Cisco Systems

Cisco Networking Academy Program

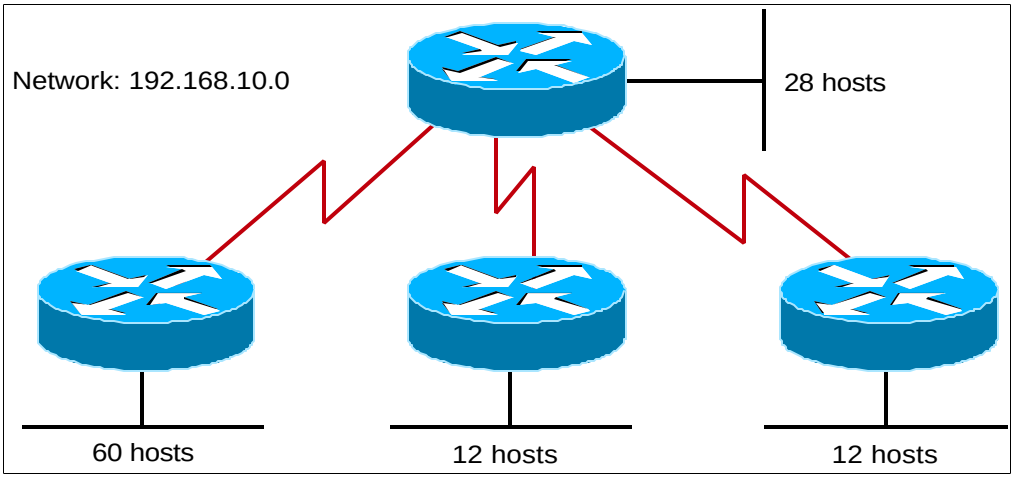
CCNP

Semester 5

v 1.0

# Lab Manual

# Lab 2.4.4 VLSM



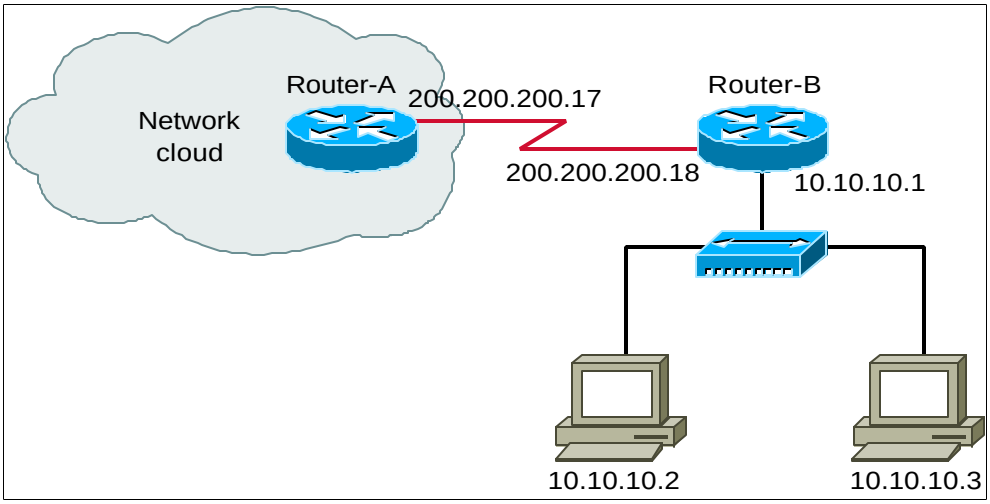

**Objectives:**

- Create an addressing scheme using variable length subnet masking (VLSM).

**Scenario:**

You are assigned the class C address 192.168.10.0 and must support the network shown in the diagram. You are not permitted to use IP unnumbered or NAT on this network. Create an addressing scheme that will meet the diagram requirements.

# Lab 2.6.1 Network Address Translation -- Configuring Static Translation




**Objective:**

Demonstrate the use of Network Address Translation through the use of static translation.

**Equipment Requirements:**

Two routers One switch Two workstations

**Background:**

A small company has been using the private address 10.10.10.0/24 for their network. Until recently they did not need access outside of their own network. Since they now need Internet access they have been issued the class C address 202.206.154.0 by ARIN. Currently the company does not require the full number of addresses in a Class C network; however, they will require the addresses as the company grows. For a variety of reasons including security reasons, the company wishes to hide the internal network from the outside. Presently only a few users need to be able to connect to the outside. These users need to have unlimited access to the outside.

**Preliminary:**

Before programming the routers, make sure that the IOS version on the router supports Network address translation. Load a new IOS version if necessary. Construct the above network section, using IGRP or RIP as your routing protocol. Do not advertise the private network. Use the network address 200.200.200.16/28 on the serial link from the stub network router (Router-B) and the Internet/main network router (Router-A). The router ip configurations are as follows:

Note: The interfaces described below might vary according to what type of router being used.

| Router-A | Router-B |
| --- | --- |
| | `Fa 0/0=10.10.10.1/24` |
| `S0/0=200.200.200.17/28` | `S0/0=200.200.200.18/28` |

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables for network 200.200.200.16/28. Also verify that the workstations are configured correctly for the network in which they reside. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping`**, **`telnet`**, and any other relevant command(s).

For this Lab we will be using Router-B as the stub network router where we will configure the network address translation. The router will be translating the inside local addresses to inside global addresses, in other words, converting the internal fake addresses into real addresses for use on the Internet.

From the "Router-B" console:

## Step 1

- Enter the EXEC mode.

## Step 2

- Enter the configuration mode by entering **`configure terminal`** command at the router prompt.

## Step 3

Establish static translation between an inside local address and an inside global address.

- Enter **`ip nat inside source static 10.10.10.2 202.206.154.2`**
- Enter **`ip nat inside source static 10.10.10.3 202.206.154.3`**

  If we needed a static translation for workstation 10.10.10.4, how would we enter the configuration information into the router?

## Step 4

Specify the inside interface.

- Enter **`interface fa 0/0`** (or correct inside interface for router used)

## Step 5

Mark the interface as connected to the inside.

- Enter **`ip nat inside`**

## Step 6

Specify the outside interface.

- Enter **`interface serial 0/0`** (or correct outside interface for router used)

## Step 7

Mark the interface as connected to the outside.

- Enter **`ip nat outside`**

## Step 8

Save configuration information.

- Enter **`CTRL-Z`**
- Enter **`copy run start`**

## Step 9

Monitoring NAT

- Enter **`show ip nat translations`**

  What information did the router respond with?

---

- Enter show **`ip nat statistics`**

  What information did the router respond with?

---

Record Hits:

---

and Misses:

---

- Enter **`show ip nat translations verbose`**

  What information did the router respond with?

---

Record Create:

---

and Use:

---

- From a workstation on the inside network ping an address on the outside

  Were you successful?

---

**From the router console:**

- Enter **`show ip nat translations verbose`**

  What additional information did the router respond with?

---

Record Create:

---

and Use:

---

- Enter **`show ip nat statistics`**

  What information did the router respond with?

---

  Record Hits:

---

  and Misses:

---

- From Router-A ping 202.206.154.2 (which is a statically assigned global address for 10.10.10.2 in our internal network)

  Were you successful?

---

  Explain why you got that result?

---

  Hint: Check Router A's routing table Since we are on a stub network and the internal IP addresses are hidden from the rest of the Internet/Network, we need to add a static route to that network. On router-A (Internet router) add a static route to network 202.206.154.0/24. Try to ping 202.206.154.2 from Router-A.

  Were you successful this time?

---

  Why did our stub router not share information about network 202.206.154.0 with the other routers?

---

  What is NAT?

---

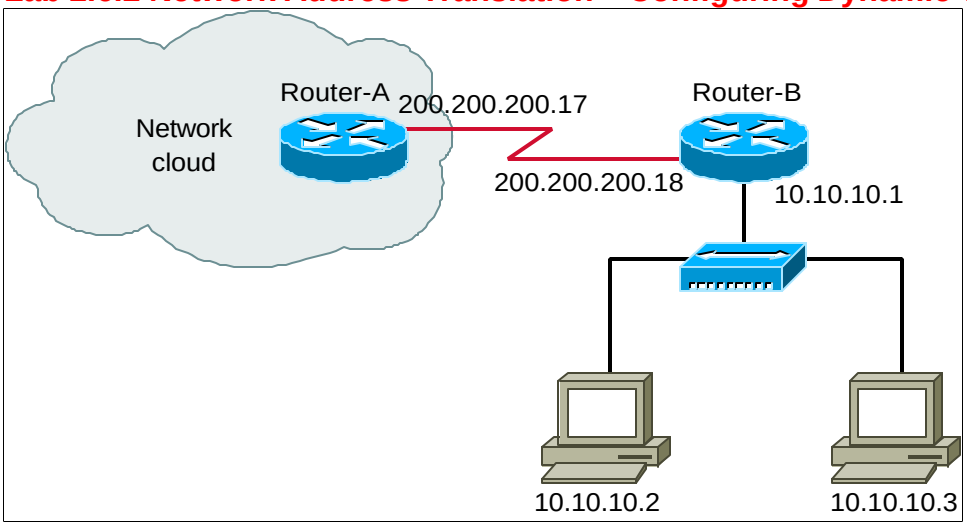
Why is NAT useful?

---

What would happen if we incorrectly marked the interfaces ( marked the fast Ethernet port as outside and the Serial as inside)?

---

# Lab 2.6.2 Network Address Translation -- Configuring Dynamic Translation




**Objective:**

Demonstrate the use of Network Address Translation through the use of dynamic address translation.

**Equipment Requirements:**

Two routers One switch Two workstations

**Background:**

A small company has been using the private address 10.10.10.0/24 for their network. Until recently they did not need access outside of their own network. Since they now need Internet access they have been issued the class C address 202.206.154.0 by ARIN. Currently the company does not require the full number of addresses in a Class C network; however, they will require the addresses as the company grows. For a variety of reasons including security reasons, the company wishes to hide the internal network from the outside. Currently most of the users need to be able to connect to the outside. These users need to have unlimited access to the outside.

Preliminary: Before programming the routers, make sure that the IOS version on the router supports Network address translation. Load a new IOS version if necessary. Construct the above network, using IGRP or RIP as your routing protocol. Do not advertise the private network. Use the network address 200.200.200.16/28 on the serial link from the stub network router(Router-B) and the Internet/Network router(Router-A).

The router IP configurations are as follows:

| Router-A | Router-B |
|---|---|
| | Fa 0/0=10.10.10.1 |
| S0/0=200.200.200.17/28 | S0/0=200.200.200.18/28 |

Note: actual interfaces used might vary depending on what type of router used.

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables for network 200.200.200.16/28. Also verify that the workstations are configured correctly for the network in which they reside. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping`**, **`telnet`**, and any other relevant command(s).

For this Lab we will be using Router-B as the stub network router where we will configure the network address translation. The router will be translating the inside local addresses to inside global addresses, in other words, converting the internal fake addresses into real addresses for use on the Internet.

**From the "Router-B" console:**

## Step 1

- Enter the EXEC mode.

## Step 2

- Enter the configuration mode by entering **`configure terminal`** command at the router prompt.

## Step 3

Define a pool of global addresses to be allocated as needed.

- Enter **`ip nat pool net-10 202.206.154.2 202.206.154.17 netmask 255.255.255.0`**

  Why is it important to include the netmask information?

---

## Step 4

Define a standard access list permitting those addresses that are to be translated.

- Enter **`access-list 2 permit 10.10.10.0 0.0.0.255`**

## Step 5

Establish dynamic source translation, specifying the access list defined in the prior step.

- Enter **`ip nat inside source list 2 pool net-10`**

## Step 6

Specify the inside interface.

- Enter **`interface fa 0/0`** (or correct inside interface for router used)

## Step 7

Mark the interface as connected to the inside.

- Enter **`ip nat inside`**

  Why do we only want to permit those addresses that are going to be translated?

---

## Step 8

Specify the outside interface.

- Enter **`interface serial 0/0`** (or correct outside interface for router used)

## Step 9

Mark the interface as connected to the outside.

- Enter **`ip nat outside`**

## Step 10

Save configuration information.

- Enter **`CTRL-Z`**
- Enter **`copy run start`**

## Step 11

Change default NAT timeout value (if required) to 120 seconds From global configuration mode

- Enter **`ip nat translation timeout 120`**

  The default timeout value is 24 hours, what is one reason we might want to reduce this amount that the entry is held in memory?

---

## Step 12

Monitoring NAT

- Enter **`show ip nat translations`**

  What information did the router respond with?

---

- Enter **`show ip nat statistics`**

  What information did the router respond with?

---

---

---

---

---

**Don't forget to add a static route to your global network on the outside router (Router-A)**

From a workstation on the inside network ping an address on the outside

From the router console

- Enter **`show ip nat translations`**

  What information did the router respond with?

---

- Enter **`show ip nat translations verbose`**

  What additional information did the router respond with?

---

- Enter **`show ip nat statistics`**

  What information did the router respond with?

---

---

---

- Change the IP address on the workstation on network 10.10.10.0 to 10.10.10.45, reboot the computer. After the computer boots ping an address on the outside.
- Enter **`show ip nat translations`**

  What new piece of information did the router respond with?

---

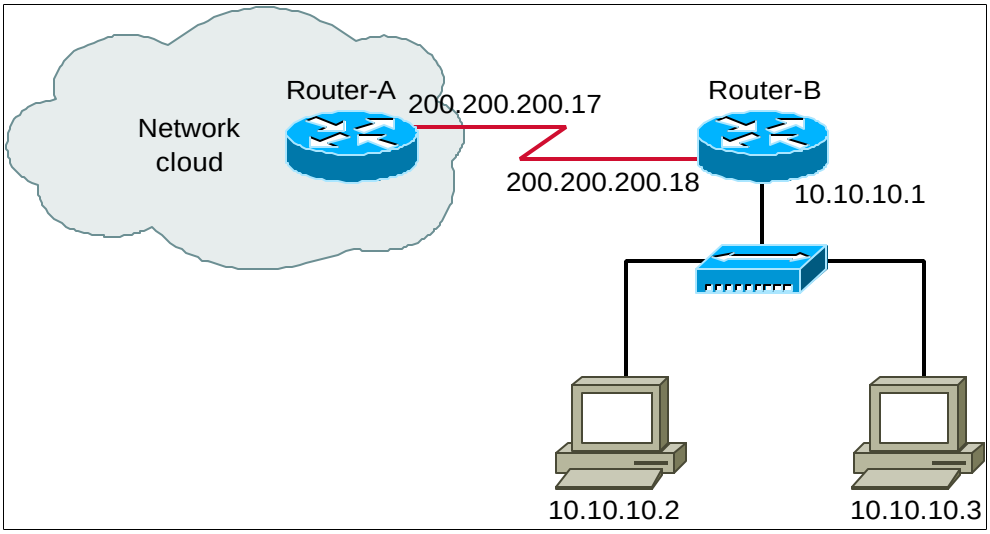
Could we use static translation and dynamic translation at the same time on the same router?

---

Can Cisco IOS NAT be applied to subinterfaces?

---

# Lab 2.6.3 Network Address Translation -- Configuring Overloading Translation




**Objective:**

Demonstrate the use of Network Address Translation through the use of overloading address translation.

**Equipment Requirements:**

Two routers One switch Two workstations

**Background:**

A small company has been using the private address 10.10.10.0/24 for their network. Until recently they did not need access outside of their own network. Since they now need Internet access they have been issued the class C address 202.206.154.0 by ARIN. Currently the company needs more than the number of addresses in a Class C network. For a variety of reasons including security reasons, the company wishes to hide the internal network from the outside. All of the users need to be able to connect to the outside. These users need to have unlimited access to the outside.

**Preliminary:**

Before programming the routers, make sure that the IOS version on the router supports Network address translation. Load a new IOS version if necessary. Construct the above network section, using IGRP or RIP as your routing protocol. Do not advertise the private network. Use the network address 200.200.200.16/28 on the serial link from the stub network router (Router-B) and the Internet/Network router (Router-A).

The router IP configurations are as follows:

| Router-A | Router-B |
|---|---|
| | `Fa 0/0=10.10.10.1/24` |
| `S0/0=200.200.200.17/28` | `S0/0=200.200.200.18/28` |

Note: actual interfaces used might vary depending on what type of router used.

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables for network 200.200.200.16/28. Also verify that the workstations are configured correctly for the network in which they reside. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping`**, **`telnet`**, and any other relevant command(s).

For this Lab we will be using Router-B as the stub network router where we will configure the network address translation. The router will be translating the inside local addresses to inside global addresses, in other words, converting the internal fake addresses into real addresses for use on the Internet.

**From the "Router-B" console:**

## Step 1

- Enter the EXEC mode.

## Step 2

- Enter the configuration mode by entering **`configure terminal`** command at the router prompt.

## Step 3

Define a pool of global addresses to be allocated as needed.

- Enter **`ip nat pool net-11 202.206.154.2 202.206.154.17 netmask 255.255.255.0`**

## Step 4

Define a standard access list.

- Enter **`access-list 3 permit 10.10.10.0 0.0.0.255`**

  What is the purpose of the access list?

  _____

## Step 5

Establish dynamic source translation, identifying the access list defined in the prior step.

- Enter **`ip nat inside source list 3 pool net-11 overload`**

  What does the word "overload" at the end of the command mean?

---

## Step 6

Specify the inside interface.

- Enter **`interface fa 0/0`** (or correct inside interface for router used)

## Step 7

Mark the interface as connected to the inside.

- Enter **`ip nat inside`**

## Step 8

Specify the outside interface.

- Enter **`interface serial 1`** (or correct outside interface for router used)

## Step 9

Mark the interface as connected to the outside.

- Enter **`ip nat outside`**

## Step 10

Save configuration information.

- Enter **`CTRL-Z`**
- Enter **`copy run start`**

## Step 11

Configure timeout values if required.

- Enter **`ip nat translation udp-timeout 120`**
- Enter **`ip nat translation dns-timeout 60`**
- Enter **`ip nat translation tcp-timeout 120`**

  Name a reason when you might want to give more time than the Cisco default timeout.

---

## Step 12

Monitoring NAT

- Enter **`show ip nat translations`**

  What information did the router respond with?

---

- Enter **`show ip nat translations verbose`**

  What additional information did the router respond with?

---

- Enter **`show ip nat statistics`**

  What information did the router respond with?

---

Did you remember to add the static route on router A?

From a workstation on the inside network ping an address on the outside

From the router console

- Enter **`show ip nat translations`**

  What information did the router respond with?

---

- Enter **`show ip nat statistics`**

  What information did the router respond with?

---

- From Router-A ping an address which has a nat listing on the translations table.

  Were you successful?

---

- Now from Router-A ping an address that is not currently in the routers translation table.

  Were you successful?

---

Explain the results of the previous questions.

---

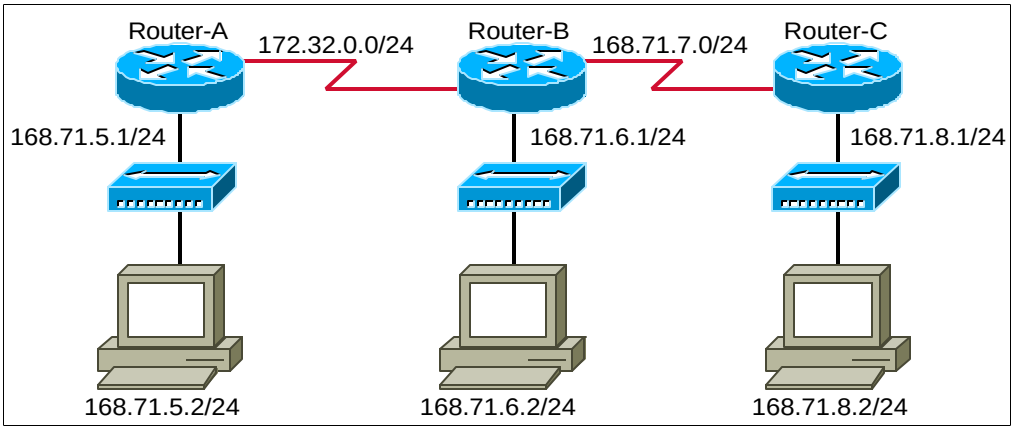
What is meant by NAT "overloading"?

---

When configuring for overloading what is the maximum number of translations that can be made with one inside global IP address?

---

# Lab 2.7.1 IP Unnumbered and Discontiguous Networks -- Configuring IP Unnumbered




**Objective:**

Demonstrate how improper IP addressing can have a negative impact on a network and the use of IP Unnumbered on a point to point serial link to save IP addresses.

**Background:**

Your company obtained an outside contractor to setup a basic network which would connect three different areas of the company. These areas do not need to access any other networks or the Internet. The resulting basic network is shown above in the graphic. The network does not operate as anticipated and it is your job to fix it.

**Equipment:**

Three Routers Three Switches Three workstation

## Step 1

Build the network in the above diagram. Use RIP or IGRP as your routing protocol

## Step 2

- Turn on Debug All on Router-A Ping S0/0 on Router-A from 168.71.8.2 workstation. Watch Router-A's debug information.

  What happened?

  _____

  _____

## Step 3

- Turn on Debug All on Router-C Ping Ethernet 0/0 on Router-A from 168.71.8.2 workstation. Watch Router-C's debug information.

  What did you see?

---

---

## Step 4

- On Router-A type **`sh ip route`**
- On Router-B type **`sh ip route`**
- On Router-C type **`sh ip route`**

  Describe the journey of the ICMP packets.

---

---

---

## Step 5

- Change the address on the 172.32.0.0 serial link so that the interfaces are in the 168.71.4.0 network.
- Ping from the workstation on network 168.71.5.0 to the workstation on 168.71.8.0

  Were you successful?

---

  Look at the routing tables Question - Determine what is reachable on the overall network?

---

## Step 6

Configure IP unnumbered on the serial links.

- On each serial interface enter **`ip unnumbered fa 0/0`** (or correct ethernet port)

Will the workstations be able to communicate?

---

- List the entries in the routing table

  What is the main purpose of IP unnumbered?

---

## Step 7

- Change the IP address of Ethernet0 on Router C to 168.71.8.17 255.255.255.240
- Clear the routing table using the command **`clear ip route *`**

  Can the workstations communicate? Why?

---

- List the entries in the routing table

  What changed in the routing table from step six to step seven?

---

## Step 8

- Change the IP Address of Ethernet 0 on Router C to 168.72.8.1 255.255.255.0
- Clear the routing table using the command **`clear ip route *`**

  Can the workstations communicate? Why?

---

---

---

---

**Reflection:**

Answer the following questions.

What benefit is gained by using IP unnumbered?

_____

How were the routers able to successfully forward packets using IP unnumbered?

_____

**Challenge Exercise:**

Can the five router lab from semesters 1-4 be configured to support IP unnumbered?

_____

_____

Record the contents of the routing table on one of the routers.

- Configure the network to support IP unnumbered.
- Compare the contents of the routing table using IP unnumbered to the routing table with subnets on the links.

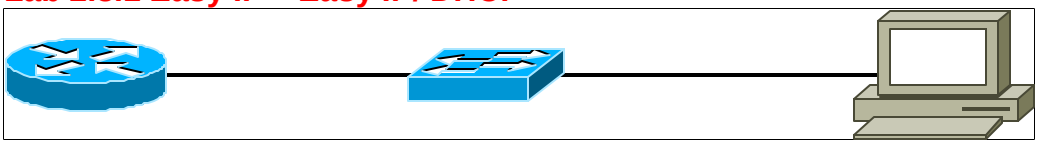
How many subnets have been saved?

_____

How does the router know how to forward packets on the network?

_____

# Lab 2.8.1 Easy IP -- Easy IP/ DHCP



**Objective:**

Demonstrate how easy IP can be used to provide dynamic IP addressing

**Background:**

You administer a small network for your company. You need a quick and easy DHCP server to give the computers on your network IP addresses. You are running a peer-to-peer network and do not have the funds for a new server. You do however have access to the network router. Your job is to make a DHCP server for your network.

**Equipment Requirements:**

- One Router (needs to be running a T version of IOS for example 12.0(5)T)
- One Switch
- One workstation

## Step 1

- Decide on the address pool that you will be using in the lab.

  Address Pool:

---

## Step 2

Configure e0 with the first usable address in the pool Address of e0:

---

## Step 3

- Configure the dhcp pool on the router
- router(config)#**`ip dhcp pool WORD`**
- router(dhcp-config**`)`**#**`network A.B.C.D/nn`**
- router(dhcp-config)#**`default-router A.B.C.D`**

Default router address:

---

## Step 4

- Connect the workstation and the router to the switch
- Set the workstation to automatically obtain an IP address
- Depending on your OS verify that the workstation received an IP address.

  For example with Windows 95 it is winipcfg and for Windows NT its ipconfig.

  Release and renew the IP address. Is the address from the pool defined in step 3?

---

What is the default Gateway?

---

Does the default Gateway match the default router address from step 3?

---

## Step 5

Your network administrator has decided he needs five servers to have static addresses and those addresses have to come from the pool.

- Configure the router so it will not give out the first five usable addresses in your network
- router(config)#**`ip dhcp excluded-address`** A.B.C.D (low address) A.B.C.D (high address)
- Release renew your clients IP address

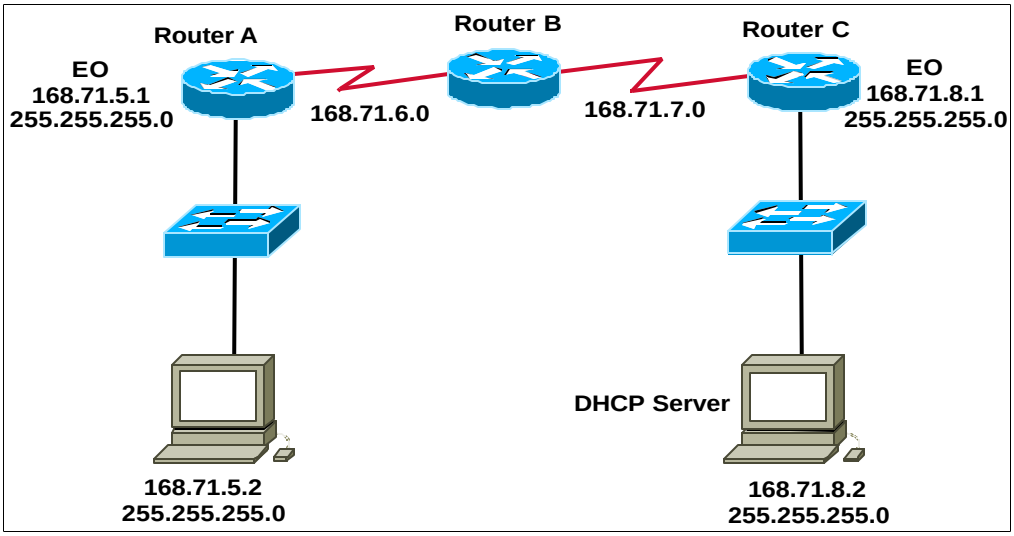
  What is the address now?

---

Did it get a new address?

---

# Lab 2.9.1 IP Helper Address




**Objectives:**

- Demonstrate the use of the IP Helper Address command to pass broadcasts from a network.

**Equipment Requirements:**

- Three Routers
- Two Switches
- One workstation
- One DHCP Server

**Preliminary**:

Before programming the routers, make sure that the IOS version on the router supports Network Address Translation. Load a new IOS version if necessary. Construct the above network section using an appropriate routing protocol.

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables. Also verify that the workstations are configured correctly for the network in which they reside.

For verification use the show ip route command, show interfaces command, show running-configuration command, ping, telnet, and any other relevant command(s).

Router configurations (interfaces subject to change based on routers used):

```
Router-A Router-B Router-C
FA0/0=168.71.5.1 S0/0=168.71.6.2 S0/1=168.71.7.2
S0/0=168.71.6.1 S0/1=168.71.7.1 FA0/0=168.71.8.1
SUBNET MASK 255.255.255.0
```

**Scenario**:

For this Lab we will be configuring IP helper on Router-A. Helper commands change broadcast addresses to a unicast address (an address of a single device on the network) so that the broadcast message can be routed to a specific destination, rather than everywhere. For our lab, we have a DHCP server on one subnet, but need it to give out IP addresses to another subnetwork. We do not have the funding for an additional DHCP server, so we must make the server that we have give out IP addresses from its current location.

## Step 1

Build the network in the above diagram. Use RIP or IGRP as your routing protocol.

## Step 2

Configure the DHCP Server with a pool of addresses that correspond to the addresses for the workstation.

## Step 3

Set the workstation to obtain an IP address automatically

Did the workstation obtain an address? Explain.

_____

## Step 4

On router A use the IP helper address command with the network number that the DHCP server resides on.

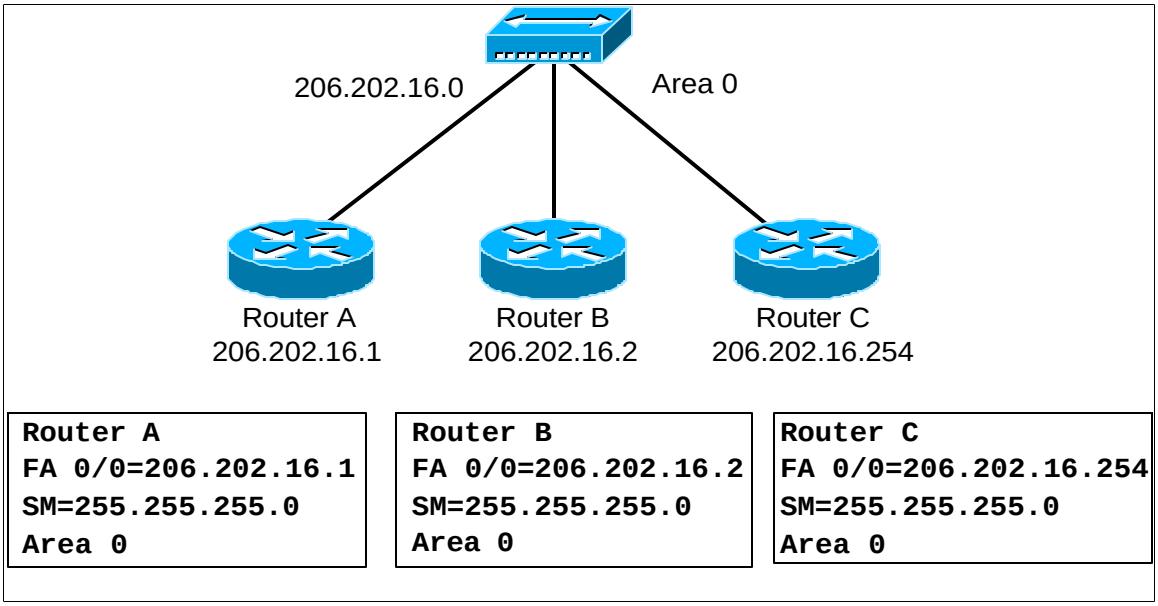
Did the workstation obtain an IP address? Explain

_____

_____

_____

## Lab 4.2.2 OSPF Routing Protocol




**Objective:**

Enable OSPF routing protocol in Area 0 only.

**Scenario:**

You have been hired by the BubbaGump ISP to setup a fast Ethernet core for their WAN.

(Note: Erase all routers before beginning)

**Tasks:**

From the "Router A" console

1. Cable the lab as shown above.
2. To configure the fastethernet interfaces and turn on the OSPF routing protocol issue the following commands:

- router-a(config)#**interface fastethernet 0/0**
- router-a(config-if)#**ip address 206.202.16.1 255.255.255.0**
- router-a(config-if)#**no shutdown**
- router-a(config-if)#**router ospf 1**
- router-a(config-router)#**network 206.202.16.0 0.0.0.255 area 0**

What does the 0.0.0.255 represent?

_____

What does the area 0 represent?

---

3. Follow the same procedure with different addresses on the other two router Fastethernet interfaces. Note: The OSPF network, wildcard mask, and area # does not change.

From the "Router C" console

4. Enter **`show running-config`** command:
5. Verify that the router has the OSPF protocol turned on and advertising the networks you defined. Check the syntax of the network statement in OSPF.
6. Enter **`show ip ospf`** command:

   What is the current LSA sequence number in area 0?

---

7. Enter **`show ip ospf`** interface

8. Enter **`show ip protocols`**

   Why are updates sent every 0 seconds?

---

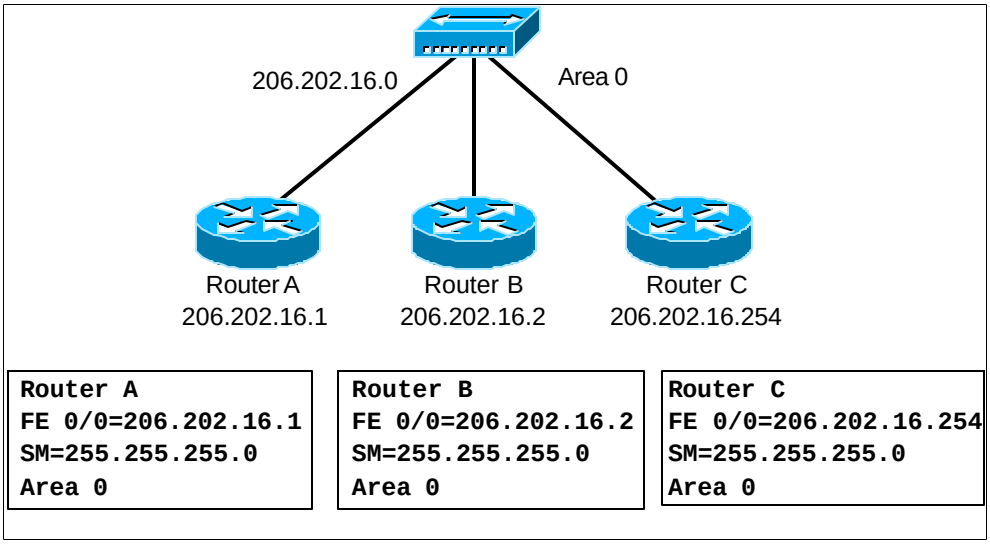
9. Which route is the DR and which router is the BDR?

---

10. What is the default AD of OSPF, and how does it compare to RIP?

---

# Lab 4.2.3 OSPF Timers




**Objective:**

Configure OSPF timers.

**Scenario:**

You have been called back by the ISP because their routers are not forming adjacencies with the routers you installed. They claim that they are getting timer errors?

From the "Router A" console

1. Enter enable exec mode and issue the command **`show ip ospf interface fastethernet 0/0`**

   What are the timer values currently set for Hello and Dead?

   ---

2. Manually change the hello and dead interval on the fastethernet interfaces by issuing the following commands:

- router-a(config)#**`interface fastethernet 0/0`**
- router-a(config-if)#**`ip ospf hello-interval 30`**
- router-a(config-if)#**`ip ospf dead-interval 120`**
- router-a(config-if)#**`control Z`**

3. Write the running-configuration to memory and issue the command **`show ip ospf neighbor`**

   What routers are listed

---

4. Enter **`show ip ospf database`**

   What routers are listed?

---

From the "Router B" console

5. Enter enable exec mode and change the timer values on "Router B"
6. After about a minute, enter **`show ip ospf neighbor`**

   What routers are listed?

---

7. Enter **`debug ip ospf adj`** and record your findings below:

---

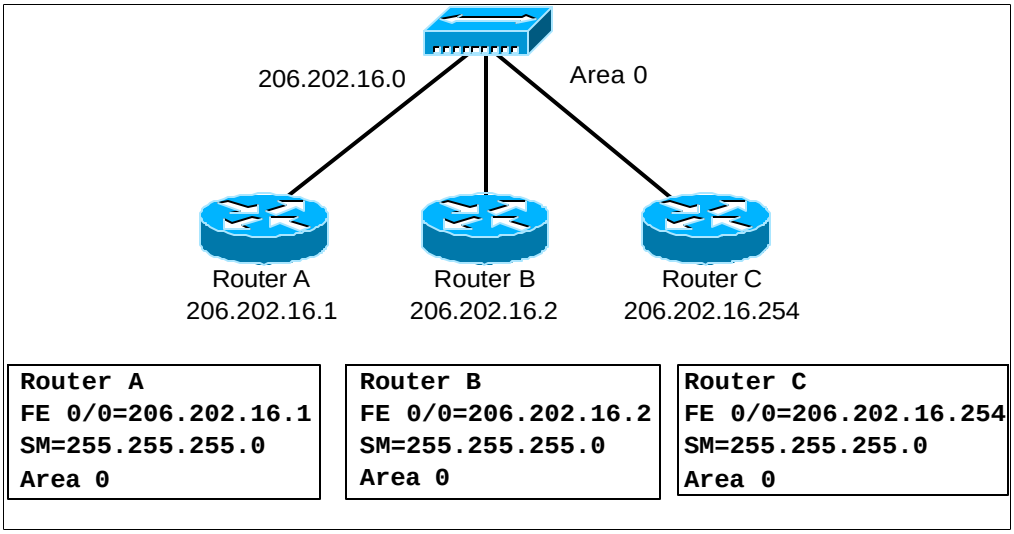
8. Change the timer values on all the routers in OSPF area 0, write the running-configurations of all the routers to memory, and reboot all routers in OSPF area 0.

From the "Router B" console

9. Enter **`enable exec mode`** and issue the command **`show ip ospf neighbor`**
10. List below the router IDs of the routers in OSPF area 0

---

# Lab 4.2.4.1 OSPF DR And BDR Selection




**Objective:**

Observe the DR and BDR selection process.

**WARNING:** There is a known bug in some 12.X IOS versions, where after the DR/BDR election process has completed, the DR can be replaced by a router with a higher ID.

**Scenario:**

You are the network administrator for the above network. You wish to see the interaction of OSPF routers in your broadcast network.

1. Write the running-configurations of all three routers to memory and turn off all three routers
2. Turn on "Router B" only
3. Enter **`show ip ospf neighbor`** and **`show ip ospf database`**

   What did the router respond with?

---

4. Enter **`show ip ospf interface`**

   What did the router respond with?

---

5. Turn on "Router A" only and wait one minute

From the "Router A" console

6. Enter **`show ip ospf neighbor`** and **`show ip ospf database`**

   What did the router respond with

---

From the "Router A" console

7. Enter **`debug ip ospf adjacencies`** from "Router A" and then turn on "Router C"

Report your findings concerning the DR/BDR election process.

8. Enter **`undebug all`** on "Router A"
9. Enter **`show ip ospf neighbor`** and **`show ip ospf database`**

   What did the router respond with

---

---

---

10. Enter **`show ip ospf interface`**

    Which router is the DR and which router is the BDR? Why?

---

---

11. Turn off all the routers and then turn on "Router A" only and wait one minute

From the "Router A" console

12. Enter **`enable exec mode`** and turn on the other two routers at the same time
13. Continuously issue the command **`show ip ospf neighbor`** as the other routers boot
14. Examine the router states as they boot. Report your findings.

From the "Router C" console

15. Enter **`show ip ospf neighbor detail`**

    What is the priority of all the routers in Area 0

---

From the "BDR Router" console

16. Enter **`debug ip ospf events`** turn off "The router that is the DR" only and wait one minute

    Predict which routers will become the DR and BDR after the DR router is dead

---

17. Enter **`show ip ospf neighbor`** after the election process has stopped

    Which router became the DR and which became the BDR? Why?

---

18. Turn on "the old DR router" only and wait one minute

    Did "the old DR router" became the DR again? Why?

---

---

19. Reboot all three routers at the same time

    Predict which routers will become the DR and BDR

---

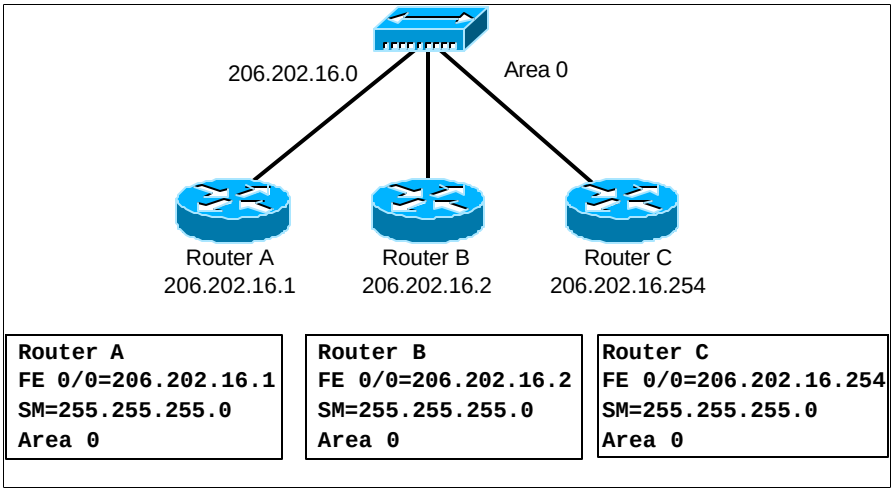
---

20. Enter **`enable exec mode`** and issue the command **`show ip ospf neighbor`**

    Which routers became the DR and BDR? Why?

---

# Lab 4.2.4.2 Force OSPF DR And BDR Selection




**Objective:**

Force the DR and BDR election process.

**Scenario:**

You have been called back by your ISP because "Router C" has been moved to a 56K link but continues to become the DR. This is causing a great slowdown in their WAN operations because each LSA must travel down this one 56K connection.

**Warning:** Boot order will have the greatest effect on the DR/DBR election process unless a priority of "0" is given to a router.

From the "Router A" console

1. Enter **`show ip ospf neighbor`**

   What is the priority of all the routers in Area 0 ?

---

2. To configure the router priority for the DR/BDR election process issue the following commands:

- router-a(config)#**`interface fastethernet 0/0`**
- router-a(config-if)#**`ip ospf priority 5`**

3. Write the running-configuration to memory

From the "Router B" console

4. Predict which router will now be the DR for Area 0 and then enter **`show ip ospf interface`**

   Examine which router is the DR for Area 0 and report your findings.

---

5. Issue the following commands on "Router B":

- router-b(config)#**`interface fastethernet 0/0`**
- router-b(config-if)#**`ip ospf priority 10`**

6. Write the running-configuration to memory, reboot all the routers in Area 0 and wait one minute.

From the "Router C" console

7. Enter **`show ip ospf neighbor`**

   Which routers are the DR and BDR for Area 0? Was there a change?

---

   Report the priority of all the other routers in Area 0

---

8. Enter **`debug ip ospf events`** and then turn off "Router A" only and wait one minute

Predict which router will become the BDR after Router A is dead

9. Enter **`undebug all`** after the election process has stopped

   Which router became the DR and which became the BDR. Why?

---

From the "Router C" console

10. To stop a router from becoming a DR/BDR issue the following commands:

- router-a(config)#**`interface fastethernet 0/0`**
- router-a(config-if)#**`ip ospf priority 0`**

11. Write the running-configuration to memory and reboot all the routers in Area 0

From the "Router A" console

12. Enter **`show ip ospf neighbor`** and report the priority of all the routers in Area 0 ?

---

13. Change the priority of all the routers to "0", write the running-configurations of all routers to memory, and reboot all the routers in Area 0.

    Report your findings below:

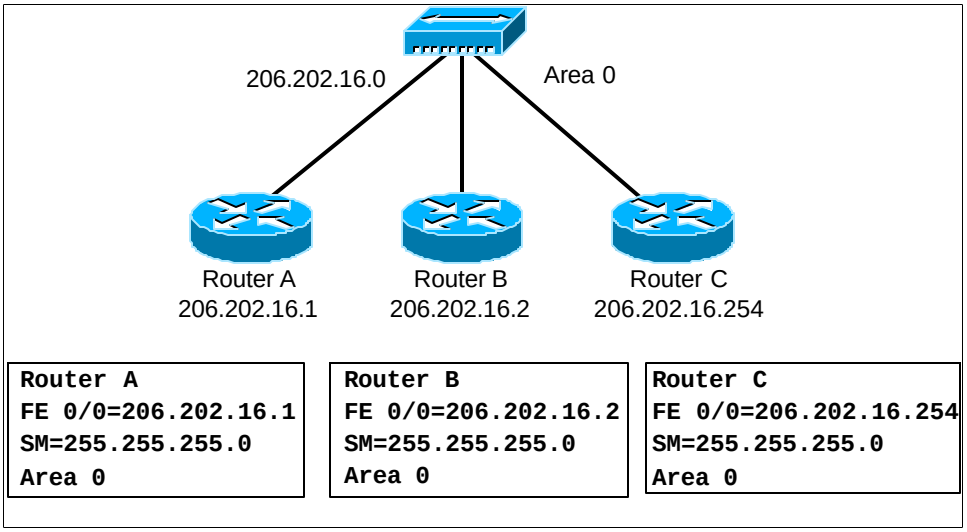
---

---

---

---

## Lab 4.3.2.1 Force OSPF Router ID




**Objective:**

Stabilize OSPF router ID with a loopback interface.

**Scenario:**

Every time there is power outage in the network, the router IDs change over to the Serial interface IP address. This is causing a great deal of instability because every time the router ID changes all the routers in OSPF Area 0 run the SPF algorithm.

(NOTE: Do not erase routers from the previous lab)

From the "Router C" console

1. Issue the following commands:

- router-c(config)#**`interface fastethernet 0/0`**
- router-c(config-if)#**`no ip address 206.202.16.254 255.255.255.0`**
- router-c(config-if)#**`control Z`**

2. Are there any error messages? Why?

---

3. Write the running-configuration to memory and reboot "Router C"
4. After the router boots enter **`enable exec mode`** and issue the command **`show running-config`**

5. Is OSPF still configured properly?

---

6. Issue the following commands:

- router-c(config)#**interface loopback 0**
- router-c(config-if)#**ip address 1.1.16.254 255.255.255.0**
- router-c(config-if)#**interface fastethernet 0/0**
- router-c(config-if)#**ip address 206.202.16.254 255.255.255.0**
- router-c(config-if)#**no shutdown**
- router-c(config-if)#**router ospf 1**
- router-c(config-router)#**network 206.202.16.0 0.0.0.255 area 0**
- router-c(config-router)#**control Z**

7. Write the running-configuration to memory and enter the command **show ip interface**

   What is the purpose of a loopback address?

---

8. Place a loopback interface on "Router A" and then enter **show ip ospf neighbor**

   What is the router id of "Router C"

---

9. Add loopback addresses to all the routers in OSPF area 0, write the running- configurations of all the routers to memory, and then reboot all the routers in Area 0

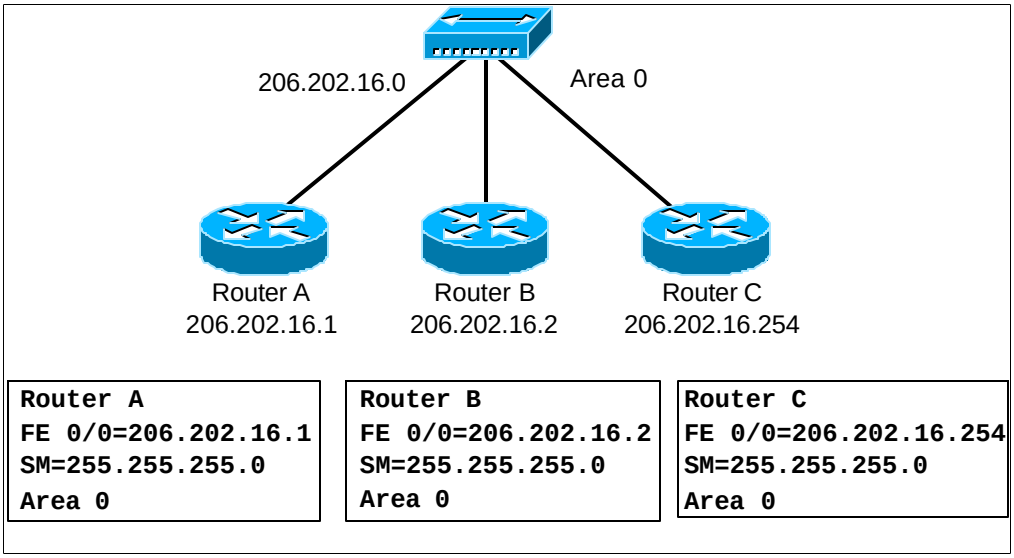
From the "Router A" console

10. Enter **enable exec mode** and issue the command **show ip ospf neighbor**

    What are the router IDs of all the routers in OSPF area 0?

---

## Lab 4.3.2.2 OSPF Authentication




**Objective:**

Configure OSPF area 0 authentication.

**Scenario:**

The BubbaGump ISP now has a hacker attacking their open OSPF WAN. You have been called on to password protect the OSPF routing protocol on their network.

From the "Router A" console

1. Turn on authentication and configure the fastethernet interfaces with an authentication password by issuing the following commands:

- router-a(config)#**`router ospf 1`**
- router-a(config-router)#**`area 0 authentication`**
- router-a(config)#**`interface fastethernet 0/0`**
- router-a(config-if)#**`ip ospf authentication-key cisco`**
- router-a(config-if)#**`control Z`**

2. Write the running-configuration to memory
3. Enter **`show ip ospf neighbors`** and report below the routers listed

---

4. Enter **`show ip ospf database`**

   What routers are listed? Why?

---

From the "Router B" console

5. Configure authentication with the same password on "Router B"
6. Enter **`show ip ospf neighbor`**

   What routers are listed?

---

7. Enter **`debug ip ospf ad`**j and report your findings below:

---

8. Add the Cisco authentication key to all the routers in OSPF area 0, write the running-configurations of all the routers to memory, and reboot all routers in OSPF area 0.

From the "Router B" console

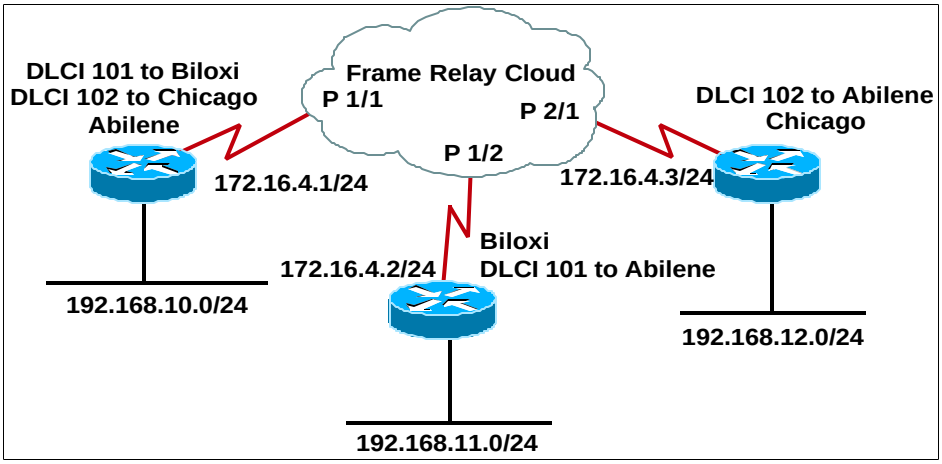
9. Enter **`enable exec mode`** and issue the command **`show ip ospf neighbor`**

   List below the router IDs of the routers in OSPF area 0

---

---

## Lab 4.4.4 OSPF Point-to-Multipoint Lab




**Objectives:**

- Configure OSPF to function correctly in a non-broadcast environment.

**Equipment Requirements:**

- Two Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Scenario:**

You are the network administrator of the above network, which has 3 sites, connected via a hub and spoke frame-relay cloud. Both Biloxi and Chicago have PVC's to Abilene. It is well documented that OSPF behaves quite differently in a Non-broadcast environment as opposed to a broadcast environment. You have decided to implement a point-to-multipoint configuration.

## Step 1

Cable the lab as shown above. The device used to simulate a frame relay cloud will be the Adtran unit.

## Step 2

Configure the serial interfaces to match the addressing scheme shown above. Use the first available address for your Ethernet interfaces. Use multipoint subinterfaces on the serial connections into the frame cloud. To configure the subinterfaces issue the following commands:

```
Abilene(config)#interface serial 0
Abilene(config-if)#encapsulation frame-relay
IETF
Abilene(config-if)#no shutdown

Abilene(config)#interface serial
0.101multipoint
Abilene(config-subif)#ip address 172.16.4.1
255.255.255.0
```

Follow this same procedure with different addresses on the other two router serial interfaces.

## Step 3

Why did we choose to use multipoint interfaces?

## Step 4

Now it is time to complete the frame-relay configuration. On Abilene, you need to set up the DLCI for both connections. The connection to Biloxi is DLCI 101 and the connection to Chicago is DLCI 102. Issue the following commands on the sub-interface:

```
Abilene(config-subif)#frame-relay interface-
dlci 101
Abilene(config-subif)#frame-relay interface-
dlci 102

Biloxi(config-subif)#frame-relay map ip
192.168.10.0 101 broadcast
Biloxi(config-subif)#frame-relay map ip
192.168.12.0 101 broadcast

Chicago(config-subif)#frame-relay map ip
192.168.10.0 102 broadcast
Chicago(config-subif)#frame-relay map ip
192.168.11.0 102 broadcast
```

## Step 5

Enable OSPF routing on each router. Advertise all networks directly connected to your router.

## Step 6

Examine the routing tables of each router. Are any entries missing? Can you ping everywhere? Report your findings.

## Step 7

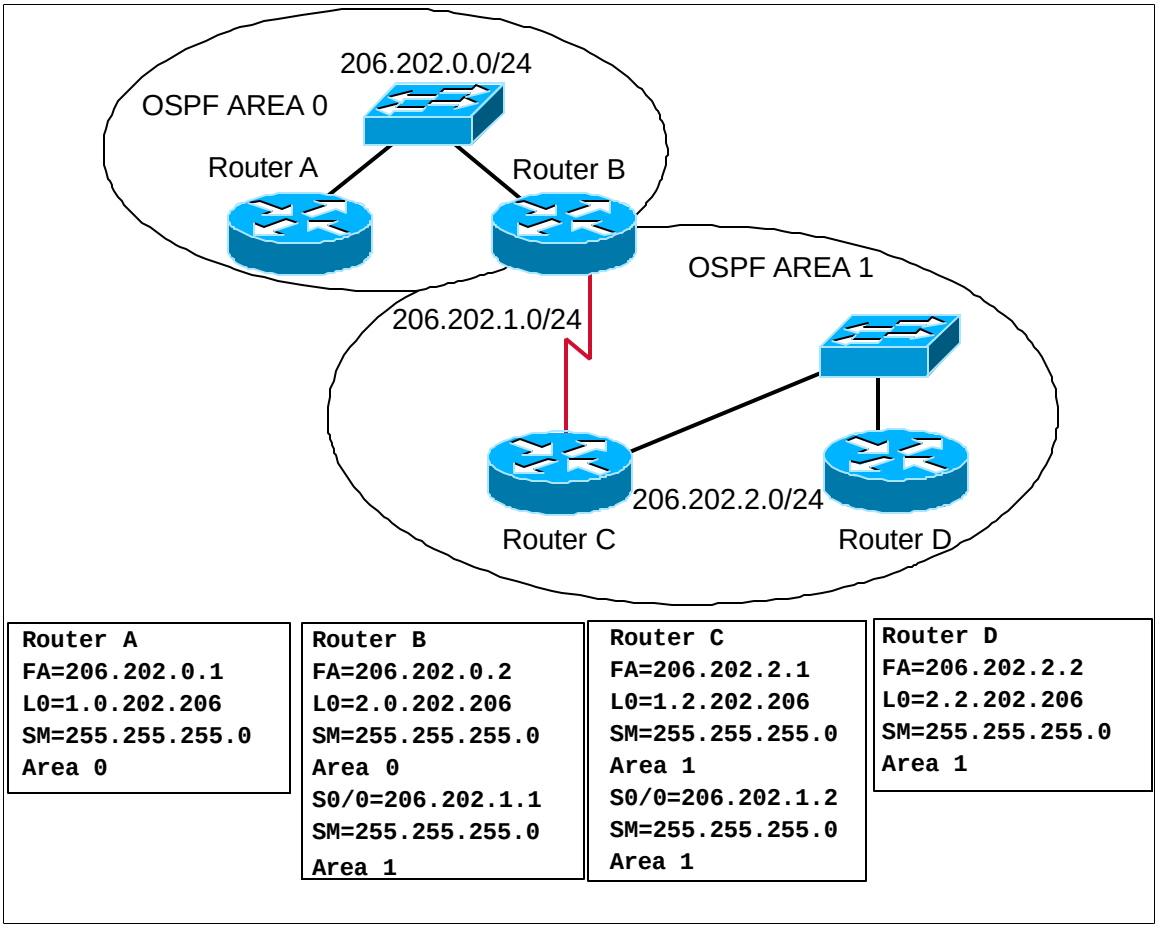
Now it is time to make OSPF behave correctly! Issue the following command on each subinterface of each router:

```
Router(config-subif)#ip ospf network point-to-
multipoint
```

## Step 8

Go back and verify complete routing tables and verify connectivity. Report your findings.

## Lab 5.1.2.1 Multi-Area OSPF Routing




**Objective:**

Enable OSPF routing protocol for Multiple areas.

**Scenario:**

You have been hired by the BubbaGump ISP to setup and add on to their WAN.

(Note: Erase all routers before beginning)

**Tasks:**

1. Cable the lab as shown above.

- From the "Router A" console
- Configure OSPF routing in Area 0
- From the "Router B" console

2. To configure the interfaces and setup multi-area OSPF issue the following commands:

- router-b(config)#**interface loopback 0**
- router-b(config-if)#**ip address 2.0.202.206 255.255.255.0**
- router-b(config-if)#**interface fastethernet 0/0**
- router-b(config-if)#**ip address 206.202.0.2 255.255.255.0**
- router-b(config-if)#**no shutdown**
- router-b(config-if)#**interface serial 0/0**
- router-b(config-if)#**ip address 206.202.1.1 255.255.255.0**
- router-b(config-if)#**clockrate 56000**
- router-b(config-if)#**router ospf 1**
- router-b(config-router)#**network 206.202.0.0 0.0.0.255 area 0**
- router-b(config-router)#**network 206.202.1.0 0.0.0.255 area 1**
- router-b(config-router)#**^Z**

3. Enter **show ip ospf** and **show ip ospf border-routers**. Report your findings below:

_____

_____

_____

From the "Router C" console

4. Issue the following commands:

- router-c(config)#**interface loopback 0**
- router-c(config-if)#**ip address 1.2.202.206 255.255.255.0**
- router-c(config-if)#**interface fastethernet 0/0**
- router-c(config-if)#**ip address 206.202.2.1 255.255.255.0**
- router-c(config-if)#**no shutdown**
- router-c(config-if)#**interface serial 0/0**
- router-c(config-if)#**ip address 206.202.1.2 255.255.255.0**
- router-c(config-if)#**router ospf 1**
- router-c(config-router)#**network 206.202.1.0 0.0.0.255 area 1**
- router-c(config-router)#**network 206.202.2.0 0.0.0.255 area 1**
- router-c(config-router)#**^Z**

5. Enter **`show ip ospf interface`**

Is the OSPF protocol turned on the correct interfaces that you defined?

---

- From the "Router D" console
- Configure OSPF routing in Area 1 only.
- After you have configured "Router D" go back to each router and verify that ospf is turned on and advertising the correct networks. Ping all interfaces.

6. Enter **`show ip ospf neighbor`** and report your findings below:

---

7. Enter **`show ip ospf border-router`** and **`show ip route`**

What information did the router respond with?

---

---

8. Enter **`show ip ospf interface`** and **`debug ip ospf events`**

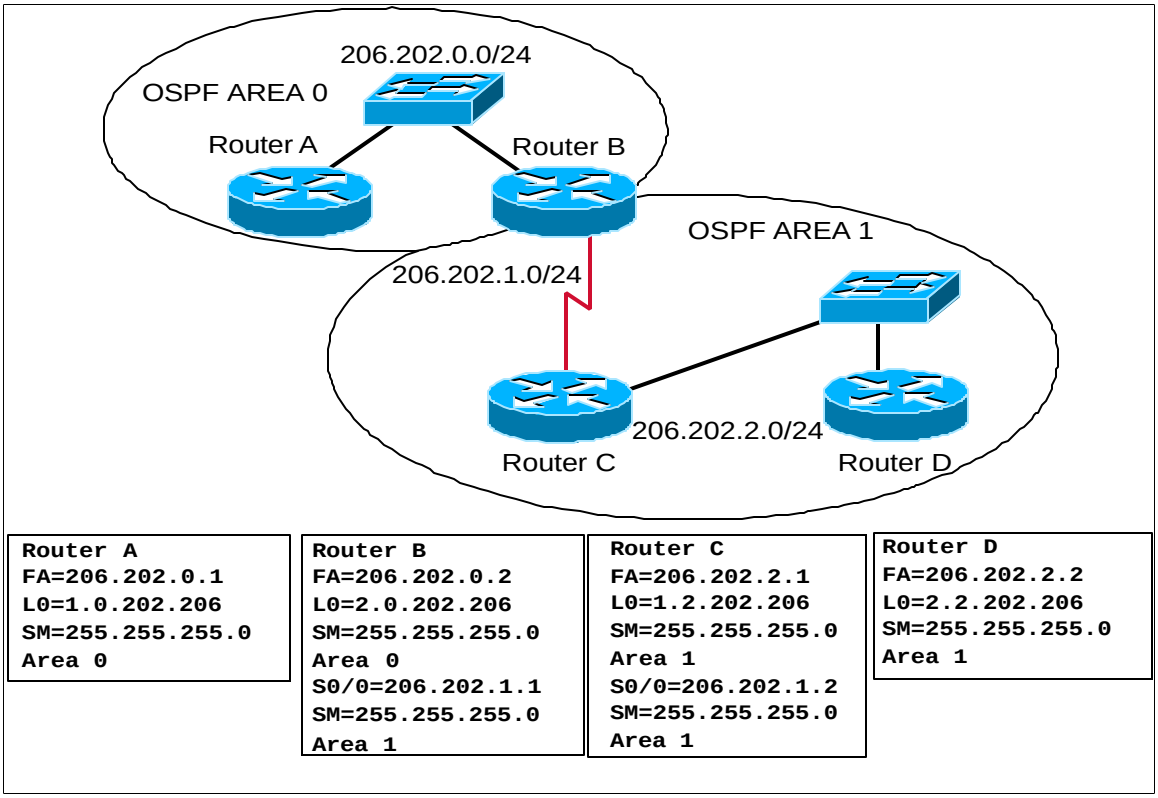
What routers are sending hellos and from what area? Why?

---

---

9. Enter **`undebug all`**

## Lab 5.1.2.2 Bandwidth




**Objective:**

Configure OSPF to calculate the correct cost of an interface.

**Scenario:**

The BubbaGump ISP has reported an issue with their OSPF WAN metrics. There is only a 56KB line on the serial link; however, the link is being reported as a T-1 metric. This must be fixed by you.

From the "Router B" console

1. Enter **`show ip ospf interface`**

   What is the cost of interface Serial 0/0 ?

   _____

2. To change the cost issue the following commands:

   - router-b(config)#**`interface serial 0/0`**
   - router-b(config-if)#**`bandwidth 56`**
   - router-b(config-router)#**`^Z`**

From the "Router C" console

3. Enter **`show ip ospf interface`**

What is the cost of interface Serial 0/0 ?

---

4. To change the cost issue the following commands:

- router-c(config)#**`interface serial 0/0`**
- router-c(config-if)#**`bandwidth 56`**
- router-c(config-router)#**`^Z`**

5. Enter **`show ip ospf interface`**

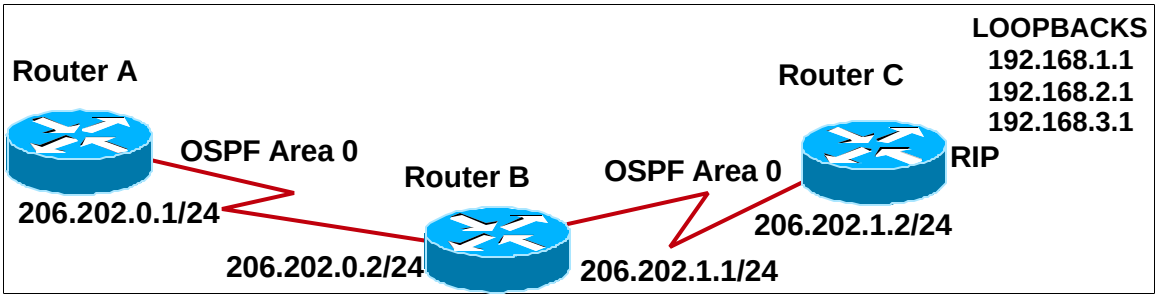
What is the new cost of interface Serial 0/0 ?

---

If uncorrected what will OSPF default the cost of a serial interface?

---

# Lab 5.3.2 OSPF External Summarization




**Objectives:**

- Use summarization with OSPF to reduce the number of external routes in the routing table.

**Equipment Requirements:**

- Three Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Scenario:**

You have a RIP routing domain and an OSPF Area 0 with redistribution. You need to reduce the number of RIP routes that enter your OSPF Area 0. You must configure a summary-address in OSPF to only advertise one route to the RIP networks.

## Step 1

Cable the lab and all interfaces as shown in the diagram. You will use loopbacks for the RIP networks.

## Step 2

Configure OSPF routing on all routers.

```
Router-a(config)#router ospf 1
Router-a(config-router)#network 206.202.0.0
0.0.3.255 area 0

Router-b(config)#router ospf 1
Router-b(config-router)# network 206.202.0.0
0.0.3.255 area 0

Router-c(config)router ospf 1
Router-c(config-router)#network 206.202.0.0
```

```
0.0.3.255 area 0
Router-c(config-router)#router rip
Router-c(config-router)#network 192.168.1.0
Router-c(config-router)#network 192.168.2.0
Router-c(config-router)#network 192.168.3.0
```

## Step 3

Verify that OSPF is configured correctly and all OSPF routes are listed in the routing table. On Router C the 192.168.1.0-192.168.3.0 networks should be directly connected, but not listed in the routing table of the other routers.

## Step 4

On Router C add the following command to redistribute all the rip routes into your OSPF Area 0:

Router-c(config)router ospf 1
Router-c(config-router)#redistribute rip subnets

## Step 5

On Router A, issue the command show ip route to see if the rip routes are being redistributed into the OSPF Area 0.

_____

_____

_____

## Step 6

On Router C, add the following command to properly summarize the RIP routes into the OSPF Area 0.

Router-c(config)router ospf 1
Router-c(config-router)#summary-address 192.168.0.0 255.255.252.0

## Step 7

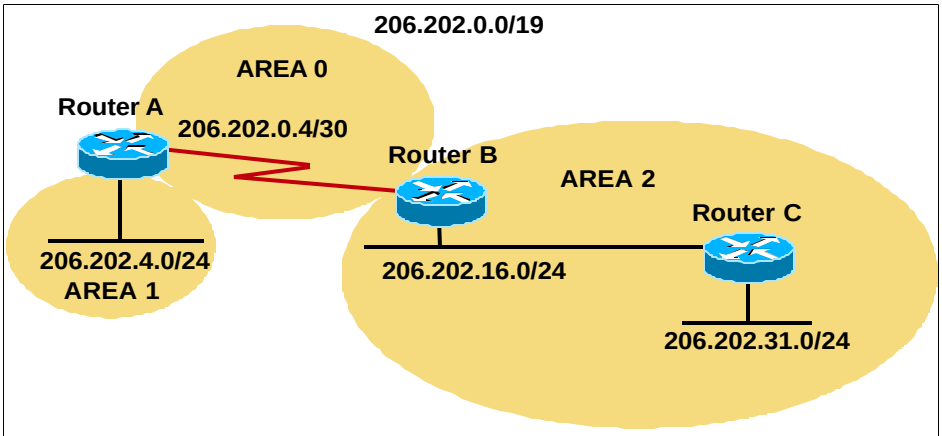
Issue the command **`show ip route`** from Router A and Router B. Record your results below.

_____

_____

_____

# Lab 5.3.3 Area Range




| Router A | Router B | Router C |
|---|---|---|
| FE0/0=206.202.4.1 | FE0/0=206.202.16.1 | FE0/0=206.202.16.2 |
| L0=1.4.202.206 | L0=1.16.202.206 | L0=2.16.202.206 |
| SM=255.255.255.0 | SM=255.255.255.0 | SM=255.255.255.0 |
| Area 1 | Area 2 | Area 2 |
| S0/0=206.202.0.5 | S0/0=206.202.0.6 | FE0/1=206.202.31.1 |
| SM=255.255.255.252 | SM=255.255.255.252 | SM=255.255.255.0 |
| Area 0 | Area 0 | Area 2 |

**Objectives:**

- Configure OSPF to summarize addresses within an area.

**Scenario:**

You have been hired by The Washington Post to setup a WAN for their 3 sites. You must setup sites in summarizable groups of addresses to reduce the number of routes in the routing table. You must use the area range command to summarize OSPF Area 2.

**Tasks:**

1. Cable the lab as shown above.

   **Configure OSPF routing in Area 0, 1 and 2 as shown above.**
   **Ping all interfaces before continuing.**

2. Enter **`show ip route`**

   Are there two separate routes to the 206.202.16.0 and 206.202.31.0 networks?

   **From the "Router B" console**

3. To setup multi-area OSPF summarization on this router issue the following commands:

```
router-b(config)#router ospf 1
router-b(config-router)#area 2 range
206.202.16.0 255.255.240.0
router-b(config-router)#^Z
```

**From the "Router A" console**

4. Enter **`show ip route`**

   What does "IA" represent?

   _____

   How many bits are in the route for 206.202.16.0 ? Why?

   _____

   What is the range of networks being advertised?

   _____

5. **`Ping and trace to 206.202.31.1`**

   What did the router reply with?

   _____

6. Enter **`trace 206.202.18.1`**

   What did the router reply with? Report your findings below:

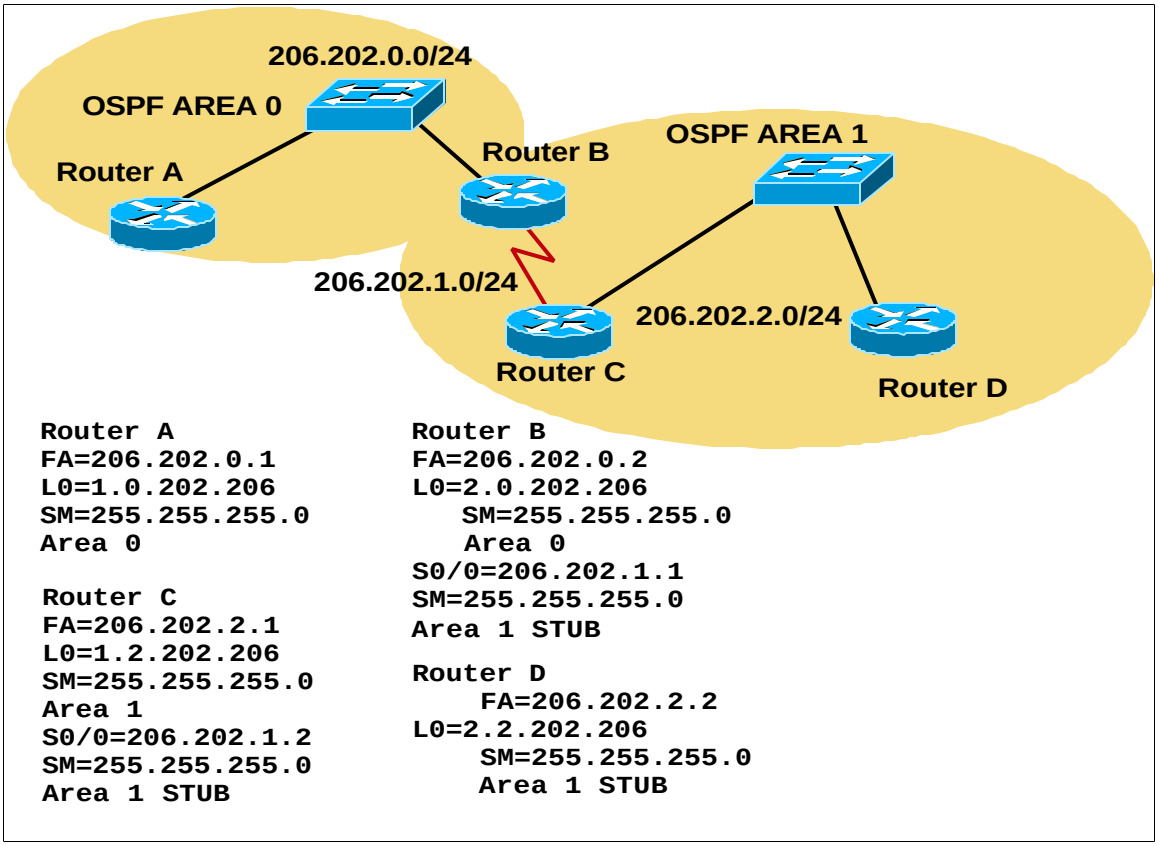
   _____

   _____

   _____

   _____

# Lab 5.4.5 Multi-Area OSPF Routing -- Stub and Totally Stubby Areas




**Objectives:**

- Configure OSPF Area 1 as Stub and Totally Stubby

**Scenario:**

The BubbaGump ISP wants to limit the number of routes that enter Area 1 so you have been called to setup the area as STUB.

**Tasks:**

**From the "Router D" console**

**NOTE: Ping all interfaces before beginning.**

1. Enter show ip ospf neighbor

   What is the neighbor state?

   _____

2. To configure an area OSPF as stub issue the following commands:

```
router-d(config)#router ospf 1
router-d(config-router)#area 1 stub
router-d(config-router)#control Z
```

3. Enter show ip ospf neighbor

   What is the neighbor state now? Why?

   _____

4. Enter show ip route

   What routes are now available?

   _____

   **From the "Router C" console**

5. Enter show ip route and show ip ospf neighbor. Report your findings below:

   _____

   _____

   _____

6. To configure this OSPF router as a stub issue the following commands:

```
router-c(config)#router osfp 1
router-c(config-router)#area 1 stub
router-c(config-router)#control Z
```

   Enter show ip route and show ip ospf neighbor

   What changed? Why?

   _____

   **From the "Router B" console**

7. Enter show ip route and show ip ospf neighbor. Report your findings below:

   _____

   _____

   _____

8. To configure area 1 only as a stub issue the following commands:

```
router-b(config)#router osfp 1
router-b(config-router)#area 1 stub
router-b(config-router)#control Z
```

9. Enter show ip route and show ip ospf neighbor

   What changed? Why?

   ---

   **From the "Router D"console**

10. Enter show ip route

    Is there a gateway of last resort set? Why?

    ---

    What routes are listed?

    ---

**Scenario:**

You have now been instructed by the BubbaGump ISP to make area 1 a totally stub network.

**From the "Router B" console**

11. To configure this OSPF area as totally stub issue the following commands:

```
router-b(config)#router osfp 1
router-b(config-router)#no area 1 stub
router-b(config-router)#area 1 stub no-summary
router-b(config-router)#area 1 default-cost 10
router-b(config-router)#control Z
```

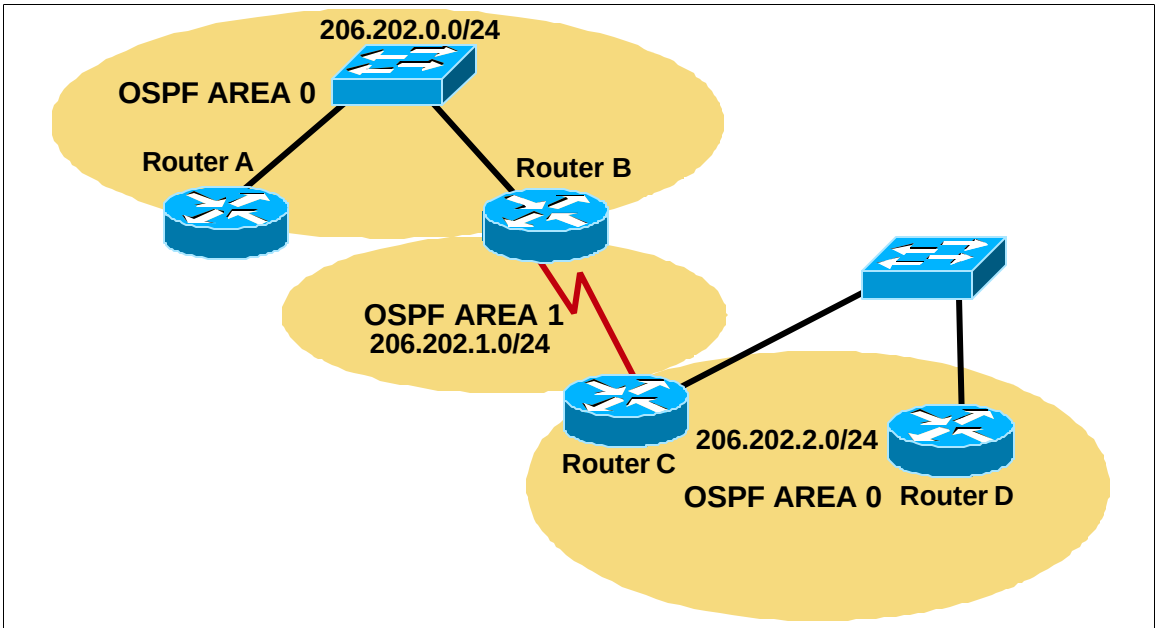
**From the "Router D" console**

12. Enter show ip ospf border-router and show ip route

    What routes are now listed?

    ---

## Lab 5.5.2 Virtual-Links




| Router A | Router B | Router C | Router D |
|---|---|---|---|
| FA=206.202.0.1 | FA=206.202.0.2 | FA=206.202.2.1 | FA=206.202.2.2 |
| L0=1.0.202.206 | L0=2.0.202.206 | L0=1.2.202.206 | L0=2.2.202.206 |
| SM=255.255.255.0 | SM=255.255.255.0 | SM=255.255.255.0 | SM=255.255.255.0 |
| Area 0 | Area 0 | Area 0 | Area 0 |
| | S0/0=206.202.1.1 | S0/0=206.202.1.2 | |
| | SM=255.255.255.0 | SM=255.255.255.0 | |
| | Area 1 | Area 1 | |

**Objectives:**

- Configure OSPF Virtual Links

**Scenario:**

The BubbaGump ISP has merged with the Newton ISP. Unfortunately, the Newton ISP already has an OSPF area 0. They will not renumber their OSPF area 0 so you must create a virtual link between the two companies.

**Tasks:**

1. Cable the lab as shown above.

   Configure OSPF routing in Area 0, 1, and 0 as shown above. Make sure you use loopback interfaces. Before continuing, what interfaces can you `ping`?

   _____

**From the "Router C" console**

2. To configure the virtual link and implement multi-area OSPF between the two companies issue the following commands:

```
router-c(config)#router ospf 1
router-c(config-router)#area 1 virtual-link 2.0.202.206
router-c(config-router)#^Z
```

**From the "Router B" console**

3. To configure the virtual link and implement multi-area OSPF between the two companies issue the following commands:

```
router-b(config)#router ospf 1
router-b(config-router)#area 1 virtual-link 1.2.202.206
router-b(config-router)#^Z
```

**WARNING: If you did not use loopback addresses on your routers this will not work.**

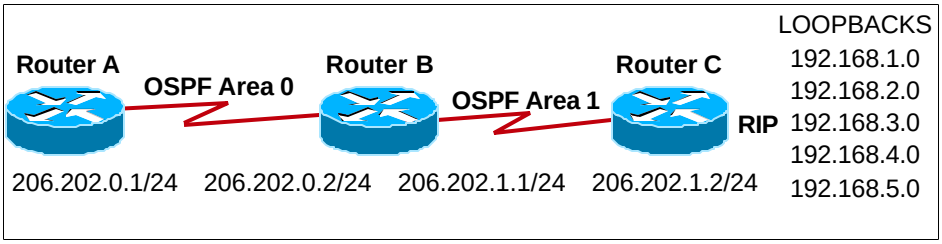
4. Enter show ip ospf virtual-links. Report your findings below:

_____

_____

_____

# Lab 5.6.1 OSPF NSSA with Route Filtering




**Objectives:**

- Use OSPF with the NSSA option to redistribute RIP routes into the OSPF core via a stub transit area.

**Scenario:**

You have a RIP routing domain and an OSPF Area 0 with redistribution. You need to reduce the number of OSPF routes that enter your OSPF Stub Area. You must allow the redistributed routes into the core. You must also filter some of your RIP routes from entering the core area.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram. You will use loopbacks for the RIP networks.

2. Configure OSPF routing on all routers.

```
Router-a(config)#router ospf 1
Router-a(config-router)#network 206.202.0.0 0.0.0.255 area 0

Router-b(config)#router ospf 1
Router-b(config-router)# network 206.202.0.0 0.0.0.255 area 0
Router-b(config-router)# network 206.202.1.0 0.0.0.255 area 1

Router-c(config)interface loopback 1
Router-c(config-if)ip address 192.168.1.1 255.255.255.0
Router-c(config-if)interface loopback 2
Router-c(config-if)ip address 192.168.2.1 255.255.255.0
Router-c(config-if)interface loopback 3
Router-c(config-if)ip address 192.168.3.1 255.255.255.0
Router-c(config)interface loopback 4
Router-c(config-if)#ip address 192,168.4.1 255.255.255.0
Router-c(config-if)interface loopback 5
Router-c(config-if)ip address 192.168.5.1 255.255.255.0
Router-c(config)router ospf 1
Router-c(config-router)#network 206.202.1.0 0.0.0.255 area 1
Router-c(config-router)#router rip
Router-c(config-router)#network 192.168.1.0
Router-c(config-router)#network 192.168.2.0
Router-c(config-router)#network 192.168.3.0
Router-c(config-router)#network 192.168.5.0
```

3. Verify that OSPF is configured correctly and all OSPF routes are listed in the routing table. On Router C the 192.168.XX.XX networks should be directly connected, but not listed in the routing table of the other routers.

4. On Router C add the following command to redistribute all the rip routes into your OSPF Area 0:

```
Router-c(config)router ospf 1
Router-c(config-router)#redistribute rip subnets
```

5. On Router A, issue the command **`show ip route`** to see if the rip routes are being redistributed into the OSPF Area 0.

6. On Router B, add the following command to properly summarize the RIP routes into the OSPF Area 0.

```
Router-b(config)router ospf 1
Router-b(config-router)#summary-address 192.168.0.0
255.255.252.0 not-advertise
```

7. Issue the command **`show ip route`** from Router A. Record your results below.

_____

8. Go to Router B and Router C and add the following command:

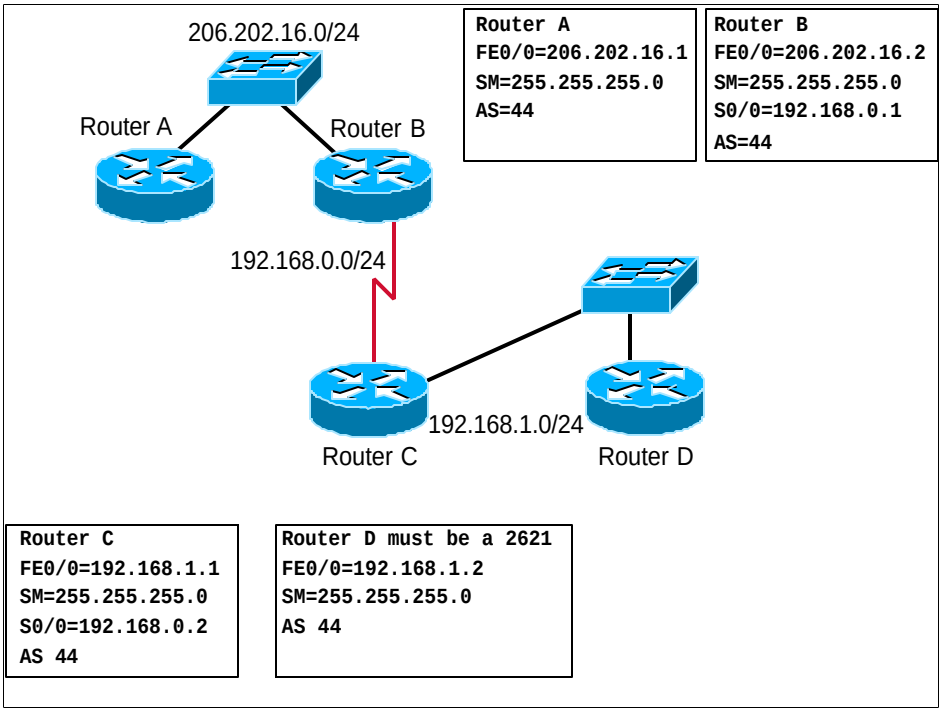
```
Router-b(config)router ospf 1
Router-b(config-router)#area 1 nssa
Router-c(config)router ospf 1
Router-c(config-router)#area 1 nssa
```

9. Issue the commands **`show ip route`** from Router A and Router B. Record your results below.

_____

_____

# Lab 6.1.1.1 EIGRP Routing Protocol




**Objective:**

Enable EIGRP routing protocol.

(Note: This is a hybrid Cisco proprietary routing protocol)

**Scenario:**

You have been hired by the Lubbock ISP to setup an EIGRP WAN.

(Note: Erase all routers before beginning)

**Tasks:**

From the "Router A" console

1. Cable the lab as shown above.
2. To configure the fastethernet interfaces and turn on the EIGRP routing protocol issue the following commands:

- router-a(config)#**interface fastethernet 0/0**
- router-a(config-if)#**ip address 206.202.16.1 255.255.255.0**
- router-a(config-if)#**no shutdown**
- router-a(config)#**router eigrp 44**
- router-a(config-router)#**network 206.202.16.0**
- router-a(config-router)#**^Z**

From the "Router B" console

3. Issue the following commands:

- router-b(config)#**interface fastethernet 0/0**
- router-b(config-if)#**ip address 206.202.16.2 255.255.255.0**
- router-b(config-if)#**no shutdown**
- router-b(config)#**interface serial 0/0**
- router-b(config-if)#**ip address 192.168.0.1 255.255.255.0**
- router-b(config-if)#**clockrate 56000**
- router-b(config-if)#**no shutdown**
- router-b(config)#**router eigrp 44**
- router-b(config-router)#**network 206.202.16.0**
- router-b(config-router)#**network 192.168.0.0**
- router-b(config-router)#**^Z**

4. Follow the same procedure with different addresses on the other two routers
5. Enter **show running-config**, **show ip route**, **and show ip protocol** on each router:

   Is the router eigrp protocol turned on and advertising the networks you defined .

---

From the "Router B" console

6. Enter the **show ip eigrp neighbors** command and report below the neighbors listed
7. Enter **show ip eigrp topology**

   Are there any successors

---

8. Enter **show ip protocols**

   What is the default administrative distance of EIGRP?

---

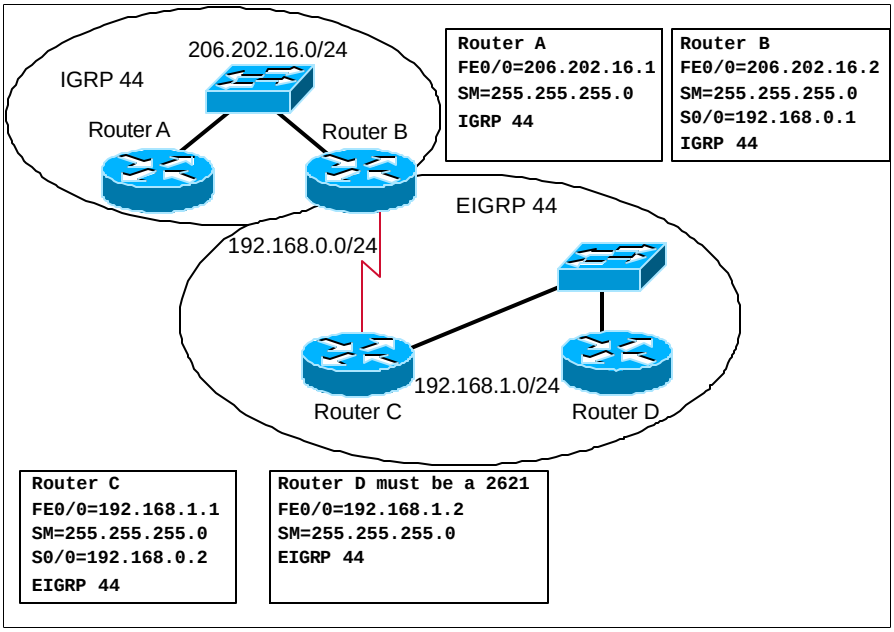
   Why is there a difference in the distances?

---

9. Enter the **`show ip route`** command and report below the routes listed

_____

# Lab 6.1.1.2 EIGRP/IGRP Redistribution




**Objective:**

Configure EIGRP and IGRP routing protocols. IGRP will automatically redistribute into EIGRP if given the same AS#.

**Scenario:**

You have been called back by the Lubbock ISP because several of their core routers do not have enough memory to run EIGRP. You must setup IGRP in the CORE only.

**Tasks:**

**From the "Router A" console**

1. Ping all interfaces before beginning.
2. To remove the EIGRP routing protocol and turn on the IGRP routing protocol issue the following commands:

- router-a(config)#**no router eigrp 44**
- router-a(config)#**router igrp 44**
- router-a(config-router)#**network 206.202.16.0**
- router-a(config-router)#**^Z**

**From the "Router B" console**

3. Issue the following commands:

- router-b(config)#**router eigrp 44**
- router-b(config-router)#**no network 206.202.16.0**
- router-b(config)#**router igrp 44**
- router-b(config-router)#**network 206.202.16.0**
- router-b(config-router)#**^Z**

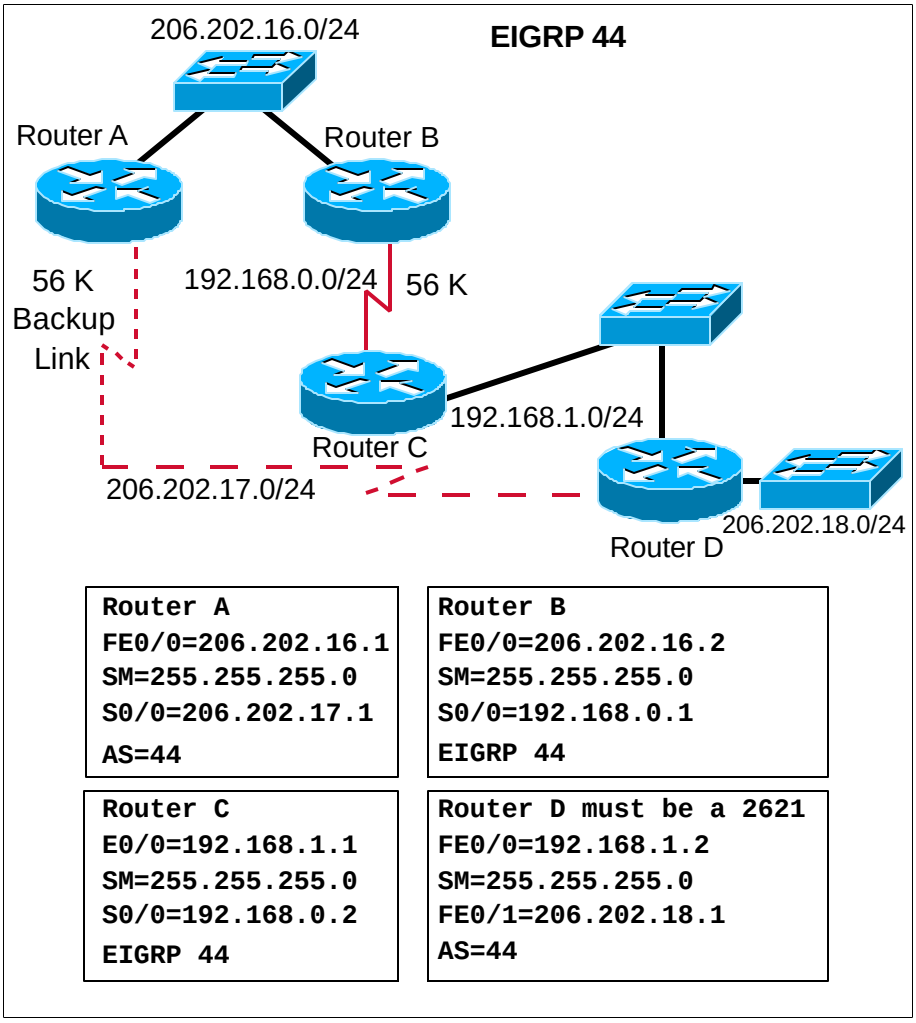
4. Write the running-configurations of all the routers to memory, and reboot all the routers.

**From the "Router C" console**

5. Enter enable exec mode and enter **show ip route** and **show ip eigrp traffic**. Report your findings below:

_____

## Lab 6.2.2 EIGRP and Backup Routes




**Objective:**

Enable EIGRP routing protocol with backup routes.

(Note: Erase "Router A" and "Router B" before beginning)

**Scenario:**

The Lubbock ISP has purchased more RAM for their core routers. They want you to setup EIGRP on their two core routers and configure a backup link. Tasks:

From the "Router A" console

1. Cable the lab as shown above.

2. Issue the following commands:

- router-a(config)#**interface fastethernet 0/0**
- router-a(config-if)#**ip address 206.202.16.1 255.255.255.0**
- router-a(config-if)#**no shutdown**
- router-a(config-if)#**interface serial 0/0**
- router-a(config-if)#**ip address 206.202.17.1 255.255.255.0**
- router-a(config-if)#**clockrate 56000**
- router-a(config)#**router eigrp 44**
- router-a(config-router)#**network 206.202.16.0**
- router-a(config-router)#**network 206.202.17.0**
- router-a(config-router)#**^Z**

From the "Router B" console

3. Issue the following commands:

- router-b(config)#**interface fastethernet 0/0**
- router-b(config-if)#**ip address 206.202.16.2 255.255.255.0**
- router-b(config-if)#**no shutdown**
- router-b(config)#**interface serial 0/0**
- router-b(config-if)#**ip address 192.168.0.1 255.255.255.0**
- router-b(config-if)#**clockrate 56000**
- router-b(config-if)#**no shutdown**
- router-b(config)#**router eigrp 44**
- router-b(config-router)#**network 206.202.16.0**
- router-b(config-router)#**network 192.168.0.0**
- router-b(config-router)#**^Z**

From the "Router D" console

4. Issue the following commands:

- router-d(config)#**interface fastethernet 0/1**
- router-d(config-if)#**ip address 206.202.18.1 255.255.255.0**
- router-d(config-if)#**no shutdown**
- router-d(config-if)#**interface serial 0/0**
- router-d(config-if)#**ip address 206.202.17.2 255.255.255.0**
- router-d(config)#**router eigrp 44**
- router-d(config-router)#**network 206.202.18.0**
- router-d(config-router)#**network 206.202.17.0**
- router-d(config-router)#**^Z**

From the "Router B" console

5. Enter **`show ip eigrp neighbors`** and **`show ip eigrp topology all-links`**

   Are there any successors for the 206.202.17.0 network ?

---

6. Enter **`show ip eigrp interfaces`**

   How many interfaces?

---

7. Enter **`show ip route`** command and list the routes below:

---

---

---

8. Enter **`trace 206.202.18.1`** and list below your findings:

---

---

---

9. Issue the following commands on "Router B":

- router-b(config)#**`interface serial 0/0`**
- router-b(config-if)#**`bandwidth 56`**
- router-b(config-if)#**`^Z`**

10. Enter **`show ip route`** command and list the routes below:

---

11. Enter **`trace 206.202.18.1`** and list below your findings:

---

12. Enter **`show ip eigrp topology 206.202.18.0`** and list below your findings:

---

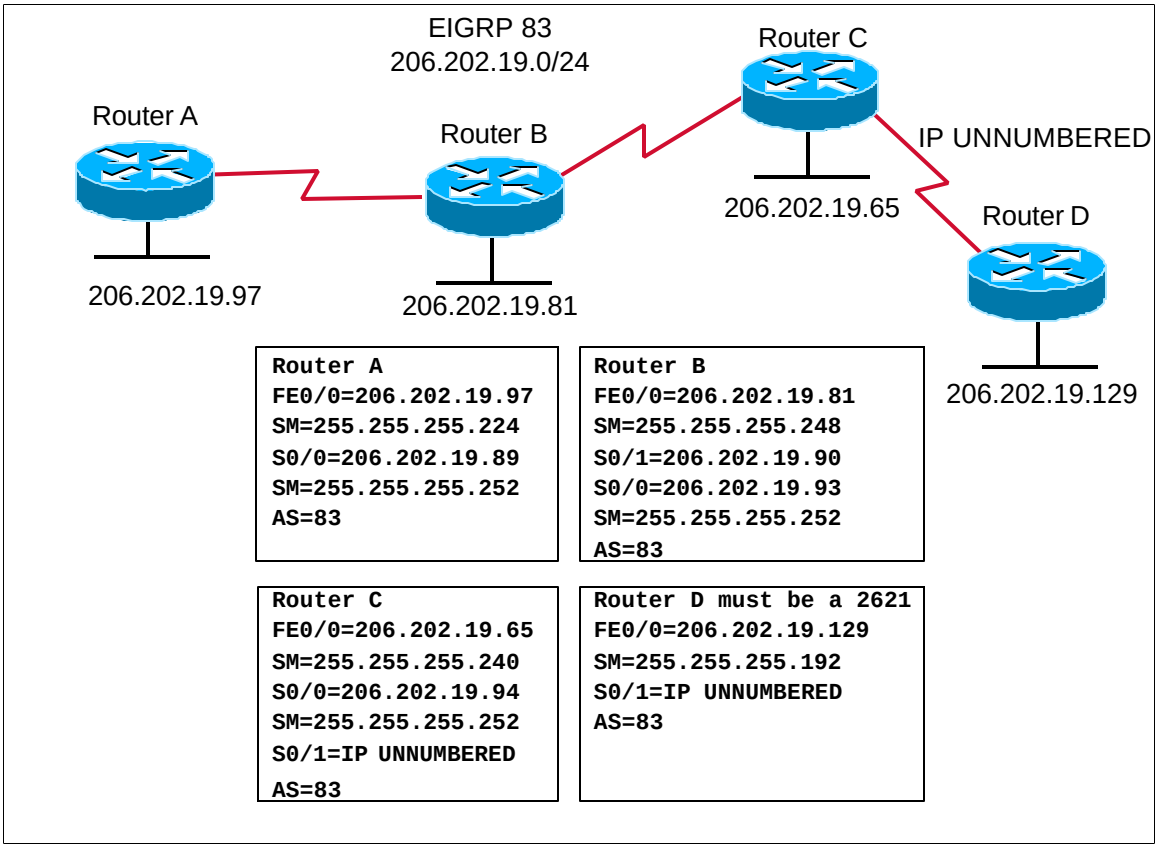
13. Issue the command **`debug eigrp fsm`** and then remove the FastEthernet cable from the FastEthernet 0/0 interface on "Router A"

---

14. Enter **`ping 206.202.18.1`** and **`show ip route`**. List your findings below:

---

## Lab 6.5.4 EIGRP VLSM




**Objective:**

Use VLSM and IP unnumbered with the EIGRP routing protocol.

**Scenario:**

You have been hired by a small school system in York, AL. You are to maximize a full Class C address using IP unnumbered and VLSM. You only have one Class C for this network setup.

From the "Router A" console

1. Cable the lab as shown above and erase all routers.
2. To configure the interfaces and turn on the EIGRP routing protocol issue the following commands:

- router-a(config)#**interface fastethernet 0/0**
- router-a(config-if)#**ip address 206.202.19.97 255.255.255.224**
- router-a(config-if)#**no shutdown**
- router-a(config-if)#**interface serial 0/0**
- router-a(config-if)#**ip address 206.202.19.89 255.255.255.252**
- router-a(config-if)#**no shutdown**

- router-a(config-if)#**router eigrp 83**
- router-a(config-router)#**network 206.202.19.0**
- router-a(config-router)#**no auto-summary**
- router-a(config-router)#**^Z**

From the "Router B" console

3. Issue the following commands:

- router-b(config)#**interface fastethernet 0/0**
- router-b(config-if)#**ip address 206.202.19.81 255.255.255.248**
- router-b(config-if)#**no shutdown**
- router-b(config-if)#**interface serial 0/0**
- router-b(config-if)#**ip address 206.202.19.93 255.255.255.252**
- router-b(config-if)#**clockrate 56000 router-b(config-if)#no shutdown**
- router-b(config-if)#**interface serial 0/1**
- router-b(config-if)#**ip address 206.202.19.90 255.255.255.252**
- router-b(config-if)#**router eigrp 83**
- router-b(config-router)#**network 206.202.19.0**
- router-b(config-router)#**no auto-summary**
- router-b(config-router)#**^Z**

4. Follow the same procedure with different addresses on the other two routers

From the "Router D" console

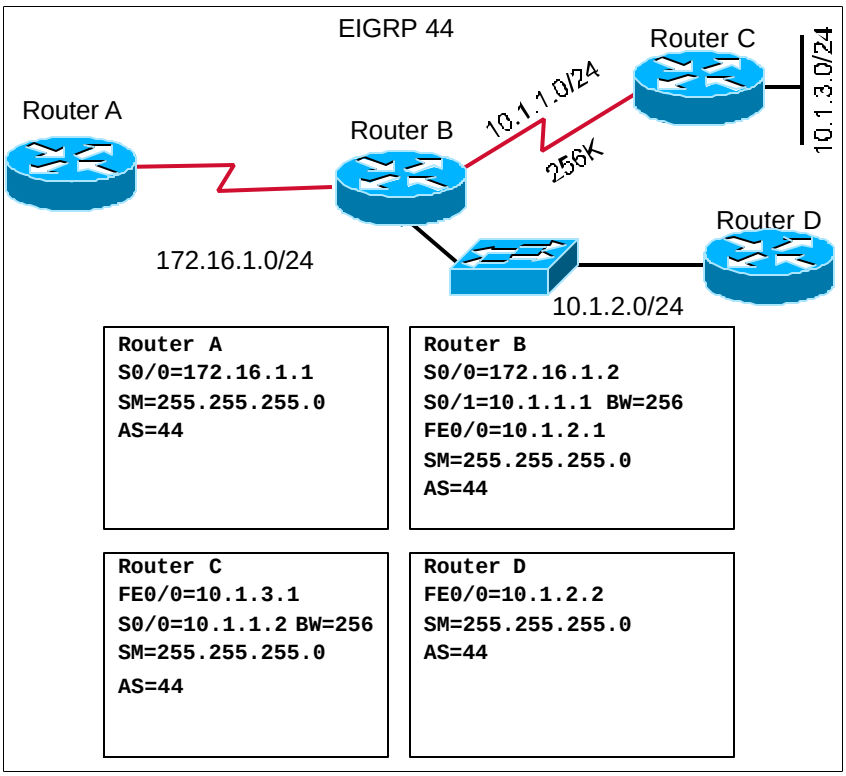
5. Enter **show ip eigrp topology 206.202.19.0** and **show ip route**. Report you findings below:

---

6. Calculate the number of hosts on each subnet by only using the routing table

---

## Lab 6.7.1 EIGRP Summarization




**Objective:**

Discover Auto-Summarization by the EIGRP routing protocol.

**Scenario:**

You have been called by the Goodwill Industries to setup a WAN for the distribution of recycled goods. You must setup EIGRP but you are to be careful of the Auto-summary feature.

**Tasks:**

From the "Router A" console

1. Cable the lab as shown above and erase all routers.
2. To configure the interfaces and turn on the EIGRP routing protocol issue the following commands:

- router-a(config)#**interface serial 0/0**
- router-a(config-if)#**ip address 172.16.1.1 255.255.255.0**
- router-a(config-if)#**no shutdown**
- router-a(config-if)#**router eigrp 44**
- router-a(config-router)#**network 172.16.1.0**
- router-a(config-router)#**^Z**

From the "Router B" console

3. Issue the following commands:

- router-b(config)#**interface fastethernet 0/0**
- router-b(config-if)#**ip address 10.1.2.1 255.255.255.0**
- router-b(config-if)#**no shutdown**
- router-b(config-if)#**interface serial 0/0**
- router-b(config-if)#**ip address 172.16.1.2 255.255.255.0**
- router-b(config-if)#**clockrate 56000**
- router-b(config-if)#**no shutdown**
- router-b(config-if)#**interface serial 0/1**
- router-b(config-if)#**ip address 10.1.1.1 255.255.255.0**
- router-b(config-if)#**bandwidth 256**
- router-b(config-if)#**router eigrp 44**
- router-b(config-router)#**network 10.1.2.0**
- router-b(config-router)#**network 172.16.1.0**
- router-b(config-router)#**network 10.1.1.0**
- router-b(config-router)#**^Z**

4. Follow the same procedure with different addresses on the other two routers

From the "Router A" console

5. Enter **show ip eigrp topology 10.0.0.0** and report your findings below:

---

From the "Router B" console

6. Enter **show ip route 10.0.0.0** and report your findings below:

---

7. Enter **show ip eigrp topology 10.0.0.0**

   What is null0 ?

---

8. Turn off the auto-summary feature of EIGRP by issuing the following commands:

- router-b(config)#**router eigrp 44**
- router-b(config-router)#**no auto-summary**
- router-b(config-router)#**^Z**

9. Enter **`show ip eigrp topology`** and report your findings below:

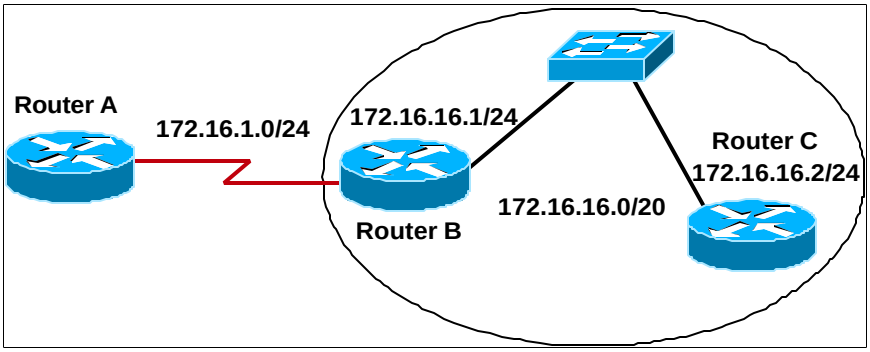
---

From the "Router A" console

10. Enter the commands **`show ip eigrp topology 10.0.0.0`** and **`show ip route`**. Report your findings below:

---

# Lab 6.7.2 EIGRP Interface Summarization




**Objectives:**

- To reduce the number of routes in the EIGRP routing table through interface summarization.

**Complete the following steps:**

1. Setup the lab as shown in the diagram.
2. Assign IP addresses to each interface. Copy and paste the 14 loopback interfaces on Router C.
3. Enable EIGRP as the routing protocol on all routers.
4. Advertise network 172.16.0.0 on all routers with AS 100

   Verify your configurations are as follows:

   Router A's configuration is:

```
hostname router-a
interface Serial0
ip address 172.16.1.1 255.255.255.0
clockrate 56000
router eigrp 100
network 172.16.0.0
```

   Router B's configuration is:

```
hostname router-b
interface FastEthernet0/0
ip address 172.16.16.1 255.255.255.0
interface Serial0/0
ip address 172.16.1.2 255.255.255.0
router eigrp 100
network 172.16.0.0
```

Router C's configuration is:

```
hostname router-c
interface Loopback0
ip address 172.16.17.1 255.255.255.0
interface Loopback1
ip address 172.16.18.1 255.255.255.0
interface Loopback2
ip address 172.16.19.1 255.255.255.0
interface Loopback3
ip address 172.16.20.1 255.255.255.0
interface Loopback4
ip address 172.16.21.1 255.255.255.0
interface Loopback5
ip address 172.16.22.1 255.255.255.0
interface Loopback6
ip address 172.16.23.1 255.255.255.0
interface Loopback7
ip address 172.16.24.1 255.255.255.0
interface Loopback8
ip address 172.16.25.1 255.255.255.0
interface Loopback9
ip address 172.16.26.1 255.255.255.0
interface Loopback10
ip address 172.16.27.1 255.255.255.0
interface Loopback11
ip address 172.16.28.1 255.255.255.0
interface Loopback12
ip address 172.16.29.1 255.255.255.0
interface Loopback13
ip address 172.16.30.1 255.255.255.0
interface Loopback14
ip address 172.16.31.1 255.255.255.0
interface FastEthernet0/0
ip address 172.16.16.2 255.255.255.0
router eigrp 100
network 172.16.0.0
```

5. Issues the command **`show ip route`** from all routers in the EIGRP network. Record your findings below:

_____

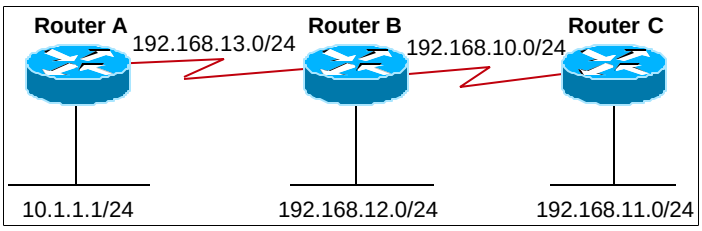
6. To reduce the number of routes on Router A. Go to Router B and issue the following command:

```
Router-b(config)#interface serial 0/0
Router-b(config-if)# ip summary-address eigrp 100 172.16.16.0
255.255.240.0
Router-b(config-if)#control Z
```

7. Issues the command **`show ip route`** from all routers in the EIGRP network. Record your findings below:

_____

## Lab 7.1.3 Distribute List




**Objectives:**

- Use a distribute list to filter routes.

**Scenario:**

Router B learns about the 10.0.0.0 via EIGRP and advertises it the rest of the autonomous system. You want to stop the updates from the 10.0.0.0 network from being propagated beyond Router B.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram. Don't forget the no shutdown command.
2. Configure EIGRP routing on all the routers.

```
Router-a(config)#router eigrp 192
Router-a(config-router)#network 192.168.13.0
Router-a(config-router)#network 10.0.0.0

Router-b(config)#router eigrp 192
Router-b(config-router)#network 192.168.10.0
Router-b(config-router)#network 192.168.12.0
Router-b(config-router)#network 192.168.13.0

Router-c(config)#router eigrp 192
Router-c(config-router)#network 192.168.10.0
Router-c(config-router)# network 192.168.11.0
```

Verify that EIGRP is configured correctly and all routes are seen.

3. Verify that EIGRP is configured correctly and all routes are seen.
4. Configure Router B with the following commands to create a distribute-list.

```
Router-b(config)#access-list 1 deny 10.0.0.0
Router-b(config)#access-list 1 permit any
Router-b(config)#router eigrp 192
Router-b(config-router)#distribute-list 1 out
serial0/0
```

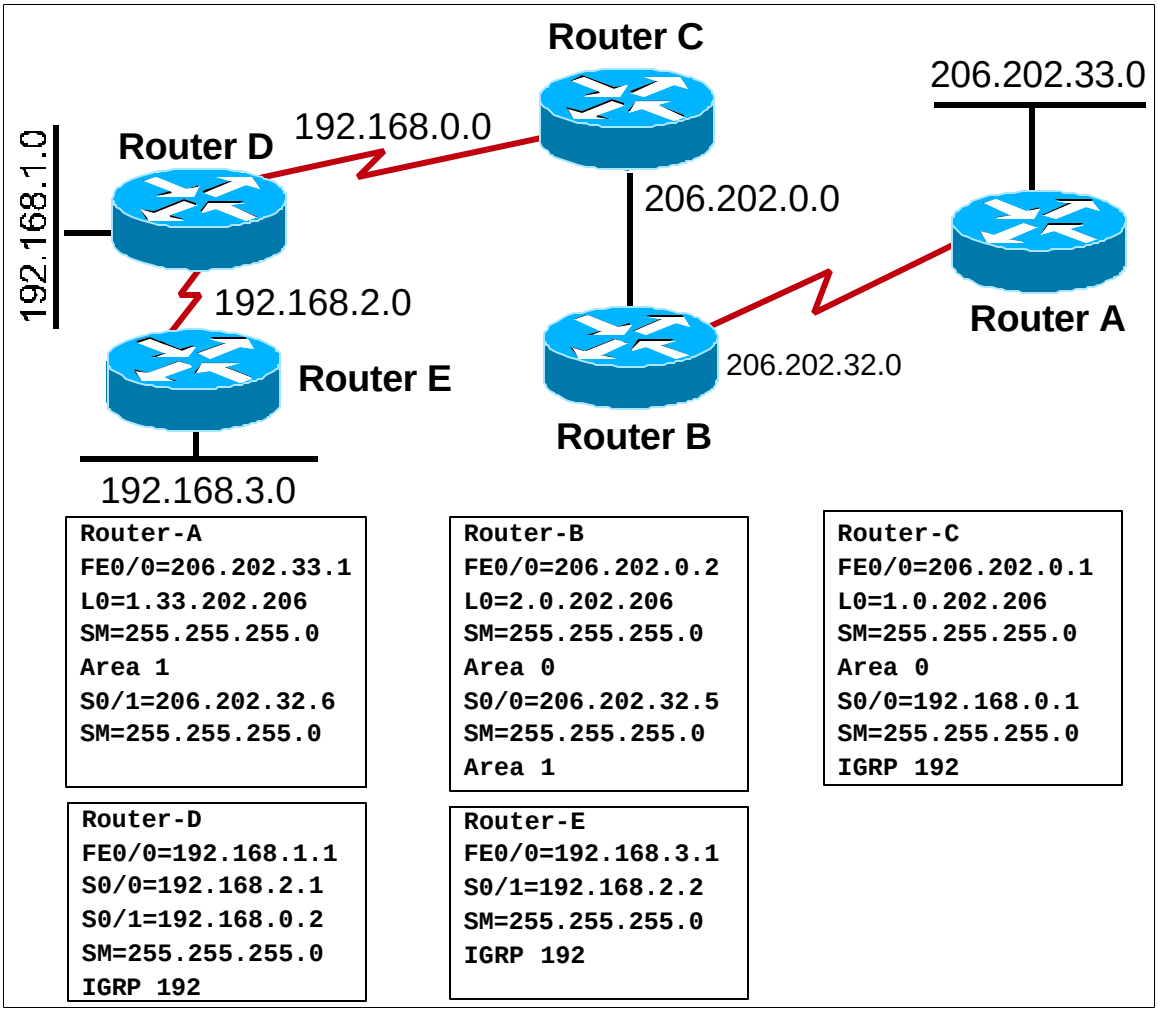
5. Issue the command **`show ip route`** on Router C to see if the 10.0.0.0 route is listed. EIGRP is very fast Issue the command **`show ip route`** on Routers A and B to see if there are any changes?
6. Configure Router C with a static route to the 10.0.0.0 network for network services with a routing protocol.

```
Router-c(config)#ip route 10.0.0.0 255.0.0.0
192.168.10.1
```

7. Issue the command **`show ip route`** on Router C to see if the static route is listed.
8. Issue the commands **`ping 10.1.1.1`** and **`trace 10.1.1.1`** from Router C. Record your results below.

_____

## Lab 7.2.1 Passive-interface and static route




**Objective:**

Configure OSPF with a passive-interface, static route and a default route.

**Scenario:**

You are having some problems on you WAN. Several of the routers do not have enough memory to utilize OSPF. You must setup static and default routes to maintain connectivity.

From the "Router B" console

1. Enter **`show ip route`**

Which router is advertising the route to 206.202.33.0/24 ?

_____

2. Enter **`show ip ospf neighbor`** and list below your findings:

3. Enter ping **206.202.33.1**

Is the ping successful?

---

4. To configure the passive-interface issue the following commands:

- router-b(config)#**`router ospf 1`**
- router-b(config-router)#**`passive-interface serial 0/0`**
- router-b(config-router)#**`Control Z`**

5. Enter **`clear ip route *`** and wait 30 seconds and then ping 206.202.33.1

Is the ping successful?

---

6. Enter **`show ip route`**

Is the route to 206.202.33.0/24 still listed in the routing table?

---

7. Enter **`show ip ospf neighbor`**

What happened to one of our OSPF neighbors?

---

---

From the "Router A" console

8. Enter **`show ip route`**

List below the routes that are available.

---

---

From the "Router B" console

9. Issue the following commands to setup a static route to the network:

- router-b(config)#**ip route 206.202.33.0 255.255.255.0 206.202.32.6**
- router-b(config)#**Control Z**

10. Enter **show ip route**

What is the administrative distance to 206.202.33.0/24? Why?

---

11. Enter **ping 206.202.33.1**

Is the ping successful?

---

From the "Router A" console

12. Enter **show ip route**

List below the routes that are available.

---

Is there a gateway of last resort?

---

13. Issue the following commands to setup a static default route to the network:

- router-a(config)#**ip route 0.0.0.0 0.0.0.0 206.202.32.5**
- router-a(config)#**Control Z**

14. Is there a gateway of last resort?

---

15. Enter **ping 206.202.0.2**

Is the ping successful?

---

From the "Router C&D" consoles

16. Enter **`show ip route`**

Is there a route for 206.202.33.0 on both routers? Why?

---

---

From the "Router B" console

- router-b(config)#**`router ospf 1`**
- router-b(config-router)#**`redistribute static`**
- router-b(config)#**`Control Z`**

From the "Router C&D" consoles

17. Enter **`show ip route`**

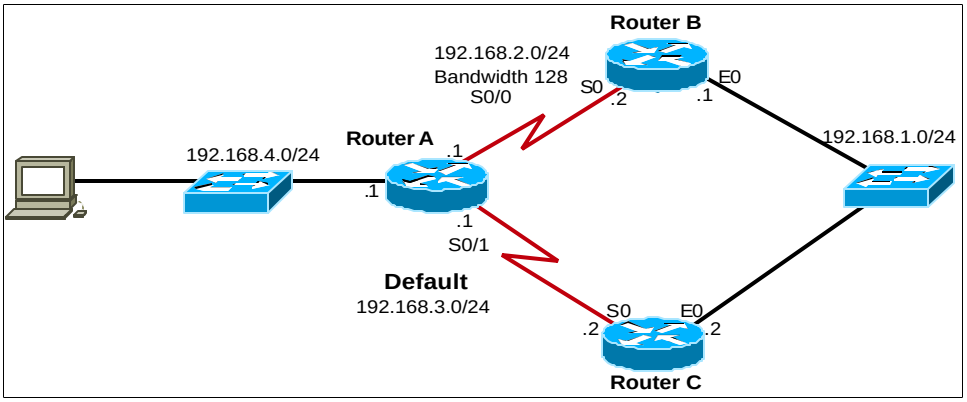
Is there a route for 206.202.33.0 ?

---

What is E2?

---

# Lab 7.3.5 Simple Route Map




**Objectives:**

- Configure a simple route-map to control traffic flow.

**Scenario:**

Based on your current configuration, all traffic destined for network 192.168.1.0 originating from 192.168.4.0 will travel via 192.168.3.0. Your task is to configure a route-map that will send all traffic destined for 192.168.1.0 via 192.168.2.0.

**Initial Configuration:**

Configure the above network as shown in the diagram above. Use OSPF as your routing protocol. Also, on interface S 0/0, issue the command bandwidth 128. This will make the link between Routers A and B appear to be slower than the link between Routers A and C, forcing OSPF to choose the link between A and C as the optimum path to 192.168.1.0. Verify all links are operational and use the trace command to verify traffic from 192.168.4.0 destined for 192.168.1.0 is using the link between Routers A and C. Now you can begin the actual lab!

**Configuring the Route map:**

1. Traffic will be entering Router A via Ethernet 0. So we must activate a route map on that interface. In this lab we will name the route map CHANGEROUTE. To enable the route map on an interface, issue the command:

   ```
   RouterA(config-if)# ip policy route-map CHANGEROUTE
   ```

2. Next we will need an access list statement in order to identify the packets that need to be policy routed. In this case, it will be packets from 192.168.4.0. This can be taken care of with a standard access list statement:

   ```
   RouterA(config)#access-list 1 permit 192.168.4.0 0.0.0.255
   ```

3. It is now time to configure the actual route map. The first step is to configure an instance of the route map. The second step is to identify the packets that need to be route mapped. The third step to tell the router where to send the packet. Use the following commands:

```
RouterA(config)# route-map CHANGEROUTE permit 10
RouterA(config-route-map)# match ip address 1
RouterA(config-route-map)# set interface serial 0/0
```

4. Verify that the route map is functioning. To view the process, issue the debug ip policy command and then ping from the workstation on 192.168.4.0.

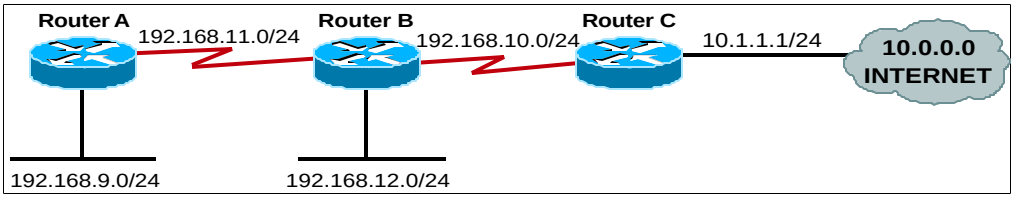
   What are the results of the debug ip policy command?

   _____

   What other command could you use to verify the route map is working and your packets are traveling over the desired link?

   _____

# Lab 7.4.1 RIP Default Route




**Objectives:**

- Use a default route with RIP to setup a gateway of last resort on all RIP routers.

**Scenario:**

You have a RIP routing domain with only one outside link. You want all routers to send packets to that gateway, if there is not an explicit route listed in the routing table. You must not advertise networks that are not part of your routing domain back into your RIP network.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram. Configure a host with ip address 10.1.1.2.

2. Configure RIP routing on all routers.

```
Router-a(config)#router rip
Router-a(config-router)#network 192.168.11.0
Router-a(config-router)#network 192.168.9.0

Router-b(config)#router rip
Router-b(config-router)#network 192.168.10.0
Router-b(config-router)#network 192.168.11.0
Router-b(config-router)#network 192.168.12.0

Router-c(config)#router rip
Router-c(config-router)#network 192.168.10.0
Router-c (config-router) #default-information originate
```

3. Verify that RIP is configured correctly and all routes are listed in the routing table. On Router C the 10.0.0.0 network should be directly connected, but not listed in the routing table of the other routers.

4. Is there a gateway of last resort set in the routing tables of all the routers? Try to ping and trace to 10.1.1.1 and 10.1.1.2 from Router A and Router B. Does it work? Record your answers below.

_____

5. Configure Router C with a default static route.
   `Router-c(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0`

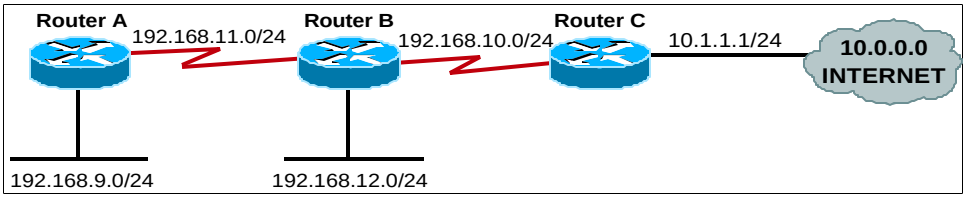
6. Issue the command **`show ip route`** on all routers to see if the default static route is listed. Is there a gateway of last resort listed in the routing table of every router?

7. Issue the commands **ping and trace 10.1.1.1 and 10.1.1.2** from all routers. Record your results below.

_____

_____

## Lab 7.4.3 IGRP Default Network




**Objectives:**

- Use a default network with IGRP to setup a gateway of last resort on all IGRP routers.

**Scenario:**

You have an IGRP routing domain with only one outside link. You want all routers to send packets to that gateway, if there is not an explicit route listed in the routing table.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram.

2. Configure IGRP routing on all routers.

```
Router-a(config)#router IGRP 109
Router-a(config-router)#network 192.168.11.0
Router-a(config-router)#network 192.168.9.0

Router-b(config)#router IGRP 109
Router-b(config-router)#network 192.168.10.0
Router-b(config-router)#network 192.168.11.0
Router-b(config-router)#network 192.168.12.0

Router-c(config)#router IGRP 109
Router-c(config-router)#network 192.168.10.0
```

3. Verify that IGRP is configured correctly and all routes are listed in the routing table. On Router C the 10.0.0.0 network should be directly connected, but not listed in the routing table of the other routers.

4. Is there a gateway of last resort set in the routing tables of all the routers? Try to ping and trace to 10.1.1.1 and 10.1.1.2 from Router A and Router B. Does it work? Record your answers below.

_____

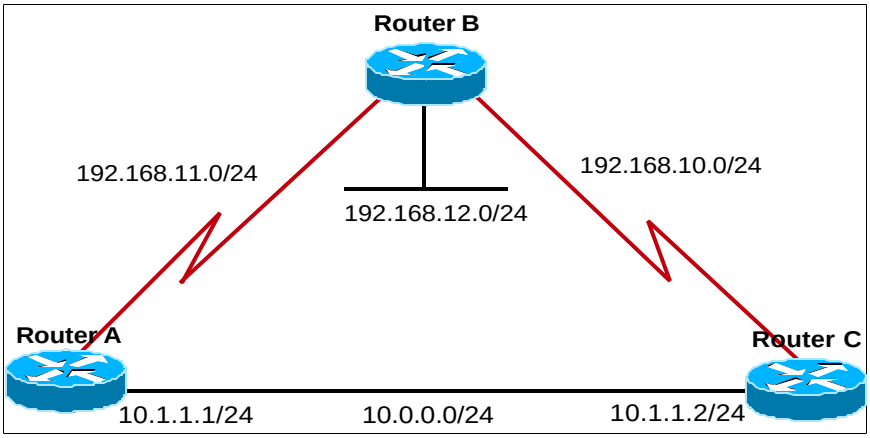
5. Configure Router C to advertise a gateway of last resort.

```
Router-c(config)#ip route 10.0.0.0 255.0.0.0 10.1.1.254 Router-
c(config)#ip default-network 10.0.0.0 Router-c(config)#router
igrp 109 Router-c(config-router)#redistribute static
```

6. Issue the command show ip route on all routers to see if the candidate default route is listed. Is there a gateway of last resort listed in the routing table of every router?

_____

## Lab 7.4.5 Floating Static Route




**Objectives:**

- Use a floating static route to setup a backup route that will only appear in the routing table when the link advertised by the routing protocol fails.

**Scenario:**

Router B learns about the 10.0.0.0 via RIP with the next hop being 192.168.10.2. Router B also has an unadvertised link to 10.0.0.0 via Router A. The link between Router B and Router A is a high cost link that is not to be used unless the link between Router B and Router C goes down.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram. Don't forget the no shutdown command.

2. Configure RIP routing on routers B and C.

```
Router-b(config)#router rip
Router-b(config-router)#network 192.168.10.0
Router-b(config-router)#network 192.168.11.0
Router-b(config-router)#network 192.168.12.0

Router-c(config)#router rip
Router-c(config-router)#network 192.168.10.0
Router-c(config-router)#network 10.0.0.0
```

3. Configure RIP routing as follows on Router A.

```
Router-a(config)#router rip
Router-a(config-router)#network 192.168.11.0
```

4. Verify that RIP is configured correctly and all routes are seen. On Router A the 10.0.0.0 network should be directly connected but from Router B it should be advertised from Router C only.

5. Configure Router B with a floating static route.

```
Router-b(config)#ip route 0.0.0.0 0.0.0.0
192.168.11.2 130
```

6. Issue the command **`show ip route`** on all routers to see if the static route is listed.

7. Issue the commands **`ping`** 10.1.1.1 and **`trace`** 10.1.1.1 from all routers. Record your results below

_____

8. Shutdown the link between Router-B and Router-C.

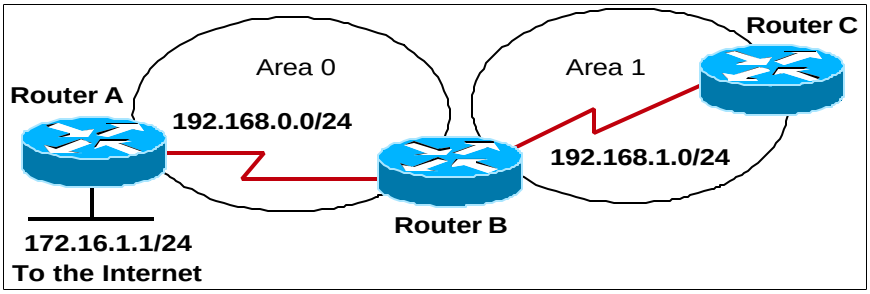
9. Issue the command **`show ip route`** on all routers to see if the static route is listed.

10. Issue the commands **`ping`** 10.1.1.1 and **`trace`** 10.1.1.1 from all routers. Record your results below.

_____

_____

## Lab 7.4.6 OSPF Default Information




**Objectives:**

- To inject a static default route into the entire OSPF routing domain.

**Note:**

This is one of the most powerful commands in OSPF routing. It informs all the routers in OSPF of an exterior default route.

**Complete the following steps:**

1. Setup the lab as shown in the diagram.
2. Assign IP addresses to each interface.
3. Enable OSPF as the routing protocol.
4. Check to see if neighbor relationships exist between all routers

Verify your configurations are as follows:

RTA's configuration is:

```
hostname router-a
Loopback0
ip address 1.1.16.172 255.255.255.0
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
interface Serial0/0
ip address 192.168.0.1 255.255.255.0
clockrate 56000
router ospf 1
network 192.168.0.0 0.0.0.255 area 0
```

```
RTB's configuration is:
```

```
hostname router-b
interface Loopback0
ip address 2.0.168.192 255.255.255.0
interface Serial0/0
ip address 192.168.1.1 255.255.255.0
interface serial 0/1
ip address 192.168.0.2 255.255.255.0
clockrate 56000
router ospf 1
```

```
network 192.168.0.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 1
RTC's configuration is:

hostname router-c
interface Loopback0
ip address 2.1.168.192 255.255.255.0
interface Serial0/1
ip address 192.168.1.2 255.255.255.0
router ospf 1
network 192.168.1.0 0.0.0.255 area 1
```

5. Go to each router and issue the command **`show ip route`**. Is there a gateway of last resort?

   _____

   On Router C:
   `Ping 172.16.1.1` and record your results below:

   _____

6. On Router A:

   Issue the following commands:

```
router-a(config)#ip route 0.0.0.0 0.0.0.0 fe0/0
router-a(config)#router ospf 1
router-a(config-router)#default-information originate
router-a(config-router)#control Z
```

7. Go to each router and issue the command **`show ip route`**.
   Is there a gateway of last resort?

   _____

   On Router C:

   `Ping 172.16.1.1` and record your results below:
   `Trace 195.6.0.1` and record your result below:

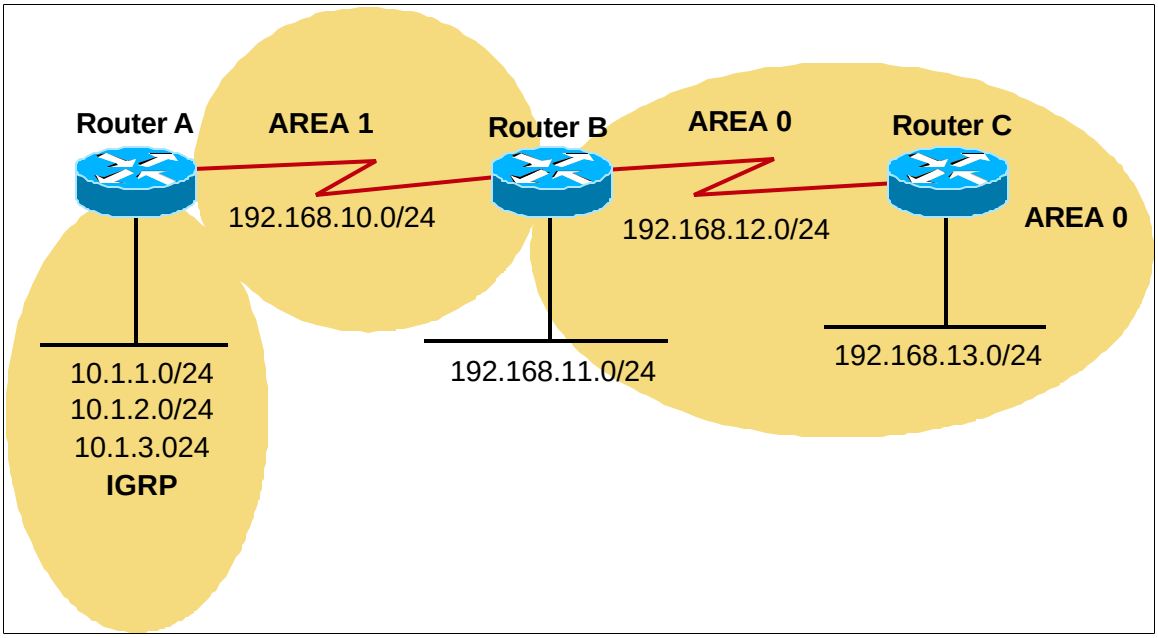
   _____

   _____

Note:

The exterior provider will setup and advertise a route back to your OPSF network. This will allow packets back into your network

## Lab 7.5.10 OSPF/IGRP Mutual Redistribution




**Objectives:**

- Setup mutual route redistribution between OSPF and IGRP.

**Scenario:**

You have an IGRP routing domain that has been added to your OSPF. You need to advertise the IGRP routes into your OSPF network and vice versa.

**Lab Task:**

1. Cable the lab and all interfaces as shown in the diagram. You will use loopbacks for the IGRP networks.

2. Configure OSPF routing on all routers.

```
Router-a(config)#interface loopback 1
Router-a(config-if)#ip address 10.1.1.1 255.255.255.0
Router-a(config-if)#interface loopback 2
Router-a(config-if)#ip address 10.1.2.1 255.255.255.0
Router-a(config-if)#interface loopback 3
Router-a(config-if)#ip address 10.1.3.1 255.255.255.0
Router-a(config-if)#router ospf 1
Router-a(config-router)#network 192.168.8.0 0.0.3.255 area 1
Router-a(config-router)#router igrp 10
Router-a(config-router)#network 10.0.0.0
```

```
Router-b(config)#router ospf 1
Router-b(config-router)# network 192.168.12.0 0.0.3.255 area 0
Router-b(config-router)# network 192.168.8.0 0.0.3.255 area 1


Router-c(config)router ospf 1
Router-c(config-router)#network 192.168.12.0 0.0.3.255 area 0
```

3. Verify that OSPF is configured correctly and all OSPF routes are listed in the routing table. On Router A the 10.1.1.0-10.1.3.0 networks should be directly connected, but not listed in the routing table of the other routers.

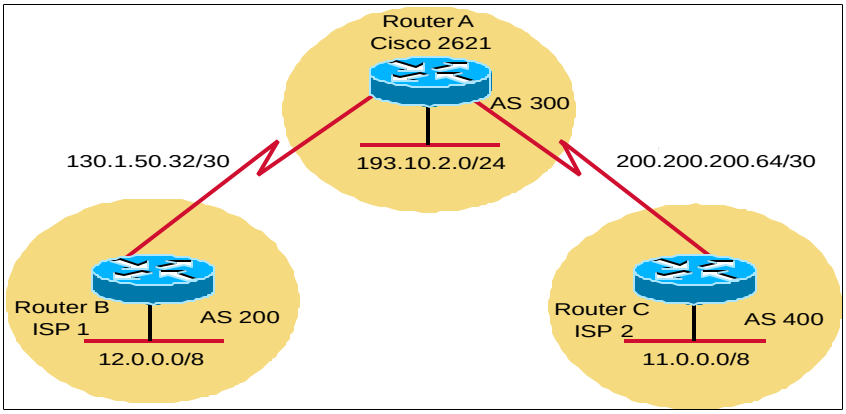
4. On Router A add the following commands to setup mutual redistribution between IGRP and OSPF:

```
Router-a(config)router ospf 1
Router-a(config-router)#redistribute igrp 10 metric 12 metric-
type 1 subnets
Router-a(config-router)#router igrp 10
Router-a(config-router)#redistribute ospf 1 metric 56 100 255 10
1500
Router-a(config-router)#default-metric 56 100 255 10 1500
```

5. Issue the command show ip route from Router A and Router B. Record your results below.

_____

# Lab 8.4.3 Configure BGP Connectivity between 2 Autonomous Systems




**Objective:**

The student should be able to configure external BGP between multiple Autonomous Systems.

**Task:**

Router A is your corporate router. You are responsible for configuring the ISP routers as well as your corporate router and ensuring that users on the corporate network can see the Internet. For lab purposes, the Internet will be the Ethernet interfaces on each of the ISP routers.

**Situation:**

Your company is now dependent on e-commerce and has decided to have two connections to the Internet going to 2 different ISPs. Your ISP has informed you that you have to run BGP to make this work. The ISP has asked that you remove your static route to them, and configure a BGP route in order to ensure that everything is operation okay before you add the second ISP to the equation.

ISP #1 has an AS number of 200 while ISP #2 has an AS number of 400.

Addressing:

```
Router A: S0: 200.200.200.65/30
S1: 130.1.50.33/30
E0: 193.10.2.1/24

Router B: S0: 130.1.50.34/30
E0: 12.0.0.1/8

Router C: S1: 200.200.200.66/30
E0: 11.0.0.1/8
```

**Overview of approach:**

1. Implement the IP addressing scheme as shown in the diagram.
2. Enable BGP routing with AS number and assign neighbor relationship with ISP #1.
3. Configure router B in ISP #1.
4. Verify operation.
5. Repeat sequence for ISP #2.
6. Verify operation.

**Steps:**

1. configure all interfaces on all routers with the appropriate IP address and subnet mask. Don't forget to issue the **`no shutdown`** command as well!
2. Go to Router A. Issue the show ip route command. Are there any routes in the routing table? If so, which ones?

---

3. We are now going to configure BGP on the corporate router. This is Router A. · To turn on BGP routing, enter global configuration mode and issue the following command: **`routerA(config)# router bgp 300`**
4. Verify that you can ping the IP address of the serial interface on Router B of ISP#1 from Router A.

   Could you successfully ping the interface?

---

5. The next step is to define BGP neighbors. To do this, return to the following mode and type the command below.

```
RouterA(config-router)# neighbor
130.1.50.34 remote-as 200
```

6. Next step is to configure the locally attached networks that should be advertised from AS#300. To do this, issue the following command:

```
RouterA(config-router)#network
193.10.2.0
```

7. Return to privileged mode and save your configuration.

   **CONFIGURE BGP ROUTING on ISP 1**

8. Enable BGP routing on Router B in ISP 1. To do this, issue the command:

```
RouterB(config)# router bgp 200
```

9. Next step is to define the neighbor router(s) to ISP 1. Use the neighbor command like before.

```
RouterB(config-router)# neighbor
130.1.50.33 remote-as 300
```

10. Final step for this half of the configuration is to define networks local to AS 200. Issue the following command:

```
RouterB(config-router)#network
12.0.0.0
```

Return to privileged mode and save your configuration.

Verify the BGP connection is working.

11. Issue the **`show ip bgp neighbors`** command.

What is the BGP state?

---

How long has the connection been up for?

---

12. Issue the **`show ip bgp`** command.

Does network 193.10.2.0 show up in the table?

---

What is the path to 193.10.2.0?

---

What does the path number represent?

---

Configure the BGP connection between Router A and Router C (ISP 2).

13. Add additional neighbor information to Router A. Use the following command:

```
RouterA(config-router)#neighbor
200.200.200.66 remote-as 400
```

14. Enable BGP on Router C. Use the following commands:

```
RouterC(config)# router bgp 400
RouterC(config-router)#neighbor
200.200.200.65 remote-as 300
```

15. Indicate the networks that are found locally on AS 400. Use the following command:

```
RouterC(config-router)#network
11.0.0.0
```

Return to privileged mode and save your configuration.

16. It is now time to reset the neighbor connections, and build a new BGP table. To do this, issue the command:

```
RouterA# clear ip bgp *
```

**VERIFY THE CONFIGURATION**

17. From Router A, ping the Ethernet interfaces of Routers B and C.

- Was the ping successful?

---

18. Verify that BGP has a route to both Ethernet interfaces.

- What command should you use?

---

- Describe the results of this command:

---

19. Verify that the IP routing table has the routes you are trying to access.

- What command should you use?

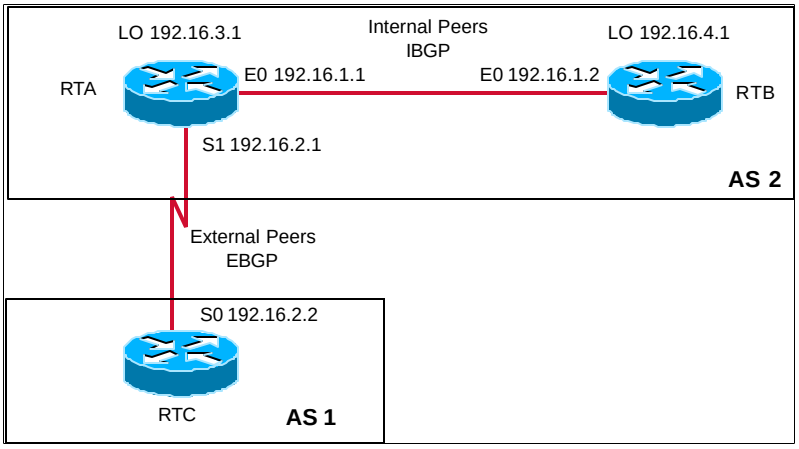
---

- Are the routes there?

---

20. Use the ping command from ISP 1 and ISP 2 to verify that each ISP can get to your network without having a static route configured.

# Lab 8.6.1.1 Building Peering Sessions: IBGP vs. EBGP




**Objective:**

To establish a basic BGP connection between routers and observe differences between internal and external BGP sessions.

Before focusing on the BGP portion of the lab, complete the following steps:

1. Setup the lab as shown in the diagram.
2. Assign IP addresses to each interface as shown in the diagram. The L0 address represents a loopback address. Make sure you set up these as well.
3. Enable OSPF as the routing protocol between Router A and Router B.
4. Advertise network 192.16.1.0 with a wildcard mask of 0.0.255.255.

Verify you configurations are as follows:

RTA's configuration is:

```
ip subnet-zero
interface Loopback0
ip address 192.16.3.1
255.255.255.0
interface Ethernet0
ip address 192.16.1.1
255.255.255.0
interface Serial1
ip address 192.16.2.1
255.255.255.0
router ospf 10
network 192.16.1.0 0.0.255.255
area 0
ip classless
```

RTB's configuration is:

```
ip subnet-zero
interface Loopback0
ip address 192.16.4.1
255.255.255.0
interface Ethernet1/1
ip address 192.16.1.2
255.255.255.0
router ospf 10
network 192.16.0.0 0.0.255.255
area 0
ip classless
```

RTC's configuration is:

```
ip subnet-zero
interface Serial1/1
ip address 192.16.2.2
255.255.255.0
ip classless
```

Now that we have the IGP set up, we can configure the BGP connections:

Begin with Router A:

1. Enter global configuration mode.
2. Enable BGP on router A for AS #2. To do this use the command:

   ```
   RTA(config)#router bgp 2 RTA(config-router)#
   ```

3. Since AS #2 is a small Autonomous system that is fully meshed and is not a transit AS, it is safe to turn off the synchronization feature of BGP. To do this issue the command:

   ```
   RTA(config-router)#no synchronization
   ```

4. Next we must define the BGP neighbor relationships. Router A has 2 BGP neighbors, namely Router B and C. To define these relationships issue the following commands:

   ```
   RTA(config-router)#neighbor 192.16.4.1 remote-
   as 2  **Note the loopback address**
   RTA(config-router)#neighbor 192.16.4.1 update-
   source Loopback 0
   RTA(config-router)#neighbor 192.16.2.2 remote-
   as 1
   ```

   Note the **`update-source Loopback 0`** statement. This command specifies the interface to be used as the source ip address of the BGP session with the neighbor.

5. Lastly, we are not going to summarize routes in this lab. So we will turn off the BGP automatic summarization at the major net boundary. To do this issue the following command:

   ```
   RTA(config-router)#no auto-summary
   ```

6. Save your configuration and move to Router B.

Configuring Router B:

1. Before enabling BGP on this router, issue the following command:

   ```
   RTB#debug ip bgp
   ```

   This command will allow you to see the negotiation between BGP neighbors.

2. Enable BGP on router B for AS #2.

   What command will you need to do this? (HINT: See step 1 from Router A)

   _____

   _____

3. Define the BGP neighbor relationships for router B.

   What command(s) should you use to do this?

   _____

   _____

4. Shut down your Ethernet interface and then bring it back up again. You should now see the neighbor negotiation process on your screen.

   List the steps of the negotiation process:

_____

_____

_____

_____

Issue the **`show ip bgp neighbor`** command.

What kind of BGP connection is this, internal or external?

_____

How do you know what kind it is?

_____

5. Save your configuration and move to router C.

Configuring Router C:

1. Enable bgp routing on Router C for AS #1.

   What command will you need to do this?

   _____

   _____

2. Define the BGP neighbor relationships for router C.

   What command will you use to do this?

   _____

   _____

3. Issue the **`show ip bgp neighbor`** command.

   What kind of BGP connection is this, internal or external?

_____

   How do you know what kind it is?

_____

4. Verify connectivity with the ping command.

   What addresses can you successfully ping?

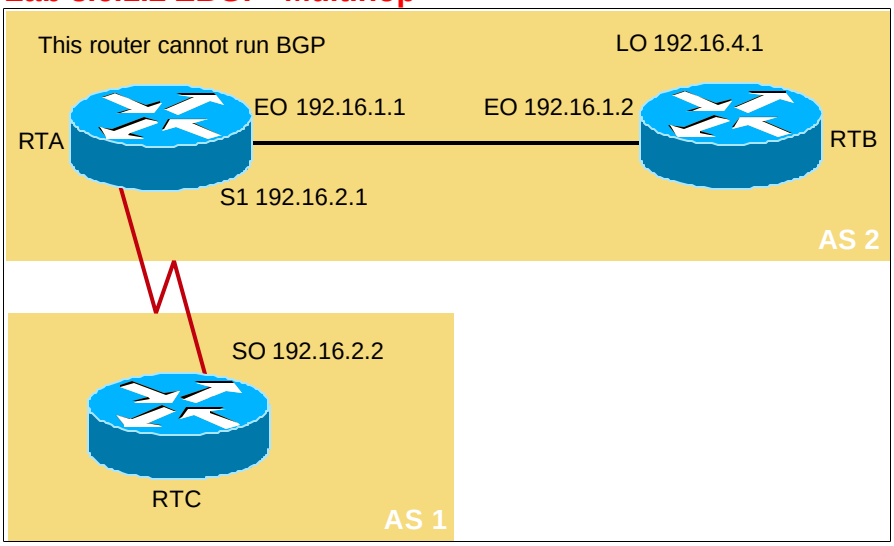
_____

What addresses can you not ping?

---

Save your configuration.

## Lab 8.6.1.2 EBGP- Multihop




**Objectives:**

- To establish a BGP connection between routers via a router that is not running BGP.

  Before focusing on the BGP portion of the lab, complete the following steps:

  1. Setup the lab as shown in the diagram.
  2. Assign IP addresses to each interface as shown in the diagram. The L0 address represents a loopback address. Make sure you set up these as well.
  3. Enable OSPF as the routing protocol between Router A and Router B.
  4. Advertise network 192.16.1.0 with a wildcard mask of 0.0.255.255.

  Verify your configurations are as follows:

RTA's configuration is:

```
ip subnet-zero
interface
Loopback0
ip address
192.16.3.1
255.255.255.0
interface
Ethernet0
ip address
192.16.2.1
255.255.255.0
router ospf 10
network 192.16.1.0
 0.0.255.255 area
0
ip classless
```

RTB's configuration is:

```
ip subnet-zero
interface
Loopback0
ip address
192.16.4.1
255.255.255.0
interface
Ethernet1/1
ip address
192.16.1.2
255.255.255.0
ip route
192.16.1.0
255.255.255.0
192.16.2.1
ip classless
```

RTC's configuration is:

```
ip subnet-zero
interface Serial1/1
ip address
192.16.2.2
255.255.255.0

ip route
192.16.1.0
255.255.255.0
192.16.2.1
ip classless
```

The task to be completed in this lab is to configure a BGP connection between AS 1 and AS 2. The dilemma is that Router A is not capable of running BGP. To make this connection, you are going to have to use the **`ebgp-multihop`** command.

**Configure Router B:**

1. Enable BGP on Router B using the router BGP 2 command.
2. Synchronization is not needed here so turn it off with the no synchronization command. 3. It is now time to enter in the BGP neighbors. Since Router A is not running BGP, it cannot be our neighbor. So our neighbor will be the serial 0 interface of Router C. To assign Router C as our neighbor, issue the following command:

```
RTB(config-router)# neighbor 192.16.2.2 remote-as 1
```

3. So far we have done nothing new. The next thing we have to do is specify that we must go through 2 hops to get to Router C. To do this, use the command:

```
RTB(config-router)# neighbor 192.16.2.2 ebgp-multihop
2
```

4. Save your configuration and move on to Router C.

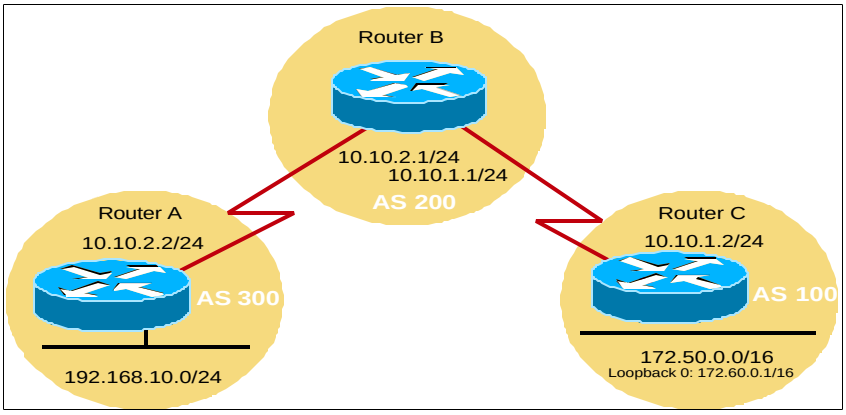
**Configure Router C:**

1. You are on your own to figure out the commands to configure Router C. However, the tasks to be completed are to enable BGP and enter in the appropriate neighbor statements. Hint: You will need 2 neighbor statements. Use the steps for Router B as a guide.

**Verification:**

Verify you can reach Router B. This can be achieved by using the ping, trace, and viewing the routing table. Use the debug commands you have learned to view the negotiation and update process. Do you notice anything different?

# Lab 8.7.5 BGP Route Aggregation




**Objectives:**

- Configure CIDR with BGP.

**Scenario:**

Router B is receiving advertisements about network 172.50.0.0 and 172.60.0.0 from Router C in AS 100. Router B needs to only advertise the 172.0.0.0 prefix to the Internet and other Autonomous Systems.

**Tasks:**

1. Cable and configure the lab as shown in the diagram. Use BGP as your routing protocol. On Router-C, advertise both networks 172.50.0.0 and 172.60.0.0 with the network command. Don't forget to advertise network 192.168.10.0 on Router A also. Before moving on to the next step, be sure that Router-A and Router-C are seeing each others routes with the **`show ip route`** and **`show ip bgp`** commands.

   _____

2. Look at the routing table of Router A, what routes do you see?

   _____

3. Login to Router-B. To enable the aggregation of the 172.0.0.0 networks, issue the following command:

   Router-B(config-router)#**`aggregate-address`** 172.0.0.0 255.0.0.0
   Router-B#**`clear ip bgp`** *

4. Now look at the routing table of Router-A. What routes do you see that begin with the prefix 172.x.x.x?

   _____

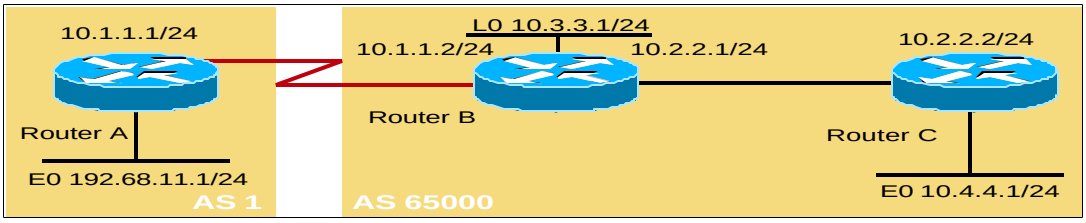
5. Did you see more than you planned? _____ Suppose we only want the 172.0.0.0 prefix to be advertised and not any more specific routes. Issue the following command to make this happen:

```
Router-B(config-router)#aggregate-address 172.0.0.0
255.0.0.0 summary-only
Router-B#clear ip bgp *
```

6. Go back to Router-A and examine the routing table. What routes do you see that begin with the prefix 172.x.x.x?

_____

## Lab 8.7.9 Next Hop Attribute




**Objectives:**

- Use the neighbor next-hop-self command to prevent routing failure between 2 routers that do not have a direct connection.

**Scenario:**

Router C learns about network 192.68.11.0/24 via EBGP from Router B with a next hop of 10.1.1.1, which is the IP address of the external neighbor to router B. However, Router C does not have a direct connection to Router A and therefore cannot reach the next hop. This will cause routing to fail. You will need to use the **`neighbor next-hop-self`** command to remedy this situation.

**Tasks:**

1. Cable the lab and all interfaces as shown in the diagram. Don't forget the no shutdown command!

   _____

2. Configure OSPF routing between routers B and C. Put both routers in area 0.

```
Router B(config)#router ospf 1
Router B(config-router)#network 10.2.2.0 0.0.0.255 area 0
Router B(config-router)#network 10.3.3.0 0.0.0.255 area 0
Router B(config-router)#passive-interface serial 0

Router C(config)#router ospf 1
Router C(config-router)#network 10.2.2.0 0.0.0.255 area 0
Router C(config-router)#network 10.4.4.0 0.0.0.255 area 0
```

3. Verify that Router B can successfully ping 10.1.1.1 and all interfaces on Router C.

   _____

4. Configure BGP on Router A.

```
Router A(config)#router BGP 1
Router A(config-router)#neighbor 10.1.1.2 remote-as 65000
Router A(config-router)#network 192.68.11.0
Router A(config-router)#no synchronization
```

5. Configure BGP on Routers B and C.

```
Router B(config)#router BGP 65000
Router B(config-router)#neighbor 10.1.1.1 remote-as 1
Router B(config-router)#neighbor 10.2.2.2 remote-as 65000
Router B(config-router)# network 10.2.2.0 mask 255.255.255.0
Router B(config-router)#no synchronization
```

```
Router C(config)#router BGP 65000
Router C(config-router)#neighbor 10.2.2.1 remote-as 65000
Router C(config-router)#network 10.4.4.0 mask 255.255.255.0
Router C(config-router)#no synchronization
```

6. Save your configurations.

_____

7. From Router C, can you ping 192.68.11.0?

_____

8. View the BGP routing table with the show ip bgp command, what can you say about network 192.168.11.0?

_____

9. Time to fix the problem! Router B needs to advertise itself as the next hop to Router C. To do this, issue the following commands:

```
Router B(config-router)#neighbor 10.2.2.2 next-hop-self
```

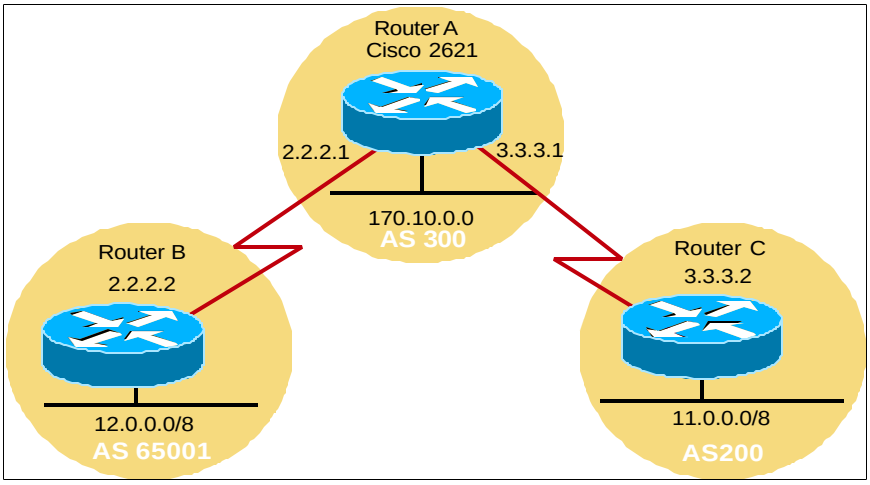
10. Now try to ping 192.68.11.1 from Router C. Were you successful?

_____

11. Save your configuration and view the routing table of Router C again. What is different?

_____

## Lab 8.8.2 Remove Private AS Numbers




**Objectives:**

- In the example above, AS 300 needs to prevent the private AS number 65001 from being leaked to the Internet when BGP routes are propagated.

**Scenario:**

Router C learns about network 192.68.11.0/24 via EBGP from Router B with a next hop of 10.1.1.1, which is the IP address of the external neighbor to router B. However, Router C does not have a direct connection to Router A and therefore cannot reach the next hop. This will cause routing to fail. You will need to use the **`neighbor next-hop-self`** command to remedy this situation.

**Tasks:**

1. Cable the lab and address the interfaces as shown in the graphic. Use the default subnet mask for all addresses. All Ethernet interfaces should use the .1 address. For example, 12.0.0.1.

---

2. Enable BGP routing on each router. Only advertise the network off the Ethernet interfaces. The configurations should be as follows:

```
RouterC(config)#router bgp 200
RouterC(config-router)#network 11.0.0.0
RouterC(config-router)#no synchronization
RouterC(config-router)#neighbor 3.3.3.1 remote-as 300

RouterB(config)#router bgp 65001
RouterB(config-router)#network 12.0.0.0
RouterB(config-router)#neighbor 2.2.2.1 remote-as 300
RouterB(config-router)#no synchronization
```

```
RouterA(config)#router bgp 300
RouterA(config-router)#network 170.10.0.0
RouterA(config-router)#neighbor 2.2.2.2 remote-as 65001
RouterA(config-router)#neighbor 3.3.3.2 remote-as 200
```

3. Verify that you can see networks 12.0.0.0, 11.0.0.0 and 170.10.0.0 in the routing table. Use the **`show ip route`** and **`show ip bgp`** commands to do this.

4. Issue the **`show ip bgp`** command on router C. What is that AS path to network 12.0.0.0?

_____

5. On router A, issue the following commands:

```
RouterA(config)#router bgp 300
RouterA(confing-router)# neighbor 3.3.3.2 remove-private-as
```

Configure BGP on Routers B and C.Save your configurations.

6. Go back to router C and issue the command:

```
RouterC#clear ip bgp *
```

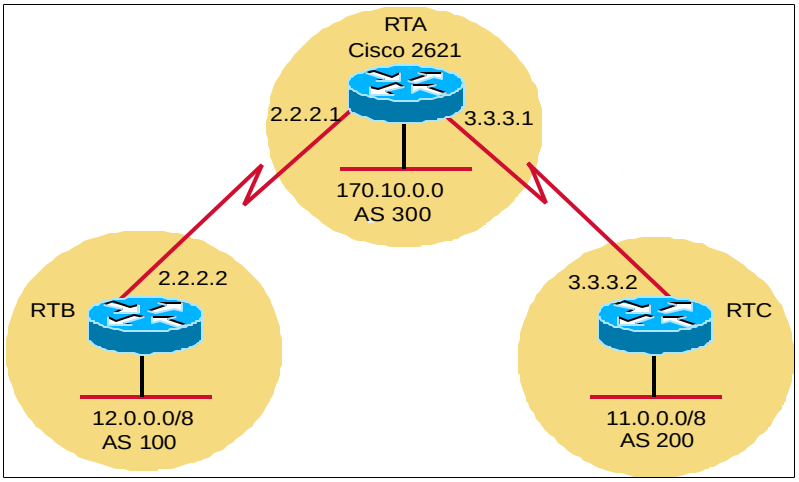
7. Wait a few seconds and issue the show ip bgp command. What is different?

_____

8. What is the usefulness of this command?

_____

## Lab 8.8.3 AS_path Filtering with a Filter List




**Objectives:**

Filter BGP updates based on the AS_path attribute.

**Scenario:**

We want to deny any update whose AS_path starts with 200 and ends with 200. In other words, we want to deny any updates originating in AS 200.

**Lab Tasks:**

1. Cable the lab and address the interfaces as shown in the graphic. Use the default subnet mask for all addresses. All Ethernet interfaces should use the .1 address. For example, 12.0.0.1.
2. Enable BGP routing on each router. Only advertise the network off the Ethernet interfaces. The configurations should be as follows:

```
RouterC(config)#router bgp 200
RouterC(config-router)#network
11.0.0.0
RouterC(config-router)#no
synchronization
RouterC(config-router)#neighbor
3.3.3.1 remote-as 300

RouterB(config)#router bgp 100
RouterB(config-router)#network
12.0.0.0
RouterB(config-router)#neighbor
2.2.2.1 remote-as 300
RouterB(config-router)#no
synchronization
```

```
RouterA(config)#router bgp 300
RouterA(config-router)#network
170.10.0.0
RouterA(config-router)#neighbor
2.2.2.2 remote-as 100
RouterA(config-router)#neighbor
3.3.3.2 remote-as 200
```

3. Verify that you can see networks 12.0.0.0, 11.0.0.0 and 170.10.0.0 in the routing table. Use the **`show ip route`** and **`show ip bgp`** commands to do this. Verify connectivity with the ping command. What are the differences in the path to network 11.0.0.0 in the routing tables of Routers A and B?

---

4. Now we have decided to filter updates originating from AS 200 as described in the scenario on Page 1. We are going to do this from Router A. Log into Router A.
5. To deny these updates, we will need to configure a special access list to do so. It is necessary in this scenario to deny updates from AS 200 but permit updates from elsewhere. The first command will be to deny updates containing AS_path attributes beginning and ending with 200. The command is:

```
RouterA(config)#ip as-path access-
list 1 deny ^200$
```

   Access list 1 denies any update whose AS_path starts with 200 (specified by the ^) and ends with 200 (specified by the $). Because Router C sends updates about 11.0.0.0 whose AS_path attributes start with 200 and end with 200, such updates will match the access list and be denied. By specifying that the update must also end with 200, the access list permits updates from another AS that may be connected to AS 200. For example, if AS 500 was attached to AS 200, the AS_path attribute would be {200, 500} so it would be permitted.

6. Since we want to permit all other updates, we need a command to do this. The command is:

```
RouterA(config)#ip as-path access-
list 1 permit .*
```

   In this access list statement, the period symbol means any character, and the asterisk symbol means a repetition of that character. Together, .* matches any value of the AS_path attribute, which in effect permits any update that has not been denied by the previous access list statement.

7. The last step is to apply the access list to a neighbor. We do not want these updates passed on to AS 100. So use the following neighbor command:

```
RouterA(config)#router bgp 300
RouterA(config)#neighbor 2.2.2.2
filter-list 1 out
```

8. To verify the expressions are working as intended, issue the command:

```
RouterA#show ip bgp regexp ^200$
```

What do you notice?

---

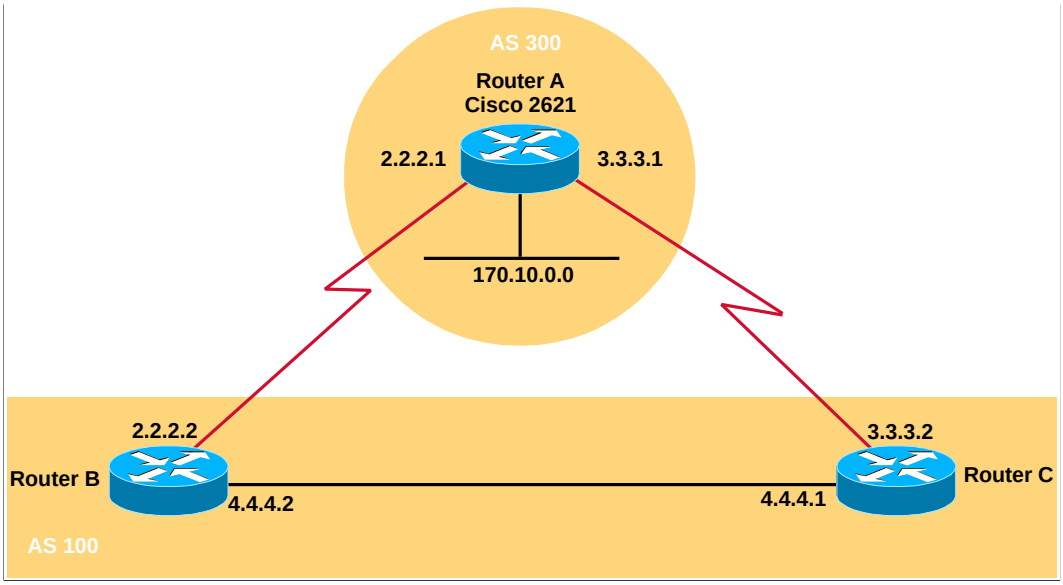
9. Log into Router B and check the routing table. Do you see a route for 11.0.0.0?

---

10. If you still see network 11.0.0.0, issue the clear ip bgp * command and wait a few seconds. Did the 11.0.0.0 network return?

---

## Lab 8.8.6 Changing the Local Preference




**Objectives:**

Configure the Local Preference attribute to indicate a preferred route to a destination with multiple routes.

**Scenario:**

You are the network administrator in AS 100. As shown in the diagram, network 170.10.0.0 can be reached via network 3.0.0.0 and 4.0.0.0. Configure the Local Preference attribute on Router C to prefer the 4.0.0.0 network over the 3.0.0.0 network.

**Lab Tasks:**

1. Cable the lab and address the interfaces as shown in the graphic. Use the default subnet mask for all addresses. All Ethernet interfaces should use the .1 address. For example, 12.0.0.1.

2. Enable BGP routing on each router. The configurations should be as follows:

```
RouterC(config)#router bgp 100
RouterC(config-router)#no synchronization
RouterC(config-router)#neighbor 3.3.3.1
remote-as 300
RouterC(config-router)#neighbor 4.4.4.2
remote-as 100
RouterC(config-router)#network 4.0.0.0

RouterB(config)#router bgp 100
RouterB(config-router)#neighbor 4.4.4.1
```

```
remote-as 100
RouterB(config-router)#neighbor 2.2.2.1
remote-as 300
RouterB(config-router)#no synchronization
RouterB(config-router)#network 4.0.0.0

RouterA(config)#router bgp 300
RouterA(config-router)#network 170.10.0.0
RouterA(config-router)#neighbor 2.2.2.2
remote-as 100
RouterA(config-router)#neighbor 3.3.3.2
remote-as 100
```

3. Verify that you can see network 170.10.0.0 in the routing table of each router. Use the **`show ip route`** and **`show ip bgp`** commands to do this.

4. Issue the `show ip bgp` command on Router C. What is the current preferred route to network 170.10.0.0?

---

5. List the different paths to network 170.10.0.0.

---

6. How do you know which path is preferred?

---

7. Now it is time to change the preferred route. We are going to use a route map to accomplish this.

8. Configure the route map as follows:

```
RouterC(config)#route-map
setlocalpref permit 10
RouterC(config)#set local-
preference 200
```

Since the default preference of the BGP route is 100, this route map will give a higher preference to the updates coming from network 4.0.0.0.

9. The last step is to assign the route map to a neighbor. We want to apply it to updates coming from Router B **IN** to Router C. To do this issue the following commands:

```
RouterC(config)#router bgp 100
RouterC(config-router)#neighbor
4.4.4.2 route-map setlocalpref in
```

10. Now issue the **`clear ip bgp *`** command on Router C and wait a few seconds for the router to relearn the routes.

11. Issue the command **`show ip bgp`**. What is different about the bpg routing table?

---

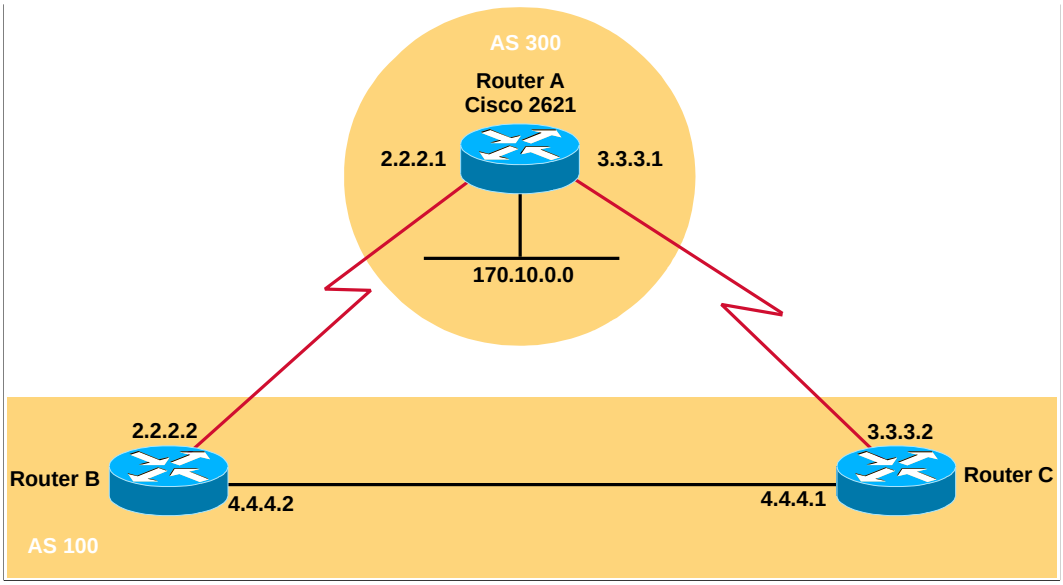
12. Which route is preferred to network 170.10.0.0?

---

13. Is the Local preference applied to any other routes?

---

# Lab 8.8.8 Multi-Exit Discriminator Attribute (MED)




**Objectives:**

- Configure the MED attribute to influence routing decisions in another AS.

**Scenario:**

In the graphic, AS 300 receives updates about network 4.0.0.0 from AS 100. Currently, Router A will access network 4.0.0.0 via 3.0.0.0. We want AS 300 to use the 2.0.0.0 network to access network 4.0.0.0. Unfortunately, you have no control over the router in AS 300. Use the MED attribute to "influence" the routing decisions of AS 300.

**Notes:**

In some situations, Router A may choose to access network 4.0.0.0 via 2.0.0.0. If this is the case, when you reach step 7 in the lab, set the metric to 100 on Router B and 50 on Router C. Before starting the lab, verify the route taken by using a trace and/or examining the routing table.

**Tasks:**

1. Cable the lab and address the interfaces as shown in the graphic. Use the default subnet mask for all addresses. The IP address on Router A E0 should be 170.10.0.1.
2. Enable BGP routing on each router. The configurations should be as follows:

```
RouterC(config)#router bgp 100
RouterC(config-router)#no synchronization
RouterC(config-router)#neighbor 3.3.3.1 remote-as 300
RouterC(config-router)#neighbor 4.4.4.2 remote-as 100
RouterC(config-router)#network 4.0.0.0
```

```
RouterB(config)#router bgp 100
RouterB(config-router)#neighbor 4.4.4.1 remote-as 100
RouterB(config-router)#neighbor 2.2.2.1 remote-as 300
RouterB(config-router)#no synchronization
RouterB(config-router)#network 4.0.0.0

RouterA(config)#router bgp 300
RouterA(config-router)#network 170.10.0.0
RouterA(config-router)#neighbor 2.2.2.2 remote-as 100
RouterA(config-router)#neighbor 3.3.3.2 remote-as 100
```

3. Verify that you can see network 4.0.0.0 in the routing table of each router. Use the `show ip route` and `show ip bgp` commands to do this.

_____

4. Issue the **`show ip bgp`** command on Router A. What is the current preferred route to network 4.0.0.0?

_____

5. List the different paths to network 4.0.0.0.

_____

6. How do you know which path is preferred?

_____

7. Our task is to influence the preferences of AS 300 by using the MED attribute from AS 100. Remember that we want AS 300 to use a route that we specify. We will start with Router B in AS 100. This is another situation where a route map will come in handy! Issue the following commands:

```
RouterB(config)#route-map setmedout permit 10
RouterB(config-route-map)#set metric 50
***Remember: The lower MED wins!***

RouterB(config)#router bgp 100
RouterB(config-router)#neighbor 2.2.2.1 route-map setmedout out

Now we need to move over to Router C and configure the MED there.
Issue the following commands:

RouterC(config)#route-map setmedout permit 10
RouterC(config-route-map)#set metric 100
***Note: This is a higher MED than Router B!***

RouterC(config)#router bgp 100
RouterC(config-router)#neighbor 3.3.3.1 route-map setmedout out
```

8. Log into Router A. Issue the **`clear ip bgp *`** command and wait a few seconds before issuing the **`show ip bgp`** command. Has there been any change in the routing behavior

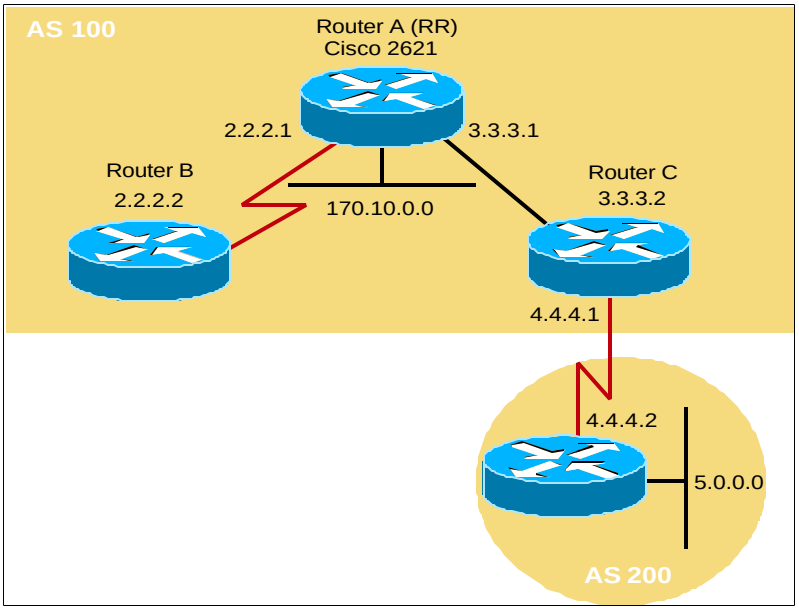
or is 3.3.3.2 still the preferred route?

---

Why?

---

# Lab 9.1.3 Route Reflectors




**Objectives:**

- Configure a Route Reflector to reduce the IBGP mesh.

**Scenario:**

The graphic above illustrates a simple IBGP configuration with three IBGP speakers (Routers A, B, and C). Without route reflectors, when Router C receives a route from an external neighbor, it must advertise it to both Routers A and B. Routers A and B do not readvertise the IBGP learned route to other IBGP speakers because the routers do not pass routes learned from internal neighbors on to other internal neighbors, thus preventing a routing information loop.

With route reflectors, all IBGP speakers need not be fully meshed because there is a method to pass learned routes to neighbors. In this model, an internal BGP peer is configured to be a route reflector responsible for passing IBGP learned routes to a set of IBGP neighbors. In the diagram above, Router A is configured as a route reflector. When the route reflector receives routes advertised from Router C, it advertises them to Router B, and vice versa. This scheme eliminates the need for the IBGP session between Routers B and C.

Your task in this lab is to configure Router A as a route reflector since there is not a full IBGP mesh in AS 100.

**Tasks:**

1. Configure all the interfaces to have the appropriate IP addresses as shown in the diagram. Use the /24 subnet mask.

2. Configure RIP as your IGP. Then enable BGP routing on all routers. Use the network command to advertise the LAN on Router A and the router in AS 200. Don't forget your neighbor statements!!! They are not shown. Advertise the following routes:

   Network 2.0.0.0 from Router B
   Network 170.10.0.0. from Router A
   Network 5.0.0.0 from Router D in AS 200

   Example: `Router(config)#Router BGP 200`
   `Router(config-router)#network 5.0.0.0 mask 255.255.255.0`

3. Examine the routing table of each router in AS 100. Do you see network 5.0.0.0 in each routing table?

   _____

   Which router is missing the entry?

   _____

   Why is the network entry missing?

   _____

4. From Router A, can you use an extended ping with source address 170.10.0.1 (interface E0) and successfully reach 5.0.0.1 (E0 of the router in AS 200)?

   _____

   If the answer to the above question is yes, then good job in your configuration! If not, did you use the neighbor next-hop-self command? Why is this command necessary?

   _____

5. Verify connectivity between the routers.

6. Log on to Router A. We are going to configure it as a route reflector. The commands to do this are as follows:

```
RouterA(config)#router bgp 100
RouterA(config-router)# neighbor 2.2.2.2 route-reflector-client
RouterA(config-router)#neighbor 3.3.3.2 route-reflector-client
```

7. Save your configuration and log on to Router B. Issue the **`clear ip bgp *`** command. Now check the BGP routing table with the **`show ip bgp`** command. Do you see an entry for network 5.0.0.0?

   _____

   In how large of a network do you think route reflectors would be useful in?

   _____

Which is better, a full IBGP mesh or route reflectors?

_____

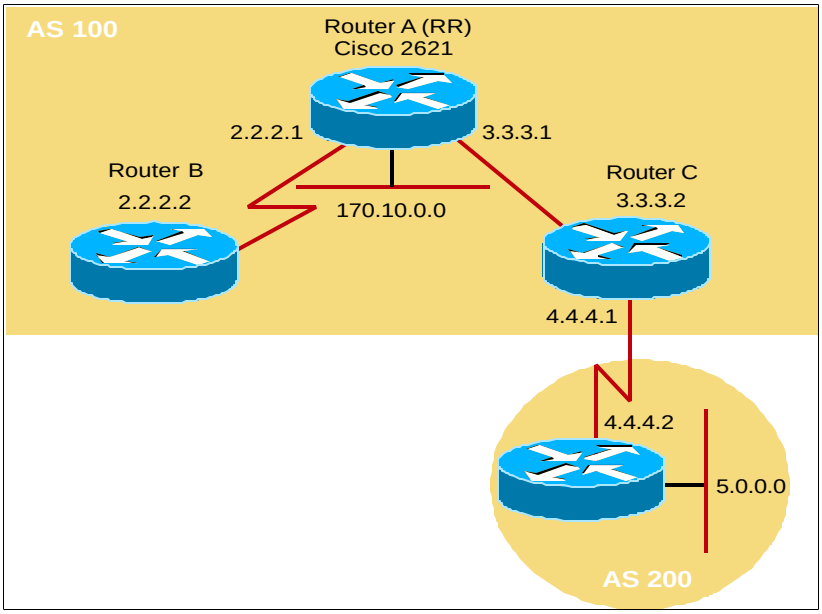
Why?

_____

8. Save you configurations as you will need them for the next lab on Route Filtering based on NLRI.

_____

# Lab 9.2.3 Identifying and Filtering Routes based on the NLRI




**Objective:**

Filter routing information using a distribute list in BGP.

**Scenario:**

Given the lab you just completed on Router Reflectors. You have decided that you want to prevent network 2.0.0.0 from being advertised to AS 200. You have decided to use a route filter on Router C.

**Lab Tasks:**

1. Examine the routing table on Router D in AS 200. Do you see a BGP advertisement for network 2.0.0.0?
2. If you do not see an advertisement for network 2.0.0.0, troubleshoot the network until you see the route in the BGP table.
3. Log into router C. This is where we are going to filter the routing updates that go into AS 200. We are going to use a distribute list in order to accomplish this task.
4. The first step in configuring a distribute list is to set up a standard access list. Since we are going to filter network 2.0.0.0 and allow all other networks, issue the following commands:

    - RouterC(config)#**access-list 1 deny 2.0.0.0 0.255.255.255**
    - RouterC(config)#**access-list 1 permit 0.0.0.0 255.255.255.255**

    These commands are denying the 2.0.0.0 network while allowing any other network to pass freely.

5. As with any access list statement, these commands do nothing until you enable them with the distribute list command. The command is listed below:

    - RouterC(config)#**router bgp 100**
    - RouterC(config-router)#**neighbor 4.4.4.2 distribute-list 1 out**

6. Log onto Router D in AS 200 and issue the **clear ip bgp *** command.

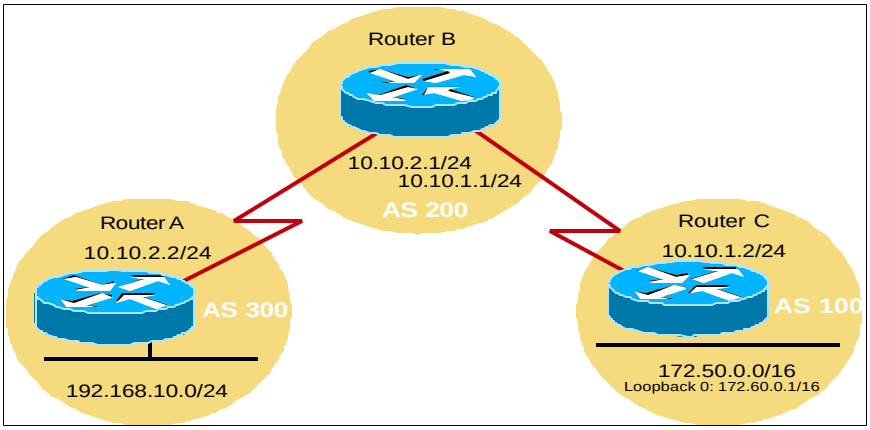
    Wait about 10 seconds and then issue the **show ip bgp** command. Did an entry for network 2.0.0.0 appear in the routing table?

---

Why do you think it is important to filter routing information?

---

## Lab 9.2.5 Prefix List




**Objectives:**

- Use a prefix list to filter routes.

**Scenario:**

Router B is receiving advertisements about network 172.50.0.0 and 172.60.0.0 from Router C in AS 100. Router B should only be able to advertise 172.0.0.0/8 to AS 300

**Tasks:**

1. Cable and configure the lab as shown in the diagram. Use BGP as your routing protocol. On Router-C, advertise both networks 172.50.0.0 and 172.60.0.0 with the network command. You will also need to advertise the **`aggregate-address`** 172.0.0.0 255.0.0.0 on Router-C. Don't forget to advertise network 192.168.10.0 on Router A also. Before moving on to the next step, be sure that Router-A and Router-C are seeing each others routes with the **`show ip route`** and **`show ip bgp`** commands.

2. Look at the routing table of Router A, what routes do you see?

   _____

3. To permit only 172.0.0.0/8 updates, we are going to configure a prefix list called supernetonly. To do this, issue the following command:

   ```
   Router-B(config)# ip prefix-list supernetonly permit 172.0.0.0/8
   ```

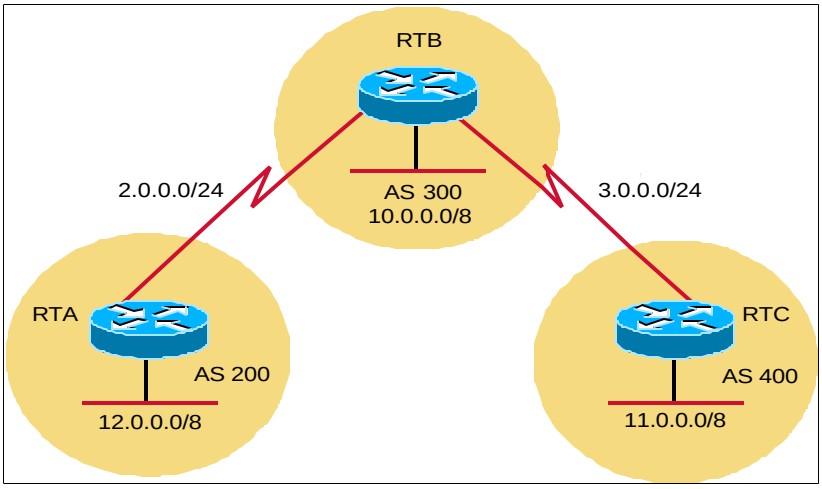
4. Just like an access-list, this has no effect until we assign it to a neighbor. To assign the prefix list to Router-A, issue the following command:

   ```
   Router-B(config-router)#neighbor 10.10.2.2 prefix-list
   supernetonly out
   ```

5. Clear your BGP routing table on Router-A with the clear ip bgp * command and examine the routing table of Router-A. What routes do you see now?

_____

## Lab 9.2.7 The Community Attribute




**Objective:**

- Use the Community Attribute to dynamically influence the routing decisions of another AS.

**Scenario:**

You are the network administrator of AS 400. You want to prevent AS 300 from advertising network 11.0.0.0 to any external AS. You have decided that setting the community attribute would be the best way to handle this situation.

**Tasks:**

1. Configure BGP on each router and advertise each LAN. Be sure to use 3.0.0.2 on Router C and 2.0.0.2 on Router A. Use the .1 addresses on Router B. Verify that you have connectivity with the **`show ip bgp`** command and the extended ping command.
2. We will be using a route map to attach the "no-export" attribute to advertisements about network 11.0.0.0. Therefore, the community attribute will require an access list to match up with the route map. The access list statement should be as follows:

    - RouterC(config)#**`access-list 1 permit 11.0.0.0 0.255.255.255`**

    Why did we choose to permit the network?

    _____

3. The next step is to use the send-community subcommand to cause the assigned community to be sent out. This is done as follows:

    - RouterC(config-router)#**neighbor 3.0.0.1 send-community**

    Why are we sending the community to this neighbor?

---

4. Next step is to configure a route map that will assign the no-export attribute to network 11.0.0.0 but leave other networks alone. This will be done as follows:

    - RouterC(config)#**route-map SETCOMMUNITY permit 10**
    - RouterC(config-route-map)#**match ip address 1**
    - RouterC(config-route-map)#**set community no-export**
    - RouterC(config-route-map)#**exit**
    - RouterC(config-route-map)#**route-map SETCOMMUNITY permit 20**

    Describe what you believe each of the above commands does:

---

5. The final step is to assign the route-map to a neighbor. This command is:

    - RouterC(config-router)#**neighbor 3.0.0.1 route-map SETCOMMUNITY out**

    Why did we set the route-map to out?

---

6. Go to Router A and Router B. Issue the **clear ip bgp *** command on each router and see if network 11.0.0.0 appears in the routing table by using the **show ip bgp** command.

    What are your findings?

---

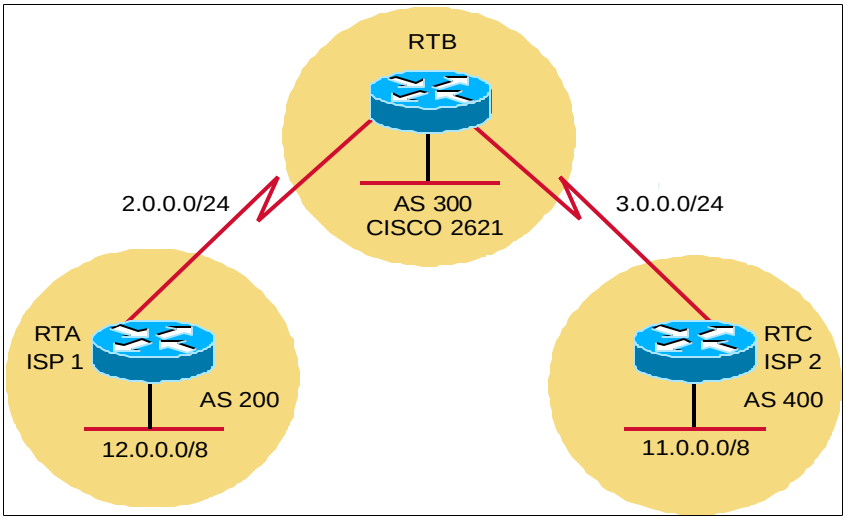
7. On Router B, issue the command **`show ip bgp 11.0.0.0`**.

   What does this command tell you?

---

8. Save your configurations.

## Lab 9.2.9 Peer Groups




**Objective:**

Configure a peer group to assign policies to a group of BGP neighbors that share the same update policies.

**Scenario:**

You are the Network Administrator for AS 300. Given a normal BGP configuration, AS 200 and 400 are receiving updates about network 10.0.0.0. You wish to do this in an efficient manor, so you decide to use a peer group. Use the peer group to filter updates about 10.0.0.0 into AS 200 and AS 400.

**Tasks:**

1. Configure BGP on each router and advertise each LAN. Be sure to use 3.0.0.2 on Router C and 2.0.0.2 on Router A. Use the .1 addresses on Router B. Verify you have connectivity with the **`show ip bgp`** command and the extended ping command.
2. The first step is to define the peer group. This is done with the following command:

    - RouterB(config)#**`Router BGP 300`**
    - RouterB(config-router)#**`neighbor EXTERNALMAP peer-group`**

    **EXTERNAL MAP is the name of the peer group**

3. Now we are going to apply a policy to the peer group. We are going to filter 10.0.0.0 updates with a distribute list that will apply to both neighbors. To do this, issue the following commands:

    - RouterB(config-router)#**neighbor EXTERNALMAP distribute-list 1 out**
    - RouterB(config-router)#**neighbor 2.0.0.2 peer-group EXTERNALMAP**
    - RouterB(config-router)#**neighbor 3.0.0.2 peer-group EXTERNALMAP**

4. Don't forget to configure the access-list!!

    - RouterB(config)#**access-list 1 deny 10.0.0.0 0.255.255.255**
    - RouterB(config)#**access-list 1 permit 0.0.0.0 255.255.255.255**

    Why did we set the distribute list to out?

---

5. Telnet to Routers A and C. Issue the **clear ip bgp *** command and watch the BGP routing table rebuild.

    Did network 10.0.0.0 show up in the BGP routing table?

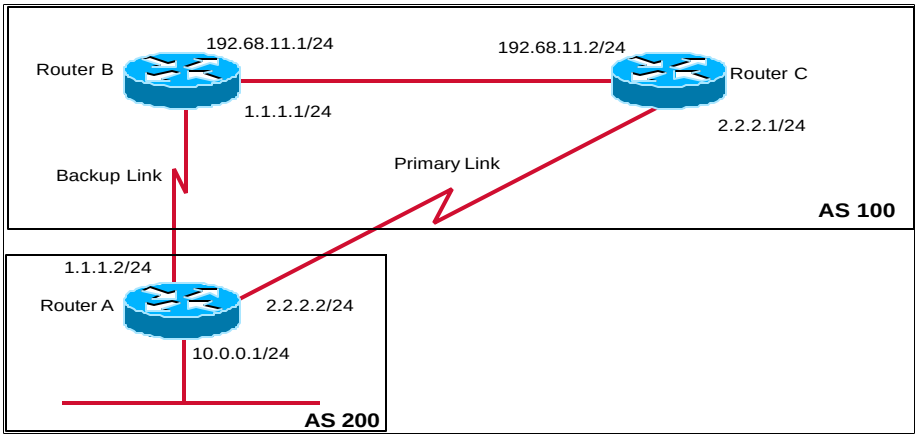
---

In this lab we did not save a lot of work by using a peer group. Can you think of a situation where a peer group would simplify configuration?

---

6. Save your configuration.

# Lab 9.4.2 Multihoming to a Single Provider




**Objective:**

Configure a multihomed connection to a single provider using default only routing, one primary, and one backup link.

**Scenario:**

You are going to setup a multihomed connection to your ISP (AS 100). One link will be used as the primary link while the other will be used as a backup link. The following policies must be applied:

- Outbound traffic from AS 200 should always go on the primary link unless that link fails.
- Inbound traffic must also come in on the primary link unless that link fails.
- No BGP updates should be permitted into AS 200.

**Tasks:**

1. Cable the lab as shown in the diagram above.
2. Fully configure routers B and C in AS 100 to support the above network. Include all necessary BGP statements, IGP routing, and advertise the network between B and C in BGP. AS 100 is going to be running IBGP as well as EBGP.
3. Now configure Router A for BGP connectivity. Advertise network 10.0.0.0.
4. Verify that BGP is running correctly. Do not factor in the 3 requirements for this network. Simply make sure you have connectivity.
5. Outbound traffic should always go on the primary link. This issue can be addressed by configuring static routes with different metrics for each link. Since the primary link is preferred, we will assign it a lower metric. The commands are as follows:

RouterA(config)#**ip route 0.0.0.0 0.0.0.0 2.2.2.1 30**
(Primary Link)
RouterA(config)#**ip route 0.0.0.0 0.0.0.0 1.1.1.1 50**
(Backup Link)

Use the trace command to get to 192.68.11.1 from Router A. What route was taken? Are you surprised? Why did it choose that route?

---

6. The next requirement is to be sure that all inbound traffic comes in on the primary link. This can be accomplished by sending different metrics into AS 100 on both links. This is easily accomplished using a route map. For simplicity, call the route maps PrimaryMetric and BackupMetric. The configuration of the route map is quite simply:

- RouterA(config)#**route-map PrimaryMetric permit 10**
- RouterA(config-Route-map)#**set metric 50**
- RouterA(config)#**route-map BackupMetric permit 10**
- RouterA(config-route-map)#**set metric 100**

Why did we set the metric lower on the primary link?

---

7. Don't forget to apply each route map to the appropriate neighbor. PrimaryMetric should be applied to 2.2.2.1. BackupMetric should be applied to 1.1.1.1.
8. The last requirement is to prevent AS 100 from sending updates into AS 200. This can be done with another route map statement. The route map will be as follows:

RouterA(config)#**route-map BlockUpdates deny 10**

Which neighbor(s) should this route map be applied to?

Should it be applied in or out?

---

9. Verify everything is functioning as outlined.

Can you ping the 192.68.11.0 network?

---

10. Use the trace command to get to the 192.68.11.0 network.

    What the primary link taken?

---

    Does the backup link work?

---

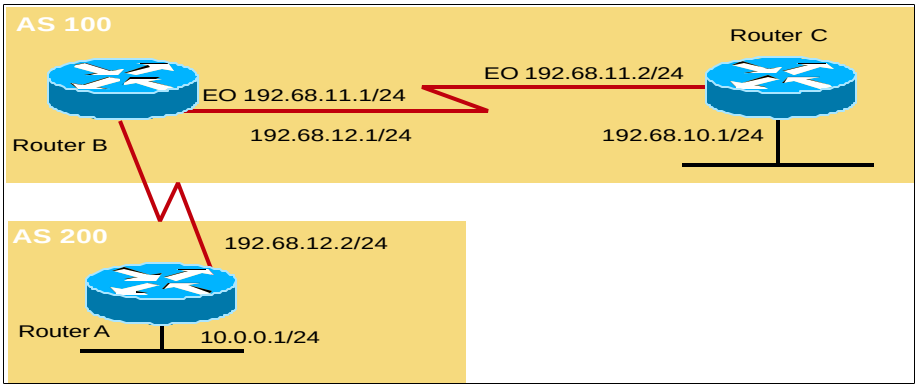
    Unplug the primary link cable.

    Can you still access network 192.68.11.0?

---

11. Reconnect and save your configuration. Note any issues you have encountered with this lab.

# Lab 9.5.4 Inject Information into BGP (Redistribution)




**Objectives:**

- Inject routes from an IGP into BGP using redistribution.

**Scenario:**

AS 200 is receiving Internet connectivity from AS 100. AS 100 is using RIP as its IGP. Router C is not running BGP but networks 192.68.10.0 and 192.68.11.0 need to be advertised to AS 200. You have decided to use redistribution to make this a reality.

**Notes:**

In some situations, Router A may choose to access network 4.0.0.0 via 2.0.0.0. If this is the case, when you reach step 7 in the lab, set the metric to 100 on Router B and 50 on Router C. Before starting the lab, verify the route taken by using a trace and/or examining the routing table.

**Tasks:**

1. Cable the network and address all interfaces as shown in the above diagram.
2. Configure RIP routing between Router B and C. Do not send RIP updates to AS 200. What command allows you to stop RIP updates from going to AS 200?

   _____

3. Configure BGP between Router A and Router B. Allow BGP to advertise network 10.0.0.0 with the network command.
4. Examine the routing table of Router A. What routes do you see that are advertised via BGP? Can you ping any networks in AS 100? If not, do you know why?

   _____

5. Time to fix the problems identified in steps 4 and 5. We need to advertise the RIP networks via BGP. This is done by a process called redistribution, which is described in the curriculum. You will need to issue the following command on Router B:

```
RouterB(config)#router bgp 100 RouterB(config-
router)#redistribute rip
```

6. Save your configuration and log into Router A. Issue the clear ip bgp * command and after a few seconds examine the routing table again.

   Do you see more routes in the routing table? Which routes in AS 100 are now being advertised?

   _____

   _____

   _____

   What networks in AS 100 can you ping from Router A? What networks can you not ping? Can you ping 10.0.0.1 from an address on 192.68.10.0?

   _____

   _____

   _____

   Any idea why you can't ping these networks?

   _____

   _____

   _____

7. Time to fix the problem. Go to Router C and configure a default route to Router B. The command is:

   ```
   RouterC(config)#ip route 0.0.0.0 0.0.0.0 192.68.11.1
   ```

8. Now try ping from Router A to C and vice-versa. Do you have full connectivity?

   _____

   _____

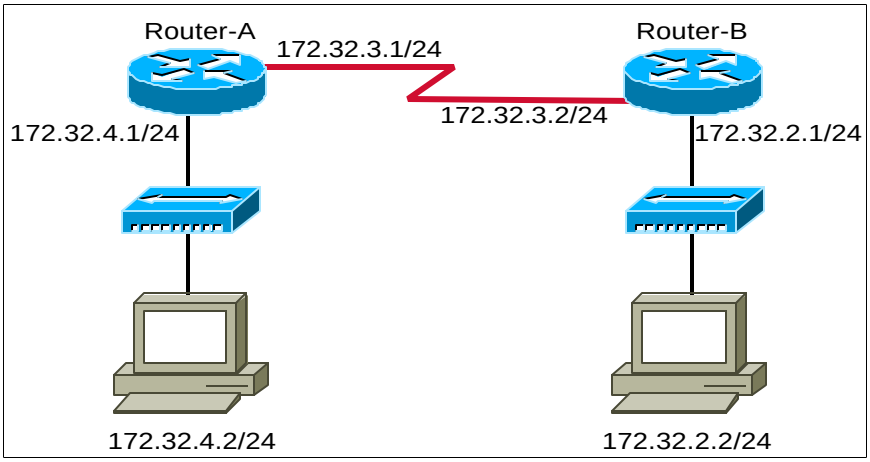
   _____

9. Save your configurations and document any issues you encountered in this lab.

   _____

   _____

# Lab 10.2.7 Standard Access Control Lists




**Objective:**

Demonstrate the use of standard access control lists.

**Equipment Requirements:**

- Two Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Scenario:**

We want to create a standard access-list which will prevent network traffic from users on network 172.32.2.0. The access-list should be applied to the correct router and on the correct interface so that users on network 172.32.2.0 will not be able to access network 172.32.4.0.

## Step 1

Construct the above circuit, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers.

Upon completion of the configuration will the two workstations be able to communicate?

_____

List the entries in the routing table

## Step 2

Determine a standard access list which will prevent access from any user on subnet 172.32.2.0.

What is the required access list?

---

---

## Step 3

Apply the access list accordingly so that the users on subnet 172.32.2.0 will not have access to subnet 172.32.4.0.

Which router did you apply the access list to?

---

On which port did you apply the access list?

---

Was the access list applied coming in to the port or going out of the port?

---

Explain your reasons for placing the access list at the location previously specified.

---

## Step 4

Issue several ping commands to test this access list.

Are hosts on subnetwork 172.32.2.0 be able to ping any host on subnet 172.32.4.0?

---

Is router-b able to ping any host on subnetwork 172.32.4.0? Is router-a able to ping any host on subnetwork 172.32.4.0?

---

**Reflection:**

Answer the following questions.

1. Why is it important to choose the correct wildcard mask for access lists?

---

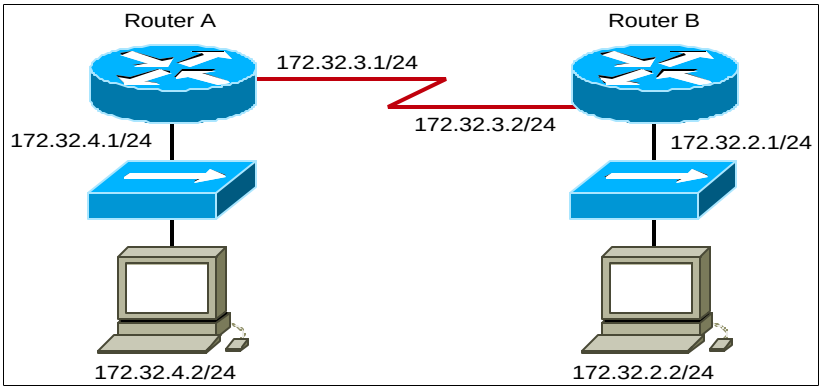
2. Can you alter the information on a particular line of an access list that exists in the middle of the list?

---

3. Typically where should standard access lists be placed on a network?

---

# Lab 10.3.2 Access-Class




**Objectives:**

- Demonstrate the use of the access-class and line commands to control vty access.

**Equipment Requirements:**

- Two Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Scenario:**

We want to create a standard access-list that will permit users on network 172.32.4.0 to telnet to Router-B. The access-list should be applied to the vty lines so that users on network 172.32.4.0 will be able to telnet to Router-B.

## Step 1

Construct the above circuit, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers.

Upon completion of the configuration, telnet from the two workstations to both routers.

Telnet from Router A to Router B and vice versa.

## Step 2

On Router B issue the following commands:

```
router-b(config)#access-list 2 permit
172.32.4.0 0.0.0.255
router-b(config)#line vty 0 4
router-b(config-line)#access-class 2 in
router-b(config-line)#^Z
```

## Step 3

On Router B, attempt to telnet to Router A

Was the telnet successful?

## Step 4

On Router A, attempt to telnet to Router B.

Was the telnet successful?

## Step 5

On the workstation with IP address 172.32.4.2, attempt to telnet to Router B

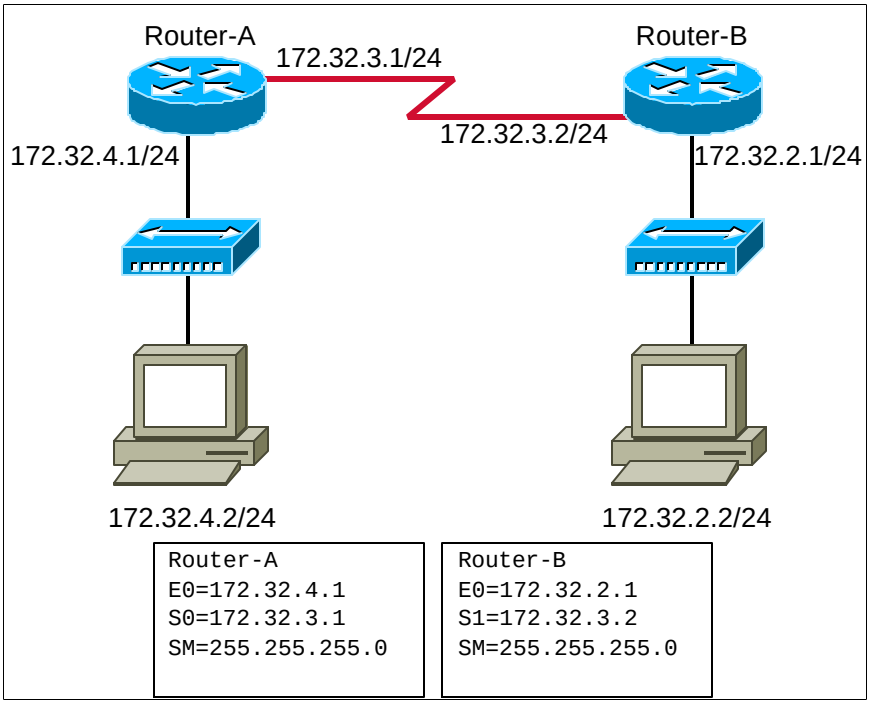
Was the telnet successful?

## Step 6

On the workstation with IP address 172.32.2.2, attempt to telnet to 172.32.3.2 and 172.32.2.1

Was the telnet successful?

# Lab 10.4.4 Extended Access Control Lists




**Objective:**

Demonstrate the use of extended access control lists.

**Equipment Requirements:**

Two Routers One Switch with two VLANS set or two switches or two hubs Two workstations

**Scenario:**

We want to create an extended access control list which will prevent telnet access from network 172.32.4.0 to Router-B. The access list should allow all other traffic including TELNET traffic destined to any other host on the network.

## Step 1

Construct the above circuit, using IGRP as your routing protocol.

Use the network address 172.32.3.0/24 on the serial link between the two routers.

Upon completion of the configuration can the two workstations communicate?

_____

## Step 2

Determine an extended access list which will prevent TELNET traffic originating from subnetwork 172.32.4.0 destined for Router-B.

The access list should allow all other traffic including TELNET traffic destined to any other host on the network. What is the required access list?

Hint: Remember that Router-B has two addresses, E0 has an IP address and S1 has an IP address. Both addresses must be accounted for in the access list.

## Step 3

Apply the access list accordingly so that the users on subnet 172.32.4.0 will not have TELNET access to Router-B.

Which router did you apply the access list to?

Why did you apply the access list to this router instead of the other one?

## Step 4

Once you have the access list on the router, what command do you use to apply it to a specific port on the router?

On which port did you apply the access list?

Was the access list applied coming in to the port or going out of the port?

Explain your reasons for applying the access list at the location previously specified.

## Step 5

Test the access list by TELNETing Router-B as well as to other devices on the different subnetworks.

Are hosts on subnetwork 172.32.4.0 be able to TELNET any host on subnet 172.32.2.0?

Are hosts on subnetwork 172.32.4.0 able to TELNET to Router-B?

Reflection:

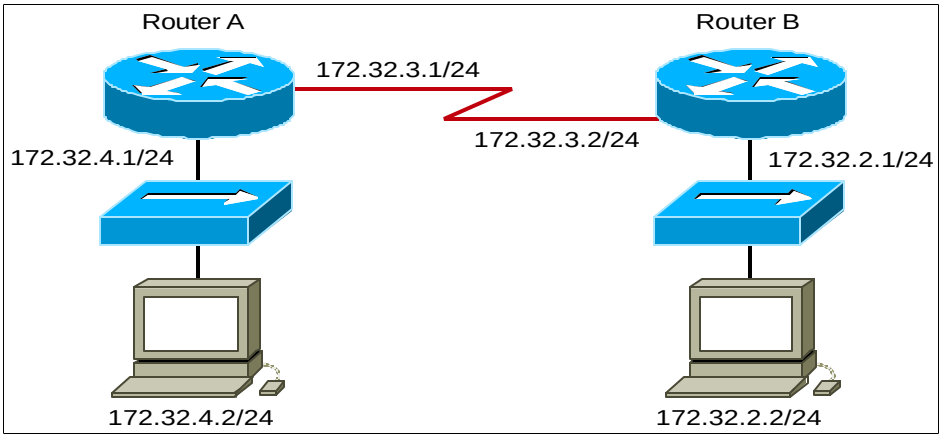
Answer the following questions.

1. Why is it important to choose the correct wildcard mask for access lists?

2. Can you selectively add or remove lines from numbered access lists?

3. Typically where should extended access lists be placed on a network?

# Lab 10.5.2 Null Interface Alternative




**Objectives:**

- Deny traffic to a specific network by using a static route to the null 0 interface.

**Equipment Requirements:**

- Two Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Scenario:**

We want to stop traffic from the 172.32.4.0 network from reaching the 172.32.2.0 network without the overhead of access-list processing. We will use the null 0 interface to drop all traffic for the 172.32.2.0 network into the proverbial bit bucket.

## Step 1

Construct the above circuit, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers.

Upon completion of the configuration, ping and trace from the 172.32.4.2 workstation to the 172.32.2.2 workstation and vice versa.

NOTE: In windows the command is "**`tracert 172.32.2.2`**"

## Step 2

On Router A issue the following command:

```
router-a(config)#ip route 172.32.2.0
255.255.255.0 null 0
router-a(config)#^Z
```

## Step 3

On Router A issue the commands **`show ip route`** and **`ping 172.32.2.1`**. Record your findings below:

_____

_____

## Step 4

On the workstation with IP address 172.32.4.2, attempt to ping 172.32.2.2

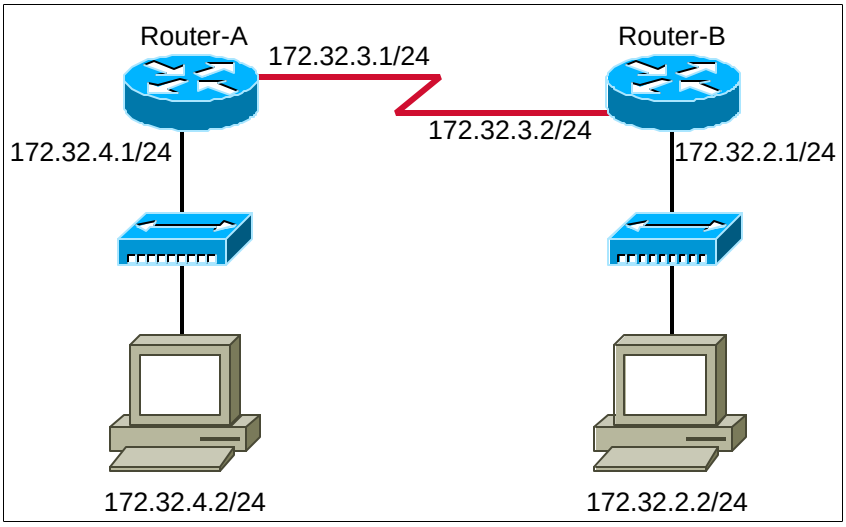
Was the ping successful?

## Step 5

On the workstation with IP address 172.32.2.2, attempt to ping to 172.32.4.2

Was the ping successful?

# Lab 10.6.4 Lock-and-Key Security (Dynamic Access Lists)




**Objective:**

Demonstrate the use of Lock-and-Key security (dynamic access lists).

**Equipment Requirements:**

- Two routers
- One switch with two VLANs set or two switches or two hubs
- Two workstations

**Preliminary:**

Construct the above network, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers.

The router ip configurations are as follows:

| Router-A | Router-B |
|---|---|
| `E0=172.32.4.1` | `E0=172.32.2.1` |
| `S0=172.32.3.1` | `S1=172.32.3.2` |
| `SM=255.255.255.0` | `SM=255.255.255.0` |

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables. Also verify that the workstations can communicate together correctly. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping`**, **`telnet`**, and any other relevant command(s).

**Scenario:**

For this Lab we will be using Router-B as the border router where we will configure the lock-and-key security (dynamic access list). We want to prevent the users in subnetwork 172.32.2.0 from accessing the rest of the network unless they have the correct username and password.

**From the "Router-B" console:**

## Step 1

- Enter the EXEC mode.

## Step 2

- Enter the configuration mode by entering **`configure terminal`** command at the router prompt.

## Step 3

Setup the access list

- Enter **`access-list 103 permit tcp any host 172.32.2.1 eq telnet`**

  What does this one line of the access list do?

---

- Enter **`access-list 103 dynamic mytest103 timeout 5 permit ip any any`**

  What does this one line of the access list do?

---

## Step 4

Apply the access list to the correct interface, and in the correct direction.

- Enter **`interface ethernet 0 Enter ip access-group 103 in`**
- Enter **`exit`**

  Will the access list be applied to information coming into interface e0 or will it be applied to information coming out of interface e0?

---

## Step 5

Define the virtual terminals that will be used for Lock-and-Key

- Enter **`line vty 0 3`**
- Enter **`login local`**
- Enter **`autocommand access-enable host timeout 2`**
- Enter **`exit`**

Note: If we left out the word "host", as soon as anyone entered a correct lock-and-key username password, then everyone one the subnetwork would have access to the rest of the network.

Which virtual terminals did we use for lock-and-key?

---

In the last command that we entered, what does the "timeout 2" mean?

---

## Step 6

Configure user authentication, for all users required.

- Enter **`username john password doe`**
- Enter **`username mary password jane`**
- Enter **`CTRL-Z`**
- Enter **`copy running-configuration startup-configuration`**

Why did we copy the running configuration to the startup config?

---

---

## Step 7

Verify that lock-and-key is working correctly

**From a workstation on subnetwork 172.32.2.0**

- Try to ping the workstation on subnetwork 172.32.4.0

Were you successful?

---

- Try to telnet to 172.32.3.1 (Router-A)

  Were you successful?

---

- Telnet to 172.32.2.1 (Router-B)
- Enter username **`john`**
- Enter password **`doe`**

  What happened next?

---

- Now try to ping the workstation on subnet 172.32.4.0

  Were you successful?

---

- Now try to telnet to 172.32.3.1 (Router-A)

  Were you successful?

---

  Why were you successful this time?

---

## Step 8

Check the access list on the router.

- From Router-B EXEC prompt:
- Enter **`show access-lists`**

  What has changed in the access list?

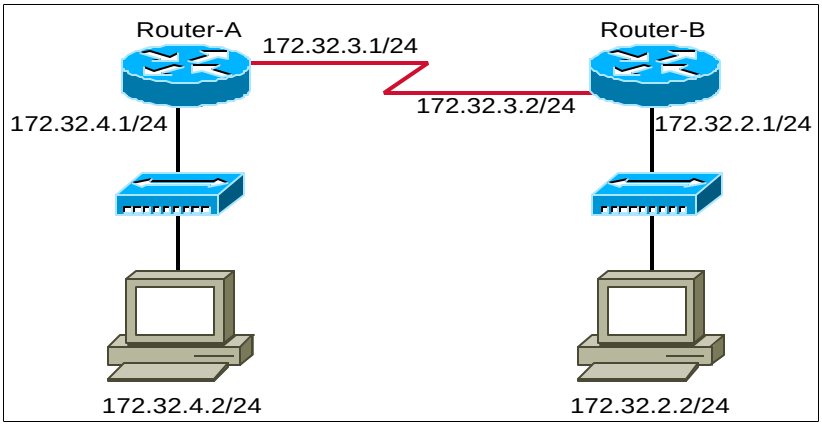
---

- Enter **`clear access-template 103 mytest103 host x.x.x.x any`**
- Enter **`show access-lists`**

  What has changed in the access list?

---

# Lab 10.7.4 Reflexive Access Control Lists




**Objective:**

Demonstrate the use of Reflexive Access Control Lists.

**Equipment Requirements:**

- Two routers
- One switch with two VLANs set or two switches or two hubs
- Two workstations

**Preliminary:**

Construct the above network, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers. The router IP configurations are as follows:

| Router-A | Router-B |
|---|---|
| `E0=172.32.4.1` | `E0=172.32.2.1` |
| `S0=172.32.3.1` | `S1=172.32.3.2` |
| `SM=255.255.255.0` | `SM=255.255.255.0` |

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables. Also verify that the workstations can communicate together correctly. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping`**, **`telnet`**, and any other relevant command(s).

**Scenario:**

For this Lab we will be using Router-B as the border router where we will configure the reflexive access list. We want to prevent the users outside of subnetwork 172.32.2.0 from accessing subnetwork 172.32.2.0. However, the users inside the subnetwork need to have access out and be able to receive information back.

**From the "Router-B" console:**

## Step 1

Enter the EXEC mode.

## Step 2

Enter the configuration mode by entering configure terminal command at the router prompt.

## Step 3

Determine if the access list should be applied to an internal interface or an external interface. Setup the access lists accordingly. We will need to configure both an inbound access list and an outbound access list. For this example the outbound access list will used to modify the inbound access list.

Note: We will be using named access lists for this example.

- Enter **`ip access-list extended filterincoming`**

  What happens to the router prompt?

---

- Enter **`permit igrp any any`**

  Why would we want to permit igrp on our incoming access list?

---

---

- Enter **`evaluate internaltraffic`**

  Describe how this access control list will work.

---

---

- Enter **exit**
- Enter **ip access-list extended filteroutgoing**

  How does the prompt change?

---

---

- Enter **permit tcp any any reflect internaltraffic**

  What does this statement in the access list do?

---

---

- Enter **exit**

## Step 4

Apply the access lists to the correct interface, and in the correct direction.

- Enter **interface serial 1**
- Enter **ip access-group filterincoming in**
- Enter **ip access-group filteroutgoing out**
- Enter **exit**

  Which access list will be applied to information coming into interface S1?

---

  Which access list will be applied to information going out of interface S1?

---

## Step 5

Set global timeout values.

- Enter **ip reflexive-list timeout 120**

  How long does it take for the reflexive access list to expire?

---

- Enter **`CTRL-Z`**
- Enter **`copy running-configuration startup-configuration`**

  Why did we copy the running configuration to the startup config?

## Step 6

Verify that reflexive access list is working correctly From console on router-B

- Enter **`show access-list`**

  What does the router respond with?

- From a workstation on subnetwork 172.32.4.0 Try to ping the workstation on subnetwork 172.32.2.0

  Were you successful?

- Try to telnet to 172.32.2.1 (Router-B)

  Were you successful?

- From a workstation on subnet 172.32.2.0 Now try to ping the workstation on subnet 172.32.4.0

Were you successful?

---

---

- Now try to telnet to 172.32.3.1 (Router-A)

  Were you successful?

---

  Why were you successful this time?

---

## Step 7

Check the access list on the router. From Router-B EXEC prompt

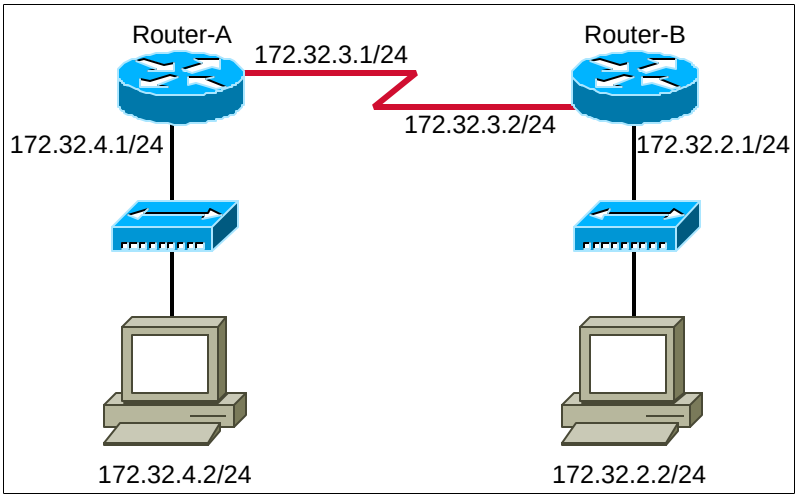
- Enter **`show access-list`**

  What has changed in the access list?

---

---

# Lab 10.8.2.1 Context Based Access Control (Basic Configuration)




**Objectives:**

- Demonstrate the use of Context Based Access Control.

**Equipment Requirements:**

- Two routers
- One switch with two VLANs set or two switches or two hubs
- Two workstations

**Preliminary:**

Before programming the routers, make sure that the IOS version on router-b supports context based access control (firewall). Load a new IOS version if necessary. Construct the above network, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers. The router ip configurations are as follows:

| Router-A | Router-B |
|---|---|
| E0=172.32.4.1 | E0=172.32.2.1 |
| S0=172.32.3.1 | S1=172.32.3.2 |
| SM=255.255.255.0 | SM=255.255.255.0 |

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables. Also verify that the workstations can communicate together correctly. For verification use the **`show ip route`** command, **`show interfaces`** command, **`show running-configuration`** command, **`ping, telnet,`** and any other relevant command(s).

Scenario: For this Lab we will be using Router-B as the border router where we will configure the context based access control (firewall). We want to prevent the users outside of subnetwork 172.32.2.0 from accessing subnetwork 172.32.2.0. However, the users inside the subnetwork need to have http access out and be able to receive http responses.

**From the "Router-B" console:**

## Step 1

Enter the EXEC mode.

## Step 2

Enter the configuration mode by entering `configure terminal` command at the router prompt.

## Step 3

Determine if the access list should be applied to an internal interface or an external interface.

For our example we will be applying it to the external interface of S1.

## Step 4

Setup the outgoing access list to permit CBAC traffic to leave the network through the firewall:

Enter **`access-list 104 permit igrp any any`**
Enter **`access-list 104 permit tcp 172.32.2.0 0.0.0.255 any eq www`**
Enter **`access-list 104 deny ip any any`**

Question - Describe what this access list does.
Answer:

_____

## Step 5

Setup the incoming access list to deny CBAC return traffic from entering the network.

Start with an access list entry denying any net traffic from a source address matching an address on the protected network, next add access list entries to permit certain ICMP return messages. Also traffic with a source address of 255.255.255.255 should be denied from the protected network.

Enter **`access-list 114 permit igrp any any`**
Enter **`access-list 114 deny ip any any`**
Question - Why did we permit igrp?
Answer:

---

Question - What if we were running EIGRP, how would this line on the access list change?
Answer:

---

## Step 6

Apply the access lists to correct interface:

Enter **`interface serial 1`**
Enter **`ip access-group 104 out`**
Enter **`ip access-group 114 in`**
Enter **`exit`**

Question - What would happen if these access lists were applied in reverse? (114 out, and 104 in)
Answer:

---

## Step 7

Define the inspection rule for application layer protocols

Enter **`ip inspect name borderfw http`**
Question - What is the name of our inspection list?
Answer:

---

## Step 8

Apply the inspection rule to an interface

Enter **`interface serial 1`**
Enter **`ip inspect borderfw out`**
Enter **`exit`**
Question - What would happen if we applied our CBAC inspection on the incoming information instead of the outgoing information?
Answer:

---

## Step 9

Verifying CBAC

Enter **`show ip inspect name borderfw`**
Question - What information does the router reply with?
Answer:

---

Enter **`show ip inspect interfaces`**
Question - Which interfaces does the router give information on after this command is executed?
Answer:

---

Enter **`show ip inspect all`**
Question - What information does this command give you?
Answer:

---

## Step 10

Debugging CBAC

Enter **`ip inspect audit-trail`** (if not previously turned on)
Question- What other commands could we use for debugging CBAC?
Answer:

---

## Step 11

Testing the CBAC.

**From Router-A global configuration**
Enter **`ip http server`** (to give us a place to surf to on our network for http traffic)
Enter **`exit`**
Question - If we had not remembered that Cisco routers had a Web interface, what else could we have used in order to get http traffic?
Answer

---

**From a workstation on subnet 172.32.2.0**
Ping Router-A
Question - Were you successful?
Answer:

---

Telnet to Router-A (172.32.4.1)
Question - Were you successful?
Answer:

---

**Open Internet Explorer or Netscape Navigator and surf to Router-A (172.32.4.1)**
Question - Were you successful?
Answer:

---

Question - How did Router-B respond at the console terminal?
Answer:

---

**From a workstation on subnet 172.32.4.0**
Ping Router-B
Question - Were you successful?
Answer:

---

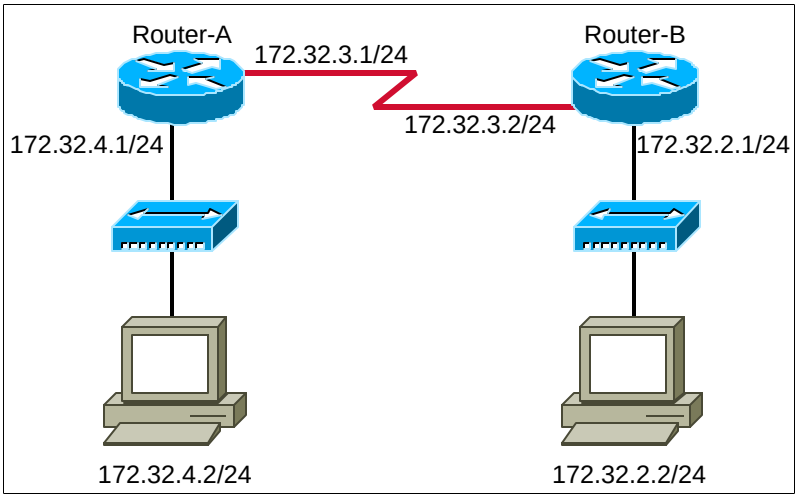
Try to telnet to Router-B Question - Were you successful?
Answer:

---

Question - Is our Context Based Access Control (firewall) working the way it should be? Why or why not?
Answer:

---

# Lab 10.8.2.2 Context Based Access Control (Advanced configuration)




**Objectives:**

- Demonstrate the use of Context Based Access Control.

**Equipment Requirements:**

- Two Routers
- One Switch with two VLANS set or two switches or two hubs
- Two workstations

**Preliminary:**

Before programming the routers, make sure that the IOS version on router-b supports context based access control (firewall). Load a new IOS version if necessary. Construct the above network, using IGRP as your routing protocol. Use the network address 172.32.3.0/24 on the serial link between the two routers. The router ip configurations are as follows:

| Router A | Router B |
|---|---|
| E0=172.32.4.1 | E0=172.32.2.1 |
| S0=172.32.3.1 | S1=172.32.3.2 |
| SM=255.255.255.0 | SM=255.255.255.0 |

When construction of the network is complete, verify that routers can communicate and are sharing their routing tables. Also verify that the workstations can communicate together correctly. For verification use the show ip route command, show interfaces command, show running-configuration command, ping, telnet, and any other relevant command(s).

**Scenario**

For this Lab we will be using Router-B as the border router where we will configure the context based access control (firewall). We want to prevent the users outside of subnetwork 172.32.2.0 from accessing subnetwork 172.32.2.0. However, the users inside the subnetwork need to have access out and be able to receive information back. We want to permit TCP, UDP, and ICMP traffic out. By default, only IGRP, and certain ICMP messages should be allowed back into the 172.32.2.0 network. The firewall should modify the incoming access list to permit FTP, and HTTP return traffic back in to the 172.32.2.0 network.

**From the "Router-B" console:**

## Step 1

Enter the EXEC mode.

## Step 2

Enter the **configuration** mode by entering configure terminal command at the router prompt.

## Step 3

Determine if the access list should be applied to an internal interface or an external interface. For our example we will be applying it to the external interface of S1.

## Step 4

Setup the outgoing access list to permit CBAC traffic to leave the network through the firewall:

```
Enter access-list 104 permit tcp 172.32.2.0 0.0.0.255 any
Enter access-list 104 permit udp 172.32.2.0 0.0.0.255 any
Enter access-list 104 permit icmp 172.32.2.0 0.0.0.255 any
Enter access-list 104 deny ip any any
```

Question - Describe what this access list does.

---

## Step 5

Setup the incoming access list to deny CBAC return traffic from entering the network. Start with an access list entry denying any net traffic from a source address matching an address on the protected network, next add access list entries to permit certain ICMP return messages. These ICMP statements are added to allow administratively prohibited, echo, echo reply, packet too big, traceroute, time exceeded, and unreachable messages to return. Also traffic with

a source address of 255.255.255.255 should be denied from the protected network.

```
Enter access-list 114 deny ip 255.255.255.255 0.0.0.0 any
Enter access-list 114 deny ip 172.32.2.0 0.0.0.255 any
Enter access-list 114 permit igrp any any
```

Question - Why did we permit igrp?

---

Question - What if we were running EIGRP, how would this line on the access list change?

---

```
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
administratively-prohibited
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
echo
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
echo-reply
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
packet-too-big
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
time-exceeded
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
traceroute
Enter access-list 114 permit icmp any 172.32.2.0 0.0.0.255
unreachable
```

Question - Why were all of these ICMP statements added to the access list?

---

```
Enter access-list 114 deny ip any any
```

## Step 6

Apply the access lists to correct interface:

```
Enter interface serial 1
Enter ip access-group 104 out
Enter ip access-group 114 in
Enter exit
```

Question - What would happen if these access lists were applied in reverse? (114 out, and 104 in)

---

## Step 7

Configure global timeouts and thresholds only if the default timeout values are not long enough, or not short enough. The default times will be appropriate for our network.

Question - Name one instance where we might want to alter the default timout values.

---

## Step 8

Define the inspection rule for application layer protocols

```
Enter ip inspect name borderfw ftp
Enter ip inspect name borderfw http java-list 44
```

Question - What is the name of our inspection list?

---

Question - What access list number will java look at in order to determine if the packet should be permitted?

---

## Step 9

Define inspection rule for generic tcp and udp inspection

```
Enter ip inspect name borderfw udp timeout 15
Enter ip inspect name borderfw tcp timeout 30
```

## Step 10

Since we defined a java applets will be inspected according to access list 44, now create the standard java access list to permit trusted websites, or deny statements to deny websites that are not trusted.

```
Enter access-list 44 permit 172.32.3.1
Enter access-list 44 permit 172.32.4.0 0.0.0.255
Enter access-list 44 deny any
```

## Step 11

Apply the inspection rule to an interface

```
Enter interface serial 1
Enter ip inspect borderfw out
Enter exit
```

Question - What would happen if we applied our CBAC inspection on the incoming information instead of the outgoing information?

---

## Step 12

Configure logging and audit trail

```
Enter service timestamps log datetime
Enter ip inspect audit-trail (if you want it to run by default)
```

## Step 13

Other configuration information, to help secure our network from intrusion.

```
Enter enable secret ccnp
```

Question - Why would we want to enable the secret password on our firewall?

---

```
Enter no cdp run
Enter interface serial 1
Enter ntp disable
Enter no ip directed-broadcast
Enter no ip proxy-arp
Enter exit
Enter no ip source-route
Enter no service tcp-small-servers
Enter no service udp-small-servers
```

Question - Why are we disabling all of these services on our firewall?

---

Enter CTRL-Z
Enter copy run start

## Step 14

Verifying CBAC

Enter **show ip inspect name borderfw**

Question - What information does the router reply with?

---

Enter **show ip inspect interfaces**

Question - Which interfaces does the router give information on after this command is executed?

---

Enter **show ip inspect all**

Question - What information does this command give you?

---

## Step 15

Debugging CBAC

Enter **ip inspect audit-trail** (if not previously turned on)

Question- What other commands could we use for debugging CBAC?

---

## Step 16

Testing the CBAC.

**From Router-A global configuration**

Enter **ip http server** (to give us a place to surf to on our network for http traffic)
Enter **exit**

Question - If we had not remembered that Cisco routers had a Web interface, what else could we have used in order to get http traffic?

---

**From a workstation on subnet 172.32.2.0**

Ping Router-A

Question - Were you successful?

---

Telnet to Router-A (172.32.4.1)

Question - Were you successful?

---

Question - How did Router-B respond at the console terminal?

---

Open Internet Explorer or Netscape Navigator and surf to Router-A (172.32.4.1)

Question - Were you successful?

---

Question - How did Router-B respond at the console terminal?

---

**From a workstation on subnet 172.32.4.0**

Ping Router-B

Question - Were you successful?

---

Try to telnet to Router-B

Question - Were you successful?

---

Question - Is our Context Based Access Control (firewall) working the way it should be? Why or why not?