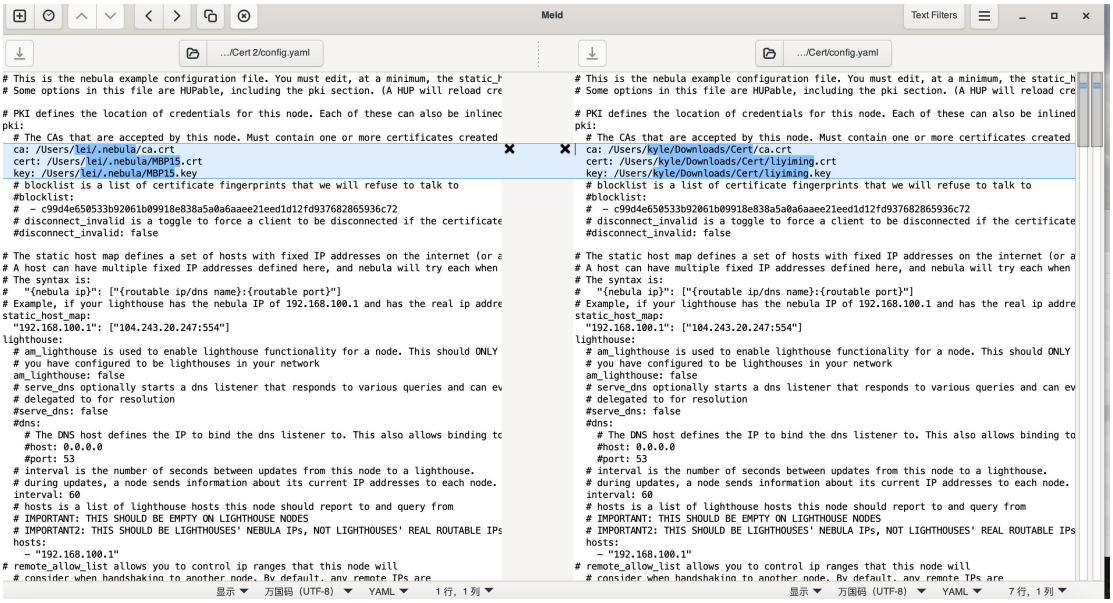
1. Installation of Nebula

```
(base) kyle@Kyles-MacBook-Pro ~ % nebula-cert -version
Version: 1.9.5
```

2. Get the ca.crt liyiming.key liyiming.crt files from the lecture

3. Make my own configuration file for all participating computers and compare with the file from lecture(config.yaml)



Use meld i found that there are only three rows different

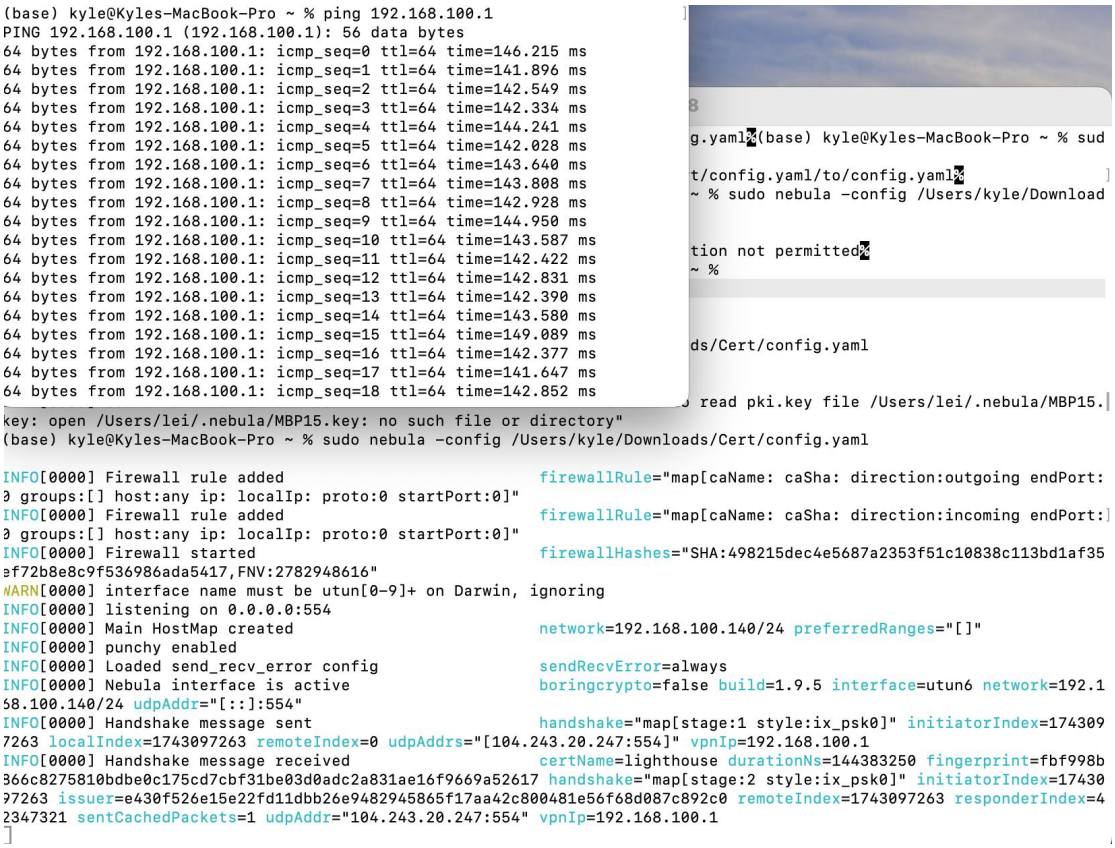
```
pki:
  # The CAs that are accepted by this node. Must contain one or more certificates crea
  ca: /Users/kyle/Downloads/Cert/ca.crt
  cert: /Users/kyle/Downloads/Cert/liyiming.crt
  key: /Users/kyle/Downloads/Cert/liyiming.key
  # blocklist is a list of certificate fingerprints that we will refuse to talk to
  #blocklist:
```

```
static_host_map:
  "192.168.100.1": ["104.243.20.247:554"]
lighthouse:
  # am_lighthouse is used to enable lighthouse functionality for a node. This should ONLY b
  # you have configured to be lighthouses in your network
  am_lighthouse: false
```

```
# however using port 0 will dynamically assign a port and i
listen:
  # To listen on both any ipv4 and ipv6 use "[::]"
  host: 0.0.0.0
  port: 554
  # Sets the max number of packets to pull from the kernel
```

4. Run nebula and check the connectivity between your computer and the light

house. The IP address of the light house in the overlay network is 192.168.100.1.So I only need to run nebula on my laptop,then open another terminal to ping 192.168.100.1 for connectivity test



```
(base) kyle@Kyles-MacBook-Pro ~ % ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1): 56 data bytes
64 bytes from 192.168.100.1: icmp_seq=0 ttl=64 time=146.215 ms
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=141.896 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=142.549 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=142.334 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=144.241 ms
64 bytes from 192.168.100.1: icmp_seq=5 ttl=64 time=142.028 ms
64 bytes from 192.168.100.1: icmp_seq=6 ttl=64 time=143.640 ms
64 bytes from 192.168.100.1: icmp_seq=7 ttl=64 time=143.808 ms
64 bytes from 192.168.100.1: icmp_seq=8 ttl=64 time=142.928 ms
64 bytes from 192.168.100.1: icmp_seq=9 ttl=64 time=144.950 ms
64 bytes from 192.168.100.1: icmp_seq=10 ttl=64 time=143.587 ms
64 bytes from 192.168.100.1: icmp_seq=11 ttl=64 time=142.422 ms
64 bytes from 192.168.100.1: icmp_seq=12 ttl=64 time=142.831 ms
64 bytes from 192.168.100.1: icmp_seq=13 ttl=64 time=142.390 ms
64 bytes from 192.168.100.1: icmp_seq=14 ttl=64 time=143.580 ms
64 bytes from 192.168.100.1: icmp_seq=15 ttl=64 time=149.089 ms
64 bytes from 192.168.100.1: icmp_seq=16 ttl=64 time=142.377 ms
64 bytes from 192.168.100.1: icmp_seq=17 ttl=64 time=141.647 ms
64 bytes from 192.168.100.1: icmp_seq=18 ttl=64 time=142.852 ms
key: open /Users/lei/.nebula/MBP15.key: no such file or directory"
(base) kyle@Kyles-MacBook-Pro ~ % sudo nebula -config /Users/kyle/Downloads/Cert/config.yaml

INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:outgoing endPort:
0 groups:[] host:any ip: localIp: proto:0 startPort:0]"
INFO[0000] Firewall rule added                           firewallRule="map[caName: caSha: direction:incoming endPort:
0 groups:[] host:any ip: localIp: proto:0 startPort:0]"
INFO[0000] Firewall started                              firewallHashes="SHA:498215dec4e5687a2353f51c10838c113bd1af35
ef72b8e8c9f536986ada5417,FNV:2782948616"
WARN[0000] interface name must be utun[0-9]+ on Darwin, ignoring
INFO[0000] listening on 0.0.0.0:554
INFO[0000] Main HostMap created                          network=192.168.100.140/24 preferredRanges="[]"
INFO[0000] punchy enabled
INFO[0000] Loaded send_recv_error config                 sendRecvError=always
INFO[0000] Nebula interface is active                    boringcrypto=false build=1.9.5 interface=utun6 network=192.1
68.100.140/24 udpAddr="[::]:554"
INFO[0000] Handshake message sent                        handshake="map[stage:1 style:ix_psk0]" initiatorIndex=174309
7263 localIndex=1743097263 remoteIndex=0 udpAddrs="[104.243.20.247:554]" vpnIp=192.168.100.1
INFO[0000] Handshake message received                    certName=lighthouse durationNs=144383250 fingerprint=fbf998b
366c8275810bdbe0c175cd7cbf31be03d0adc2a831ae16f9669a52617 handshake="map[stage:2 style:ix_psk0]" initiatorIndex=17430
97263 issuer=e430f526e15e22fd11dbb26e9482945865f17aa42c800481e56f68d087c892c0 remoteIndex=1743097263 responderIndex=4
2347321 sentCachedPackets=1 udpAddr="104.243.20.247:554" vpnIp=192.168.100.1
```