GraceStone
Professionals

ICND2 Lab Exercises

Lesson Companion

Joe Rinehart

MBA, CCIE #14256

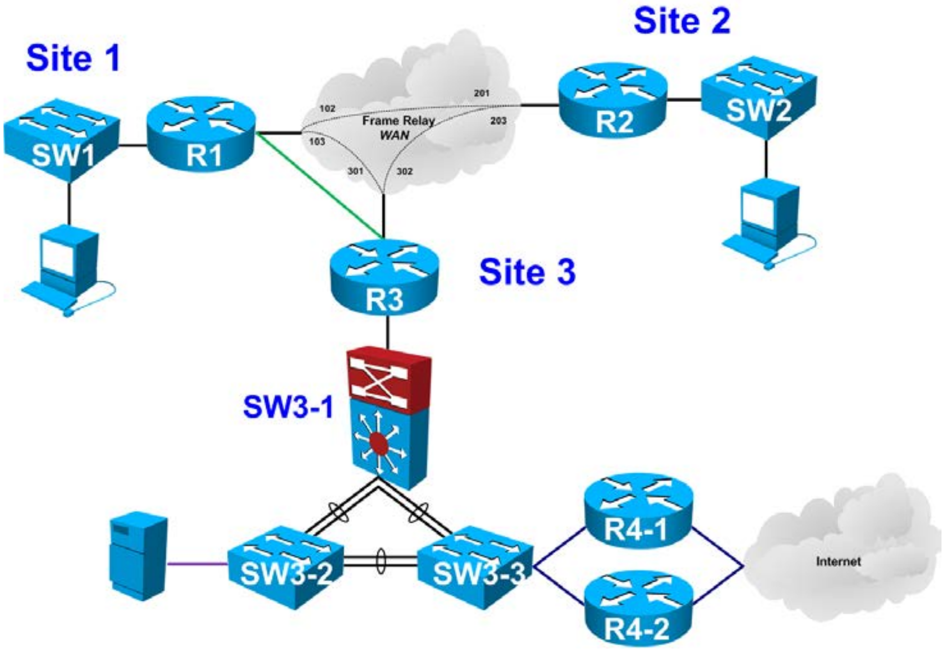
CCNP/DP/VP

October 11, 2014

Table of Contents

Introduction

The Overall Topology



The CCNA/ICND2 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:

- Five (3) Cisco 2900 class routers
- Two (2) Cisco 2800 class routers
- Five (5) Cisco Catalyst switches
- Two (2) computer workstations
- One (1) server
- Wide Area Network connectivity
- Simulated Internet connection

Purpose of the Lab Project

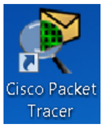
A thorough understanding of networking concepts is the foundation upon which understanding is essentially built. While theoretical knowledge is important, the application of that knowledge is equally important, and forms the basis for effective performance in real-world environments. Early versions of 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, CCNA R&S students need practical, experience-based exercises.

1.1 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.

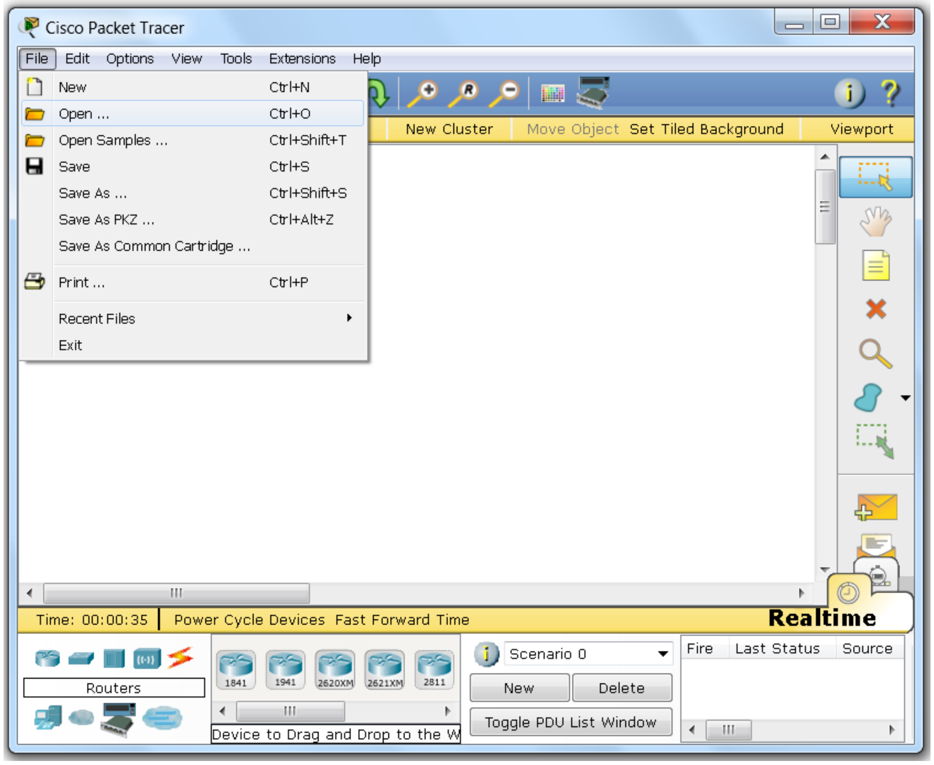
1.1.1. Launch Packet Tracer

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

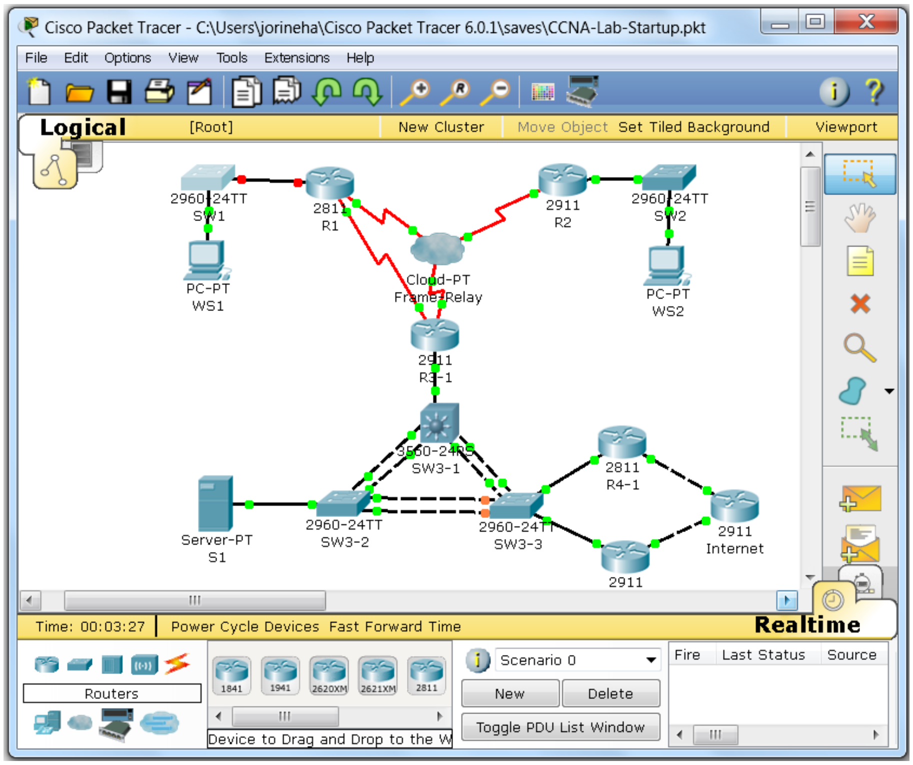


1.1.2. Load the Basic Lab Topology

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



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



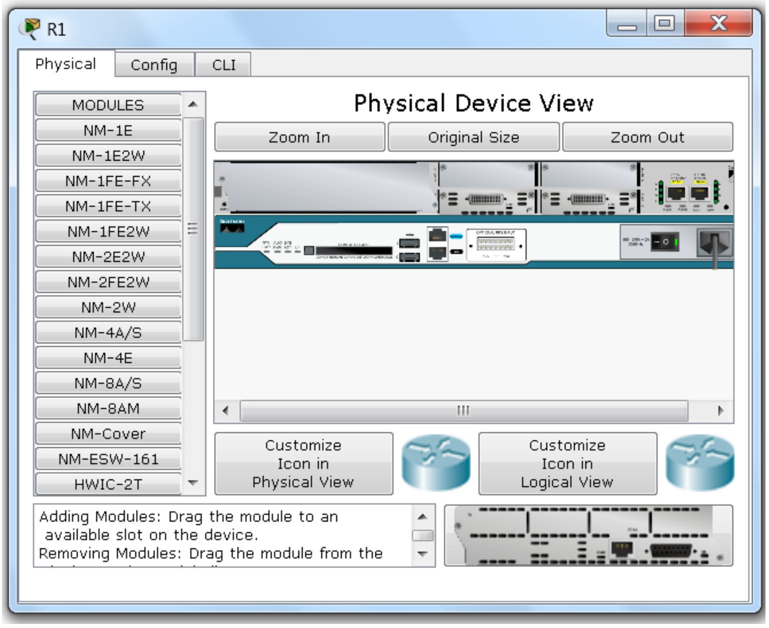
1.1.3. Getting Familiar with the User Interface

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

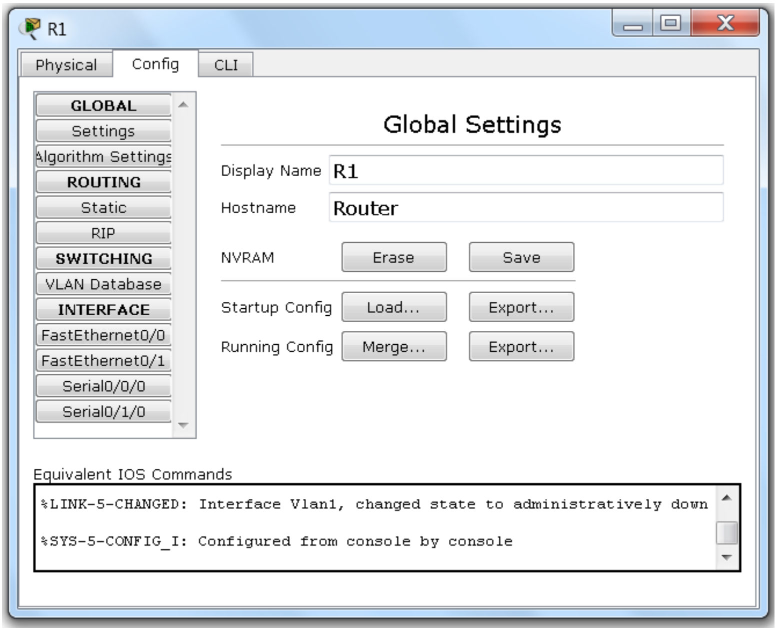
- **Interacting with devices**: As part of the lessons, you will perform various configuration and verification tasks that require you to log into the devices directly. The simplest and easiest way to do that is to double click the image of the device you want to access, and the following window will 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



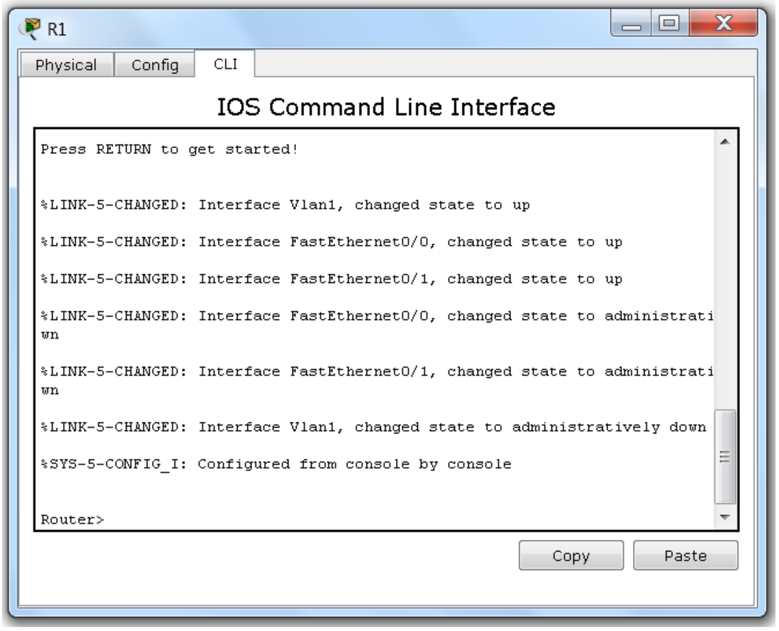
Display Name R1

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>
```

Initial configurations have already been loaded to eliminate unnecessary tasks (enable password, line/vty configurations, ssh, etc.)

**** NOTE that the topology referenced in the videos of the lessons is different due to changes that were made to the CCNA 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. ****

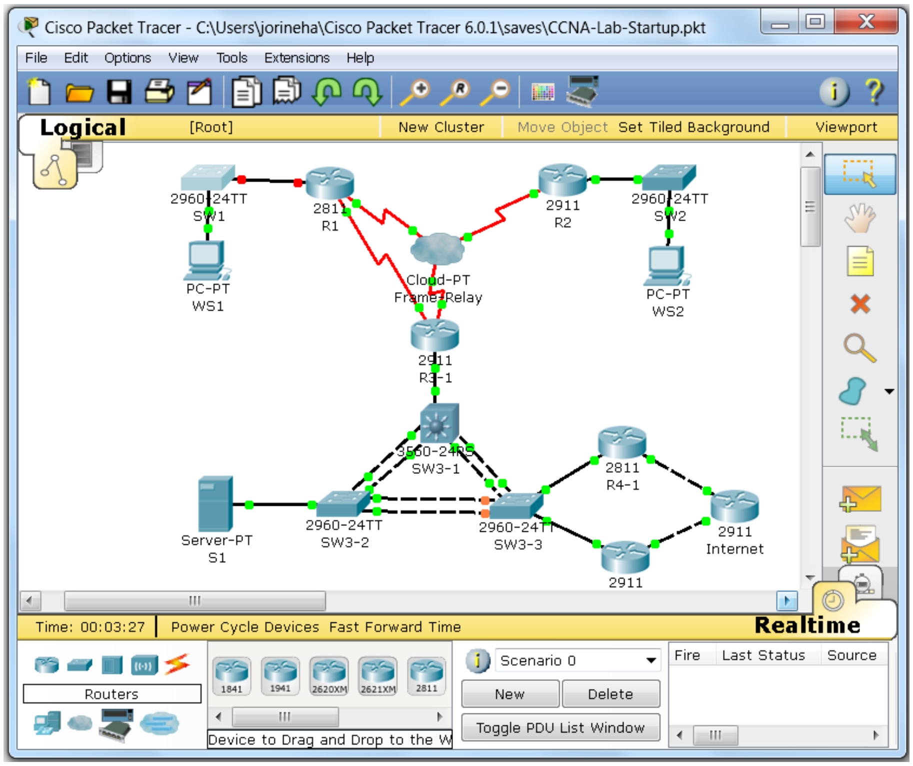
Lesson 1 Lab Exercises

2.1 VLAN Configuration Exercises

When Local Area Networks (LANs) first came into mainstream use, end-users gained the ability to share resources (file sharing, printers, the Internet, etc.), but rapid growth of the technology created performance issues. In order to contain network traffic (including broadcasts), network designers introduced ***Virtual LANs***, or ***VLANs***. Each VLAN created distinct broadcast domains and enabled the partitioning of groups of users. The purpose of this lab exercise is to familiarize you with the various technical tasks regarding VLANs.

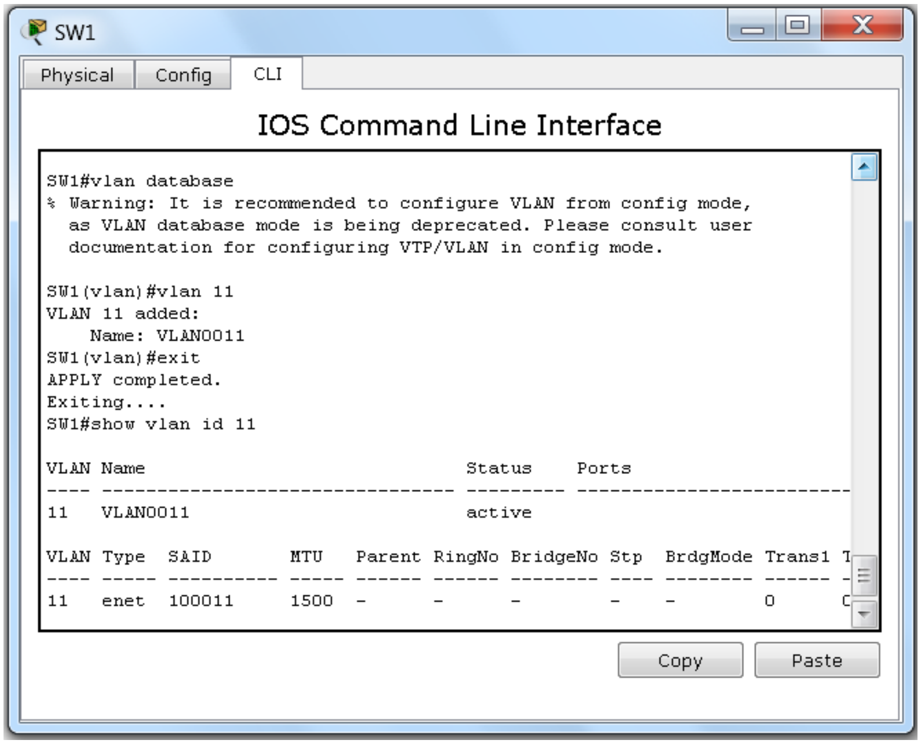
2.1.1. Configure VLANs on SW1 (Site 1)

In this lab topology, you may have noticed the presence of three distinct sites, each with various devices. Site 1 and Site 2 are nearly identical, with Site 3 appearing more complex. In this segment of the lab, you will configure two VLANs on SW1. To begin, simply double click the image of SW1 to bring up the three tabbed device window and then click the CLI tab.



- **VLAN Database Method**: One of the older methods of configuring VLANs on a switch involved a specialized CLI configuration mode called

vlan database mode. To configure a VLAN using this method, perform the following steps:



```
SW1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW1(vlan)#vlan 11
VLAN 11 added:
    Name: VLAN0011
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#show vlan id 11

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
11   VLAN0011                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 T
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -
11   enet  100011     1500  -      -      -        -    -        0      0
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Enter vlan database mode**: To create a new VLAN on SW1, type the command **vlan database** directly into the command line. Note: Do not enter global configuration mode. Ignore the warning about vlan database method being deprecated
- **Create a VLAN:** Create a VLAN with the ID of 11 using the **vlan 11** command
- **Exit VLAN database mode**: Enter the **exit** command to return to privileged exec mode
- **Verify VLAN**: Type the command **show vlan id 11** to verify that you created the VLAN successfully. Another fact to be aware of is that a ***default VLAN*** (VLAN 1) exists on every switch and cannot be modified or deleted. You will be utilizing both VLAN 1 and VLAN 11 during these lab exercises

- **Configure a VLAN interface**: On Cisco switches, a VLAN can have a Layer 3 interface, which is referred to as a VLAN interface or switch virtual interface (SVI). On Layer 2 switches, only one SVI may remain active at a time; Layer 3 switches do not have this limitation. On SW1, enter SVI configuration mode and assign addressing as follows:

    - **Enter VLAN configuration mode**: Enter SVI configuration mode with the command **interface vlan 1** (the prompt will change to ***config-if***)
    - **Enable the interface**: Since the VLAN 1 SVI is administratively down by default, enable the interface using the **no shutdown** command
    - **Add Description**: Identify the interface as reserved for management with the designation **description MANAGEMENT VLAN**
    - **Configure IPV4 addressing**: Enter the command **ip address 192.168.1.111 255.255.255.0**

- **Default gateway**: Set the default gateway using the command **ip default-gateway 192.168.1.1**
- **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 or 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.

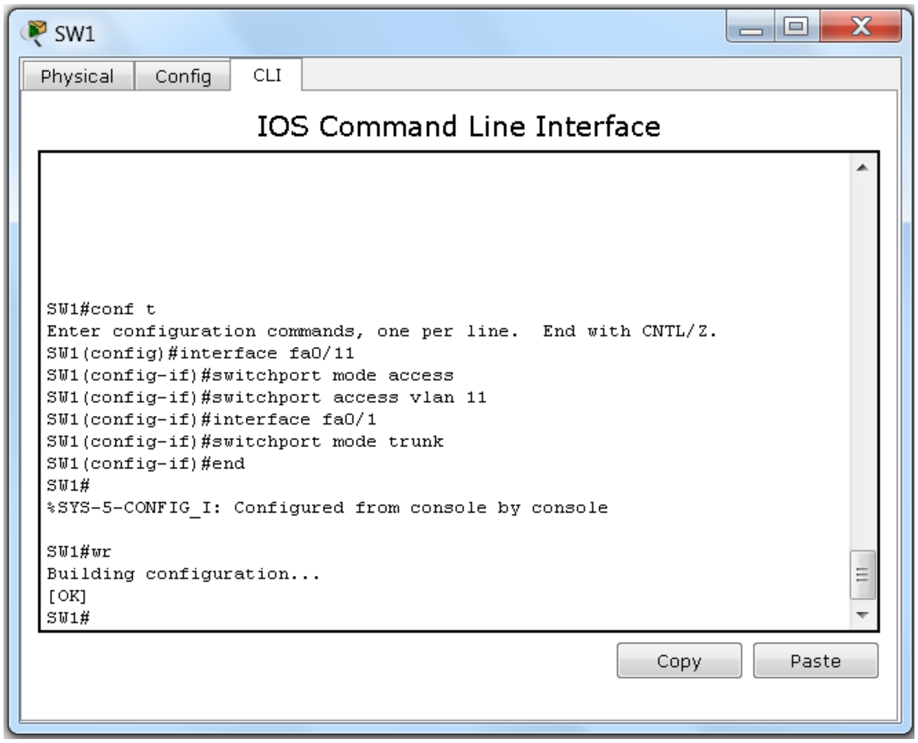
2.1.2. Configure Switch Ports on SW1

When a Cisco Layer 2 switch powers up, it will typically load a default configuration, in which certain basic values are assumed and placed on the device. To complicate matters, default configurations do not usually show up when using the **show running-configuration** or **show startup-configuration** commands. Switch interfaces, for example, have a default configuration as well, though the following are all of the possible port modes, using the **switchport** command in interface configuration mode:

- **switchport mode access**: Access mode only allows the Layer 2 port to participate in one VLAN at a time. Access ports typically host end-devices such as workstations, servers, IP phones, etc.
- **switchport mode trunk**: Trunk mode allows multiple VLANS to traverse the Layer 2 port, usually to connect to another switch or router.

- **Switchport mode dynamic:** Dynamic mode will cause the Layer 2 port to enter into a negotiation process to determine whether it will act as an access port or a trunk port. Switch ports exchange ***Dynamic Trunk Protocol (DTP)*** frames to make this determination. Two options accompany the **dynamic** command:

    - **Auto:** Does not send out DTP frames actively, but will form a trunk port if the port on the other side of the connection is set to ***desirable*** mode (see below). ***This is the default port configuration on Layer 2 switches***
    - **Desirable**: Sends out DTP frames actively in order to form a trunk port. If the port on the other side is set to either ***desirable*** or ***auto***, the port will create a trunk



```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface fa0/11
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 11
SW1(config-if)#interface fa0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#end
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#wr
Building configuration...
[OK]
SW1#
```

- **Configure Access Ports**: WS1 sits on the Production VLAN (VLAN 11) on Fa0/11 and will only need access to that single VLAN. Configure an access port as follows:
    - **Set port Fa0/11 to access mode**: Use the command **switchport mode access**
    - **Assign the port to VLAN 11**: By default, all ports get assigned to VLAN 1 (the default VLAN), so change the VLAN assignment with the **switchport access vlan 11** command

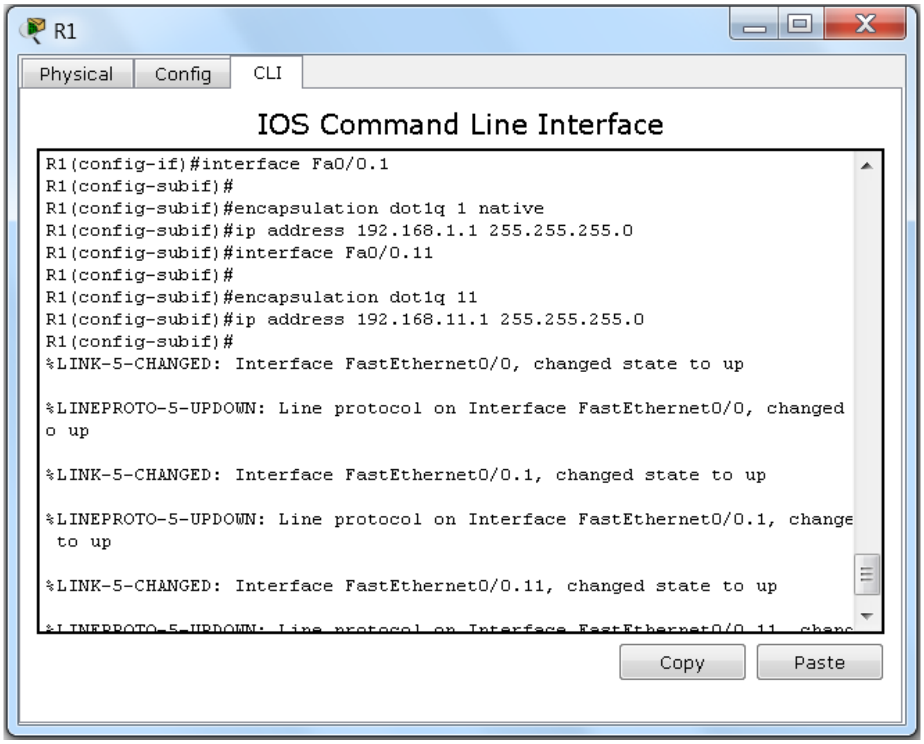
- **Configure Trunk Ports:** R1 will host interfaces for both VLAN 1 and VLAN 11. Set Fa0/1 to trunk unconditionally (no negotiation) using the

switchport mode trunk command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command).

- **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 or 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.

2.1.3. Configure Trunking and InterVLAN Routing on R1 (Site 1)

Unlike switch ports, router LAN ports operate in Layer 3 mode by default; a router does not understand or participate in VLANs/trunks natively, and thus requires additional configuration. A router can attach to a switch port set to access mode, but to perform trunking additional configuration is required. Configure the Fa0/0 interface (attached to trunk port Fa0/1 on SW1) for trunking using the following process:



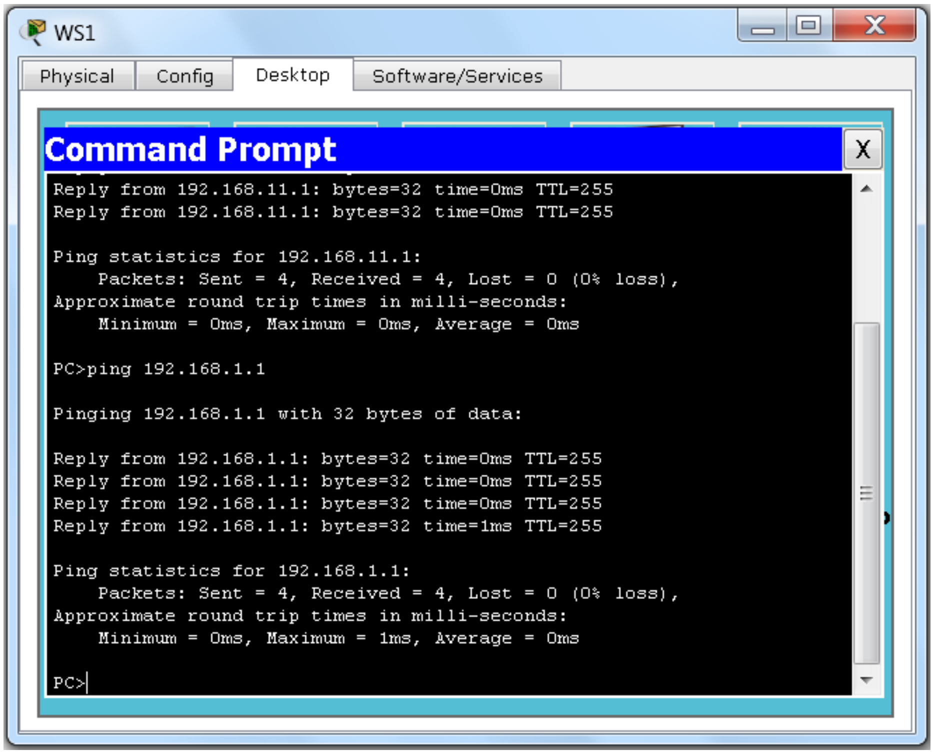
```
R1(config-if)#interface Fa0/0.1
R1(config-subif)#
R1(config-subif)#encapsulation dot1q 1 native
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#interface Fa0/0.11
R1(config-subif)#
R1(config-subif)#encapsulation dot1q 11
R1(config-subif)#ip address 192.168.11.1 255.255.255.0
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, change
 to up

%LINK-5-CHANGED: Interface FastEthernet0/0.11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.11, chang
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).

- **Enter interface configuration mode**: Enact interface-level configuration mode using the command **interface gi0/0.**
- **Enable the LAN interface of R1**: Unlike switch ports, router ports are normally administratively disabled by default. Activate the interface with the command **no shutdown.**
- **Configure R1's VLAN 1 interface**: Use the following steps:
    - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.1** (the .1 does not have any special significance, just reflects the best practice of using the VLAN ID as the identifier)
    - **Specify VLAN 1**: Manually set the VLAN ID using the command **encapsulation dot1q 1 native** (802.1q is the trunking protocol, and requires a native (untagged) VLAN on both sides of the trunk connection)
    - **IP address assignment**: Use the command **ip address 192.168.1.1 255.255.255.0** to assign an IPv4 address to the subinterface
- **Configure R1's VLAN 11 interface**: Use the following steps:
    - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.11** (see note on .1 above)
    - **Specify VLAN 11**: Manually set the VLAN ID using the command **encapsulation dot1q 11** (802.1q is the trunking protocol, and requires a native (untagged) VLAN on both sides of the trunk connection). Do ***not*** include the **native** keyword, as it will cause the trunk to fail (native VLAN on SW-1 is 1, and the native VLAN settings have to match on both ends of a trunk connection)
    - **IP address assignment**: Use the command **ip address 192.168.11.1 255.255.255.0** to assign an IPv4 address to the subinterface

2.1.4. Test Connectivity Across VLANs in Site 1

To ensure that the overall VLAN configuration functions as intended, you should perform basic testing using WS1 in site 1. Conduct the testing at Site 1 using the steps below:



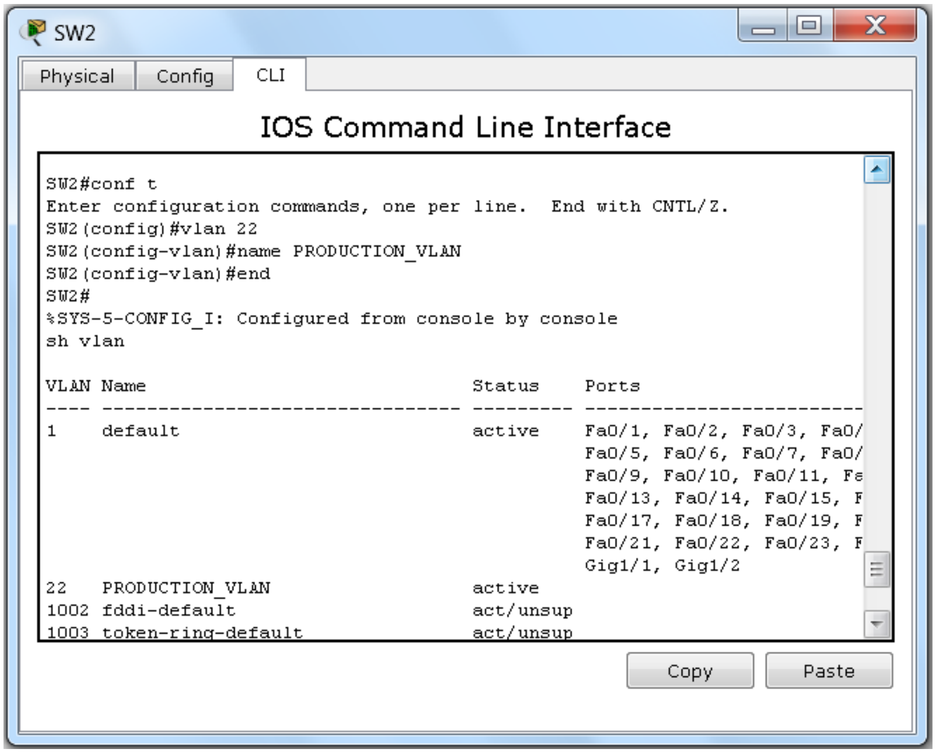
```
Reply from 192.168.11.1: bytes=32 time=0ms TTL=255
Reply from 192.168.11.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

- **Access Workstation 1 in Site 1:** WS1 in Site 1 sits in VLAN 11, connected to SW1 using an access port, making it a perfect choice as a testing point. Click on the icon WS1 in Packet Tracer, which will display a four-tabbed screen with the labels ***Physical***, ***Config***, ***Desktop***, and ***Software/Services***. Choose the ***Desktop*** option, and then click ***Command Prompt*** to open a CLI session on WS1.
- **Verify Connectivity to R1:** At the command line, type **ping 192.168.11.1** (the IPv4 address of the Fa0/0.11 subinterface that you created on R1). A successful ping indicates that SW1 and R1 both have the correct VLAN configuration, and that connectivity is successful.
- **Verify InterVLAN Routing:** At the command prompt, now type **ping 192.168.1.1**. This successful ping is for a network ***not*** local to WS1 (VLAN 11 uses IPv4 network 192.168.11.0/24), requiring R1 to perform routing from VLAN 11 to VLAN 1 (R1's Fa0/0.1 subinterface), and back again. Both of these successful tests indicate that the VLAN configurations on the devices in Site 1 are correct.

2.1.5. Configure VLANs on SW2 (Site 2)

Even if you only casually examine the topology of Site 2, you can easily conclude that the setup is identical to Site 1. The only real differences between these two sites are VLAN identifiers and IPv4 addressing. Repeat the same steps from the previous exercise to the devices in site 2 as follows:

- **VLAN Configuration Mode**: On site one, you used an older vlan database method for creating VLANs on the switch; on SW2, you will use the more recent, recommended method, entitled ***vlan configuration mode***. To configure a VLAN using this method, perform the following steps:



```
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#vlan 22
SW2(config-vlan)#name PRODUCTION_VLAN
SW2(config-vlan)#end
SW2#
%SYS-5-CONFIG_I: Configured from console by console
sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/
                                                Fa0/9, Fa0/10, Fa0/11, Fa
                                                Fa0/13, Fa0/14, Fa0/15, F
                                                Fa0/17, Fa0/18, Fa0/19, F
                                                Fa0/21, Fa0/22, Fa0/23, F
                                                Gig1/1, Gig1/2
22   PRODUCTION_VLAN                  active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Create a VLAN:** Create a VLAN with the ID of 22 using the **vlan 22** command
  - **Name the VLAN:** Assign a name to the new VLAN using the command **name PRODUCTION_VLAN**
  - **Exit global configuration mode**: Enter the **end** command to return to privileged exec mode
  - **Verify VLAN**: Type the command **show vlan id 22** to verify that you created the VLAN successfully.

- **Configure a VLAN interface**: On SW2, enter SVI configuration mode and assign addressing as follows:

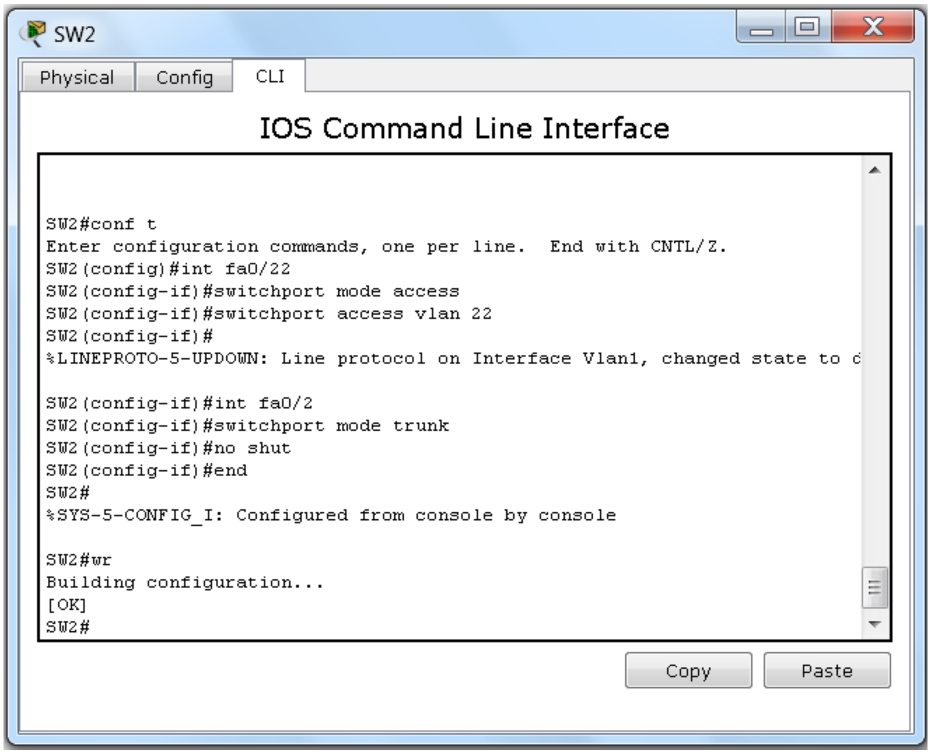
    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter VLAN configuration mode**: Enter SVI configuration mode with the command **interface vlan 1** (the prompt will change to ***config-if***)
    - **Enable the interface**: Since the VLAN 1 SVI is administratively down by default, enable the interface using the **no shutdown** command
    - **Add Description**: Identify the interface as reserved for management with the designation **description MANAGEMENT VLAN**
    - **Configure IPV4 addressing**: Enter the command **ip address 192.168.2.222 255.255.255.0**
- **Default gateway**: Set the default gateway using the command **ip default-gateway 192.168.2.2**
- **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 or 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.

2.1.6. Configure Switch Ports on SW2

As with SW1, you need to configure the necessary ports to create the connectivity needed with the attached workstation (WS2) as well as R2. Repeat the previous configuration steps on SW2 as follows:

- **Configure Access Ports**: WS2 sits on the Production VLAN (VLAN 22) on Fa0/22 and will only need access to that single VLAN. Configure an access port as follows:
    - **Set port Fa0/22 to Access mode**: Use the command **switchport mode access**
    - **Assign the port to VLAN 22**: By default, all ports get assigned to VLAN 1 (the default VLAN), so change the VLAN assignment with the **switchport access vlan 22** command

- **Configure Trunk Ports:** R2 will host interfaces for both VLAN 1 and VLAN 11. Set Fa0/2 to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command)
- **Exit configuration mode:** Return to privileged mode using either the **exit** or **end** commands.
- **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 or 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#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#int fa0/22
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 22
SW2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to d

SW2(config-if)#int fa0/2
SW2(config-if)#switchport mode trunk
SW2(config-if)#no shut
SW2(config-if)#end
SW2#
%SYS-5-CONFIG_I: Configured from console by console

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

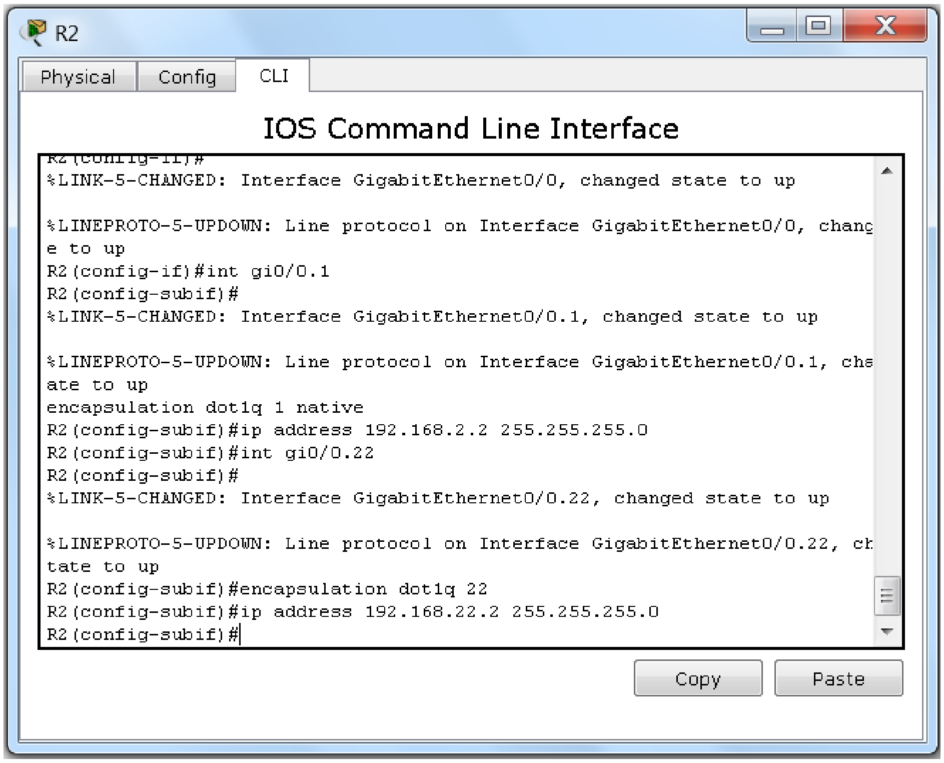
2.1.7. Configure Trunking and InterVLAN Routing on R2 (Site 2)

As with R1, you need to complete trunking (i.e., “router on a stick”) configuration on R2’s LAN interface using these steps:

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).

- **Enter interface configuration mode**: Enact interface-level configuration mode using the command **interface gi0/0**.
- **Enable the LAN interface of R2**: Unlike switch ports, router ports are normally administratively disabled by default. Activate the interface with the command **no shutdown**.
- **Configure R2's VLAN 1 interface**: Use the following steps:
  - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.1**
  - **Specify VLAN 1**: Manually set the VLAN ID using the command **encapsulation dot1q 1 native**
  - **IP address assignment**: Use the command **ip address 192.168.2.2 255.255.255.0** to assign an IPv4 address to the subinterface
- **Configure R1's VLAN 22 interface**: Use the following steps:
  - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.22**
  - **Specify VLAN 22**: Manually set the VLAN ID using the command **encapsulation dot1q 22**

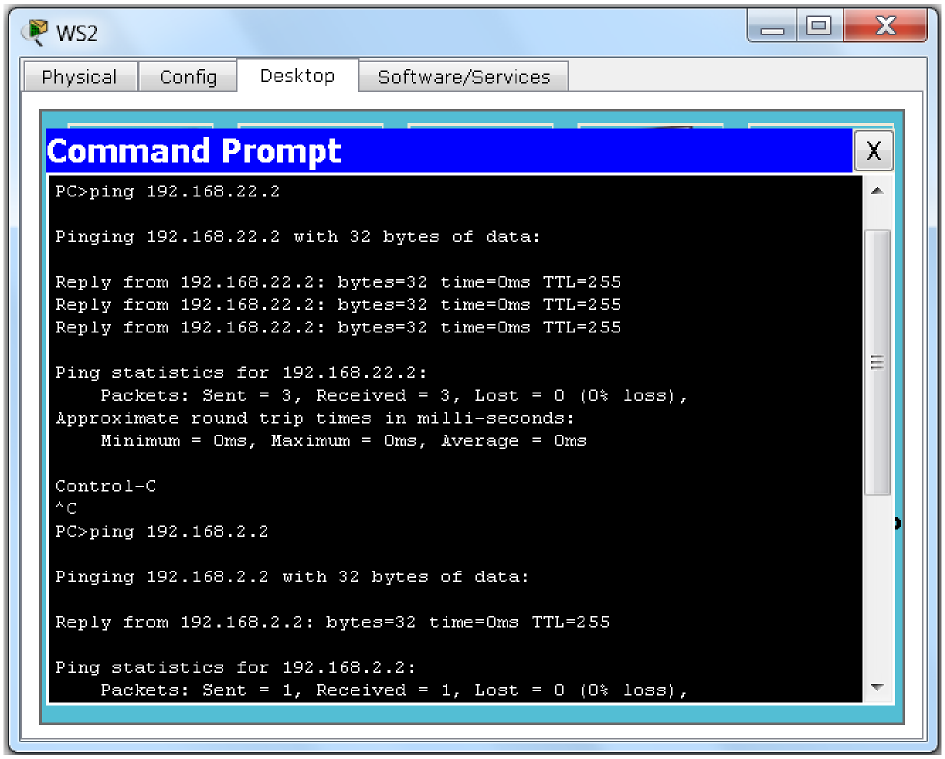
- **IP address assignment**: Use the command **ip address 192.168.22.2 255.255.255.0** to assign an IPv4 address to the subinterface



```
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, chang
e to up
R2(config-if)#int gi0/0.1
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, cha
ate to up
encapsulation dot1q 1 native
R2(config-subif)#ip address 192.168.2.2 255.255.255.0
R2(config-subif)#int gi0/0.22
R2(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.22, ch
tate to up
R2(config-subif)#encapsulation dot1q 22
R2(config-subif)#ip address 192.168.22.2 255.255.255.0
R2(config-subif)#
```

2.1.8. Test Connectivity Across VLANs in Site 2

To ensure that the overall VLAN configuration functions as intended, you should perform basic testing using WS2 in Site 2. Conduct the testing at Site 2 using the steps below:



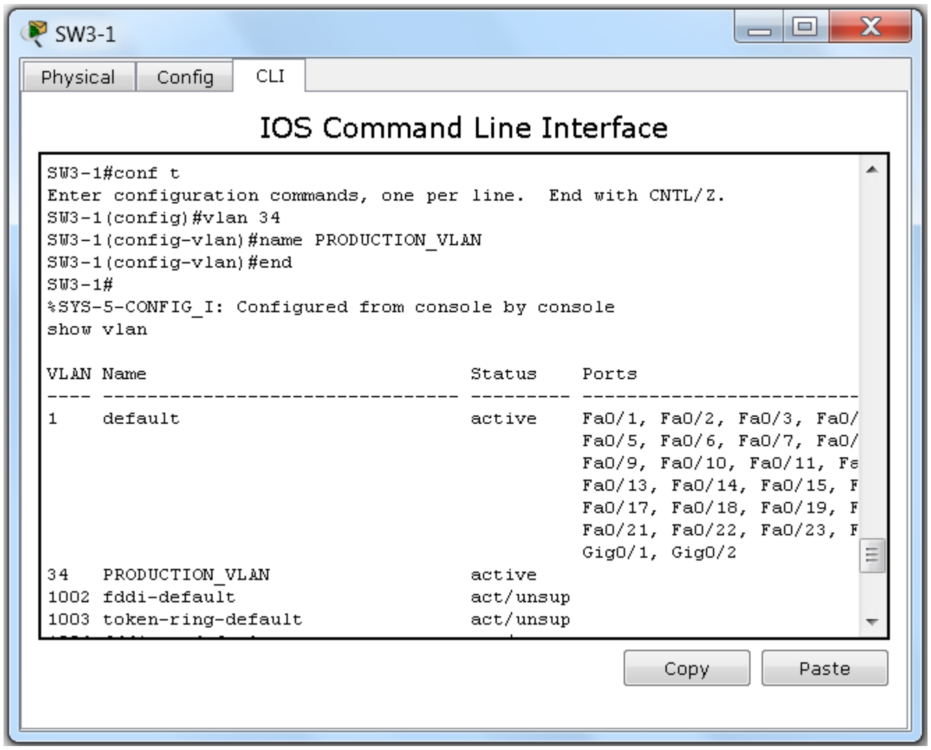
```
PC>ping 192.168.22.2

Pinging 192.168.22.2 with 32 bytes of data:

Reply from 192.168.22.2: bytes=32 time=0ms TTL=255
Reply from 192.168.22.2: bytes=32 time=0ms TTL=255
Reply from 192.168.22.2: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.22.2:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.2.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- **Access Workstation 2 in Site 2:** WS2 in Site 2 sits in VLAN 22 connected to SW2 using an access port, making it a perfect choice as a test point. Click on the icon WS2 in Packet Tracer, which will display a four-tabbed screen with the labels ***Physical***, ***Config***, ***Desktop***, and ***Software/Services***. Choose the ***Desktop*** option, and then click ***Command Prompt*** to open a CLI session on WS2.
- **Verify Connectivity to R2:** At the command line, type **ping 192.168.22.2** (the IPv4 address of the Gi0/0.22 subinterface that you created on R2). A successful ping indicates that SW2 and R2 both have the correct VLAN configuration, and that connectivity is successful.
- **Verify InterVLAN Routing:** At the command prompt, now type **ping 192.168.2.2**. This successful ping is for a network not local to WS2 (VLAN 22 uses IPv4 network 192.168.22.0/24), requiring R2 to perform routing from VLAN 22 to VLAN 1 (R2's Gi0/0.1 subinterface), and back again. Both of these successful tests indicate that the VLAN configurations on the devices in Site 2 are correct.

2.1.9. Configure VLANs on SW3-1 in Site 3

As you can observe from the topology earlier diagram, Site 3 contains three routers, three switches, and one server, and thus distinctly different from the previously configured sites. While you will use similar configuration methods in here, expect a number of additional steps. Configure VLANs on SW3-1 in site 3 as follows:

- **VLAN Configuration Mode**: You will only configure individual VLANs on SW3-1 for reasons which will become clear in later exercises. As you did previously use ***vlan configuration mode,*** as shown below:



```
SW3-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-1(config)#vlan 34
SW3-1(config-vlan)#name PRODUCTION_VLAN
SW3-1(config-vlan)#end
SW3-1#
%SYS-5-CONFIG_I: Configured from console by console
show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/
                                                Fa0/9, Fa0/10, Fa0/11, Fa
                                                Fa0/13, Fa0/14, Fa0/15, F
                                                Fa0/17, Fa0/18, Fa0/19, F
                                                Fa0/21, Fa0/22, Fa0/23, F
                                                Gig0/1, Gig0/2
34   PRODUCTION_VLAN                  active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Create a VLAN:** Create a VLAN with the ID of 34 using the **vlan 34** command
  - **Name the VLAN:** Assign a name to the new VLAN using the command **name PRODUCTION_VLAN**
  - **Exit global configuration mode**: Enter the **end** command to return to privileged exec mode

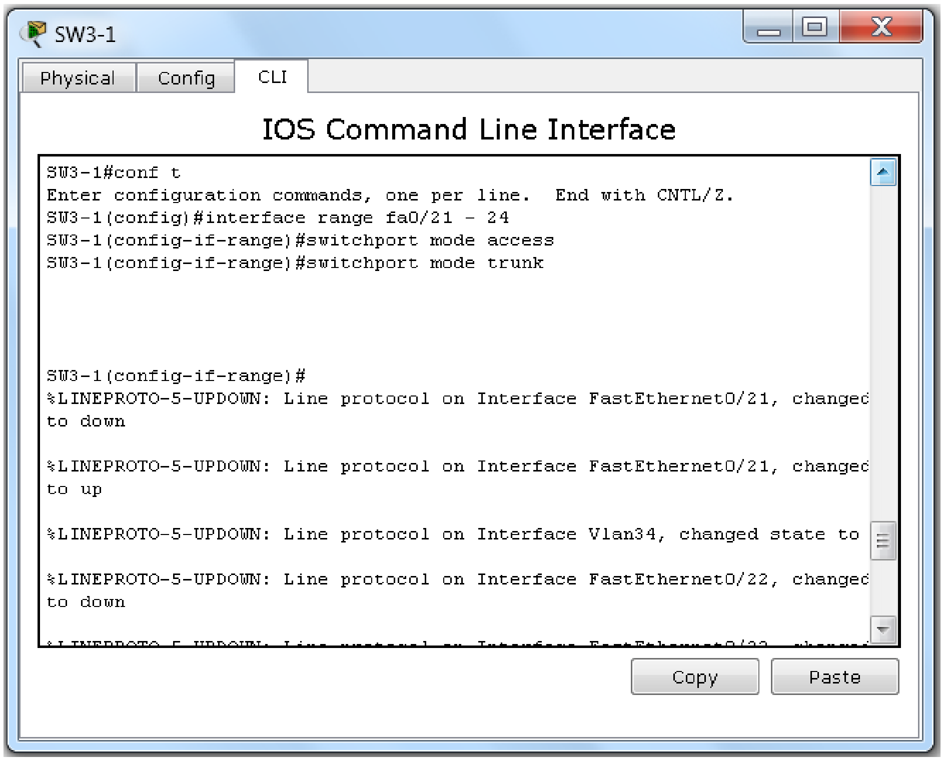
  - **Verify VLAN**: Type the command **show vlan id 34 (or simply show vlan)** to verify that you created the VLAN successfully.
  - **Create VLAN 33**: S2 will participate in a server-only VLAN, VLAN 33, so create it using the **vlan 33** command.
- **Configure VLAN interfaces**: Because SW3-1 is a Layer 3 switch, it does not have the limitation of only hosting a single SVI/VLAN interface. Configure SVI interfaces for both active VLANs as shown below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter VLAN interface configuration mode**: Enter SVI configuration mode with the command **interface vlan 1** (the prompt will change to ***config-if***)
  - **Enable the interface**: Since the VLAN 1 SVI is administratively down by default, enable the interface using the **no shutdown** command
  - **Add Description**: Identify the interface as reserved for management with the designation **description MANAGEMENT VLAN**
  - **Configure IPV4 addressing**: Enter the command **ip address 192.168.3.111 255.255.255.0**

- **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 or 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.

2.1.10. Configure Switch Ports on SW3-1

As with SW2, you need to configure the necessary ports to create the connectivity needed with the various ports in use on SW3-1. Perform the following configuration steps:

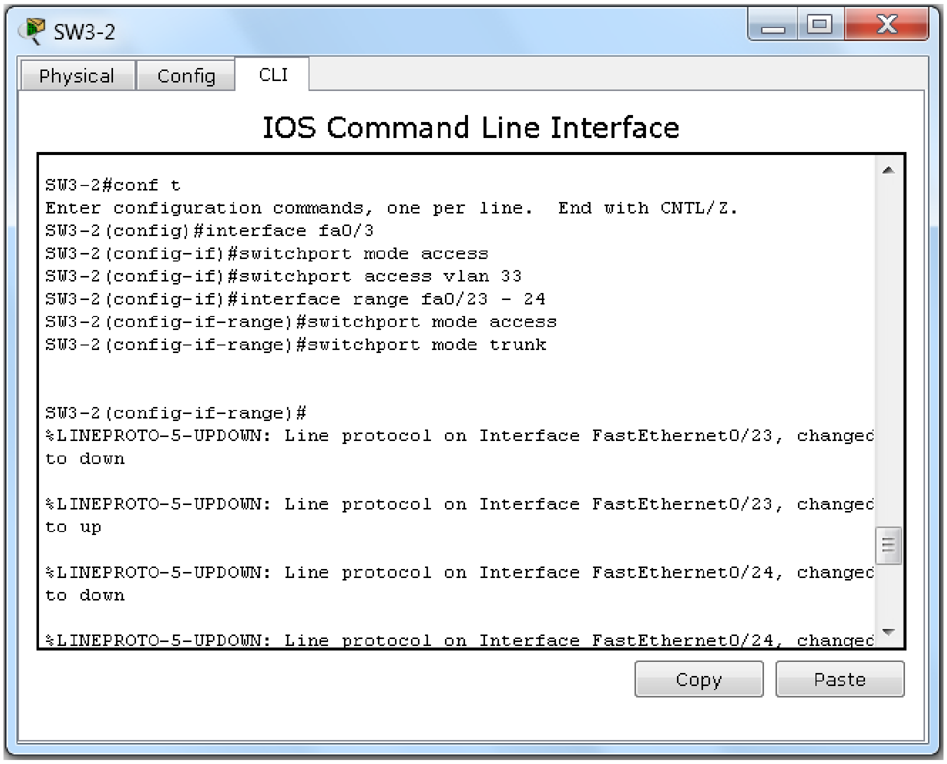


```
SW3-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-1(config)#interface range fa0/21 - 24
SW3-1(config-if-range)#switchport mode access
SW3-1(config-if-range)#switchport mode trunk




SW3-1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan34, changed state to

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed
```

- **Configure a Trunk Port to R3-1:** SW3-1 has direct connection to R3-1 (Fa0/3) which needs to be configured as a trunk connection. Set the port to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command).
- **Configure Trunk Ports to SW3-2 and SW3-3:** SW3-1 also has two direct connections to SW3-2 (Fa0/23-24) and SW3-3 (Fa0/21-22) which also need to be configured as trunk connections. Set the ports to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command). Alternatively, you can do the configuration for all ports at once using the **interface range** command.
- **Exit configuration mode:** Return to privileged mode using either the **exit** or **end** commands.
- **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 or 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.

2.1.11. Configure Switch Ports on SW3-2

As with SW3-1, you need to configure the active ports on SW3-2 to interface with adjoining devices, in this case, SW3-1, SW3-3, and S1. Perform the necessary following configuration steps as outlined here:



```
SW3-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-2(config)#interface fa0/3
SW3-2(config-if)#switchport mode access
SW3-2(config-if)#switchport access vlan 33
SW3-2(config-if)#interface range fa0/23 - 24
SW3-2(config-if-range)#switchport mode access
SW3-2(config-if-range)#switchport mode trunk


SW3-2(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed
```

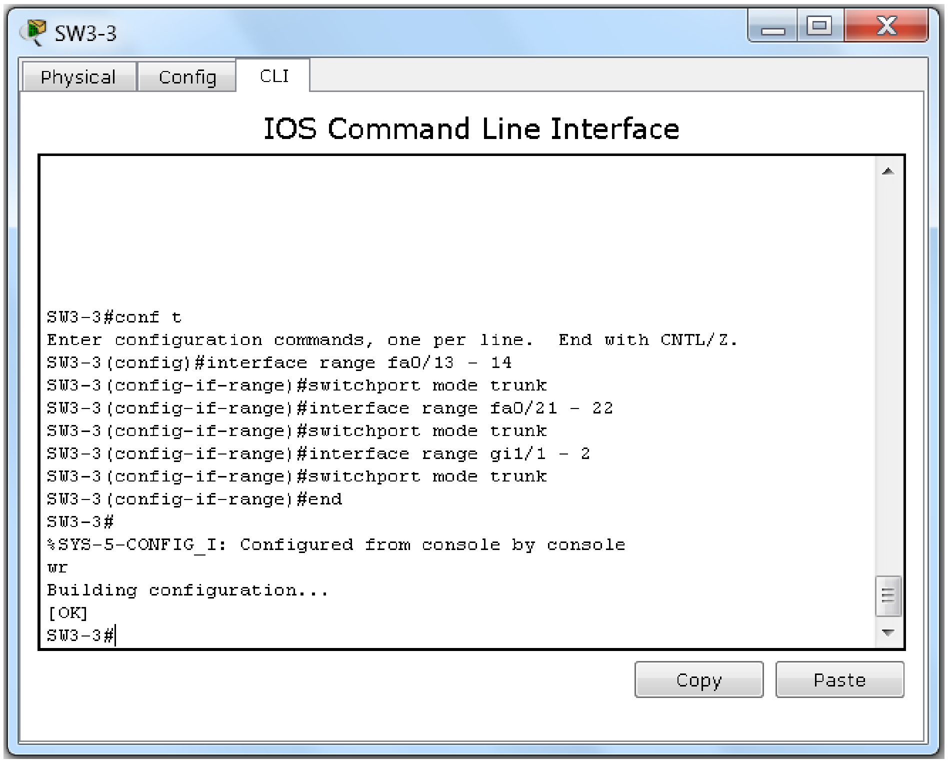
- **Configure an Access Port**: S3 sits on the Server VLAN (VLAN 33) on Fa0/3 and will only need access to that single VLAN. Configure an access port as follows:
  - **Set port Fa0/3 to Access mode**: Use the command **switchport mode access**
  - **Assign the port to VLAN 33**: By default, all ports get assigned to VLAN 1 (the default VLAN), so change the VLAN assignment with the **switchport access vlan 33** command

- **Configure Trunk Ports to SW3-2 and SW3-3:** SW3-1 also has two direct connections to SW3-2 (Fa0/23-24) and SW3-3 (Gi1/1-2) which also need to be configured as trunk connections. Set the ports to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command). Alternatively, you can do the configuration for all ports at once using the **interface range** command.

- **Exit configuration mode:** Return to privileged mode using either the **exit** or **end** commands.
- **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 or 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.

2.1.12. Configure Switch Ports on SW3-3

As with the previous switches, you need to configure connectivity at the individual port level in order for the VLANs to become functional. Configure the ports on SW3-3 as follows:



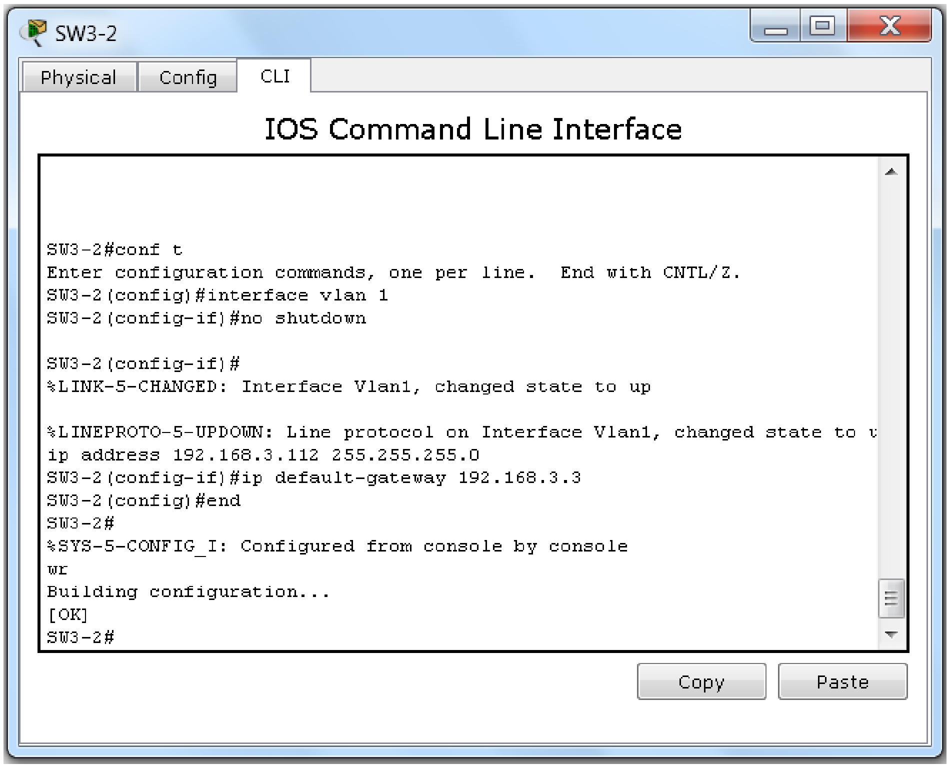
```
SW3-3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-3(config)#interface range fa0/13 - 14
SW3-3(config-if-range)#switchport mode trunk
SW3-3(config-if-range)#interface range fa0/21 - 22
SW3-3(config-if-range)#switchport mode trunk
SW3-3(config-if-range)#interface range gi1/1 - 2
SW3-3(config-if-range)#switchport mode trunk
SW3-3(config-if-range)#end
SW3-3#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW3-3#
```

- **Configure Trunk Ports to R4-1 and R4-2:** Site 3 hosts the Internet connection which services all sites, and uses two routers for redundancy purposes. SW3-3 has direct connections both devices, R4-1 (Fa0/13) as well as R4-2 (Fa0/14), which need to be configured as trunk connections. Set the ports to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command).

Alternatively, you can do the configuration for all ports at once using the **interface range** command.

- **Configure Trunk Ports to SW3-2 and SW3-3:** SW3-1 also has two direct connections to SW3-1 (Fa0/21-22) and SW3-2 (Gi1/1-2) which also need to be configured as trunk connections. Set the ports to trunk unconditionally (no negotiation) using the **switchport mode trunk** command (if you happen to receive an error doing this, use the command **switchport mode access** first and then repeat the use of the **switchport mode trunk** command). Alternatively, you can do the configuration for all ports at once using the i**nterface range** command.
- **Exit configuration mode:** Return to privileged mode using either the **exit** or **end** commands.
- **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 or 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.

2.1.13. Configure VLANs Interfaces on SW3-2 and in SW3-3



```
SW3-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-2(config)#interface vlan 1
SW3-2(config-if)#no shutdown

SW3-2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to u
ip address 192.168.3.112 255.255.255.0
SW3-2(config-if)#ip default-gateway 192.168.3.3
SW3-2(config)#end
SW3-2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
SW3-2#
```

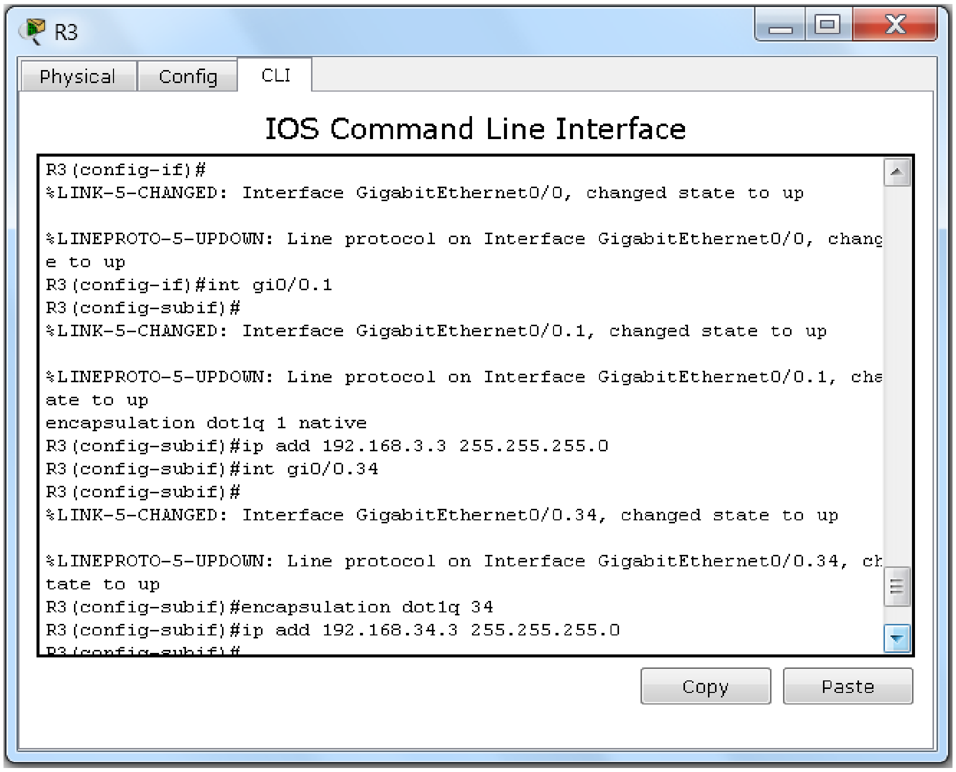
During the step dealing with VLAN creation on SW3-1, you created SVI/VLAN interfaces, but not on the remaining switches in Site 3. While you will use similar configuration methods in here, expect a number of additional steps. Configure VLANs on SW3-1 in site 3 as follows:

- **Configure VLAN interfaces**: As with SW1 and SW2 in other sites, SW3-2 and 3-3 are Layer 2 switches, which only allow a single SVI/VLAN interface. Create management VLAN 1 interface on each device using the process below:
  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter VLAN interface configuration mode**: Enter SVI configuration mode with the command **interface vlan 1** (the prompt will change to ***config-if***)
  - **Enable the interface**: Since the VLAN 1 SVI is administratively down by default, enable the interface using the **no shutdown** command
  - **Add Description**: Identify the interface as reserved for management with the designation **description MANAGEMENT VLAN**
  - **Configure IPV4 addressing**: Enter the command **ip address 192.168.3.112 255.255.255.0** for SW3-2 and **ip address 192.168.3.113 255.255.255.0** for SW3-3

- **Default gateway**: Set the default gateway using the command **ip default-gateway 192.168.3.3**
- **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 or 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.

2.1.14. Configure Trunking and Routing on R3-1 (Site 3)

As with R1 and R2, you need to complete trunking (i.e., “router on a stick”) configuration on R3-1’s LAN interface. Note that because SW3-1 is a ***Layer 3*** switch, that it can also perform InterVLAN routing if needed. Configure trunking on R3-1 using these steps:



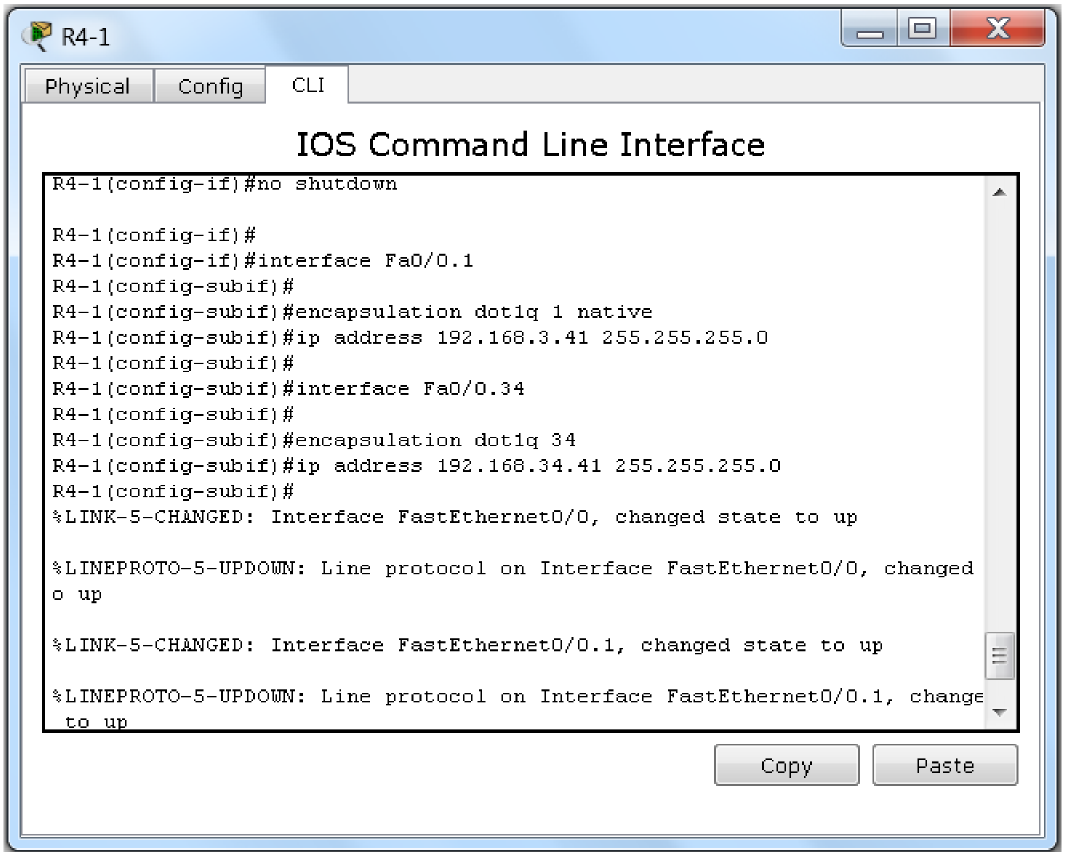
```
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, chang
e to up
R3(config-if)#int gi0/0.1
R3(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, cha
ate to up
encapsulation dot1q 1 native
R3(config-subif)#ip add 192.168.3.3 255.255.255.0
R3(config-subif)#int gi0/0.34
R3(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.34, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.34, ch
tate to up
R3(config-subif)#encapsulation dot1q 34
R3(config-subif)#ip add 192.168.34.3 255.255.255.0
R3(config-subif)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
- **Enter interface configuration mode**: Enact interface-level configuration mode using the command **interface gi0/0.**
- **Enable the LAN interface of R3-1**: Unlike switch ports, router ports are normally administratively disabled by default. Activate the interface with the command **no shutdown**.
- **Configure R3-1’s VLAN 1 interface**: Use the following steps:
    - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.1**
    - **Specify VLAN 1**: Manually set the VLAN ID using the command **encapsulation dot1q 1 native**

    - **IP address assignment**: Use the command **ip address 192.168.3.3 255.255.255.0** to assign an IPv4 address to the subinterface
- **Configure R3-1's VLAN 34 interface**: Use the following steps:
    - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.34**
    - **Specify VLAN 34**: Manually set the VLAN ID using the command **encapsulation dot1q 34**
    - **IP address assignment**: Use the command **ip address 192.168.34.3 255.255.255.0** to assign an IPv4 address to the subinterface
- **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 or 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.

2.1.15. Configure Trunking and Routing on R4-1/R4-2 (Site 3)

Site 3 also serves as the entire network's connection point to the Internet, using a pair of redundant 2911 routers. As with R3-1 you will need to complete trunking (i.e., "router on a stick") configuration on R4-1's and R4-2's LAN interfaces, respectively. Configure trunking on these devices as follows:



```
R4-1(config-if)#no shutdown

R4-1(config-if)#
R4-1(config-if)#interface Fa0/0.1
R4-1(config-subif)#
R4-1(config-subif)#encapsulation dot1q 1 native
R4-1(config-subif)#ip address 192.168.3.41 255.255.255.0
R4-1(config-subif)#
R4-1(config-subif)#interface Fa0/0.34
R4-1(config-subif)#
R4-1(config-subif)#encapsulation dot1q 34
R4-1(config-subif)#ip address 192.168.34.41 255.255.255.0
R4-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, change
 to up
```

- **Configure Trunking on R4-1:**
  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter interface configuration mode**: Enact interface-level configuration mode using the command **interface Fa0/0**
  - **Enable the LAN interface of R4-1**: Unlike switch ports, router ports are normally administratively disabled by default. Activate the interface with the command **no shutdown**
  - **Configure R4-1's VLAN 1 interface**: Use the following steps:
    - **Subinterface creation:** Create a logical subinterface on Fa0/0 using the command **interface Fa0/0.1**
    - **Specify VLAN 1**: Manually set the VLAN ID using the command **encapsulation dot1q 1 native**
    - **IP address assignment**: Use the command **ip address 192.168.3.41 255.255.255.0** to assign an IPv4 address to the subinterface

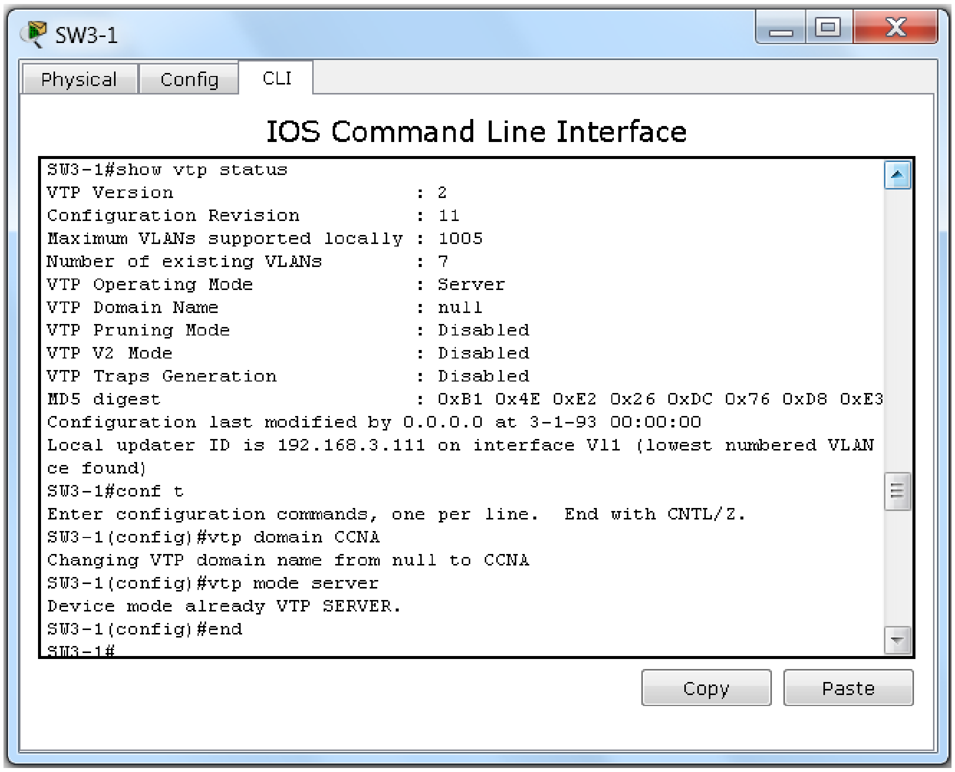
    - **Configure R4-1's VLAN 34 interface**: Use the following steps:
        - **Subinterface creation:** Create a logical subinterface on Fa0/0 using the command **interface Fa0/0.34**
        - **Specify VLAN 34**: Manually set the VLAN ID using the command **encapsulation dot1q 34**
        - **IP address assignment**: Use the command **ip address 192.168.34.41 255.255.255.0** to assign an IPv4 address to the subinterface
    - **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 or 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.
- **Configure Trunking on R4-2:**
    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter interface configuration mode**: Enact interface-level configuration mode using the command **interface gi0/0**
    - **Enable the LAN interface of R4-2**: Unlike switch ports, router ports are normally administratively disabled by default. Activate the interface with the command **no shutdown**
    - **Configure R4-2's VLAN 1 interface**: Use the following steps:
        - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.1**
        - **Specify VLAN 1**: Manually set the VLAN ID using the command **encapsulation dot1q 1 native**

        - **IP address assignment**: Use the command **ip address 192.168.3.42 255.255.255.0** to assign an IPv4 address to the subinterface
    - **Configure R4-2's VLAN 34 interface**: Use the following steps:
        - **Subinterface creation:** Create a logical subinterface on Gi0/0 using the command **interface Gi0/0.34**
        - **Specify VLAN 34**: Manually set the VLAN ID using the command **encapsulation dot1q 34**
        - **IP address assignment**: Use the command **ip address 192.168.34.42 255.255.255.0** to assign an IPv4 address to the subinterface

    - **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 or 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.

2.1.16. Configure VTP on the switches in Site 3

As you have already learned, many tasks throughout a network involve manual configuration, which can consume a great deal of time. IP routing, for example, can potentially use dynamic routing protocols to mitigate static configurations. Applying the same concept to switched networks, network administrators can automate small tasks to simplify device management. This is the thought process behind ***VLAN Trunk Protocol***, which permits a master switch (called a ***vtp server***) to take on the task of VLAN management. Configure VTP on SW3-1, SW3-2, and SW3-3 using these steps:

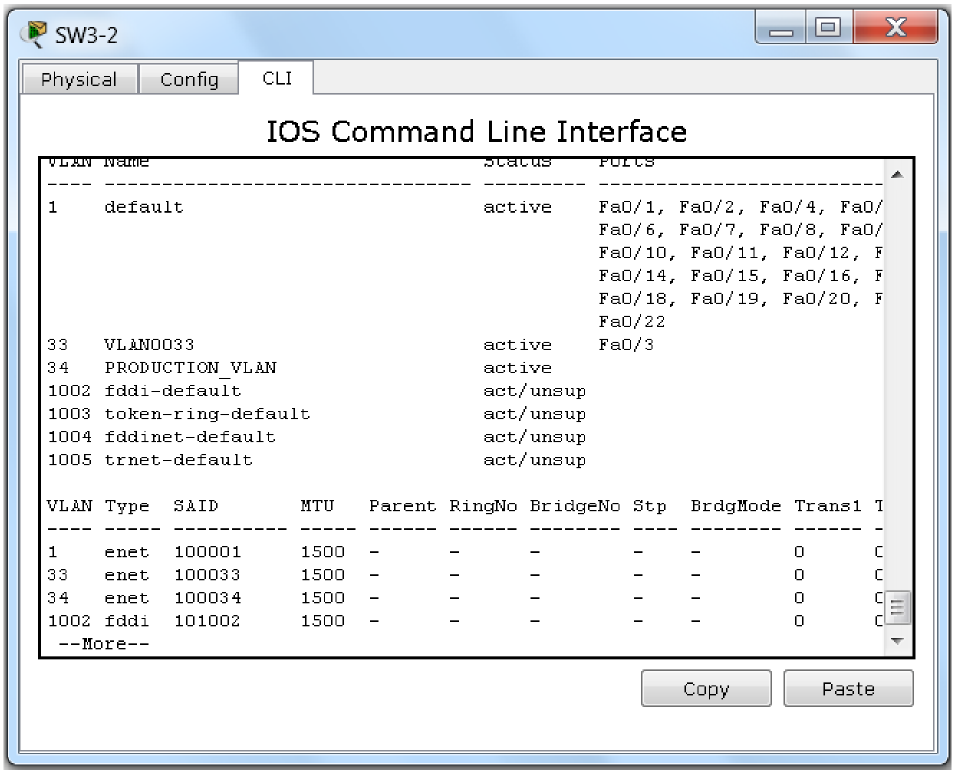


```
SW3-1#show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : null
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xB1 0x4E 0xE2 0x26 0xDC 0x76 0xD8 0xE3
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 192.168.3.111 on interface Vl1 (lowest numbered VLAN
ce found)
SW3-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-1(config)#vtp domain CCNA
Changing VTP domain name from null to CCNA
SW3-1(config)#vtp mode server
Device mode already VTP SERVER.
SW3-1(config)#end
SW3-1#
```

- Configure SW3-1 as a VTP Server:
    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Display the current VTP Settings**: To see the default VTP settings currently on SW3-1, use the **show vtp status** command
    - **Set the VTP Domain**: As you can see from the previous output (see screen shot above), the default VTP domain is ***null***, which will prevent the protocol from operating. Change this setting using the command **vtp domain CCNA**
    - **Set other required parameters**: Required parameters include a domain name, trunk connections, and VLAN 1 in an active state. Since you configured these previously, no additional settings need to be altered.
    - **Set SW3-1 to act as the VTP Server**: While still in global configuration mode, enter the command **vtp mode server**. If the switch is running with the default mode setting, you should see the error message ***Device mode already VTP SERVER***.

- **Ignore Domain Mismatch errors**: For VTP to operate, the domain name and passwords (if one is configured) must match. Since you have not completed the VTP configuration on SW3-2 and SW3-3, simply ignore these warnings.
- **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 or 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.

- Configure SW3-2 as a VTP Client:



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/
                                                Fa0/10, Fa0/11, Fa0/12, F
                                                Fa0/14, Fa0/15, Fa0/16, F
                                                Fa0/18, Fa0/19, Fa0/20, F
                                                Fa0/22
33   VLAN0033                         active    Fa0/3
34   PRODUCTION_VLAN                  active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 T
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ -
1    enet  100001     1500  -      -      -        -    -        0      C
33   enet  100033     1500  -      -      -        -    -        0      C
34   enet  100034     1500  -      -      -        -    -        0      C
1002 fddi  101002     1500  -      -      -        -    -        0      C
 --More--
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Display the current VTP Settings**: To see the default VTP settings currently on SW3-2, use the **show vtp status** command

  - **Set the VTP Domain**: As discussed previously, the default domain is ***null*** and must match the setting on SW3-1 in order to operate. Change this setting using the command **vtp domain CCNA**
  - **Set other required parameters**: Required parameters include a domain name, trunk connections, and VLAN 1 in an active state. Since you configured these previously, no additional settings need to be altered.
  - **Set SW3-2 to act as a VTP Client**: While still in global configuration mode, enter the command **vtp mode client**. Following this step, you should see the system message ***Changing VTP domain name from null to CCNA***.
  - **Ignore Domain Mismatch errors**: While you changed the VTP domain to match SW-1, SW3-3's configuration is unchanged. Ignore any error messages on mismatches.
  - **Verify that VTP is operational**: Since you have already used the **show vtp status** command, you can verify operational status by displaying VLANs with the **show vlans** command (remember that you did not configure any VLANs on SW3-2).
  - **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 or 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.

- Configure SW3-3 as a VTP Client:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Display the current VTP Settings**: To see the default VTP settings currently on SW3-3, use the **show vtp status** command
  - **Set the VTP Domain**: As discussed previously, the default domain is ***null*** and must match the setting on SW3-1 in order to operate. Change this setting using the command **vtp domain CCNA**
  - **Set other required parameters**: Required parameters include a domain name, trunk connections, and VLAN 1 in an active state.

Since you configured these previously, no additional settings need to be altered.

- **Set SW3-3 to act as a VTP Client**: While still in global configuration mode, enter the command **vtp mode client**. Following this step, you should see the system message ***Changing VTP domain name from null to CCNA***.
- **Verify that VTP is operational**: Use the **show vtp status** command, you can verify operational status by displaying VLANs with the **show vlans** command (remember that you did not configure any VLANs on SW3-2).
- **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 or 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.

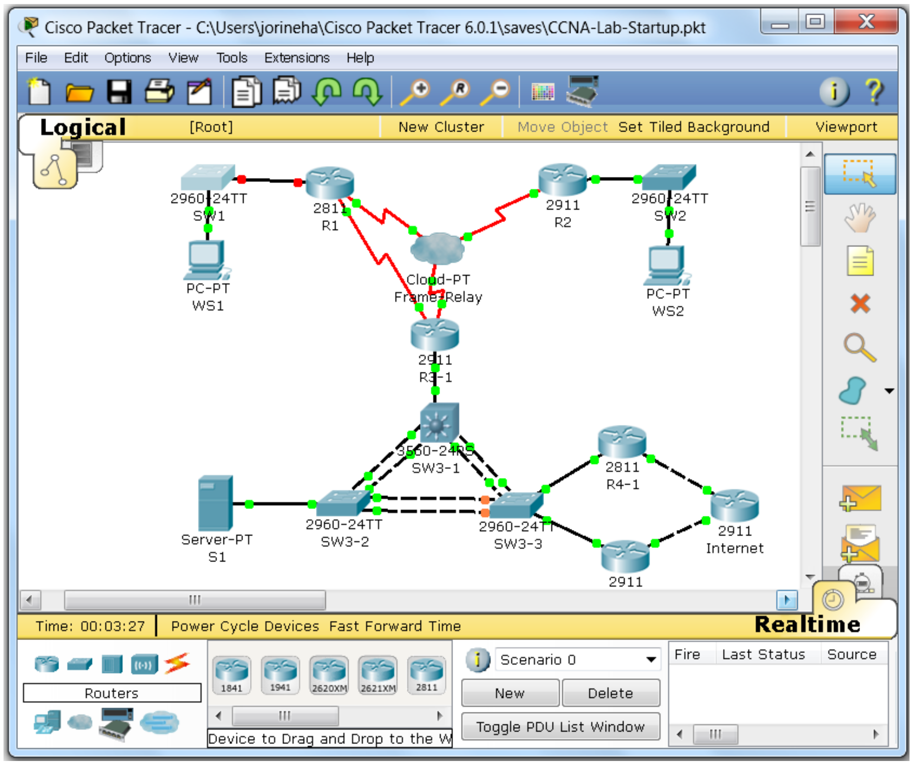
Lesson 2 Lab Exercises

3.1 Spanning-Tree Protocol Configuration Exercises

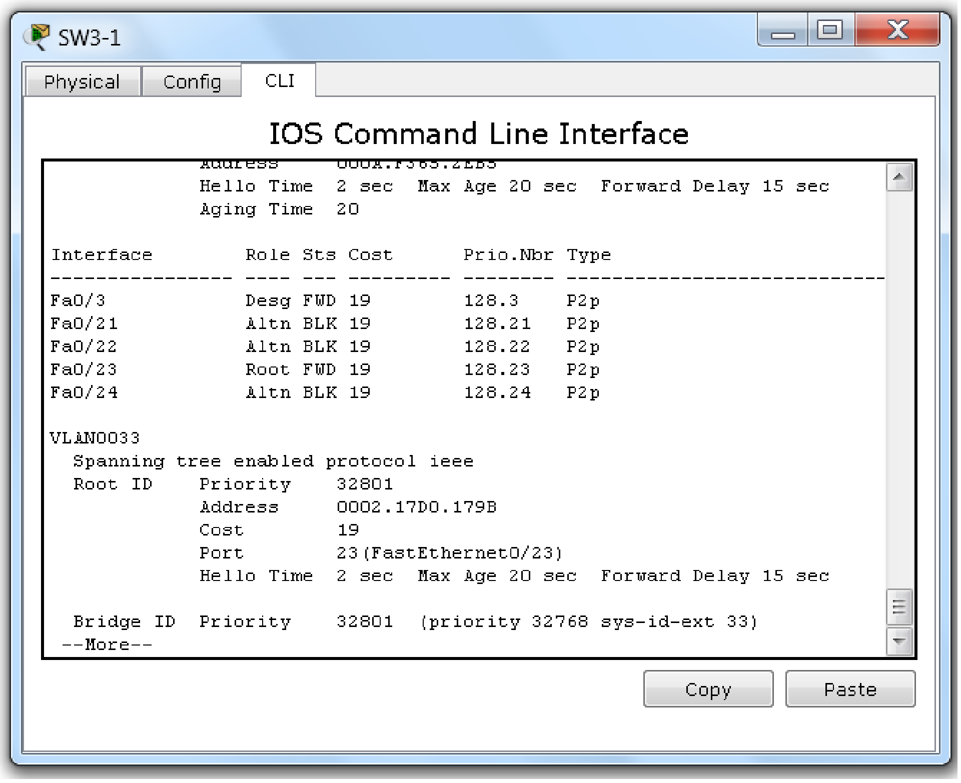
Many networking protocols appear to have an intense obsession with the prevention of loops in the overall infrastructure. This certainly rings true with Layer 3 routing protocols, but also extends to Layer 2 protocols as well. In the new 200-101 version of the CCNA exam ***802.1d Spanning-Tree Protocol is no longer an exam topic***, but understanding the fundamental operation of STP can help shed light on other Layer 2 protocol operations.

3.1.1. Observe and Configure 802.1d Spanning-Tree Protocol Operation in Site 3

Spanning-Tree Protocol (IEEE standard 802.1d) runs by default on many Cisco switches, whether Layer 2 or Layer 3 devices. STP determines the best path through the network at Layer 2, using cost (based on the bandwidth of the port) as the basis for choosing this path. Unfortunately, only a single path gets chosen, and redundant ports are placed in blocking mode, and thus unavailable for forwarding. Since Site 3 has multiple switches, it presents the best opportunity to observe and configure STP operation, as shown below for reference.



- **Discovering the root switch**: STP chooses a single switch in the domain to act as the root, which issues all hello messages and manages the process in the network. Election of the root switch (or bridge) is automated, but seldom chooses the most optimal device. Discover which switch has become the root as follows:



```
             Address     000A.F363.2EB3
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/21           Altn BLK 19        128.21   P2p
Fa0/22           Altn BLK 19        128.22   P2p
Fa0/23           Root FWD 19        128.23   P2p
Fa0/24           Altn BLK 19        128.24   P2p

VLAN0033
  Spanning tree enabled protocol ieee
  Root ID    Priority    32801
             Address     0002.17D0.179B
             Cost        19
             Port        23(FastEthernet0/23)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32801  (priority 32768 sys-id-ext 33)
 --More--
```

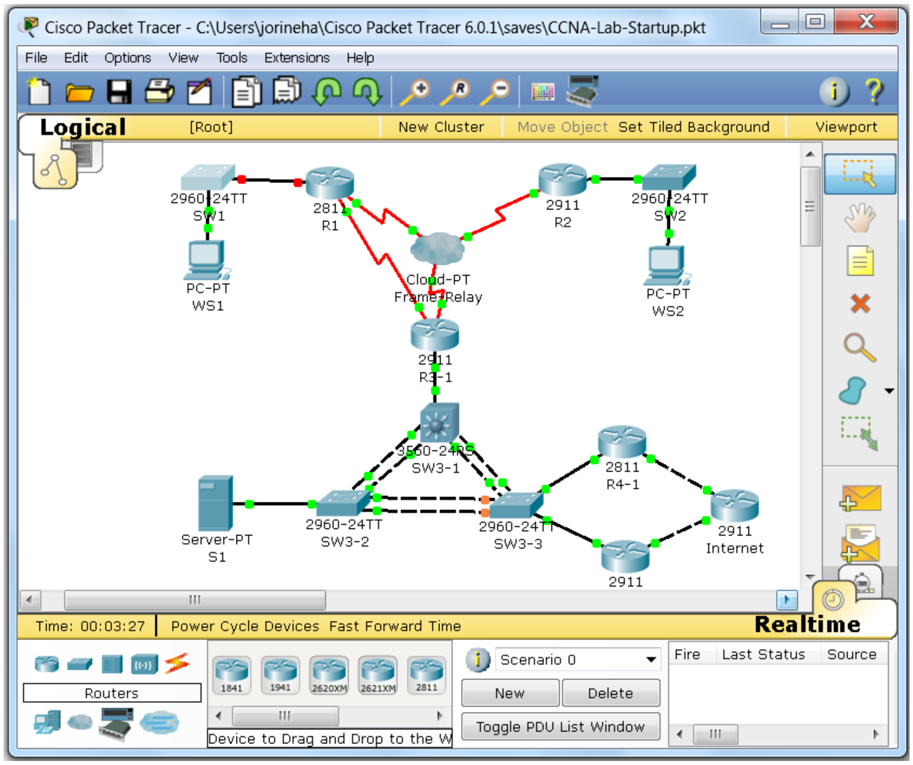
- **Make S3-1 the root switch:** To force a specific switch to become the STP root, you can change the priority setting, either using of the methods outlined below :

    - **Priority command**: An older method for specifying the root bridge is through the use of the **spanning-tree vlan <range> priority <0-61440>** command. This manually changes the default priority (32801 is shown above), so setting this parameter to anything below the current root switch's priority would make the new switch root.
    - **Root primary/secondary:** Another form of the previous command accomplishes the same result, but is a more of a macro than a command per se. The format of this command is **spanning-tree vlan <range> root primary**. Issue the following version of the command to make SW3-1 to become root: **spanning-tree vlan 1,33,34 root primary**.

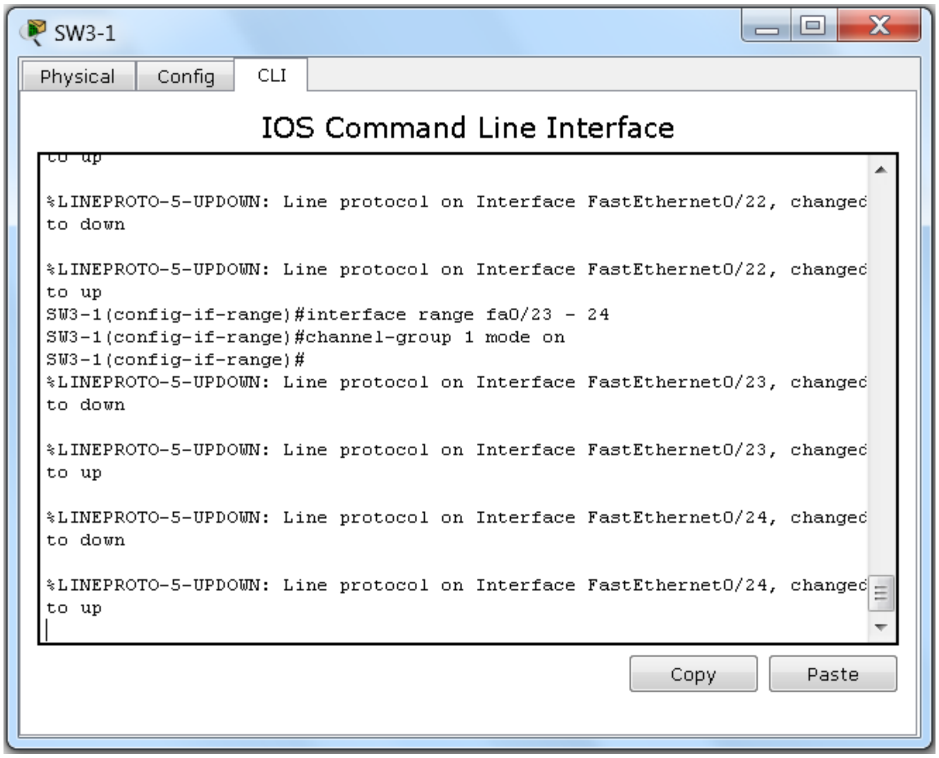
- **Verify that SW3-1 has become root**: Exit global configuration mode and return to privileged exec mode. Issue the command **show spanning-tree**; you should now see "**This bridge is the root**," as well as all ports in forwarding state.
- **Save the configuration**: At your discretion, you can use **copy running-config startup-config** to save your changes, or simply the command **write mem**. On an actual router or 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.

3.1.2. Configure 802.1d Spanning-Tree Enhancements in Site 3

Spanning-Tree Protocol (IEEE standard 802.1d) certainly fulfills its purpose in building a loop-free Layer 2 topology, but does so at a high price: Convergence requires a ***minimum*** of 50 seconds (MaxAge of 20 seconds + 2 x Forward Delay of 15 seconds, for a total of 50 seconds). To counteract these drawbacks, Cisco introduced several enhancements to STP. Since Spanning-Tree is running in Site 3, configuration exercises will take place there, shown below for reference.


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCNA-Lab-Startup.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
2960-24TT SW1
2811 R1
2911 R2
2960-24TT SW2
PC-PT WS1
Cloud-PT Frame Relay
PC-PT WS2
2911 R3-1
3560-24PS SW3-1
2811 R4-1
Server-PT S1
2960-24TT SW3-2
2960-24TT SW3-3
2911 Internet
2911
Time: 00:03:27 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811
Device to Drag and Drop to the W
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source

- **Configure Etherchannel on SW3-1:** To prevent forcing an STP topology change on changes between SW3-1 and its neighboring switches, configure Etherchannel on those trunk links using the process below:



```
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed
to up
SW3-1(config-if-range)#interface range fa0/23 - 24
SW3-1(config-if-range)#channel-group 1 mode on
SW3-1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed
to up
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range fa0/21 – 22 command** (these are the links to SW3-3)
- **Enable Etherchannel on Fa0/21 and Fa0/22:** Create the link bundle using the command **channel-group 1 mode on**. This will create a new logical Layer 2 interface called a port-channel.
- **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range fa0/23 – 24 command** (these are the links to SW3-2)
- **Enable Etherchannel on Fa0/23 and Fa0/24:** Create the link bundle using the command **channel-group 2 mode on**. This will create a second port-channel interface.
- **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 or 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.

- **Configure Etherchannel on SW3-2:** Repeat the previous steps on SW 3-2 as follows:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range fa0/21 – 22 command** (these are the links to SW3-1)
    - **Enable Etherchannel on Fa0/21 and Fa0/22:** Create the link bundle using the command **channel-group 1 mode on**. This will create a new logical Layer 2 interface called a port-channel, and match the configuration on SW3-1.
    - **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range Gi1/1 – 2 command** (these are the links to SW3-3)
    - **Enable Etherchannel on Gi1/1 and Gi1/2:** Create the link bundle using the command **channel-group 3 mode on**. This will create a second port-channel interface.
    - **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 or 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.

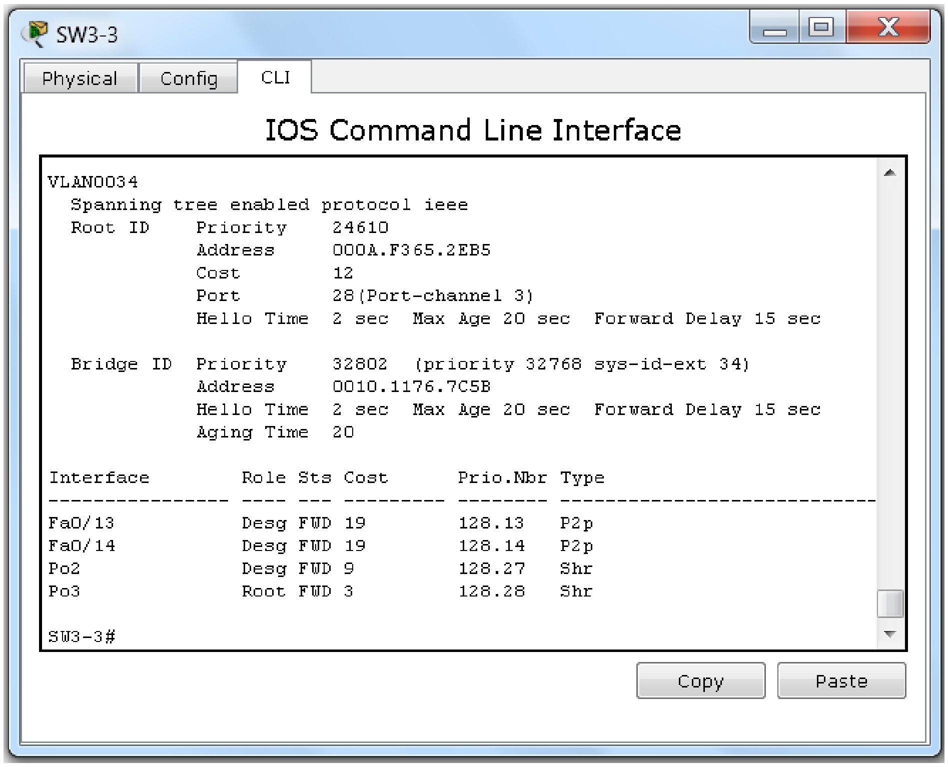
- **Configure Etherchannel on SW3-3:** Repeat the previous steps on SW3-1 and SW3-2 as follows:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range fa0/21 – 22 command** (these are the links to SW3-1)
    - **Enable Etherchannel on Fa0/21 and Fa0/22:** Create the link bundle using the command **channel-group 2 mode on**. This will create a

new logical Layer 2 interface called a port-channel, and match the configuration on SW3-1.

- **Enter interface configuration mode:** To simplify entering identical configurations on each set of interfaces, use the **interface range Gi1/1 – 2 command** (these are the links to SW3-2)
- **Enable Etherchannel on Gi1/1 and Gi1/2:** Create the link bundle using the command **channel-group 3 mode on**. This will create a second port-channel interface.
- **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 or 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.

- **Verify the Etherchannel Configurations on SW3-3**

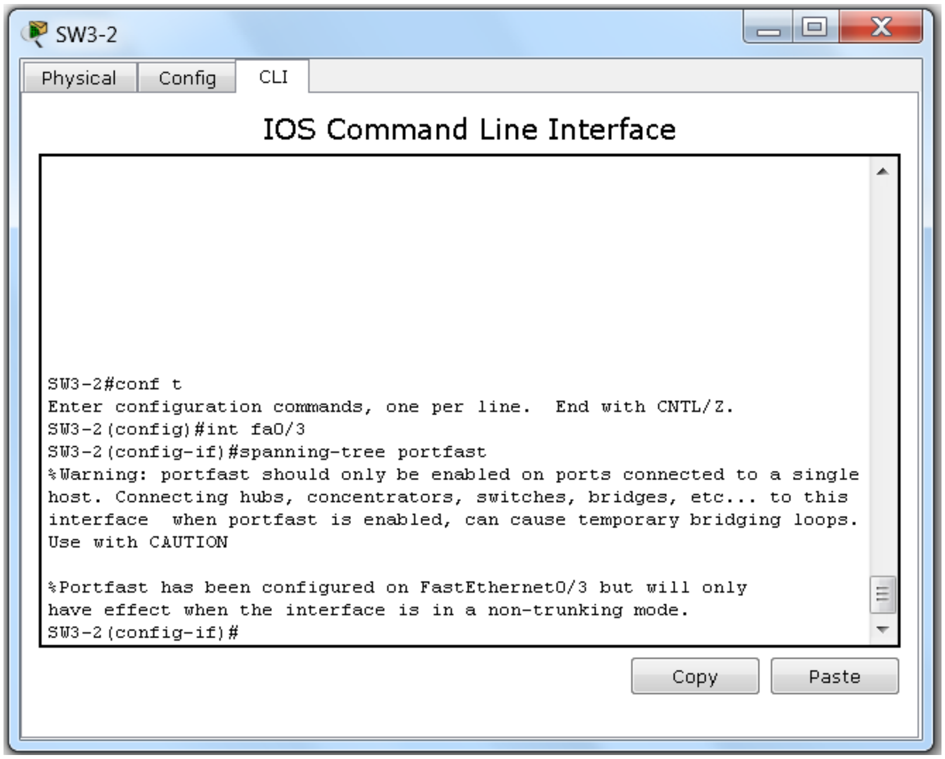


```
VLAN0034
  Spanning tree enabled protocol ieee
  Root ID    Priority    24610
             Address     000A.F365.2EB5
             Cost        12
             Port        28(Port-channel 3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32802  (priority 32768 sys-id-ext 34)
             Address     0010.1176.7C5B
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/13           Desg FWD 19        128.13   P2p
Fa0/14           Desg FWD 19        128.14   P2p
Po2              Desg FWD 9         128.27   Shr
Po3              Root FWD 3         128.28   Shr

SW3-3#
```

- **Display Spanning-Tree Data**: To verify that the Etherchannel (Port-Channel) are functioning as expected in Spanning-Tree, issue the **show spanning-tree** command at the CLI in privileged mode. You should see Fa0/13 and Fa0/14 (links to R4-1/R4-2 respectively), but also Po2 (Port-Channel 2) and Po3 (Port-Channel 3) on all VLANS.

That indicates that the Etherchannel configuration is operational. If these ports as missing, repeat the previous steps to correct any problems.

- **Configure Portfast on SW3-2:** Running Spanning-Tree on switch ports attached to end nodes (e.g., workstations, servers, etc.) is unnecessary, and can be mitigated using Portfast. Portfast bypasses the listening and learning states and places the port immediately into forwarding state. Configure this feature on Fa0/3 (the link to S3) using these steps:



```
SW3-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3-2(config)#int fa0/3
SW3-2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
SW3-2(config-if)#
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter interface configuration mode:** Enter the interface configuration with the command interface **Fa0/3**.
  - **Activate Portfast on Fa0/3:** To enable Portfast on the interface to Server 3 (S3), issue the command **spanning-tree portfast**. You can safely ignore the warning, though remember that the bpduguard feature can be enabled to prevent the port from creating bridging loops.

- **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 or 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.

  **** Note that Packet Tracer 6.0.1 does not currently support Uplinkfast or Backbonefast ****

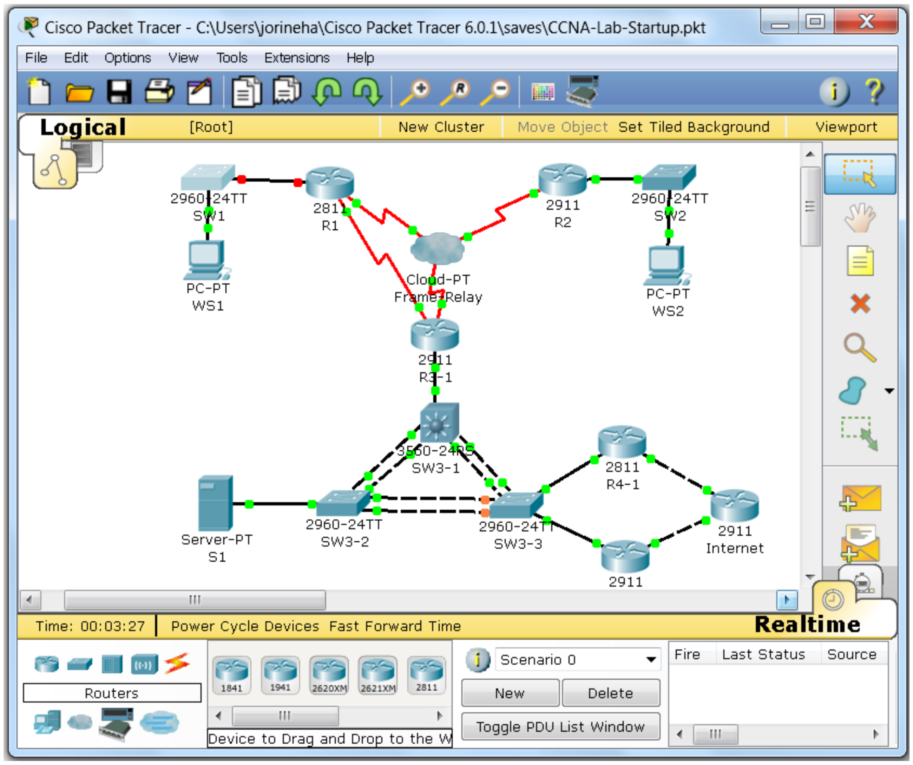
Lesson 3 Lab Exercises

4.1 RSTP Configuration Exercises

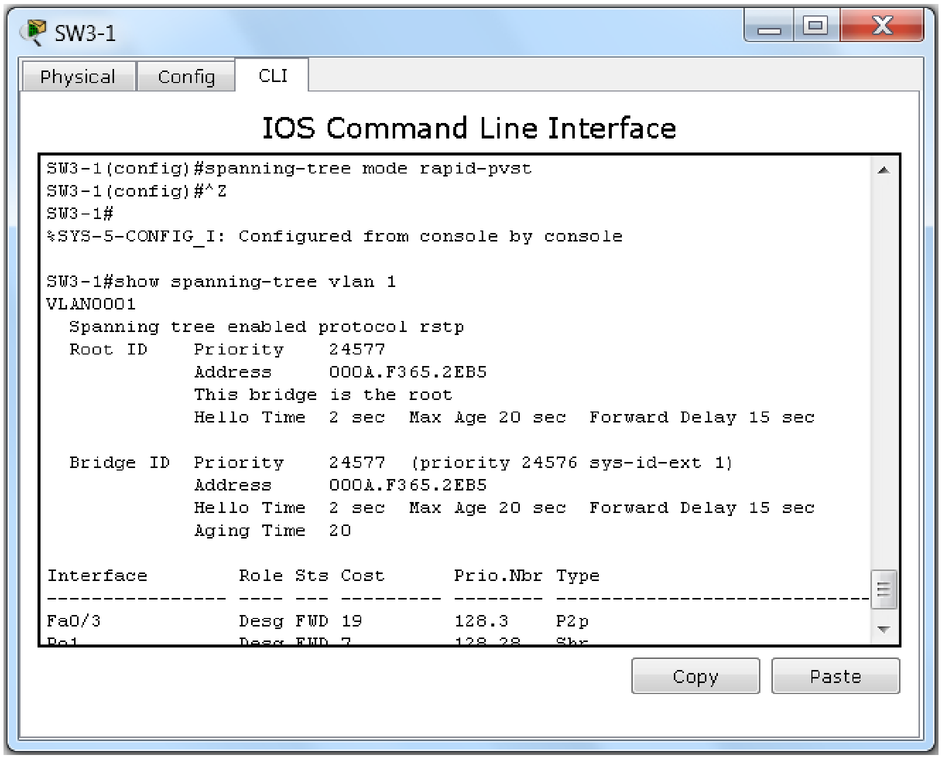
At one time, 802.1d Spanning-Tree Protocol represented an engineering breakthrough, but as networks grew, network engineers started to realize its limitations. As previously mentioned, Cisco introduced enhancements to mitigate some of the obvious shortcomings (e.g., Etherchannel, Portfast, Uplinkfast, etc.), but these were proprietary solutions. In 2001, the IEEE incorporated these enhancements and designated it as 802.1w Rapid Spanning-Tree Protocol (RSTP). While backwards compatibility was built into 802.1w, it represented a major step forward, as well as an update to 802.1d STP.

4.1.1. Convert all Switches in Site 3 to RSTP

Due to its comparative age and technical limitations, most engineers would naturally want to migrate any existing Spanning-Tree instances to RSTP. Cisco's specific implementation of RSTP creates separate instances per VLAN, which is why you will typically hear it referred to as Rapid-PVST. To begin the conversion process on the switches in site 3, open Packet Tracer and click on SW3-1, as displayed below:



- **Change the Operating Mode of the Switches to RSTP:** Converting Cisco switches to RSTP is a simple matter, although older switches do not support this functionality (e.g., the Catalyst 2900XL series is an example). Perform this task as follows:



```
SW3-1(config)#spanning-tree mode rapid-pvst
SW3-1(config)#^Z
SW3-1#
%SYS-5-CONFIG_I: Configured from console by console

SW3-1#show spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     000A.F365.2EB5
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     000A.F365.2EB5
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------------
Fa0/3            Desg FWD 19        128.3    P2p
Po1              Desg FWD 7         128.28   Shr
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Display Spanning-Tree configuration options**: In global configuration mode, enter the command **spanning-tree mode ?**, which will display pvst (802.1d STP) and rapid-pvst (802.1w RSTP). Another option not supported in Packet Tracer but present in most Cisco switches is 802.1s Multiple Spanning-Tree Protocol.
- **Complete the configuration:** Enter the command **spanning-tree mode rapid-pvst**.
- **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.
- **Verify RSTP operation**: From privileged mode, issue the command show spanning-tree, and look for the statement ***spanning tree enabled protocol rstp***.

- **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 or 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.

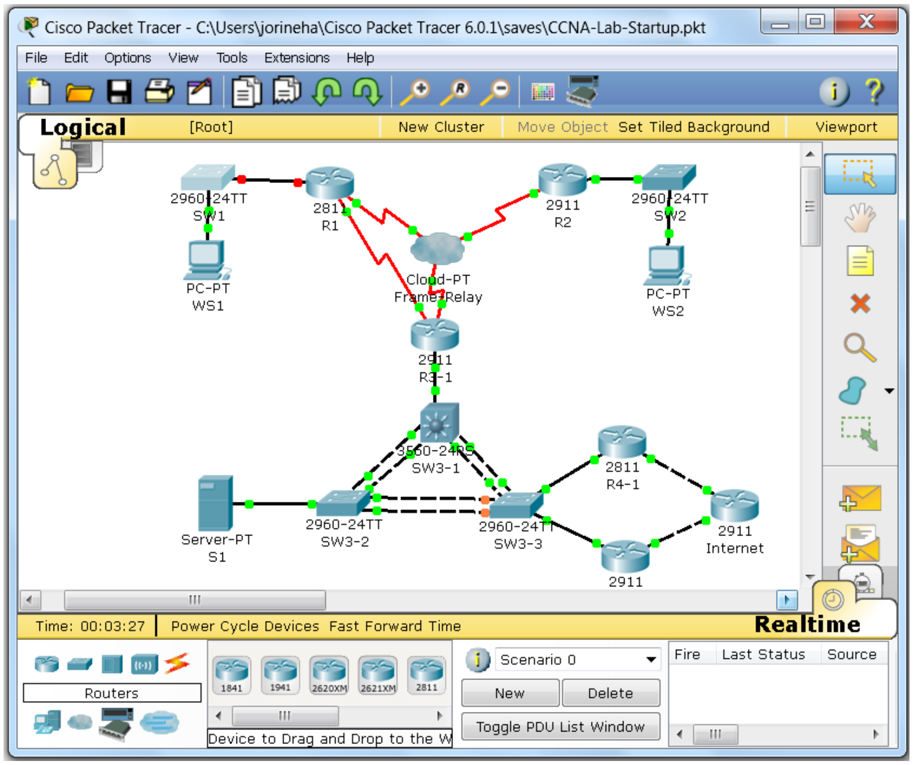
Lesson 4 Lab Exercises

5.1 Basic Access-List Configuration Exercises

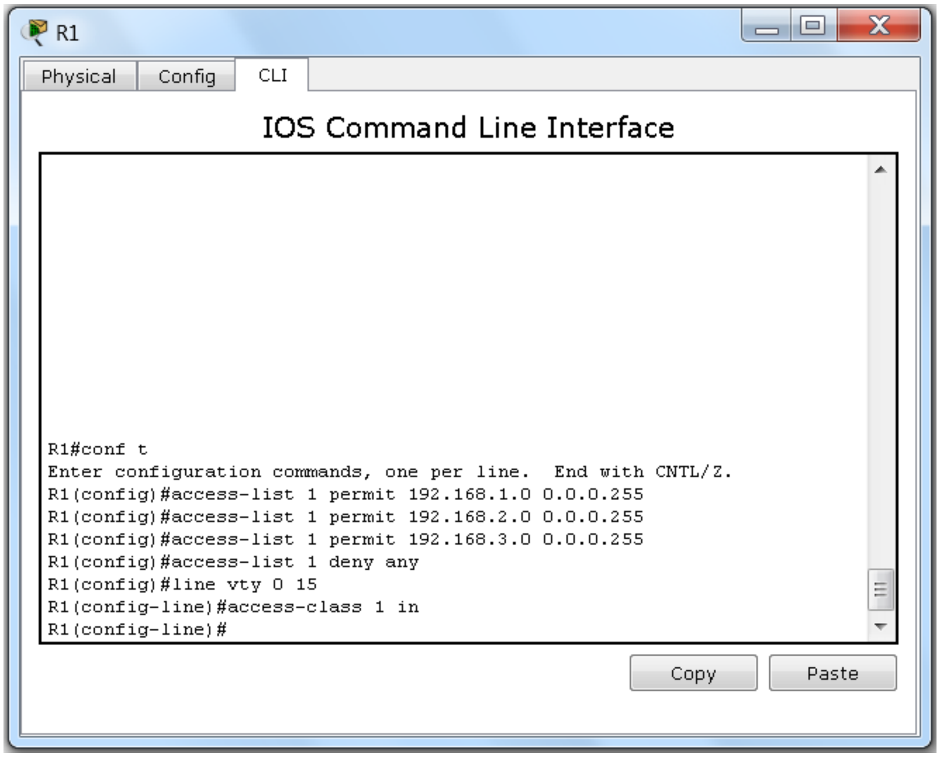
In the world of Cisco networking, access-lists are one of the most frequently used configuration elements, and used for security, NAT, VPN's, and a wide variety of other uses. While the next lesson (Lesson 5, Cisco Access-Lists) covers these in much greater detail, you should begin to get familiar with the fundamentals of this feature.

5.1.1. Restrict Remote Access to Lab Devices

One of the more specific uses of an access-list is to enforce device access to potential users. In order to get comfortable with this feature, you will configure access restrictions as a security measure, on devices in the lab. To start this, open Packet Tracer and click on R1, as displayed below:



- **Create and Apply an Access-List to allow only Management VLAN Access:** There are three management VLANs in the lab topology, at each site. In Site 1, this subnet is 192.168.1.0/24, for Site 2 the network is 192.168.2.0/24, and in Site 3 the address range is 192.168.3.0/24. Create and apply an access-list that will restrict remote access only to devices in one of these three networks. Perform this task as follows:

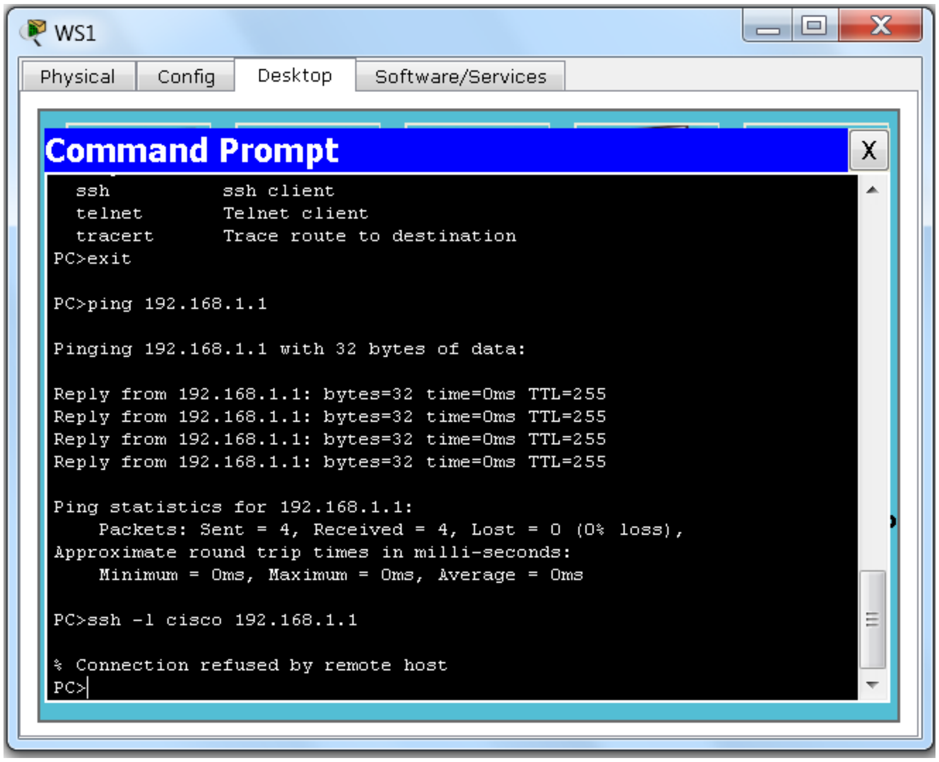


```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.2.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.3.0 0.0.0.255
R1(config)#access-list 1 deny any
R1(config)#line vty 0 15
R1(config-line)#access-class 1 in
R1(config-line)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
- **Create an Access List Entry for Site 1:** In global configuration mode, specify the 192.168.1.0/24 network with the command **access-list 1 permit 192.168.1.0 0.0.0.255** (the wildcard mask is the inverse of a subnet mask, so 255.255.255.0 would read as 0.0.0255 as shown above).
- **Create an Access List Entry for Site 2:** In global configuration mode, specify the 192.168.2.0/24 network with the command **access-list 1 permit 192.168.2.0 0.0.0.255**.
- **Create an Access List Entry for Site 3:** In global configuration mode, specify the 192.168.3.0/24 network with the command **access-list 1 permit 192.168.3.0 0.0.0.255**.
- **Create an Access-List Entry Blocking All Other Addresses**: If none of the previously configured addresses match the source of a remote access session, the session will be blocked/denied. Though this is already present implicitly in access-lists, use the statement **access-list 1 deny any** to explicitly identify it.
- **Enter VTY Line Configuration Mode**: Enter into line configuration mode using the command **line vty 0 15**.

- **Apply the Access-List Filter to the Router's virtual terminal lines**: Creating an access-list does not filter any traffic, unless that list is applied. To restrict traffic to remote CLI access, apply the access list to the VTY lines using the statement **access-class 1 in** ("in" refers to the direction of traffic, in this case, inbound to R1)
- **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 or 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.

- **Test the Access-List:** In order to verify if the traffic restriction is operating correctly, you will need to perform testing. Test the access-list functionality using the following steps:



```
  ssh          ssh client
  telnet       Telnet client
  tracert      Trace route to destination
PC>exit

PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ssh -l cisco 192.168.1.1

% Connection refused by remote host
PC>
```

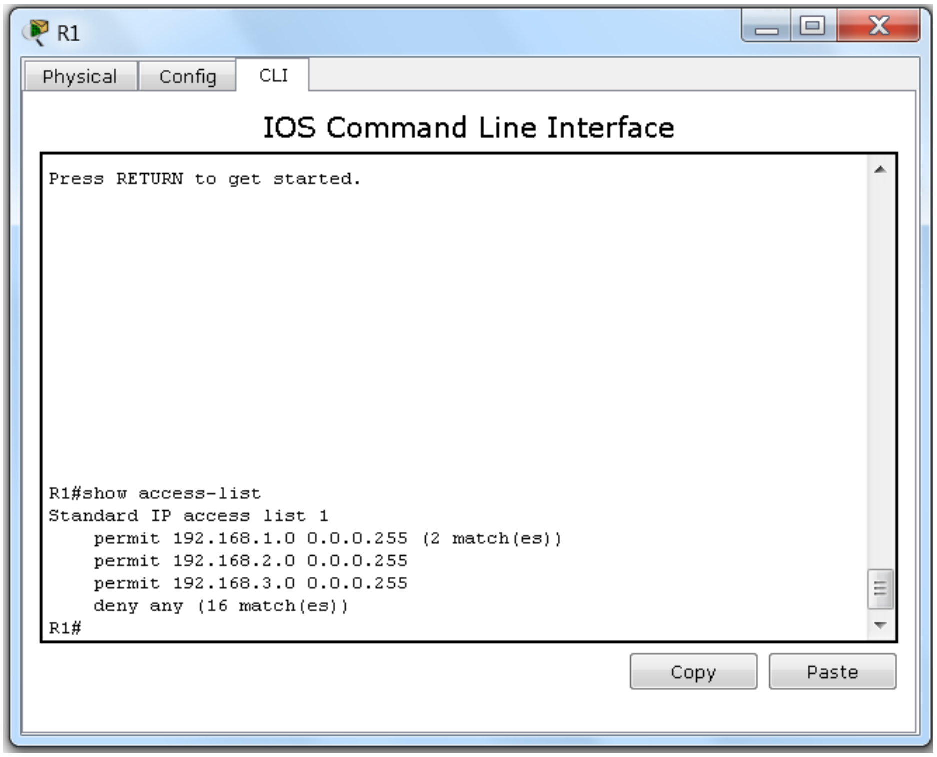
- **Access the Command Prompt on Workstation 1 in Site 1**: Click on the packet Tracer icon for Workstation 1 (WS1) and navigate to the ***Desktop*** Tab. From the many selections on the page, select and click on the **Command Prompt** icon.

- **Ping R1's Management VLAN Interface from WS1**: To confirm that you have connectivity between WS1 (which is on network 192.168.11.0/24) and R1 (which is on both the Management and Production VLANs), use the **ping 192.168.1.1** command. The output should be successful and match the graphic above.
- **Attempt to Establish an SSH Session to R1 from WS1:** To access R1 using SSH, use the CLI command **ssh –l cisco 192.168.1.1**. If the filter is working correctly you will receive the response ***Connection refused by remote host***. Close the command prompt window.
- **Access SW1 in Site 1:** To perform a second test, click on the SW1 icon in Packet Tracer and select the CLI tab. Press **<enter>** to activate a CLI session (you should not have to log in, since the console line is set to not require it).
- **Ping R1's Management VLAN Interface from SW1**: SW1 and R1 share the same Management VLAN (192.168.1.0/24), but confirm that connectivity is in place. Issue the command **ping 192.168.1.1** which should be successful.
- **Attempt to Establish an SSH Session to R1 from SW1:** To access R1 using SSH, use the CLI command **ssh –l cisco 192.168.1.1**. If the filter has been configured correctly, you should see a password prompt. Type in **cisco** and press **<enter>**. You should now see the familiar user exec prompt of **R1>**.
- **Close the SSH Session and Log Out of SW1**: Use the exit command to close the SSH session and close the SW1 window.
- **Log into R1 Again**: Click on the Packet Tracer R1 icon and select the CLI tab (if not already open).
- **Display the Access-List Counters**: Both the successful and unsuccessful login attempts will generate an increment to the access-list counter. Display the counter using the **show access-list** or **show access-list 1** commands. Both the ***permit 192.168.1.0*** and ***deny any*** entries should have some value other than zero, similar to the output below.

- **Optionally, configure the identical filters on the remaining Cisco devices in the lab**: If desired, duplicate the configuration used on R1 on the remaining devices in the lab, as follows:

  - SW1
  - R2
  - SW2
  - R3-1
  - SW3-1

- SW3-2
- SW3-3
- R4-1
- R4-2



```
Press RETURN to get started.









R1#show access-list
Standard IP access list 1
    permit 192.168.1.0 0.0.0.255 (2 match(es))
    permit 192.168.2.0 0.0.0.255
    permit 192.168.3.0 0.0.0.255
    deny any (16 match(es))
R1#
```

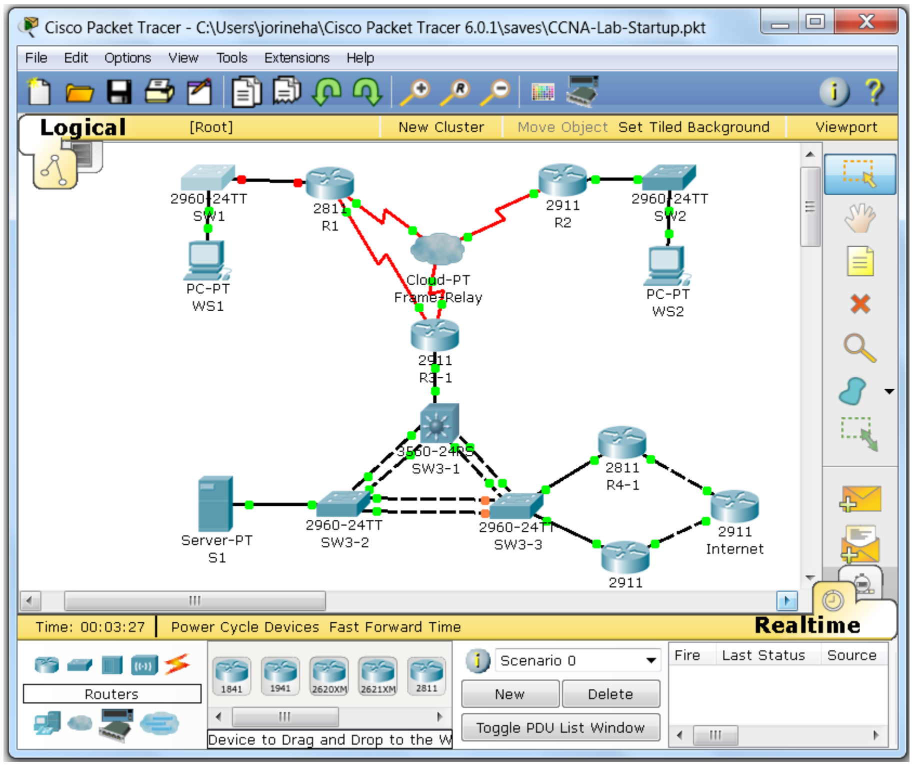
Lesson 5 Lab Exercises

6.1 Cisco Access-List Configuration Exercises

In the previous lab exercise, you used a simple (standard) access to prevent remote access from any other address than the Management VLANs in the lab topology. In this set of labs, you will use standard and extended access-lists to perform more granular traffic filtering.

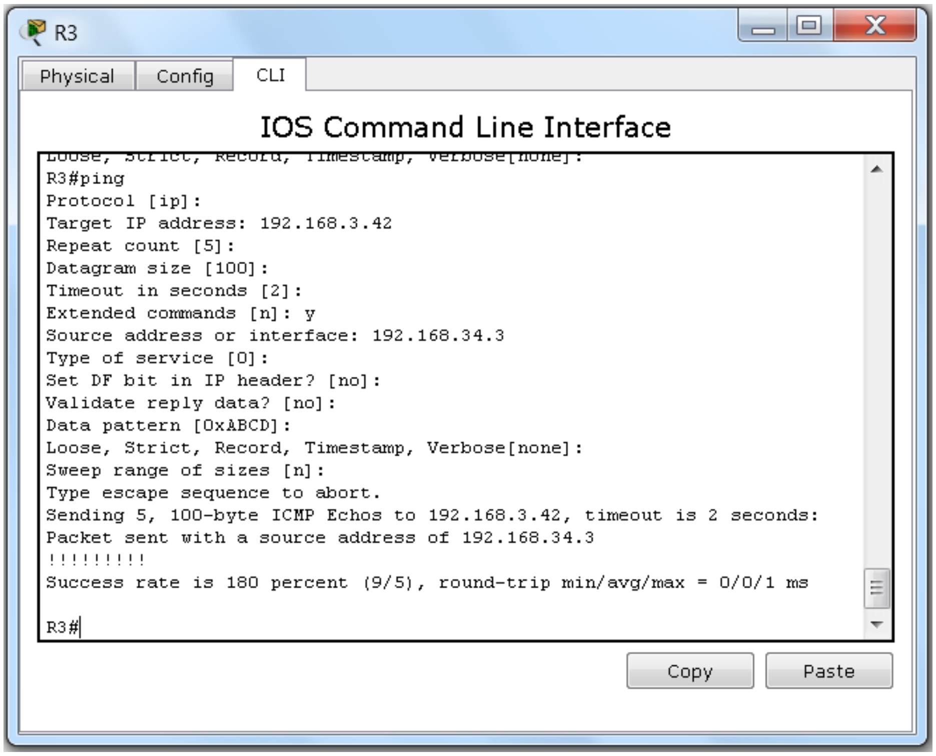
6.1.1. Restrict ICMP Between R3-1 and R4-2

Access-lists are one of the most flexible packet filters available to a Cisco network engineer, and knowing how to use them properly is essential to mastering CCNA-level skills. To use access-lists for packet filtering, select R3-1 in Packet Tracer as follows:



- **Create and Apply a Standard Numbered Access-List Prevent ICMP from R3-1 to R4-2:** Standard access-lists can be configured as numbered (1-99) or named, and match packets based on ***source addresses*** only. While this can certainly be helpful (as demonstrated in the previous lab), this type of access-list is not very granular. To demonstrate this, create and apply an access-list that will restrict all traffic to the

Management VLAN of R4-2 to only the 192.168.3.0/24 subnet. Perform this task as follows:



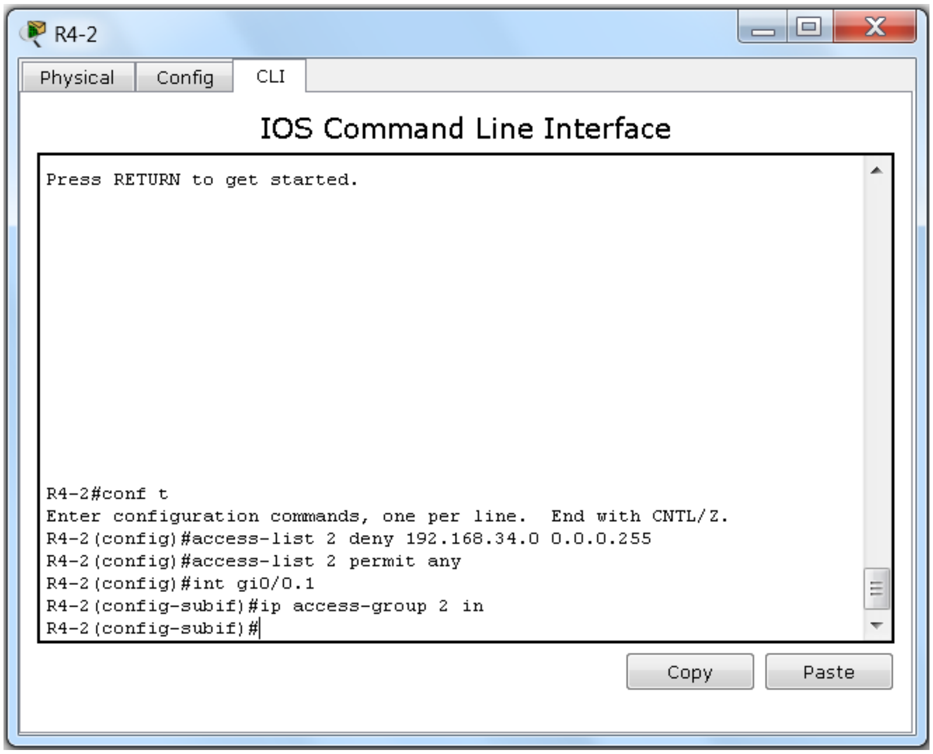
```
Loose, Strict, Record, Timestamp, Verbose[none]:
R3#ping
Protocol [ip]:
Target IP address: 192.168.3.42
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.34.3
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply 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 192.168.3.42, timeout is 2 seconds:
Packet sent with a source address of 192.168.34.3
!!!!!!!!!
Success rate is 180 percent (9/5), round-trip min/avg/max = 0/0/1 ms

R3#
```

- **Verify Connectivity Between VLAN 34 on R3-1 and VLAN 3 on R4-2:** Network best practices dictate the need to test the health and connectivity of networks before attempting tasks similar to the one required here. Select the CLI window of R3-1, and perform an extended ping which will allow you to specify the source network. Issue the command **ping** at the CLI and supply the values below for the test:

  - **Protocol**: IP (the default, simply press **<enter>**)
  - **Target IP Address**: 192.168.3.42
  - **Repeat count**: 5 (the default, simply press **<enter>**)
  - **Datagram size**: 100 (the default, simply press **<enter>**)
  - **Timeout in Seconds**: 2 (the default, simply press **<enter>**)
  - **Extended commands**: Enter **Y** and press **<enter>**
  - **Source address or interface**: 192.168.34.3
  - **Type of service**: 0 (the default, simply press **<enter>**)
  - **Set DF bit in IP Header**: no (the default, simply press **<enter>**)

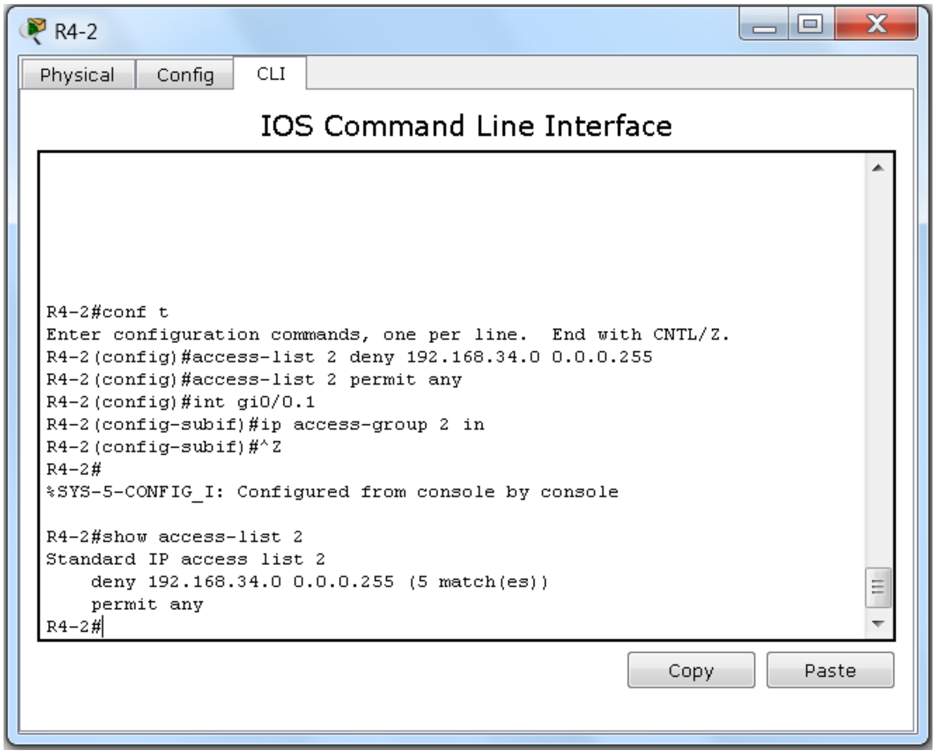
- **Validate reply data:** no (the default, simply press **<enter>**)
- **Data pattern:** 0xABCD (the default, simply press **<enter>**)
- **Loose, Strict, Record, Timestamp, Verbose:** none (the default, simply press **<enter>**)
- **Sweep range of sizes:** n (the default, simply press **<enter>**)
- **Result:** Success, though the first packet or two may fail while ARP performs the Layer 3 to Layer 2 mapping

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
- **Create the Packet Filter on R4-2**: In global configuration mode, create a standard access-list on R4-2 (destination) using the commands **access-list 2 deny 192.168.34.0 0.0.0.255** and **access-list 2 permit ip any**
- **Apply the Filter:** To prevent the designated packets from entering the Management VLAN, apply the access-list to the Gi0/0.1 interface with the **ip access-group 2 in** command.



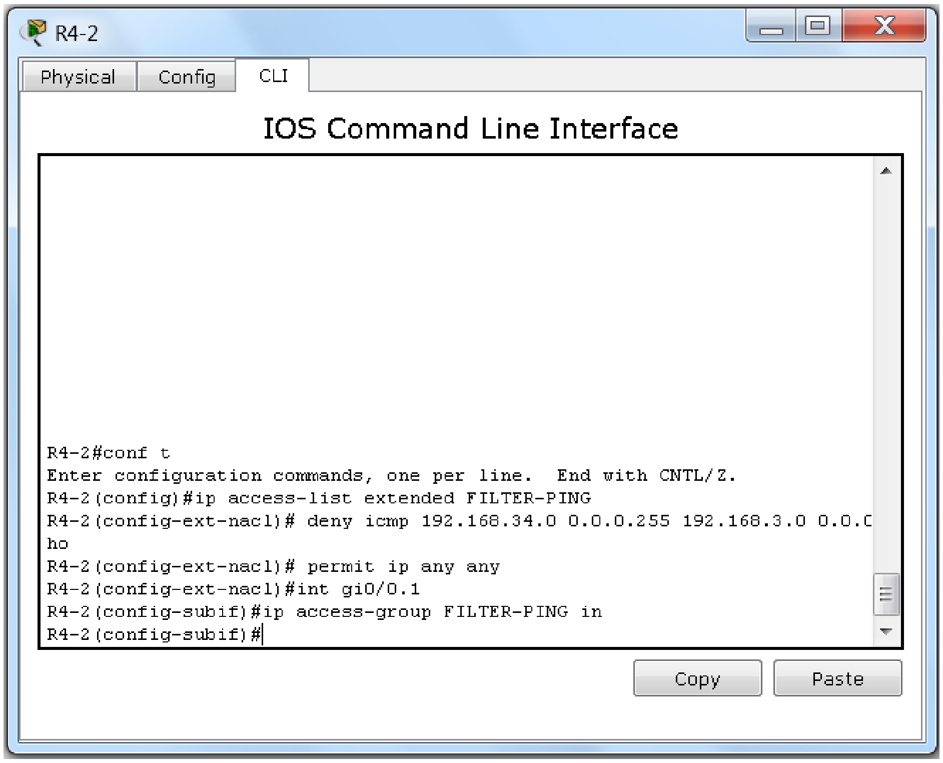
```
Press RETURN to get started.









R4-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-2(config)#access-list 2 deny 192.168.34.0 0.0.0.255
R4-2(config)#access-list 2 permit any
R4-2(config)#int gi0/0.1
R4-2(config-subif)#ip access-group 2 in
R4-2(config-subif)#
```

- **Test the Access-List:** Repeat the previous test using the same settings. This time the ping should fail, with the error message ***UUUUUUUUU*** displayed (U = unreachable)
- **Display the Access-List Counters**: Return to R4-2 and exit configuration mode if necessary. From privileged mode, issue the command **show access-list 2** and verify that the counters for the 192.168.34.0 entry are nonzero.
- **Enter global configuration mode:** Enter configuration mode again using the **configure terminal** command from privileged mode.
- **Enter interface configuration mode:** Enter interface mode with the command **interface Gi0/0.1**.
- **Remove the Filter from the Interface**: Delete the filter using the command **no ip access-group 2**.
- **Delete the Access-List**: Completely delete the access-list from R4-2 by issuing the command **no access-list 2** from global configuration 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 or 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.



```
R4-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-2(config)#access-list 2 deny 192.168.34.0 0.0.0.255
R4-2(config)#access-list 2 permit any
R4-2(config)#int gi0/0.1
R4-2(config-subif)#ip access-group 2 in
R4-2(config-subif)#^Z
R4-2#
%SYS-5-CONFIG_I: Configured from console by console

R4-2#show access-list 2
Standard IP access list 2
    deny 192.168.34.0 0.0.0.255 (5 match(es))
    permit any
R4-2#
```

- **Create and Apply an Extended Named Access-List Prevent ping from R3-1 to R4-2:** In reality, the standard access-list in the previous exercise did not specifically discard ICMP traffic, but rather ***all*** traffic originating from the 192.168.34.0/24 subnet. This does not mean that standard access-lists are ineffective, but rather that their abilities are much more limited. In this exercise, discard ping traffic between 192.168.34.0/24 and 192.168.3.0/24 between R3-1 and R4-2. Configure the access-list on R4-2 using the steps below:

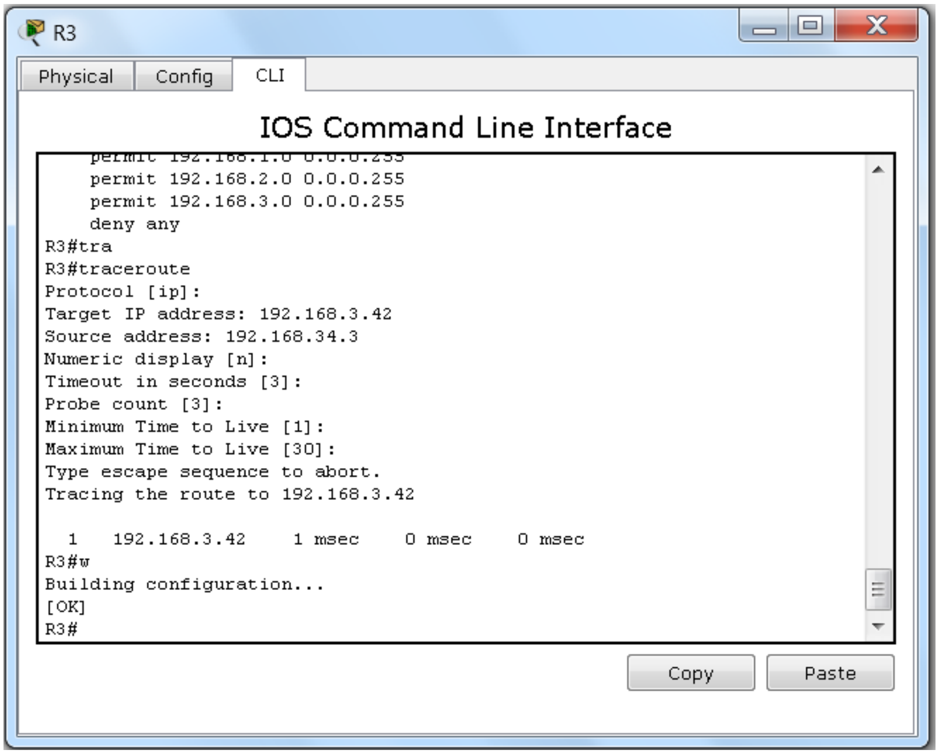


```
R4-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4-2(config)#ip access-list extended FILTER-PING
R4-2(config-ext-nacl)# deny icmp 192.168.34.0 0.0.0.255 192.168.3.0 0.0.C
ho
R4-2(config-ext-nacl)# permit ip any any
R4-2(config-ext-nacl)#int gi0/0.1
R4-2(config-subif)#ip access-group FILTER-PING in
R4-2(config-subif)#
```

  - **Enter global configuration mode:** Enter configuration mode again using the **configure terminal** command from privileged mode.
  - **Create an Extended Named Access-List:** Like standard access-lists, extended access-lists can be configured using a numeric range (100-199) or a name. Create a named access-list using the command **ip access-list extended FILTER-PING**.
  - **Deny Ping Packets between VLAN 34 and VLAN 3**: Filter ICMP echo packets (usually referred to as ping packets) between the designated networks by adding the access-list entry **deny icmp 192.168.34.0 0.0.0.255 192.168.3.0 0.0.0.255 echo**.
  - **Permit all Other ICMP and IP Packets**: Allow all other traffic (including other ICMP packets) by using the **command permit ip any any**.

- **Enter interface configuration mode:** Enter interface mode with the command **interface Gi0/0.1**.
- **Apply the Filter to the Subinterface:** Place the access-list inbound to R4-2 by applying the command **ip access-group FILTER-PING in**.
- **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 or 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.
- **Return to the CLI of R3-1**: Close the access window to R4-2 and open (or reopen) the Packet Tracer Window to R3-1.
- **Verify the Functionality of the Access-List:** As done previously, perform an extended ping which will allow you to specify the source network. Issue the command **ping** at the CLI and supply the values below for the test:

  - **Protocol**: IP (the default, simply press **<enter>**)
  - **Target IP Address**: 192.168.3.42
  - **Repeat count**: 5 (the default, simply press **<enter>**)
  - **Datagram size**: 100 (the default, simply press **<enter>**)
  - **Timeout in Seconds**: 2 (the default, simply press **<enter>**)
  - **Extended commands**: Enter **Y** and press **<enter>**
  - **Source address or interface**: 192.168.34.3
  - **Type of service**: 0 (the default, simply press **<enter>**)
  - **Set DF bit in IP Header**: no (the default, simply press **<enter>**)
  - **Validate reply data:** no (the default, simply press **<enter>**)
  - **Data pattern:** 0xABCD (the default, simply press **<enter>**)
  - **Loose, Strict, Record, Timestamp, Verbose:** none (the default, simply press **<enter>**)
  - **Sweep range of sizes:** n (the default, simply press **<enter>**)
  - **Result:** The ping should fail, with the error message ***UUUUUUUUU*** displayed (U = unreachable)



```
    permit 192.168.1.0 0.0.0.255
    permit 192.168.2.0 0.0.0.255
    permit 192.168.3.0 0.0.0.255
    deny any
R3#tra
R3#traceroute
Protocol [ip]:
Target IP address: 192.168.3.42
Source address: 192.168.34.3
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Type escape sequence to abort.
Tracing the route to 192.168.3.42

  1   192.168.3.42     1 msec     0 msec     0 msec
R3#w
Building configuration...
[OK]
R3#
```

- **Perform an Extended Traceroute**: To demonstrate that other ICMP traffic is permitted by the access-list, perform an extended traceroute on R3-1 with the following options:

  - **Protocol**: IP (the default, simply press **<enter>**)
  - **Target IP Address**: 192.168.3.42
  - **Source IP Address**: 192.168.34.3
  - **Numeric display**: n (the default, simply press **<enter>**)
  - **Timeout in Seconds**: 3 (the default, simply press **<enter>**)
  - **Extended commands**: Enter **Y** and press **<enter>**
  - **Source address or interface**: 192.168.34.3
  - **Probe count**: 3 (the default, simply press **<enter>**)
  - **Minimum Time to Live**: 1 (the default, simply press **<enter>**)
  - **Maximum Time to Live:** 30 (the default, simply press **<enter>**)
  - **Result:** The traceroute should succeed, listing a single Layer 3 hop of 192.168.3.42.

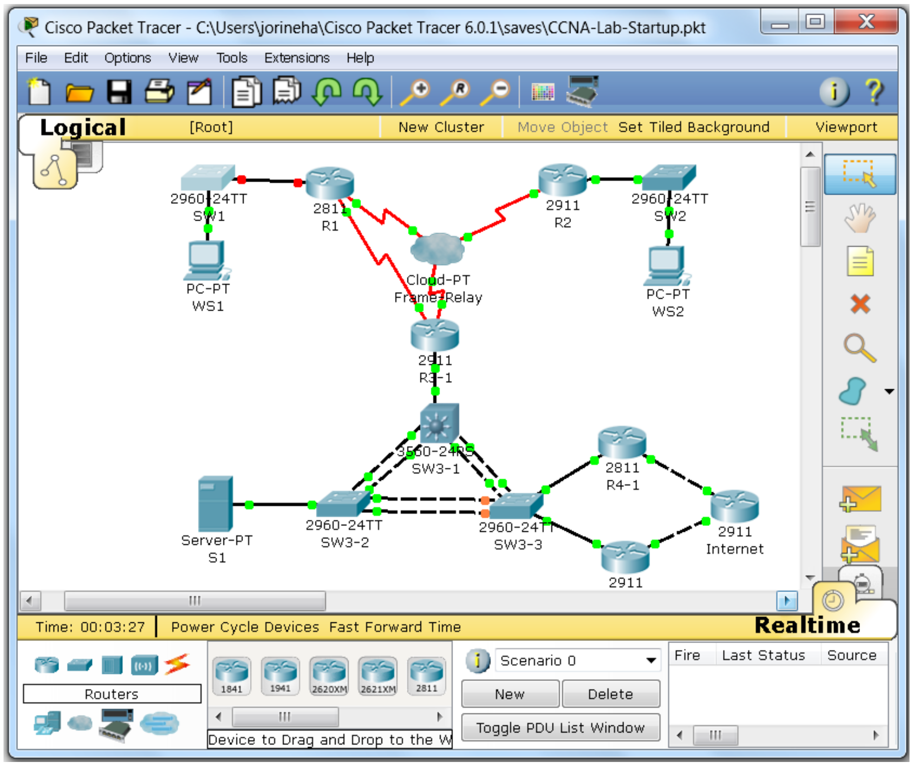
Lesson 6 Lab Exercises

7.1 VLSM/Distance Vector Routing Configuration Exercises

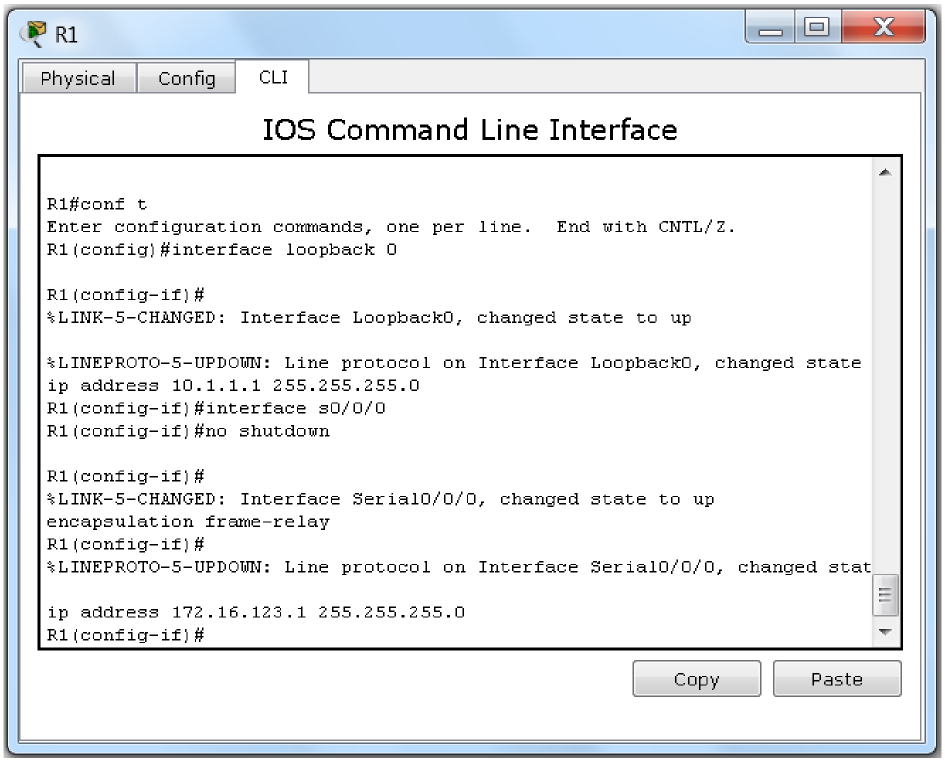
At the core of the ICND2 (and by extension, the CCNA R&S certification) are the principles of IP routing, dynamic routing in particular. Having a thorough understanding of the fundamentals of routing can make the difference between success and failure, not only on the exam, but also in a networking career. In these labs, you will configure distance vector routing using the RIP protocol, and witness firsthand how VLSM support is critical in modern networks.

7.1.1. Configure RIP without VLSM Support (RIP V1)

The first version of Routing Information Protocol only supported classful networks, that is, strictly adhering to the old Class, A, B & C network structure. As such, subnet masks are ***not*** transmitted in routing updates. To understand how this impacts networks, you will configure version 1 of RIP and observe the results. To begin, open Packet Tracer and click on R1:



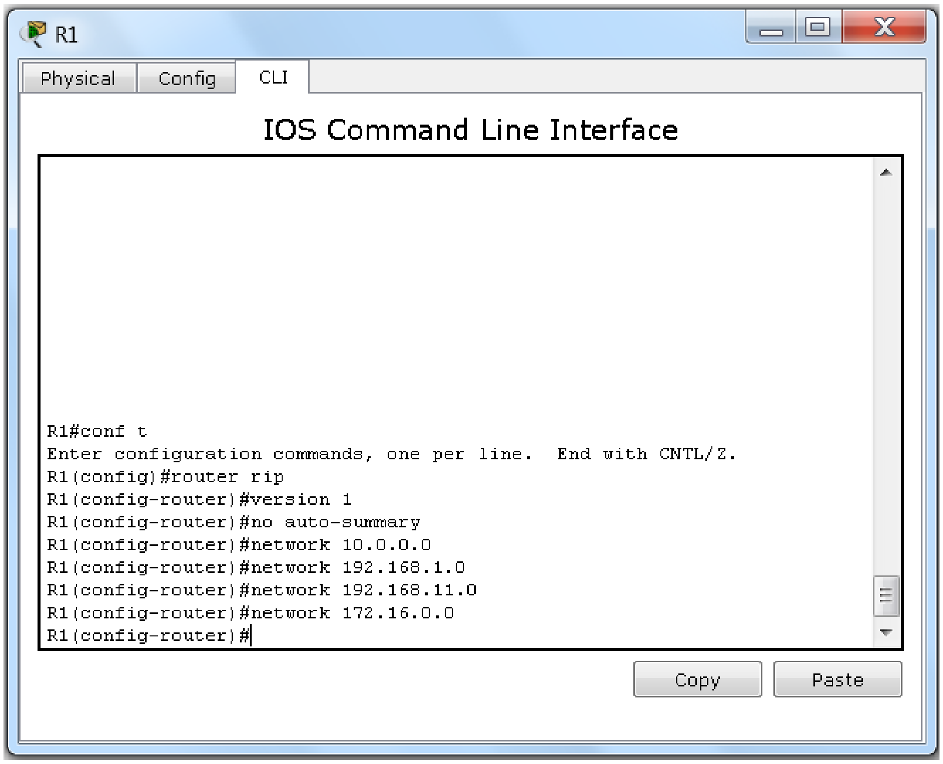
- **Configure Additional Interfaces on R1:** To populate the IP routing table on the other devices in the lab, configure other interfaces on R1, as outlined below:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
ip address 10.1.1.1 255.255.255.0
R1(config-if)#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 172.16.123.1 255.255.255.0
R1(config-if)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Configure a Loopback Interface:** Enter the interface configuration with the command **interface loopback 0**. Assign an address with the command **ip address 10.1.1.1 255.255.255.255**
- **Configure a Serial WAN Interface**: Enter configuration mode for the serial interface using the command **interface Se0/0/0**. Enable the interface with the **no shutdown** command. Set the interface for frame relay operation by entering **encapsulation frame-relay**, and add an ip address with the command **ip address 172.16.123.1 255.255.255.0**.

- **Enable RIP Version 1 Operation on R1**: Begin the RIP routing process as follows:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 1
R1(config-router)#no auto-summary
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

- **Begin the RIP Process**: Start the routing process with the command **router rip**
- **Disable Automatic Summarization**: Enter the **no auto-summary** command in RIP router configuration mode
- **Specify Version 1 (important for this exercise)**: Enter the command **version 1** (otherwise the process will receive V2 messages)
- **Enable RIP on all Interfaces**: Identify the interfaces to participate in the routing process by issuing the following commands:

  - **network 10.0.0.0** (loopback interface)
  - **network 192.168.1.0** (management VLAN)
  - **network 192.168.11.0** (production VLAN)
  - **network 172.16.123.0** (serial interface)

- **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 or 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.

- **Configure Additional Interfaces on R2:** To populate the IP routing table on the other devices in the lab, configure other interfaces on R1, as outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Configure a Loopback Interface:** Enter the interface configuration with the command **interface loopback 0**. Assign an address with the command **ip address 10.2.2.2 255.255.255.255**
  - **Configure a Serial WAN Interface**: Enter configuration mode for the serial interface using the command **interface Se0/0/0**. Enable the interface with the **no shutdown** command. Set the interface for frame relay operation by entering **encapsulation frame-relay**, and add an ip address with the command **ip address 172.16.123.2 255.255.255.0**.

- **Enable RIP Version 1 Operation on R2**: Begin the RIP routing process as follows:

  - **Begin the RIP Process**: Start the routing process with the command **router rip**
  - **Disable Automatic Summarization**: Enter the **no auto-summary** command in RIP router configuration mode
  - **Specify Version 1 (important for this exercise)**: Enter the command **version 1** (otherwise the process will receive V2 messages)
  - **Enable RIP on all Interfaces**: Identify the interfaces to participate in the routing process by issuing the following commands:

    - **network 10.0.0.0** (loopback interface)
    - **network 192.168.2.0** (management VLAN)
    - **network 192.168.22.0** (production VLAN)
    - **network 172.16.123.0** (serial interface)

  - **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 or 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

- **Configure Additional Interfaces on R3-1:** To populate the IP routing table on the other devices in the lab, configure other interfaces on R3-1, as outlined below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Configure a Loopback Interface:** Enter the interface configuration with the command **interface loopback 0**. Assign an address with the command **ip address 10.3.3.3 255.255.255.255**
    - **Configure a Serial WAN Interface**: Enter configuration mode for the serial interface using the command **interface Se0/0/0**. Enable the interface with the **no shutdown** command. Set the interface for frame relay operation by entering **encapsulation frame-relay**, and add an ip address with the command **ip address 172.16.123.3 255.255.255.0**.

- **Enable RIP Version 1 Operation on R3-1**: Begin the RIP routing process as follows:

    - **Begin the RIP Process**: Start the routing process with the command **router rip**
    - **Disable Automatic Summarization**: Enter the **no auto-summary** command in RIP router configuration mode
    - **Specify Version 1 (important for this exercise)**: Enter the command **version 1** (otherwise the process will receive V2 messages)
    - **Enable RIP on all Interfaces**: Identify the interfaces to participate in the routing process by issuing the following commands:

        - **network 10.0.0.0** (loopback interface)
        - **network 192.168.3.0** (management VLAN)
        - **network 192.168.34.0** (production VLAN)
        - **network 172.16.123.0** (serial interface)

    - **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 or 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

- **Configure a Loopback Interface on R4-1:** To populate the IP routing table on the other devices in the lab, configure other interfaces on R1, as outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Configure a Loopback Interface:** Enter the interface configuration with the command **interface loopback 0**. Assign an address with the command **ip address 10.3.4.1 255.255.255.255**

- **Enable RIP Version 1 Operation on R4-1**: Begin the RIP routing process as follows:

  - **Begin the RIP Process**: Start the routing process with the command **router rip**
  - **Disable Automatic Summarization**: Enter the **no auto-summary** command in RIP router configuration mode
  - **Specify Version 1 (important for this exercise)**: Enter the command **version 1** (otherwise the process will receive V2 messages)
  - **Enable RIP on all Interfaces**: Identify the interfaces to participate in the routing process by issuing the following commands:

    - **network 10.0.0.0** (loopback interface)
    - **network 192.168.3.0** (management VLAN)
    - **network 192.168.34.0** (production VLAN)

  - **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 or 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.

- **Configure a Loopback Interface on R4-2:** To populate the IP routing table on the other devices in the lab, configure other interfaces on R1, as outlined below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Configure a Loopback Interface:** Enter the interface configuration with the command **interface loopback 0**. Assign an address with the command **ip address 10.3.4.2 255.255.255.255**

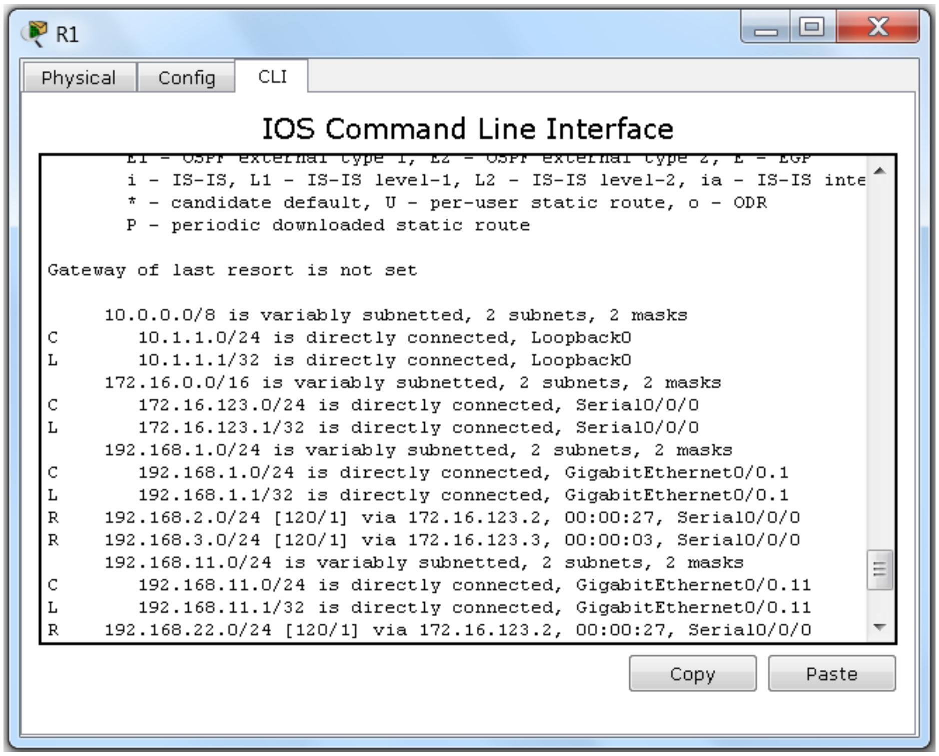
- **Enable RIP Version 1 Operation on R4-2**: Begin the RIP routing process as follows:

    - **Begin the RIP Process**: Start the routing process with the command **router rip**
    - **Disable Automatic Summarization**: Enter the **no auto-summary** command in RIP router configuration mode
    - **Specify Version 1 (important for this exercise)**: Enter the command **version 1** (otherwise the process will receive V2 messages)
    - **Enable RIP on all Interfaces**: Identify the interfaces to participate in the routing process by issuing the following commands:

        - **network 10.0.0.0** (loopback interface)
        - **network 192.168.3.0** (management VLAN)
        - **network 192.168.34.0** (production VLAN)

- **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 or 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.

- **Observe Routing Behavior in the Network**: Open (or reopen) the CLI window to R1 and enter the command **show ip route**. Note the following:
  - **Included routes**: The routes below are contained in the IP routing table:
    - 10.1.1.1/32 (Connected network, class A address)
    - 192.168.1.0/24 (Connected network, class C address)
    - 192.168.11.0/24 (Connected network, class C address)
    - 172.16.123.0/24 (Connected network, class B address)
    - 192.168.2.0/24 (RIP network, class C address)
    - 192.168.22.0/24 (RIP network, class C address)
    - 192.168.3.0/24 (RIP network, class C address)
    - 192.168.34.0/24 (RIP network, class C address)
  - **Missing routes**: The routes listed below are expected but missing from the IP routing table:
    - 10.2.2.2/32 (Connected network, class A address)
    - 10.3.3.3/32 (Connected network, class A address)
    - 10.3.4.1/32 (Connected network, class A address)
    - 10.3.4.2/32 (Connected network, class A address)



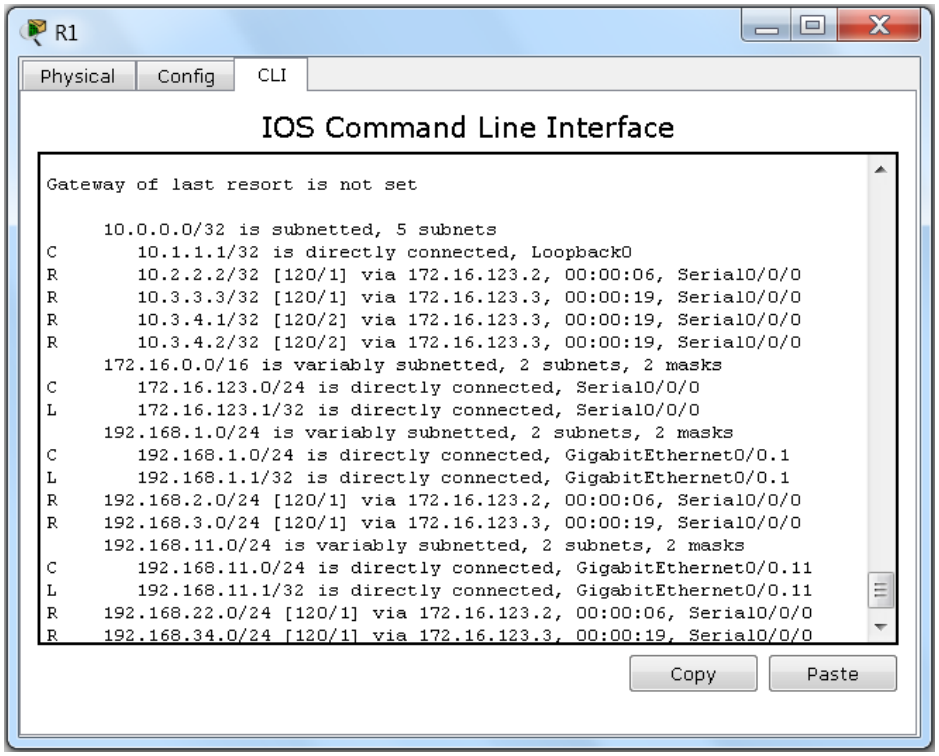
```
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inte
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback0
L       10.1.1.1/32 is directly connected, Loopback0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.123.0/24 is directly connected, Serial0/0/0
L       172.16.123.1/32 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0.1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.1
R    192.168.2.0/24 [120/1] via 172.16.123.2, 00:00:27, Serial0/0/0
R    192.168.3.0/24 [120/1] via 172.16.123.3, 00:00:03, Serial0/0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0.11
L       192.168.11.1/32 is directly connected, GigabitEthernet0/0.11
R    192.168.22.0/24 [120/1] via 172.16.123.2, 00:00:27, Serial0/0/0
```

- **Classful (non-VLSM/CIDR) Behavior**: Because RIP is running in version 1, only class-based networks are advertised. In addition, since the 10.0.0.0 is present in the routing table, any of the other subnetted networks (such as the missing loopback interface addresses) will not appear. In addition, the 172.16.123.0/24 network will appear in the routing tables of R4-1 and R4-2 as the classful network 172.16.0.0/16. RIP version 1 cannot transmit, process, or understand subnetted networks, which demonstrates its obvious limitations.

- **Change Routing to RIP Version 2:** To demonstrate the differences between classful and classless networks, log into all the routers in the network and perform the following configuration changes:

  - **Enter configuration mode**: Enter into global configuration mode with the **configure terminal** or **config t** command.
  - **Enter router configuration mode**: Enter into RIP routing configuration mode by entering **router rip**.
  - **Change RIP to Version 2 (classless)**: Change the routing version to 2 with the command **version 2**.
  - **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 or 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
  - **Repeat this process on all routers:** Beginning with R1, apply these changes throughout the network, as outlines above

- **Observe Changes in Routing Behavior in the Network**: Open (or reopen) the CLI window and enter the command **show ip route**. Note the following changes:



```
Gateway of last resort is not set

     10.0.0.0/32 is subnetted, 5 subnets
C       10.1.1.1/32 is directly connected, Loopback0
R       10.2.2.2/32 [120/1] via 172.16.123.2, 00:00:06, Serial0/0/0
R       10.3.3.3/32 [120/1] via 172.16.123.3, 00:00:19, Serial0/0/0
R       10.3.4.1/32 [120/2] via 172.16.123.3, 00:00:19, Serial0/0/0
R       10.3.4.2/32 [120/2] via 172.16.123.3, 00:00:19, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.123.0/24 is directly connected, Serial0/0/0
L       172.16.123.1/32 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0.1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.1
R    192.168.2.0/24 [120/1] via 172.16.123.2, 00:00:06, Serial0/0/0
R    192.168.3.0/24 [120/1] via 172.16.123.3, 00:00:19, Serial0/0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0.11
L       192.168.11.1/32 is directly connected, GigabitEthernet0/0.11
R    192.168.22.0/24 [120/1] via 172.16.123.2, 00:00:06, Serial0/0/0
R    192.168.34.0/24 [120/1] via 172.16.123.3, 00:00:19, Serial0/0/0
```

- **Included routes**: The routes below are contained in the IP routing table:

  - 10.1.1.1/32 (Connected network)
  - 192.168.1.0/24 (Connected network)
  - 192.168.11.0/24 (Connected network)
  - 172.16.123.0/24 (Connected network)
  - 10.2.2.2/32 (RIP network)
  - 10.3.3.3/32 (RIP network)
  - 10.3.4.1/32 (RIP network)
  - 10.3.4.2/32 (Connected network)
  - 192.168.2.0/24 (RIP network)
  - 192.168.22.0/24 (RIP network)
  - 192.168.3.0/24 (RIP network)
  - 192.168.34.0/24 (RIP network)

- **Missing routes**: None, because subnetted networks are supported.
- **Classless (VLSM/CIDR) Behavior**: In version 2, RIP can understand and advertise subnetted networks, avoiding both wasted address space as well as fuller route inclusion.

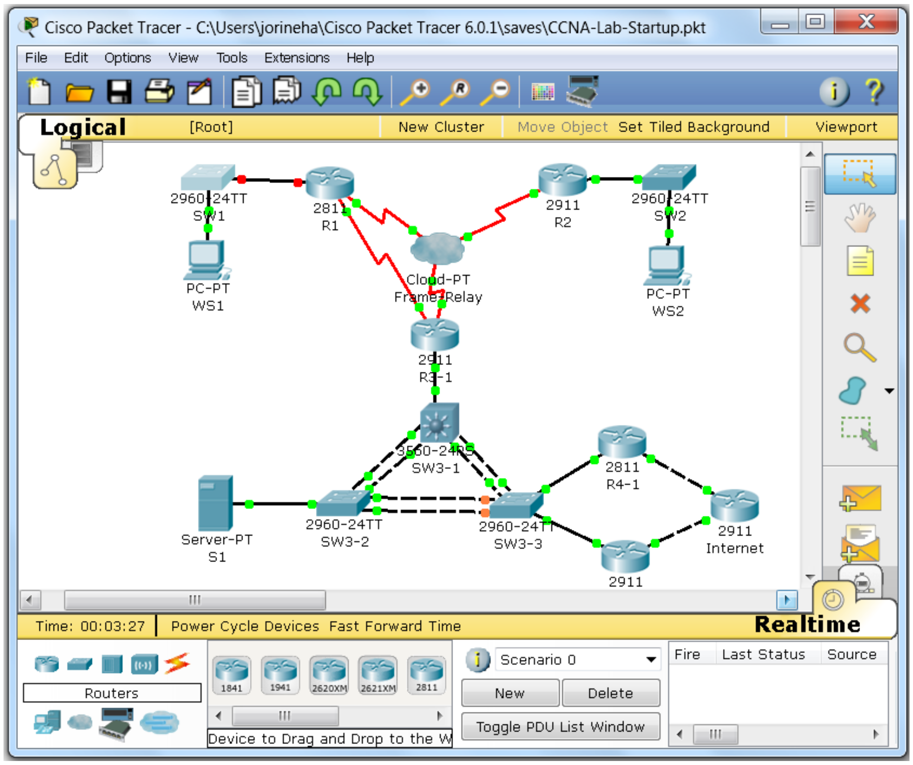
Lesson 7 Lab Exercises

8.1 EIGRP Routing Configuration Exercises

As demonstrated in the previous lab exercises, RIP as a routing protocol has many shortcomings, not the least of which is its 15 hop limit. One of Cisco's earliest innovations was the Interior Gateway Routing Protocol (IGRP), which introduced the capability of judging best routes based on bandwidth and delay. While IGRP had the same classful problem as version 1 of RIP, its updated version, EIGRP, does not. In these lab exercises you will configure EIGRP in place of RIP.

8.1.1. Configure EIGRP on the Devices in the Lab

EIGRP is a hybrid routing protocol, with elements of both distance-vector and link-state protocols. In the family of more advanced routing protocols, EIGRP is one of the simplest to configure, with steps similar to RIP. To begin, open Packet Tracer and click on R1, as shown in the image below:



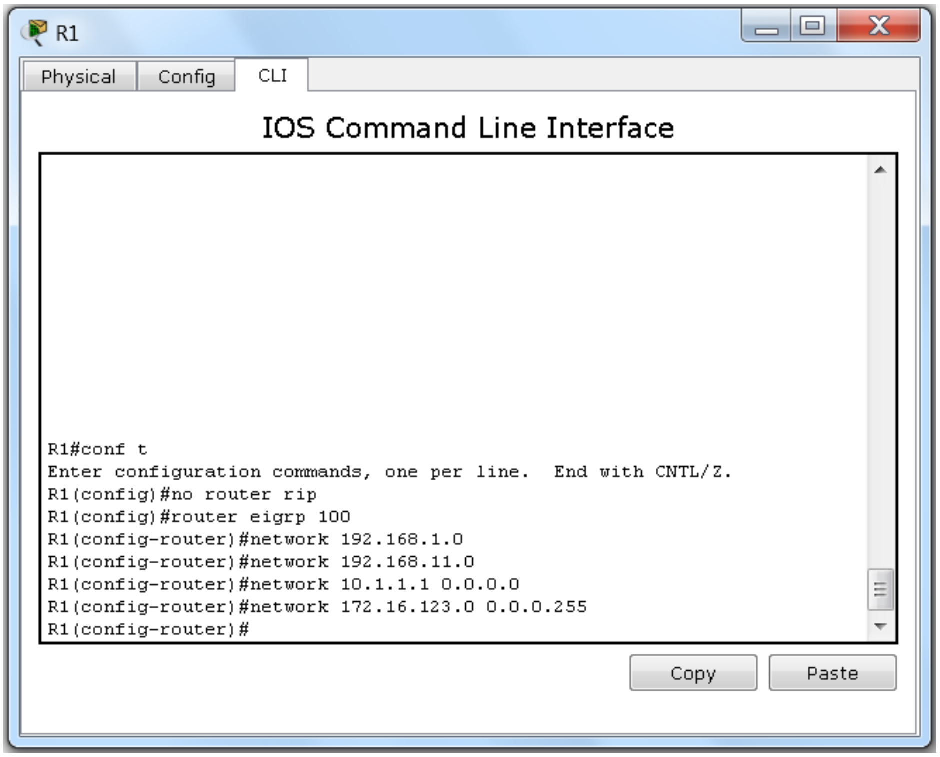
- **Remove RIP Routing from R1:** Take the RIP routing process off R1 using the steps outlined below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by

simply pressing **<enter>** (the console line already contains the configuration)

- **Remove RIP from R1:** Remove RIP routing using the **no router rip** command

- **Configure EIGRP on R1**: Configure an EIGRP routing process using the following steps:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no router rip
R1(config)#router eigrp 100
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 10.1.1.1 0.0.0.0
R1(config-router)#network 172.16.123.0 0.0.0.255
R1(config-router)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Begin the EIGRP routing process:** Start EIGRP on R1 with the command **router eigrp 100** (100 is an autonomous system number which must match on all devices)
- **Disable automatic summarization:** Automatic summarization will cause all networks to be summarized to its classful boundary, so disable it with the **no auto-summary** command
- **Place VLANs 1 and 11 in EIGRP**: Enter the command **network 192.168.1.0** and **network 192.168.11.0** (network statements can use major network numbers like RIP, as shown here)

- **Place Loopback 0 in EIGRP**: Enter the command **network 10.1.1.1 0.0.0.0** (To specify specific networks, masks are permitted; 0.0.0.0 is the wildcard mask specifying a /32 network)
    - **Place the serial interface in EIGRP:** Use the command **network 172.16.123.0 0.0.0.255** to place the WAN interface into EIGRP (another example of a mask, in this case a /24 network)
    - **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 or 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.

- **Remove RIP Routing from R2:** Take the RIP routing process off R2 using the steps outlined below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Remove RIP from R2:** Remove RIP routing using the **no router rip** command

- **Configure EIGRP on R2**: Configure an EIGRP routing process using the following steps:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Begin the EIGRP routing process:** Start EIGRP on R2 with the command **router eigrp 100** (100 is an autonomous system number which must match on all devices)
    - **Disable automatic summarization:** Automatic summarization will cause all networks to be summarized to its classful boundary, so disable it with the **no auto-summary** command.
    - **Place VLANs 1 and 22 in EIGRP**: Enter the command **network 192.168.0.0 0.0.255.255** (this places ***both*** interfaces in the processes in a single statement)
    - **Place Loopback 0 in EIGRP**: Enter the command **network 10..0.0.0** (since this interface is the only one with an address in

    - the 10.0.0.0/8 range, the major network number will only match that interface)
    - **Place the serial interface in EIGRP:** Use the command **network 172.16.123.0 0.0.0.255** to place the WAN interface into EIGRP (same as before)
    - **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 or 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

- **Remove RIP Routing from R3-1:** Take the RIP routing process off R3-1 using the steps outlined below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Remove RIP from R3-1:** Remove RIP routing using the **no router rip** command

- **Configure EIGRP on R3-1**: Configure an EIGRP routing process using the following steps:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Begin the EIGRP routing process:** Start EIGRP on R3-1 with the command **router eigrp 100** (100 is an autonomous system number which must match on all devices)
    - **Disable automatic summarization:** Automatic summarization will cause all networks to be summarized to its classful boundary, so disable it with the **no auto-summary** command.
    - **Place all interfaces in EIGRP**: Enter the command **network 0.0.0.0** (this places both interfaces in the processes in a single statement)
    - **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 or 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.

- **Remove RIP Routing from R4-1:** Take the RIP routing process off R4-1 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove RIP from R4-1** Remove RIP routing using the **no router rip** command

- **Configure EIGRP on R4-1**: Configure an EIGRP routing process using the following steps:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Begin the EIGRP routing process:** Start EIGRP on R4-1 with the command **router eigrp 100** (100 is an autonomous system number which must match on all devices)
  - **Disable automatic summarization:** Automatic summarization will cause all networks to be summarized to its classful boundary, so disable it with the **no auto-summary** command.
  - **Place all interfaces in EIGRP**: Enter the command **network 0.0.0.0** (this places both interfaces in the processes in a single statement)
  - **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 or 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.

- **Remove RIP Routing from R4-2:** Take the RIP routing process off R4-2 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by

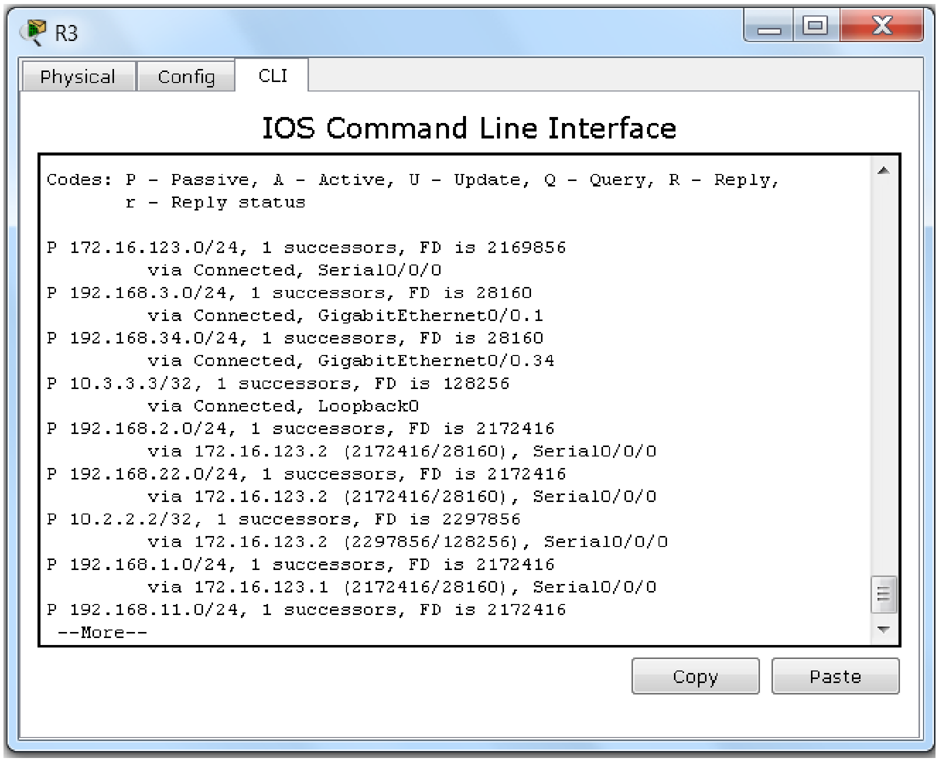
    simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove RIP from R4-2** Remove RIP routing using the **no router rip** command

- **Configure EIGRP on R4-2**: Configure an EIGRP routing process using the following steps:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Begin the EIGRP routing process:** Start EIGRP on R4-2 with the command **router eigrp 100** (100 is an autonomous system number which must match on all devices)
  - **Disable automatic summarization:** Automatic summarization will cause all networks to be summarized to its classful boundary, so disable it with the **no auto-summary** command.
  - **Place all interfaces in EIGRP**: Enter the command **network 0.0.0.0** (this places both interfaces in the processes in a single statement)
  - **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 or 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.

- **Review EIGRP Protocol Mechanics:** Open the CLI window of R3-1 in order to review aspects of EIGRP operation, as outlined below:

  - **Tables Used by EIGRP:** The EIGRP protocol makes uses of several data tables in order to perform protocol operations. Display these tables and there entries as follows:



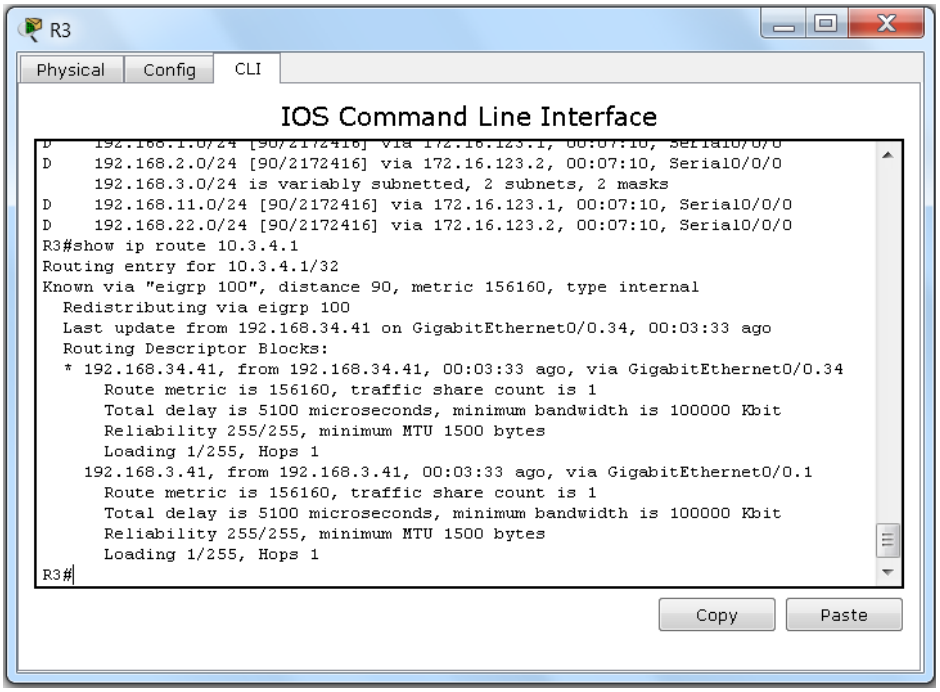
```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.123.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 192.168.3.0/24, 1 successors, FD is 28160
         via Connected, GigabitEthernet0/0.1
P 192.168.34.0/24, 1 successors, FD is 28160
         via Connected, GigabitEthernet0/0.34
P 10.3.3.3/32, 1 successors, FD is 128256
         via Connected, Loopback0
P 192.168.2.0/24, 1 successors, FD is 2172416
         via 172.16.123.2 (2172416/28160), Serial0/0/0
P 192.168.22.0/24, 1 successors, FD is 2172416
         via 172.16.123.2 (2172416/28160), Serial0/0/0
P 10.2.2.2/32, 1 successors, FD is 2297856
         via 172.16.123.2 (2297856/128256), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 2172416
         via 172.16.123.1 (2172416/28160), Serial0/0/0
P 192.168.11.0/24, 1 successors, FD is 2172416
 --More--
```

- **Neighbor table**: Use the **show ip eigrp neighbors** command to display information on directly connected EIGRP neighbors (address, interface, hold time, etc.)
- **Topology table**: Show the EIGRP topology database (which populates the IP routing table) with the command **show ip eigrp topology**
- **IP routing table**: To display the content of the EIGRP specific routing table, use the **show ip route eigrp** command

o **EIGRP hello messages**: To display the active hello messages on the CLI, use these steps:

- **Debug command**: To display all EIGRP related traffic generated by the router, enter the command **debug eigrp packets**
- **Observe hello packets**: After the debug command is entered, all EIGRP packets will display, most of which will be hello messages. Observe the information they contain, when possible
- **Stop the debug output**: Enter the command **undebug all** to stop the messages from displaying on the command line. You may not be able to see the letters typed it but the messages will cease

- **Configure EIGRP Route Preference Parameters:** Alter the default settings in the network and change route selection using the process steps below:
    - **Go to the CLI of R3-1:** In Packet Tracer, double click the icon for R3-1 and select the CLI tab
    - **Display the IP routing table:** Bring up the routing table on R3-1 by entering the **show ip route eigrp** command, and note the following:



```
D    192.168.1.0/24 [90/2172416] via 172.16.123.1, 00:07:10, Serial0/0/0
D    192.168.2.0/24 [90/2172416] via 172.16.123.2, 00:07:10, Serial0/0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.11.0/24 [90/2172416] via 172.16.123.1, 00:07:10, Serial0/0/0
D    192.168.22.0/24 [90/2172416] via 172.16.123.2, 00:07:10, Serial0/0/0
R3#show ip route 10.3.4.1
Routing entry for 10.3.4.1/32
Known via "eigrp 100", distance 90, metric 156160, type internal
  Redistributing via eigrp 100
  Last update from 192.168.34.41 on GigabitEthernet0/0.34, 00:03:33 ago
  Routing Descriptor Blocks:
  * 192.168.34.41, from 192.168.34.41, 00:03:33 ago, via GigabitEthernet0/0.34
      Route metric is 156160, traffic share count is 1
      Total delay is 5100 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
    192.168.3.41, from 192.168.3.41, 00:03:33 ago, via GigabitEthernet0/0.1
      Route metric is 156160, traffic share count is 1
      Total delay is 5100 microseconds, minimum bandwidth is 100000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 1
R3#
```

        - **Single routes for most networks**: Most remote networks contain a single "best path" because of limited redundancy in the network
        - **Two equal-cost routes to R4-1 & R4-2**: Two equal cost/successor routes exist for the Loopback interfaces of R4-1 (10.3.4.1) and R4-2 (10.3.4.2)
        - **Equal metrics to R4-1 & R4-2**: The EIGRP metric (bandwidth of 100000 Kbit + delay of 100 usec) is identical on the LAN subinterfaces of both routers, which inherit the settings from the physical Gigabit interfaces. This results in two valid routes to the loopback interfaces, as EIGRP supports equal-cost (and unequal cost) load balancing (the bandwidth and delay of the Fa0/0 interface of R4-1 were altered for lab purposes)

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Change bandwidth parameters for the Gi0/0.1 interface**: To alter the metric for the Gi0/0.34 interface, enter interface configuration mode using the **interface Gi0/0.1** command. Change the default bandwidth on the subinterface by next typing the protocol-independent command of **bandwidth 1000**. Alternatively, you could have changed the delay setting
- **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 or 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
- **Display the IP routing table:** Bring up the routing table on R3-1 by entering the **show ip route eigrp** command, and note that there is only one route now
- **Display the EIGRP topology table:** To show the change the EIGRP metric for the 10.3.4.1 network, issue the show **ip eigrp topology**. Note that the entry for this network has only ***one*** successor with the original metric of 156160, but the other route, now a feasible successor, has a metric of 2690560.
- **Close Packet Tracer:** To complete this specific exercise, close the window to R3-1, and if desired, close Packet Tracer.

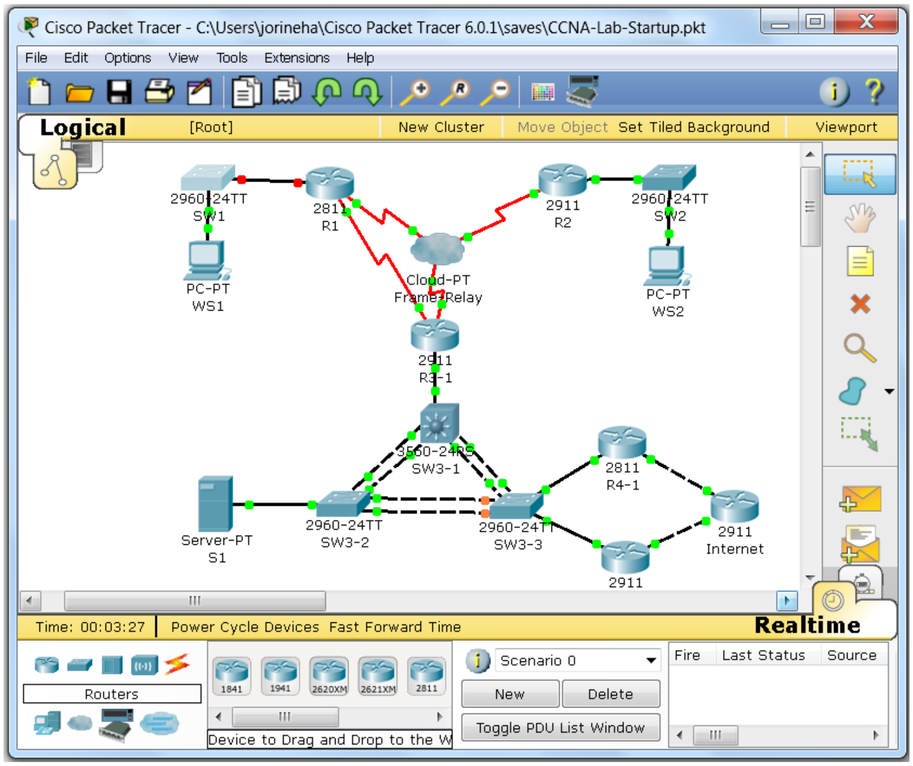
Lessons 8 & 9 Lab Exercises

9.1 OSPF Routing Configuration Exercises

Even though EIGRP is a simple, though efficient routing protocol, it may not be an ideal fit for some networks. To begin with, EIGRP is currently Cisco proprietary, although efforts are underway to change that. In the present environment, however, only a network of all Cisco routing devices would be suitable for EIGRP. Unlike EIGRP, OSPF is a standardized protocol supported by nearly every routing device manufactured, and thus an excellent choice for mixed networks, as well as large ones. In these lab exercises, you will replace EIGRP with OSPF, first in a single area, and then in multiple areas.

9.1.1. Configure Single-Area OSPF on the Devices in the Lab

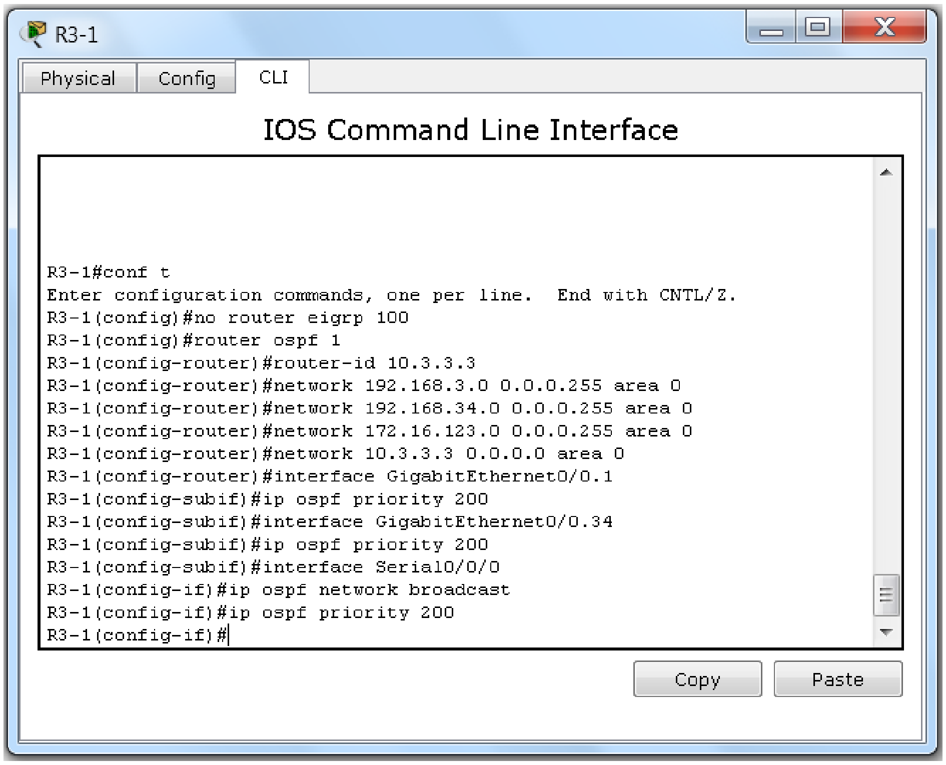
OSPF observes strict rules with regard to the network, particularly with regard to hierarchy, usually with multiple areas. In this exercise, you will convert the existing network to OSPF, and implement a single area. To begin, open Packet Tracer and click on R1, as shown in the image below:



- **Remove EIGRP Routing from R3-1:** Take the EIGRP routing process off R3-1 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove EIGRP from R3-1:** Remove EIGRP routing using the **no router eigrp 100** command

- **Configure OSPF on R3-1**: Configure OSPF on R3-1 as follows:



```
R3-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3-1(config)#no router eigrp 100
R3-1(config)#router ospf 1
R3-1(config-router)#router-id 10.3.3.3
R3-1(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3-1(config-router)#network 192.168.34.0 0.0.0.255 area 0
R3-1(config-router)#network 172.16.123.0 0.0.0.255 area 0
R3-1(config-router)#network 10.3.3.3 0.0.0.0 area 0
R3-1(config-router)#interface GigabitEthernet0/0.1
R3-1(config-subif)#ip ospf priority 200
R3-1(config-subif)#interface GigabitEthernet0/0.34
R3-1(config-subif)#ip ospf priority 200
R3-1(config-subif)#interface Serial0/0/0
R3-1(config-if)#ip ospf network broadcast
R3-1(config-if)#ip ospf priority 200
R3-1(config-if)#
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Start OSPF routing:** Initiate OSPF on R3-1 with the command **router ospf 1** (1 is a ***locally significant*** process-id which does ***not*** have to match on all devices)
  - **Specify Loopback 0 as the router id**: Rather than having the router choose the OSPF router if, explicitly configure it by using the **router-id 10.3.3.3** command in OSPF router configuration mode

  - **Place VLANs 1 and 34 in OSPF**: Enter the commands **network 192.168.3.0 0.0.0.255 area 0** and **network 192.168.34.0 0.0.0.255 area 0** to place both interfaces into OSPF (network statements use wildcard masks like EIGRP, but must include the area-id, as shown here)
  - **Place Loopback 0 into OSPF**: Enter the command **network 10.3.3.3 0.0.0.0 area 0** (note that this is a /32 network)
  - **Place the serial interface in OSPF:** Use the command **network 172.16.123.0 0.0.0.255 area 0** to place the WAN interface into OSPF
  - **Configure OSPF over the WAN:** Frame-relay does not transport broadcasts/multicasts natively, so you have to change the default network type that OSPF uses. Enter interface configuration mode with the command **interface Se0/0/0** and enter the command **ip ospf network broadcast**
  - **Designate R3-1 as the Designated Router for the LAN/WAN:** Election of the DR/BDR is an automated process, but can result in less than optimal placement. Since R3-1 is best placed for this task, force the election to favor R3-1 by adding the statement **ip ospf priority 200** to the following interfaces on R3-1:
    - Interface Gi0/0.1 (VLAN 1)
    - Interface Gi0/0.34 (VLAN 34)
    - S0/0/0 (WAN interface)

- **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 or 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.

- **Remove EIGRP Routing from R1:** Take the EIGRP routing process off R1 using the steps outlined below:
  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove EIGRP from R1:** Remove EIGRP routing using the **no router eigrp 100** command

- **Configure OSPF on R1**: Configure OSPF on R1 as follows:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Start OSPF routing:** Initiate OSPF on R1 with the command **router ospf 1**
  - **Specify Loopback 0 as the router id**: Rather than having the router choose the OSPF router if, explicitly configure it by using the **router-id 10.1.1.1** command in OSPF router configuration mode
  - **Place VLANs 1 and 11 in OSPF**: Enter the command **network 192.168.1.0 0.0.0.255 area 0** and **network 192.168.11.0 0.0.0.255 area 0** (similar to EIGRP)
  - **Place Loopback 0 into OSPF**: Enter the command **network 10.1.1.1 0.0.0.0 area 0**
  - **Place the serial interface in OSPF:** Use the command **network 172.16.123.0 0.0.0.255 area 0** to place the WAN interface into OSPF
  - **Configure OSPF over the WAN:** Enter interface configuration mode with the command **interface Se0/0/0** and enter the command **ip ospf network broadcast** (matches settings on R3-1)
  - **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 or 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

- **Remove EIGRP Routing from R2:** Take the EIGRP routing process off R2 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove EIGRP from R2:** Remove EIGRP routing using the **no router eigrp 100** command

- **Configure OSPF on R2**: Configure OSPF on R2 as follows:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Start OSPF routing:** Initiate OSPF on R2 with the command **router ospf 1**
  - **Specify Loopback 0 as the router id**: Rather than having the router choose the OSPF router if, explicitly configure it by using the **router-id 10.2.2.2** command in OSPF router configuration mode
  - **Place VLANs 1 and 22 in OSPF**: Enter the command **network 192.168.0.0 0.0.0.255 area 0** to place both interfaces into OSPF in a single statement (as you did with EIGRP)
  - **Place Loopback 0 into OSPF**: Enter the command **network 10.2.2.2 0.0.0.0 area 0**
  - **Place the serial interface in OSPF:** Use the command **network 172.16.123.0 0.0.0.255 area 0** to place the WAN interface into OSPF
  - **Configure OSPF over the WAN:** Enter interface configuration mode with the command **interface Se0/0/0** and enter the command **ip ospf network broadcast** (in order to match the settings with R1 & R3-1)
  - **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 or 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

- **Remove EIGRP Routing from R4-1:** Take the EIGRP routing process off R4-1 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove EIGRP from R4-1:** Remove EIGRP routing using the **no router eigrp 100** command

- **Configure OSPF on R4-1**: Configure OSPF on R4-1 as follows:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Start OSPF routing:** Initiate OSPF on R4-1 with the command **router ospf 1**
  - **Specify Loopback 0 as the router id**: Rather than having the router choose the OSPF router if, explicitly configure it by using the **router-id 10.3.4.1** command in OSPF router configuration mode
  - **Place VLANs 3 and 34 in OSPF**: Enter the command **network 192.168.0.0 0.0.0.255 area 0** to place both interfaces into OSPF in a single statement (as you did with EIGRP)
  - **Place Loopback 0 into OSPF**: Enter the command **network 10.3.4.1 0.0.0.0 area 0**
  - **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 or 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

- **Remove EIGRP Routing from R4-2:** Take the EIGRP routing process off R4-2 using the steps outlined below:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Remove EIGRP from R4-2:** Remove EIGRP routing using the **no router eigrp 100** command

- **Configure OSPF on R4-2**: Configure OSPF on R4-2 as follows:

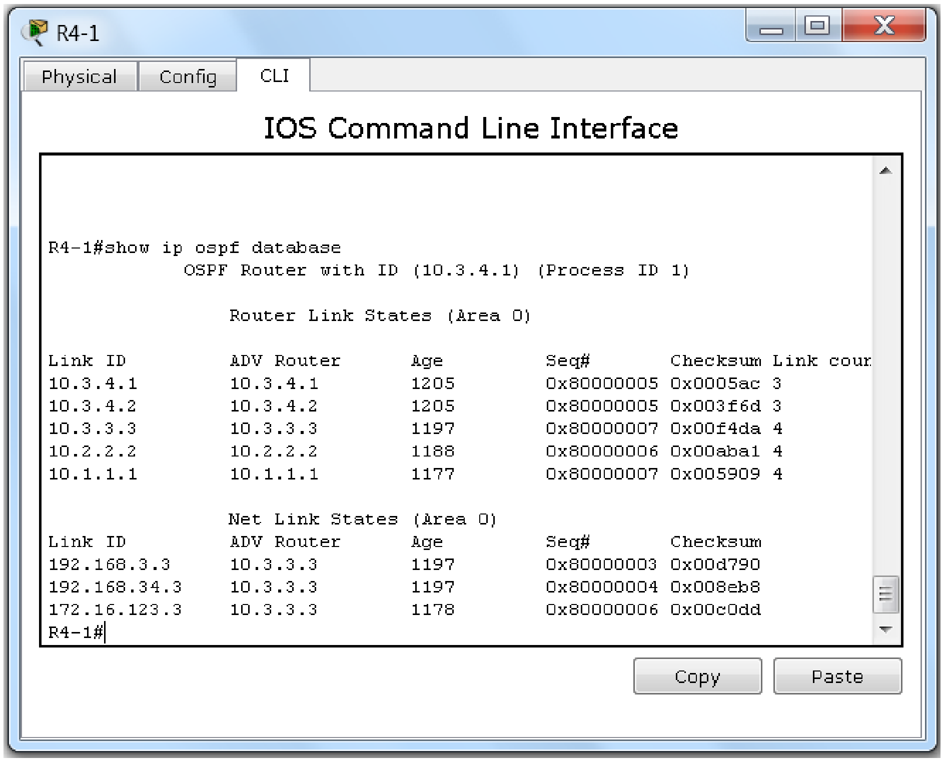
  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Start OSPF routing:** Initiate OSPF on R4-2 with the command **router ospf 1**

    - **Specify Loopback 0 as the router id**: Rather than having the router choose the OSPF router if, explicitly configure it by using the **router-id 10.3.4.2** command in OSPF router configuration mode
    - **Place VLANs 3 and 34 in OSPF**: Enter the command **network 192.168.0.0 0.0.0.255 area 0** to place both interfaces into OSPF in a single statement (as you did with EIGRP)
    - **Place Loopback 0 into OSPF**: Enter the command **network 10.3.4.2 0.0.0.0 area 0**
    - **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 or 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.

- **Review OSPF Protocol Mechanics:** Open the CLI window of R4-1 in order to review aspects of OSPF operation, as outlined below:

    - **Tables Used by OSPF:** As with EIGRP, OSPF makes uses of several data tables in order to perform protocol operations. Display these tables and there entries as follows:

        - **Neighbor table**: Use the **show ip ospf neighbors** command to display information on directly connected neighbors (priority, interface, state, dead time, etc.)
        - **Link-state database**: Show the contents of the OSPF topology database (which populates the IP routing table) with the command **show ip ospf database**
        - **IP routing table**: To display the content of the EIGRP specific routing table, use the **show ip route ospf** command



```
R4-1#show ip ospf database
            OSPF Router with ID (10.3.4.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link cour
10.3.4.1        10.3.4.1        1205        0x80000005 0x0005ac 3
10.3.4.2        10.3.4.2        1205        0x80000005 0x003f6d 3
10.3.3.3        10.3.3.3        1197        0x80000007 0x00f4da 4
10.2.2.2        10.2.2.2        1188        0x80000006 0x00aba1 4
10.1.1.1        10.1.1.1        1177        0x80000007 0x005909 4

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.3.3     10.3.3.3        1197        0x80000003 0x00d790
192.168.34.3    10.3.3.3        1197        0x80000004 0x008eb8
172.16.123.3    10.3.3.3        1178        0x80000006 0x00c0dd
R4-1#
```

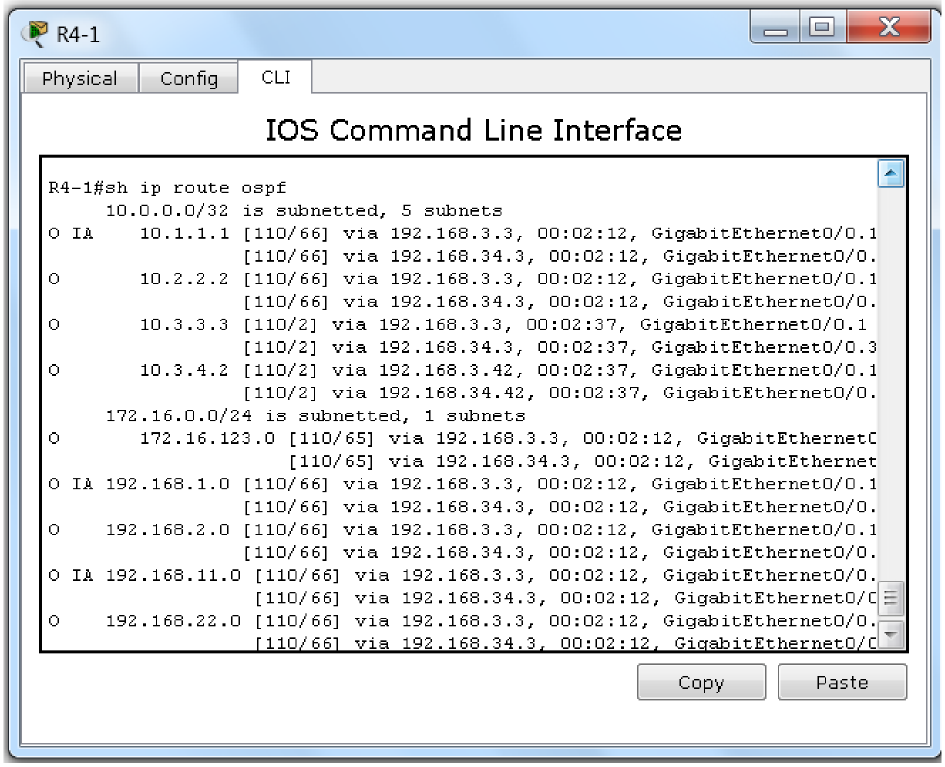
9.1.2. Configure Multi-Area OSPF on the Devices in the Lab

Using OSPF in a single area may satisfy the demands of a small network, but this approach does not scale well to larger networks. One of the benefits of OSPF is to contain the impact of routing changes in a smaller construct, called an area. In this exercise you will migrate the OSPF network from a single area to multiple areas, as follows:

- **Maintain the WAN Links in Area 0:** Since the frame-relay network definitely acts as a transit area for all traffic between sites, it is a logical choice for the Backbone area, or Area 0. Do not make any changes to the WAN links on R1, R2, and R3-1.
- **Migrate all other Interfaces on R1 to a New Area 1**: Split off the loopback and VLAN interfaces in Site 1 to a new area (designated Area 1), using the following process:
    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter OSPF router configuration mode:** In order to change the area assignments, enter into OSPF configuration mode using the command **router ospf 1**.

- **Move loopback 0 to Area 1:** Remove loopback 0 from area 0 by issuing the command **no network 10.1.1.1 0.0.0.0 area 0**, followed by the command **network 10.1.1.1 0.0.0.0 area 1** (this temporarily removes loopback 0 from OSPF altogether, but realigns it to the new area).
- **Move VLAN 1 and VLAN 11 to Area 1:** Remove the VLAN interfaces from area 0 by issuing the command **no network 192.168.0.0 0.0.255.255 area 0**, followed by the command **network 192.168.0.0 0.0.255.255 area 0** (OSPF converges very quickly so the changes will be propagated rapidly throughout the rest of the network).
- **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 or 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

- **Observe the Impact of the Changes on R1**: Use R4-1 as an observation point for the changes just introduced:



```
R4-1#sh ip route ospf
     10.0.0.0/32 is subnetted, 5 subnets
O IA    10.1.1.1 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.1
                 [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/0.
O       10.2.2.2 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.1
                 [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/0.
O       10.3.3.3 [110/2] via 192.168.3.3, 00:02:37, GigabitEthernet0/0.1
                 [110/2] via 192.168.34.3, 00:02:37, GigabitEthernet0/0.3
O       10.3.4.2 [110/2] via 192.168.3.42, 00:02:37, GigabitEthernet0/0.1
                 [110/2] via 192.168.34.42, 00:02:37, GigabitEthernet0/0.
     172.16.0.0/24 is subnetted, 1 subnets
O       172.16.123.0 [110/65] via 192.168.3.3, 00:02:12, GigabitEthernetC
                     [110/65] via 192.168.34.3, 00:02:12, GigabitEthernet
O IA 192.168.1.0 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.1
                 [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/0.
O    192.168.2.0 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.1
                 [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/0.
O IA 192.168.11.0 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.
                  [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/C
O    192.168.22.0 [110/66] via 192.168.3.3, 00:02:12, GigabitEthernet0/0.
                  [110/66] via 192.168.34.3, 00:02:12, GigabitEthernet0/C
```

- **Open a CLI window on R4-1:** Go to the main Packet Tracer screen and click on the icon for R4-1, and select the CLI window.

- **Note the changes to the affected routes:** Enter the command **show ip route ospf** to display the IP routing table. When the entire network was in a single area, all remote network entries in the IP routing table were designated with an O (for OSPF, specifically routes within an area, or intra-area), where now networks in Area 1 are marked with an IA (Inter-area routes). If you examine the OSPF topology database, you will notice an entirely new database segment dedicated just to Area 1.

- **Migrate all non-backbone interfaces on R2 to a New Area 2**: Split off the loopback and VLAN interfaces in Site 2 to a new area (designated Area 2), using the following process:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter OSPF router configuration mode:** In order to change the area assignments, enter into OSPF configuration mode using the command **router ospf 1**.
  - **Move loopback 0 to Area 2:** Remove loopback 0 from area 0 by issuing the command **no network 10.2.2.2 0.0.0.0 area 0**, followed by the command **network 10.2.2.2 0.0.0.0 area 2**.
  - **Move VLAN 1 and VLAN 22 to Area 2:** Remove the VLAN interfaces from area 0 by issuing the command **no network 192.168.0.0 0.0.255.255 area 0**, followed by the command **network 192.168.0.0 0.0.255.255 area 2** (OSPF converges very quickly so the changes will be propagated rapidly throughout the rest of the network).
  - **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 or 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

- **Migrate all non-backbone interfaces on R3-1 to a New Area 3**: Split off the loopback and VLAN interfaces in Site 3 to a new area (designated Area 3), using the following process:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by

simply pressing **<enter>** (the console line already contains the configuration)

- **Enter OSPF router configuration mode:** In order to change the area assignments, enter into OSPF configuration mode using the command **router ospf 1**
- **Move loopback 0 to Area 3:** Remove loopback 0 from area 0 by issuing the command no **network 10.3.3.3 0.0.0.0 area 0**, followed by the command **network 10.3.3.3 0.0.0.0 area 3**.
- **Move VLAN 1 and VLAN 34 to Area 3:** Remove the VLAN interfaces from area 0 by issuing the commands **no network 192.168.3.0 0.0.0.255 area 0 and no network 192.168.34.0 0.0.0.255 area 0** , followed by the commands **network 192.168.3.0 0.0.255.255 area 3** and **network 192.168.34.0 0.0.0.255 area 3** (OSPF converges very quickly so the changes will be propagated quickly throughout the rest of the network).
- **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 or 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.

- **Migrate all interfaces on R4-1 to Area 3**: Move all interfaces on R4-1 interfaces to Area 3, using the following process:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter OSPF router configuration mode:** In order to change the area assignments, enter into OSPF configuration mode using the command **router ospf 1**.
  - **Move loopback 0 to Area 3:** Remove loopback 0 from area 0 by issuing the command **no network 10.3.4.1 0.0.0.0 area 0**, followed by the command **network 10.3.4.1 0.0.0.0 area 3**.
  - **Move VLAN 1 and VLAN 34 to Area 3:** Remove the VLAN interfaces from area 0 by issuing the commands **no network 192.168.3.0 0.0.0.255 area 0 and no network 192.168.34.0 0.0.0.255 area 0**, followed by the commands **network 192.168.3.0 0.0.255.255 area 3** and **network 192.168.34.0 0.0.0.255 area 3** (OSPF converges very quickly so the changes will be propagated quickly throughout the rest of the network).

    - **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 or 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

- **Migrate all interfaces on R4-2 to Area 3**: Move all interfaces on R4-2 interfaces to Area 3, using the following process:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter OSPF router configuration mode:** In order to change the area assignments, enter into OSPF configuration mode using the command **router ospf 1**
    - **Move loopback 0 to Area 3:** Remove loopback 0 from area 0 by issuing the command **no network 10.3.4.2 0.0.0.0 area 0**, followed by the command **network 10.3.4.2 0.0.0.0 area 3**.
    - **Move VLAN 1 and VLAN 34 to Area 3:** Remove the VLAN interfaces from area 0 by issuing the commands **no network 192.168.3.0 0.0.0.255 area 0 and no network 192.168.34.0 0.0.0.255 area 0** , followed by the commands **network 192.168.3.0 0.0.255.255 area 3** and **network 192.168.34.0 0.0.0.255 area 3** (OSPF converges very quickly so the changes will be propagated rapidly throughout the rest of the network).
    - **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 or 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.

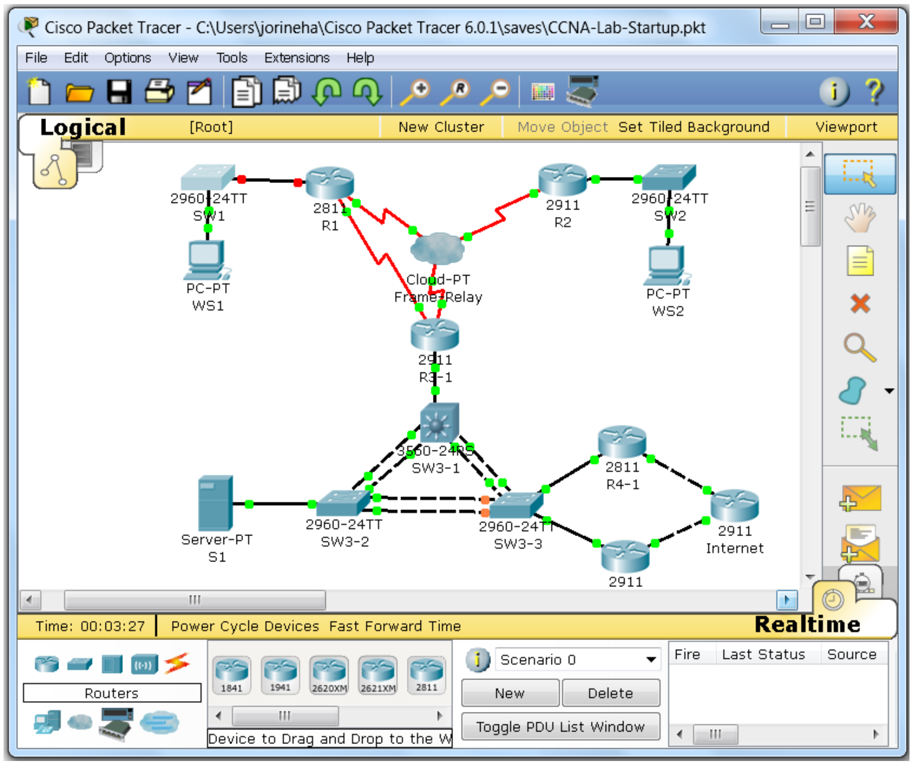
Lesson 10 Lab Exercises

10.1 Address Summarization Exercises

Lesson 10 focuses on several aspects of IPV4 address design (much of which was covered in the ICND1 subnetting lessons), while address summarization was not. The purpose of these lab exercises is to focus on route summarization capabilities in OSPF specifically.

10.1.1. Configure Protocol Independent Route Summarization

Most routing protocols have one or more methods for summarizing IPV4 addresses in the network. OSPF uses the **area-range** command for internal address and **summary-address** for external addresses. BGP uses the **aggregate-address** command, and RIP uses a form of the **summary-address** command as well. EIGRP has both automatic and per-interface capabilities, which is unique among routing protocols. Since Packet Tracer 6.0.1 does not support OSPF address summarization, you will configure another method that can be used in place of the more protocol-oriented features. To begin, open Packet Tracer and click on R2, as shown in the image below:



Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCNA-Lab-Startup.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
2960-24TT SW1
PC-PT WS1
2811 R1
Cloud-PT Frame-Relay
2911 R2
2960-24TT SW2
PC-PT WS2
2911 R3-1
3560-24PS SW3-1
Server-PT S1
2960-24TT SW3-2
2960-24TT SW3-3
2811 R4-1
2911 Internet
2911
Time: 00:03:27 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811
Device to Drag and Drop to the W
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Configure a Static Route Summarizing Loopback 0:** Create a static route in global configuration mode, using the command **ip route**, with the following settings:
    - **10.2.2.0 255.255.255.0:** This is a /24 network that the host route falls within.
    - **Null 0:** A logical interface which causes packets to be immediately dropped.
    - **Full statement: ip route 10.1.1.0 255.255.255.0 null0**
    - **Why packets to 10.2.2.2 will not be dropped**: IP routing operates on the principle of the longest match. Packets destined to R2 will use the route 10.2.2.0/24, and once at the router will choose the 10.2.2.2/32 connected route, and pass to loopback 0 successfully
- **Remove Loopback 0 from the OSPF Process**: Enter into OSPF configuration mode with the **router ospf 1** command. Remove Loopback 0 with the command **no network 10.2.2.2 0.0.0.0 area 2**
- **Redistribute the Static Route into OSPF**: Issue the command **redistribute static subnets** (if you omit the keyword subnets, only the classful networks will be imported)
- **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 or 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.
- **Observe the results:** To verify the results of the changes made to the network, log into R1 and issue the following commands
    - **show ip route ospf**: Note the presence of the redistributed (imported) route as an OSPF E2 (external) route. Also, note the absence of the 10.2.2.2 route
    - **Ping 10.2.2.2**: Even without the presence of the 10.2.2.2/32 host route, pings to the address are successful, because of the longest match principle

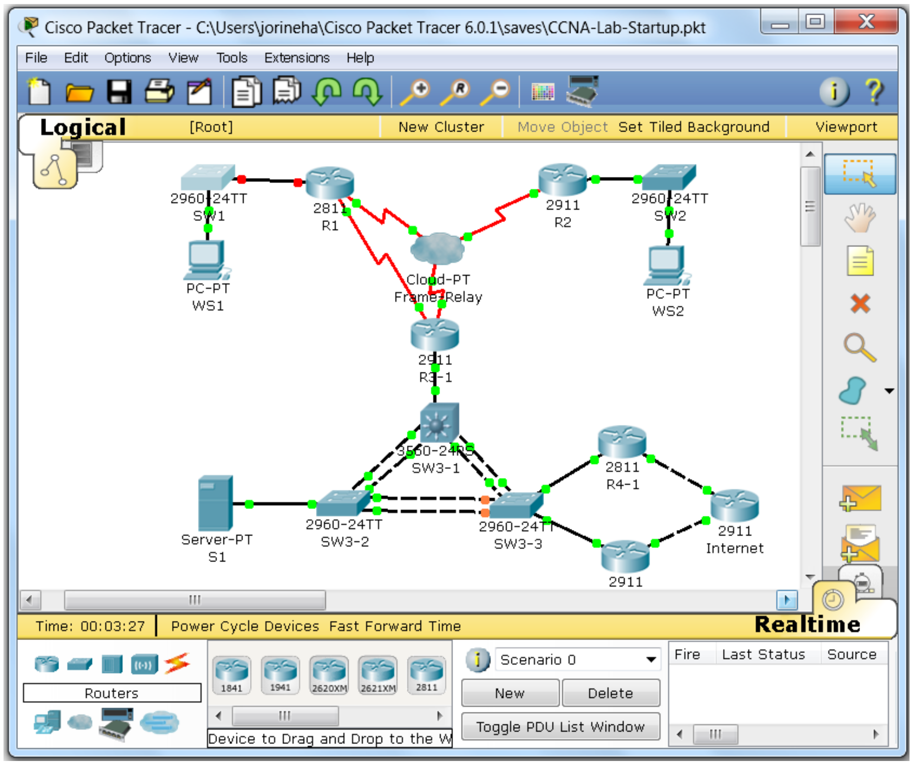
Lesson 11 Lab Exercises

11.1 PPP-Based WAN Lab Exercises

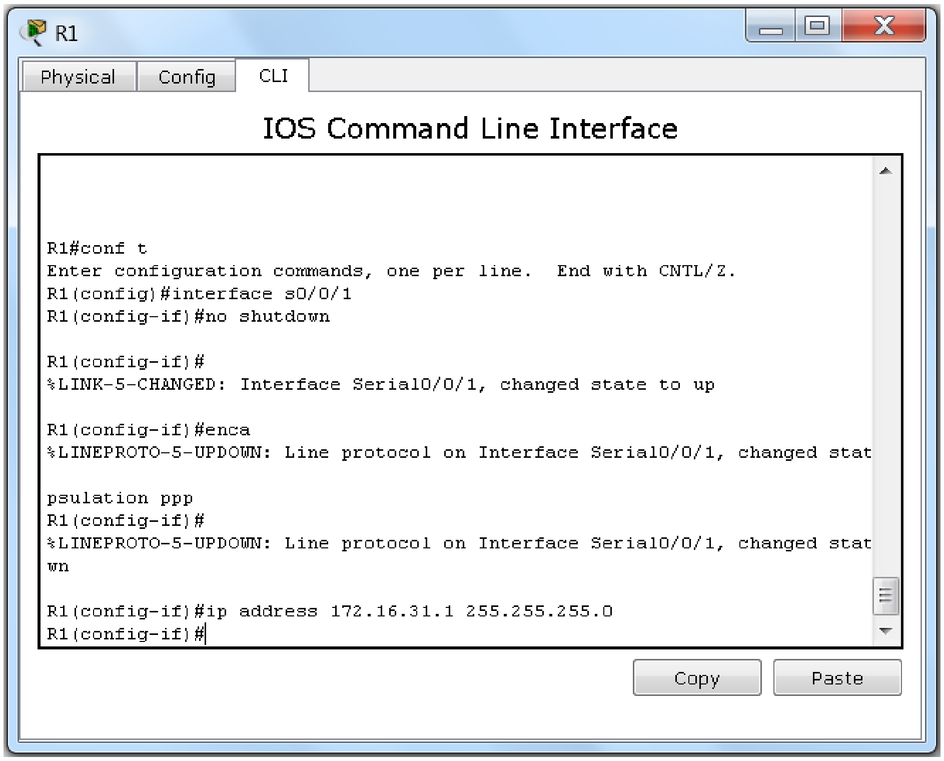
Local Area Networks (LANs) tied together computing devices within close proximity of one another, hence the term “local” area network. Wide Area Networks, as the name suggests, connect sites (typically composed of LANs/campuses) spread across some distance from one another. Understanding and implementing this type of connectivity is a significant element of the CCNA/ICND2 exam.

11.1.1. Configure Basic PPP Across a Simulated Private Line Connection

Point-to-point connections in production environments typically utilize leased lines, obtained through a service provider such as AT&T and Verizon in the U.S. One very ***important*** thing to remember is that the default encapsulation on Cisco serial interfaces is HDLC (proprietary), which will only interoperate with other Cisco devices. For this reason, Point-to-Point Protocol (PPP) is typically the Layer 2 protocol of choice for copper private line type connectivity. To begin the configuration process, open Packet Tracer and double click on the R1 icon:



- **Configure a PPP WAN Link on R1:** Using the steps below, configure PPP on the simulated private line link between R1 and R3:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface s0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R1(config-if)#enca
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed stat

psulation ppp
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed stat
wn

R1(config-if)#ip address 172.16.31.1 255.255.255.0
R1(config-if)#
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Configure a Serial WAN Interface**: Enter configuration mode for the serial interface using the command **interface Se0/0/1**. Enable the interface with the **no shutdown** command. Set the interface for PPP operation by entering **encapsulation PPP**, and add an ip address with the command **ip address 172.16.31.1 255.255.255.0**.
  - **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 or 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.

- **Configure a PPP WAN Link on R3-1:** Using the steps below, configure PPP on the simulated private line link between R3-1 and R1:

    - **Open a CLI Window to R3-1:** Close the R1 CLI window and return to the main Packet Tracer screen. Double-click the icon for R3-1 and open a new CLI window to that device
    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Configure a Serial WAN Interface**: Enter configuration mode for the serial interface using the command **interface Se0/0/1**. Enable the interface with the **no shutdown** command. Set the interface for PPP operation by entering **encapsulation PPP**, and add an ip address with the command **ip address 172.16.31.3 255.255.255.0**
    - **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 or 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

- **Verify the PPP Connection Between R1 & R3-1:** Conduct a brief test to verify the integrity of the PPP private line connection:

    - **Open a CLI Window to R3-1:** Open or reopen the CLI window to R3-1 and go to privileged exec mode.
    - **Show the Interface Parameters of Serial0/0/1:** Issue the command **show interface Se0/0/0** and note the following:

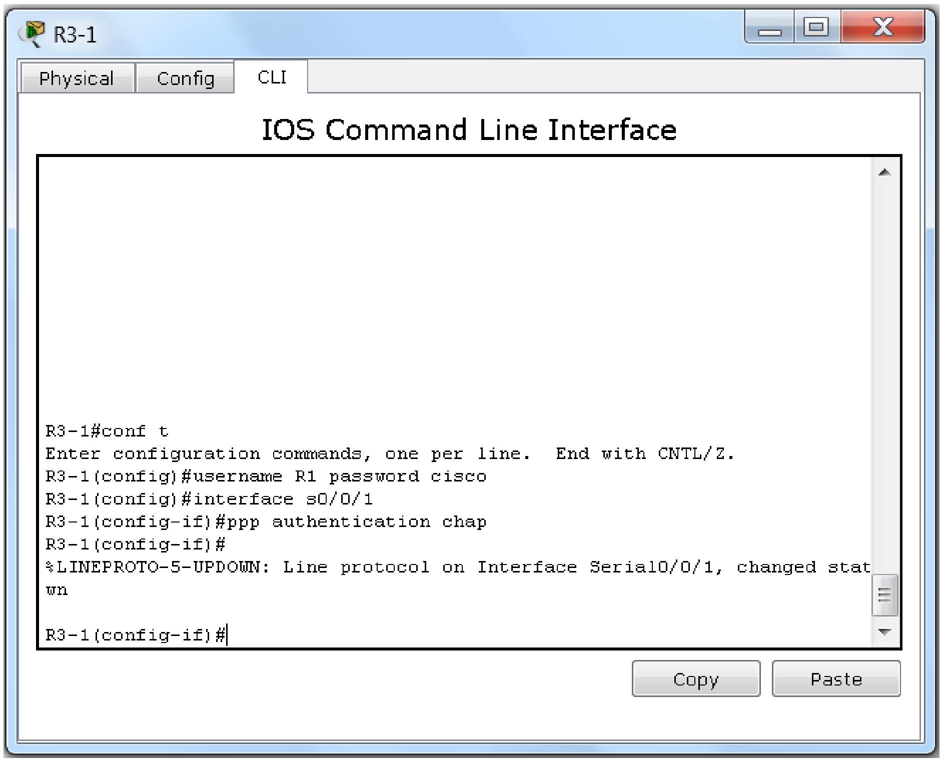
        - **Interface status**: Currently up/up, indicating that both Layer 1 and Layer 2 are fully operational. If HDLC was configured on R3-1, the status would show up/down (Layer 1 functional, Layer 2 non-functional) because of a protocol mismatch
        - **LCP Open**: Indicates that the Link Control Protocol has successfully negotiated the necessary Layer 2 parameters to make a connection
        - **Open: IPCP,CDPCP:** Indicates that both Cisco Discovery Protocol (CDP) and IPV4 are operational (in the case of IPCP, this means that Layer 3 communication is possible)

- **Perform a Connectivity Test**: At the CLI, issue the **ping 172.16.31.1** command to send echo packets to the other end of the PPP connection. The ping should succeed, indicating that the connection is fully functional.

11.1.2. Configure PPP Authentication between R1 & R3-1

One of the many features supported by PPP is authentication, which requires the use of credentials to complete a successful connection. This was particularly important when dial-up connectivity was the primary method for connection to the Internet, though it is still supported across serial links. PPP supports two authentication methods, Password Authentication Protocol (PAP), which sends credentials in clear text, and Challenge Handshake Authentication Protocol (CHAP) which only sends an encrypted has value. Configure CHAP authentication across the PPP link as follows:

- **Configure PPP CHAP Authentication on R3-1:** Using the steps below, configure authentication on the between R1 and R3-1:



```
R3-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3-1(config)#username R1 password cisco
R3-1(config)#interface s0/0/1
R3-1(config-if)#ppp authentication chap
R3-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed stat
wn

R3-1(config-if)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by

simply pressing **<enter>** (the console line already contains the configuration)

  - **Create login credentials:** In order to use authentication, the devices need to have username/password credentials configured. Use the command **username R1 password cisco** to create these on R3-1 (note that the name of the ***remote*** router needs to be used here, not the local name)
  - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface Se0/0/1**.
  - **Activate CHAP authentication:** Instruct PPP to use authentication on the link, and utilize CHAP by entering the command **ppp authentication chap**.
  - **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 or 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.
  - **Interface goes down:** Once authentication is placed on the interface, the Layer 2 process via LCP goes down, because authentication is only configured in one direction

- **Configure PPP CHAP Authentication on R1:** Using the steps below, configure authentication on the between R1 and R3-1:

  - **Open a CLI session on R1**: Close the window for R3-1, and double-click on the R1 icon in Packet Tracer and then select the CLI tab.
  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
  - **Create login credentials:** In order to use authentication, the devices need to have username/password credentials configured. Use the command **username R3-1 password cisco** to create these on R1.
  - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface Se0/0/1**.
  - **Activate CHAP authentication:** Instruct PPP to use authentication on the link, and utilize CHAP by entering the command **ppp authentication chap**.

- **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 or 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.
- **Interface comes back up:** Once authentication is placed on the interface, the Layer 2 process via LCP brings the link back up, since the process is running in both directions now. Optionally, you can enable debugging with the CLI command **debug ppp** authentication and observe the messages being sent back and forth.

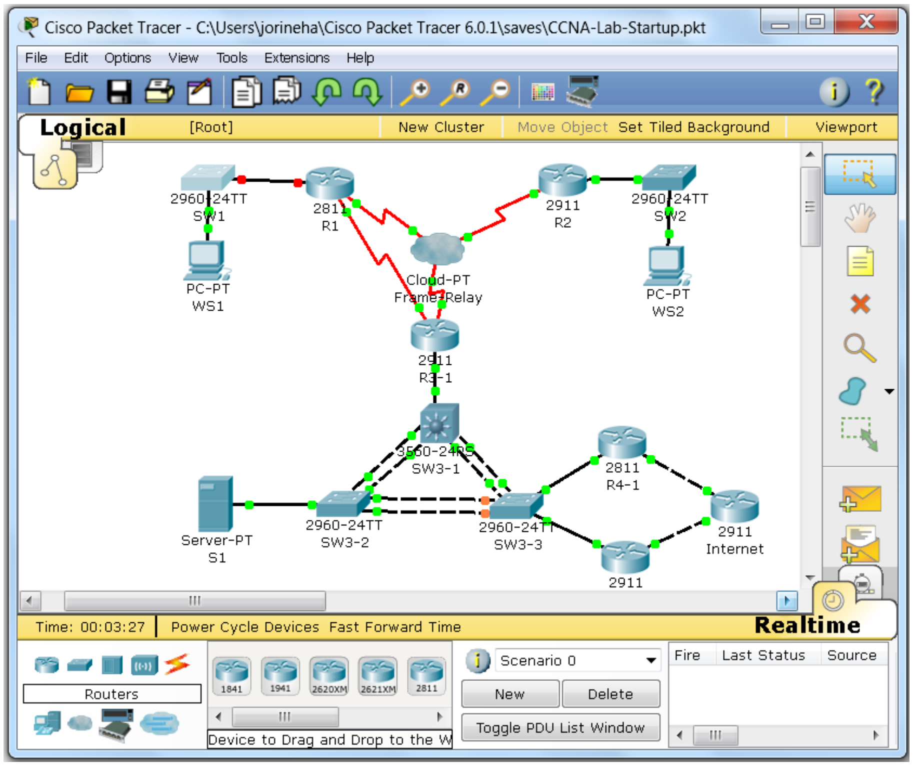
Lesson 12 Lab Exercises

12.1 Frame-Relay Based WAN Lab Exercises

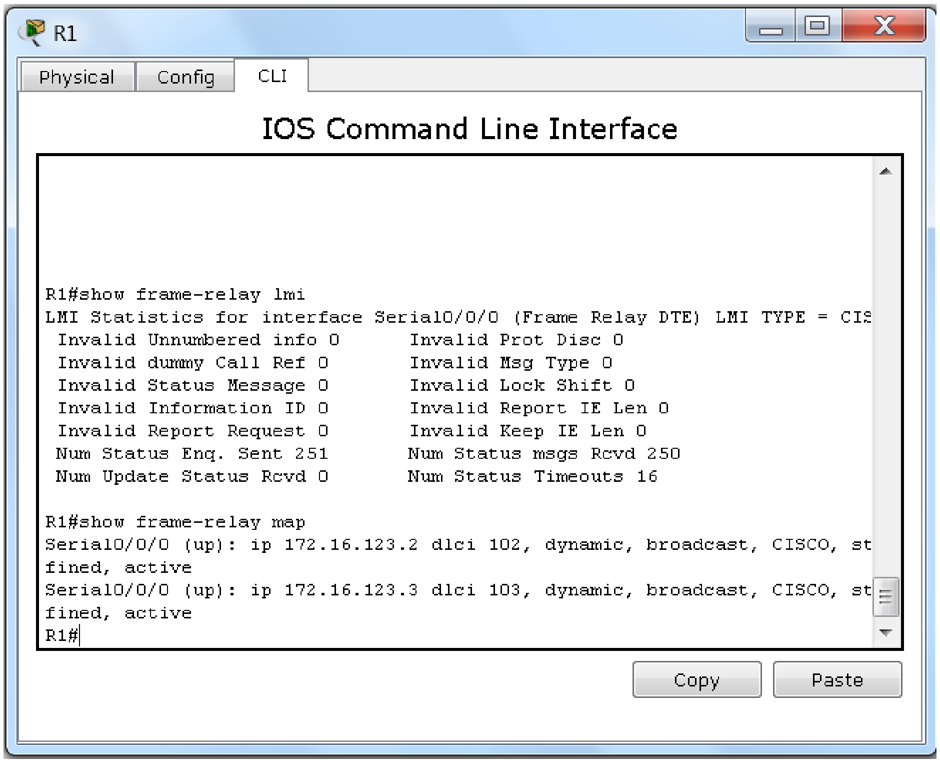
Private line networks, though secure and efficient, have several drawbacks, including per-mile distance charges, idle bandwidth, and so forth. To combat these issues, telecommunications providers created Frame-Relay; this technology shared bandwidth between customers as well as eliminated a substantial share of mileage limitations. Similar to HDLC and PPP, frame-relay is a Layer 2 protocol and allows the end-customer to utilize any Layer 3 addressing (usually IPV4, but can also include deprecated protocols such as IPX and Appletalk). Even though frame-relay is considered a legacy technology (having been displaced by VPNs for example), it is still a required aspect of the ICND2/CCNA exams. In this set of exercises, you will configure this WAN protocol between R1, R2 and R3-1.

12.1.1. Configure Frame-Relay Across the WAN in the Lab

In earlier exercises, you configured a very simple frame-relay network using physical interfaces, and in this exercise you will implement point-to-point subinterfaces for frame-relay. To begin the configuration process, open Packet Tracer and double click on the R1 icon:



- **Observe Frame-Relay Protocol Mechanics:** To better understand the operation of Frame-Relay, review the various aspects of protocol operation, as follows:



```
R1#show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE = CIS
 Invalid Unnumbered info 0      Invalid Prot Disc 0
 Invalid dummy Call Ref 0       Invalid Msg Type 0
 Invalid Status Message 0       Invalid Lock Shift 0
 Invalid Information ID 0       Invalid Report IE Len 0
 Invalid Report Request 0       Invalid Keep IE Len 0
 Num Status Enq. Sent 251       Num Status msgs Rcvd 250
 Num Update Status Rcvd 0       Num Status Timeouts 16

R1#show frame-relay map
Serial0/0/0 (up): ip 172.16.123.2 dlci 102, dynamic, broadcast, CISCO, st
fined, active
Serial0/0/0 (up): ip 172.16.123.3 dlci 103, dynamic, broadcast, CISCO, st
fined, active
R1#
```

  - **Local Management Interface:** In order to operate correctly, status messages must be exchanged between the customer premise equipment (CPE) and service provider devices. LMI acts as a Keepalive mechanism, but also provides ***Data Link Connection Identifiers*** (Layer 2 addresses) available for use. To display information on LMI, use the **frame-relay lmi** command. To view the active exchanges, you can use the **debug frame-relay lmi** command at the command line. If LMI messages are not being exchanged, there may be Layer 2 issues.
  - **Inverse ARP:** As with Ethernet traffic, mapping must take place between Layer 3 and Layer 2 addresses in order to transmit data. In frame-relay this can take place through manual mapping, or through the use of the Inverse-ARP protocol. To demonstrate this, type show **frame-relay map** at the command line, and the output should match the figure above. Note the IP address, the DLCI it is mapped to, and the word ***dynamic***, indicating that this is an automated process. Though this may

seem like a simple way to go about this, it presents many problems, most notably for routing (split horizon, for example)

  - **Permanent Virtual Circuits:** Service providers create the DLCI values, which are then communicated to CPE using the LMI protocol. When mapped properly, these create virtual point-to-point connections referred to as ***Permanent Virtual Circuits***. To display the values being transmitted, use the command **show frame-relay pvc**. The information displayed is interpreted below:

    - **DLCI**: The identifier assigned by the service provider. Some reserved values are not usable.
    - **Interface**: The specific interface receiving the DLCI from the provider
    - **PVC Status**: One of three values, ***Active*** (up and able to pass traffic), ***Deleted*** (configured locally but not being sent by LMI), ***Inactive*** (configured locally but down)

- **Configure Point-to-Point Frame-Relay Interfaces:** Remove the existing interface on the serial interface and configure subinterfaces using these steps:

  - **Configure subinterfaces on R1**: If not already open, double-click on the R1 icon in Packet Tracer and then select the CLI tab

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
    - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface Se0/0/0**
    - **Remove configuration from Serial 0/0/0:** Remove the configured IP address with the **no ip address command**. In addition, remove the ospf configuration with the **no ip ospf network** command
    - **Create a subinterface to R2:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.102 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.12.1 255.255.255.0**. Finally, add the DLCI by entering **frame-relay interface-dlci 102**.
    - **Create a subinterface to R3-1:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.103 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.13.1**

255.255.255.0. Finally, add the DLCI by entering **frame-relay interface-dlci 103**.

- **Edit the OSPF Configuration:** Enter OSPF router configuration mode by entering the command **router ospf 1**. Next, remove the current WAN configuration with the statement **no network 172.16.123.0 0.0.0.255 area 0**. Finally, add the subinterfaces to the routing process by using the command **network 172.16.0.0 0.0.255.255 area 0**
- **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 or 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

- **Configure subinterfaces on R2**: Close the R1 CLI window, then double-click on the R2 icon in Packet Tracer and then select the CLI tab.

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
    - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface Se0/0/0**
    - **Remove configuration from Serial 0/0/0:** Remove the configured IP address with the **no ip address command**. In addition, remove the ospf configuration with the **no ip ospf network** command
    - **Create a subinterface to R1:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.201 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.12.2 255.255.255.0**. Finally, add the DLCI by entering **frame-relay interface-dlci 201**
    - **Create a subinterface to R3-1:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.203 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.23.2 255.255.255.0**. Finally, add the DLCI by entering **frame-relay interface-dlci 203**
    - **Edit the OSPF Configuration:** Enter OSPF router configuration mode by entering the command **router**

ospf 1. Next, remove the current WAN configuration with the statement **no network 172.16.123.0 0.0.0.255 area 0**. Finally, add the subinterfaces to the routing process by using the command **network 172.16.0.0 0.0.255.255 area 0**

- **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 or 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

- **Configure subinterfaces on R3-1**: Close the R2 CLI window, then double-click on the R3-1 icon in Packet Tracer and then select the CLI tab.

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
  - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface Se0/0/0**
  - **Remove configuration from Serial 0/0/0:** Remove the configured IP address with the **no ip address command**. In addition, remove the ospf configurations with the **no ip ospf network** and **no ip ospf priority** commands.
  - **Create a subinterface to R1:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.301 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.13.3 255.255.255.0**. Finally, add the DLCI by entering **frame-relay interface-dlci 301**
  - **Create a subinterface to R2:** Create a point-to-point subinterface by issuing the command **interface s0/0/0.302 point-to-point**. In addition, add a new IP address using the command **ip address 172.16.23.3 255.255.255.0**. Finally, add the DLCI by entering **frame-relay interface-dlci 302**
  - **Edit the OSPF Configuration:** Enter OSPF router configuration mode by entering the command **router ospf 1**. Next, remove the current WAN configuration with the statement **no network 172.16.123.0 0.0.0.255 area 0**. Finally, add the subinterfaces to the routing

process by using the command **network 172.16.0.0 0.0.255.255 area 0**

- **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 or 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

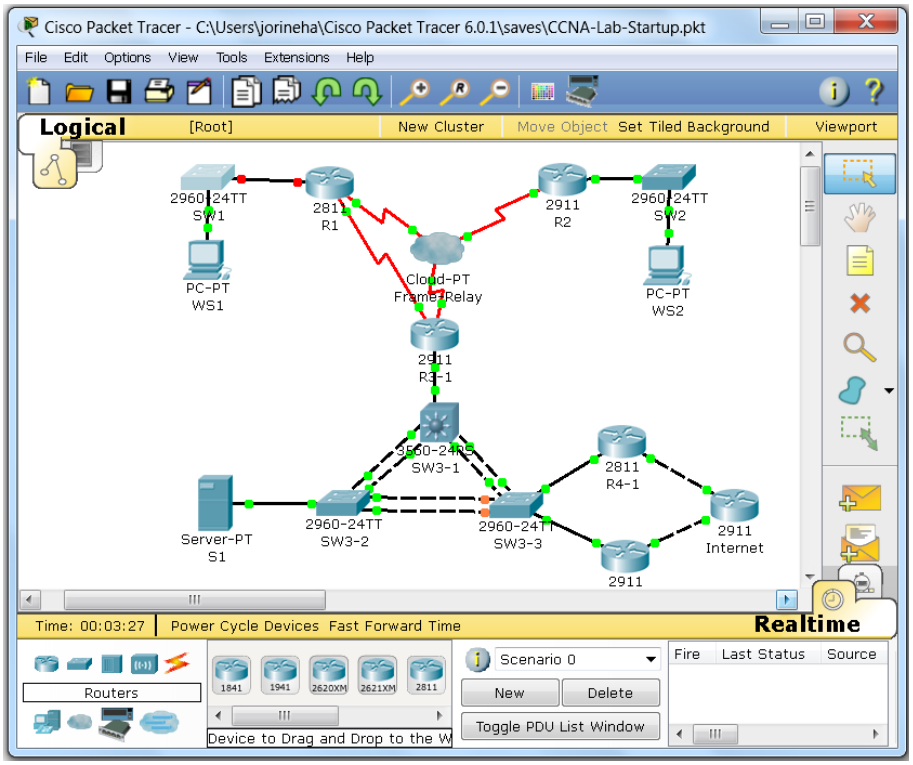
Lesson 13 Lab Exercises

13.1 Virtual Private Network Lab Exercises

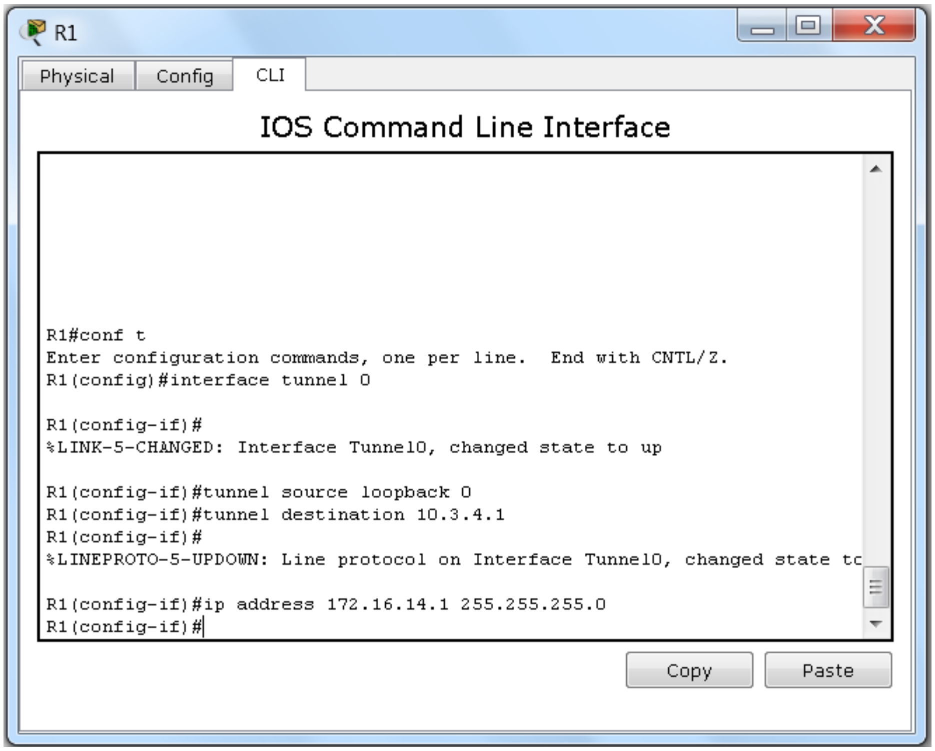
Frame-relay networks once enjoyed widespread popularity with customers, and considered a standard offering from telecommunications providers. However, as with all technologies, something newer, less expensive, and more flexible came along, namely, VPNs.

13.1.1. Configure a Site-to-Site VPN Between R1 and R4-2

As mentioned in the previous lesson, frame-relay became less desirable once it became practical to host secure connections across the Internet. Today, both site-to-site and remote access VPNs form an integral part of many enterprises, highlighting the importance of having the necessary skills to support them. To begin the VPN configuration process, open Packet Tracer and double click on the R1 icon:


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCNA-Lab-Startup.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
2960-24TT SW1
PC-PT WS1
2811 R1
Cloud-PT Frame-Relay
2911 R2
2960-24TT SW2
PC-PT WS2
2911 R3-1
3560-24PS SW3-1
Server-PT S1
2960-24TT SW3-2
2960-24TT SW3-3
2811 R4-1
2911 Internet
2911
Time: 00:03:27 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source
Device to Drag and Drop to the W

- **Create a GRE Tunnel Interface**: Create a Generic Routing Encapsulation between R1 and R4-1 using the steps below:



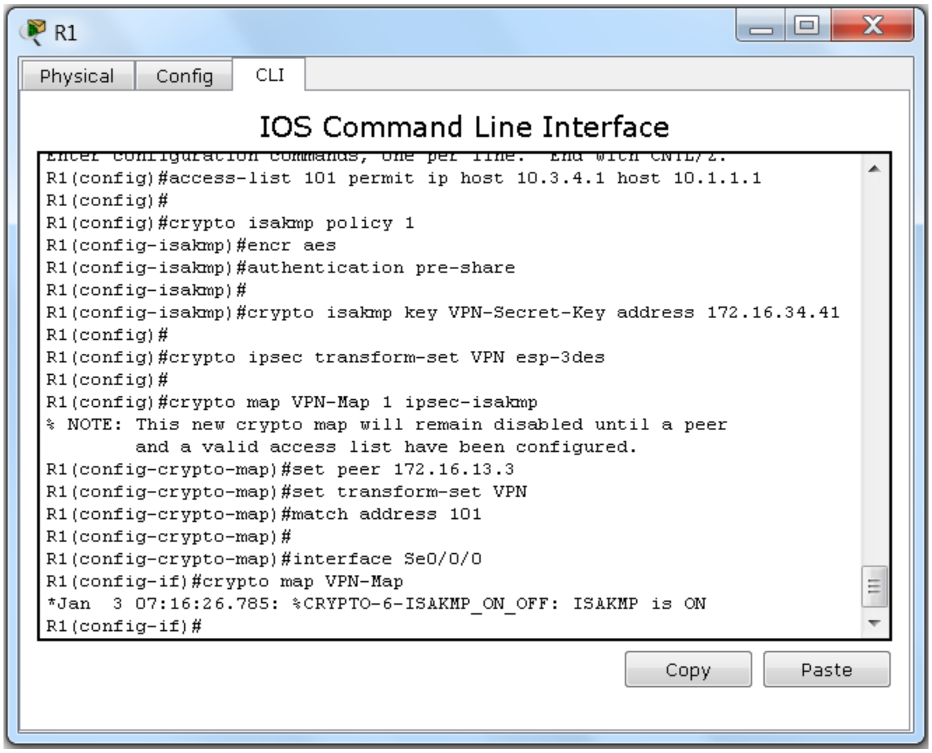
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface tunnel 0

R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

R1(config-if)#tunnel source loopback 0
R1(config-if)#tunnel destination 10.3.4.1
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state tc

R1(config-if)#ip address 172.16.14.1 255.255.255.0
R1(config-if)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface tunnel 0**.
- **Set the tunnel endpoints**: Specify S0/0/0.103 as the source of the interface using the command **tunnel source S0/0/0.103** command. To identify the Fa0/0 interface on 4-1, use the command **tunnel destination 192.168.34.41**. The Layer 2 protocol indicator should come up immediately as a result
- **Configure an IPV4 address on the interface**: Configure a new IP address by entering **ip address 172.17.14.1 255.255.255.0**.
- **Configure a static route**: To force routing to the loopback interface of R4-1 across the tunnel, use the command **ip route 10.3.4.1 255.255.255.255 172.17.14.4**
- **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 or 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

- **Open a CLI window to R4-1**: Close the window accessing R1 and return to Packet Tracer and double-click the icon for R4-1, selecting the CLI tab
- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface tunnel 0**
- **Set the tunnel endpoints**: Specify Fa0/0.34 as the source of the interface using the command **tunnel source Fa0/0.34** command. To identify the Se0/0/0.103 interface on R1, use the command **tunnel destination 172.16.13.1**. The Layer 2 protocol indicator should come up immediately as a result.
- **Configure an IPV4 address on the interface**: Configure a new IP address by entering **ip address 172.17.14.4 255.255.255.0**.
- **Configure a static route**: To force routing to the loopback interface of R1 across the tunnel, use the command **ip route 10.1.1.1 255.255.255.255 172.17.14.1**.
- **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 or 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.
- **Test connectivity across the tunnel:** Test the viability of the connection (as well as show how a tunnel operates) by using the command **traceroute 10.1.1.1**. To begin with, the success of the traceroute shows that the tunnel is working, but also only displays a single Layer 3 hop (the rest are hidden due to the tunnel being a point-to-point connection)

- **Configure an IPsec Encrypted Connection:** With the GRE tunnel now operational, configure the encrypted part of the connection, using the following detailed steps:



```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 101 permit ip host 10.3.4.1 host 10.1.1.1
R1(config)#
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#
R1(config-isakmp)#crypto isakmp key VPN-Secret-Key address 172.16.34.41
R1(config)#
R1(config)#crypto ipsec transform-set VPN esp-3des
R1(config)#
R1(config)#crypto map VPN-Map 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 172.16.13.3
R1(config-crypto-map)#set transform-set VPN
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#
R1(config-crypto-map)#interface Se0/0/0
R1(config-if)#crypto map VPN-Map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Define IPSec Interesting Traffic**: The first step in creating a VPN connection is to identify the traffic to be encrypted. This is determined by an extended access-list, identifying both source and destination traffic. To identify traffic simply between the loopback interfaces, use the command **access-list 101 permit ip host 10.3.4.1 host 10.1.1.1**
- **IKE/ISAKMP Configuration**: To encrypt the traffic, R1 & R4-1 have to securely exchange keys using the Internet Key Exchange Protocol. Configure this as follows:

    - **Create the policy**: Begin creation of the policy by entering the command **crypto isakmp policy 1** (1 is the priority)
    - **Specify the key encryption type**: Several types are available (des, 3des, and aes), use aes by entering the statement **encr aes**.
    - **Identify the authentication to be used**: While options exist for preshared and other types, use preshared for

    - the sake simplicity; use the command **authentication preshare**.
    - **Specify the Diffie-Hellman group id**: This can have a value of 768-bit (group 1, the default) or 1024-bit (group 2). Configure 1024-bit by entering the **group 2** command. Next, exit policy configuration mode with the **exit** command.
    - **Configure the preshared key**: In order to encrypt the traffic, a key must be created for to randomize the traffic. Use the following command: **crypto isakmp key VPN-Secret-Key address 172.16.13.3**.
    - **Create a transform-set**: Specify the encryption type in the transform set (so named because it transforms the traffic). Several combinations are available, but choose esp-aes (Encapsulating Security Payload, using aes). Configure this using the command **crypto ipsec transform-set VPN esp-3des**.
    - **Configure an encryption (crypto) map**: The crypto map ties together the previous configuration elements into a single construct. Begin with the statement **crypto map VPN-Map 1 ipsec-isakmp**. Next, identify the peer (matches the IPV4 address in the crypto map on the other router). Use the statement **set peer 172.16.13.3.** Next, set the transform set created earlier with the command **set transform-set VPN**. Finally, call the access-list identifying the designated traffic with the statement **match address 101**
    - **Apply the crypto map to an interface**: In this case, one of the WAN subinterfaces is the best choice, since packets will enter the router though one of them. Enter interface configuration mode with the command **interface S0/0/0**. Last of all, apply the map to the subinterface with the statement **crypto map VPN-MAP**
    - **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 or 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

- **Open a CLI session on R4-1**: Return to Packet Tracer and click the icon for R4-1 in site 3
- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by

simply pressing **<enter>** (the console line already contains the configuration).

- **Define IPSec Interesting Traffic**: The first step in creating a VPN connection is to identify the traffic to be encrypted. This is determined by an extended access-list, identifying source and destination traffic. To identify traffic simply between the loopback interfaces, use the command **access-list 101 permit ip host 10.3.4.1 host 10.1.1.1**.
- **IKE/ISAKMP Configuration**: To encrypt the traffic, R1 & R4-1 have to securely exchange keys using the Internet Key Exchange Protocol. Configure this as follows:

    - **Create the policy**: Begin creation of the policy by entering the command **crypto isakmp policy 1** (1 is the priority).
    - **Specify the key encryption type**: Several types are available (des, 3des, and aes), use aes by entering the statement **encr aes**.
    - **Identify the authentication to be used**: While options exist for several types, use preshared for the sake simplicity; use the command **authentication preshare**
    - **Specify the Diffie-Hellman group id**: This can have a value of 768-bit (group 1, the default) or 1024-bit (group 2). Configure 1024-bit by entering the **group 2** command. Next, exit policy configuration mode with the **exit** command
    - **Configure the preshared key**: In order to encrypt the traffic, a key must be created for to randomize the traffic. Use the following command: **crypto isakmp key VPN-Secret-Key address 172.16.13.3**
    - **Create a transform-set**: Specify the encryption type in the transform set (so named because it transforms the traffic). Several combinations are available, but choose esp-aes (***Encapsulating Security Payload***, using aes). Configure this using the command **crypto ipsec transform-set VPN aes**.
    - **Configure an encryption (crypto) map**: The crypto map ties together the previous configuration elements into a single construct. Begin with the statement **crypto map VPN-Map 1 ipsec-isakmp**. Next, identify the peer (matches the IPV4 address in the crypto map on the other router). Use the statement **set peer 172.16.13.3.** Next, set the transform set created earlier with the command **set transform-set VPN**. Finally, call the access-list identifying the designated traffic with the statement **match address 101**.
    - **Apply the crypto map to an interface**: In this case, the FastEthernet interface is the best choice, since packets

will enter the router though it. Enter interface configuration mode with the command **Fa0/0**. Last of all, apply the map to the subinterface with the statement **crypto map VPN-MAP**

- **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 or 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.

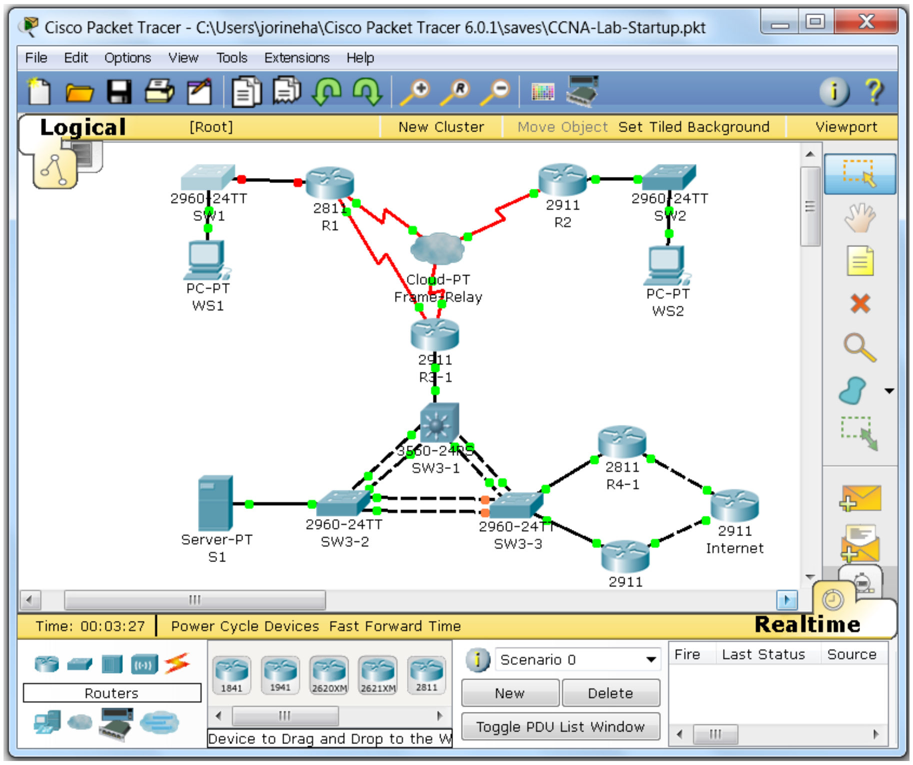
Lesson 14 Lab Exercises

14.1 Network Address Translation Lab Exercises

The designers of the Internet Protocol never imagined that the protocol would go on to nearly universal acceptance, let alone predict the huge amount of devices requiring addressing. In many ways, IPV4 became a victim of its own success, as addresses began to deplete rapidly, with only a handful of workarounds. Classless Interdomain Routing (CIDR) was one of these, and did away with the old classes of addressing, as well as Network Address Translation (covered here). Ultimately, IPV6 (covered in the next lab) solved the shortcomings of IPV4 and is already in the process of displacing it. Even so, NAT is in widespread use today in production networks, and a valuable skill to have as a network engineer. In this set of lab exercises, you will perform NAT configuration on the devices in the lab.

14.1.1. Configure a Simulated Internet Connection

While NAT may be used internally to assist in network migrations, the most common use case is on connections to and from the Internet. In this exercise, you will configure an emulated Internet connection to serve that purpose, to prepare for later NAT configuration. To begin this process, open Packet Tracer and double click on the R4-1 icon:



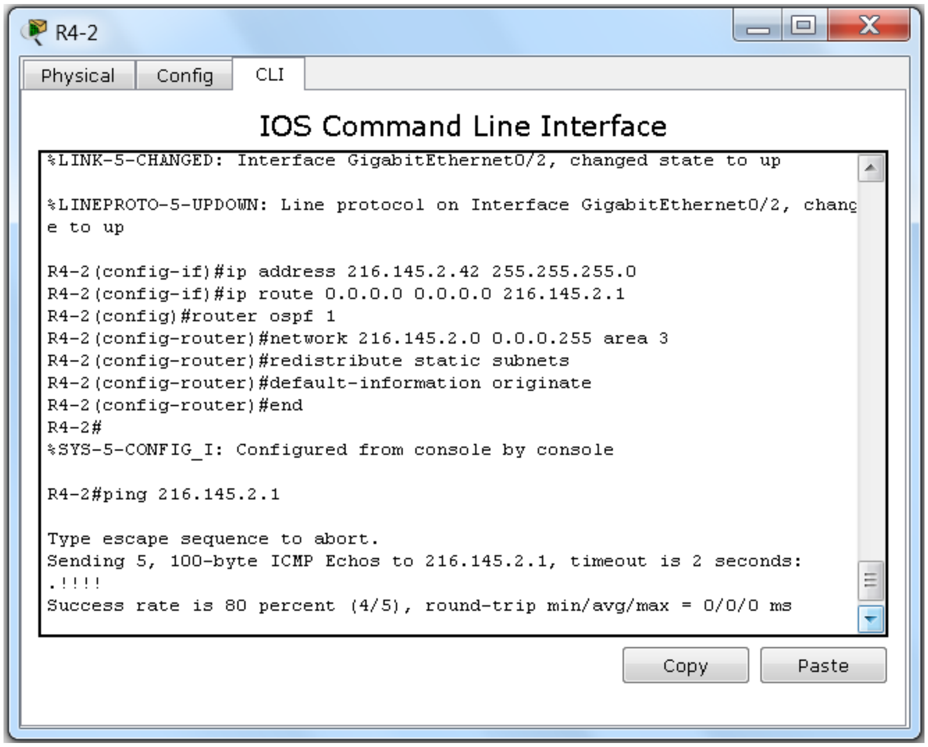
- **Configure Internet Connectivity on R4-1:** Since Internet connectivity is considered a business-critical asset today, many enterprises deploy redundant connections, as reflected in the design of the overall lab. Configure an outbound Internet connection on R4-1 as follows:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
  - **Enter interface configuration mode**: Initiate configuration mode on the Internet-facing interface of R4-1, using the command **interface Fa0/1**
  - **Enable the interface:** Enable the outbound interface with the command **no shutdown**. This should bring up the interface immediately
  - **Assign publicly routable addressing:** In order to connect to the Internet, R4-1 must have a globally routable IPV4 address. Configure addressing on the interface with the command **ip address 216.145.1.41 255.255.255.0**
  - **Test connectivity to the Internet router**: Test the connection to the Internet router by issuing the command **ping 216.145.1.1**. The ping should be successful
  - **Create a static default route**: Add a default route to R4-1 using the command **ip route 0.0.0.0 0.0.0.0 216.145.1.1**.
  - **Edit the OSPF configuration:** Enter OSPF configuration mode with the statement **router ospf 1**, and make the following changes:

    - **Add the new interface to OSPF**: Include the Fa0/1 interface in OSPF by using the command **network 216.145.1.0 0.0.0255 area 3.**
    - **Import the default route into OSPF**: As you did in the route summarization lab, inject the static route by entering **redistribute static subnets**.
    - **Advertise the default route to the OSPF network**: To complete the propagation of the default route to all routers, use the command **default-information-originate**
    - **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 or 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.

- **Configure Internet Connectivity on R4-2:** Repeat the process used on R4-1 on R4-2 as follows:



```
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, chang
e to up

R4-2(config-if)#ip address 216.145.2.42 255.255.255.0
R4-2(config-if)#ip route 0.0.0.0 0.0.0.0 216.145.2.1
R4-2(config)#router ospf 1
R4-2(config-router)#network 216.145.2.0 0.0.0.255 area 3
R4-2(config-router)#redistribute static subnets
R4-2(config-router)#default-information originate
R4-2(config-router)#end
R4-2#
%SYS-5-CONFIG_I: Configured from console by console

R4-2#ping 216.145.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 216.145.2.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
  - **Enter interface configuration mode**: Initiate configuration mode on the Internet-facing interface of R4-2, using the command **interface Gi0/1.**
  - **Enable the interface:** Enable the outbound interface with the command **no shutdown**. This should bring up the interface immediately.
  - **Assign publicly routable addressing:** In order to connect to the Internet, R4-2 must have a globally routable IPV4 address. Configure addressing on the interface with the command **ip address 216.145.2.42 255.255.255.0**.

- **Test connectivity to the Internet router**: Test the connection to the Internet router by issuing the command **ping 216.145.2.1**. The ping should be successful.
- **Create a static default route**: Add a default route to R4-2 using the command **ip route 0.0.0.0 0.0.0.0 216.145.2.1**.
- **Edit the OSPF configuration:** Enter OSPF configuration mode with the statement **router ospf 1**, and make the following changes:

  - **Add the new interface to OSPF**: Include the Gi0/1 interface in OSPF by using the command **network 216.145.2.0 0.0.0255 area 3**
  - **Import the default route into OSPF**: As you did in the route summarization lab, inject the static route by entering **redistribute static subnets**.
  - **Advertise the default route to the OSPF network**: To complete the propagation of the default route to all routers, use the command **default-information-originate**
  - **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 or 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.

**** Because the interfaces of R4-2 are gigabit interfaces, their cost will be lower, making the default route/Internet connection will be preferred over R4-1 ****

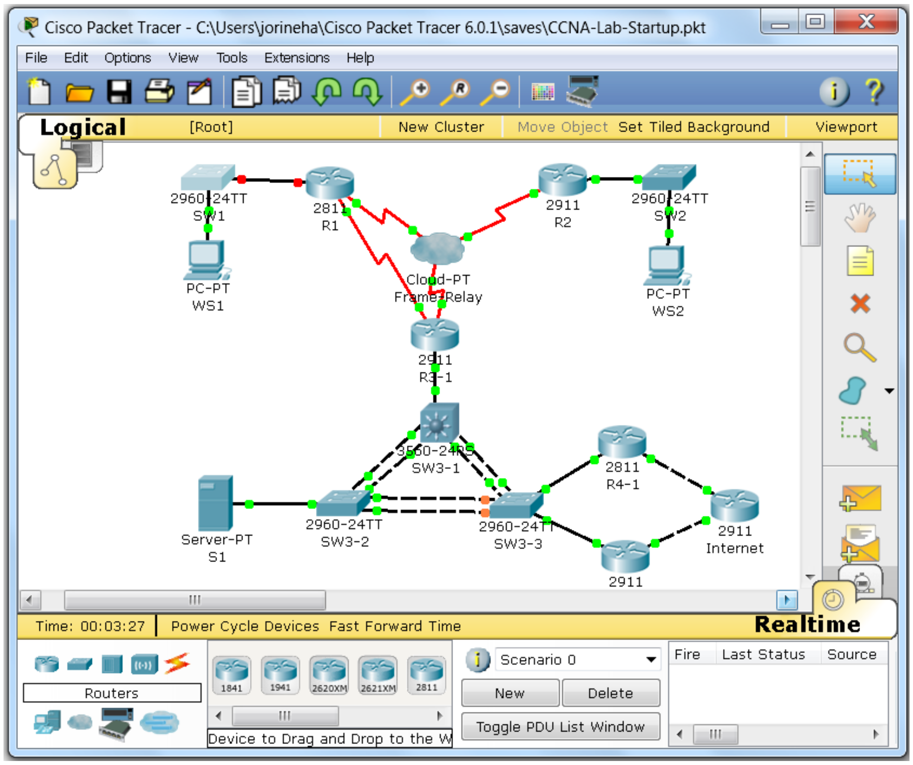
- **Configure HSRP on the VLANs of R4-1 and R4-2:** Due to the importance of the Internet connection, configure Hot Standby Router Protocol on VLANs 1 & 34 on routers R4-1 & R4-2, as follows:

  - **Configure HSRP on R4-1**: Create HSRP instances on the VLAN interface of R4-1, using these steps:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).

    - **Enter interface configuration mode**: Initiate configuration mode on the VLAN 1 interface with the command **interface Fa0/0.1**
    - **Create an HSRP process on VLAN 1:** Enter the command **standby 1 ip 192.168.3.33** to set the group IP address. Have this HSRP router take over upon failure of the other by entering the command **standby 34 preempt**
    - **Enter interface configuration mode**: Initiate configuration mode on the VLAN 34 interface with the command **interface Fa0/0.34**
    - **Create an HSRP process on VLAN 34:** Enter the command **standby 34 ip 192.168.34.33** to set the group IP address. Have this HSRP router take over upon failure of the other by entering the command **standby 34 preempt**
    - **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 or 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.

  - **Configure HSRP on R4-2**: Create HSRP instances on the VLAN interface of R4-2, using the following steps:


Cisco Packet Tracer - C:\Users\jorineha\Cisco Packet Tracer 6.0.1\saves\CCNA-Lab-Startup.pkt
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
2960-24TT SW1
2811 R1
2911 R2
2960-24TT SW2
PC-PT WS1
Cloud-PT Frame-Relay
PC-PT WS2
2911 R3-1
3560-24PS SW3-1
2811 R4-1
Server-PT S1
2960-24TT SW3-2
2960-24TT SW3-3
2911 Internet
2911
Time: 00:03:27 Power Cycle Devices Fast Forward Time
Realtime
Routers
1841 1941 2620XM 2621XM 2811
Device to Drag and Drop to the W
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration)
- **Enter interface configuration mode**: Initiate configuration mode on the VLAN 1 interface with the command **interface Gi0/0.1**
- **Create an HSRP process on VLAN 1:** Enter the command **standby 1 ip 192.168.3.33** to set the group IP address. Increase the priority to 120 with the command **standby 1 priority 120**. Have this HSRP router take over upon failure of the other by entering the command **standby 1 preempt**. Finally, decrease the priority if the Internet connection fails, with the command **standby 1 track Gigabit 0/2**
- **Enter interface configuration mode**: Initiate configuration mode on the VLAN 34 interface with the command **interface Gi0/0.34**
- **Create an HSRP process on VLAN 34:** Enter the command **standby 34 ip 192.168.34.33** to set the group IP address. Increase the priority to 120 with the command **standby 34 priority 120**. Have this HSRP router take over upon failure of the other by entering the command **standby 34 preempt**. Finally, decrease

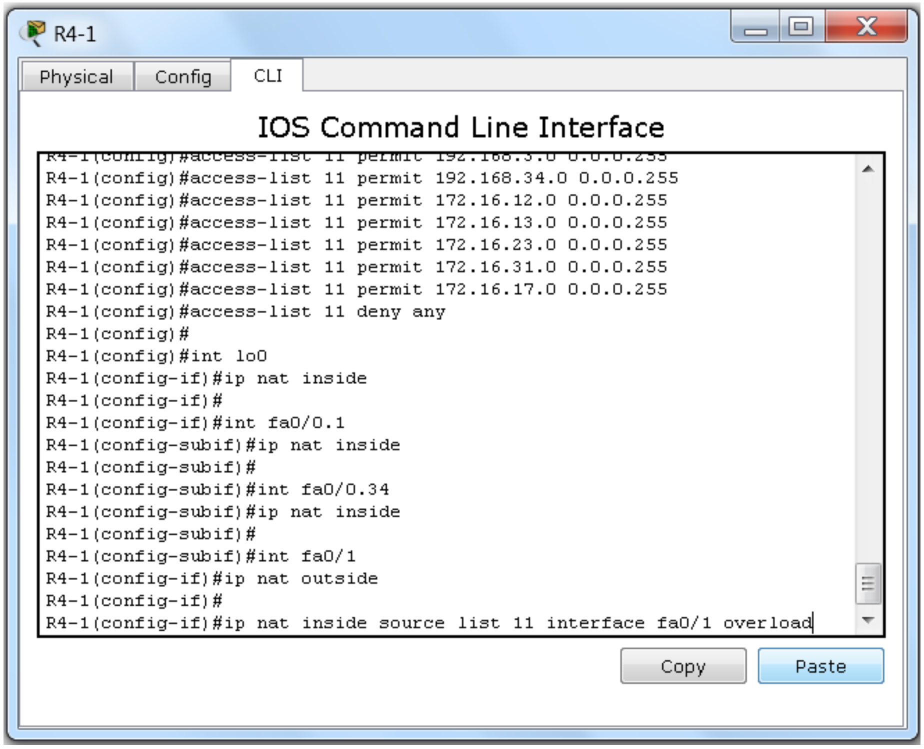
the priority if the Internet connection fails, with the command **standby 34 track Gigabit 0/2**

- **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 or 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
- **Display HSRP Settings:** You may optionally choose to verify the HSRP settings on R4-2 by entering the command **show standby brief** (for abbreviated output) or simply **show standby** (for fuller output)

14.1.2. Configure Port Address Translation on R4-1 and R4-2

While NAT may be used internally to assist in network migrations, the most common use case is on connections to and from the Internet. In this exercise, you will configure an emulated Internet connection to serve that purpose, to prepare for later NAT configuration. To begin this process, open Packet Tracer and double click on the R4-1 icon

- **Configure NAT Overload/PAT on R4-1:** In order for internal hosts to access the Internet, configure Port Address Translation on R4-1 as follows:



```
R4-1(config)#access-list 11 permit 192.168.3.0 0.0.0.255
R4-1(config)#access-list 11 permit 192.168.34.0 0.0.0.255
R4-1(config)#access-list 11 permit 172.16.12.0 0.0.0.255
R4-1(config)#access-list 11 permit 172.16.13.0 0.0.0.255
R4-1(config)#access-list 11 permit 172.16.23.0 0.0.0.255
R4-1(config)#access-list 11 permit 172.16.31.0 0.0.0.255
R4-1(config)#access-list 11 permit 172.16.17.0 0.0.0.255
R4-1(config)#access-list 11 deny any
R4-1(config)#
R4-1(config)#int lo0
R4-1(config-if)#ip nat inside
R4-1(config-if)#
R4-1(config-if)#int fa0/0.1
R4-1(config-subif)#ip nat inside
R4-1(config-subif)#
R4-1(config-subif)#int fa0/0.34
R4-1(config-subif)#ip nat inside
R4-1(config-subif)#
R4-1(config-subif)#int fa0/1
R4-1(config-if)#ip nat outside
R4-1(config-if)#
R4-1(config-if)#ip nat inside source list 11 interface fa0/1 overload
```

- **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
- **Create an access-list:** Routing devices (and firewalls) do not simply perform NAT just because the source addresses are RFC 1918 private addresses. Rather, you need to explicitly identify the address ranges marked for translation, using a standard named/numbered access list. Configure this as outlined here:

  - **access-list 11 permit host 10.1.1.1**
  - **access-list 11 permit host 10.2.2.2**
  - **access-list 11 permit host 10.3.3.3**
  - **access-list 11 permit host 10.3.4.1**
  - **access-list 11 permit host 10.3.4.2**
  - **access-list 11 permit host 10.1.1.1**
  - **access-list 11 permit 192.168.1.0 0.0.0.255**
  - **access-list 11 permit 192.168.11.0 0.0.0.255**
  - **access-list 11 permit 192.168.2.0 0.0.0.255**
  - **access-list 11 permit 192.168.22.0 0.0.0.255**
  - **access-list 11 permit 192.168.3.0 0.0.0.255**
  - **access-list 11 permit 192.168.34.0 0.0.0.255**
  - **access-list 11 permit 172.16.12.0 0.0.0.255**
  - **access-list 11 permit 172.16.13.0 0.0.0.255**
  - **access-list 11 permit 172.16.23.0 0.0.0.255**
  - **access-list 11 permit 172.16.31.0 0.0.0.255**
  - **access-list 11 permit 172.16.17.0 0.0.0.255**
  - **access-list 11 deny any**

- **Identify the interfaces facing the inside and outside of the network**: Explicitly configure the interfaces below with the statements next them:

  - **Loopback 0**: **ip nat inside**
  - **Fa0/0.1**: **ip nat inside**
  - **Fa0/0.34**: **ip nat inside**
  - **Fa0/1: ip nat outside**

- **Map the interfaces and access-list**: The final step is to create mappings between the access-list and the interfaces in the NAT/PAT process. Configure this using the command **ip nat inside source list 1 interface Fa0/1 overload**.
- **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 or 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.

- **Configure NAT Overload/PAT on R4-2:** In order for internal hosts to access the Internet, configure Port Address Translation on R4-2 as follows:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
    - **Create an access-list:** Routing devices (and firewalls) do not simply perform NAT just because the source addresses are RFC 1918 private addresses. Rather, you need to explicitly identify the address ranges marked for translation, using a standard named/numbered access list. Configure this as outlined here:

        - **access-list 11 permit host 10.1.1.1**
        - **access-list 11 permit host 10.2.2.2**
        - **access-list 11 permit host 10.3.3.3**
        - **access-list 11 permit host 10.3.4.1**
        - **access-list 11 permit host 10.3.4.2**
        - **access-list 11 permit host 10.1.1.1**
        - **access-list 11 permit 192.168.1.0 0.0.0.255**
        - **access-list 11 permit 192.168.11.0 0.0.0.255**
        - **access-list 11 permit 192.168.2.0 0.0.0.255**
        - **access-list 11 permit 192.168.22.0 0.0.0.255**
        - **access-list 11 permit 192.168.3.0 0.0.0.255**
        - **access-list 11 permit 192.168.34.0 0.0.0.255**
        - **access-list 11 permit 172.16.12.0 0.0.0.255**
        - **access-list 11 permit 172.16.13.0 0.0.0.255**
        - **access-list 11 permit 172.16.23.0 0.0.0.255**
        - **access-list 11 permit 172.16.31.0 0.0.0.255**
        - **access-list 11 permit 172.16.17.0 0.0.0.255**
        - **access-list 11 deny any**

    - **Identify the interfaces facing the inside and outside of the network**: Explicitly configure the interfaces below with the statements next them:

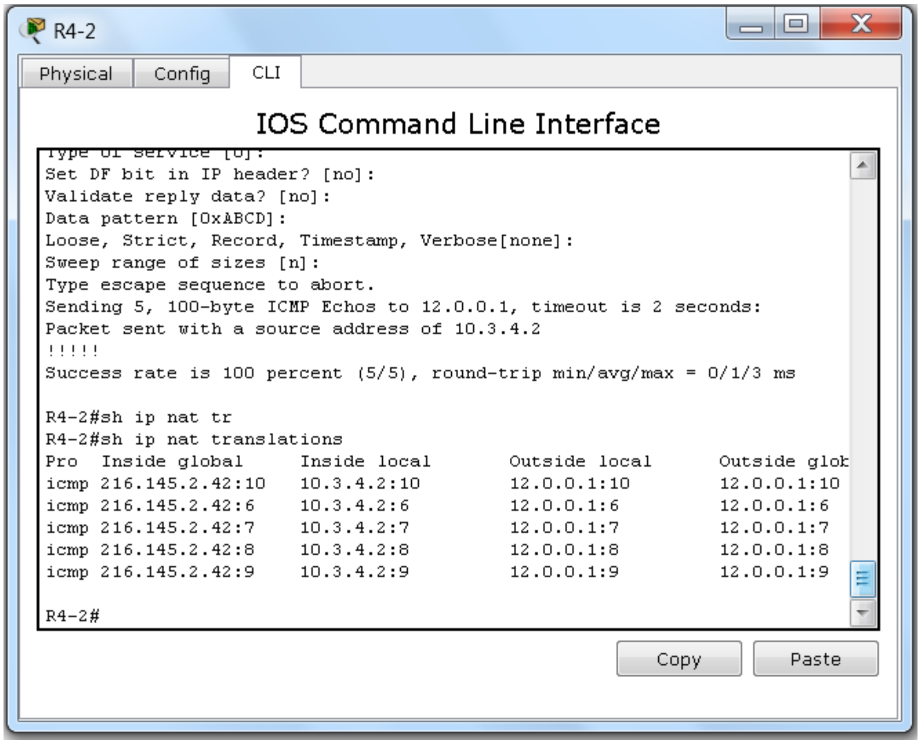
    - **Loopback 0**: **ip nat inside**
    - **Gi0/0.1**: **ip nat inside**
    - **Gi0/0.34**: **ip nat inside**
    - **Gi0/2: ip nat outside**

  - **Map the interfaces and access-list**: The final step is to create mappings between the access-list and the interfaces in the NAT/PAT process. Configure this using the command **ip nat inside source list 1 interface Gi0/2 overload**.
  - **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 or 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.

- **Verify NAT functionality on R4-2**: Perform a brief test to confirm that NAT is correctly configured on R4-2, using the steps below:

  - **Perform an extended ping on R4-2**: In privileged mode at the command line issue the command **ping <enter>** and specify the following values:

    - **Protocol**: IP (the default, simply press **<enter>**)
    - **Target IP Address**: 12.0.0.1
    - **Repeat count**: 5 (the default, simply press **<enter>**)
    - **Datagram size**: 100 (the default, simply press **<enter>**)
    - **Timeout in Seconds**: 2 (the default, simply press **<enter>**)
    - **Extended commands**: Enter **Y** and press **<enter>**
    - **Source address or interface**: 10.3.4.2
    - **Type of service**: 0 (the default, simply press **<enter>**)
    - **Set DF bit in IP Header**: no (the default, simply press **<enter>**)
    - **Validate reply data:** no (the default, simply press **<enter>**)
    - **Data pattern:** 0xABCD (the default, simply press **<enter>**)
    - **Loose, Strict, Record, Timestamp, Verbose:** none (the default, simply press **<enter>**)
    - **Sweep range of sizes:** n (the default, simply press **<enter>**)
    - **Result:** The ping should succeed.



```
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 12.0.0.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.4.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

R4-2#sh ip nat tr
R4-2#sh ip nat translations
Pro  Inside global      Inside local       Outside local      Outside glob
icmp 216.145.2.42:10    10.3.4.2:10        12.0.0.1:10        12.0.0.1:10
icmp 216.145.2.42:6     10.3.4.2:6         12.0.0.1:6         12.0.0.1:6
icmp 216.145.2.42:7     10.3.4.2:7         12.0.0.1:7         12.0.0.1:7
icmp 216.145.2.42:8     10.3.4.2:8         12.0.0.1:8         12.0.0.1:8
icmp 216.145.2.42:9     10.3.4.2:9         12.0.0.1:9         12.0.0.1:9

R4-2#
```

- **Observe the results**: While still at the command line, enter the command show **ip nat translations**. The output (as shown above), should contain five entries, corresponding to the five pings sent in the previous step.

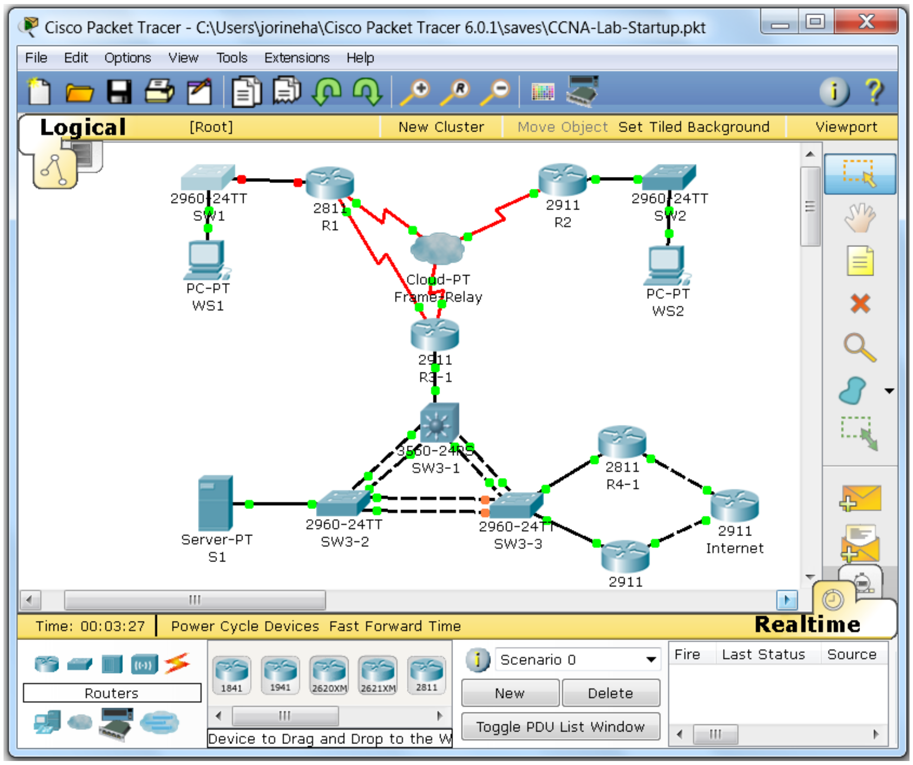
Lesson 15 Lab Exercises

15.1 IPV6 Lab Exercises

As discussed in the previous lab instructions, IP version 6 represents an entirely new redesigned protocol, intended to replace the current version of the Internet Protocol. Though the numbering format (for 128-bit addresses) may take some getting used to, the internal mechanics of the protocol are not overly difficult to grasp. To build the necessary skills to address IPV6 topics, you will perform a number of tasks in this lab to assist in that regard.

15.1.1. Configure IPV6 Addressing on Routers R1, R2 & R3

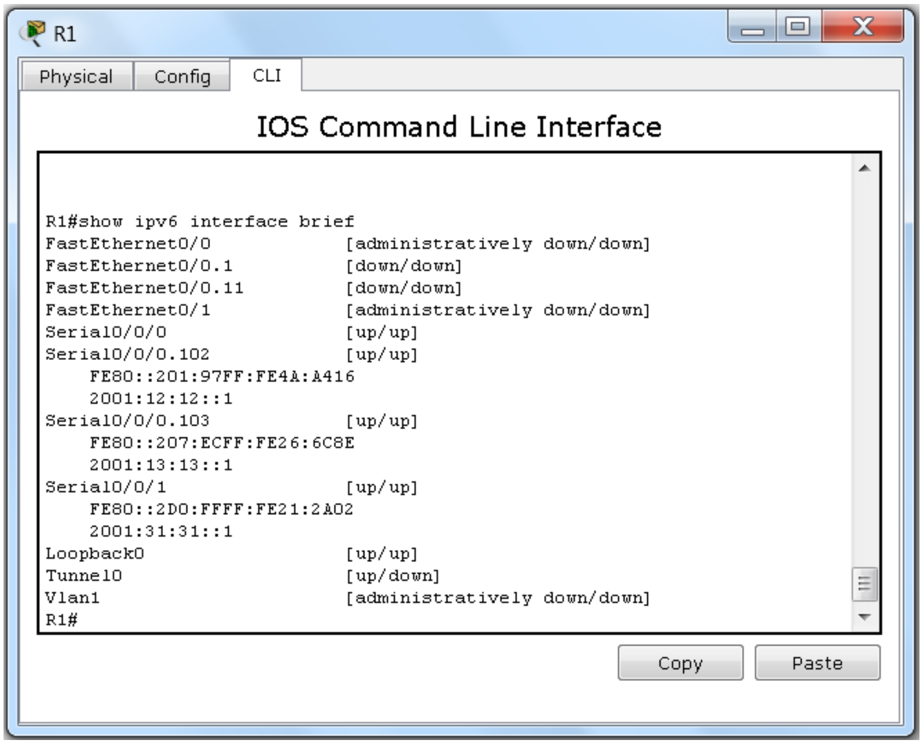
One of the most common implementations of IPV6 is deploying it concurrently with IPV6 in the network. The first configuration task will consist of adding IPV6 addresses to the devices in the lab network. To begin, open Packet Tracer and double click on the R1 icon, as shown below:



- **Configure IPV6 on R1:** Enable IPV6 and assign addresses to the WAN interface only as follows:
  - o **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal**

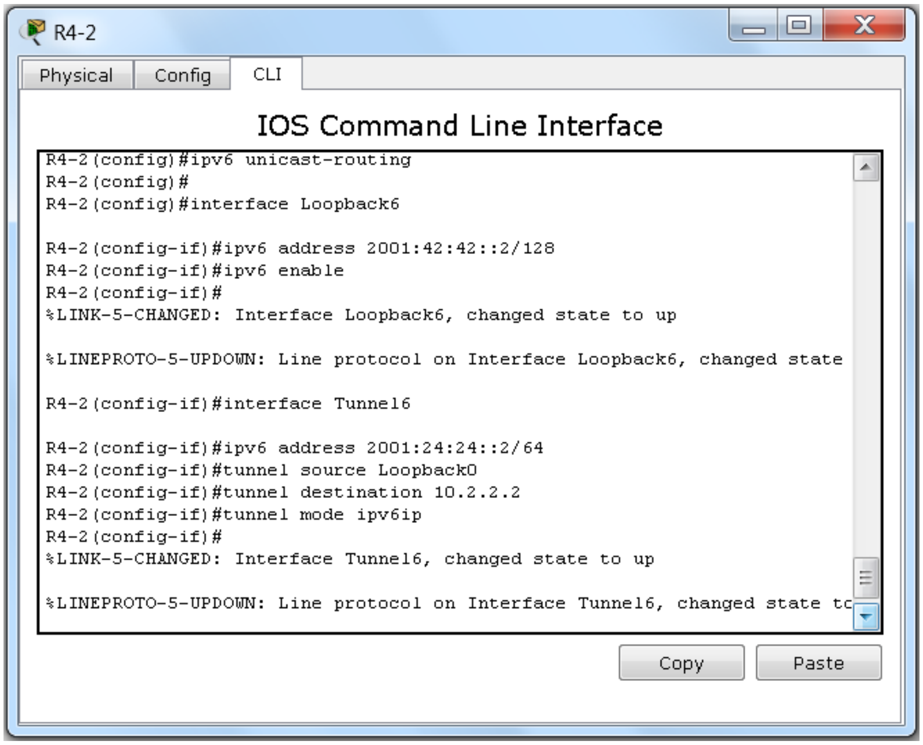
command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).

- **Enable routing for IPV6:** Routing for IPV6 must be explicitly enable in order to function, so enter the command **ipv6 unicast-routing**.
- **Enter interface configuration mode**: Initiate configuration mode on the WAN interface with the command **interface SE0/0/0.102.**
- **Configure IPV6 addressing on Se0/0/0.102:** Assign a globally routable address with the statement **ipv6 address 2001:12:12::1/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
- **Configure IPV6 addressing on Se0/0/0.103:** Assign a globally routable address with the statement **ipv6 address 2001:13:13::1/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
- **Configure IPV6 addressing on Se0/0/1:** Assign a globally routable address with the statement **ipv6 address 2001:31:31::1/64.** In addition, to enable link-local addressing, add the command **ipv6 enable**.
- **Verify IPV6 addressing:** To confirm the addressing on the interfaces, issue the **show ipv6 interface brief** command, which should have output similar to that displayed here:



```
R1#show ipv6 interface brief
FastEthernet0/0            [administratively down/down]
FastEthernet0/0.1          [down/down]
FastEthernet0/0.11         [down/down]
FastEthernet0/1            [administratively down/down]
Serial0/0/0                [up/up]
Serial0/0/0.102            [up/up]
    FE80::201:97FF:FE4A:A416
    2001:12:12::1
Serial0/0/0.103            [up/up]
    FE80::207:ECFF:FE26:6C8E
    2001:13:13::1
Serial0/0/1                [up/up]
    FE80::2D0:FFFF:FE21:2A02
    2001:31:31::1
Loopback0                  [up/up]
Tunnel0                    [up/down]
Vlan1                      [administratively down/down]
R1#
```

- **Configure IPV6 on R2:** Enable IPV6 and assign addresses to the WAN interface only as follows:



```
R4-2(config)#ipv6 unicast-routing
R4-2(config)#
R4-2(config)#interface Loopback6

R4-2(config-if)#ipv6 address 2001:42:42::2/128
R4-2(config-if)#ipv6 enable
R4-2(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state

R4-2(config-if)#interface Tunnel6

R4-2(config-if)#ipv6 address 2001:24:24::2/64
R4-2(config-if)#tunnel source Loopback0
R4-2(config-if)#tunnel destination 10.2.2.2
R4-2(config-if)#tunnel mode ipv6ip
R4-2(config-if)#
%LINK-5-CHANGED: Interface Tunnel6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel6, changed state tc
```

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
  - **Enable routing for IPV6:** Routing for IPV6 must be explicitly enable in order to function, so enter the command ipv6 unicast-routing
  - **Enter interface configuration mode**: Initiate configuration mode on the WAN interface with the command **interface SE0/0/0.201.**
  - **Configure IPV6 addressing on Se0/0/0.201:** Assign a globally routable address with the statement **ipv6 address 2001:12:12::2/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
  - **Configure IPV6 addressing on Se0/0/0.203:** Assign a globally routable address with the statement **ipv6 address 2001:23:23::2/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.

  - **Verify IPV6 addressing:** To confirm the addressing on the interfaces, issue the **show ipv6 interface brief** command, and review the output.

- **Configure IPV6 on R3-1:** Enable IPV6 and assign addresses to the WAN interface only as follows:

  - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
  - **Enable routing for IPV6:** Routing for IPV6 must be explicitly enable in order to function, so enter the command **ipv6 unicast-routing**.
  - **Enter interface configuration mode**: Initiate configuration mode on the WAN interface with the command **interface SE0/0/0.301.**
  - **Configure IPV6 addressing on Se0/0/0.301:** Assign a globally routable address with the statement **ipv6 address 2001:13:13::3/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
  - **Configure IPV6 addressing on Se0/0/0.302:** Assign a globally routable address with the statement **ipv6 address 2001:23:23::23/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
  - **Configure IPV6 addressing on Se0/0/1:** Assign a globally routable address with the statement **ipv6 address 2001:31:31::3/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.
  - **Verify IPV6 addressing:** To confirm the addressing on the interfaces, issue the **show ipv6 interface brief** command, and review the output.
  - **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 or 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.

- **Verify IPV6 Connectivity Between R3-1, R1 & R2**: To complete confirmation of the IPV6 configuration, perform ping tests to the other IPV6 addresses, as outlined here:

        - **Test between R3-1 & R1**: Use ping to confirm connectivity on both interfaces between R1 and R3-1 using these commands:

            - **ping ipv6 2001:13:13::1** (should be successful).
            - **ping ipv6 2001:31:31::1** (should be successful).

        - **Test between R3-1 & R2**: Enter the **ping ipv6 2001:23:23::2** command to test the connection (should be successful).

15.1.2. Configure EIGRP Routing for IPV6 on Routers R2 & R4-2

Most of the routing options in IPV4 are duplicated in IPV6, including static and dynamic routing. Routing protocols supported on IPV6 are RIP (referred to as RIPng), OSPFv3, EIGRP, and others. In addition, several coexistence mechanisms exist (you employed one, dual-stack, previously). Many of the other transition mechanisms involve some type of tunneling, which will be included in this lab. Configure EIGRP for IPV6 between R2 and R4-2 using the process below. To begin, open Packet Tracer and double click on the R2 icon, as described below:

- **Configure IPV6 EIGRP Routing on R2:** Configure IPV6 EIGRP routing on R2 as follows:

    - **Create a GRE Tunnel Interface**: Create a Generic Routing Encapsulation between R2 and R4-2 using the steps below:

        - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
        - **Enable routing for IPV6:** Routing for IPV6 must be explicitly enable in order to function, so enter the command **ipv6 unicast-routing**.
        - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface tunnel 6**.
        - **Configure the GRE tunnel for IPV6**: Set the tunnel mode to support IPV6 traffic with the command **tunnel mode ipv6ip**.
        - **Set the tunnel endpoints**: Specify loopback 0 as the source of the interface using the command **tunnel source Loopback 0** command. To identify the loopback 0 interface on 4-2, use the command **tunnel destination 10.3.4.2**. The Layer 2 protocol indicator should come up immediately as a result.

        - **Configure an IPV6 address on the interface**: Configure a new IP address by entering **ipv6 address 2001:24:24::2/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.

    - **Configure an IPV6 loopback interface:** Create an IPV6-only loopback interface as follows:

        - **Enter interface configuration mode**: Enter interface configuration mode by entering **interface loopback6**.
        - **Configure IPV6 Addressing**: Assign an address with the command ipv6 address 2001:2:2::2/128.
        - **Enable the interface for IPV6**: Enable link-local addressing by using the command **ipv6 enable**.

    - Configure EIGRP for IPV6 on R2:

        - **Start the EIGRP IPV6 routing process**: As with IPV4, create a routing process for EIGRP using the router command, with the syntax **ipv6 router eigrp 100**.
        - Assign the router-id: EIGRP for IPV6 will not operate without a router-id configured, which oddly enough must be an IPV4 address. Use the command **router-id 10.2.2.2**.
        - **Enable the routing process**: By default EIGRP routing is in a down state, so enable it using the **no shutdown** command.
        - **No network commands:** In the IPV6 version of EIGRP, instead of using **network** statements to specify the participating interfaces, configuration takes place on the interfaces themselves. On both loopback 6 and Tunnel 6, use the command **ipv6 eigrp 100** to complete the configuration process.
        - **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 or 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.

- **Configure IPV6 EIGRP Routing on R4-2:** Configure IPV6 EIGRP routing on R4-2 as follows:

    - **Create a GRE Tunnel Interface**: Create a Generic Routing Encapsulation between R4-2 and R2 using the steps below:

    - **Enter global configuration mode:** If you have not already done so, enter configuration mode using the **configure terminal** command from privileged mode. Enter privileged exec mode by simply pressing **<enter>** (the console line already contains the configuration).
    - **Enable routing for IPV6:** Routing for IPV6 must be explicitly enable in order to function, so enter the command **ipv6 unicast-routing**.
    - **Enter interface configuration mode**: Invoke interface configuration mode with the command **interface tunnel 6**.
    - **Configure the GRE tunnel for IPV6**: Set the tunnel mode to support IPV6 traffic with the command **tunnel mode ipv6ip**.
    - **Set the tunnel endpoints**: Specify loopback 0 as the source of the interface using the command **tunnel source Loopback 0** command. To identify the loopback 0 interface on 4-2, use the command **tunnel destination 10.2.2.2**. The Layer 2 protocol indicator should come up immediately as a result.
    - **Configure an IPV6 address on the interface**: Configure a new IP address by entering **ipv6 address 2001:24:24::4/64**. In addition, to enable link-local addressing, add the command **ipv6 enable**.

- **Configure an IPV6 loopback interface:** Create an IPV6-only loopback interface as follows:

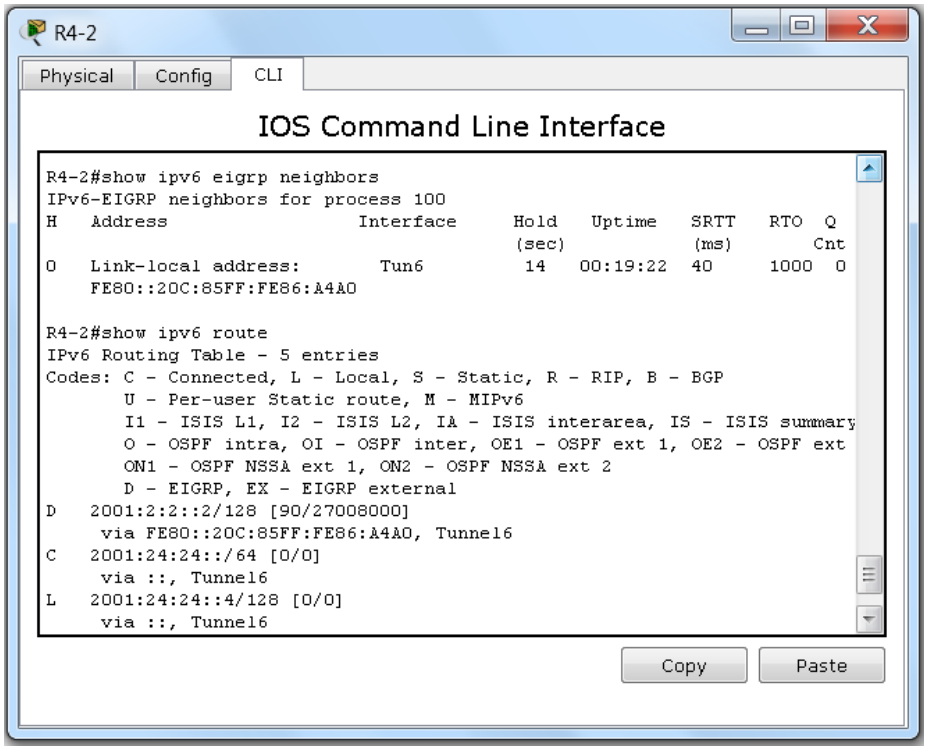
    - **Enter interface configuration mode**: Enter interface configuration mode by entering **interface loopback6**.
    - **Configure IPV6 Addressing**: Assign an address with the command **ipv6 address 2001:42:42::4/128**.
    - **Enable the interface for IPV6**: Enable link-local addressing by using the command **ipv6 enable**.

- Configure EIGRP for IPV6 on R4-2:

    - **Start the EIGRP IPV6 routing process**: As with IPV4, create a routing process for EIGRP using the router command, with the syntax **ipv6 router eigrp 100**.
    - Assign the router-id: EIGRP for IPV6 will not operate without a router-id configured, which oddly enough must be an IPV4 address. Use the command **router-id 10.3.4.2**.
    - **Enable the routing process**: By default EIGRP routing is in a down state, so enable it using the **no shutdown** command.

    - **No network commands:** In the IPV6 version of EIGRP, instead of using **network** statements to specify the participating interfaces, configuration takes place on the interfaces themselves. On both loopback 6 and Tunnel 6, use the command **ipv6 eigrp 100** to complete the configuration process.
    - **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 or 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.

- **Verify IPV6 EIGRP Routing:** Verify that IPV6 EIGRP routing is functioning correctly on R4-2 by using the following process:



```
R4-2#show ipv6 eigrp neighbors
IPv6-EIGRP neighbors for process 100
H   Address                     Interface     Hold   Uptime    SRTT    RTO  Q
                                              (sec)            (ms)        Cnt
0   Link-local address:          Tun6          14    00:19:22  40      1000  0
    FE80::20C:85FF:FE86:A4A0

R4-2#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
D   2001:2:2::2/128 [90/27008000]
     via FE80::20C:85FF:FE86:A4A0, Tunnel6
C   2001:24:24::/64 [0/0]
     via ::, Tunnel6
L   2001:24:24::4/128 [0/0]
     via ::, Tunnel6
```

- **Display the IPV6 EIGRP neighbor table**: To verify that neighbor relationships are intact, issue the command show ipv6 eigrp neighbors (see figure above).
- **Show the contents of the IPV6 routing table**: To verify the presence of an IPV6 EIGRP route, enter the statement show ipv6 route, and look for the routing entry of 2001:2:2::2/128 with the D (EIGRP) route identifier.
- **Verify full connectivity**: To complete the testing process, issue the command **ping ipv6 2001:2:2::2**. If all configurations are operational, the ping should succeed.

Final Device Configurations

16.1 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:

16.1.1. R1

```
hostname R1

enable secret cisco

ipv6 unicast-routing

username R3-1 password cisco
username cisco secret cisco

crypto isakmp policy 1
 encr aes
 authentication pre-share

crypto isakmp key VPN-Secret-Key address 172.16.34.41

crypto ipsec transform-set VPN esp-3des

crypto map VPN-Map 1 ipsec-isakmp
 set peer 172.16.13.3
 set transform-set VPN
 match address 101

ip ssh version 2
ip domain-name cisco.com

interface Loopback0
 ip address 10.1.1.1 255.255.255.255

interface Tunnel0
 ip address 172.17.14.1 255.255.255.0
 tunnel destination 192.168.34.41
 tunnel mode gre ip

interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown

interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.0

interface FastEthernet0/0.11
 encapsulation dot1Q 11
 ip address 192.168.11.1 255.255.255.0

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

interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 crypto map VPN-Map

interface Serial0/0/0.102 point-to-point
 ip address 172.16.12.1 255.255.255.0
 frame-relay interface-dlci 102
 ipv6 address 2001:12:12::1/64
 ipv6 enable

interface Serial0/0/0.103 point-to-point
 ip address 172.16.13.1 255.255.255.0
 frame-relay interface-dlci 103
 ipv6 address 2001:13:13::1/64
 ipv6 enable

interface Serial0/0/1
 ip address 172.16.31.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 ipv6 address 2001:31:31::1/64
 ipv6 enable

interface Vlan1
 no ip address
 shutdown

router ospf 1
 router-id 10.1.1.1
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 1
 network 10.1.1.1 0.0.0.0 area 1

ip classless
ip route 10.3.4.1 255.255.255.255 172.17.14.4

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 192.168.3.0 0.0.0.255
access-list 1 deny any
access-list 101 permit ip host 10.3.4.1 host 10.1.1.1

line con 0
 password cisco
 privilege level 15

line aux 0

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.1.2. R2

```
 hostname R2

enable secret  cisco

ipv6 unicast-routing

username cisco secret  cisco

license udi pid CISCO2911/K9 sn FTX15249Z6U

ip ssh version 2
ip domain-name cisco.com
ip name-server 192.168.33.33

spanning-tree mode pvst
```

```
interface Loopback0
 ip address 10.2.2.2 255.255.255.255

interface Loopback6
 no ip address
 ipv6 address 2001:2:2::2/128
 ipv6 eigrp 100
 ipv6 enable

interface Tunnel6
 no ip address
 mtu 1476
 ipv6 address 2001:24:24::2/64
 ipv6 eigrp 100
 tunnel source Loopback0
 tunnel destination 10.3.4.2
 tunnel mode ipv6ip

interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.2.2 255.255.255.0

interface GigabitEthernet0/0.22
 encapsulation dot1Q 22
 ip address 192.168.22.2 255.255.255.0

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

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

interface Serial0/0/0
 no ip address
 encapsulation frame-relay
```

```
interface Serial0/0/0.201 point-to-point
 ip address 172.16.12.2 255.255.255.0
 frame-relay interface-dlci 201
 ipv6 address 2001:12:12::2/64
 ipv6 enable

interface Serial0/0/0.203 point-to-point
 ip address 172.16.23.2 255.255.255.0
 frame-relay interface-dlci 203
 ipv6 address 2001:23:23::2/64
 ipv6 enable

interface Serial0/0/1
 no ip address
 shutdown

interface Vlan1
 no ip address
 shutdown

router ospf 1
 router-id 10.2.2.2
 log-adjacency-changes
 redistribute static subnets
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 2
 network 10.2.2.2 0.0.0.0 area 2

ipv6 router eigrp 100
 router-id 10.2.2.2
 no shutdown

ip classless
ip route 10.2.2.0 255.255.255.0 Null0

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 192.168.3.0 0.0.0.255
access-list 1 deny any

line con 0
 password cisco
 privilege level 15
 no login

line aux 0

line vty 0 4
```

```
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.1.3. R3-1

```
hostname R3-1

enable secret cisco

ipv6 unicast-routing

username R1 password cisco
username cisco secret cisco

license udi pid CISCO2911/K9 sn FTX1524V64G

ip ssh version 2
ip domain-name cisco.com

spanning-tree mode pvst

interface Loopback0
 ip address 10.3.3.3 255.255.255.255

interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto

interface GigabitEthernet0/0.1
 bandwidth 1000
 encapsulation dot1Q 1 native
 ip address 192.168.3.3 255.255.255.0
 ip ospf priority 200

interface GigabitEthernet0/0.34
 encapsulation dot1Q 34
 ip address 192.168.34.3 255.255.255.0
 ip ospf priority 200
```

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

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

interface Serial0/0/0
 no ip address
 encapsulation frame-relay

interface Serial0/0/0.301 point-to-point
 ip address 172.16.13.3 255.255.255.0
 frame-relay interface-dlci 301
 ipv6 address 2001:13:13::4/64
 ipv6 enable

interface Serial0/0/0.302 point-to-point
 ip address 172.16.23.3 255.255.255.0
 frame-relay interface-dlci 302
 ipv6 address 2001:23:23::3/64
 ipv6 enable

interface Serial0/0/1
 ip address 172.16.31.3 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 ipv6 address 2001:31:31::3/64
 ipv6 enable

interface Vlan1
 no ip address
 shutdown

router ospf 1
 router-id 10.3.3.3
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.34.0 0.0.0.255 area 3
 network 192.168.3.0 0.0.0.255 area 3
 network 10.3.3.3 0.0.0.0 area 3
```

```
ip classless

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 192.168.3.0 0.0.0.255
access-list 1 deny any

line con 0
 password cisco
 no login
 privilege level 15

line aux 0

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.1.4. R4-1

```
hostname R4-1

enable secret 5 cisco

username cisco secret cisco

crypto isakmp policy 1
 encr aes
 authentication pre-share

crypto isakmp key VPN-Secret-Key address 172.16.13.1

crypto ipsec transform-set VPN esp-3des

crypto map VPN-Map 1 ipsec-isakmp
 set peer 172.16.13.1
 set transform-set VPN
 match address 101
```

```
ip ssh version 2
ip domain-name cisco.com

spanning-tree mode pvst

interface Loopback0
 ip address 10.3.4.1 255.255.255.255
 ip nat inside

interface Tunnel0
 ip address 172.17.14.4 255.255.255.0
 tunnel destination 172.16.13.1
 tunnel mode gre ip

interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 crypto map VPN-Map

interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.3.41 255.255.255.0
 ip nat inside
 standby version 2
 standby 1 ip 192.168.3.33
 standby 1 preempt

interface FastEthernet0/0.34
 encapsulation dot1Q 34
 ip address 192.168.34.41 255.255.255.0
 ip nat inside
 standby version 2
 standby 34 ip 192.168.34.33
 standby 34 preempt

interface FastEthernet0/1
 ip address 216.145.1.41 255.255.255.0
 ip nat outside
 duplex auto
 speed auto

interface Vlan1
 no ip address
 shutdown

router ospf 1
 router-id 10.3.4.1
 log-adjacency-changes
 redistribute static subnets
 network 10.3.4.1 0.0.0.0 area 3
 network 192.168.0.0 0.0.255.255 area 3
 network 216.145.1.0 0.0.0.255 area 3
 default-information originate

ip nat inside source list 11 interface FastEthernet0/1 overload
ip classless
ip route 10.1.1.1 255.255.255.255 172.17.14.1
ip route 0.0.0.0 0.0.0.0 216.145.1.1

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 192.168.3.0 0.0.0.255
access-list 1 deny any
access-list 101 permit ip host 10.1.1.1 host 10.3.4.1
access-list 11 permit host 10.1.1.1
access-list 11 permit host 10.2.2.2
access-list 11 permit host 10.3.3.3
access-list 11 permit host 10.3.4.1
access-list 11 permit host 10.3.4.2
access-list 11 permit 192.168.1.0 0.0.0.255
access-list 11 permit 192.168.11.0 0.0.0.255
access-list 11 permit 192.168.2.0 0.0.0.255
access-list 11 permit 192.168.22.0 0.0.0.255
access-list 11 permit 192.168.3.0 0.0.0.255
access-list 11 permit 192.168.34.0 0.0.0.255
access-list 11 permit 172.16.12.0 0.0.0.255
access-list 11 permit 172.16.13.0 0.0.0.255
access-list 11 permit 172.16.23.0 0.0.0.255
access-list 11 permit 172.16.31.0 0.0.0.255
access-list 11 permit 172.16.17.0 0.0.0.255
access-list 11 deny any

no cdp run

line con 0
 password 7 0822455D0A16
 privilege level 15
 no login

line aux 0

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.1.5. R4-2

```
hostname R4-2

enable secret cisco

ipv6 unicast-routing

username cisco secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

license udi pid CISCO2911/K9 sn FTX1524VP8Z

ip ssh version 2
ip domain-name cisco.com

spanning-tree mode pvst

interface Loopback0
 ip address 10.3.4.2 255.255.255.255
 ip nat inside

interface Loopback6
 no ip address
 ipv6 address 2001:42:42::4/128
 ipv6 eigrp 100
 ipv6 enable

interface Tunnel6
 no ip address
 mtu 1476
 ipv6 address 2001:24:24::4/64
 ipv6 eigrp 100
 ipv6 enable
 tunnel source Loopback0
 tunnel destination 10.2.2.2
 tunnel mode ipv6ip

interface GigabitEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto

interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.3.42 255.255.255.0
 ip access-group FILTER-PING in
 ip nat inside
 standby version 2
 standby 1 ip 192.168.3.33
 standby 1 priority 120
 standby 1 preempt
 standby 1 track GigabitEthernet0/2

interface GigabitEthernet0/0.34
 encapsulation dot1Q 34
 ip address 192.168.34.42 255.255.255.0
 ip nat inside
 standby version 2
 standby 34 ip 192.168.34.33
 standby 34 priority 120
 standby 34 preempt
 standby 34 track GigabitEthernet0/2

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

interface GigabitEthernet0/2
 ip address 216.145.2.42 255.255.255.0
 ip nat outside
 duplex auto
 speed auto

interface Vlan1
 no ip address
 shutdown

router ospf 1
 router-id 10.3.4.2
 log-adjacency-changes
 redistribute static subnets
 network 10.3.4.2 0.0.0.0 area 3
 network 192.168.0.0 0.0.255.255 area 3
 network 216.145.2.0 0.0.0.255 area 3
 default-information originate

ipv6 router eigrp 100
 router-id 10.3.4.2
 no shutdown

ip nat inside source list 11 interface GigabitEthernet0/2 overload
ip classless
ip route 0.0.0.0 0.0.0.0 216.145.2.1

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 192.168.3.0 0.0.0.255
access-list 1 deny any
ip access-list extended FILTER-PING
 deny icmp 192.168.34.0 0.0.0.255 192.168.3.0 0.0.0.255 echo
 permit ip any any
access-list 11 permit host 10.1.1.1
access-list 11 permit host 10.2.2.2
access-list 11 permit host 10.3.3.3
access-list 11 permit host 10.3.4.1
access-list 11 permit host 10.3.4.2
access-list 11 permit 192.168.1.0 0.0.0.255
access-list 11 permit 192.168.11.0 0.0.0.255
access-list 11 permit 192.168.2.0 0.0.0.255
access-list 11 permit 192.168.22.0 0.0.0.255
access-list 11 permit 192.168.3.0 0.0.0.255
access-list 11 permit 192.168.34.0 0.0.0.255
access-list 11 permit 172.16.12.0 0.0.0.255
access-list 11 permit 172.16.13.0 0.0.0.255
access-list 11 permit 172.16.23.0 0.0.0.255
access-list 11 permit 172.16.31.0 0.0.0.255
access-list 11 permit 172.16.17.0 0.0.0.255
access-list 11 deny any

line con 0
 password cisco
 privilege level 15
no login

line aux 0

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
```

```
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.2 *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:

16.2.1. SW1

```
hostname SW1

enable secret cisco

ip ssh version 2
ip domain-name cisco.com

username cisco secret cisco

spanning-tree mode pvst

interface FastEthernet0/1
 switchport mode trunk

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
 switchport access vlan 11
 switchport mode access

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
 description MANAGEMENT VLAN
 ip address 192.168.1.111 255.255.255.0

ip default-gateway 192.168.1.1

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 192.168.3.0 0.0.0.255
access-list 1 deny any
line con 0
 password cisco
 privilege level 15
 no login

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.2.2. SW2

```
 hostname SW2
 enable secret cisco

ip ssh version 2
ip domain-name cisco.com

username cisco secret cisco
spanning-tree mode pvst

interface FastEthernet0/1

interface FastEthernet0/2
 switchport mode trunk

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
 switchport access vlan 22
 switchport mode access

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1
 description MANAGEMENT VLAN
 ip address 192.168.2.222 255.255.255.0

ip default-gateway 192.168.2.2

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 192.168.3.0 0.0.0.255
access-list 1 deny any
line con 0
 password cisco
 privilege level 15
```

```
no login

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.2.3. SW3-1

```
hostname SW3-1

enable  cisco

ip routing

username cisco secret cisco

ip ssh version 2
ip domain-name cisco.com

spanning-tree mode rapid-pvst
spanning-tree vlan 1-4094 priority 24576

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk

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
 channel-group 1 mode on
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/22
 channel-group 1 mode on
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/23
 channel-group 2 mode on
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet0/24
 channel-group 2 mode on
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface GigabitEthernet0/1
interface GigabitEthernet0/2

interface Port-channel 1
 switchport mode trunk

interface Port-channel 2
 switchport mode trunk

interface Vlan1
 description MANAGEMENT VLAN
 ip address 192.168.3.111 255.255.255.0

interface Vlan34
 description PRODUCTION_VLAN
 ip address 192.168.34.111 255.255.255.0

ip classless

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 192.168.3.0 0.0.0.255
access-list 1 deny any

banner motd ————————————————————Welcome to CCNA Lab SW3-1!————————————————————

line con 0
 password cisco
 privilege level 15
 no login

line aux 0

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.2.4. SW3-2

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

hostname SW3-2

enable secret cisco

ip ssh version 2
ip domain-name cisco.com

username cisco secret cisco

spanning-tree mode rapid-pvst
spanning-tree vlan 1-1024 priority 28672

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3
 switchport access vlan 33
 switchport mode access
 spanning-tree portfast

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
 channel-group 1 mode on
 switchport mode trunk

interface FastEthernet0/24
 channel-group 1 mode on
 switchport mode trunk

interface GigabitEthernet1/1
 channel-group 3 mode on
 switchport mode trunk

interface GigabitEthernet1/2
 channel-group 3 mode on
 switchport mode trunk

interface Port-channel 1
 switchport mode trunk

interface Port-channel 3
 switchport mode trunk

interface Vlan1
 ip address 192.168.3.112 255.255.255.0
description MANAGEMENT VLAN

ip default-gateway 192.168.3.3
```

```
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 192.168.3.0 0.0.0.255
access-list 1 deny any

line con 0
 password cisco
 privilege level 15
 no login

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```

16.2.5. SW3-3

```
hostname SW3-3

enable secret cisco

ip ssh version 2
ip domain-name cisco.com

username cisco secret cisco

spanning-tree mode rapid-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
 switchport mode trunk

interface FastEthernet0/14
 switchport mode trunk

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21
 channel-group 2 mode on
 switchport mode trunk

interface FastEthernet0/22
 channel-group 2 mode on
 switchport mode trunk

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1
 channel-group 3 mode on
 switchport mode trunk
```

```
interface GigabitEthernet1/2
 channel-group 3 mode on
 switchport mode trunk

interface Port-channel 2
 switchport mode trunk

interface Port-channel 3
 switchport mode trunk

interface Vlan1
 ip address 192.168.3.113 255.255.255.0
description MANAGEMENT VLAN

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 192.168.3.0 0.0.0.255
access-list 1 deny any

line con 0
 password cisco
 privilege level 15
 no login

line vty 0 4
 access-class 1 in
 password cisco
 login
 transport input ssh
line vty 5 15
 access-class 1 in
 password cisco
 login
 transport input ssh

end
```