KAPLAN

IT LEARNING

Cisco Simulations

Kaplan IT Learning CCNA

Simulator: Cisco Labs

IT Certification Test Preparation

Contents

How to Use This Tool 4
Initial purchase and setup 4
Performing the CCNA simulation exercise scenarios 6
Performing your own exercises 6
Saving configurations 6
Creating and modifying the default connections 6
Configuration Options 6
Partial List of Supported Commands 7
Simulation Exercises 13
Simulation 1 – NationalAct 14
Simulation 2 – Globecomm 15
Scenario 3 - CDPress 16
Scenario 4 - DreamSuites 17
Scenario 5 – Wonder Web 18
Scenario 6 - Nutex 19
Scenario 7 – Northern Company 20
Scenario 8 – United Sales 21
Scenario 9 - VisionWorx 22
Scenario 10 - Verigon 23
Scenario 11 - Interconn 25
Scenario 12 – Metroil 27
Solutions 29
Simulation 1 – NationalAct 30
Simulation 2 – Globecomm 35
Scenario 3 - CDPress 37
Scenario 4 – DreamSuites 39
Scenario 5 – Wonder Web 41
Scenario 6 - Nutex 43
Scenario 7 – Northern Company 45
Scenario 8 – United Sales 47
Scenario 9 - VisionWorx 51

Scenario 10 - Verigon 54
Scenario 11 - Interconn 57
Scenario 12 – Metroil 60

How to Use This Tool

About the Kaplan IT Learning CCNA Simulator

The Kaplan IT Learning CCNA Simulator is an interactive tool that can be used to practice configuration tasks on routers and switches. The exclusive exercises included with this product are designed to allow you to practice skills that will be tested on the CCNA exam. Whether you pursue the two-test approach to the CCNA (640-822 and 640-816) or the one-test approach (640-802), you will encounter simulation item types. Our simulation tool allows you to practice the skills required to pass the CCNA exam, as well as to become familiar and comfortable with the real-world exam experience.

Only the Kaplan IT CCNA Simulator offers these exclusive learning features:

- A fully pre-configured network for the simulated learning environment, including a LAN, a WAN, simulated cabling, named interfaces, and simulated IP addresses for each device.
- Twelve scenarios for practicing configurations, along with step-by-step explanations for how to achieve the scenario goals. These exercises cover the objectives for the CCNA exams.

Although the Kaplan IT Learning CCNA Simulator comes with its own set of exercises, **you can perform many other configuration tasks on the virtual equipment** (with the exception of a small set of uncommon commands that may not be supported). This allows you to use the simulator as a self-directed lab.

Help and documentation

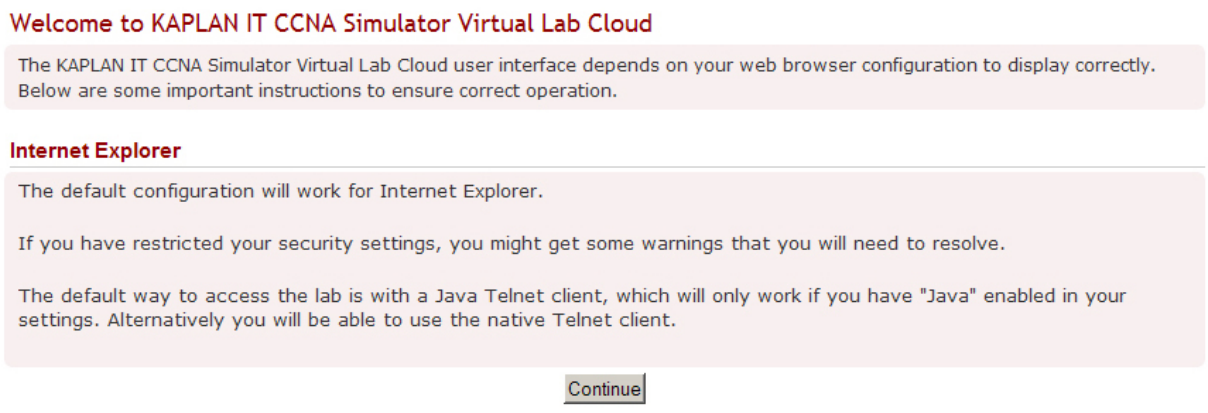
The Kaplan IT Learning CCNA Simulator is based on the MIMIC Virtual Lab engine. Documentation refers to the product as the MIMIC Virtual Lab or the Kaplan IT CCNA Simulator Virtual Lab Cloud.

The right-hand pane contains a Table of Contents that includes a User Guide and FAQ.

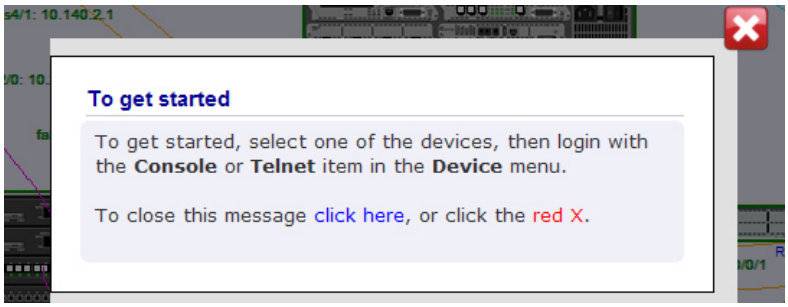
Initial purchase and setup

After you purchase your license, you will receive an email from the MIMIC License Issuer [license @gambitcomm.com] with the subject line *MIMIC Virtual Lab Cloud Rental Confirmation*. The email contains your personal hyperlink to the simulator. Bookmark the link in your browser for easy access.

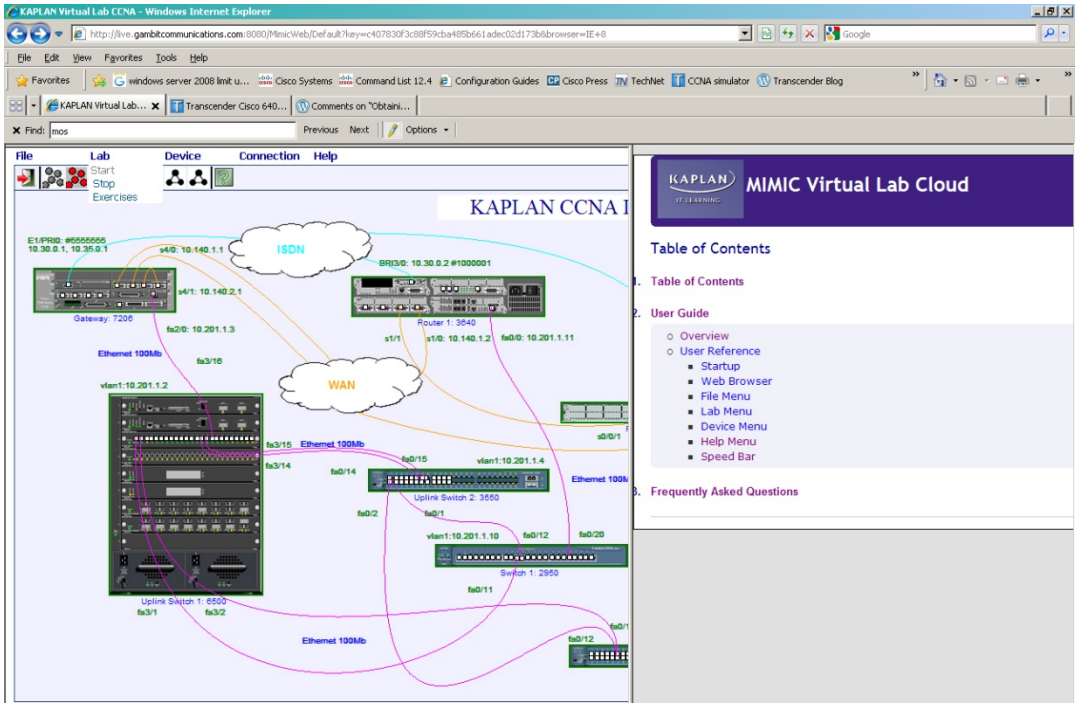
When you open the hyperlink, the virtual lab cloud rental will start.



When the engine opens, click the red X to close the dialog box and begin working.



You can use the slider to adjust the size of the right-hand Table of Contents pane. Slide it to the left to display more text, or slide it to the right to display more of the virtual devices.



Performing the CCNA simulation exercise scenarios

To perform the CCNA simulation exercise scenarios, advance to Scenario 1 in this PDF (page 14).

For instructions on basic operation of the simulator, refer to the User Guide in the Table of Contents.

To download a new copy of this PDF from the simulator, go to **Lab > Exercises**.

Performing your own exercises

To perform tasks not specified in the given exercises, perform the following steps:

- Ensure the devices are started. When the selected devices are surrounded by green, the devices are started. If they are not started, click the device(s) you want to use and select **Start**.
- Click the device and select either **Console** or **Telnet**. The **Console** option allows you to practice as if you were physically connected to the device with a console cable. Selecting **Telnet** will simulate connecting over the network using the telnet program.
- Operate the devices as you would any set of routers and switches. You can practice exercises from other sources such as textbooks or study guides that you may have.
- If you make changes to the running devices, you will want to restart them before beginning the exercises in this PDF.

Saving configurations

In the Kaplan IT Learning CCNA Simulator, as on a Cisco router or switch, the command to save changes to the configuration is **copy running configuration startup configuration** (which can be shortened to **copy run start**). If you execute this command in the Kaplan IT CCNA Simulator, you will be prompted to answer **Do you want to save changes**. If you select **Yes** at the prompt, then any changes you made to the router or switch in the simulator will be saved after you stop the device, and the changes will be reflected the next time you start the router or switch.

It is recommended that you answer **No** at the prompt to clear all configuration changes so that each exercise has the same beginning state. If you inadvertently save your changes or intentionally save your changes to finish an exercise at a later time, you can go back to that router or switch and clear the changes by selecting **File > Reset** from the Console menu.

This CCNA Simulator product allows users to bookmark where they are when they quit the simulator. In other words, you do not have to start over at the beginning the next time you go into the simulator.

Creating and modifying the default connections

The Kaplan IT Learning CCNA simulator comes with connections preconfigured between the routers and switches that mimic cables in the real world. These connections can be moved or deleted, and new connections can be created by clicking **Connection** in the Console menu. The exercises that are provided with the Kaplan IT Learning CCNA Simulator depend on the default connections that have been set up at installation. Although these connections can be altered, any changes may affect the outcome of the exercises.

Configuration Options

To activate the **Connection** menu, you must first click a cable or virtual connection (represented by blue, pink, or yellow lines running between two or more devices in the network diagram), or click an unused port on a device.

Connection Menu	The Connection menu lets you manipulate the selected connection.
Connection > Disconnect	This menu item disconnects the link. This is analogous to unplugging a cable at either end, or physically cut it. The Lab will attempt to simulate this condition just like in the real world. The link will be shown with a dashed line.
Connection > Reconnect	This menu item reconnects the disconnected link. This is analogous to plugging the cable in at both ends.
Connection > Remove	This menu item removes the selected link. This is analogous to removing the cable entirely. The difference between disconnecting and removing the cable is that the latter allows connecting a different cable to a different port to either end.
Connection > Add	Selecting an unused port (ie. no cable connected to it) and clicking this menu item highlights all the ports that this port can be connected to. Once you select the second end-point, a cable will be drawn to connect them. Initially the cable will be unplugged, but you can reconnect it to gain connectivity between the ports.

Partial List of Supported Commands

Command	**Mode**
debug frame-relay lmi	en
debug ip igrp transactions	en
debug ip ospf [database | events | neighbor]	en
debug ip rip	en
debug isdn q931	en
deny	ipa
description	ci
dialer [fast-idle | idle-timeout]	ci
dialer map	ci
dialer pool-member	ci

dialer remote-name	ci
dialer string	ci
dialer-group	ci
dialer-list	ct
disable	en
disconnect	um, en
duplex	ci
enable	um, ct
enable [password | secret]	en, ct
encapsulation dot1q	ci
encapsulation frame-relay [cisco | ietf]	ci
encapsulation [isl | ppp]	ci
end	ct
exclude	um, en
exec-timeout	en
exit	en, ci, ct, ipa
exponential-weighting-constant	ct
fair-queue	ct
frame-relay	ct
frame-relay adaptive-shaping {becn | foresight}	mc
frame-relay bc [in | out] bits	mc
frame-relay be [in | out] bits	mc
frame-relay cir [in | out] bps	mc
frame-relay idle-timer [in | out] seconds	mc
line aux 0	ct
line console 0	ct
line vty 0 4	ct
logging	ct
login	cl
logout	um, en
mac-address	ci
map-class	ct
match	cm
neighbor remote-as	ro
net (is-is)	ro
network (bgp)	ro
network (eigrp)	ro
network (rip)	ro
no access-list	en

no banner	en
no banner login	en
no cdp enable	ci
no cdp holdtime	ct
no cdp run	ct
no cdp timer	ct
no clock rate	ci
no debug eigrp packets	en
no description	ci
no dialer-list	ct
no duplex	ci
no enable password	en
no encapsulation	ci
no frame-relay switching	ct
no ip access-group	ci
no ip address	ci
no ip classless	en
no ip default-gateway	cm
no ip host	en
ping	um, en
police	cl
policy-map	ct
ppp authentication	ci
priority	cl
queue-limit	ct
random-detect	ct
rate-limit	ci
reload	en
remark	ipa
router bgp	ct
router eigrp	ct
router igrp	ct
router ospf	ct
router rip	ct
service-policy	ci, cl, cm, mc, pm
show access-lists	um, en
show arp	um, en
show backup	um, en
show buffers	um, en
show cdp	um, en
show cdp entry *	um, en

show cdp entry name	um, en
show cdp interface	um, en
show cdp neighbors	um, en
show clock	um, en
show compress	um, en
show configuration	um, en
show controllers	um, en
show dialer	um, en
show flash all	um, en
show flash chips	um, en
show flash detailed	um, en
show flash error	um, en
show running-config	en
show running-config interface	en
show snmp	um, en
show startup-config	um, en
show terminal	um, en
show users	um, en
show users all	um, en
show users wide	um, en
show version	um, en
shutdown	ci
snmp trap	ci
snmp trap link-status	ci
systat	um, en
systat all	um, en
terminal history size	um, en
terminal length	um, en
terminal width	um, en
traceroute	en
trunk group	ci
undebug all	en
where	um

Switch IOS Commands	Mode
access-list	ct
banner	ct
cdp	ct, ci
clear arp-cache	en
clear port-security	en
configure	en
connect	en
copy	en
debug	en
description	ci
disable	en
disconnect	en
show flash:	en
show history show hosts	en
show interfaces	en
show interfaces switchport show interfaces vlan	en
show ip, show ipv6, show location	en
show logging, show mac-address-table	en
show port-security, show running-config, show snmp, show spanning-tree, show startup-config, show terminal	en
show users	en
show version	en
show vlan	en
show vtp status shutdown	en, ci
snmp-server switchport access vlan	ct, ci
systat telnet	en, um, en
terminal	en
traceroute	en
trunk	ci
vlan	cm
vlan database	cm
vtp where	vl, um, en

Catalyst Switch Commands	Mode
show trunk	en
clear trunk	en
set interface	en
set trunk	en

Mode Legend

um = User EXEC mode

en = Privileged EXEC mode (enable command)

ct = Global Configuration mode (configure terminal command)

ci = config-if mode (interface command)

cl = config-line mode (line command)

cm = config-cmap mode (class-map command)

ipa = ip access-list configuration (named access-lists)

mc = map-class

pm = policy-map

ro = router config

vl = VLAN

Simulation Exercises

Simulation 1 – NationalAct

You are the Cisco administrator for NationalAct. You are setting up a series of routers to run the EIGRP routing protocol. You configured the first two routers, **Router 1** and **Router 2**. You test your configuration by running the `show ip eigrp neighbors` command and find that the two routers are forming a neighbor relationship, but you cannot ping from one router to another over the connected interface. You need to correct the problem and ensure that you can ping from **Router 1** to **Router 2**.

1. Start **Router 1** and **Router 2**.
    a. Right-click each router.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to each router by right-clicking the router and selecting **Console**.
2. Log in to the two routers using these login credentials and commands:

    ```
    Username: lab
    Password: lab123
    router1>/router2> enable
    Enable password: enable123
    ```

3. Load the configuration files for this exercise from flash with the following commands:
    a. On **Router 1**, issue this command:

        ```
        copy flash:StartupR1Eigrp.txt run
        ```

        When prompted with

        ```
        Destination filename [running-config]?
        ```

        Press Enter.

        The configuration file will load, which will prepare the router for this exercise.
    b. On **Router 2**, issue this command:

        ```
        copy flash:StartupR2Eigrp.txt run
        ```

        when prompted with

        ```
        Destination filename [running-config]?
        ```

        Press **Enter**

        The configuration file will load, which will prepare the router for this exercise.
4. Determine and correct the problem.
5. Verify and save the configuration.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Simulation 2 – Globecomm

You are a network technician for Globecomm, where you manage the **Sales** VLAN and the **Accounting** VLAN. The lead network designer has instructed you to prepare a switch named **Switch 1** to support four new computers. You are given the following requirements:

- **Computer A** will be plugged into FastEthernet port 15 and should be placed in the **Accounting** VLAN.
- **Computer B** will be plugged into FastEthernet port 17 and should be placed in the **Sales** VLAN.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Switch 1**.
    a. Right-click **Switch 1**.
    b. Select **Start** from the menu.
    c. Wait for the switch to be surrounded in green.
    d. Connect to the switch by right-clicking the switch and selecting **Console**.
2. Log in to **Switch 1** using these login credentials and commands:

```
Username: lab
Password: lab123
switch1> enable
Enable password: enable123
```

3. Create the **Accounting** VLAN and the **Sales** VLAN.
4. Assign ports correctly to the VLANs.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 3 - CDPress

You are a junior Cisco technician at CDPress. The switch that you are working with (**Switch 1** in the Console) has two devices connected to it. Your manager has asked you to determine how frames sent to various MAC addresses will be handled. Using the following instructions, connect to **Switch 1**:

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Switch 1**, **Uplink Switch 1**, **Uplink Switch 2**, and **Router 1**.
    a. Right-click each component.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to each component by right-clicking and selecting **Console**.
2. Log in to **Switch 1** using these login credentials and commands:

```
Username: lab
Password: lab123
switch1> enable
Enable password: enable123
```

Use the Simulator to answer the following questions:

1. To which interface(s) will a frame addressed to 0006.524e.b18a be sent?
    A. FastEthernet port 20
    B. FastEthernet port 11
    C. FastEthernet port 16
    D. FastEthernet port 21
2. To which interface(s) will a frame addressed to 0005.cc5a.548a be sent?
    A. FastEthernet port 16 only
    B. All ports except FastEthernet port 11 and 20
    C. FastEthernet ports 11 and 20 only
    D. The frame will be dropped by the switch

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 4 - DreamSuites

You are a junior Cisco technician at DreamSuites. You are configuring a new client computer that will reside on VLAN **20**. You need to know the default gateway address to configure on the computer. Using **Router 2** in the Console, determine the gateway for the computer that will be placed on VLAN **20**.

1. Start **Router 2**.
    a. Right-click the component.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to each component by right-clicking and selecting **Console**.
2. Log in to **Router 2** using these login credentials and commands:

    ```
    Username: lab
    Password: lab123
    router2> enable
    Enable password: enable123
    ```

3. Load the configuration file for this exercise using this command:

    ```
    copy flash:r2exercise4.txt run
    ```

    when prompted with

    ```
     Destination filename [running-config]?
    ```

    Press **Enter**

    The configuration file will load, which will prepare the router for this exercise
4. Find the gateway for the computer that will be placed on VLAN **20**.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 5 – Wonder Web

You are a junior Cisco administrator for Wonder Web. The network has a Cisco 3640 router (**Router 1**) connected to a Cisco 2950 switch (**Switch 1**). Five computers are connected to **Switch 1**. The IP addresses of the computers are 192.168.5.10 - 192.168.5.14, with a subnet mask of 255.255.255.0. Additional computers may be added in the future. You must prevent these five computers, and any computers added to the subnet in the future, from connecting to a server located at 201.15.68.20. The access list should not prevent the computers in the subnet from sending traffic to any other destination, nor should it restrict any traffic originating from other subnets. Your boss has asked you to configure this access list on the interface connected to the switch.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1** and **Switch 1**.
    a. Right-click each component.
    b. Select **Start** from the menu.
    c. Wait for the component to be surrounded in green.
    d. Connect to the switch by right-clicking the switch and selecting **Console**.
2. Log in to **Router 1** using these login credentials and commands:

    ```
    Username: lab
    Password: lab123
    router1> enable
    Enable password: enable123
    ```

3. Configure the access list on the interface connected to the switch.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 6 - Nutex

You are a junior Cisco technician for Nutex. You manage a Cisco 3640 router named **Router 1** that is connected to a Cisco 2950 switch named **Switch 1**. **Switch 1** has a server with an IP address of 250.16.58.2 that should only be accessible from one computer (192.168.3.1) that resides in a remote subnet (192.168.3.0 /24). No other computers from that subnet should be permitted to access the server. Connect to the router and configure an ACL that accomplishes this without preventing traffic to any other destinations for the remaining computers in the subnet.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1** and **Switch 1**.
    a. Right-click each component.
    b. Select **Start** from the menu.
    c. Wait for the component to be surrounded in green.
    d. Connect to **Router 1** by right-clicking it and selecting **Console**.
2. Log in to **Router 1** using these login credentials and commands:

```
Username: lab
Password: lab123
router1> enable
Enable password: enable123
```

3. Configure the required ACL.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 7 – Northern Company

You are a Cisco technician for the Northern Company. You installed a router in a branch office that was pre-configured at the head office. This router is a Cisco 2811 named **Router 2**. The router has passwords configured, but all the passwords need to be changed. The following passwords are currently configured:

- Enable or privileged password: **enable123**
- VTY password (password for telnet): none set

You must change the passwords as follows:

- Enable or privileged password: **letmein** (this password should be encrypted)
- VTY password (password for telnet): **cisco**

You also need to create the following user account for yourself on **Router 2**:

- Username: Tech1
- Password: **wordpass**

After creating your user account, delete the existing user account named **lab.** After creating the encrypted enable or privileged password, delete the current plain text password.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 2**.
    a. Right-click **Router 2**.
    b. Select **Start** from the menu.
    c. Wait for the component to be surrounded in green.
    d. Connect to **Router 2** by right-clicking it and selecting **Console**.
2. Log in to **Router 2** using these login credentials and commands:

```
Username: lab
Password: lab123
router2> enable
Enable password: enable123
```

3. Change the existing passwords, create your user account, and delete the existing user account and plain text password.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 8 – United Sales

You are a Cisco technician for United Sales. You just accepted a transfer to a new location where you will start by managing two routers. **Router 1** is a Cisco 3640 and **Router 2** is a Cisco 2811. The routers are connected with a serial connection. The previous administrator intended to configure the routers for single area OSPF, but they are not forming a neighbor relationship. You must troubleshoot the problem and configure the routers so that they form a neighbor relationship.

1. Start **Router 1 and Router 2**.
    a. Right-click each component.
    b. Select **Start** from the menu.
    c. Wait for the component to be surrounded in green.
    d. Connect to each router by right-clicking it and selecting **Console**
2. Log in to **Router 1** and **Router 2** using these login credentials and commands:

```
Username: lab
Password: lab123
router1>/router2> enable
Enable password: enable123
```

3. Execute the following commands on **Router 1** and **Router 2** to load the configuration for this exercise:

```
router1#   copy flash:R1ospftr.txt run
router2#   copy flash:R2ospftr.txt run
```

when prompted with

```
 Destination filename [running-config]?
```

Press **Enter**

The configuration file will load, which will prepare each router for this exercise

4. Troubleshoot and configure both routers so that they form a neighbor relationship.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 9 - VisionWorx

You are a new Cisco administrator for VisionWorx. Your first assignment is to configure two existing routers for OSPF. They should be in a single area, area 0. **Router 1** is a Cisco 3640 and **Router 2** is Cisco 2811. The two routers have a configuration, but it must be changed to meet these new requirements.

Interface to configure between the two routers:

- **Router 1** Serial 1/1 IP address 192.168.1.5/24
- **Router 2** Serial 0/0/1 IP address 192.168.1.10/24
- OSPF process ID 200

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1** and **Router 2**.
    a. Right-click each router.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to each router by right-clicking the router and selecting **Console**.
2. Log in to the two routers using these login credentials and commands:

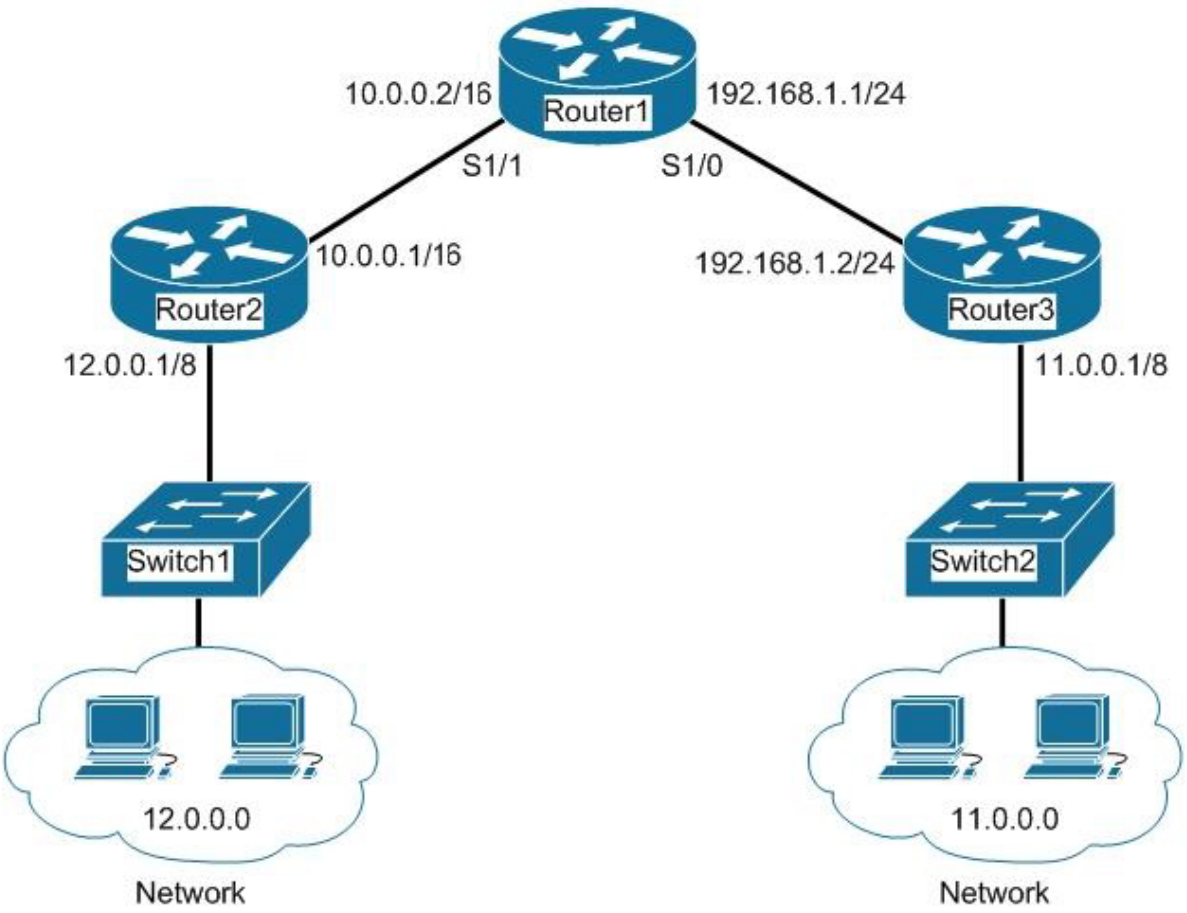
```
Username: lab
Password: lab123
router1>/router2> enable
Enable password: enable123
```

3. Change the routers' configuration.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 10 - Verigon

You are the Cisco administrator for Verigon. The office that you manage has received the first of three routers that will be arriving in the next three weeks. **Router 1** is a Cisco 3640 that will later be connected to two other routers. The following diagram shows the planned network:



The plan for the network is to configure static routes on **Router 1** to enable traffic to be routed correctly from the 12.0.0.0/8 network on one end to the 11.0.0.0/8 network on the other end. Static routing was chosen over dynamic routing to reduce routing update traffic. Your task is to configure the following items on **Router 1** in anticipation of the arrival of the other routers:

- Address the proper interfaces on **Router 1**.
- Create routes to networks that are required to enable traffic to be routed correctly from the 12.0.0.0/8 network on one end to the 11.0.0.0/8 network on the other end.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1**.
    a. Right-click **Router 1**.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to **Router 1** by right-clicking the router and selecting **Console**.
2. Log in to **Router 1** using these login credentials and commands:

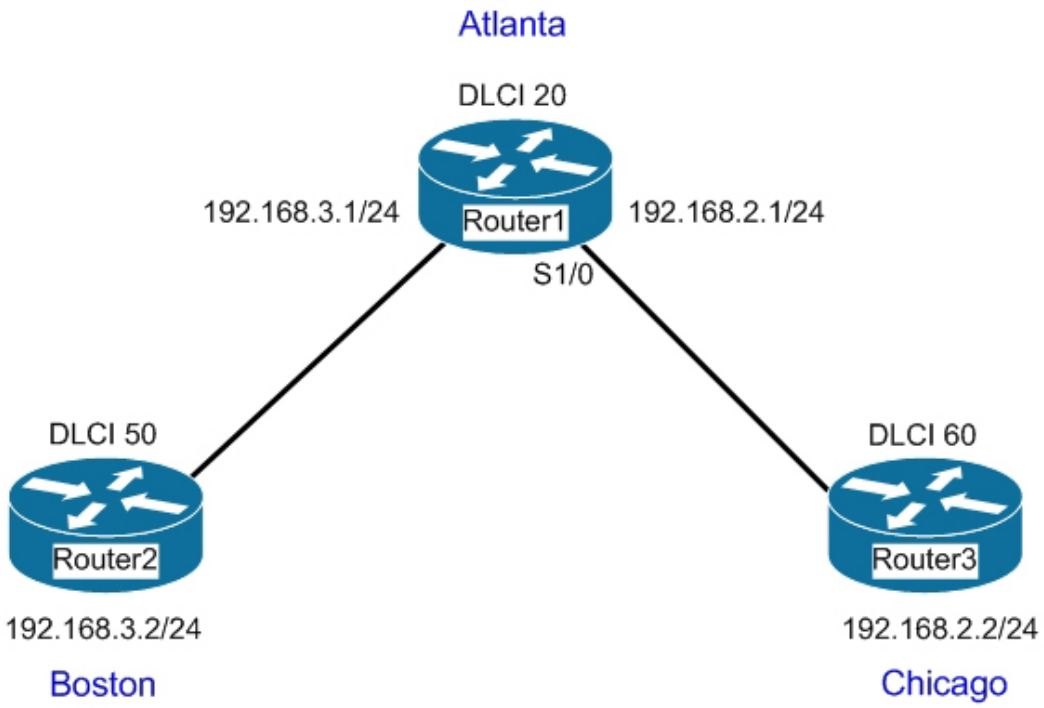
```
Username: lab
Password: lab123
router1> enable
Enable password: enable123
```

3. Configure **Router 1** as required.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 11 - Interconn

You are a Cisco administrator for Interconn. The company has offices in Atlanta, Boston, and Chicago. You work in the Atlanta office. Routers are to be configured in each office to host Frame Relay connections. The network will be configured as follows:



The router for the Atlanta office has arrived and although the other routers are not in place yet, you must configure the Atlanta router to support the given diagram. The router is a Cisco 3640 named **Router 1**.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1**.
   a. Right-click **Router 1**.
   b. Select **Start** from the menu.
   c. Wait for the router to be surrounded in green.
   d. Connect to **Router 1** by right-clicking the router and selecting **Console**.
2. Log in to **Router 1** using these login credentials and commands:

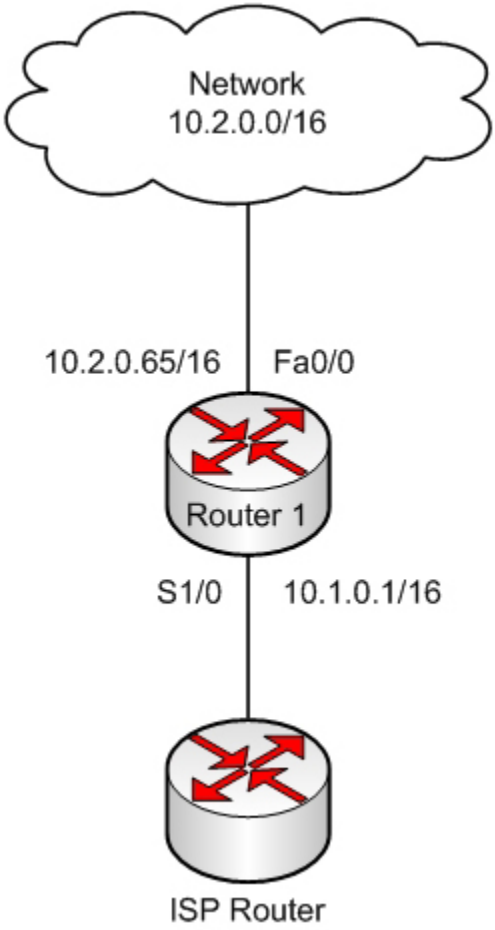
```
Username: lab
Password: lab123
router1> enable
Enable password: enable123
```

3. Configure **Router 1** as required.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Scenario 12 – Metroil

You are the Cisco administrator for Metroil. You have been assigned the task of configuring a router that will be installed in a new office. The router is a Cisco 3640 named **Router 1**. It will host a connection to the Internet service provider (ISP) as shown in the following diagram:



The ISP has issued 10 public IP addresses to the network to be used for Internet access. The range of these addresses is 200.5.5.2-200.5.5.11. The network has 30 hosts that need simultaneous access to the Internet. You need to configure **Router 1** to perform network address translation (NAT) for the hosts. The hosts all reside in the 10.2.0.0/16 network and their actual addresses range from 10.2.0.65-10.0.0.94. Configure **Router 1** to provide this functionality.

Note: You do not need to load a configuration file to complete this exercise.

1. Start **Router 1**.
    a. Right-click **Router 1**.
    b. Select **Start** from the menu.
    c. Wait for the router to be surrounded in green.
    d. Connect to **Router 1** by right-clicking the router and selecting **Console**.

2. Log in to **Router 1** using these login credentials and commands:

```
Username: lab
Password: lab123
router1> enable
Enable password: enable123
```

3. Configure **Router 1** as required.

Note: DO NOT save changes in the Console at the end of this exercise. When you complete an exercise, right-click and **Stop** the devices used in the exercise, and click **No** at the prompt to discard changes. This will allow you to reuse the routers for other exercises. If you inadvertently save your changes, you can return all devices to their original state by selecting **File > Reset** from the toolbar menu in the Console.

Solutions

Simulation 1 – NationalAct

To determine why you cannot ping between the routers, you must log in to the routers and verify the EIGRP configuration. Perform the following actions:

1. If not logged in already, log in to **Router 1**.

```
User Access Verification
Username: lab
Password: lab123
router1>enable
Password: enable123
router1#
```

2. Use the **show ip protocols** command to verify the current EIGRP configuration of **Router 1**.

```
router1# show ip protocols
Routing Protocol is "eigrp 56"
   Outgoing update filter list for all interfaces is not set
   Incoming update filter list for all interfaces is not set
   Default networks flagged in outgoing updates
   Default networks accepted from incoming updates
   EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
   EIGRP maximum hopcount 100
   EIGRP maximum metric variance 1
   Redistributing: eigrp 56
   Automatic network summarization is not in effect
   Routing for Networks:
         192.168.1.1/32
   Routing Information Sources:
         Gateway      Distance      Last Update
                      90            00:00:11
                      90            00:00:11
   Distance: internal 90 external 170

   <additional output omitted>
```

3. Make note of the key settings:

   EIGRP number 56
   Network 192.168.1.1/32

4. If not logged in already, log in to **Router 2**.

```
User Access Verification
Username: lab
Password: lab123
router2>enable
Password: enable123
router2#
```

5. Use the **show ip protocols** command to check the current EIGRP configuration of **Router 2**.

```
router2# show ip protocols
Routing Protocol is "eigrp 56"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
EIGRP maximum hopcount 100
EIGRP maximum metric variance 1
Redistributing: eigrp 56
Automatic network summarization is not in effect
Routing for Networks:
      192.18.1.1/32
Routing Information Sources:
      Gateway      Distance      Last Update
                   90            00:00:11
                   90            00:00:11
Distance: internal 90 external 170

<additional output omitted>
```

6. Make note of the key settings:

EIGRP number 56
Network 192.18.1.1/32

The network statement on **Router 2** is incorrect. The **Router 2** interface that connects to **Router 1** should be in the 192.168.1.0 network, but the output shows EIGRP routing for the 192.18.1.1 network. This indicates that EIGRP was configured with an incorrect network statement. When the network statement does not match the network of the interface, EIGRP cannot function on that interface. Before correcting the network statements, you should verify the IP addresses of the connected interfaces. Beginning with **Router 1**, execute the **show running configuration** command:

```
router1# show run
Building configuration...
Current configuration : 3357 bytes
!
```

Scroll down to the information pertaining to the address of the interface connecting **Router 1** and **Router 2**. (Serial 1/1)

```
!
interface Serial1/1
 bandwidth 64
 ip address 192.168.1.1 255.255.255.0
 encapsulation hdlc
 no shutdown
```

Note that the address is 192.168.1.1/24.

7. Execute the same command on **Router 2**:

```
router2# show run
Building configuration...
Current configuration : 3357 bytes
```

Scroll down to the information pertaining to the address of the interface connecting **Router 1** and **Router 2**. (Serial 0/0/1)

```
!
interface Serial0/0/1
 bandwidth 1544
 ip address 192.18.1.1 255.255.255.0
 encapsulation hdlc
 no shutdown
!
```

Note that the address is 192.18.1.1/24.

The addresses of the interfaces are not in the same subnet which is why you cannot ping from **Router 1** to **Router 2**. One of the routers must be correctly addressed and must have the network statement corrected to match the new address. You should correct **Router 2**. First, enter configuration mode and then enter the configuration mode for interface Serial 0/0/1:

```
router2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router2(config)# interface s0/0/1
router2(config-if)#
```

8. Remove the incorrect IP address, and assign the proper address and mask. Assign **Router 2** the IP address 192.168.1.2/24:

```
router2(config)# interface s0/0/1
router2(config-if)# no ip address
router2(config-if)# ip address 192.168.1.2 255.255.255.0
```

9. To correct the EIGRP network statement, exit interface configuration mode, and enter the configuration mode for EIGRP process 56:

```
router2(config-if)# ip address 192.168.1.2 255.255.255.0

router2(config-if)# exit
router2(config)# router eigrp 56
router2(config-router)#
```

10. Delete the old statement and enter the correct one:

```
router2(config-router)# no network 192.18.1.1 0.0.0.0
router2(config-router)# network 192.168.1.0
router2(config-router)#
```

Note: The original network statement was entered as 32 bits, as indicated by the output of the **show run** command:

```
Routing for Networks:
    192.18.1.1/32
```

Therefore, the original network statement must be removed in terms of 32 bits by using a wildcard mask of 0.0.0.0. Had the network statement been entered as 24 bits, the IOS would assume a class C mask with a Class C address, by default, when either adding or removing a network statement. When entering the correct network statement, you can enter `network 192.168.1.0` without a mask.

11. To verify, exit both the configuration mode for EIGRP and the global configuration mode (type exit twice), and run the **show ip protocols** command:

```
router2(config-router)# exit

router2(config)# exit

router2# show ip protocols
Routing Protocol is "eigrp 56"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 56
  Automatic network summarization is not in effect
  Routing for Networks:
    192.168.1.0/24
  Routing Information Sources:
    Gateway      Distance      Last Update
                 90            00:00:11
                 90            00:00:11
  Distance: internal 90 external 170
```

12. Ping **Router 1** from **Router 2**:

```
router2# ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/4/12 ms
router2#
```

13. Ensure that the two routers are still EIGRP neighbors by executing the **show ip eigrp neighbor** command:

```
router2# show ip eigrp neighbors
IP-EIGRP neighbors for process 0
H   Address             Interface   Hold   Uptime  SRTT   RTO   Q
Seq  Type
                        (sec)          (ms)        Cnt  Num
0   192.168.1.1         Se0/0/1     10
0   192.168.1.1         Se0/0/1     10
```

The output shows the problem has been corrected.

Simulation 2 – Globecomm

To prepare **Switch 1** for the introduction of four new computers, you must first create the two VLANs. To do so, perform the following operations:

1. Log in to **Switch 1** and provide user access verification using the following commands:

```
User Access Verification

Username: lab
Password:lab123
switch1>enable
Password:enable123
switch1#
```

2. Enter global configuration mode using the following commands:

```
switch1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)#
```

3. Enter configuration mode for VLAN 2 and create the **Accounting** VLAN using the following commands:

```
switch1(config)# vlan 2
switch1(config-vlan)# name accounting
switch1(config-vlan)#
```

4. Exit configuration mode for VLAN 2 and enter configuration mode for VLAN 3. Create the **Sales** VLAN using the following commands:

```
switch1(config-vlan)# exit
switch1(config)# vlan 3
switch1(config-vlan)# name sales
switch1(config-vlan)#
```

5. After the VLANs are created, ports must be assigned to the VLANs. Exit configuration mode for VLAN 3 and enter configuration mode for FastEthernet port 15 using the following commands:

```
switch1(config-vlan)# exit
switch1(config)# interface fastethernet 0/15
```

6. Assign the port for **Computer A** (`fastethernet 0/15`) to the **Accounting** VLAN (`Vlan 2`):

```
switch1(config)# interface fastethernet 0/15
switch1(config-if)# switchport access vlan 2
switch1(config-if)# exit
```

7. Assign the port for **Computer B** (`fastethernet 0/17`) to the **Sales** VLAN (`Vlan 3`):

```
switch1(config)# interface fastethernet 0/17
switch1(config-if)# switchport access vlan 3
switch1(config-if)# exit
switch1(config)# exit
switch1#
```

8. Verify your work using the following **show vlan** command.

```
switch1# show vlan
VLAN Name                    Status            Ports
---- ----------------------- ----------------- ------------------
-------------
1    default                 active      Fa0/1, Fa0/2, Fa0/3,
Fa0/4,
                                         Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                         Fa0/9, Fa0/10, Fa0/12, Fa0/13,
                                         Fa0/14, Fa0/16, Fa0/18, Fa0/19,
                                         Fa0/20, Fa0/21, Fa0/22, Fa0/23,
                                         Fa0/24,
2    accounting              active      Fa0/15,
3    sales                   active      Fa0/17,
1002 fddi-default            active
1003 token-ring-default      active
1004 fddinet-default         active
1005 trnet-default           active
```

9. As the output indicates, the VLANS are correctly created and the ports are correctly assigned.

Scenario 3 - CDPress

Note: Uplink **Switch 1**, **Uplink Switch 2**, **Router 1**, and **Switch 2** must be started for this exercise.

To answer the questions, complete the following operations:

1. Connect to **Switch 1** using the following commands:

```
User Access Verification
Username: lab
Password: lab123
switch1>enable
Password: enable123
```

2. Look at the MAC address table to determine the MAC addresses currently connected to the switch. On **Switch 1**, run the following command to reveal the MAC address table:

```
switch1# show mac-address-table

      Mac Address Table

------------------------------------------

Vlan     Mac Address        Type         Ports

----     -----------        --------     -----

All      000b.4638.5a00     STATIC       CPU

All      0100.0ccc.cccc     STATIC       CPU

All      0100.0ccc.cccd     STATIC       CPU

All      0100.0cdd.dddd     STATIC       CPU

1        0006.524e.b18a     DYNAMIC      Fa0/11

1        cc01.1657.0000     DYNAMIC      Fa0/20

Total Mac Addresses for this criterion: 6

switch1#
```

Question 1

1. To which interface(s) will a frame addressed to 0006.524e.b18a be sent?
   A. FastEthernet port 20
   B. FastEthernet port 11
   C. FastEthernet port 16
   D. FastEthernet port 21

Devices are currently attached to FastEthernet 11 and 20. This means that the answer is FastEthernet port 11 because a frame destined for 0006.524e.b18a would be sent to that interface, and no other since a device with that MAC address is connected to that interface.

2. To which interface(s) will a frame addressed to 0005.cc5a.548a be sent?
   A. FastEthernet port 16 only
   B. All ports except FastEthernet port 11 and 20
   C. FastEthernet ports 11 and 20 only
   D. The frame will be dropped by the switch

Because the MAC address for 0005.cc5a.548a is unknown, the switch will send it to all ports EXCEPT the two that are known, specifically 11 and 20.

Scenario 4 – DreamSuites

To determine the default gateway for the computer which will be in VLAN **20**, you must connect to **Router 2** and determine the IP address of the subinterface that is assigned to VLAN **20**. The easiest way to do this is to use the following operations:

1. Log in to **Router 2**, enter privileged mode and execute the **show running-configuration** command as shown:

```
User Access Verification
Username: lab
Password:lab123
router2>enable
Password:enable123
router2# show run
```

2. Examine the output and look for the interfaces that are configured with subinterfaces, the VLANs to which they belong, and the corresponding IP addresses, as shown in the following partial output:

```
!
interface FastEthernet0/0
 bandwidth 100000
 ip address 192.168.6.1 255.255.255.0
   no shutdown
 full-duplex
!
interface FastEthernet0/0.1
 encapsulation dot1Q 20
 ip address 192.168.5.1 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 30
 ip address 192.168.6.1 255.255.255.0
!
interface FastEthernet0/1
 bandwidth 100000
 no ip address
   shutdown
```

The FastEthernet 0/0 interface has two sub interfaces created, 0.1 and 0.3.

0.1 is assigned to VLAN **20**.

0.3 is assigned to VLAN **30**.

Because the computer will be in VLAN **20**, the address assigned to that sub interface (192.168.5.1) should be the gateway for the computer.

Scenario 5 – Wonder Web

To prevent these five computers and any future computers in the subnet from connecting to a server located at 201.15.68.20, an access list that prevents this traffic must be created on the FastEthernet 0/0 interface on **Router 1**. To accomplish this task, perform the following operations:

1. Log in to the router and enter configuration mode using the following commands:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#
```

2. Create an access list that denies all connections to the computer at 201.15.68.20 from the 192.168.5.0 subnet using the following command:

```
router1(config)# access-list 101 deny 192.168.5.0 0.0.0.255 host
201.15.68.20
```

3. All access lists have an implied `deny all` statement at the end of the list. Add an additional line that permits traffic from this subnet to any other destination using the following command:

```
Router1(config)# access-list 101 permit ip any any
```

4. Apply the ACL to the proper interface (FastEthernet 0/0) using the following commands:

```
Router1(config)# interface fa0/0

Router1(config-if)# ip access-group 101 in

Router1(config-if)#
```

5. To verify the access list, exit to privileged mode and execute the **show running-configuration** command:

```
Router1(config-if)#exit

Router1(config)exit

Router1#show running-configuration
```

The partial output of the **show running-configuration** command is as follows:

```
!
interface FastEthernet0/0
bandwidth 100000
ip address 10.201.1.11 255.255.255.0
ip access-group 101 in        Notice the list applied
no shutdown
full-duplex
!
interface FastEthernet0/1
 bandwidth 100000
 no ip address
  shutdown
!
interface Null0
 bandwidth 4294967
 no ip address
 encapsulation isl
!
interface Serial0/0/0
bandwidth 1544
 --More—
!
access-list 101 deny ip 192.168.5.0 0.0.0.255 201.15.68.20
0.0.0.0
access-list 101 permit ip any any     Notice the list parameters
```

Scenario 6 - Nutex

To allow only one computer (192.168.3.1) that resides in a remote subnet (192.168.3.0 /24) from accessing 250.16.58.2, perform the following operations:

1. Log in to **Router 1** and enter configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#
```

2. Create an access list that permits traffic from 192.168.3.1 to access 250.16.58.2 using the following command:

```
router1(config)# access-list 101 permit ip 192.168.3.1 0.0.0.0
250.16.58.2 0.0.0.0
```

3. Add a statement that denies the rest of the subnet using the following command:

```
router1(config)# access-list 101 deny ip 192.168.3.0 0.0.0.255
250.16.58.2 0.0.0.0
```

4. Add a statement that allows all other traffic patterns using the following command:

```
router1(config)# access-list 101 permit ip any any
```

5. Apply the access list to the FastEthernet 0/0 interface (the interface that connects to **Switch 1**) and configure it as outgoing. As such, the access list controls traffic headed in the direction of the server connected to a switch port on **Switch 1** using the following commands:

```
router1(config)# interface fa0/0

router1(config-if)# ip access-group 101 out
```

6. To verify the list and its application, execute the **show running-configuration** command:

```
router1(config-if)# exit

router1(config)# exit

router1# show running-config
```

The partial output of the **show running-configuration** command is as follows:

```
interface Ethernet2/3
 description 0
 bandwidth 10000
 no ip address
  shutdown
!
interface FastEthernet0/0
 bandwidth 100000
 ip address 10.201.1.11 255.255.255.0
 ip access-group 101 out      Note the access list applied
 no shutdown
 full-duplex
!
interface Null0
 bandwidth 4294967
 no ip address
 encapsulation isl
 --More--
!
access-list 101 permit ip 192.168.3.1 0.0.0.0 250.16.58.2 0.0.0.0
access-list 101 deny ip 192.168.3.0 0.0.0.255 250.16.58.2 0.0.0.0
access-list 101 permit ip any any    Note the parameters of the list
```

Note: The order of the statements in the list is important. The statement that allows 192.168.3.1 must be listed before the statement that denies the subnet, otherwise 192.168.3.1 will be denied because it is a part of the subnet. The last statement is also important. There is an implied '`deny`' at the end of all ACLs. If you exclude the last statement, all traffic that does not match the statements before it will be denied.

Scenario 7 – Northern Company

To create an account for **Tech1** with a password of **wordpass**, complete the following operations:

1. Log in to **Router 2** and enter configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router2>enable
Password:enable123
router2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router2(config)#
```

2. Create your user name and password with the following command:

```
router2(config)# username tech1 password wordpass
```

3. Delete the existing account named lab with the following command:

```
router2(config)# no username lab
```

4. To change the enable or privileged password to **letmein** and ensure that it is encrypted, execute the following command:

```
router2(config)# enable secret letmein
```

5. Delete the existing unencrypted enable or privileged password with the following command:

```
router2(config)# no enable password
```

6. Enter the configuration mode for a terminal connection by executing the **line vty 0 4** command and reset the `vty` password:

```
router2(config)# line vty 0 4

router2(config-line)# password cisco
```

7. Enter the command that instructs the router to prompt for the telnet password when a connection is attempted:

```
router2(config-line)# login
```

8. All the operations can be verified by examining the running configuration. To do this, exit global configuration mode:

```
router2(config-line)# exit

router2(config)# exit
```

9. Execute the following command:

```
router2# show run

Building configuration...

Current configuration : 3357 bytes
```

10. Make note of the following sections (some output omitted):

```
boot system flash slot0:

enable secret 5 $1$QjqB$fvfzb0yjJWpjLbRjoHOEF
```
New encrypted enable password

```
username tech1 password 0 wordpass
```

Note: The output displays your new user account and password. Notice the older account is not displayed.

11. To complete the operation, scroll through the output and verify that the terminal password (line vty) password has been reset as shown:

```
line vty 0 4

exec-timeout 10 0

password cisco

login
```

Scenario 8 – United Sales

To troubleshoot and configure the routers so that they form a neighbor relationship complete the following operations:

1. If you have not already done so, log in to **Router 1** with the following commands:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1#
```

2. Execute the **show run** command to display OSPF configurations on the router:

```
router1# show run

Building configuration...

Current configuration : 3357 bytes

More-
```

3. Scroll through the output to the section on the interface serial 1/1 (the interface connecting to **Router 2**) and ospf:

```
encapsulation hdlc

 shutdown

!

interface Serial1/1

 bandwidth 64

 ip address 192.168.1.1 255.255.255.0

 encapsulation hdlc

 no shutdown

!

interface Serial1/2

 bandwidth 1544

 no ip address

 encapsulation hdlc

 shutdown
```

```
!
interface Serial1/3
 bandwidth 1544
 no ip address
 encapsulation hdlc
 shutdown
!
!
router ospf 122
 network 192.168.1.0 0.255.255.255 area 2
!
!
```

Note: The IP address of the interface is 192.168.1.1/24. Also, the router is advertising the 192.168.1.0/24 network to area 2.

4. If you have not already done so, log in to **Router 2** with the following commands:

```
User Access Verification
Username: lab
Password:lab123
Router2>enable
Password:enable123
Router2#
```

5. Execute the **show run** command to see how OSPF is configured on the router:

```
Router2# show run

Building configuration...

Current configuration : 3357 bytes
```

6. Scroll to the portion of the output for interface serial 0/0/1 (the interface connecting to **Router 1**) and OSPF:

```
interface Serial0/0/0
 bandwidth 1544
 no ip address
 encapsulation hdlc
 shutdown
!
```

```
interface Serial0/0/1
 bandwidth 1544
 ip address 192.168.1.2 255.255.255.0
 encapsulation hdlc
 no shutdown
!
!
router ospf 122
 network 192.168.1.0 0.255.255.255 area 1
!
```

Note: The IP address of the interface is 192.168.1.2/24. Also, the router is advertising the 192.168.1.0/24 network to area 1.

The interfaces are correctly configured with addresses in the same subnet, and OSPF is routing for the correct network (192.168.1.0/24).

The two routers are routing to DIFFERENT areas. For a single area, they should both be configured to area 0 or the backbone.

To correct this, perform the following operations on both routers:

1. Enter configuration mode:

```
router2#

router2#config t

Enter configuration commands, one per line.  End with CNTL/

router2(config)#
```

2. Now enter OSPF configuration mode for the process 122 (process number used when OSPF was configured):

```
router2(config)# router ospf 122

router2(config-router)#
```

3. Delete the incorrect statement that advertises the 192.168.1.0 /24 network to area 1:

```
router2(config-router)# no network 192.168.1.0 0.255.255.255 area
1
```

4. Replace this with a statement that advertises the 192.168.1.0/24 network to area 0:

```
router2(config-router)# network 192.168.1.0 0.0.0.255 area 0

router2(config-router)# exit
```

5. Perform the same corrections on **Router 1** and advertise the 192.168.1.0/24 network to area 0.

   Note: **Router 2** is routing to area 2, whereas **Router 1** was routing to area 1. You must specify the location to which it is currently routing when you remove it.

6. You can confirm the correction by verifying that the routers form the relationship with the **show ip ospf neighbor** command:

```
router2#show ip ospf neighbor

Neighbor ID Pri  Stat   Dead Time   Address       Interface

192.168.1.1   1     FULL/  -   00:00:??   192.168.1.1
Serial0/0/1

192.168.1.1   1     FULL/  -   00:00:??   192.168.1.1
Serial0/0/1

router2#
```

   Note: The output may only show on the first router you correct, but if the output shows on either router, then the routers have formed the relationship.

Scenario 9 - VisionWorx

To configure the routers properly, complete the following operations:

1. Log in to **Router 1** and enter configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#
```

2. To address the interface connected to **Router 2**, enter configuration mode for the interface with the following command:

```
router1(config)# interface serial 1/1

router1(config-if)#
```

3. Apply the IP address from the instructions as follows:

```
router1(config)# interface serial 1/1

router1(config-if)# ip address 192.168.1.5 255.255.255.0
```

4. Enable the interface as follows:

```
router1(config-if)# no shutdown
```

5. Exit to global configuration mode and enter configuration mode for the OSPF process 200 (this can be any number as long as it matches on both routers) as follows:

```
router1(config-if)# exit

router1(config)# router ospf 200

router1(config-router)#
```

6. Configure the network for OSPF process 200 as follows:

```
router1(config-router)# network 192.168.10.0 0.0.0.255 area 0
```

7. **Router 1** is complete. Now log in to **Router 2** and enter configuration mode:

```
User Access Verification
Username: lab
Password:
router2>enable
Password:
router2# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router2(config)#
```

8. To address the interface connected to **Router 1**, enter configuration mode for the interface with the following command:

```
router2(config)# interface serial 0/0/1

router2(config-if)#
```

9. Apply the IP address from the instructions as follows:

```
router2(config-if)# ip address 192.168.1.10 255.255.255.0

router2(config-if)#
```

10. Enable the interface as follows:

```
router2(config-if)# no shutdown
```

11. Exit to global configuration mode and enter configuration mode for OSPF process 200 as follows:

```
router2(config-if)# exit

router2(config)# router ospf 200

router2(config-router)#
```

12. Configure the network for OSPF process 200 as follows:

```
router2(config-router)#

router2(config-router)#
```

13. Both routers are complete. To verify, from either router exit to privileged mode. Verify that an OSPF neighbor relationship has been formed as follows:

```
router2(config-router)# exit

router2(config)# exit

router2#

1d00h: %SYS-5-CONFIG_I: Configured from console by console

router2# show ip ospf neighbor


Neighbor ID     Pri   Stat      Dead Time   Address
Interface

192.168.1.5    1    FULL/  -   00:00:??    192.168.1.5
Serial0/0/1

192.168.1.5    1    FULL/  -   00:00:??    192.168.1.5
Serial0/0/1

router2#
```

Scenario 10 - Verigon

To address the proper interfaces on **Router 1** and create routes to networks that are required to enable traffic to be routed correctly from the 12.0.0.0/8 network on one end to the 11.0.0.0/8 network on the other end, perform the following operations:

1. Log on to **Router 1** and enter configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#
```

2. According to the diagram, the two interfaces that must be configured with IP addresses are serial 1/0 and serial 1/1. Start by entering configuration mode for interface serial 1/0:

```
router1(config)# interface s1/0

router1(config-if)#
```

3. Configure the proper address according to the diagram:

```
router1(config-if)# ip address 192.168.1.1 255.255.255.0

router1(config-if)#
```

4. Enable the interface:

```
router1(config-if)# no shutdown

1d00h: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

1d00h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
changed state

to uprouter1(config-if)#
```

5. Exit to global configuration mode and enter the configuration mode for the next interface, serial 1/1:

```
router1(config-if)# exit

router1(config)# interface s1/1

router1(config-if)#
```

6. Configure the proper addressing according to the diagram:

```
router1(config-if)# ip address 10.0.0.2 255.0.0.0

router1(config-if)#
```

7. Enable the interface:

```
router1(config-if)# no shutdown

1d00h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1,
changed state

to downrouter1(config-if)#
```

With both interfaces addressed, you can configure the required static routes. According to the diagram, the only networks that **Router 1** will not be aware of are the 11.0.0/8 network and the 12.0.0.0/8 network. All other networks are directly connected and will automatically be placed in the routing table. You must configure two routes.

8. Exit to global configuration mode:

```
router1(config-if)# exit

router1(config)#
```

9. To route traffic to the 11.0.0.0/8 network, the next hop address will be the interface at 192.168.1.2/24 on **Router 3**. Therefore, configure this static route as follows:

```
router1(config)# ip route 11.0.0.0 255.0.0.0 192.168.1.2
```

   To route traffic to the 12.0.0.0/8 network the next hop address will be the interface at 10.0.0.1/8 on **Router 2**.Therefore configure this static route:

```
router1(config)# ip route 12.0.0.0 255.0.0.0 10.0.0.1

router1(config)#
```

10. To verify that the static routes exist on **Router 1**, exit global configuration mode and execute the **show ip route** command:

```
router1(config)# exit

router1#

1d01h: %SYS-5-CONFIG_I: Configured from console by console

router1# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
       area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
       EGP

       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter

       * - candidate default, U - per-user static route, o - ODR

      P - periodic downloaded static route

Gateway of last resort is not set

S    11.0.0.0 [1/0] via 192.168.1.2

S    12.0.0.0 [1/0] via 10.0.0.1
```

Note: The two routes exist in the routing table.

Scenario 11 - Interconn

To configure **Router 1** to satisfy the requirements of the diagram, the following items must be configured:

- Interface Serial 1/0 must be configured with two sub interfaces to host the two Frame Relay connections that will go to **Router 2** (Boston) and **Router 3** (Chicago).
- The two sub interfaces must be properly addressed according to the diagram.
- The encapsulation type (Frame Relay) must be set on the physical interface, Serial 1/0.
- Each sub interface must be mapped to the planned DLCI of the opposite end of the connections (in this scenario, Boston or **Router 2** to DLCI 50, and Chicago or **Router 3** to DLCI 60).

To configure these items, complete the following operations:

1. If you have not already done so, log in to **Router 1** and enter global configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#
```

2. Enter the configuration mode for Serial 1/0 so that encapsulation can be configured:

```
router1(config)# interface s1/0

router1(config-if)#
```

3. Set the encapsulation for Frame relay with the following command:

```
router1(config-if)# encapsulation frame-relay
```

4. Create two sub interfaces for each connection (one to **Router 2** and one to **Router 3**) and the sub interfaces must be addressed and mapped to a DLCI starting with the connection to Boston:

```
router1(config-if)# interface serial1/0.1 point-to-point

router1(config-subif)# ip address 192.168.3.1 255.255.255.0

router1(config-subif)# frame-relay interface-dlci 50

router1(config-fr-dlci)#
```

5. Configure the other interface to Chicago:

```
router1(config-fr-dlci)# interface serial1/0.2 point-to-point

router1(config-subif)# ip address 192.168.2.1 255.255.255.0

router1(config-subif)# frame-relay interface-dlci 60

router1(config-fr-dlci)#
```

6. To verify your work, exit to privileged mode and execute the **show running-configuration** command:

```
router1(config-subif)# exit

router1(config)# exit

router1#

1d00h: %SYS-5-CONFIG_I: Configured from console by console

router1# show run

Building configuration...

Current configuration : 3357 bytes

!
```

7. Scroll to the section on Serial1/0 to verify the configuration:

```
interface Serial1/0
 bandwidth 64
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay map  0 50
 frame-relay map  0 60
 shutdown
!
interface Serial1/0.1
 description 0
 bandwidth 64
 ip address 192.168.1.1 255.255.255.0
 encapsulation hdlc
 no shutdown
!
interface Serial1/0.2
 description 0
 bandwidth 64
 ip address 192.168.2.1 255.255.255.0
 encapsulation hdlc
 no shutdown
```

This section shows the DLCI map (your output may differ slightly)

Scenario 12 – Metroil

To configure **Router 1** to provide this functionality, the following tasks must be performed:

- Interfaces FastEthernet 0/0 and Serial 1/0 must be addressed according to the diagram.
- The pool of available public addresses must be configured.
- NAT must be configured to use the address pool and it must reference an access list that describes interior addresses allowed to use the public IP addresses.
- An access list that describes interior addresses allowed to use the public IP addresses must be created.
- NAT must be enabled on the two interfaces.

To complete this list, perform the following operations:

1. If you have not done so already, log in to **Router 1** and enter global configuration mode:

```
User Access Verification
Username: lab
Password:lab123
router1>enable
Password:enable123
router1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router1(config)#
```

2. To address the serial1/0 interface , enter the configuration mode for the interface:

```
router1(config)# interface serial1/0

router1(config-if)#
```

3. Configure the address and enable the interface:

```
router1(config-if)# ip address 10.1.0.1 255.255.0.0

router1(config-if)# no shutdown
```

4. To address the FastEthernet 0/0 interface, exit the configuration mode for Serial 0/0 and enter configuration mode for FastEthernet 0/0:

```
router1(config-if)# exit

router1(config)# interface fa0/0
```

5. Address and enable the interface as follows:

```
router1(config-if)# ip address 10.2.0.65 255.255.0.0

router1(config-if)# no shutdown
```

6. Define the address pool for NAT along with the proper mask. To do this, exit configuration mode for FastEthernet 0/0:

```
router1(config-if)# exit
```

7. Define the pool with a name and a proper mask. You can use any name, but it must be matched when you reference it in the statement directing the NAT process to use the pool. The name used in this tutorial is **public**.

```
router1(config)# ip nat pool public 200.5.5.2 200.5.5.11 netmask
255.255.255.240
```

8. Configure the NAT process to use the pool of addresses and also to use an access list (which is yet to be created) to define the interior addresses allowed to use the public addresses in the pool. The access list number (list 1) chosen is arbitrary, but it must match the name of the access list when you create it.

```
router1(config)# ip nat inside source list 1 pool public overload
```

Note: The **overload** parameter is required because there are more private IP addresses than there are public IP addresses.

9. Create the access list with the proper wildcard mask that defines the interior addresses allowed to use the public addresses in the pool:

```
router1(config)# access-list 1 permit 10.2.0.64 0.0.0.31
```

10. To enable NAT on the FastEthernet 0/0 interface enter configuration mode for that interface:

```
router1(config)# interface fa0/0
```

11. Once in configuration mode for the FastEthernet 0/0 interface, enable NAT:

```
router1(config-if)# ip nat inside
```

12. Exit configuration mode for FastEthernet 0/0 and enter configuration mode for Serial 1/0 and enable NAT there as well:

```
router1(config-if)# exit

router1(config)# interface serial1/0

router1(config-if)# ip nat outside
```

13. To verify your work, exit to privileged mode and execute the **show running configuration** command:

```
router1(config-if)# exit

router1(config)# exit

router1# show run

Building configuration...
```

```
Current configuration : 3357 bytes
```

14. Scroll to the following sections (some output omitted) to verify the configuration:

```
!
interface FastEthernet0/0
 bandwidth 100000
 ip address 10.2.0.1 255.255.0.0
 ip nat inside        NAT is configured on this interface
  no shutdown
 full-duplex
!
interface Null0
 bandwidth 4294967
 no ip address
 encapsulation isl
!
interface Serial1/0
 bandwidth 64
 ip address 10.1.0.1 255.255.0.0
 ip nat outside       NAT is configured on this interface
 encapsulation hdlc
 no shutdown
ip nat pool public 200.5.5.2 200.5.5.11 netmask 255.255.255.240
ip nat inside source list 1 pool public overload
 access-list 1 permit 10.2.0.64 0.0.0.31
```

NAT configuration shown above