

Lab Report: Personal Overlay Network with Nebula

(Cloud Lighthouse + NAT-ed PCs)

1. Objective

Use a cloud VM as a public Lighthouse to let my home Mac/PCs join the same encrypted overlay (192.168.100.0/24) despite NAT.

2. Cloud Lighthouse Deployment

Provider	Google Cloud (Always-Free tier)
Instance	e2-micro (1 vCPU, 1 GB) – free region
OS	Ubuntu 22.04 LTS
Public IP	34.34.34.34 (static)
Firewall rule	Allow UDP 4242

Screenshots

- VM created & external IP assigned
 - Firewall rule “nebula-udp-4242” listed
-

3. Local Side Preparation

Machine	Overlay IP	OS
MacBook Pro	192.168.100.15	macOS 14
Mac mini	192.168.100.10	macOS 14

Installed via: brew install nebula

4. Certificate & Config Workflow

Step 4.1 – CA & certs

- Received from lecturer: ca.crt, myname.crt/key
- Generated extra certs for two more devices with nebula-cert sign …

Screenshots

- CA public key fingerprint
- Three signed certificates listed

Step 4.2 – **config.yaml** **tuning**

Compared template vs lighthouse config with Beyond-Compare; only three blocks differ:

- tun.ip (device unique)
- lighthouse.hosts (lighthouse IP)
- am_lighthouse: false on clients

Screenshots

- Side-by-side diff (lighthouse vs client)

5. Connectivity Verification

Lighthouse start

```
sudo nebula -config /etc/nebula/config.yaml
```

log: "Running on 34.34.34.34:4242 … handshake manager ready"

Client start

```
sudo nebula -config ~/.nebula/config.yaml
```

log: "Handshake message sent to 192.168.100.1" → "Handshake completed"

Screenshots

- Lighthouse sees both clients in "lighthouse hosts" list
- Each client shows the other with correct overlay IP & latency

Traffic test

- ping 192.168.100.1 – 19 ms
 - ping 192.168.100.10 from MBP – 22 ms (direct tunnel)
-

6. Summary

- Cloud VM acts as free, always-on Lighthouse
- Home Macs behind NAT obtain stable overlay addresses
- Full mesh encrypted without opening home routers
- Config & certificate repo tagged v1.0 on GitHub for reproducibility

```
正在 Ping 192.168.100.1 具有 32 字节的数据：  
来自 192.168.100.1 的回复：字节=32 时间=2ms TTL=252  
来自 192.168.100.1 的回复：字节=32 时间=2ms TTL=252  
来自 192.168.100.1 的回复：字节=32 时间=1ms TTL=252  
来自 192.168.100.1 的回复：字节=32 时间=1ms TTL=252
```

```
192.168.100.1 的 Ping 统计信息：  
数据包：已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位):  
最短 = 1ms, 最长 = 2ms, 平均 = 1ms
```