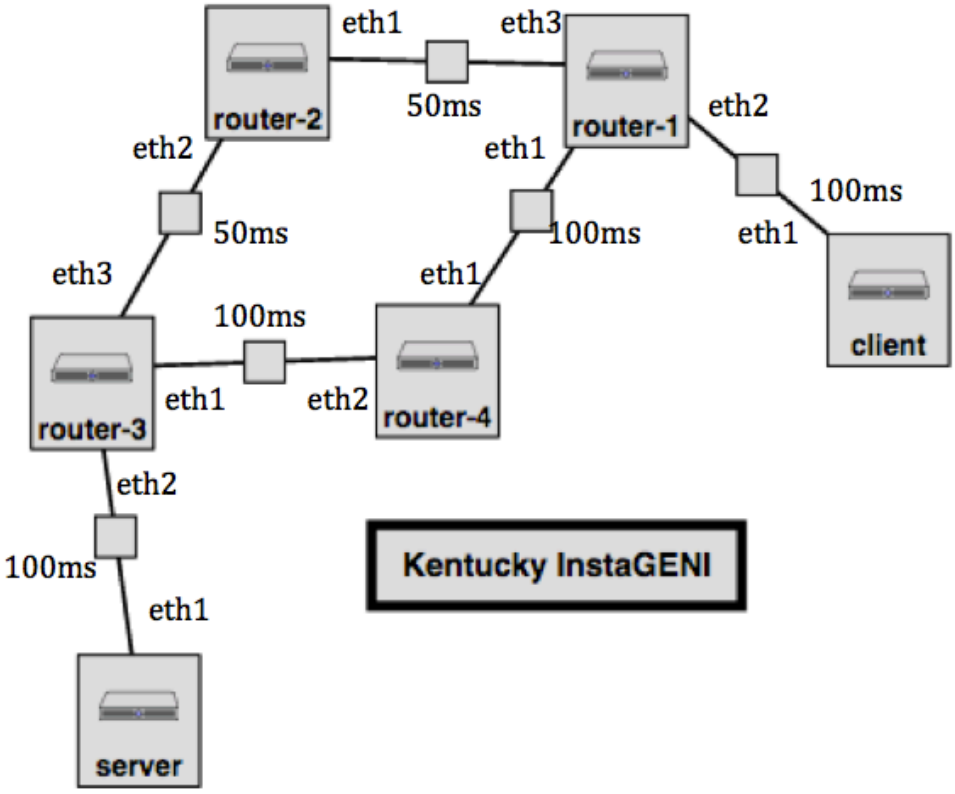
Experiment Details:
Our goal is to study the 1+1 and 1:1/1:N protection scheme for network. As we mentioned above we should set up our topology first (RSPEC code will be in a separate file).

1+1
As in figure, there are two paths from client to server. If we ping server from client, the packets should through 2 paths (P1: client - router1 - ruter2 – router3 – server; P2: client - router1 – ruter4 – router3 – server). We should give latency on each link, so we can easily calculate the RTT of each path, which P1 is 600ms and P2 is 800ms.



on client
sudo tc qdisc add dev eth1 root netem delay 100ms 0ms
on server
sudo tc qdisc add dev eth1 root netem delay 100ms 0ms
on router1
sudo tc qdisc add dev eth1 root netem delay 100ms 0ms
sudo tc qdisc add dev eth2 root netem delay 100ms 0ms
sudo tc qdisc add dev eth3 root netem delay 50ms 0ms
on router2
sudo tc qdisc add dev eth2 root netem delay 50ms 0ms
sudo tc qdisc add dev eth1 root netem delay 50ms 0ms

on router3
sudo tc qdisc add dev eth1 root netem delay 100ms 0ms
sudo tc qdisc add dev eth2 root netem delay 100ms 0ms
sudo tc qdisc add dev eth3 root netem delay 50ms 0ms
on router4
sudo tc qdisc add dev eth1 root netem delay 100ms 0ms
sudo tc qdisc add dev eth2 root netem delay 100ms 0ms

Now, we will show how 1+1 protection scheme works. Since there are 2 paths, the RTT will take the average from both paths. So the RTT should be 700ms. Let's check our result.

on client
ping –c 20 192.168.20.10

```
--- 192.168.20.10 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19000ms
rtt min/avg/max/mdev = 703.198/703.749/707.713/1.077 ms
lw1577@client:~$
```

In this figure, we can find the RTT is as we assumed, which is near 700ms. Now, if we bring router2's eth1 down, the P1 will be failed. So, the packet could only through P2, which makes RTT be 800ms. Let's check the result.

on router2
sudo ifconfig eth1 down
on client
ping –c 10 192.168.20.10

```
lw1577@client:~$ ping -c 10 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_req=1 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=2 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=3 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=4 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=5 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=6 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=7 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=8 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=9 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=10 ttl=61 time=803 ms

--- 192.168.20.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 803.296/803.516/803.778/1.215 ms
lw1577@client:~$
```

From this figure, we can find as we assumption, the RTT becomes 800ms. What if we

bring router2's eth1 up and bring router4's eth1 down? Then P1 will be in good condition and P2 will be failed. Let's check our results by experiments results.

on router2
sudo ifconfig eth1 up
on router4
sudo ifconfig eth1 down
on client
ping –c 10 192.168.20.10

```
lw1577@client:~$ ping -c 10 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_req=1 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=2 ttl=61 time=609 ms
64 bytes from 192.168.20.10: icmp_req=3 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=4 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=5 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=6 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=7 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=8 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=9 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=10 ttl=61 time=603 ms

--- 192.168.20.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9000ms
rtt min/avg/max/mdev = 603.298/604.109/609.004/1.640 ms
```

From our results, it is obviously that the RTT becomes nearly 600ms. This means all the packets through P2, but P1 is failed. What happened if we bring router4's eth1 up and bring router2's eth1 down during the ping period? Let's check the result.

on router4
sudo ifconfig eth1 up
on client
ping –c 10 192.168.20.10
on router2
sudo ifconfig eth1 down

```
lw1577@client:~$ ping -c 10 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_req=1 ttl=61 time=703 ms
64 bytes from 192.168.20.10: icmp_req=2 ttl=61 time=705 ms
64 bytes from 192.168.20.10: icmp_req=3 ttl=61 time=703 ms
64 bytes from 192.168.20.10: icmp_req=4 ttl=61 time=703 ms
64 bytes from 192.168.20.10: icmp_req=5 ttl=61 time=703 ms
64 bytes from 192.168.20.10: icmp_req=7 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=8 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=9 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=10 ttl=61 time=803 ms

--- 192.168.20.10 ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9009ms
rtt min/avg/max/mdev = 703.252/748.204/803.823/49.549 ms
```

We can obviously find the RTT switched from 700ms to 800ms at icmp_req 5 and icmp_req 7 and icmp_req 6 lost. Since only one ICMP packet lost, we may give the conclusion that the recovery cost of 1+1 is very low.

Since the 1+1 protection scheme means the sender sends packets through 2 paths to receiver. If one path failed, packets through another path could reach to the receiver. Since every packet sends out through 2 paths and the receiver will pick one from the packets, the recovery cost of 1+1 protection could be very low. The response to link failure would be very fast. Actually, no additional recovery time needed, the time differences are cost by the different rates between different paths (delay in this experiment). What about the advantage of 1+1 protection? Since each path needs the back up path, this means we need considerable resources for this protection scheme. The cost of network architecture would be really high.

1:1/1:N
1:1 protection scheme means each path will have a backup path. However, the backup path only carries packets when the normal path failed. 1:N protection scheme means N paths share one backup path. The backup path only carries packets when the normal path failed. The experiment will focus on the 1:1 protection scheme.

First, we use the same topology as the 1+1 scheme.
We assume P1 (client - router1 - ruter2 – router3 – server) is the normal path and P2 (client - router1 – ruter4 – router3 – server) is the backup path. Due to our lack experience and limited time in GENI portal, we choose to manually switch P1 to P2 when P1 failed during the ping period.

on router4
sudo ifconfig eth1 down
sudo ifconfig eth1 up(during ping period, after router2's eth1 down)
on client
ping –c 20 192.168.20.10
on router2
sudo ifconfig eth1 down(during ping period)

```
lw1577@client:~$ ping -c 20 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_req=1 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=2 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=3 ttl=61 time=603 ms
64 bytes from 192.168.20.10: icmp_req=4 ttl=61 time=604 ms
64 bytes from 192.168.20.10: icmp_req=17 ttl=61 time=805 ms
64 bytes from 192.168.20.10: icmp_req=18 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=19 ttl=61 time=803 ms
64 bytes from 192.168.20.10: icmp_req=20 ttl=61 time=803 ms

--- 192.168.20.10 ping statistics ---
20 packets transmitted, 8 received, 60% packet loss, time 19096ms
rtt min/avg/max/mdev = 603.361/703.741/805.122/100.128 ms
lw1577@client:~$
```

We can obviously find the RTT switched from 600ms to 800ms between icmp_req 4 and icmp_req 17 and icmp_req 5 to icp_req 16 lost. Since 12 ICMP packets lost, we may give the conclusion that the recovery cost of 1+1 is much higher than 1+1 protection scheme.

In this experiment, we switched to the backup path manually so it may not be as accurate as the real condition. In the real network architecture, the network will take the same steps as we did in this experiment. The network will detect and confirm the path failure and then switch to the backup path. This will takes more recovery time. However, 1:1 protection scheme is still very fast but high resource cost since each path has a backup path. 1:1 takes less network cost as 1+1 since 1:1 only need to send packets to receiver once instead of twice as 1+1 protection scheme.

1:N protection scheme is very like 1:1 the only difference is that N paths share one backup path. So, 1:N may still response to path failure very fast (may slightly slow than 1:1). 1:N may save a lot of network resources but you need to design the network very carefully. Also, if several paths fail, the backup path may get very “crowded” and this causes the network to be “slow”.