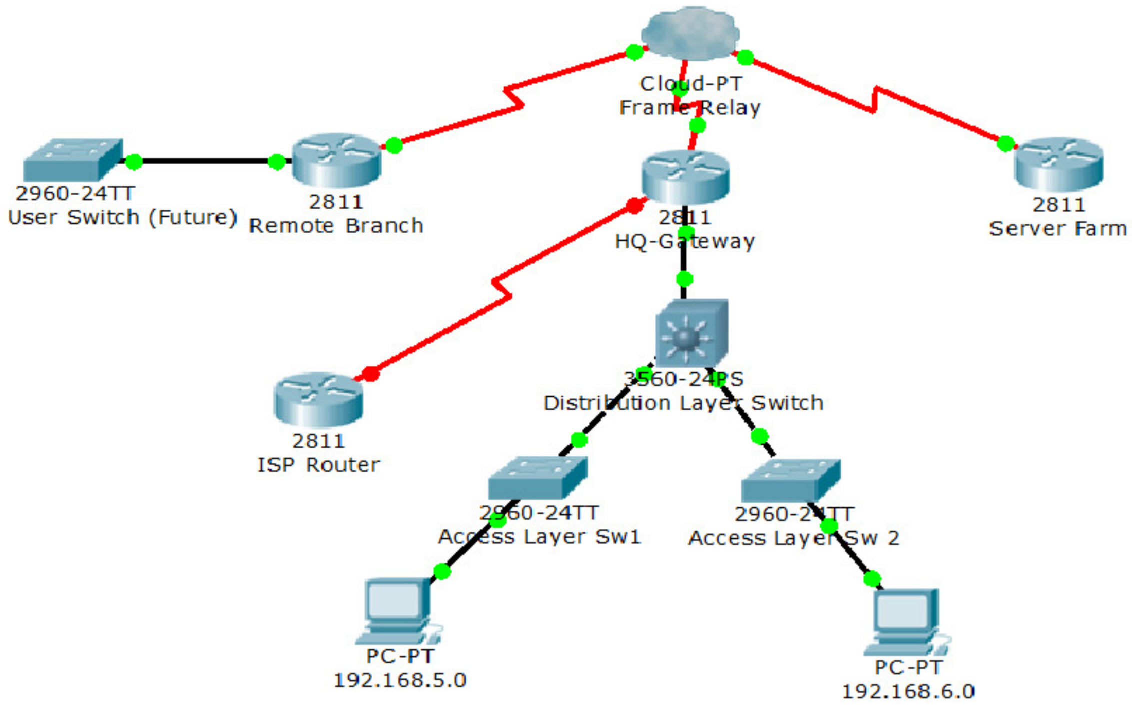
Lab 3 – Network Expansion



BEFORE YOU BEGIN – Clear all router/switch configurations and VLANs using the Introduction Lab as a guide if needed.

For this lab you will need:

- HQ - 3 Internal Subnets (VLANs)
  - VLAN 5 - 192.168.5.0/24
  - VLAN 6 - 192.168.6.0/24
  - VLAN 10 – 192.168.10.0/24 – used for switch and router management.
  - 192.168.1.0/30 Distribution Routing Subnet (GW router to Dist SW)
- 3 External ISP Subnets
  - WAN subnet – 200.200.200.0/30
  - Internet IPs leased from provider – 201.201.201.0/30

    - Internet IPs assigned to ACME.com – 202.202.202.1/32 – test IP

- Frame Relay Subnets
    - 172.32.1.0/30 – Subnet for point to point frame relay to branch
    - 172.32.1.4/30 – Subnet for point to point frame relay to server farm
- Frame Relay DLCIs:
    - Gateway to branch – 403
    - Branch to gateway – 304
    - Gateway to servers – 406
    - Servers to gateway – 604
- Server Farm Subnets
    - 10.1.1.1/24 – Web Server IP
    - 10.1.2.1/24 – Finance Server IP
    - 10.1.3.1/24 – DNS Server IP
- Remote Branch LAN Subnet
    - 192.168.200.0/24
- 6 Routers (2 used for hosts, 1 gateway router, 1 ISP router, 2 WAN Routers)
    - ***You will need to use routers 4 and 5 for the ISP to Gateway connection, using a serial interface***
- 4 Layer 2 switches (1 for Remote Branch)
- Configurations from Lab 1 and 2

Start with a diagram/drawing. In doing this task, you will find what you need for the lab topology based on your pod diagram by figuring out what equipment and ports are needed.

Stuck? Ask your instructor or TA for assistance! This part is a crucial skill that you will need throughout the course.

Important! You may need to adjust your Lab 1 and 2 configurations to accommodate your new topology.

Now that you have your diagram and ports laid out, we can start to configure the devices.

Lab 3 preparation:

Labs 1 and 2 are a pre-requisite for this lab. You will need to start with the configs from lab 2. Edit and re-paste the configurations you used, or start with Lab 1 from the beginning and continue through Lab 2, then start Lab3 when finished.

PART A:

LAN Modifications: (Multi-layer Switching)

In this section of the lab you will move the routing for the HQ VLANs from the gateway router (Router on a stick) to the Distribution Switch (MLS). This will allow for our internal users on VLANs 5 and 6 to route at wire speed, instead of using the router and its processing and CPU.

In this section, you will use these commands, amongst others, for verification in this section:

show ip int brief
show ip dhcp binding
show int gi0/0
show int trunk
show ip route

First, we will move the DHCP Pools to the distribution layer switch.

On the distribution layer switch, copy the DHCP configurations you used for the gateway router. Leave all NAT configurations on the router, you are only moving DHCP.

Use the ***"no"*** commands on the router to remove the DHCP Pools and the DHCP exclude address.

This will allow us to hand out DHCP addresses to our HQ hosts once we move their default gateways to the distribution layer switch.

Second, move the Gateway IP addresses to our distribution layer switch using VLAN Interfaces. (SVIs)

For this step, we will want to remove the "router on a stick" configurations we used in labs 1 and 2. Use the "default" command to accomplish this:

Example:

"***Default interface gi 0/1"***

Once you have defaulted the interface configuration, we will prepare the interface for routing to the switch later in this section. Use the following sample commands to configure your new "routed interface" on the Gateway router. You will need to re-add your ***"ip nat inside"*** command as well. (Your interface may be different)

```
GATEWAY#show run int gi 0/0
Building configuration...

Current configuration : 104 bytes
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
ip nat inside
 !
End
```

On the distribution layer switch, we will need to turn on the routing function on this switch using the ***“ip routing”*** command.

Once routing is enabled, we will place 2 new interfaces on the switch, and also change the IP address of the management vlan.

Use the following sample commands to add the 2 new interfaces for VLANs 5 and 6:

```
DIST1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DIST1(config)#int vlan 6
DIST1(config-if)#ip add 192.168.6.1 255.255.255.0
DIST1(config-if)#no shut
```

Also, change the VLAN 10 (MGMT) IP of this switch to be the default gateway, the .1.

At this point, you should have connectivity to your PCs from the new gateway, and from your PCs to the MGMT IPs of the switches.

Verify using the ping command.

Next, we will bring up the routed connection between the switch and the router. Remember we added the 192.168.1.1/30 IP address to the routers gigabit interface. We will now add the .2 address to the switch interface. We can do this 1 of 2 ways, and in this case we are going to put the IP address directly on the Gigabit interface of the distribution layer switch. Use the ***“no switchport”*** command to turn the layer 2 switchport to a layer 2 “routed” port.

Sample Config:

```
DIST1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DIST1(config)#int gi 0/4
DIST1(config-if)#no switchport
```

```
DIST1(config-if)#ip add 192.168.1.2 255.255.255.252
DIST1(config-if)#no shut
```

Use the ping command to verify connectivity to the gateway router from the switch:

```
DIST1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
DIST1#
```

Ping from a host to your new Gateway IP address, you should be unsuccessful. ***Why?***

```
HOST1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
HOST1#
```

We fail to ping the new router IP because we are now crossing from on router (your gateway) to another. In order to do this, we will need either a default route, or a routing protocol.

Next, we will configure a routing protocol on the distribution switch and the gateway router.

For now, we will use the RIPv2 routing protocol for our LAN infrastructure. The RIP routing protocol using a metric call "hops" to determine a route to a network. A connection between 2 routers will count as one "hop".

We will need to add a network statement for each IP interface we want to "participate" in the RIP routing protocol. The next section is a sample of the router RIP section we will need on the Distribution switch:

```
DIST1(config)#router rip
DIST1(config-router)#version 2
DIST1(config-router)#network 192.168.5.0
DIST1(config-router)#network 192.168.6.0
DIST1(config-router)#network 192.168.10.0
DIST1(config-router)#network 192.168.1.0
DIST1(config-router)#end
```

Note we have one network statement for each network we have on the distribution layer switch. (2 host subnets, one MGMT subnet, and one router subnet)

Now we will need to add RIP routing to the Gateway router. For now, we will only add the network we used to connect to the distribution layer switch:

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#router rip
GATEWAY(config-router)#version 2
GATEWAY(config-router)#network 192.168.1.0
GATEWAY(config-router)#end
GATEWAY#
```

At this point, the RIPv2 routing protocol show be routing for our LAN subnets. We can verify this with the ***“show ip route command”***:

Here is an example of the command on the Gateway router:

```
GATEWAY#show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
    ia - IS-IS inter area, * - candidate default, U - per-user static route
    o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

   192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/30 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R    192.168.5.0/24 [120/1] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
R    192.168.6.0/24 [120/1] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
R    192.168.100.0/24 [120/1] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
GATEWAY#
```

We are not done with the RIP configuration. We will need to add a configuration to the Gateway router to “redistribute” the default route that we setup to get to our ISP from our LAN. We will do this with the “default-information originate” command. This will allow for us to distribute the static default route to the other routers in the environment, like the distribution layer switch.

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#router rip
GATEWAY(config-router)#default-information originate
GATEWAY(config-router)#end
GATEWAY#
```

Verify using the “show ip route” command on the Distribution layer switch:

```
DIST1#show ip ro
```

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

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

C    192.168.5.0/24 is directly connected, Vlan5
C    192.168.6.0/24 is directly connected, Vlan6
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, GigabitEthernet0/4
C    192.168.100.0/24 is directly connected, Vlan100
R*   0.0.0.0/0 [120/1] via 192.168.1.1, 00:00:20, GigabitEthernet0/4
DIST1#
```

Note that we now have a Static route, known via RIP, via the 192.168.1.1 IP address (Our Gateway router)

Verify you have connectivity all the way through our gateway router by pinging our "acme.com" IP of 202.202.202.1 from your host machines.

PART B:

Frame Relay Configuration:

Commands you will use in this section for verification:

- Show frame-relay map
- Show frame-relay pvc
- Show ip route
- ping

Use the following sample configurations to setup the frame relay connections from the gateway router to your branch and server farm routers. These connections will work in a "hub and spoke" topology, where the Gateway router is the hub.

FRS Configuration:

First, on the frame relay switch, we will need to setup the PVCs, using the DLCI numbers provided above. This router will work as a layer 2 frame relay switch, so the configuration will also include that part. The commands you will need to the interfaces are basically stating the following:

"When a frame comes in this interface, on this DLCI, "switch" it to this other interface, on that DLCI."

Here is a sample config for you! Remember your interfaces may vary depending on which routers you used. Use your physical and logical diagrams to map out the proper interfaces.

```
hostname FRS

no ip routing
frame-relay switching

interface Serial1/2
 no ip address
 encapsulation frame-relay
 no ip route-cache
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 304 interface Serial1/4 403
 no shut

interface Serial1/4
 no ip address
 encapsulation frame-relay
 no ip route-cache
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 403 interface Serial1/2 304
 frame-relay route 406 interface Serial1/6 604
 no shut

interface Serial1/6
 no ip address
 encapsulation frame-relay
 no ip route-cache
 clock rate 64000
 frame-relay intf-type dce
 frame-relay route 604 interface Serial1/4 406
 no shut
```

Now that we have done the work of the "internet service provider's" side of the frame relay, we will need to work on the "customer" side of the links.

Remember we are using a "hub and spoke" topology for our frame relay. We will make use of sub-interfaces for a few different reasons for now. Reason 1, on the gateway router we will have 2 frame relay connections, with only one physical interface. Reason 2, we will want some room for expansion later on for the branch and server farm routers. (See challenge section)

Branch and Server Routers:

On the branch and server farm routers, configure a frame relay sub-interface to connect back to the gateway router. Note the use of *the Interface DLCI command*. This command allows us to use a

dynamic style to setup our frame-relay mapping. The mapping includes a DLCI to an IP address. "Mapping" layer 2 to layer 3 addressing.

The following configurations set the encapsulation type to frame relay, sets the interface DLCI, and dynamically sets a mapping of that DLCI to the interface IP. Note that we set the encapsulation to frame relay on the physical interface, since all sub-interfaces would have to be the same encapsulation type. Since this is the DTE side of the connection for both frame relay and the physical layer, we will not need a clock rate command.

Example:

```
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
!
interface Serial0/0/0.304 point-to-point
 ip address 172.32.1.2 255.255.255.252
 frame-relay interface-dlci 304
```

Note that the DLCI here matches what is configured on the physical interface of the FRS connected to this router. These are called "locally significant" DLCIs, and need to match on the switch and router for the PVC to be established.

Perform the same setup for both the branch and server farm routers, using the correct IP addresses and DLCIs.

Gateway Router:

Now you will need to setup your Gateway router for the sub-interfaces to both the branch and server routers. Just as you did in the steps above, except now you will have 2 sub-interfaces, one for each neighbor.

Here is a sample configuration:

```
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 no clock rate 2000000
 !
!
interface Serial0/0/0.403 point-to-point
 ip address 172.32.1.1 255.255.255.252
 frame-relay interface-dlci 403
!
interface Serial0/0/0.406 point-to-point
 ip address 172.32.1.5 255.255.255.252
 frame-relay interface-dlci 406
```

Note that we have one sub-interface for each router. We have now configured the frame relay switch, and all three routers. We can now verify our configurations. Here are some example outputs from a few verification commands, with explanations:

Notice with a ***"show frame-relay pvc"*** command that we see 2 Active PVCs on the Gateway Router*. If you do not see 2 active PVCs, troubleshoot your connections using a layered approach, and check your configurations.*

```
GATEWAY#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          2            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0
<Output Omitted>
```

Notice with the ***"show frame-relay map"*** command, we have dynamic mappings, shown here with the broadcast keyword.

```
GATEWAY#show frame-relay map
Serial0/0/0.403 (up): point-to-point dlci, dlci 403(0x193,0x6430), broadcast
          status defined, active
Serial0/0/0.406 (up): point-to-point dlci, dlci 406(0x196,0x6460), broadcast
          status defined, active
GATEWAY#
```

Ping both of the new connections and make sure you have layer 3 connectivity over the new links.

Remote Branch Configuration:

Now that we have established frame Relay to the new routers, we will need to setup the sites.

You will use a "router on a stick" setup for your branch office.

Use the following steps like you have done in previous labs to accomplish this task:

- Setup the switch with a hostname (ex. BRAN-SW)
- Setup a trunk between the router and the switch to carry traffic for the new end user VLAN, 100
- Setup the rest of the switch to have access ports in the new VLAN (interface range command)
- Shutdown any ports connected to any other switch or router in the lab, we don't want any configuration leaks (Spanning tree, VTP, etc.)
- Every port should use spanning tree portfast, and be statically set as an access port.
- Setup the interface on the router to be the gateway for your new EU VLAN.

Add RIP routing for your branch.

Now that you have your frame relay and LAN segments set up on your new branch, it is time to setup routing so your branch end users can get back to HQ. You will need to add your new network to the Gateway Router, and setup RIP version 2 on the branch.

Remember, we can use the “show ip int brief” command to help with what network statements we will use in RIP. For example, if I see 2 interfaces in the “show ip int brief command, and I want both of them to be routed, setup a network statement for each network.

Here is an example:

```
BRANCH-RT#show ip int brie
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/1.100 192.168.100.1   YES manual up                    up
Serial0/0/0            unassigned      YES manual up                    up
Serial0/0/0.304        172.32.1.2      YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
```

```
BRANCH-RT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BRANCH-RT(config)#router rip
BRANCH-RT(config-router)#version 2
BRANCH-RT(config-router)#network 192.168.100.0
BRANCH-RT(config-router)#network 172.32.0.0
BRANCH-RT(config-router)#passive-interface gigabitEthernet 0/1
BRANCH-RT(config-router)#end
BRANCH-RT#
```

We can also tell RIP not to send any RIP updates out the Ethernet interface, since there is no router on the other end. We do this with the “passive-interface” command.

We now have to add our serial link network to the gateway routers RIP configuration, so it knows to send RIP updates to us. Add the network statement that is needed on the Gateway router, using your knowledge about RIP network statements and the example above.

We can now verify our routing using the “show ip route” command:

```
BRANCH-RT#show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
Gateway of last resort is 172.32.1.1 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 172.32.1.1, 00:00:11, Serial0/0/0.304
      172.32.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.32.1.0/30 is directly connected, Serial0/0/0.304
L        172.32.1.2/32 is directly connected, Serial0/0/0.304
R        172.32.1.4/30 [120/1] via 172.32.1.1, 00:00:11, Serial0/0/0.304
R     192.168.1.0/24 [120/1] via 172.32.1.1, 00:00:11, Serial0/0/0.304
R     192.168.5.0/24 [120/2] via 172.32.1.1, 00:00:11, Serial0/0/0.304
R     192.168.6.0/24 [120/2] via 172.32.1.1, 00:00:11, Serial0/0/0.304
      192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.100.0/24 is directly connected, GigabitEthernet0/1.100
L        192.168.100.1/32 is directly connected, GigabitEthernet0/1.100
BRANCH-RT#
```

Note that we now see all advertised routes for HQ on the Branch router. Verify you see the branch routes on the Gateway router as well.

Server Farm Configuration:

We will now setup our server farm router like our branch router, with one exception. Since we have not setup a switch in this environment yet, we will **"simulate"** the LAN addresses that will be used by the server VLANs with loopback addresses. Use the following list of instructions to setup your environment:

- For each server subnet listed at the beginning of the lab (IP section), setup a loopback interface using the gateway of each subnet for an IP
- Add the RIP routing protocol for your Server Farm Router, include all IP subnets to be routed. (Passive Interfaces should be employed where necessary)
- Adjust RIP routing statements on the Gateway router as necessary

Verify your configurations:

- **Perform a show IP route on the Server Farm Router**
- **Use a ping sourced from your WWW network loopback interface to one of your hosts at HQ. Also, ping the Ethernet of the branch router from the same source.**

Example:

```
SERVER-FARM#show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 172.32.1.5 to network 0.0.0.0
```

```
R*    0.0.0.0/0 [120/1] via 172.32.1.5, 00:00:01, Serial0/0/0.604
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.1.1.0/24 is directly connected, Loopback1
L        10.1.1.1/32 is directly connected, Loopback1
C        10.1.2.0/24 is directly connected, Loopback2
L        10.1.2.1/32 is directly connected, Loopback2
C        10.1.3.0/24 is directly connected, Loopback3
L        10.1.3.1/32 is directly connected, Loopback3
      172.32.0.0/16 is variably subnetted, 3 subnets, 2 masks
R        172.32.1.0/30 [120/1] via 172.32.1.5, 00:00:02, Serial0/0/0.604
C        172.32.1.4/30 is directly connected, Serial0/0/0.604
L        172.32.1.6/32 is directly connected, Serial0/0/0.604
R     192.168.1.0/24 [120/1] via 172.32.1.5, 00:00:02, Serial0/0/0.604
R     192.168.5.0/24 [120/2] via 172.32.1.5, 00:00:03, Serial0/0/0.604
R     192.168.6.0/24 [120/2] via 172.32.1.5, 00:00:03, Serial0/0/0.604
R     192.168.100.0/24 [120/2] via 172.32.1.5, 00:00:03, Serial0/0/0.604

SERVER-FARM#ping 192.168.5.6 source 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.6, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
SERVER-FARM#
```

Not seeing RIP routes? Make sure you are advertising your correct subnets with the ***“Network”*** command in RIP on both sides.

NAT Configuration Modification:

At this point you will need to modify your NAT configuration so that the branch users and your server farm networks can use the external IP address pool for NAT.

You should complete this task by adding your new IP ranges for these networks to the access control list used by NAT, and add any inside NAT interfaces that are necessary.

Use a ping sourced from the loopback addresses that represent these IP addresses.

Here is an example:

```
SERVER-FARM#ping 202.202.202.1 source 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.202.202.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms
SERVER-FARM#
```

Now we will setup a static NAT for an outside user to be able to get to our WWW server. We will use the loopback IP for the WWW network to accomplish this task.

Static NAT for your WWW server:

Create a static NAT mapping for your web server, an outside to inside translation. Use the IP address you used for your loopback on the gateway router. We will use a static mapping that ONLY forwards port 80 requests to our www server. Here is an example:

ip nat outside source static tcp 201.201.201.1 80 10.1.1.1 80 extendable

You will need the “extendable” keyword so this translation can be used by more than one outside user.

Below you will see a before and after output from a telnet from the ISP router to the new IP translation, notice that instead of being unreachable, we now are connecting to the Server Farm Router, it is now refusing the connection instead of timing out:

Before:

```
ISP#telnet 201.201.201.1 80
Trying 201.201.201.1, 80 ...
% Connection timed out; remote host not responding
```

After:

```
ISP#
ISP#telnet 201.201.201.1 80
Trying 201.201.201.1, 80 ...
% Connection refused by remote host
```

PART C:

ACL Configuration:

At this point, we want to setup some security in our environment. We want to make sure that users from the outside can only get to port 80 on our web server. All other ports should be closed to the outside.

We will setup an access list on our serial interface connected to our ISP that will only allow port 80 connections to the outside IP of 201.201.201.1. This is the one we setup for our www. We will need to make sure though that all other traffic is allowed back in to our hosts, ONLY if it was first established from the inside. In other words, if a user wants to get to that acme.com site, we will want that traffic to be allowed back in. We will use inspection to accomplish this.

First, we will setup an extended access list called internet-in. We will apply this ACL to all traffic coming in from the internet. Make sense?

This ACL is very simple. It reads; allow port 80 traffic to 201.201.201.1 from anywhere, and deny everything else:

```
ip access-list extended INTERNET
 permit tcp any host 201.201.201.1 eq www
```

Note there is an implicit ***"deny ip any any"*** at the bottom of this ACL.

Now let's apply the ACL to our serial interface connected to our ISP for inbound traffic.

```
interface Serial0/0/1
 ip address 200.200.200.2 255.255.255.252
 ip access-group INTERNET in
```

Of course, when we apply this ACL to the internet interface, it will literally deny everything but that port 80 traffic to the specific IP. That is not the desired outcome**. We can test this by applying it and see if we can still get traffic back from the internet to our hosts.**

Example:

```
HOST1#ping 202.202.202.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.202.202.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Now let's add some inspection rules to allow traffic that we initiate from the inside back through. For now, we will apply a configuration that will inspect TCP, UDP, and ICMP. This inspection rule will need to be applied to the traffic leaving the same serial interface.

Here is an example configuration:

```
GATEWAY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GATEWAY(config)#ip inspect name internet-in tcp
GATEWAY(config)#ip inspect name internet-in udp
GATEWAY(config)#ip inspect name internet-in icmp
GATEWAY(config)#int s0/0/1
GATEWAY(config-if)#ip inspect internet-in out
GATEWAY(config-if)#end
```

To test our configurations, try to ping from an internal host or server to the 202.202.202.1 loopback on the ISP router. We can also test the internal connection to the web server with a telnet to port 80.

Not getting expected results? Check configs, use a t-shoot method like “bottom up”, and ask a TA for assistance. Good luck!!!!

Lab Challenges:

Setup a new Frame Relay PVC between your branch and the server farm so they have direct access to each other. Use the next /30 subnet available in the space you used for the other frame relay connections.

Setup all routers and switches to allow telnet access to the management VLAN IPs. Use an ACL to allow connections from the other management IPs only.

Change your telnet setup to use SSH version 2 for authentication. Use local usernames that have strong encryption. (Do this on the VTY lines only!)