

- The first step is to familiarize yourself with “screen”. Type “screen” at the Linux prompt, read the instructions, and hit Enter. Then you can type “Ctrl+A” followed by different letters to do different things. E.g., “Ctrl+A” followed by “c” creates a new shell window, “Ctrl+A” followed by “n” goes to the next window, and “Ctrl+A” followed by “p” goes to the previous window. You'll need to have more than one thing running at once on D-day and screen is usually the easiest way to do that.
- On each of your endpoints, add a 50 kbps rate limit by editing your /etc/network/interfaces to add this right after the configuration for eth0:


```
up tc qdisc add dev eth0 root tbf rate 50kbit latency 50ms burst 1540
```
- On the three interfaces your router has that aren't the NAT/VPN, you should add a delay that is 10ms times the last digit of your LoboID (or 100ms if the last digit is 0). So, for eth1, for example, and with a last digit on my LoboID of 4, I would do:


```
up tc qdisc add dev eth1 root netem delay 40ms
```
- Do a “sudo apt-get install openvpn” and then “man openvpn” on your router. You can run openvpn to connect to the VPN in one of your screens of your router with “sudo openvpn --config netsNN-client.conf”. You should edit your config file to add an ifconfig line after the remote line to set your IP address in the VPN subnet:

```
---snip---
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 64.106.46.58 9011

# The next line is the line you will add, to set your IP in the VPN subnet
# X is 200 plus the VPN number
# Y is 100 plus your group number
ifconfig 192.168.X.Y 255.255.255.0

# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
remote-random
---snip---
```

- You're going to need to reconfigure your subnet numbers and IP addresses so that you and your groupmate adhere to the following scheme, where N is your group number.
 - One of you should have an endpoint at 10.N.1.66 that uses the default TCP cubic congestion control algorithm, and the other of you should have a TCP cubic endpoint at 10.N.4.66.
 - One of you should have an endpoint at 10.N.2.77 that uses the TCP reno congestion control algorithm, and the other of you should have a TCP reno endpoint at 10.N.5.77.
 - To change a machine to use reno, add this line near the top of /etc/sysctl.conf:


```
net.ipv4.tcp_congestion_control=reno
```
- On your router, do a “sudo apt-get install quagga” and follow the instructions that I forwarded from the TA about how to set up BGP on quagga. That email has the configuration files you need to get started attached to it. If you're using the “a” certificate for your group, your AS number should be 65700+N, where N is your group number. If you're using the “b” certificate,

your AS number should be $65800+N$. So, if you're group number 14 and group member 14a, your AS number should be 65714. If you're group number 3 and group member 3b, your AS number should be 65803. Your BGP peers should be: 1) your groupmate's router, 2) all the other students in the VPN you're connecting to (when specifying their AS numbers pay attention to whether they're a or b). We sent out the definitive list of who is in what VPN soon already. If you know what other groups are connecting to the VPN you're in then you can infer their BGP router IP address because they should be following the scheme above, which you should also be following (192.168.X.Y where X is $200 +$ the VPN number and Y is $100 +$ your group number).

- During D-day you should run your server on both endpoints and collect a tcpdump pcap file on all three of your virtual machines. Be sure to try these things out and debug them before D-day.
 - To run your server code, run it in a separate screen. Remember that it should be running on both endpoints. You can use the server code of another student if yours is not fully debugged yet.
 - To run tcpdump, in a separate screen, do “`sudo tcpdump -n -i eth0 -s 65535 -w filename.pcap`”. You should run tcpdump on all three virtual machines, and at the end of D-day you'll turn in three pcap files: yourlastname-reno.pcap, yourlastname-cubic.pcap, and yourlastname-router.pcap. On the router you should grab the pcap on the interface that you use to connect to your groupmate.

Notes:

- If this document conflicts with anything I sent out earlier go by this document rather than the earlier one.
- You'll need to share a physical computer with your groupmate so you can connect to them directly.
- Of the two VPNs assigned to your group, you'll connect to one VPN, and your groupmate to the other.
- You should delete the static route you have with your groupmate and the first thing you should try to get working with BGP is BGP with your groupmate to route to them without a static route rule, i.e., your router should learn about their subnets via BGP. Note that by “delete the static route you have with your groupmate” I mean you should remove any routing rules you have for getting to their subnet. You still need an interface on a subnet you share with them so that your routers can communicate directly.