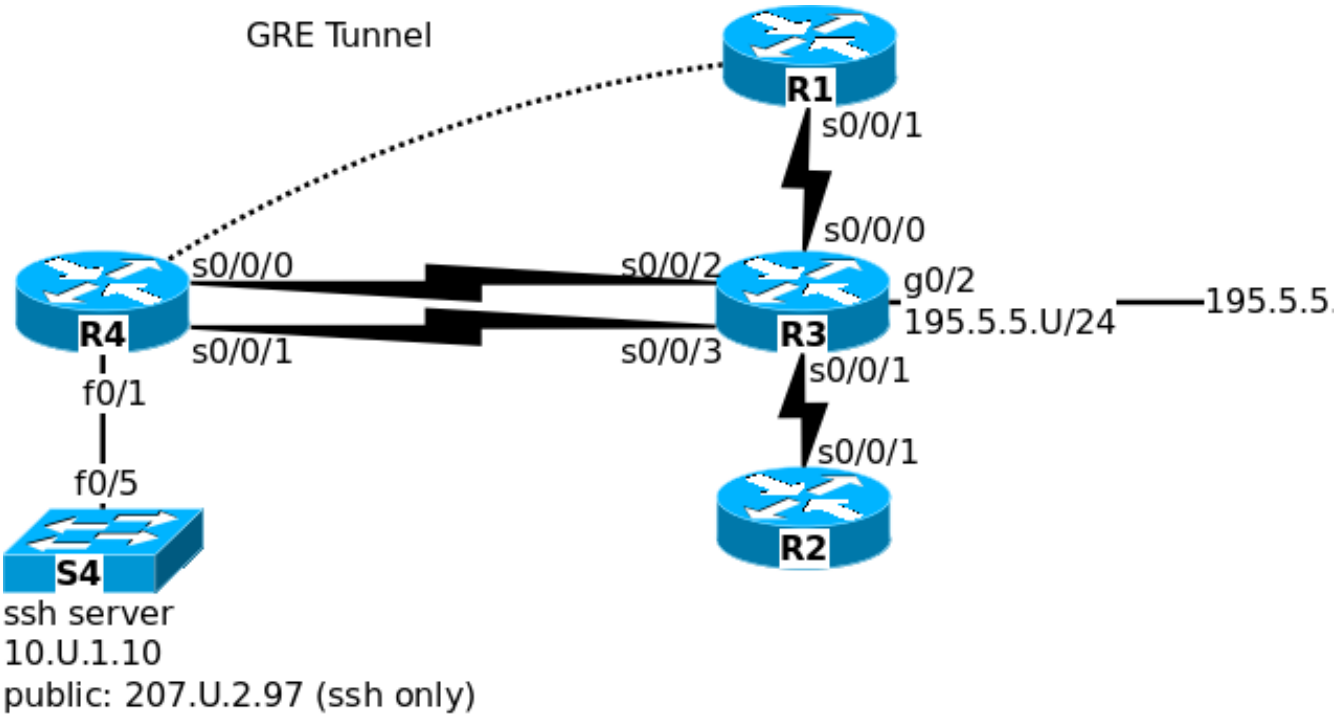
1. Topology



2. Addressing:

R3	g0/2	195.5.5.U / 24	R4	multilink1	207.U.1.2 / 30
	multilink1	207.U.1.1 / 30		f0/1	10.U.1.1 / 24
	s0/0/1	207.U.2.1 / 30		tunnel 1	source **multilink1**, destination 208.U.2.2, mtu (1500 - gre header) ipv6 2001:db8:208:U::2/64
	s0/0/0	208.U.2.1 /30		NatPool	207.U.2.100 - 207.U.2.110 / 28
R2	s0/0/1	207.U.2.2 / 30			
	f0/1	172.20.U.1 / 24			
R1	s0/0/1	208.U.2.2 /30	S4	vlan 10	10.U.1.10 / 24
	tunnel 1	source s0/0/1 destination 207.U.1.2 ipv6 2001:db8:208:U::1/64 mtu (1500 - gre header)			

3. R3 Configuration:

3.1. R3 configuration starts with the configuration from Lab7.

a. Hostname username_L08_R3

b. Standard setup: vtp mode transparent, enable secret class, no ip domain lookup, logging sync on the console, telnet on the vty lines)

c. Addressing: assign addresses as specified (including new interface s0/0/0)
d. The multilink connection from R3 to R4 should use 1-way chap authentication (R3 server) R4 should login with username Router4 password cisco.
e. The serial link from R3 to R2 should use PPP encapsulation with 1-way PAP authentication (R3 server). R2 should login with username Router2 password cisco.
f. The additional serial link from R3 to R1 should use HDLC encapsulation
g. Static route: Create a static route to the R4 NAT pool
h. Dynamic Routing: Route with EIGRP AS 20.
Advertise all directly connected networks including the new s0/0/0 network.
Redistribute the static route to the NAT Pool.

3.2. R2 Configuration:
a. hostname username_L08_R2
b. Standard setup: vtp mode transparent, enable secret class, no ip domain lookup, logging sync on the console, telnet on the vty lines)
c. ip addresses from the address table
d. Default route: configure a default route via the serial interface.

3.3. R1 Configuration:
a. hostname username_L08_R1
b. Standard setup: vtp mode transparent, enable secret class, no ip domain lookup, logging sync on the console, telnet on the vty lines)
c. ip addresses from the address table
d. Dynamic routing with EIGRP AS 20.

3.4. R4 Configuration with the configuration from Lab 7 (S2 is gone but you will not be penalized for configuration to S2 LAN).
a. Standard setup (hostname username_L07_R4, enable secret class, no ip domain lookup, logging sync on the console, telnet on the vty lines)
b. Configure addressing from the table including the GRE tunnel to Remote and the multilink interface with 1-way chap authentication from step 4.4.
c. Routing:
d. R4 should have a default route via R3 in exit interface format
e. R4 should have a host route (/32) to the DNS server 198.8.8.8 via the tunnel in exit interface format.
f. R4 should implement NAT with overload:
g. traffic going to the DNS server should NOT use NAT
h. Implement PAT with the NatPool for all other traffic coming from the S4 LAN going to the outside world.
i. R4 should implement port forwarding.
j. ssh connections to 207.U.2.97 port 22 should be forwarded to the ssh server on S4.

3.5. S4 Configuration:
a. Same as L07.
b. Shutdown all interfaces f0/1-24 first.
c. Paste L07 config.
d. No shut f0/5 and int vlan 10.

4. Connectivity testing:

4.1. On R4:
   a. # debug ip nat
   b. R4 should be able to ping 199.9.9.9. You should not see any NAT translations.
   c. R4 should be able to ping 199.9.9.9 source f0/1. You should see NAT translations.
   d. R4 should be able to ping 2001:db8:208:U::1. You should not see NAT translations although you may see GRE messages.
   e. R4 should be able to ssh to S4 (ssh -l cisco 10.U.1.10)
   f. S4 should be able to ping 199.9.9.9. You should see NAT translations on R4.
   g. S4 should be able to ping dns.8278.com. You should see GRE. (DNS lookup and ping should travel over the tunnel).
   h. S4 should be able to telnet to R2 using address 207.U.2.2.
   i. R3 should be able to ssh to S4 (ssh -c aes128-cbc -l cisco 207.U.2.97) [see note below about ciphers]

5. Access-list 101.

5.1. Access-list 101 should filter traffic going to R2 (and S3 if it was configured).. You want to place this access-list on one device and one interface.
   a. Which is the best device to code the access-list? _____
   b. Which is the best interface to code the access-list? ____
   c. What direction (in/out) should you code the access-list.

5.2. Requirements. Code and apply access-list 101.
   a. deny telnet to 207.U.2.2 port.
   b. all other traffic should be allowed.

5.3. Test the access-list.
   a. From R4, verify that you cannot telnet to 207.U.2.2
   b. From R4, verify that you can ping 207.U.2.2
   c. From R2, verify that you cannot telnet 207.U.2.2
   d. From R2, verify that you can ping 207.U.2.2.

5.4. Verify matches and upload your ACL.
   a. show access-lists
      Verify that you have matches against all entries in the ACL.
   b. TFTP upload your ACL.
      show access-lists | redirect tftp://199.9.9.9/*username*.acl1

6. Access-list 102.

6.1. Access-list 102 should be configured on R3 to filter traffic going to R1.
   a. Which is the best interface to code the access-list? ____
   b. What direction (in/out) should you code the access-list.

6.2. Requirements. Code and apply access-list 102 on R3.
   a. Permit telnet to 208.U.2.2
   b. Explicitly deny all other traffic.

6.3. Test the ACL.
   a. From R4, verify that you cannot ping 208.U.2.2
   b. From R4, verify that you can telnet to 208.U.2.2

6.4. Verify matches. # sh access-lists

7. Access-list 102 on R1:

7.1. Code the same acl 102 on R1 to permit telnet to 208.U.2.2 and deny all other traffic.

7.2. Apply the ACL on s0/0/1.
   a. Which direction? _____
   b. Apply the ACL?
   c. Wait 30 seconds and view the console log messages on R1.
   d. Which necessary traffic is denied.
   e. Modify ACL 102 on R1 to allow the additional required traffic.

7.3. Why does the ACL on R1 require an extra entry when the same ACL on R3 did not?

7.4. Verify matches and upload the R1 ACL.
   a. show access-lists
      Verify that you have matches against all entries in the ACL.
   b. TFTP upload your ACL.
      show access-lists | redirect tftp://199.9.9.9/*username*.acl2

8. 3rd Access-list requirements.

8.1. R3 will control the traffic leaving and entering R4 and S4 (plus any PCs in vlan 10 which might be connected to S4 at some future time.

8.2. **On R3**, create 2 named extended ACLs
(config)# ip access-list extended IN3
99 deny ip any any
(config)# ip access-list extended OUT3
99 deny ip any any
Recall: every extended acl already end with an implicit "deny ip any any".
Coding the rules explicitly lets you see the count of the number of frames dropped.

8.3. Apply IN3 inbound on s0/0/2 on R3.
Apply OUT3 outbound on s0/0/2 on R3.

8.4. Remember that traffic is normally bidirectional. When you allow traffic in one direction, you must reverse your rule to allow the reply in the opposite direction.

9. Code ACE 10 to allow icmp echo-request traffic from anywhere to 199.9.9.9 and the echo-replies to return.

	action	protocol	source	destination	qualifier
IN3 10					echo
OUT3 10					echo-reply

9.1. #show access-list

9.2. Verify that S4 can ping **199.9.9.9**

9.3. Verify that S4 cannot ping 195.5.5.254

9.4. # show access-list Verify that the counters for ACE's 10 and 99 increased.

10. Code ACE 20 to allow http from hosts in the S4 network to any http server (port 80). When coding the S4 network, remember that R4 is doing NAT.

	action	protocol	source net	source port	dest net	dest port	qualifier
IN3 20							
OUT3 20							established

10.1. Let me emphasize: ACLs are NOT connection-tracking
The established parameter does NOT mean that the router is tracking the session.
The established parameter can only be used for TCP connections.
The established flag only checks to see that the ACK or RST flags are set.
This can be spoofed very easily.

10.2. # show access-list

10.3. Verify that S4 can telnet 199.9.9.9 80
This will test tcp connectivity to the http port

10.4. Verify that R4 cannot telnet 199.9.9.9 80

10.5. # show access-list Verify that the counters for ACE's 20 and 99 increased.

11. Code ACE entries 31,32,33 ... to allow telnet from hosts in the S4 network to any telnet server in the 195.5.5.5 network except for 195.5.5.254.

telnet to the 195 address on R3 should work.
telnet to the 195 address on your neighbour's R3 should work
telnet to 195.5.5.254 should fail

When coding the S4 network, remember that R4 is doing NAT.

	action	protocol	source net	source port	dest net	dest port	qualifier
OUT3 30							established

11.1. # show access-list

11.2. Verify that S4 can telnet 195.5.5.U

11.3. Verify that S4 cannot telnet 195.5.5.254

11.4. Verify that R4 cannot telnet 195.5.5.254

11.5. # show access-list Verify that the counters for ACEs increased.

12. Add a UDP entry: Code ACE entries 40 to allow syslog messages from R4 to 199.9.9.9.

syslog is one of a very small handful of protocols which sends traffic and does not get a reply

	action	protocol	source net	source port	dest net	dest port	qualifier
IN3 40							

12.1. # show access-list

12.2. on R4: (config)# logging 199.9.9.9

12.3. on R4: (config)# end

12.4. The log messages that appear on your console screen will also be sent to 199. If you don't have log messages, enter config mode and exit back to privileged exec.

12.5. # show access-list Verify that the counters for ACEs increased.

13. Code ACE 50 to allow ssh from R3 to S4.

Remember that R4 is port-forwarding. Remember also that this time an outside host is initiating the connection.

	action	protocol	source net	source port	dest net	dest port	qualifier
IN3 50							
OUT3 50							

13.1. # show access-list

13.2. Verify that R3 can ssh to S4 using the public IP address.

13.3. # show access-list

a. Verify that the counters for ACE 50 increased in IN3
b. The counters for ACE 50 in OUT3 will not change. Why not?

14. Add a final set of entries: Code ACE entries 60 to R4 to ping over the tunnel: ping 2001:db8:208:U::1

Remember that this traffic is traveling over the GRE tunnel. We did an encapsulation exercise last week where we talked about encapsulation with GRE.

	action	protocol	source	dest	qualifier
IN3 60					
OUT3 60					

14.1. # show access-list

14.2. on R4: (config)# ping 2001:db8:2008:U::1

14.3. # show access-list Verify that the counters for ACEs increased.

14.4. R4 is pinging an IPv6 address. Why does an IPv4 ACL on R3 filter the ping?

15.TFTP upload:

15.1. Upload your R3 config to 199.9.9.9

15.2. #show access-lists

a. Verify that you have matches against every line in your ACLs. (with the possible exception on lines 50 and 99 in OUT3). Marks are split between configuration and testing. You will not get the testing marks if your ACL has not recorded the testing matches.
b. If you have ACL lines without matches, redo the appropriate test.
c. If you modified the ACL, reupload your config file for R3.

15.3. TFTP upload your ACL from R3.
show access-lists | redirect tftp://199.9.9.9/*username*.acl3

16.Erase startup-config on all devices.