100**
- **176.44.211.28**
- **86.21.244.2**
- **67.41.12.6**
- **167.41.12.6**
- **207.110.67.41**
- **41.22.78.9**
- **12.100.208.77**
- **197.41.188.6**

Answers are as follows:

- **192.168.1.0:** Class C (192-223)
- **10.47.12.6:** Class A (1-126)
- **1.1.1.1:** Class A (1-126)
- **128.150.6.200:** Class B (128-191)
- **1.2.3.4:** Class A (1-126)
- **135.14.16.44** Class B (128-191)
- **12.34.56.78:** Class A (1-126)
- **7.6.5.4:** Class A (1-126)
- **200.200.200.200:** Class C (192-223)
- **172.16.200.10** Class B (128-191)
- **216.145.1.2:** Class C (192-223)
- **198.230.12.111:** Class C (192-223)
- **223.200.187.30:** Class C (192-223)
- **191.1.88.76** Class B (128-191)
- **50.40.30.20:** Class A (1-126)
- **100.100.100.100:** Class A (1-126)
- **176.44.211.28** Class B (128-191)
- **86.21.244.2:** Class A (1-126)
- **67.41.12.6:** Class A (1-126)
- **167.41.12.6** Class B (128-191)
- **207.110.67.41:** Class C (192-223)
- **41.22.78.9:** Class A (1-126)
- **12.100.208.77:** Class A (1-126)
- **197.41.188.6:** Class C (192-223)

1.1.118. Distinguishing between public and private (RFC 1918) addresses

When the Internet was turned over to the private sector, the system grew at a rapid rate that started to vastly deplete the pool of routable addresses. To alleviate this, certain ranges within each address class were designated as private---not routable on the Internet but usable within an organization. For each IP address below, indicate whether it represents a public or private address (answers to follow):

- **192.168.1.0**
- **1.1.1.1**
- **128.150.6.200**
- **1.2.3.4**
- **172.15.16.44**
- **12.34.56.78**
- **10.254.254.12**

- **200.200.200.200**
- **172.16.200.10**
- **216.145.1.2**
- **192.167.12.111**
- **10.0.0.1**
- **192.169.88.76**
- **172.31.30.20**
- **100.100.100.100**
- **172.30.211.28**
- **10.21.244.2**
- **172.22.12.6**
- **167.41.12.6**
- **207.110.67.41**
- **192.168.78.9**
- **12.100.208.77**

Answers are as follows:

- **192.168.1.0:** Private (192.168.X.X)
- **1.1.1.1:** Private (globally routable)
- **128.150.6.200:** Private (globally routable)
- **1.2.3.4:** Private (globally routable)
- **172.15.16.44:** Private (globally routable)
- **12.34.56.78:** Private (globally routable)
- **10.254.254.12:** Private (10.X.X.X)
- **200.200.200.200:** Private (globally routable)
- **172.16.200.10:** Private (172.16.X.X – 172.31.X.X)
- **216.145.1.2:** Private (globally routable)
- **192.167.12.111:** Private (globally routable)
- **10.0.0.1:** Private (10.X.X.X)
- **192.169.88.76:** Private (globally routable)
- **172.31.30.20:** Private (172.16.X.X – 172.31.X.X)
- **100.100.100.100:** Private (globally routable)
- **172.30.211.28:** Private (172.16.X.X – 172.31.X.X)
- **10.21.244.2:** Private (10.X.X.X)
- **172.22.12.6** Private (172.16.X.X – 172.31.X.X)
- **167.41.12.6:** Private (globally routable)
- **207.110.67.41:** Private (globally routable)
- **192.168.78.9:** Private (192.168.X.X)
- **12.100.208.77:** Private (globally routable)

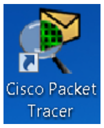
Lesson 11 Lab Exercises

Utilize the Address Resolution Protocol (ARP)

The Internet Protocol is not a single protocol in and of itself, but a collection or suite of protocols designed to work together to achieve network communication. One IP service in this regard is the ***Address Resolution Protocol (ARP)***, which maps Layer 2 MAC addresses to Layer 3 IP addresses. This lab exercise will demonstrate the components and operation of ARP.

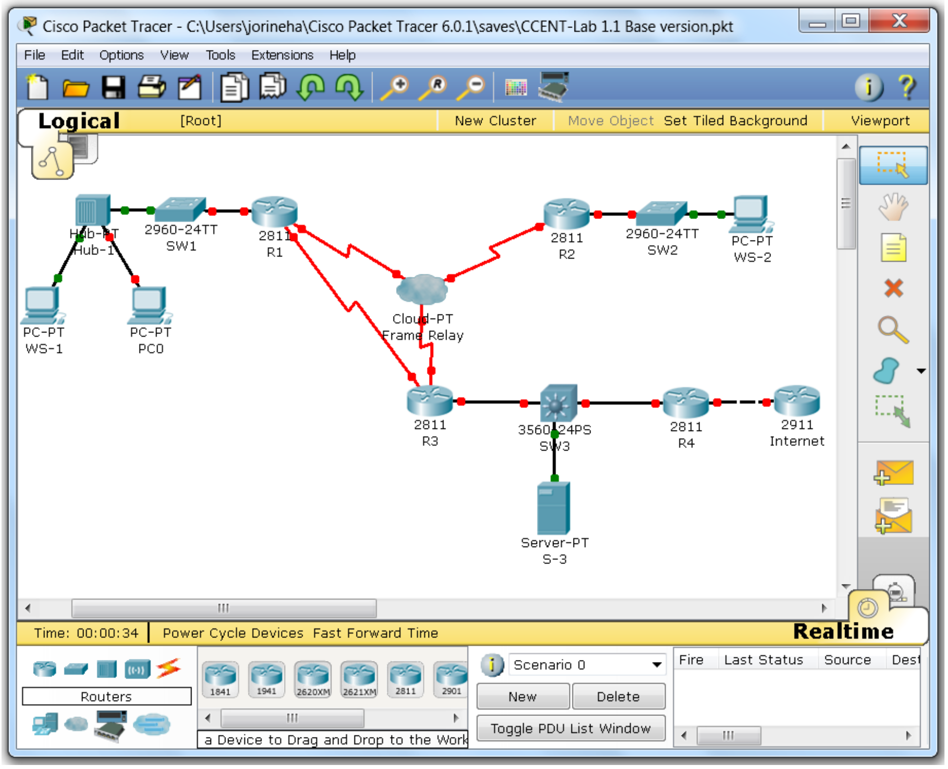
1.1.119. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



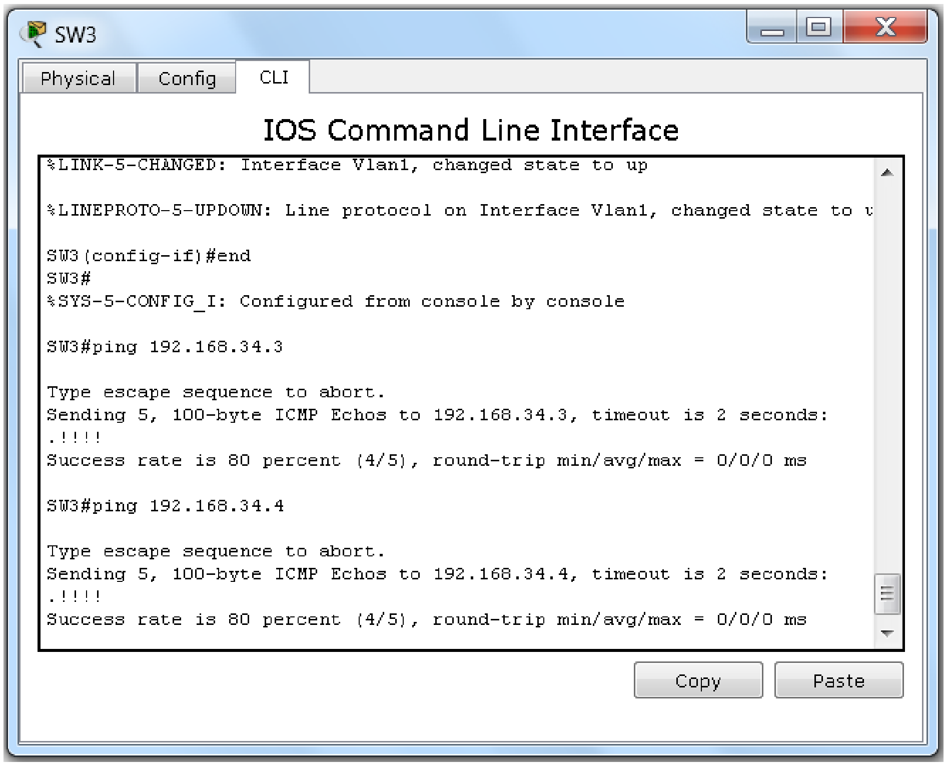
1.1.120. Select SW3 by double clicking the image

Begin by accessing SW3 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



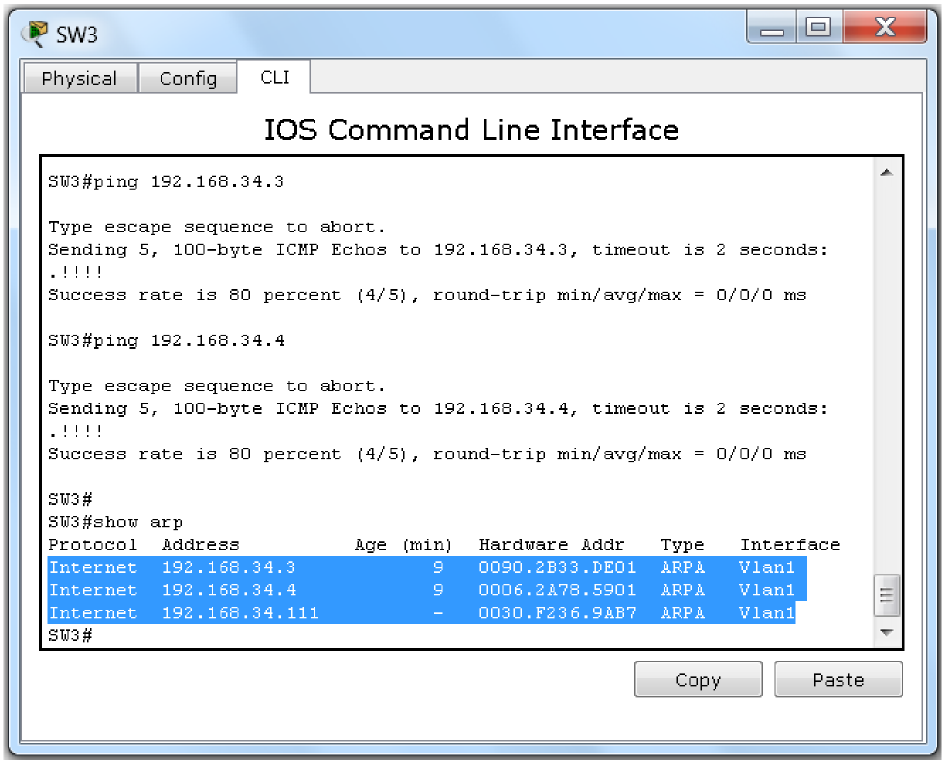
1.1.121. Create traffic that will show ARP in operation

As mentioned in Lesson 11, IP requires a binding relationship between the IP address and the LAN or MAC address of a device in order to enable network communication. In this lab exercise, you will use the ping utility to create traffic between SW3, R3 & R4 in order to trigger the ARP process. Execute these steps as follows:



```
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to u

SW3(config-if)#end
SW3#
%SYS-5-CONFIG_I: Configured from console by console

SW3#ping 192.168.34.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW3#ping 192.168.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

- Enter global configuration mode using the **configure terminal** command
- Enter interface configuration mode using the command **int vlan 1**
- Shut down the logical interface with the **shutdown** command (you will see the interface go down)
- Issue the **no shutdown** command to restore the interface
- Use the **end** command to return to privileged exec mode (this process will clear any existing **arp** entries)
- Issue the **show arp** command to show existing entries. You should only see an entry for 192.168.34.111 (the IP address of the VLAN 1 interface on SW3, which is local to the switch)
- Execute a **ping** to 192.168.34.3 (R3's LAN interface). You will notice that a packet or two is lost in the process, this is due to R3's LAN interface MAC and IP addresses not having an ARP table entry
- Execute a second **ping** to 192.168.34.4 (R4's LAN interface). You will notice that a packet or two is lost in the process, this is due to R4's LAN interface MAC and IP addresses not having an ARP table entry
- Issue the **show arp** command again to display the new bindings created as a result of the ping traffic. Both R3 & R4 should have entries now.



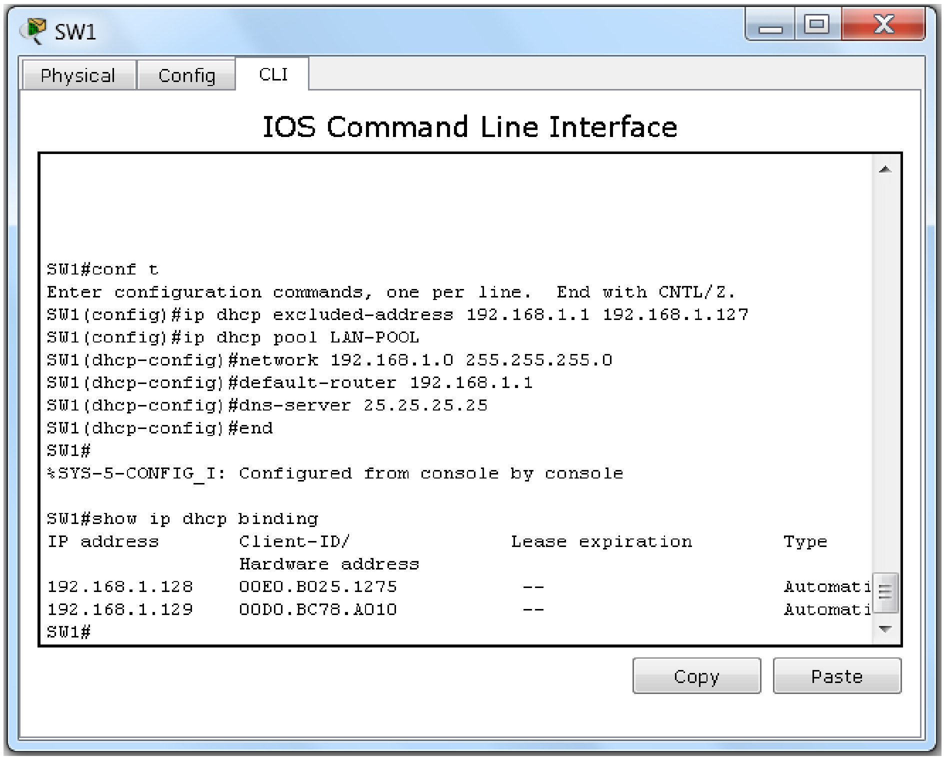
```
SW3#ping 192.168.34.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW3#ping 192.168.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW3#
SW3#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.34.3            9   0090.2B33.DE01  ARPA   Vlan1
Internet  192.168.34.4            9   0006.2A78.5901  ARPA   Vlan1
Internet  192.168.34.111          -   0030.F236.9AB7  ARPA   Vlan1
SW3#
```

Utilize the Dynamic Host Configuration Protocol (DHCP)

In the early days of networking, technicians and engineers had to manually enter IP addresses on every device that required connectivity. In small networks that may seem trivial, but what happens when you have hundreds of workstations? In addition, if the addresses have to be changed at some point, it would create an enormous amount of work to achieve. For these and other reasons, the ***Dynamic Host Configuration Protocol*** (***DHCP***) was created, drawing on earlier efforts such as ***Reverse Address Resolution Protocol*** (***RARP***) and the ***Bootstrap Protocol*** (***Bootp***). One workstation, WS-2, has a statically assigned address, but the two others, WS1-1 & WS2-2, require DHCP for addresses. Since R1, SW1 and the workstations all share the same LAN segment, either of the two devices can provide this, but use SW1 for this purpose. Configure DHCP for the workstations as follows:

- Enter global configuration mode on SW1 using the **config t** command
- Next, define the IP addresses that you do not want the workstations to use, using the command **ip dhcp excluded-address 192.168.1.1 192.168.1.127**
- Create the DHCP pool of addresses and associated settings using the command **ip dhcp pool LAN-POOL**
- Specify the 192.168.1.0/24 as the DHCP network range using the command **network 192.168.1.0 255.255.255.0**
- Identify the default gateway with the command **default-router 192.168.1.1**
- Specify the server that will be providing ***Domain Name Services*** (***DNS***, the servers that map ***Uniform Resource Locators*** (***URL***) such as www.cisco.com, and the IP addresses of the server). Use the command **dns-server 25.25.25.25**

- Exit DHCP pool configuration mode using the **exit** command
- Save the configuration using the **wr mem** command
- Display the DHCP bindings using the **show ip dhcp bindings** command. Two entries should appear, indicating that your configuration works



```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.127
SW1(config)#ip dhcp pool LAN-POOL
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#dns-server 25.25.25.25
SW1(dhcp-config)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.128    00E0.B025.1275           --                     Automati
192.168.1.129    00D0.BC78.A010           --                     Automati
SW1#
```

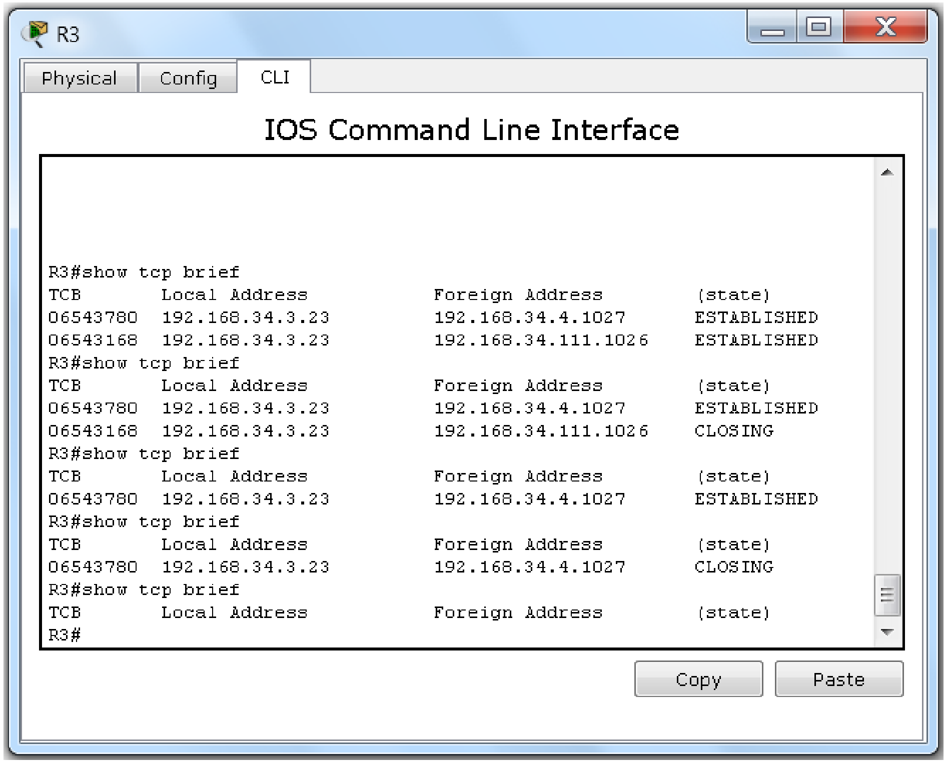
Observe the Operation of the Transmission Control Protocol (TCP)

The Transport Layer provides end-to-end connectivity to applications and has both TCP and UDP to fulfill those duties. TCP, while more reliable, has a substantial amount of overhead to perform its functions, as opposed to UDP which has very little. In order to observe the operation of TCP, you will establish several remote terminal sessions to R3, and then observe the results. Perform this task as follows:

- Open a CLI session on SW3 and initiate a telnet session using the command **telnet 192.168.34.3** (the LAN interface IP address of R3). When prompted for a password, enter **cisco**, which you configured on the vty lines in an earlier lab exercise.
- Open a CLI session on R4 and initiate a telnet session using the command **telnet 192.168.34.3** (the LAN interface IP address of R3). When prompted for a password, enter **cisco**, which you configured on the vty lines in an earlier lab exercise.
- Open the CLI of R3 and execute the command **show tcp**, which will generate a lot of detailed information. To simplify the output, reenter the command with the keyword **brief** (**show tcp brief**). The two sessions should display, note the following:

- **Local Address:** Should read 192.168.34.3.23, which shows the destination address (192.168.34.3) and the TCP port being used (23)
- **Foreign Address:** Should read 192.168.34.111 and 192.168.34.4, with port numbers greater than 1024. These numbers are the random source port chosen by TCP during session establishment
- **Established:** Indicates that the TCP handshake was successful and that a session is fully established

- Return to SW3 and end the telnet session using the exit command. Return to R3 quickly and issue the **show tcp brief** command again. You should see that the ***established*** entry has changed to ***closing*** (indicating that the TCP session is being torn down). After a few moments the session should be disappear if you use the command again.
- Repeat the same steps on R4. Note the ***closing*** state, and eventual drop of the session



```
R3#show tcp brief
TCB       Local Address           Foreign Address        (state)
06543780  192.168.34.3.23         192.168.34.4.1027      ESTABLISHED
06543168  192.168.34.3.23         192.168.34.111.1026    ESTABLISHED
R3#show tcp brief
TCB       Local Address           Foreign Address        (state)
06543780  192.168.34.3.23         192.168.34.4.1027      ESTABLISHED
06543168  192.168.34.3.23         192.168.34.111.1026    CLOSING
R3#show tcp brief
TCB       Local Address           Foreign Address        (state)
06543780  192.168.34.3.23         192.168.34.4.1027      ESTABLISHED
R3#show tcp brief
TCB       Local Address           Foreign Address        (state)
06543780  192.168.34.3.23         192.168.34.4.1027      CLOSING
R3#show tcp brief
TCB       Local Address           Foreign Address        (state)
R3#
```

Lesson 12 Lab Exercises

Calculating Subnet, Broadcast Address, and Host Addresses for an IP

One of the most common ICND1 questions concerns a student's ability to discover the particular details of a subnet based on an IP address and mask. Since this skill can mean the difference between passing and failing, you will have the opportunity to calculate these values from the list below. For each address/mask pair, calculate the subnet address, the broadcast address, and the range of valid hosts:

1.1.122. Subnet Addresses to Calculate

- 10.41.116.8/24 (255.255.255.0)
- 192.168.46.112/30 (255.255.255.252)
- 135.11.66.9/25 (255.255.255.128)
- 99.8.44.129/23 (255.255.254.0)
- 172.21.116.2/27 (255.255.255.224)
- 199.189.12.20/26 (255.255.255.192)
- 1.2.3.4/20 (255.255.240.0)

1.1.123. Answers

- 10.41.116.8/24 (255.255.255.0)
  - Subnet Address: 10.41.116.0
  - Broadcast Address: 10.41.116.255
  - Range of Valid Hosts: 10.41.116.1 - 10.41.116.254

- 192.168.46.112/30 (255.255.255.252)
  - Subnet Address: 192.168.46.112
  - Broadcast Address: 192.168.46.115
  - Range of Valid Hosts: 192.168.46.113 - 192.168.46.114

- 135.11.66.9/25 (255.255.255.128)
  - Subnet Address: 135.11.66.0
  - Broadcast Address: 135.11.66.127
  - Range of Valid Hosts: 135.11.66.1 - 135.11.66.126

- 99.8.44.129/23 (255.255.254.0)
  - Subnet Address: 99.8.44.0
  - Broadcast Address: 99.8.45.255
  - Range of Valid Hosts: 99.8.44.1 - 99.8.45.254

- 172.21.116.2/27 (255.255.255.224)
  - Subnet Address: 126.21.116.0
  - Broadcast Address: 126.21.116.31
  - Range of Valid Hosts: 126.21.116.1 - 126.21.116.30
- 199.189.12.20/26 (255.255.255.192)
  - Subnet Address: 199.189.12.0
  - Broadcast Address: 199.189.12.63
  - Range of Valid Hosts: 199.189.12.1 - 199.189.12.62
- 1.2.3.4/20 (255.255.240.0)
  - Subnet Address: 1.2.0.0
  - Broadcast Address: 1.2.15.255
  - Range of Valid Hosts: 1.2.0.1 - 1.2.15.254

Choosing a Subnet Mask for A Number of Hosts

Another common subnetting task for the ICND1 exam, as well as in practical settings, is to choose a subnet mask to support a specific number of hosts. Based on the requirements below, choose a mask from the range that will fully support the number of hosts required:

1.1.124. Subnet Addresses to Choose

- 192.168.200.0/24 (8 usable hosts)
- 47.80.197.0/23 (60 usable hosts)
- 133.144.12.0/24 (120 usable hosts)
- 216.145.11.0/24 (30 usable hosts)
- 172.16.12.0/16 (2 usable hosts)
- 193.44.78.0/25 (20 usable hosts)
- 189.112.213.0/26 (16 usable hosts)

1.1.125. Answers

- 192.168.200.0/24 (8 usable hosts)
  - Subnet Address: 192.168.200.0
  - Broadcast Address: 192.168.200.15
  - Range of Valid Hosts: 192.168.200.1 - 192.168.200.14
  - Hosts Supported: 14 (14 – 8 = 6 spare)
- 47.80.197.0/23 (60 usable hosts)

  - Subnet Address: 47.80.197.0
  - Broadcast Address: 47.80.197.63
  - Range of Valid Hosts: 47.80.197.1 - 47.80.197.62
  - Hosts Supported: 62 (62 – 6 = 2 spare)

- 133.144.12.0/24 (120 usable hosts)

  - Subnet Address: 133.144.12.0
  - Broadcast Address: 133.144.12.127
  - Range of Valid Hosts: 133.144.12.1 - 133.144.12.126
  - Hosts Supported: 126 (126 – 120 = 6 spare)

- 216.145.11.0/24 (30 usable hosts)

  - Subnet Address: 216.145.11.0
  - Broadcast Address: 216.145.11.31
  - Range of Valid Hosts: 216.145.11.1 - 216.145.11.30
  - Hosts Supported: 30 (30 – 30 = 0 spare)

    ***** Having no room for growth is not advisable in a production environment *****

- 172.16.12.0/24 (2 usable hosts)

  - Subnet Address: 172.16.12.0
  - Broadcast Address: 172.16.12.3
  - Range of Valid Hosts: 172.16.12.1 - 172.16.12.2
  - Hosts Supported: 2 (2 – 2 = 0 spare)

  ***** Having no room for growth is not advisable in a production environment, although perfectly acceptable on a point-to-point link *****

- 193.44.78.0/25 (20 usable hosts)

  - Subnet Address: 193.44.78.0
  - Broadcast Address: 193.44.78.31
  - Range of Valid Hosts: 193.44.78.1 - 193.44.78.30
  - Hosts Supported: 30 (30 – 20 = 10 spare)

- 189.112.213.0/26 (16 usable hosts)

  - Subnet Address: 189.112.213.0
  - Broadcast Address: 189.112.213.31
  - Range of Valid Hosts: 189.112.213.1 - 189.112.213.30
  - Hosts Supported: 30 (30 – 16 = 14 spare)

Choosing a Subnet Mask for A Number of Networks

Another common subnetting task for the ICND1 exam, as well as in practical settings, is to choose a subnet mask to support a specific number of networks. Using the previous list and the requirements below, choose a mask from the range that will fully support the number of networks required:

1.1.126. Subnet Addresses to Choose

- 192.168.200.0/24 (4 networks)
- 47.80.197.0/23 (16 networks)
- 133.144.12.0/24 (12 networks)
- 216.145.11.0/24 (3 networks)
- 172.16.12.0/16 (2 networks)
- 193.44.78.0/25 (6 networks)
- 189.112.213.0/26 (3 networks)

1.1.127. Answers

- 192.168.200.0/24 (4 networks)
  - Subnet Mask: 255.255.255.192 (/26)
  - Number of Subnets: 4
  - Hosts per Subnet: 62
  - Subnets:
    - 192.168.200.0/26
    - 192.168.200.64/26
    - 192.168.200.128/26
    - 192.168.200.192/26
- 47.80.197.0/23 (16 networks)
  - Subnet Mask: 255.255.255.224 (/27)
  - Number of Subnets: 16
  - Hosts per Subnet: 30
  - Subnets:
    - 47.80.196.0/27
    - 47.80.196.32/27
    - 47.80.196.4/27
    - 47.80.196.96/27
    - 47.80.196.128/27
    - 47.80.196.160/27
    - 47.80.196.192/27
    - 47.80.196.224/27

        - 47.80.197.0/27
        - 47.80.197.32/27
        - 47.80.197.4/27
        - 47.80.197.96/27
        - 47.80.197.128/27
        - 47.80.197.160/27
        - 47.80.197.192/27
        - 47.80.197.224/27

- 133.144.12.0/24 (12 networks)

    - Subnet Mask: 255.255.255.240 (/28)
    - Number of Subnets: 16
    - Hosts per Subnet: 14
    - Subnets:

        - 133.144.12.0/27
        - 133.144.12.16/27
        - 133.144.12.32/27
        - 133.144.12.48/27
        - 133.144.12.64/27
        - 133.144.12.80/27
        - 133.144.12.96/27
        - 133.144.12.112/27
        - 133.144.12.128/27
        - 133.144.12.144/27
        - 133.144.12.160/27
        - 133.144.12.176/27
        - 133.144.12.192/27
        - 133.144.12.208/27
        - 133.144.12.224/27
        - 133.144.12.240/27

- 216.145.11.0/24 (3 networks)

    - Subnet Mask: 255.255.255.192 (/26)
    - Number of Subnets: 4
    - Hosts per Subnet: 62
    - Subnets:

        - 216.145.11.0/26
        - 216.145.11.64/26
        - 216.145.11.128/26
        - 216.145.11.192/26

- 172.16.12.0/24 (2 networks)

    - Subnet Mask: 255.255.255.128 (/25)

    - Number of Subnets: 2
    - Hosts per Subnet: 126
    - Subnets:
        - 172.16.12.0/25
        - 172.16.12.128/25

- 193.44.78.0/25 (6 networks)
    - Subnet Mask: 255.255.255.240 (/28)
    - Number of Subnets: 8
    - Hosts per Subnet: 14
    - Subnets:
        - 193.44.78.0/28
        - 193.44.78.16/28
        - 193.44.78.32/28
        - 193.44.78.48/28
        - 193.44.78.64/28
        - 193.44.78.80/28
        - 193.44.78.96/28
        - 193.44.78.112/28

- 189.112.213.0/26 (3 networks)
    - Subnet Mask: 255.255.255.240 (/28)
    - Number of Subnets: 4
    - Hosts per Subnet: 14
    - Subnets:
        - 189.112.213.0/28
        - 189.112.213.16/28
        - 189.112.213.32/28
        - 189.112.213.48/28

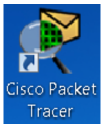
Lesson 13 Lab Exercises

Working with Connected IP (IPv4) Routes

Connected routes (sometimes referred to as ***directly connected***) exist in the IP routing table of a router or L3 switch by virtue of configured interface addresses. To get better acquainted with this concept, you will perform several tasks in this lab exercise, as follows:

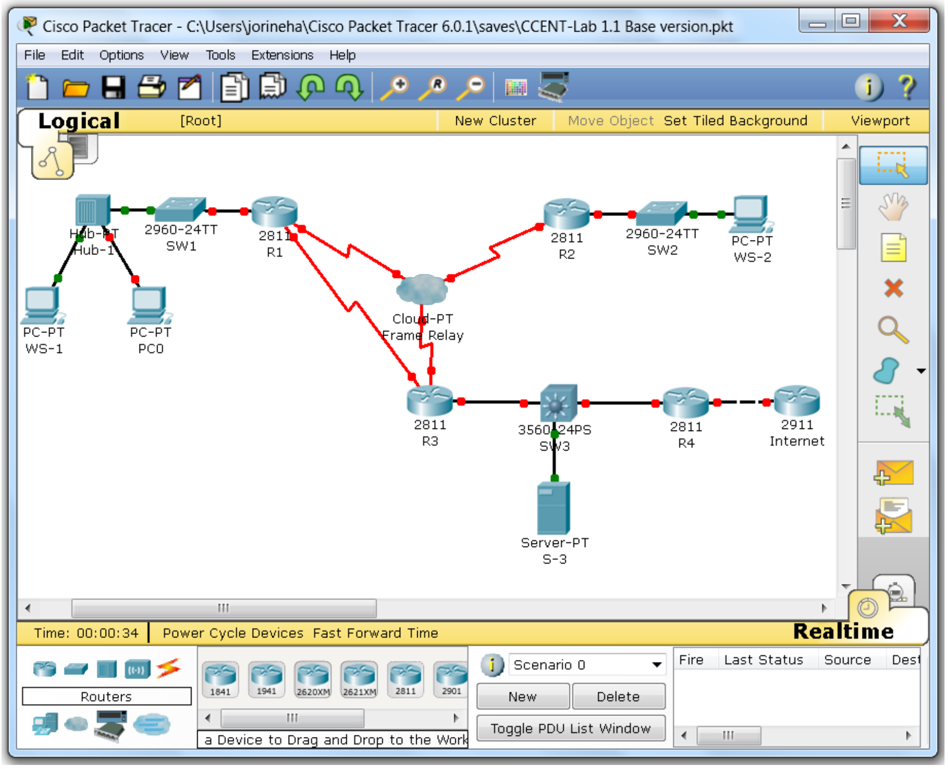
1.1.128. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



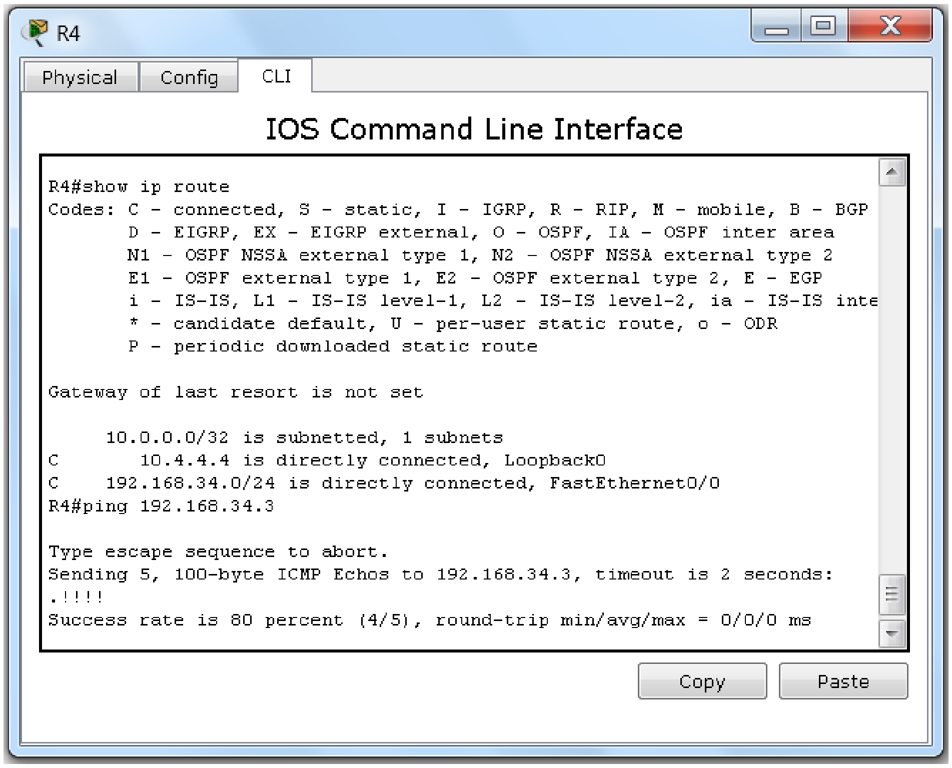
1.1.129. Select R4 by double clicking the image

Begin by accessing R4 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



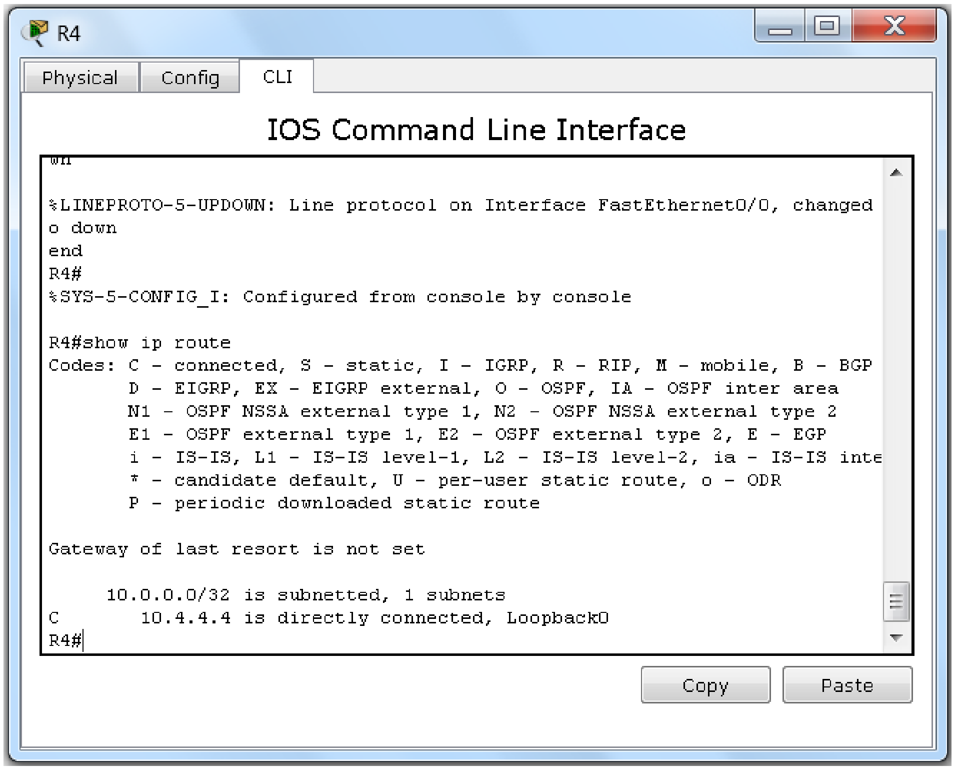
1.1.130. Display the IP (IPv4) Routing Table on R4

The IP routing table (sometimes referred to as a ***forwarding table***) on a router contains all of the networks/subnets that the device knows about. If there is no entry in the table for a particular network, the device considers it unreachable and will drop the packet. An exception to this behavior exists with regard to default routes, which will be analyzed later. Display the available networks on R4 by performing the following steps:



```
R4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/32 is subnetted, 1 subnets
C       10.4.4.4 is directly connected, Loopback0
C    192.168.34.0/24 is directly connected, FastEthernet0/0
R4#ping 192.168.34.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.34.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

- Because you previously configure the console line of the router to enter into privileged mode with no login process, you can simply press **<enter>** to begin
- Enter the command **show ip route** to display the current entries on the IP routing table, which should match the image above
- Both routes displayed, 10.4.4.4/32 and 192.168.34.0/24 exist in the routing table by virtue of configuration. In earlier labs, you configured the Loopback 0 and FastEthernet 0/0 interfaces with these addresses.
- Since R3 (192.168.34.4/24) exists on the same network as FastEthernet 0/0, you can ping that address directly, as shown above. Use the command **ping 192.168.34.3** to verify connectivity.
- Next, enter global configuration mode with the **config t** (short for **configure terminal**, a handy shortcut)
- Enter interface configuration mode using the command **interface Fa0/0**, and then enter the **shutdown** command. You should see the interface go down.
- Use the **end** command to return to exit configuration mode, and execute the **show ip route** command again. Notice that since the interface configured with the 192.168.34.4 address is down, that R4 no longer knows about that subnet.



```
wn

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
o down
end
R4#
%SYS-5-CONFIG_I: Configured from console by console

R4#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/32 is subnetted, 1 subnets
C       10.4.4.4 is directly connected, Loopback0
R4#
```

- Attempt to ping 192.168.34.3 again. You will notice that the ping fails because there is no longer a connected route to that network.
- Return to configuration mode (global, then interface mode for Fa0/0), and restore the interface using the **no shutdown** command. If you try the ping again, you will be successful.

Working with Static Routes

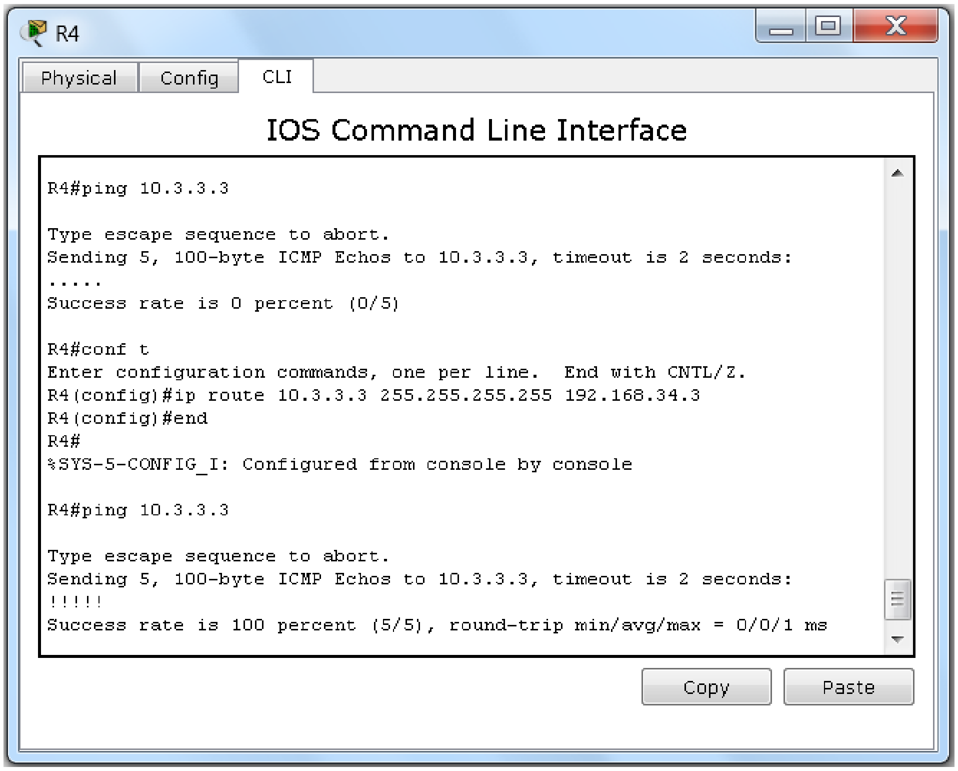
One of the simplest methods for creating entries in the IP (IPv4) routing table of a router is to configure them manually using ***static routes***, so named because once entered they do not change. Configure static routing on R3 and R4 as follows:

1.1.131. Display the IP (IPv4) Routing Table on R4

As in the previous lab task, display the IP routing table on R4 using the command **show ip route**. Since you re-enabled Fa0/0 after shutting it down previously, the two directly connected routes should display as follows:

- 10.4.4.4/32 (Loopback 0)
- 192.168.34.0/24 (Fa0/0)

Now execute a ping to R3's Loopback 0 interface (10.3.3.3/32) using the command **ping 10.3.3.3**. You will see the ping fail because there is no routing entry for that network in the routing table of R4



```
R4#ping 10.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip route 10.3.3.3 255.255.255.255 192.168.34.3
R4(config)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console

R4#ping 10.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

1.1.132. Configure a Static Route to Network 10.3.3.3/32 on R4

To create an entry to 10.3.3.3 in the routing table of R4, you will need to add a static route to the table, using the following simple steps:

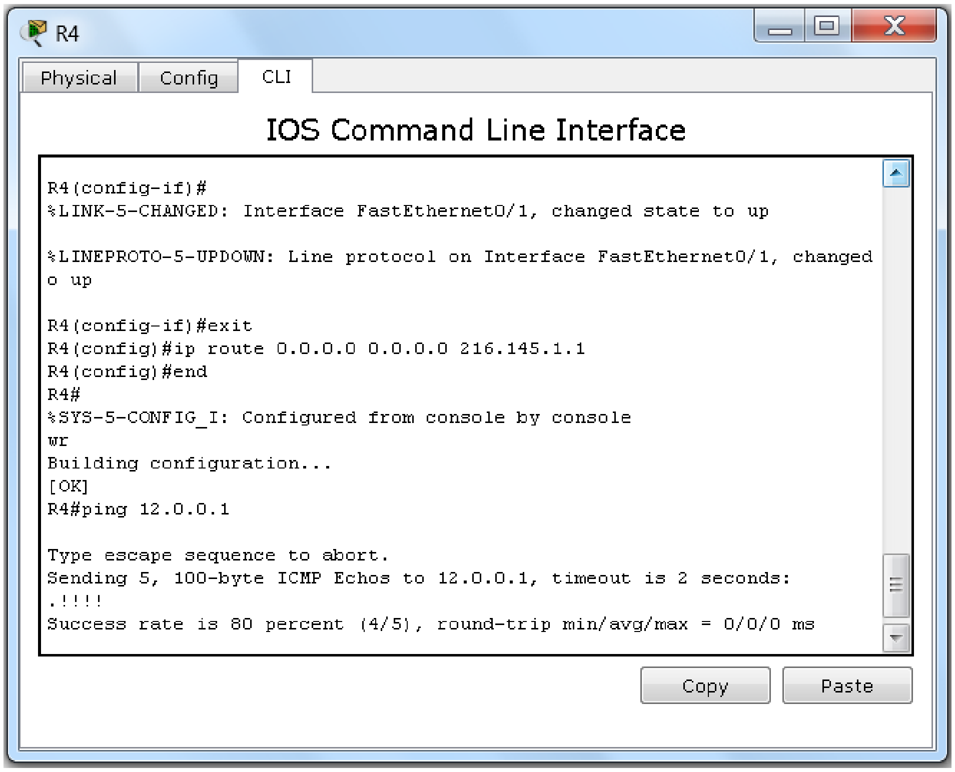
- Enter global configuration mode using the command **configure terminal** (or **conf t** for short)
- Create a static routing entry using the command **ip route 10.3.3.3 255.255.255.255 192.168.34.3**. Remember the significance of each part of the command:
  - **Network**: 10.3.3.3 (Loopback 0 interface address on R3)
  - **Mask**: 255.255.255.255 (mask to match)
  - **Next-Hop**: 192.168.34.3 (what interface/network to use to reach the desired address)
- Exit configuration mode using the **end** command
- Perform the **ping** command again (**ping 10.3.3.3**) which should now succeed
- Enter the command **show ip route**, and you will see the new route with the ***S*** indicator (S=***Static***, C=***Connected***, etc.)

Working with Default Routes

When a packet is destined for an unknown network (that is, not contained in its routing table), the router will discard it. In the previous lab exercise, you experienced this when you first attempted to ping the Loopback interface of R3 from R4. In many cases it would be difficult to have a routing table that literally contains every possible route, which raises the need for a "catch all" route. Just as a route with the mask 255.255.255.255 (also called a host route) is the most mathematically specific (meaning it will only match ***one*** IP address), a ***default*** route is the most mathematically general (matches ***every*** possible route). This is virtually identical to the ***default gateway*** that you configured on the switches earlier in the lab. In essence, it instructs the router to send all traffic to the specified address if it cannot find another route in the IP routing table (which is also why it can be called the ***gateway of last resort***). In many circumstances, a default route points to a local site's Internet connection. Configure a default static routing on R4 as follows:

1.1.133. Configure Internet Connectivity on R4

R4 has a direct connection to the Internet router on Fa0/1, but at present the interface is shut down and unconfigured. Configure and enable the interface using the following steps:



```
R4(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
o up

R4(config-if)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 216.145.1.1
R4(config)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R4#ping 12.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

- Enter global configuration mode using the **configure terminal** (or **conf t**) command
- Enter interface configuration mode using the command **interface fa0/1**
- Configure a routable IP address on the interface with the command **ip address 216.145.1.100 255.255.255.0**
- Enable the interface using the **no shutdown** command (you should see the interface come up immediately)

- Exit interface configuration mode using the **exit** command (this will return you to global configuration mode, the **end** command would have left configuration mode altogether)
- Configure a static default route by entering **ip route 0.0.0.0 0.0.0.0 216.145.1.1** (the IP address of the Internet router)
- Exit configuration mode by typing the **end** command
- Save your configuration using the **write memory** (or **wr mem**) command
- Display the contents of the ip routing table on R4 by executing the **show ip route** command. Note that there is a static route new entry with the ***** identifier, as well as the words g***ateway of last resort is 216.145.1.1 to network 0.0.0.0***
- Ping routable Internet addresses by issuing the following commands

  - **ping 12.0.0.1**
  - **ping 124.0.0.1**
  - **ping 135.12.0.1**

- Note that even though these networks do not exist in the ip routing table, the default route forwards them to the Internet and back again

Dynamic Routing

Static routes allow a network administrator to have direct and granular control over IP routing in a network, but in a large production environment this can become labor intensive. To counteract this, network designers introduced dynamic routing protocols, which allow devices to exchange routing information, as well as respond to changing conditions. One of the first protocols developed was the Routing Information Protocol (RIP), which has a very simple (though limited) design. Please note that RIP no longer appears on the CCENT (100-101) exam, though you will configure it here to illustrate how these protocols operate. Configure RIP routing on R3 and R4 as follows:

1.1.134. Configure RIP Version 2 Routing on R3

Of all routing protocols, RIP is the easiest to configure. Configure RIP on R3, using the following process:

- Enter global configuration mode using the **configure termina**l or **config t** commands
- Enter RIP configuration mode using these commands:

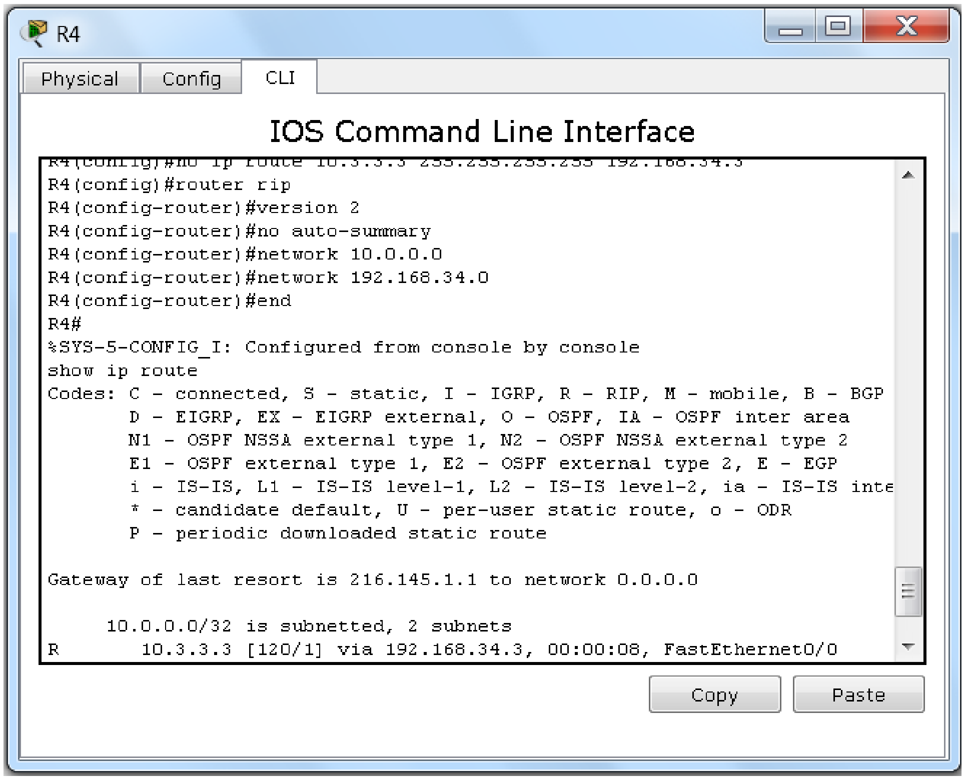
  - **router rip**: Initiates the RIP routing process
  - **version 2**: Version 1 is outdated and does not support subnet masks, variable mask types, or multicast updates. Version 1 is the default if this keyword is omitted
  - **no auto-summary**: By default, RIP will summarize all networks according to the old class A, B, & C rules. This command disables that behavior.
  - **Network 10.0.0.0**: Indicates which interface will participate in the routing process. RIP uses major network numbers for this

function, so since 10.3.3.3 is from a class A address, it matches any interface with the IP address of 10.0.0.0 – 10.255.255.254. This statement identifies the Loopback 0 interface as being part of the routing process. In this case, since this interface is not connected to any other device, this address will be advertised as a route, but not send any updates out to neighboring routers

- **Network 192.168.34.0:** Since this interface (Fa0/0) connects R3 to R4, this command will enable RIP updates to be sent & received, as well as the IP network to be advertised.

1.1.135. Remove the Static Route and Enable RIP Version 2 Routing on R4

In this lab exercise, the previously configured static route on R4 to network 10.3.3.3 no longer serves a useful purpose. Remove the route as follows:



```
R4(config)#no ip route 10.3.3.3 255.255.255.255 192.168.34.3
R4(config)#router rip
R4(config-router)#version 2
R4(config-router)#no auto-summary
R4(config-router)#network 10.0.0.0
R4(config-router)#network 192.168.34.0
R4(config-router)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 216.145.1.1 to network 0.0.0.0

     10.0.0.0/32 is subnetted, 2 subnets
R       10.3.3.3 [120/1] via 192.168.34.3, 00:00:08, FastEthernet0/0
```

- Enter global configuration mode using the **configure termina**l or **config t** commands Exit configuration mode by typing the **end** command
- Remove the static route by entering the statement **no ip route 10.3.3.3 255.255.255.255 192.168.34.3**
- Repeat the exact same set of commands used to enable RIP on R3
- Save your configuration using the **write memory** (or **wr mem**) command
- Use the command **show ip route** to display the ip routing table. You should see the route 10.3.3.3 with the letter R (for RIP) now displayed

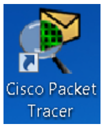
Lesson 14 Lab Exercises

Router Architecture & Hardware

While similarities exist between Cisco IOS-based Catalyst switches and Cisco routers, the differences run far deeper. Since both utilize the IOS operating system, the overall syntax, command structure, and command line of both are strikingly alike. Because of this similarity, this lesson on router operations and configuration would have many similar themes as the one focused on switches. Rather than simply repeat these parallel topics, you will instead focus on distinctive aspects of router hardware. For these purposes, you will examine R3 as the candidate device.

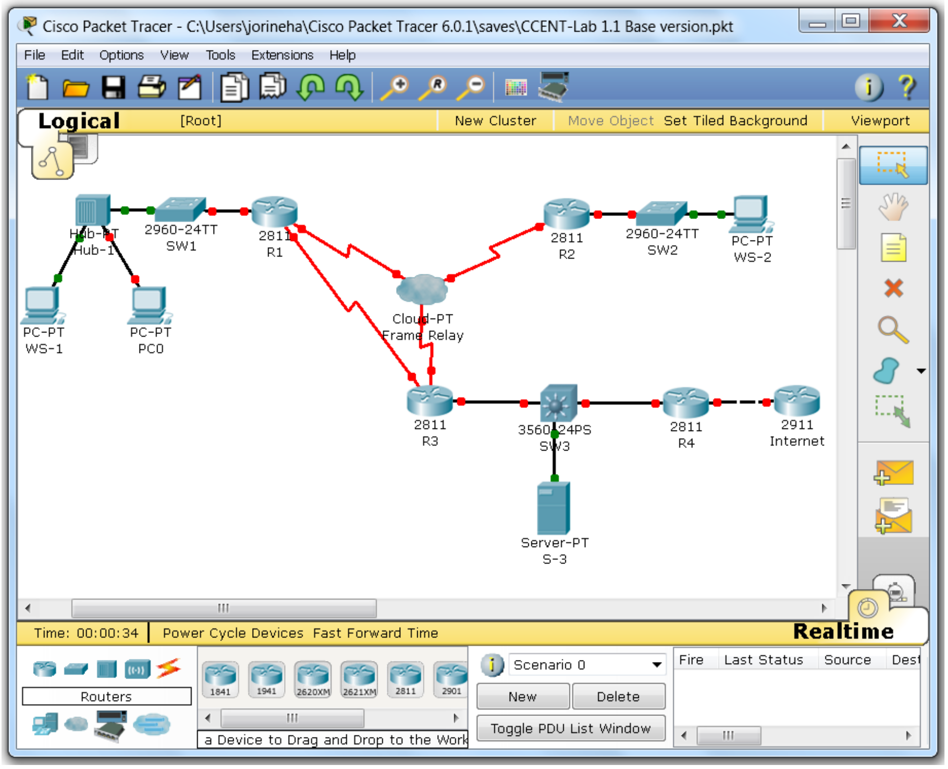
1.1.136. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



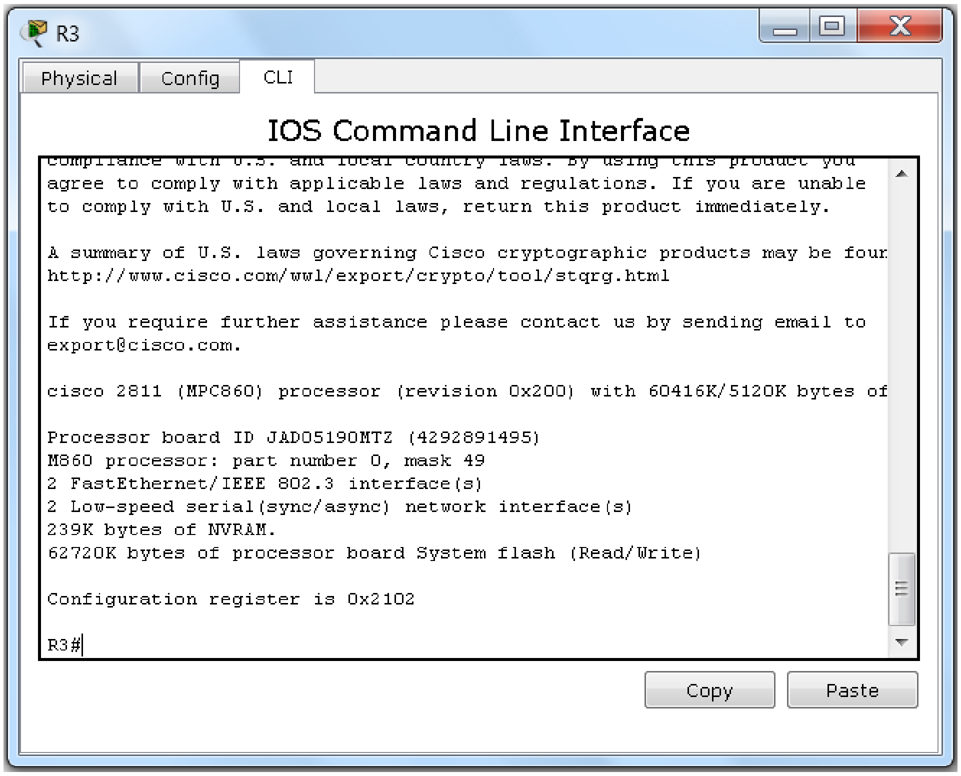
1.1.137. Select R3 by double clicking the image

Begin by accessing R3 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCENT-Lab 1.1 Base version.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Hub-PT
Hub-1
2960-24TT
SW1
2811
R1
Cloud-PT
Frame Relay
2811
R2
2960-24TT
SW2
PC-PT
WS-2
PC-PT
WS-1
PC-PT
PC0
2811
R3
3560 24PS
SW3
2811
R4
2911
Internet
Server-PT
S-3
Time: 00:00:34 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811 2901
a Device to Drag and Drop to the Work
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Dest

1.1.138. Review device hardware information on SW1

Once inside the command line interface of R3, type the command **show version**; this will display detailed hardware information on the device in question, as follows:



```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be foun
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of

Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

R3#
```

As already mentioned, you can see immediate similarities between the above output and that of the switch examined previously:

- **Model Number**: Cisco 2811 (first generation Integrated Services Router)
- **Interfaces**: Aside from the model number, the number and type of interfaces are clearly identified:
    - 2 Fast Ethernet (onboard interfaces built into the system board)
    - 2 Serial (used for Wide Area network interfaces, made available by the use of a WAN Interface Card (WIC) installed in an available slot
- **Available Memory**: Helpful when deciding what software images are supported.
- **Software Version/Image**: Though not displayed in the image above, the show version command also indicates what software is stored on the device, and what version is in use.
- **Configuration Register**: A specialized setting that changes the way that the device boots up and begins operating (more on this in a moment)
- **Reboot Cause**: Thought not displayed here, this indicates what created the boot process, such as “power on” (self-explanatory) or a software error. This can be invaluable when diagnosing hardware or software issues on the router

1.1.139. Understand the Operation of the Configuration Register

The configuration register is a sixteen-bit number expressed in hexadecimal format, shown in decimal on the device, as follows:

- Example as shown above: 0x2102, decoded as follows:

  - **0x**: Indicates that the number following is a decimal representation of a hexadecimal (base-16, as opposed to base-10 which is the familiar decimal system that humans use)
  - **2**: The first **four** bits of the register expressed in decimal (binary 0000-1111, or 0-15 decimal)
  - **1**: The second **four** bits of the register expressed in decimal (binary 0000-1111, or 0-15 decimal)
  - **0**: The third **four** bits of the register expressed in decimal (binary 0000-1111, or 0-15 decimal)
  - **2**: The fourth and final **four** bits of the register expressed in decimal (binary 0000-1111, or 0-15 decimal)

- Rather than learning all of the binary/hexadecimal details of the configuration register, instead memorize the most helpful combinations as follows:

  - **0x2102**: Normal mode of operation, ignores break key, boots into ROM if boot fails, 9600 console baud rate, processes startup-config
  - **0x2142**: Ignores break key, boots into ROM if boot fails, 9600 console baud rate, ignores startup-config (brings up the router thinking that it is a new, unconfigured device). This setting is most often used when performing a password reset
  - **0x2100**: Boots into ROM Monitor mode, ignores break key, boots into ROM if boot fails, 9600 console baud rate, processes startup-config
  - Other settings can change the console baud rate, enable/disable use of the break key, etc.

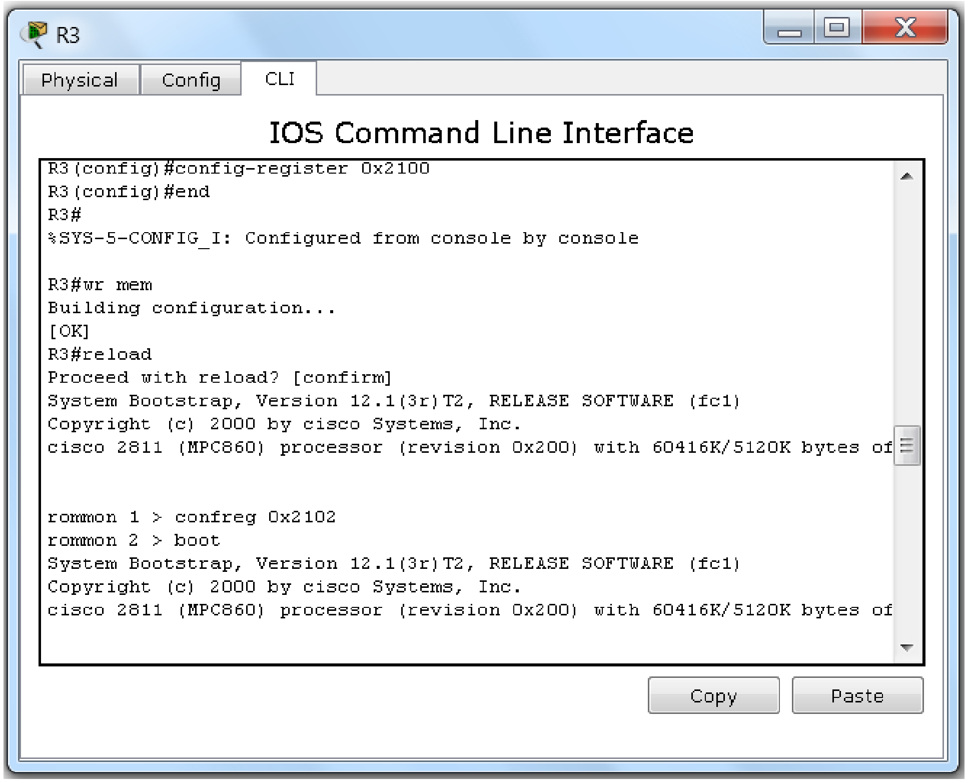
1.1.140. Changing the Configuration Register

Two methods exist for changing the contents of the configuration mode, each of which you will use in order to demonstrate the operation, using the following steps:

- Set the configuration register using the **configuration-register** command:

  - Enter global configuration mode on R3 using the **configure terminal** or **config t** commands
  - Change the configuration register to boot from ROM Monitor mode using the command **config-register 0x2100**
  - Exit from configuration mode using the **end** command
  - Save the configuration changes using the **write memory** or **wr mem** commands
  - Reboot the router using the command **reload** in privileged exec mode

- Notice that the router now boots into ROM Monitor Mode (notice the **rommon 1>** prompt)



```
R3(config)#config-register 0x2100
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#wr mem
Building configuration...
[OK]
R3#reload
Proceed with reload? [confirm]
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of


rommon 1 > confreg 0x2102
rommon 2 > boot
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of
```

- Set the configuration register using the **confreg** command in ROM Monitor mode:
  - There are a very narrow set of commands available in ROM Monitor mode:
    - **boot**: Instructs the router to go through the boot process
    - **confreg**: Changes the configuration register, much as the **config-register** does in normal configuration mode
    - **dir**: Lists system files
    - **help**: Invokes the help function in ROM Monitor
    - **reset**: Reset the system
    - **set**: Display or set the ROMMON system values (used for recovery from catastrophic failures)
    - **tftpdnld**: Invokes the use of TFTP to download a file (IOS image, for example) to the router, in conjunction with the **set** command
    - **unset**: Used to revert a ROMMON system value
  - Restore the default configuration register setting by using the command **confreg 0x2102** in ROMMON mode
  - Reboot the router by issuing the **boot** command
  - You will notice that the now router reboots normally

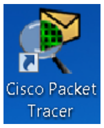
Lesson 15 Lab Exercises

Layer 2 Security

Cisco devices in general (and switches in particular), have numerous Layer 2 security features designed to combat unwanted incursions. Appropriate Use of these mechanisms can add the benefits of a secure environment to a production network. Configure these features in the lab environment as follows:

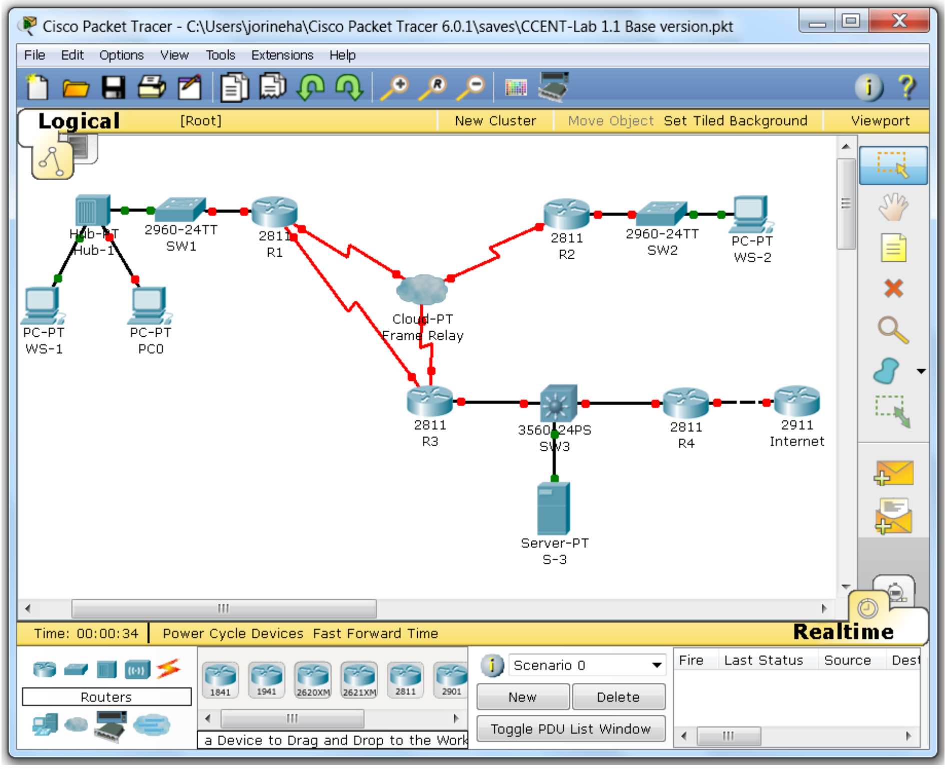
1.1.141. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



1.1.142. Select SW1 by double clicking the image

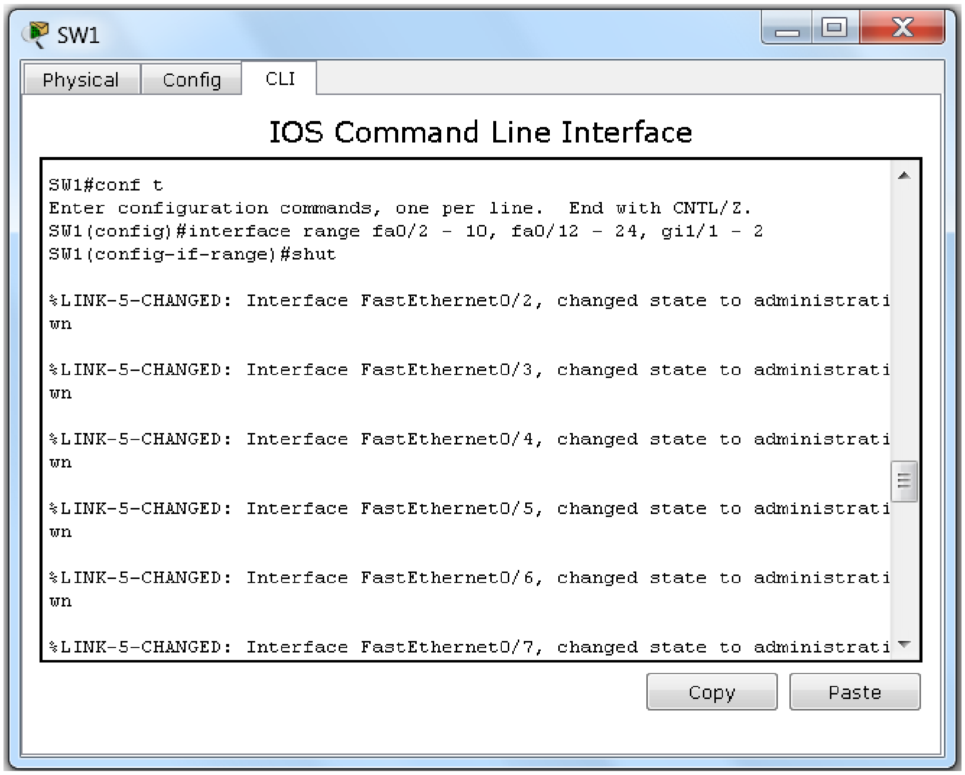
Begin by accessing SW1 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



1.1.143. Shut down unused ports on SW1

In a production environment, would-be attackers will use any potential weakness in the network as an entry point. Often, switch (and/or router) ports not in use remain active, and possibly forgotten, inadvertently leaving a security hole. Manually shut down the idle ports on SW1 using the following process:

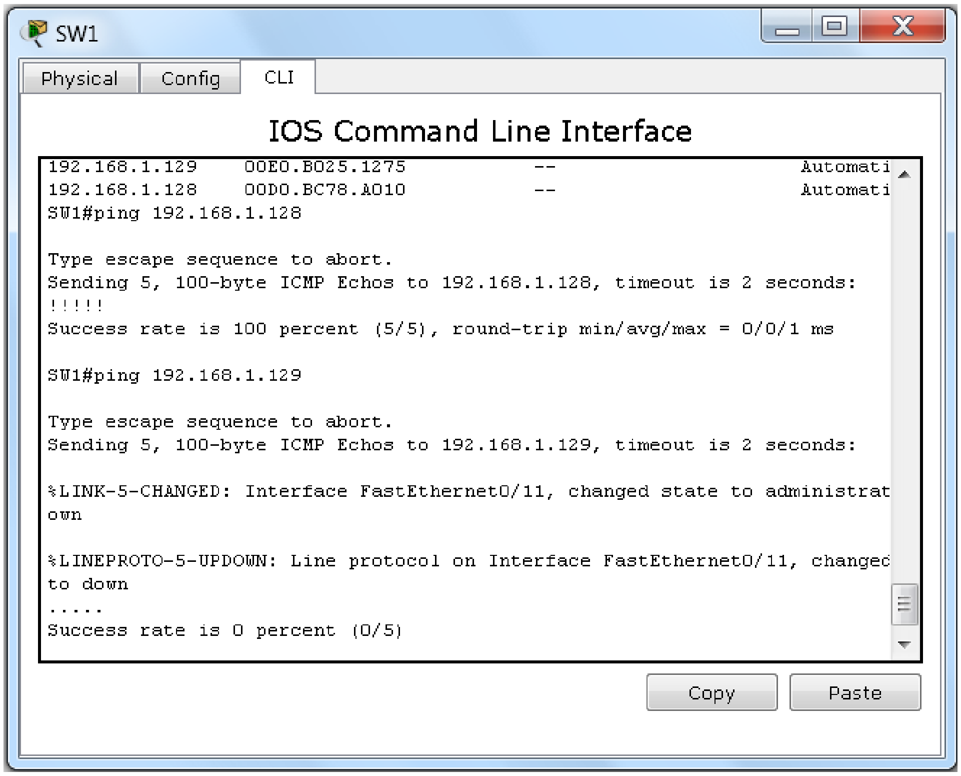
- Determine ports not in use by using the **show ip interface** brief command
  - In the output, notice that only two ports are up, ***Fa0/1*** (to R1) and **Fa0/11** (to Hub-1)
  - Inactive port ranges are ***Fa0/2 – 10***, ***Fa0/12 – 24*** and ***Gi1/1 - 2***
- Enter global configuration mode by using the **configure terminal** or **config t** commands
- Shut down each port range using the **interface range** command:
  - **interface range fa0/2 – 10, shutdown**
  - **interface range fa0/12 – 24, shutdown**
  - **interface range gi1/1 – 2, shutdown**
- Optionally, you could have used the command **interface range fa0/2 – 10, fa0/12 – 24, gi1/1 – 2** with the **shutdown** command
- If desired, shut down the unused ports on the other devices in the lab



```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface range fa0/2 - 10, fa0/12 - 24, gi1/1 - 2
SW1(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administrati
wn

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administrati
```

1.1.4. Enable port-security on SW1

Among the several Layer 2 security features available on Cisco Catalyst switches, port-security is among the simplest and easiest to implement. Use with caution, as administrators can create unintended consequences if used incorrectly. Implement Layer 2 port security on Fa0/11 of SW1 in following manner:



```
192.168.1.129    00E0.B025.1275          --                     Automati
192.168.1.128    00D0.BC78.A010          --                     Automati
SW1#ping 192.168.1.128

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.128, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW1#ping 192.168.1.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2 seconds:

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administrat
own

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changec
to down
.....
Success rate is 0 percent (0/5)
```

- Clear the current CAM (switching) table with the clear mac-address table command in privileged exec mode
- Enter global configuration mode by using the **configure terminal** or **config t** commands
- Enter interface configuration mode on Fa0/11 (connected to the hub) using the **interface fa0/11** command
- Enable Layer port-security on the interface with the command **switchport port-security**
- Specify that only ***one*** MAC address is permitted on the port by entering the command **switchport port-security maximum 1** (note that because of the hub that ***two*** MAC addresses live on that port)
- Instruct the switch to shut down the port if the policy is violated using the **switchport port-security violation shutdown** command
- Exit configuration mode by entering the **end** command
- To trigger MAC address learning on the switch, issue the following commands:

    - Display the IP addresses of the attached workstations using the **show ip dhcp binding** command (two should entries display)

- Issue a ping to the first address listed (should succeed with no issues)
- Next, issue another ping to the second address, which should attempt to learn a second MAC address on the interface
- At this point, the interface should shut down
- Issue the **show port-security** to verify that the port is in a violation/shut down mode.

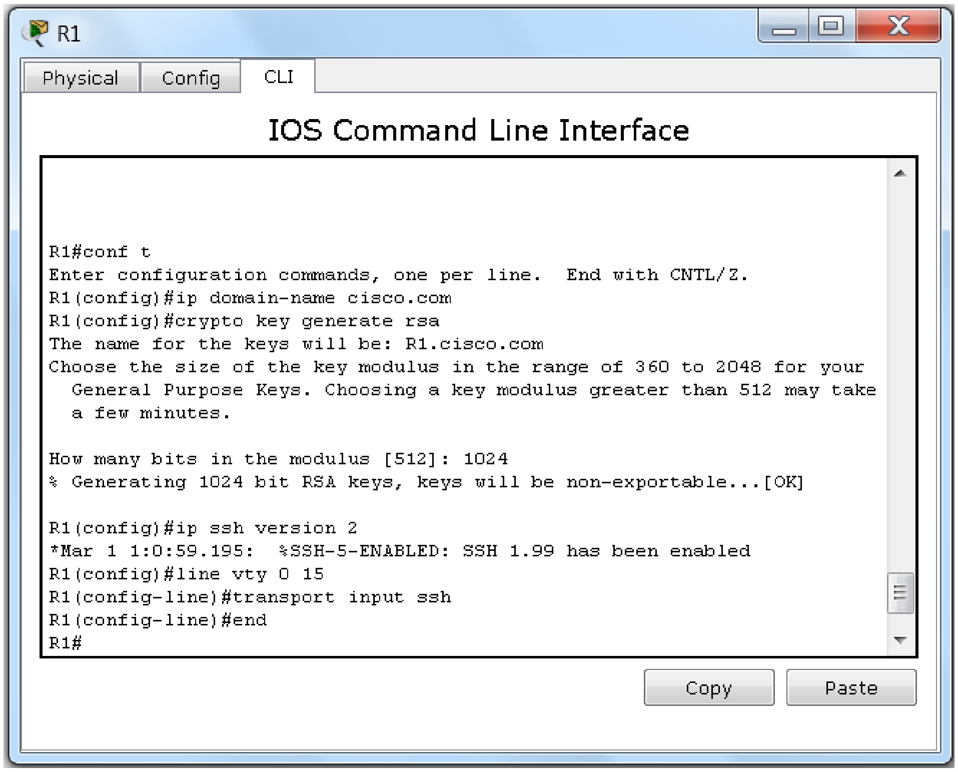
- To remove port-security, remove the port-security commands on the interface; issue a shutdown command, followed by the no shutdown command. This should restore normal operation

Layer 3 Security

While Cisco routers do not implement such features as Layer 2 port-security, they do have extensive Layer 3 security capabilities (note that switches have some of these as well). Enact Layer 3 security mechanisms on R1 using the instructions below:

1.1.5. Enable secure remote access with the secure shell (SSH) protocol

One universal skill needed by network engineers revolves around the ability remotely access devices. Telnet serves this function, but represents a security risk since it transmits all data in plain text. This could expose user accounts and passwords readily to a network attacker. Create secure access on R1 as follows:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name cisco.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#ip ssh version 2
*Mar 1 1:0:59.195:  %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
```

- Enter global configuration mode by using the **configure terminal** or **config t** commands
- Create encryption Keys (used to scramble the data according to a specific formula) using the process outlined below:

    - Assign a domain name to R1 with the command **ip domain-name cisco.com**
    - Instruct the router to generate the key by issuing the command **crypto generate rsa**. When asked for a modulus, enter the number 1024 and press **<enter>**

- Enable the ssh protocol and specify the version with the configuration command **ip ssh version 2** (R1 will signal that the protocol is activated)
- Disallow all telnet connections to R1 by configuring the virtual terminal lines to use shh exclusively as outlined here

    - Enter global configuration mode by using the **configure terminal** or **config t** commands
    - Enter terminal line configuration mode with the command **line vty 0 15**
    - Specify ssh as the only acceptable protocol by issuing the command **transport input ssh**
    - Type the **end** command to exit configuration mode
    - Save the configuration using the **write mem** or **wr mem** commands

- Test the new configuration by logging in to the command line interface of SW1 and attempting to login to R1, using these commands:

    - Initiate a telnet connection to R1 with the command **telnet 192.168.1.1**
    - R1 will refuse the connection with the message [Connection to 192.168.1.1 closed by foreign host]
    - Initiate an ssh session with the command **ssh –l cisco 192.168.1.1**
    - Enter the password ***cisco*** to authenticate
    - Exit from the session using the **exit** command

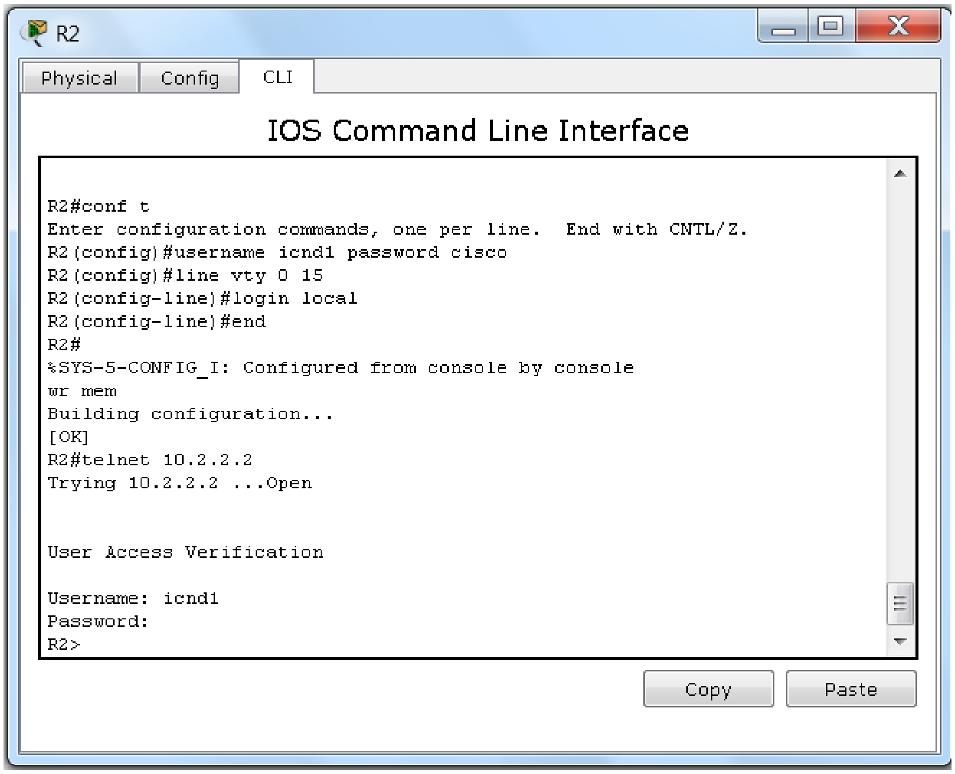
1.1.6. Configure local user authentication on R1

Utilizing access to devices using passwords is simple to implement, but a security risk if an unauthorized user learns and uses it. To combat this, most networks use an authentication process which assigns credentials to those accessing the system. Administrators can use a centralized server for this purpose, which better automates the process, though this can also be done locally on a device. Create a user-based authentication mechanism on R2 with the following configuration:

- Create an entry in the locally stored configuration database using this process:

    - Enter global configuration mode by using the **configure terminal** or **config t** commands

- Create a user with the command **username icnd1 password cisco**



```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username icnd1 password cisco
R2(config)#line vty 0 15
R2(config-line)#login local
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
wr mem
Building configuration...
[OK]
R2#telnet 10.2.2.2
Trying 10.2.2.2 ...Open


User Access Verification

Username: icnd1
Password:
R2>
```

- Instruct R2 to use the locally configured user account using these steps:
    - Enter terminal line configuration mode by typing **line vty 0 15**
    - Specify local authentication using the **login local** command
    - Exit configuration mode with the **end** command
    - Save the configuration using the **write mem** or **wr mem** commands

- Test the new configuration with the following process:
    - Use the command **telnet 10.2.2.2** (the local Loopback 0 interface, which will invoke the login process)
    - Notice that the login process has changed; instead of a password prompt, you will be asked for a username (supply the previously created credentials)
    - Log out by using the **exit** command

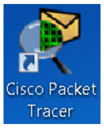
Lesson 16 Lab Exercises

Wide Area Network Configuration

When computer networks first emerged in the marketplace, they consisted of resources located in close proximity to one another (hence the term ***Local Area Network*** that you learned earlier). As the technology grew, businesses, schools, and other entities desired to link together these LANs, which gave rise to Wide Area Networks. In this set of lab exercises, you will configure two different types of WAN connections, as follows:

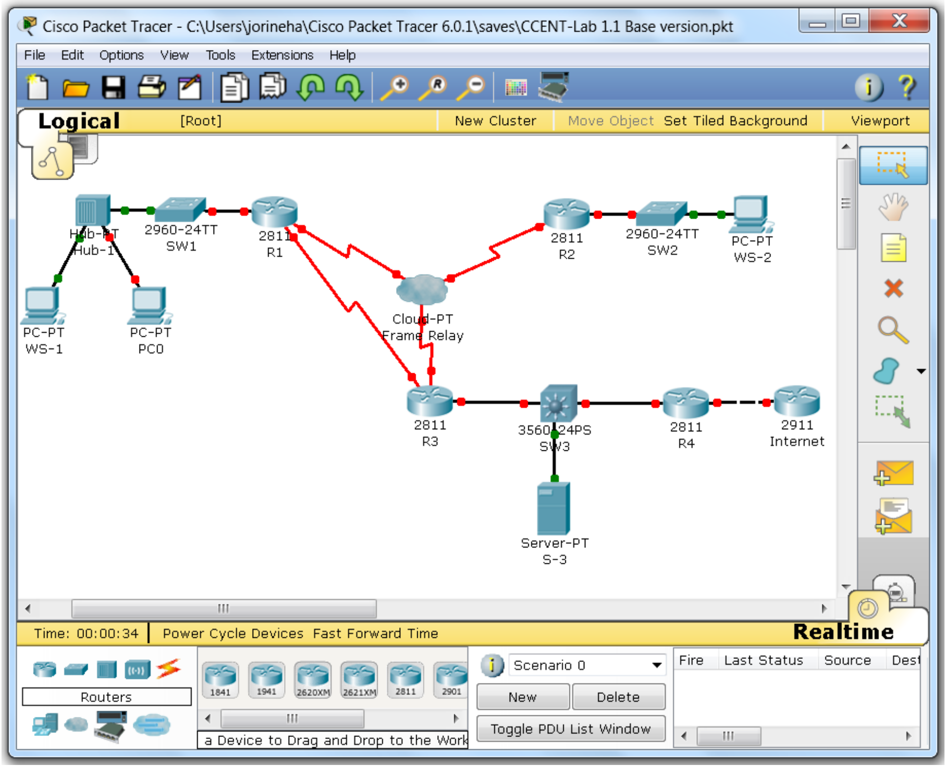
1.1.7. Launch Packet Tracer

Launch Packet Tracer from your Windows computer, either by using the Start menu, or by double-clicking the Desktop icon, as shown here:



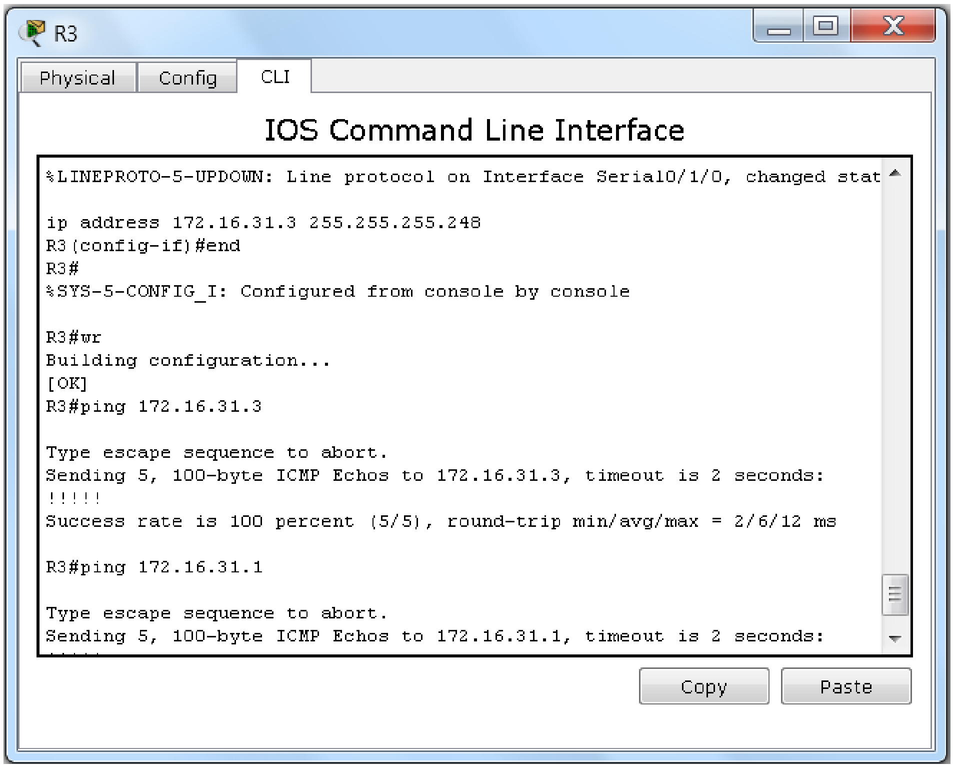
1.1.8. Select R1 by double clicking the image

Begin by accessing R1 by double clicking the image (as you have done in the previous lab exercises) to bring up the three tabbed device window and then click the CLI tab.



1.1.9. Configure a point-to-point private line connection between R1 & R3

Early network designers introduced dedicated phone lines to create connections between devices and networks remote from one another. Since these lines only connected two locations, they were named point-to-point lines, using various speeds available at the time. Create a simulated point-to-point private line connection between R1 & R3 using the following process:



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed stat

ip address 172.16.31.3 255.255.255.248
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#wr
Building configuration...
[OK]
R3#ping 172.16.31.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/6/12 ms

R3#ping 172.16.31.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.31.1, timeout is 2 seconds:
```

- Configure the serial interface of R1 with these steps:
  - Enter global configuration mode on R1 by using the **configure terminal** or **config t** commands
  - Invoke interface configuration mode on the second serial interface using the command **interface s0/1/0**
  - Enable the serial interface with the command **no shutdown** (remember that the default encapsulation type on Cisco serial interface is the High-Level Data Link Control, which is implemented in a proprietary manner)
  - You will notice that the interface does not comes from up a Layer 1 (***…is down***) standpoint, or a Layer 2 standpoint (***…line protocol is down***). Keep in mind that the interface on R3 must also be up for HDLC/Layer 2 to operate.
  - Assign an IP address to the interface using the command **ip address 172.16.31.1 255.255.255.248** (only six usable addresses designated)
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Configure the serial interface of R3 with these steps:

  - Enter global configuration mode on R1 by using the **configure terminal** or **config t** commands
  - Invoke interface configuration mode on the second serial interface using the command **interface s0/1/0**
  - Enable the serial interface with the command **no shutdown** (remember that the default encapsulation type on Cisco serial interface is the High-Level Data Link Control, which is implemented in a proprietary manner)
  - You will notice that the interface comes on Layer 1 and Layer 2, because the connection on R1 is already functional
  - Assign an IP address to the interface using the command **ip address 172.16.31.3 255.255.255.248** (only six usable addresses designated)
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Test the new connectivity between R1 and R3

  - On R3, ping the local IP address with the command **ping 172.16.31.2** (should succeed)
  - Issue a second ping to the remote side of the connection (R1) with the command **ping 172.16.31.1** (should succeed)

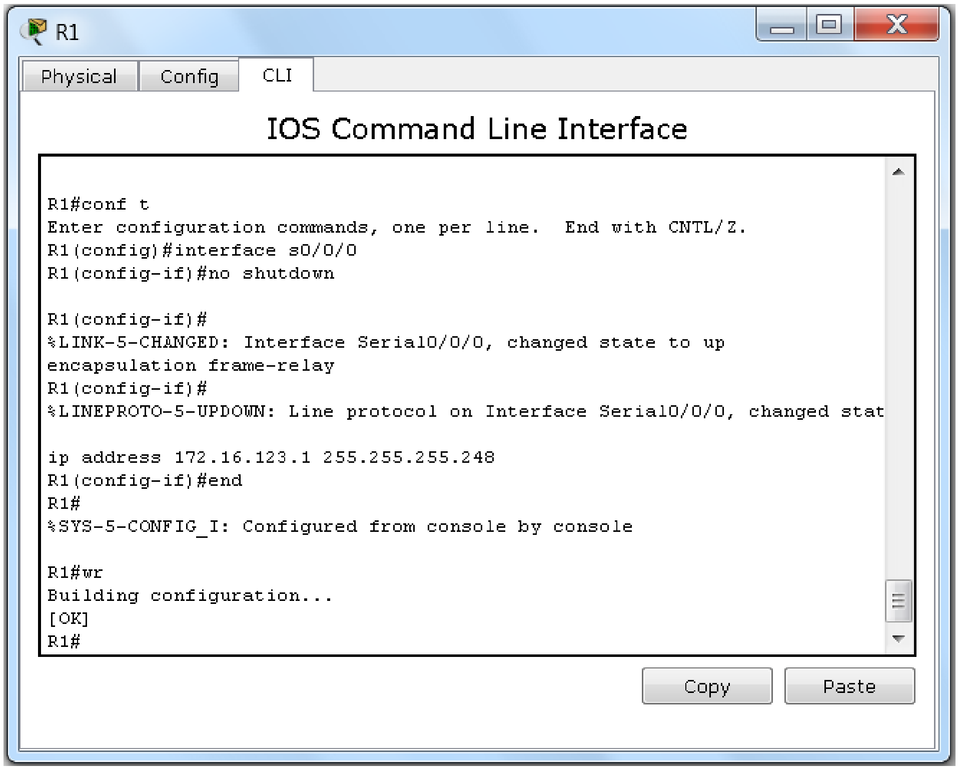
1.1.10. Configure frame-relay connections between R1, R2 & R3

Another older WAN technology that followed private line connectivity is ***frame relay***, a Layer 2 protocol that permitted a single connection from a site rather than multiple ones (which would be the case with private lines). Though superseded by Internet-based Virtual Private Networks (VPN's), frame relay continues to be an ICND1/ICND2 exam topic. Though this will receive more extensive coverage in ICND2, you will create a simple network in the lab environment, using the following guidelines:

- Configure the serial interface of R1 with these steps:

  - Enter global configuration mode on R1 by using the **configure terminal** or **config t** commands
  - Invoke interface configuration mode on the second serial interface using the command **interface s0/0/0**
  - Enable the serial interface with the command **no shutdown**
  - You will notice that the interface comes up on Layer 1 (***…is up***) but not on Layer 2 (**…line protocol is down**), because the encapsulation is still HDLC
  - Change the default encapsulation using the command **encapsulation frame-relay** (now the line protocol should come up)
  - Assign an IP address to the interface using the command **ip address 172.16.123.1 255.255.255.248** (only six usable addresses designated)
  - Exit configuration mode using the **end** command

- Save your configuration using the **write memory** (or **wr mem**) command



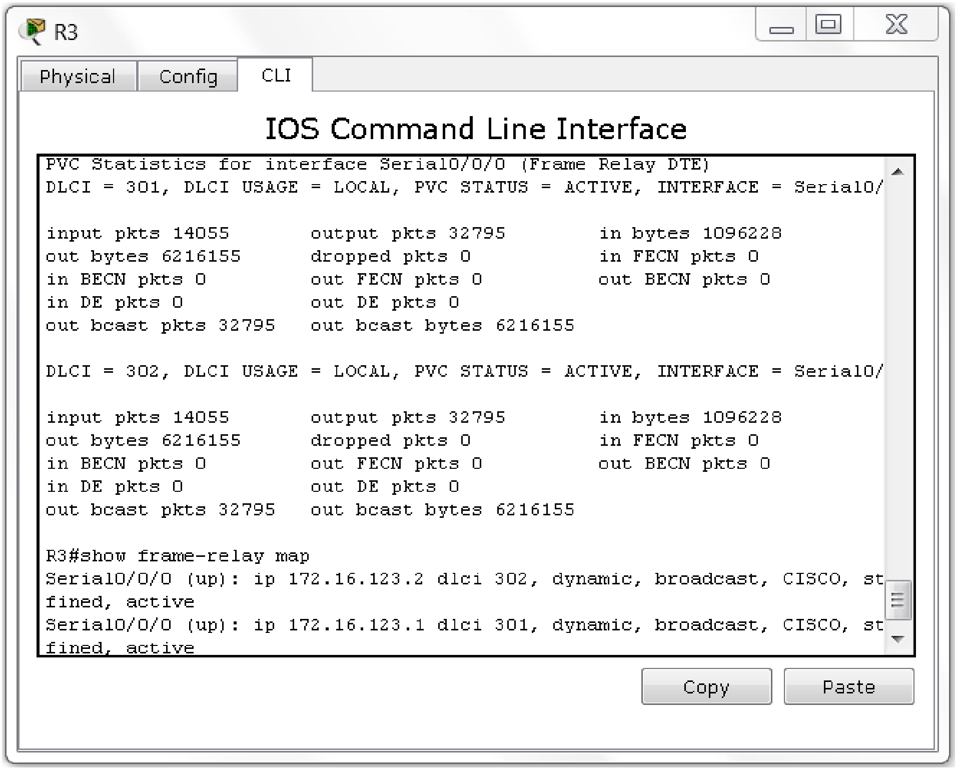
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
encapsulation frame-relay
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed stat

ip address 172.16.123.1 255.255.255.248
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
[OK]
R1#
```

- Configure the serial interface of R2 with these steps:
  - Enter global configuration mode on R2 by using the **configure terminal** or **config t** commands
  - Invoke interface configuration mode on the second serial interface using the command **interface s0/0/0**
  - Enable the serial interface with the command **no shutdown**
  - You will notice that the interface comes up on Layer 1 (***…is up***) but not on Layer 2 (**…line protocol is down**), because the encapsulation is still HDLC
  - Change the default encapsulation using the command **encapsulation frame-relay** (now the line protocol should come up)
  - Assign an IP address to the interface using the command **ip address 172.16.123.2 255.255.255.248** (only six usable addresses designated)
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Configure the serial interface of R3 with these steps:
  - Enter global configuration mode on R3 by using the **configure terminal** or **config t** commands
  - Invoke interface configuration mode on the second serial interface using the command **interface s0/0/0**

  - Enable the serial interface with the command **no shutdown**
  - You will notice that the interface comes up on Layer 1 (***…is up***) but not on Layer 2 (**…line protocol is down**), because the encapsulation is still HDLC
  - Change the default encapsulation using the command **encapsulation frame-relay** (now the line protocol should come up)
  - Assign an IP address to the interface using the command **ip address 172.16.123.3 255.255.255.248** (only six usable addresses designated)
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Test the frame-relay connection between sites using these diagnostic commands:



```
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
DLCI = 301, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/

input pkts 14055       output pkts 32795        in bytes 1096228
out bytes 6216155      dropped pkts 0           in FECN pkts 0
in BECN pkts 0         out FECN pkts 0          out BECN pkts 0
in DE pkts 0           out DE pkts 0
out bcast pkts 32795   out bcast bytes 6216155

DLCI = 302, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/

input pkts 14055       output pkts 32795        in bytes 1096228
out bytes 6216155      dropped pkts 0           in FECN pkts 0
in BECN pkts 0         out FECN pkts 0          out BECN pkts 0
in DE pkts 0           out DE pkts 0
out bcast pkts 32795   out bcast bytes 6216155

R3#show frame-relay map
Serial0/0/0 (up): ip 172.16.123.2 dlci 302, dynamic, broadcast, CISCO, st
fined, active
Serial0/0/0 (up): ip 172.16.123.1 dlci 301, dynamic, broadcast, CISCO, st
fined, active
```

  - Return to the CLI interface on R3, if not already there
  - Verify the functional status of the Permanent Virtual Circuits (PVC's, defined between all sites) with the **show frame-relay pvc** command
  - You should see the message PVC STATUS = ACTIVE for both
  - Verify that frame-relay inverse ARP is functioning using the **show frame-relay map command**
  - Frame-relay inverse ARP maps Layer 2 addresses (in this base, the Data Link Connection Identifier) to IP addresses, in a way similar to ARP between Ethernet MAC and IP addresses

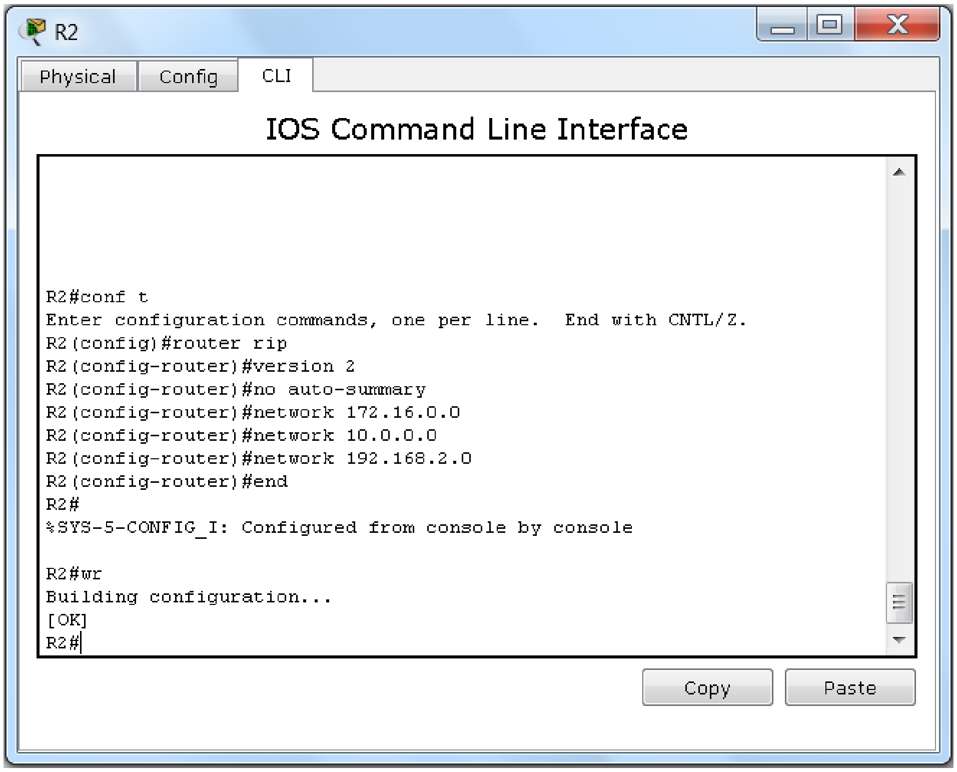
  - Ping the other addresses listed in the map command using the commands **ping 172.16.123.1** and **ping 172.16.123.2** commands (these should succeed)

1.1.11. Enable RIPV2 routing on the WAN links between R1, R2 & R3

In the IP routing lab, you enabled the RIP (version 2) routing process between R3 & R4; now you will expand this to include R1 & R2, along with the new WAN links previously created. Complete IP routing configuration as follows:

- Complete the remainder of RIP routing on R3 as follows:
  - Enter global configuration mode on R3 by using the **configure terminal** or **config t** commands
  - Enter RIP configuration mode using the command **router rip**
  - Add both WAN interfaces to the process by entering the command **network 172.16.0.0** (this is the major network/Class B address that both S0/0/0 and S0/1/0 both use)
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Configure RIP V2 routing on R2 using these steps:



```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 172.16.0.0
R2(config-router)#network 10.0.0.0
R2(config-router)#network 192.168.2.0
R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr
Building configuration...
[OK]
R2#
```

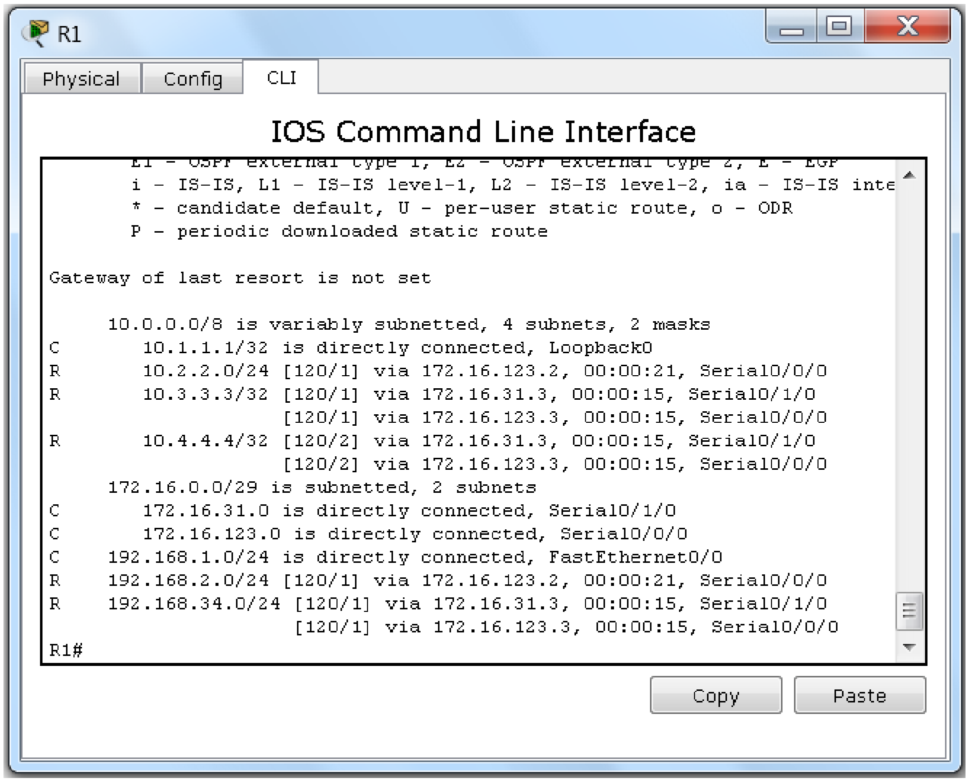
  - Enter global configuration mode on R2 by using the **configure terminal** or **config t** commands

  - Enter RIP configuration mode using the command **router rip**
  - Set the RIP version to 2 with the command **version 2**
  - Disable automatic summarization with the command **no auto-summary**
  - Add both WAN interfaces to the process by entering the command **network 172.16.0.0** (this is the major network/Class B address that S0/0/0 uses)
  - Add the remaining interfaces to the process with the commands **network 10.0.0.0** and **network 192.168.2.0**
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Configure RIP V2 routing on R1 using these steps:

  - Enter global configuration mode on R1 by using the **configure terminal** or **config t** commands
  - Enter RIP configuration mode using the command **router rip**
  - Set the RIP version to 2 with the command **version 2**
  - Disable summarization using the command **no auto-summary**
  - Add both WAN interfaces to the process by entering the command **network 172.16.0.0** (this is the major network/Class B address that both S0/0/0 and S0/1/0 use)
  - Add the remaining interfaces to the process with the commands **network 10.0.0.0** and **network 192.168.1.0**
  - Exit configuration mode using the **end** command
  - Save your configuration using the **write memory** (or **wr mem**) command

- Verify RIP routing on R1 with these instructions:



```
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
R       10.2.2.0/24 [120/1] via 172.16.123.2, 00:00:21, Serial0/0/0
R       10.3.3.3/32 [120/1] via 172.16.31.3, 00:00:15, Serial0/1/0
                    [120/1] via 172.16.123.3, 00:00:15, Serial0/0/0
R       10.4.4.4/32 [120/2] via 172.16.31.3, 00:00:15, Serial0/1/0
                    [120/2] via 172.16.123.3, 00:00:15, Serial0/0/0
     172.16.0.0/29 is subnetted, 2 subnets
C       172.16.31.0 is directly connected, Serial0/1/0
C       172.16.123.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 172.16.123.2, 00:00:21, Serial0/0/0
R    192.168.34.0/24 [120/1] via 172.16.31.3, 00:00:15, Serial0/1/0
                     [120/1] via 172.16.123.3, 00:00:15, Serial0/0/0
R1#
```

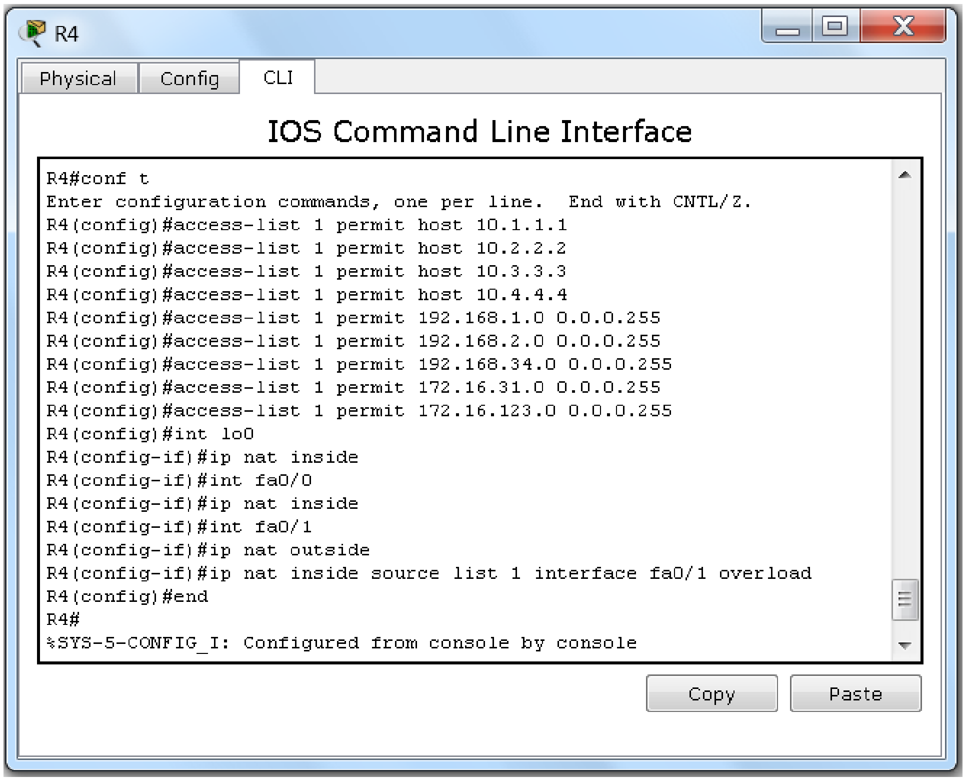
- First, verify that RIP is operating by issuing the command **show ip protocols** (this should generate about a page of output)
- Verify that the following addresses appear as gateways: ***172.16.123.2, 172.16.123.3, 172.16.31.3***
- Display the IP routing table using the **show ip route** command (should be nearly identical to what is displayed above

Network Address Translation Configuration

As the Internet experienced rapid growth, the number of publicly routable IP address began to deplete, giving rise to conservation mechanisms. Two of the major techniques introduced were the creation of private address ranges (RFC 1918) and Network Address Translation (NAT, which translates private address to one or more public addresses). In this lab, you will configure Port Address Translation (the translation of many private addresses to a single external address) on R4, for connection to the Internet. Create this process using the following steps:

1.1.12. Define the addresses to translate using access control lists

In order for NAT to function, the router needs to know what addresses it needs to perform translation on. Access lists (sometimes called access control lists) can identify ranges of addresses, in this case based on source addresses (these are called ***standard access-lists***). Configure this on R4 as follows:



```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#access-list 1 permit host 10.1.1.1
R4(config)#access-list 1 permit host 10.2.2.2
R4(config)#access-list 1 permit host 10.3.3.3
R4(config)#access-list 1 permit host 10.4.4.4
R4(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R4(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R4(config)#access-list 1 permit 192.168.34.0 0.0.0.255
R4(config)#access-list 1 permit 172.16.31.0 0.0.0.255
R4(config)#access-list 1 permit 172.16.123.0 0.0.0.255
R4(config)#int lo0
R4(config-if)#ip nat inside
R4(config-if)#int fa0/0
R4(config-if)#ip nat inside
R4(config-if)#int fa0/1
R4(config-if)#ip nat outside
R4(config-if)#ip nat inside source list 1 interface fa0/1 overload
R4(config)#end
R4#
%SYS-5-CONFIG_I: Configured from console by console
```

- **access-list 1 permit host 10.1.1.1** (identical to 10.1.1.1 255.255.255.255; specifies an exact binary match. Masks for access lists as inverse and called ***wildcards masks***. You get the wildcard mask by subtracting 255 from each octet, which would yield the mask 0.0.0.0 in this case)
- **access-list 1 permit host 10.2.2.2** (Loopback 0 address of R2)
- **access-list 1 permit host 10.3.3.3** (Loopback 0 address of R3)
- **access-list 1 permit host 10.4.4.4** (Loopback 0 address of R4)
- **access-list 1 permit 192.168.1.0 0.0.0.255** (LAN Interface of R1)
- **access-list 1 permit 192.168.2.0 0.0.0.255** (LAN Interface of R2)
- **access-list 1 permit 192.168.34.0 0.0.0.255** (LAN Interface of R3 & R4)
- **access-list 1 permit 172.16.31.0 0.0.0.255** (WAN Private Line between R1 & R3)

1.1.13. Identify the interfaces used in the NAT Process

NAT also has to understand which interfaces contain the private addresses (or addresses to translate **from**; these addresses were identified in the access-list) Configure this on R4 as follows:

- **Inside Interfaces:** These interfaces contain the addresses that will be translated. In some cases these addresses may be on devices farther inside the network. The command to enable this is **ip nat inside**. Use this commands on these interfaces:

  - Loopback 0
  - Fa0/0

- **Outside Interface:** These interfaces contain one or more global addresses that the addresses are translated ***to***. The command to enable this is **ip nat outside**. Use this on interface Fa0/1

1.1.14. Specify the NAT inside-to-outside mapping

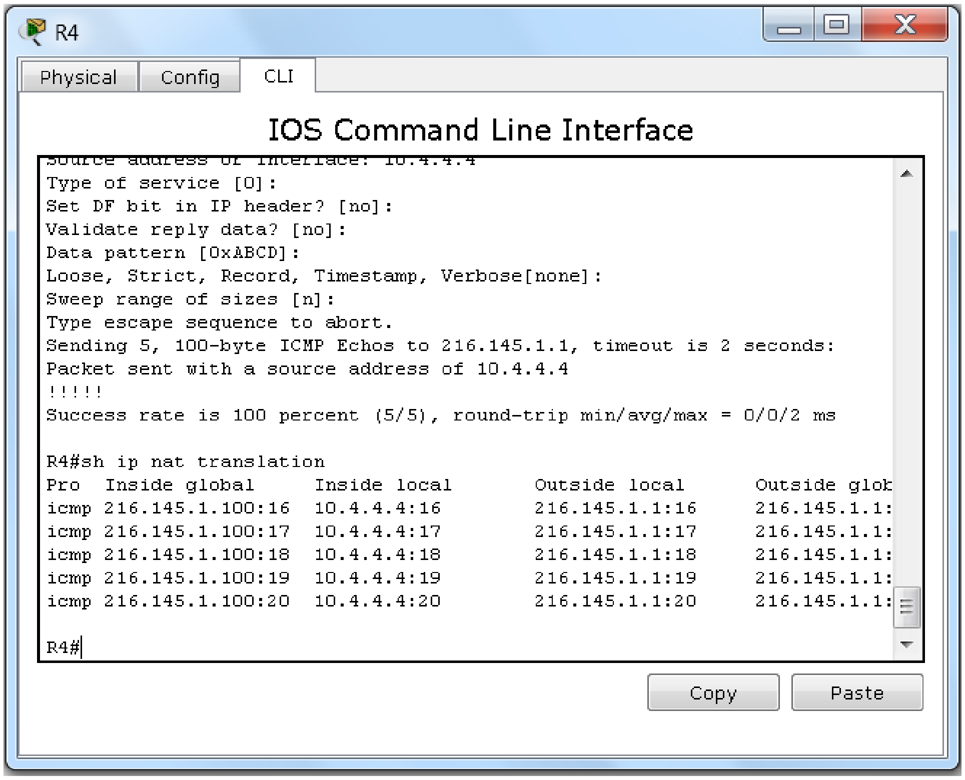
The final step to configuring NAT/PAT on a Cisco router involves mapping the source addresses from the access-list to outside address(es) or interface(s). Configure this on R4 in global configuration mode using the command **ip nat inside source list 1 interface Fa0/1 overload**. The meaning of the individual statements is decoded here:

- **ip nat inside source:** Indicates that the translation process begins with the addresses on the inside of the network (identified in the access-list)
- **list 1**: Indicates that the addresses to be translated are contained in standard access list 1 (standard access-lists uses the numerical identifiers 1-99, though they can be created by name as well). Another **source** keyword (**static**) ties address/port translation in a fixed manner to a single address/port

- **interface Fa0/1**: Specifies that the IP address on the outside interface (in this case/ Fa0/1) will serve as the translation point. A pool of addresses can be used instead of the interface by using the **pool** keyword
- **overload**: Specifies that the single IP address of the outside interface will be used in the translation process, and that Port Address Translation will take place

1.1.15. Test the NAT/PAT configuration using an extended ping

To ensure that the NAT process is working correctly, you need to generate traffic from one of the inside addresses to an outside address. Creating traffic sourced from another device inside the network (R1, R2, R3, etc.) can work, but for the sake of simplicity, you will use R4. Create the traffic as follows:



```
Source address or interface: 10.4.4.4
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.145.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.4.4.4
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

R4#sh ip nat translation
Pro  Inside global     Inside local       Outside local      Outside glob
icmp 216.145.1.100:16  10.4.4.4:16        216.145.1.1:16     216.145.1.1:
icmp 216.145.1.100:17  10.4.4.4:17        216.145.1.1:17     216.145.1.1:
icmp 216.145.1.100:18  10.4.4.4:18        216.145.1.1:18     216.145.1.1:
icmp 216.145.1.100:19  10.4.4.4:19        216.145.1.1:19     216.145.1.1:
icmp 216.145.1.100:20  10.4.4.4:20        216.145.1.1:20     216.145.1.1:

R4#
```

- In privileged exec mode, create an extended ping with the **ping** command, using the following options:

  - **Protocol**: IP
  - **Target IP address**: 216.145.1.1
  - **Repeat count**: 5
  - **Datagram size**: 100
  - **Timeout in seconds**: 2
  - **Extended commands**: Yes
  - **Source address or interface**: 10.4.4.4
  - **Type of service**: 0
  - **Set DF bit in header**: No

  - **Validate reply data**: No
  - **Data pattern**: 0xABCD
  - **Loose, strict, record, timestamp, verbose**: None
  - **Sweep range of sizes**: No

- Verify translation using the **show ip nat translations** command, yielding output similar to the illustration above

Final Device Configurations

Final Router Configurations

Once you have completed all of the lab exercises in this document, you may view your own router configurations and compare those to the master configurations here:

1.1.16. R1

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname R1

enable secret cisco

ip ssh version 2
ip domain-name cisco.com

spanning-tree mode pvst

interface Loopback0
 ip address 10.1.1.1 255.255.255.255

interface FastEthernet0/0
 description LAN Interface
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown

interface Serial0/0/0
 ip address 172.16.123.1 255.255.255.248
 encapsulation frame-relay

interface Serial0/1/0
 ip address 172.16.31.1 255.255.255.248

interface Vlan1
 no ip address
 shutdown
```

```
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.1.0
 no auto-summary

ip classless

line con 0
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 password cisco
 login
 transport input ssh
line vty 5 15
 password cisco
 login
 transport input ssh

end
```

1.1.17. R2

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname R2

enable secret cisco

username icnd1 password 0 cisco

ip ssh version 2

spanning-tree mode pvst

interface Loopback0
 ip address 10.2.2.2 255.255.255.0
```

```
interface FastEthernet0/0
 description LAN
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown

interface Serial0/0/0
 ip address 172.16.123.2 255.255.255.248
 encapsulation frame-relay

interface Serial0/1/0
 no ip address
 shutdown

interface Vlan1
 no ip address
 shutdown

router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 no auto-summary

ip classless

no run

line con 0
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 password cisco
 login local
 transport input telnet
line vty 5 15
 password cisco
 login local
 transport input telnet

end
```

1.1.18. R3

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname R3

enable secret cisco

spanning-tree mode pvst

interface Loopback0
 ip address 10.3.3.3 255.255.255.255

interface FastEthernet0/0
 description LAN
 ip address 192.168.34.3 255.255.255.0
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown

interface Serial0/0/0
 ip address 172.16.123.3 255.255.255.248
 encapsulation frame-relay

interface Serial0/1/0
 ip address 172.16.31.3 255.255.255.248

interface Vlan1
 no ip address
 shutdown

router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.34.0
 no auto-summary

ip classless

line con 0
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 password cisco
 login
 transport input telnet
line vty 5 15
 password cisco
 login
 transport input telnet

end
```

1.1.19. R4

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname R4

enable secret cisco

spanning-tree mode pvst

interface Loopback0
 ip address 10.4.4.4 255.255.255.255
 ip nat inside

interface FastEthernet0/0
 description LAN
 ip address 192.168.34.4 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
```

```
interface FastEthernet0/1
 ip address 216.145.1.100 255.255.255.0
 ip nat outside
 duplex auto
 speed auto

interface Vlan1
 no ip address
 shutdown

router rip
 version 2
 network 10.0.0.0
 network 192.168.34.0
 no auto-summary

ip nat inside source list 1 interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 216.145.1.1

access-list 1 permit host 10.1.1.1
access-list 1 permit host 10.2.2.2
access-list 1 permit host 10.3.3.3
access-list 1 permit host 10.4.4.4
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 172.16.31.0 0.0.0.255
access-list 1 permit 172.16.123.0 0.0.0.255

line con 0
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 password cisco
 login
 transport input telnet
line vty 5 15
 password cisco
 login
 transport input telnet

end
```

1.1.20. Internet Router

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname Internet

license udi pid CISCO2911/K9 sn FTX1524USNH

spanning-tree mode pvst

interface Loopback0
 ip address 12.0.0.1 255.0.0.0

interface Loopback1
 ip address 124.0.0.1 255.0.0.0

interface Loopback2
 ip address 24.0.0.1 255.0.0.0

interface Loopback3
 ip address 35.0.0.1 255.0.0.0

interface Loopback4
 ip address 135.12.0.1 255.255.0.0

interface GigabitEthernet0/0
 ip address 216.145.1.1 255.255.255.0
 duplex auto
 speed auto

interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown

interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown

interface Vlan1
 no ip address
 shutdown
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 216.145.1.100

line con 0

line aux 0

line vty 0 4
 login

end
```

Final Switch Configurations

Once you have completed all of the lab exercises in this document, you may view your own switch configurations and compare those to the master configurations here:

1.1.21. SW1

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW1

enable secret cisco

spanning-tree mode pvst

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
shutdown

interface FastEthernet0/3
shutdown

interface FastEthernet0/4
shutdown

interface FastEthernet0/5
shutdown

interface FastEthernet0/6
shutdown
```

```
interface FastEthernet0/7
shutdown

interface FastEthernet0/8
shutdown

interface FastEthernet0/9
shutdown

interface FastEthernet0/10
shutdown

interface FastEthernet0/11
 switchport access vlan 11
 switchport mode access
 switchport port-security

interface FastEthernet0/12
shutdown

interface FastEthernet0/13
shutdown

interface FastEthernet0/14
shutdown

interface FastEthernet0/15
shutdown

interface FastEthernet0/16
shutdown

interface FastEthernet0/17
shutdown

interface FastEthernet0/18
shutdown

interface FastEthernet0/19
shutdown

interface FastEthernet0/20
shutdown

interface FastEthernet0/21
shutdown
```

```
interface FastEthernet0/22
shutdown

interface FastEthernet0/23
shutdown

interface FastEthernet0/24
shutdown

interface GigabitEthernet1/1
shutdown

interface GigabitEthernet1/2
shutdown

interface Vlan1
 ip address 192.168.1.2 255.255.255.248

ip default-gateway 192.168.1.1

line con 0
 password cisco
 privilege level 15

line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login

end
```

1.1.22. SW2

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW2

enable secret cisco

spanning-tree mode pvst
```

```
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1
 ip address 192.168.2.111 255.255.255.0

ip default-gateway 192.168.2.2

line con 0
 password cisco
 privilege level 15

line vty 0 4
 password cisco
 login
 transport input telnet
line vty 5 15
 password cisco
 login
 transport input telnet

end
```

1.1.23. SW3

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption

hostname SW3

enable secret cisco

spanning-tree mode pvst

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5
interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface Vlan1
 ip address 192.168.34.111 255.255.255.0

ip classless

line con 0
```

```
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 password cisco
 login
 transport input telnet
 privilege level 15
line vty 5 15
 password cisco
 login
 transport input telnet

end
```