(1) Network Topology Setup

To setup the Network topology we use namespaces as explained previously. To create a network namespace we use the command

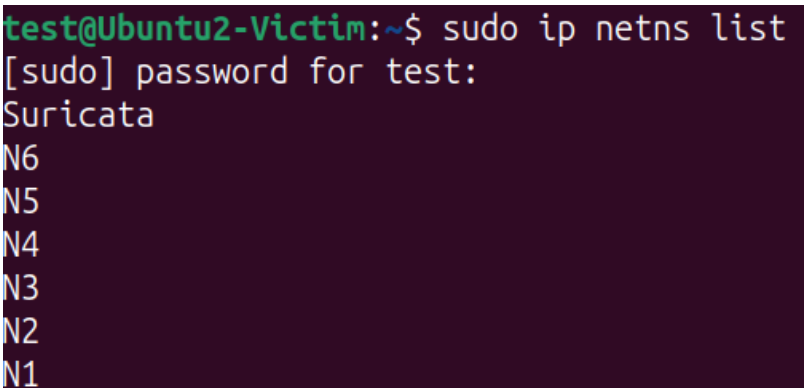
```
sudo ip netns add <name>
```

So we add 6 network namespaces named N1 through N6 and another namespace called Suricata. The Namespace Suricata will be where the suricata will be monitoring traffic by acting as a waypoint for the traffic from the 5 namespaces to the 6th Namespace, alerting and blocking if a rule is triggered.

After creating the namespaces we can list them using the command

```
sudo ip netns list
```

The result looks like this



The next step will be to connect these namespaces via a virtual connection or "cable", created using the command -

```
sudo ip link add <name> type veth peer name <name>
```

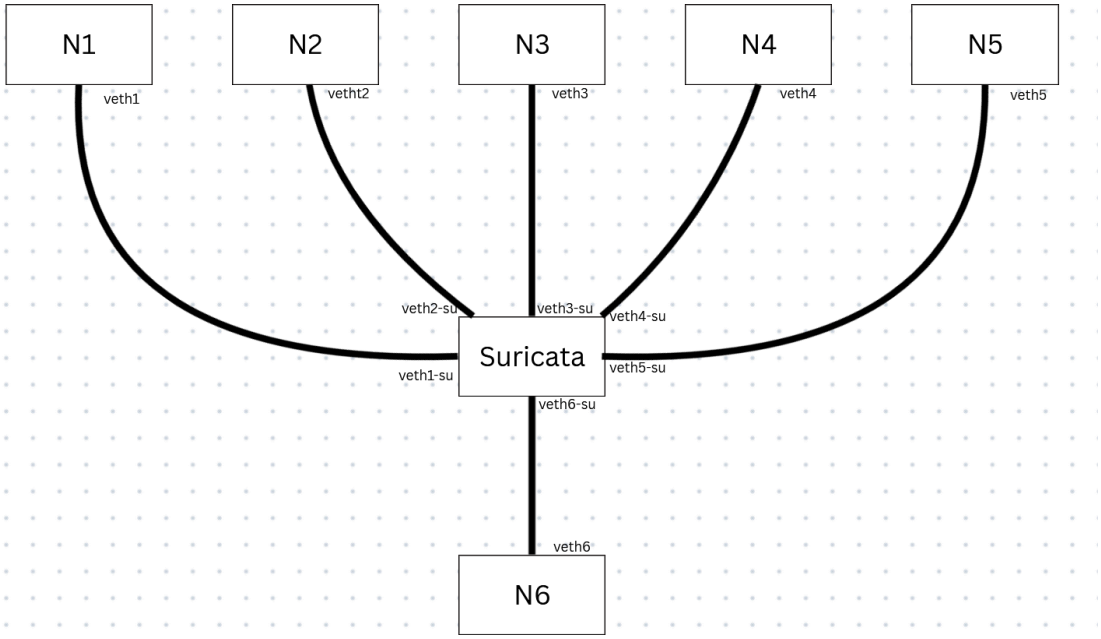
This creates a virtual ethernet pair which acts as a pipe for forwarding network traffic, we name them veth1 through veth6 for connection on the namespace side and veth1-su through veth6-su to connect it on the Suricata Namespace side.

> **Deletion of either of the cable pair will result in the deletion of the whole connection pair**

Now we bind the virtual ethernet cables to respective Namespaces using -

```
sudo ip link set <veth> netns <name>
```

Thus we create a network topology that looks like this



Next we assign IP addresses to respective namespaces using

```
sudo ip netns exec N1 ip address add 10.0.1.2/24 dev veth1
```

- **exec** - runs command in that namespace
- **dev** - is to specify the device/interface

We will be assigning IP address 10.0.1.2/24 for N1 through 10.0.6.2/24 for N6 and 10.0.1.1/24 through 10.0.6.1/24 for connection on Suricata side for each namespace. The namespaces have been assigned but they are still in the down state so we use command

```
sudo ip netns exec Suricata ip link set dev veth1-su up
```

We do this for all available interfaces till we get UP in all caps when executing command `sudo ip address`. Any side that does not have its pair in the UP state will show LOWERLAYERDOWN.

```
13: veth6-su@if14: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state LOWERLAYERDOWN group default qlen 1000
    link/ether d6:37:ec:1a:ea:b1 brd ff:ff:ff:ff:ff:ff link-netns N6
    inet 10.0.6.1/24 scope global veth6-su
       valid_lft forever preferred_lft forever
```

After setting all of them up we get the UP state that means both end can communicate

```
14: veth6@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 6e:af:5d:85:d7:c2 brd ff:ff:ff:ff:ff:ff link-netns Suricata
    inet 10.0.6.2/24 scope global veth6
       valid_lft forever preferred_lft forever
    inet6 fe80::6caf:5dff:fe85:d7c2/64 scope link
       valid_lft forever preferred_lft forever
```

Now we need to set up gateway as the Suricata namespace will be used as a router so it can inspect incoming and outgoing packets. Thus we use command -

```
sudo ip netns exec N1 ip route add default via 10.0.1.1
```

This will be done for all namespaces, they will be referring to their respective IP address as gateway.

When using ping to test connection we notice that ping shows a 100% packet loss as no packet is reaching its intended destination. This is because, by default all namespaces receive packet and hold it, we have to allow forwarding them. This is done using the command -

```
sudo sysctl -w net.ipv4.ip_forward=1
```

as this problem is occurring in the Suricata namespace we execute the command its name space by prefixing the above command with `sudo ip netns exec Suricata sysctl ..` . Now we can ping all other namespaces. this completes our Network Topology setup.