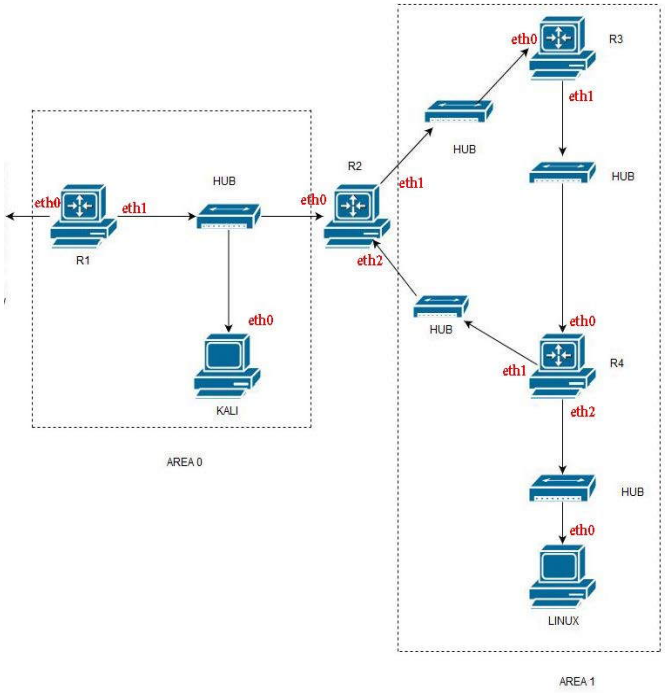
Vital Lab

Open Shortest Path First (OSPF)

Instructions

In this lab exercise we will implement the OSPF routing protocol.

Recall the diagram shared in the previous lab:



Part 1: Enable OSPF Daemon

On each of the routers R1, R2, R3, and R4 execute the following commands to enable the OSPF daemon:

```
> cd /etc/frr
> nano daemons
```

Change the `ospfd=no` configuration to `ospfd=yes` and save. Restart **frrouting** by executing:

```
> systemctl restart frr
```

Part 2: Configure CN-R1 OSPF in Area 0

We need to configure R1 such that it advertises which networks the device is able to route to. Launch the R1 virtual image and execute the following commands:

```
> sudo su
> vtysh
CN-RTR > configure terminal
CN-RTR > router ospf
# advertise networks that R1 know about
CN-RTR > network 10.10.10.0/29 area 0
CN-RTR > network 10.20.1.0/24 area 0
```

Part 3: Configure R2, R3, & R4

Advertise the networks that R2 is aware of. Aggregate all the 10.10.11.0 subnets into one advertisement - the 10.10.11.0 network.

```
> sudo su
> vtysh
CN-RTR > configure terminal
CN-RTR > router ospf
```

Do similar actions for R3 and R4, except for **R4 do not run OSPF on eth2** (see no passive-interface command).

Part 4: Set Default Routes and Masquerade

We want to be able to ping the SFTP server (128.238.77.36) from any router or host within the Computer Networks course. Start R1 and apply the following configurations as root to enable persistent MASQUERADE using iptables:

```
> iptables -t nat -A POSTROUTING -o eth0 -d 128.238.77.36 -j MASQUERADE
> iptables-save | tee /etc/iptables.conf
```

Insert the following lines in */etc/rc.local* …

```
# load iptables rules from file
iptables-restore < /etc/iptables.conf
```

Verify that your configuration has been persisted with the following command …

```
> iptables -t nat -L
```

You will have to use vtysh on R2, R3, and R4 to set the default IP route to R1 for all 128.238.77.0/24 addresses. You will have to browse the vtysh documentation to find the exact command.

Submissions

1. Screenshot configurations of R1, R2, R3, and R4.
2. ICMP results from R3 to R1, etc.
3. Wireshark screenshots on R1.
4. Screenshots depicting successful ping requests to 128.238.77.36 from R1, R2, R3, and R4

Please remember to submit your lab results as a single PDF document. While you may work in groups, you MUST submit your own work!