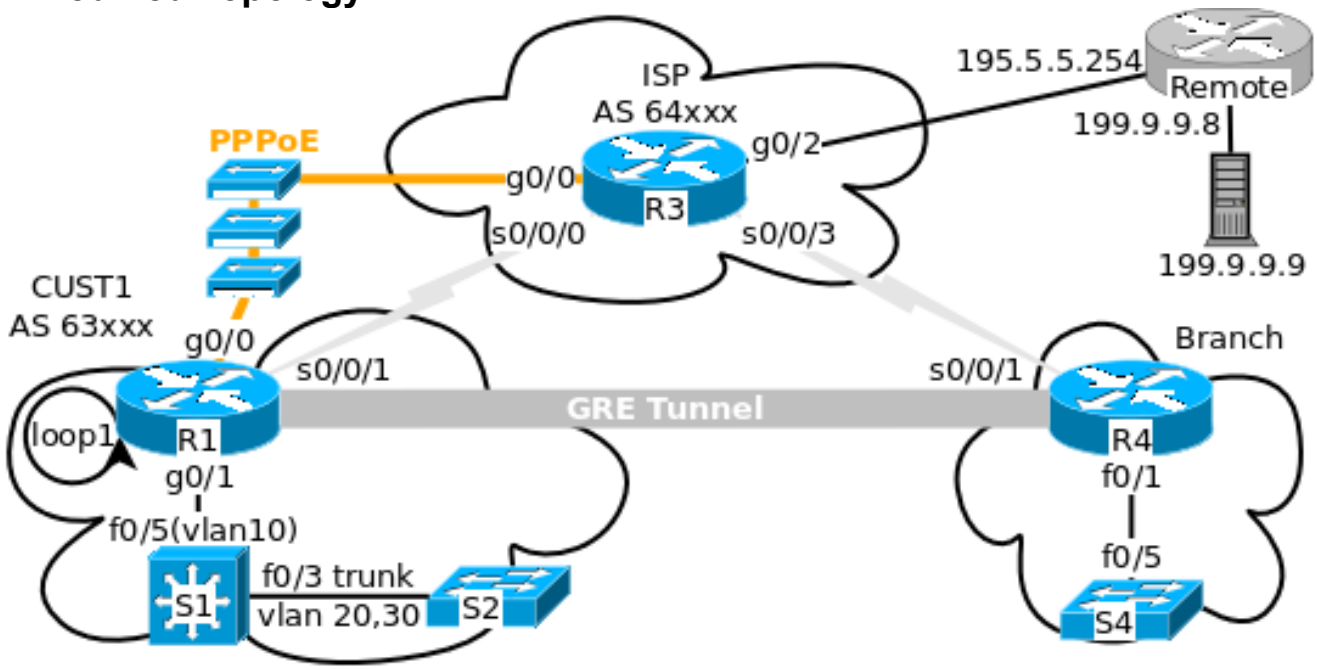
1. Modified Topology:



2. Addressing Table:

Device	Interface	IP Address	Subnet Mask
R1	Gi0/0	PPPoE Client	
	Gi0/1	10.U.1.1	255.255.255.0
	Loop1	205.U.200.49	255.255.255.240
	Se0/0/1	192.168.5.1	255.255.255.252
	Tunnel0	192.168.5.9	255.255.255.252
R3	Gi0/0	PPPoE Provider	
	Gi0/2	195.5.5.U	255.255.255.0
	S0/0/0	192.168.5.2	255.255.255.252
	S0/0/3	192.168.5.5	255.255.255.252
R4	Fa0/1	10.U.4.1	255.255.255.0
	S0/0/1	192.168.5.6	255.255.255.252
	Tunnel0	192.168.5.10	255.255.255.252
S1	vlan 10	10.U.1.5	255.255.255.0
	vlan 20	205.U.200.33	255.255.255.252
	vlan 30	172.30.U.130	255.255.255.192

3. Background / Scenario

Continue with the configuration from Lab5. CUST1 has a PPPoE connection to the ISP; Branch has a GRE tunnel connection to CUST1. The CUST1 AS is expanded to configure S1 as a multi-layer switch and OSPF to route within the AS. Both CUST1 and Branch will implement NAT to provide Internet connectivity for their internal hosts with RFC1918 addresses.

4. Objectives:

a. Configure dynamic routing with OSPF between CUST1 and S1 (interior gateway routing).
b. Configure a discard route.
c. On Branch, configure NAT with overload using the IP address of an the exit interface.
d. On CUST1, configure NAT with overload using a POOL.
e. Use "show ip nat translations" and "debug ip nat" to observe translations.

5. Switch Configurations:

5.1. S4 Configuration:

```
config t
vtp mode transparent
interface range f0/1-24
 shutdown
interface f0/5
 switchport mode access
 switchport access vlan 10
 no shut
end
```

5.2. S2 Configuration:

```
config t
vtp mode transparent
vlan 20
vlan 30
interface range f0/1-24
 shutdown
interface f0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,30
 switchport mode trunk
 no shut
end
```

5.3. S1 Configuration:

a. hostname *username*_L05_S1 (username is your college username)
b. vtp mode transparent
c. Configure telnet on the vty lines.
d. Create vlans 10,20,30
e. Shutdown interfaces f0/1-24
f. Interface f0/5 should be an access port in vlan 10. Bring up the interface
g. Interface f0/3 should be a trunk allowed vlans 20,30. Bring up the interface.
h. Assign SVI IP addresses from the address table.
i. Enable ip routing and configure OSPF area 0. Advertise all directly connected networks.

6. Router Configurations:

6.1. Recover your ISP (R3) router configuration from last week.
   a. Paste the config to R3.
   b. Bring up the physical interfaces used in the topology (g0/0, g0/2, s0/0/0, s0/0/3).
   c. Verify that ISP can ping 199.9.9.9.

6.2. Recover your CUST1 (R1) configuration from last week.
   a. Paste the config to R1.
   b. Bring up the interfaces used in the topology (g0/0, g0/1, s0/0/1)
   c. Verify that CUST1 can:
      - ping 199.9.9.9
      - ping 199.9.9.9 source loop1
      - ping 199.9.9.9 source g0/1

6.3. Recover your Branch (R4) configuration from last week
   a. Paste the config to R4.
   b. Bring up the interfaces used in the topology (s0/0/1, f0/1)
   c. Verify that Branch can ping 199.9.9.9 source f0/1.

7. OSPF and BGP Modifications on CUST1:

7.1. Configure OSPF area 0 on CUST1 as follows:
   a. Route for the g0/1 network.
   b. Propagate the default route.

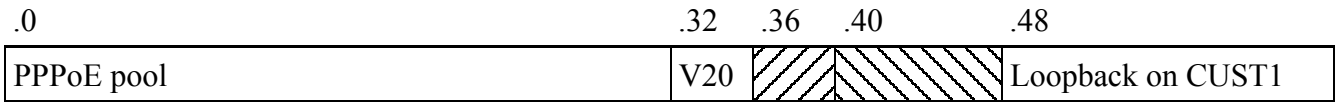
7.2. Verify:
   a. On Cust1: show ip ospf nei — S1 should be a neighbour
   b. On Cust1: sh ip route ospf — Cust1 should have ospf routes to the vlan 20 and 30 nets
   c. On S1: sh ip route — S1 should have a default route learned via OSPF (O*E2)

7.3. Modify the BGP configuration on CUST1:
   a. Branch1 will not run BGP so delete the neighbour statement for Branch1.
   b. CUST1 should not advertise the RFC1918 networks. Delete the network statement for the 10.x.x.x network.
   c. BGP can advertise any network that appears in the routing table. This includes directly connected networks AND networks learned via OSPF.
      - Verify that CUST1 has routes to all vlans on S1. (vlan 10 directly connected, vlan 20 and 30 via OSPF)
      - Only vlan 20 is a public network. Configure BGP on CUST1 to advertise this network.

7.4. Verify:
   a. ISP should not have routes to any of the 10.x.x.x networks.
   b. ISP should have routes to the loopback network on CUST1 and the vlan 20 network on S1.
   c. On S1: ping 199.9.9.9 source vlan 20. The ping should succeed.

8. Discard route #1.

Recall: In sem3, you observed discard routes with EIGRP. When EIGRP advertises a supernet, it creates a route to null 0 so that data to unreachable subnets is discarded instead of being forwarded via a default route. In this topology, Remote has a route to the 205.U.200.0/26 network and some of that address space is unallocated



8.1. Verify that a routing loop exists because of the the static / default routing on Remote and ISP.
   a. On CUST1: configure ssh version 2:`(config)# ip ssh version 2`
   b. On CUST1: ssh to 199.9.9.9 `#ssh -l cisco 199.9.9.9` (password cisco)
   c. On 199.9.9.9: (traceroute is not installed so you will use tracepath instead)
      - tracepath -n 205.U.200.x where x is the IP address of the dialer on CUST1
        This should succeed.
      - tracepath -n 205.U.200.36
        what devices bounce the ping back and forth?

8.2. On ISP, configure a discard route so that any traffic to unallocated address space in the 205.U.200.0/26 network is discarded instead of routed back to Remote:
```
(config)# ip route 205.U.200.0 255.255.255.192 null0
```

8.3. Verify:
   a. that the TFTP server can still ping 205.U.200.x (x is the ip address of dialer 1 on CUST1)
   b. that a ping from the TFTP server to 205.U.200.36 fails at the ISP.

8.4. Exit from the ssh session on the TFTP server.

9. Routing and NAT with overload on Branch:

9.1. Update the routing configuration:
   a. Delete the BGP routing configuration on Branch.
   b. Configure a default route on Branch via the tunnel.

9.2. Configure NAT with overload translating to the IP of the exit interface (tunnel 0).
   a. **Ignore the serial interface**. It is configured only to establish the GRE tunnel.
   b. Configure the inside and outside interfaces where the inside interface connects to the Branch LAN and the outside interface connects to the upstream CUST1 router.
   c. Configure access-list 1 to permit the inside addresses that should be translated.
   d. Configure the translation rule to implement NAT with overload translating to the address of the exit interface (tunnel 0).

9.3. Configure telnet to use the IP address of f0/1 as the source IP:
   a. (config)# ip telnet source-interface f0/1
   b. Verify: Branch can telnet to S1 vlan 20 (205.U.200.33) source f0/1
   c. Verify: Branch can telnet to S1 vlan 20 (205.U.200.33) [should use ip of f0/1 as the source]

9.4. # show ip nat translations and find the translation for the tcp telnet connection:
recall: Translations timeout. If the translation table is empty, repeat the telnet and check again.
   a. record the source IP address (inside local)
   b. record the source port (inside local port)
   c. record the translated src ip (inside global)
   d. record the translated src port (inside global)

10.Configure NAT with a pool and overload on CUST1:

10.1. Some of the interfaces connected to CUST1 and S1 have public IP addresses. These interfaces should already have connectivity to external hosts. Verify:
   a. CUST1 can ping 199.9.9.9 source loop1
   b. S1 can ping 199.9.9.9 source vlan 20

10.2. List all of the interface and the associated networks on CUST1 and S1 which have RFC1918 addresses and no connectivity to external hosts (Again, ignore s0/0/1 which is only configured to establish the GRE tunnel)

	Interface	Network	Mask	Wildcard Mask
R1				
S1				

10.3. Configure the outside interface connecting from CUST1 to ISP. Since NAT operates at the network layer, the exit interface must be an interface with an IP address.

10.4. Configure the inside interfaces (**ignore s0/0/1**).
   a. Which interfaces on CUST1 have RFC1918 addresses? _____
   b. Are there additional interfaces on CUST1 connect to downstream hosts with RFC1918 addresses. (Downstream hosts are hosts which must travel through CUST1 to get to ISP, Remote, and the TFTP server)? ___

10.5. Configure access-list 2. It should permit **all** of the RFC1918 networks connected to R1 or S1.

10.6. Configure the NAT pool.
   a. Call the pool NATPOOL
   b. The pool should include all of the usable addresses in the 205.U.200.40/29 subnet.

10.7. Configure the translation rule with overload to translate addresses permitted by access-list 2 to an address from the pool.

10.8. On CUST1:
   a. debug ip nat
   b. Verify that the source IP address is translated when CUST1 pings 195.5.5.U source g0/1
   c. Even though CUST1 is translating the address, the ping should fail. Explain why.

10.9. On CUST!: configure BGP to advertise the NATPOOL
   a. Add a network statement for the 205.U.200.40/29 subnet.
   b. eBGP will only advertise a network specified with a mask if there is a route to the network in its routing table. But the pool is not part of a network assigned to a physical interface. So this becomes a 2nd use for a discard route. Still on CUST1, configure a discard route to the 205.U.200.40/29 subnet.

10.10. Check the routing table on ISP. Verify that there is a route to the 205.U.200.40/29 subnet learned via BGP.

10.11. Verify connectivity:
   a. on S1: ping 199.9.9.9 source vlan 20 Does this connection use NAT on CUST1? ____
   b. on S1: ping 199.9.9.9 source vlan 30 Does this connection use NAT on CUST1? ____
   c. on Branch: ping 199.9.9.9 Does this connection use NAT on CUST1? ____
   d. on Branch: ping 199.9.9.9 source f0/1 Does this connection use NAT on CUST1? ____

10.12. The last ping from Branch source f0/1 actually does double NAT. Document the translations:
   a. on CUST1 and Branch: `# clear ip nat translation *`
   b. on Branch: `# ping 199.9.9.9 source f0/1`
   c. on CUST1 and Branch: `# show ip nat trans`
   d. Record the changes to the source IP address as the icmp echo-request travels to 199.9.9.9.

	source IP address	destination IP address
original ping		
after translation on Branch		
after translation on CUST1		

11. TFTP uploads:

11.1. Upload the config files for ISP, CUST1, Branch, and S1 to 199.9.9.9.

12. If you want to verify the uploads.

12.1. ON ISP:

```
(config)# ip ssh version 2
(config)# end
ssh -l cisco 199.9.9.9   (login with password cisco)
ls -l /var/lib/tftpboot/username* (your college username)
exit
```

13. Cleanup:

13.1. On all your devices:

```
erase startup-config
reload    (do NOT save)
```