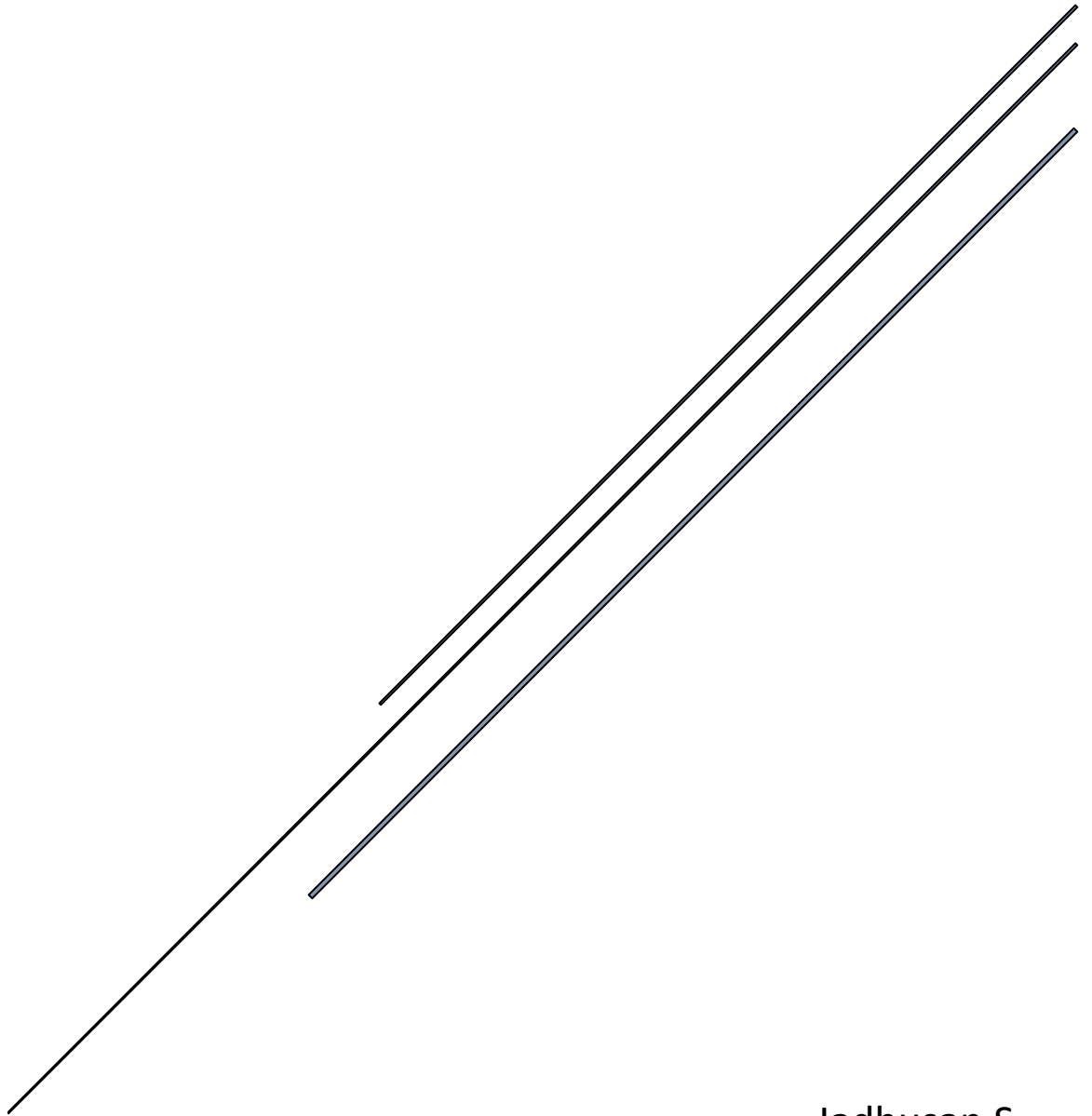


# INFRASTRUCTURE SECURITY LABS



Jadhusan S

## Setup

In the realm of computer networks, network administrators often encounter complex scenarios that require innovative solutions. One such solution involves the use of Virtual Local Area Networks (VLANs) to enhance network segmentation and security. In this context, we will explore a setup using GNS3 and VMware® Workstation Pro to emulate a network environment, along with VLAN Access-Lists (VACLs) and Private VLANs (PVLANS) for improved control and isolation.

### Resources

GNS3 2.2.19

VMware® Workstation 16 Pro. – GNS3 VM

Windows 10 Pro. - Host machine

### Network

GNS3 with 2 Virtual Network Adapter.

Custom(VMNET 1)

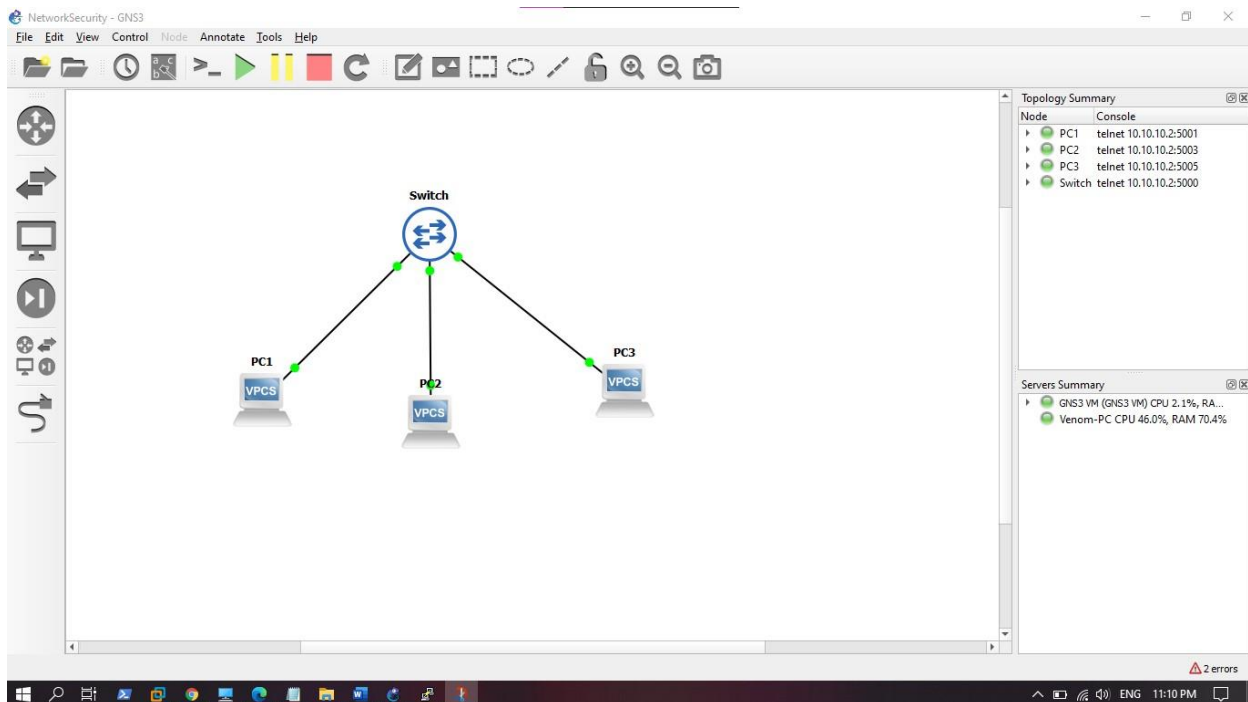
Custom(VMNET 2)

## VLAN Access-List (VACL)

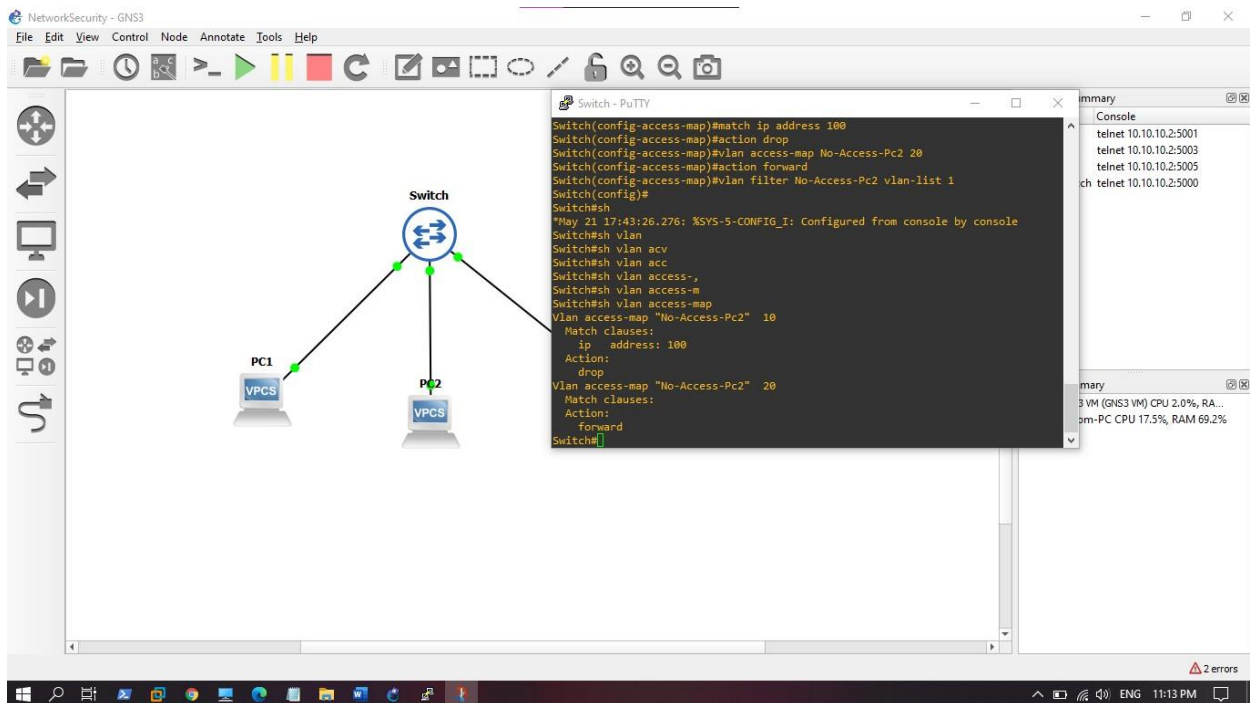
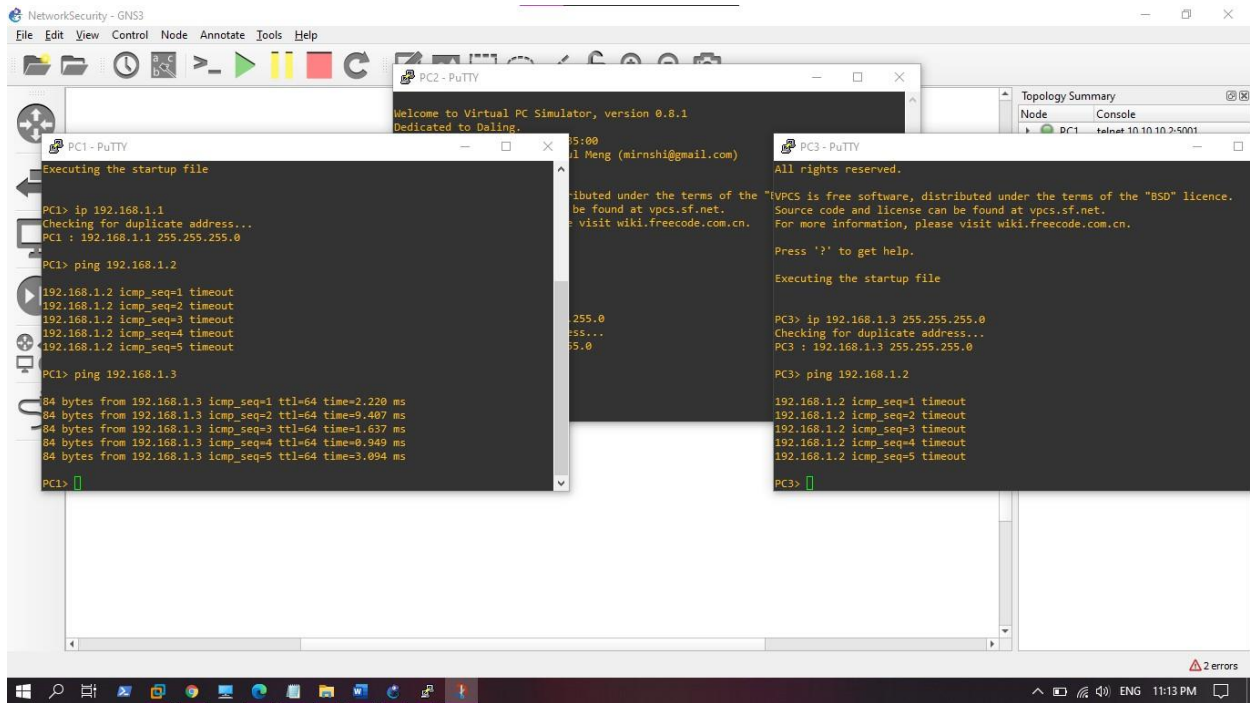
```
access-list 100 permit ip any host 192.168.1.2
vlan access-map No-Access-Pc2 10
match ip address 100
action drop
vlan access-map No-Access-Pc2 20
action forward
vlan filter No-Access-Pc2 vlan-list 1
```

- Sequence number 10 will look for traffic that matches access-list 100. All traffic that is permitted in access-list 100 will match here. The action is to drop this traffic.
- Sequence number 20 doesn't have a match statement so everything will match, the action is to forward traffic.

As a result, all traffic from any host to destination IP address 192.168.1.2 will be dropped, everything else will be forwarded.







## Private VLAN

Community VLAN: All ports within the community VLAN are able to communicate with each other and the promiscuous port.

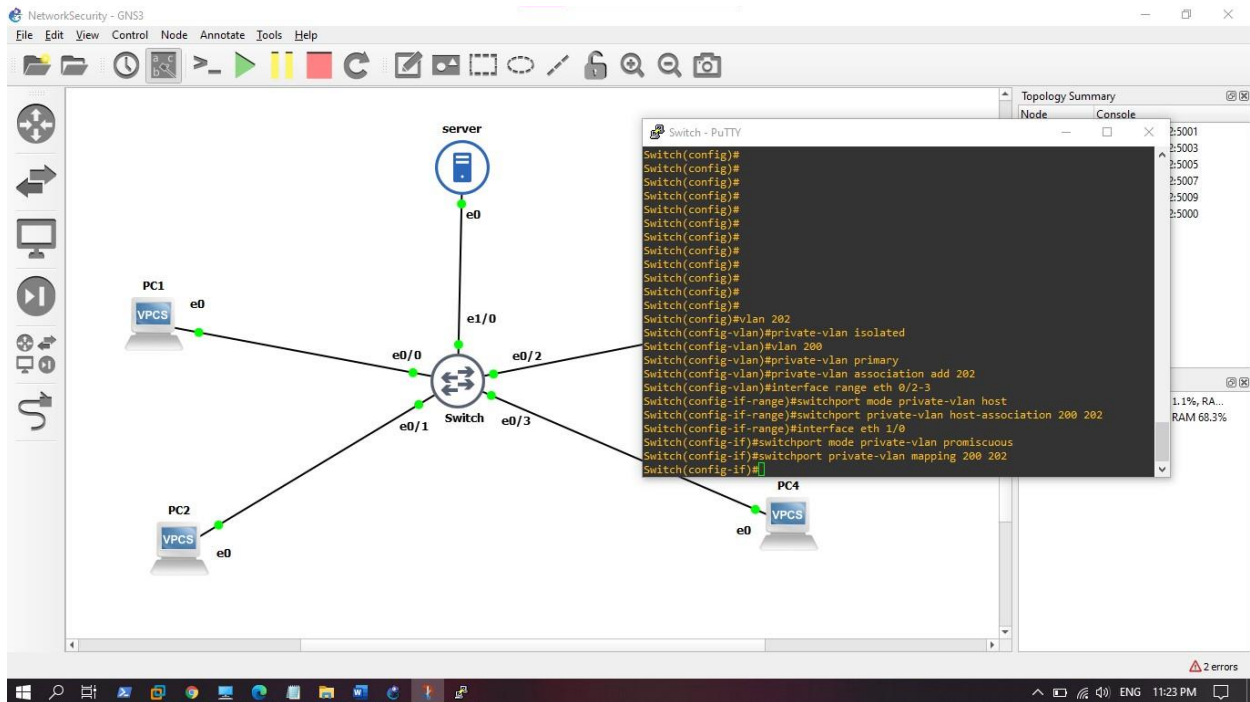
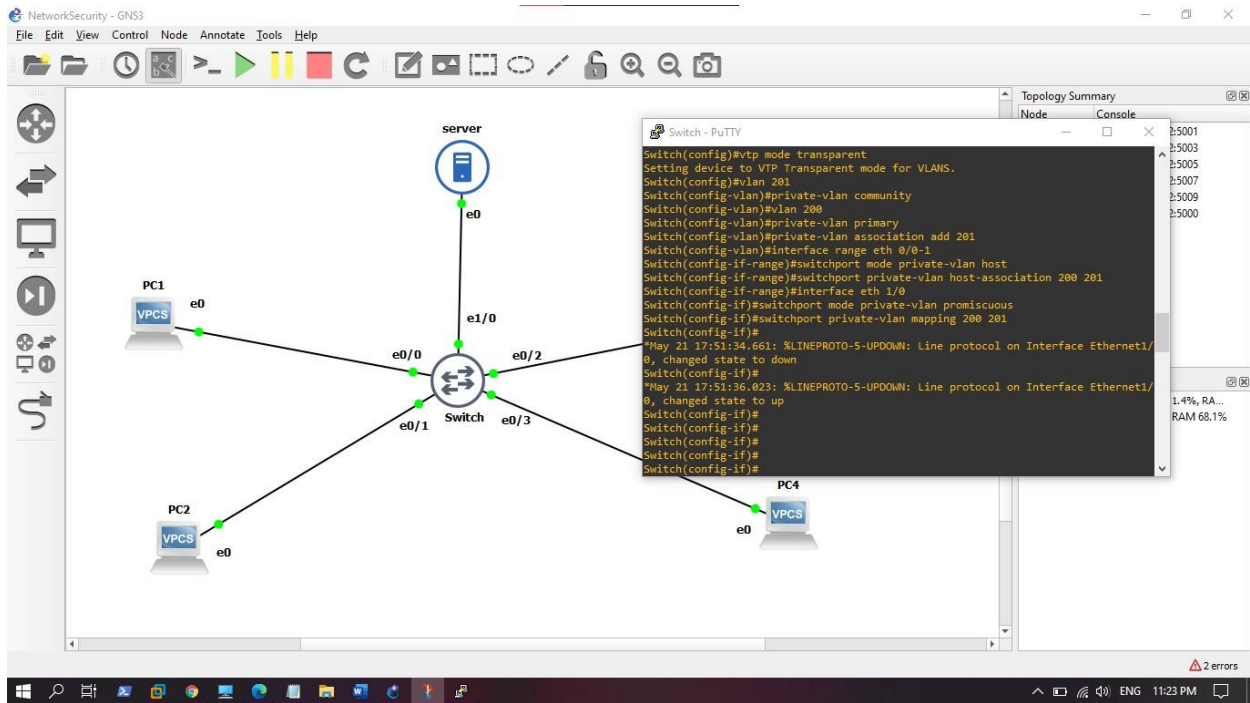
Isolated VLAN: All ports within the isolated VLAN are unable to communicate with each other but they can communicate with the promiscuous port.

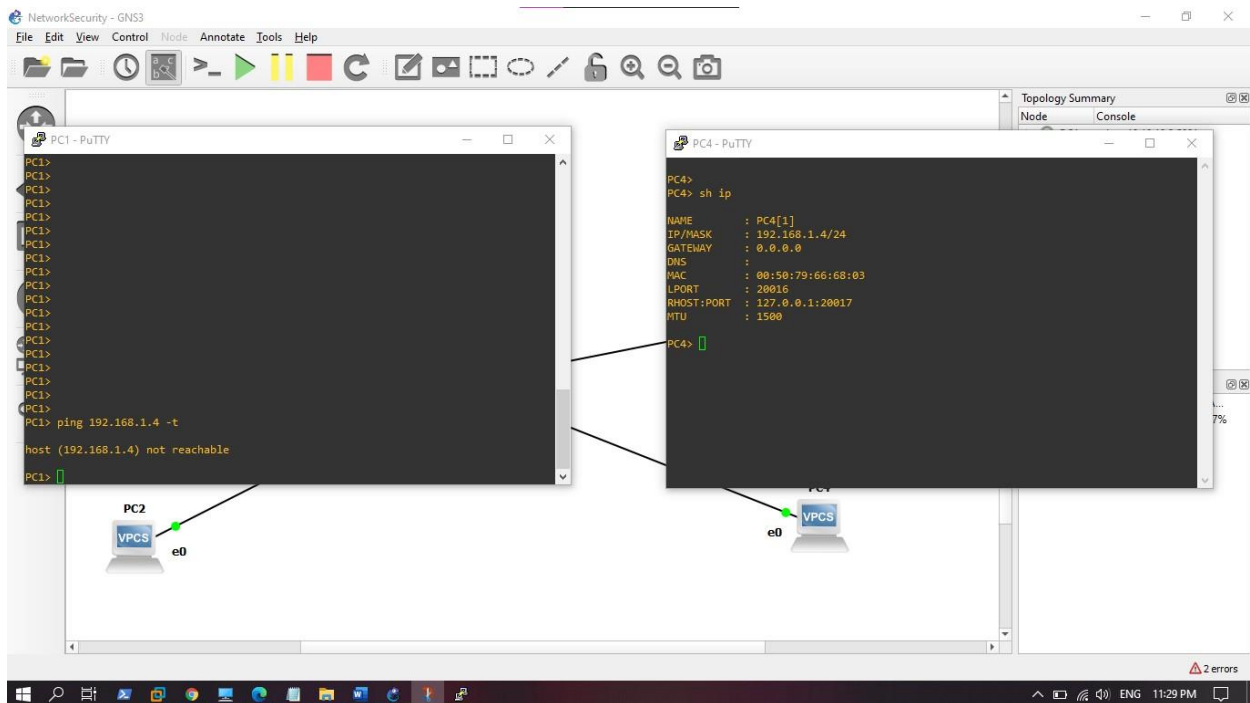
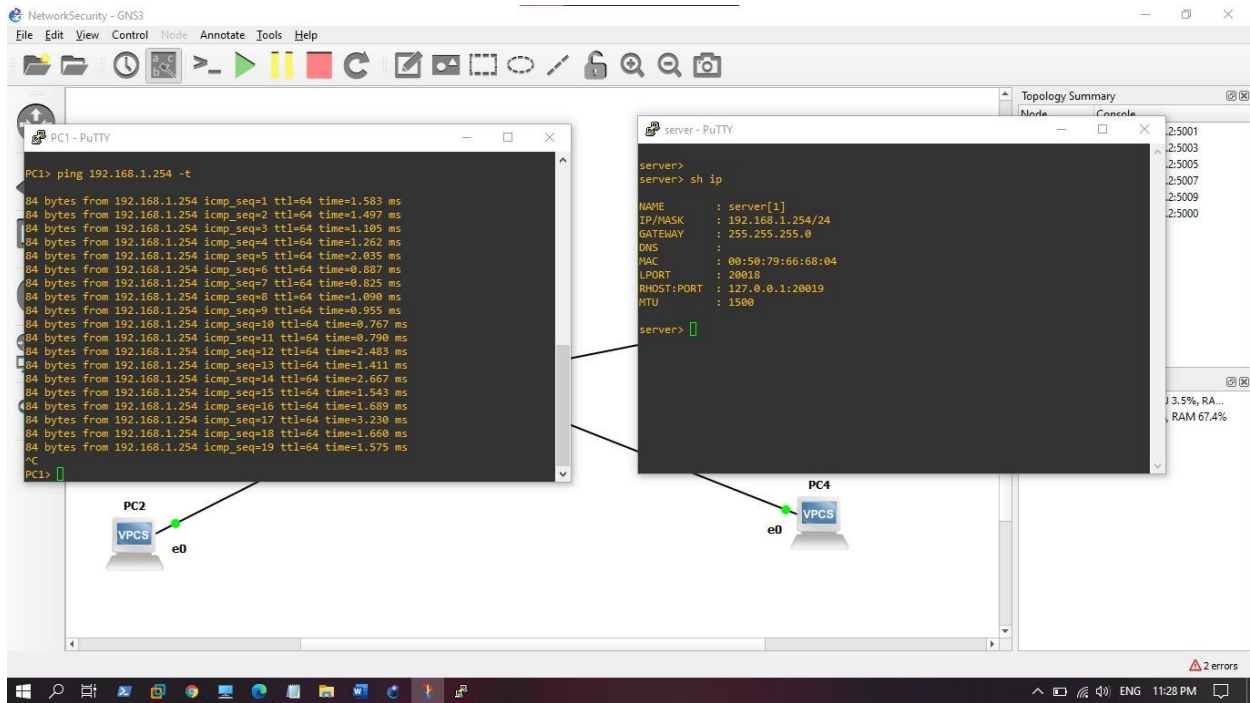
## Community VLAN

```
vtp mode transparent
vlan 201
private-vlan community
vlan 200
private-vlan primary
private-vlan association add 201
interface range eth 0/0-1
switchport mode private-vlan host
switchport private-vlan host-association 200 201
interface eth 1/0
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 201
```

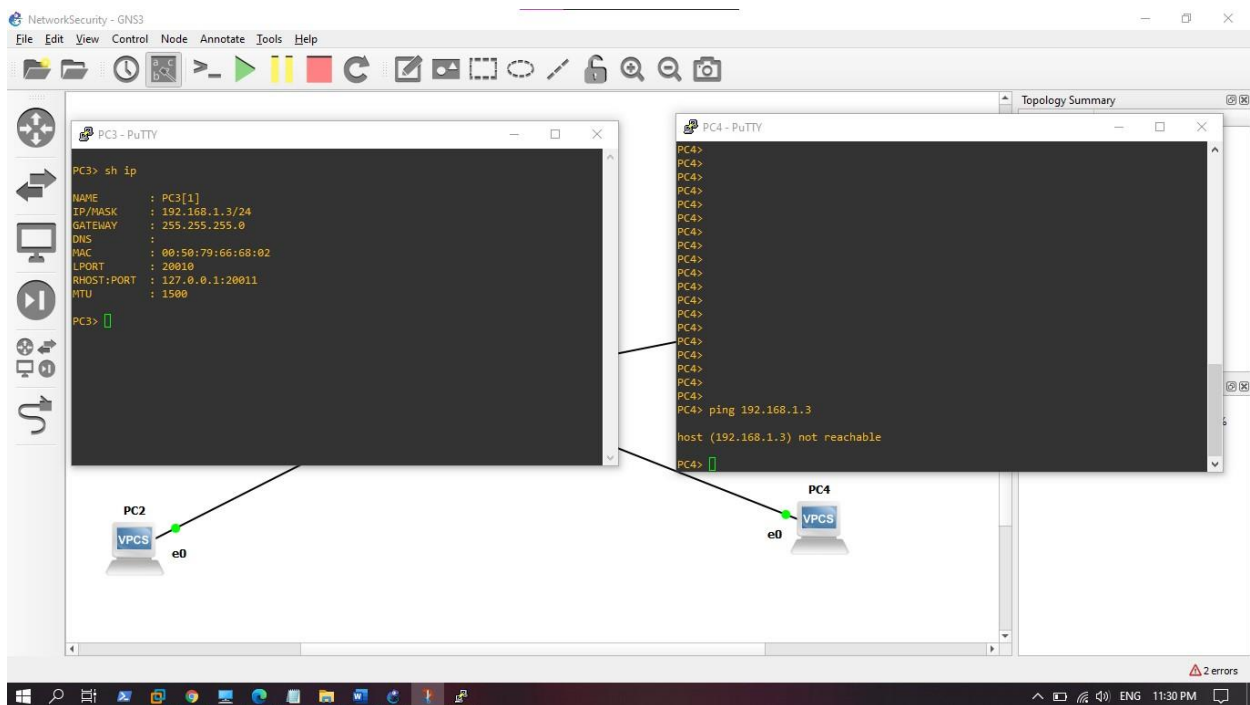
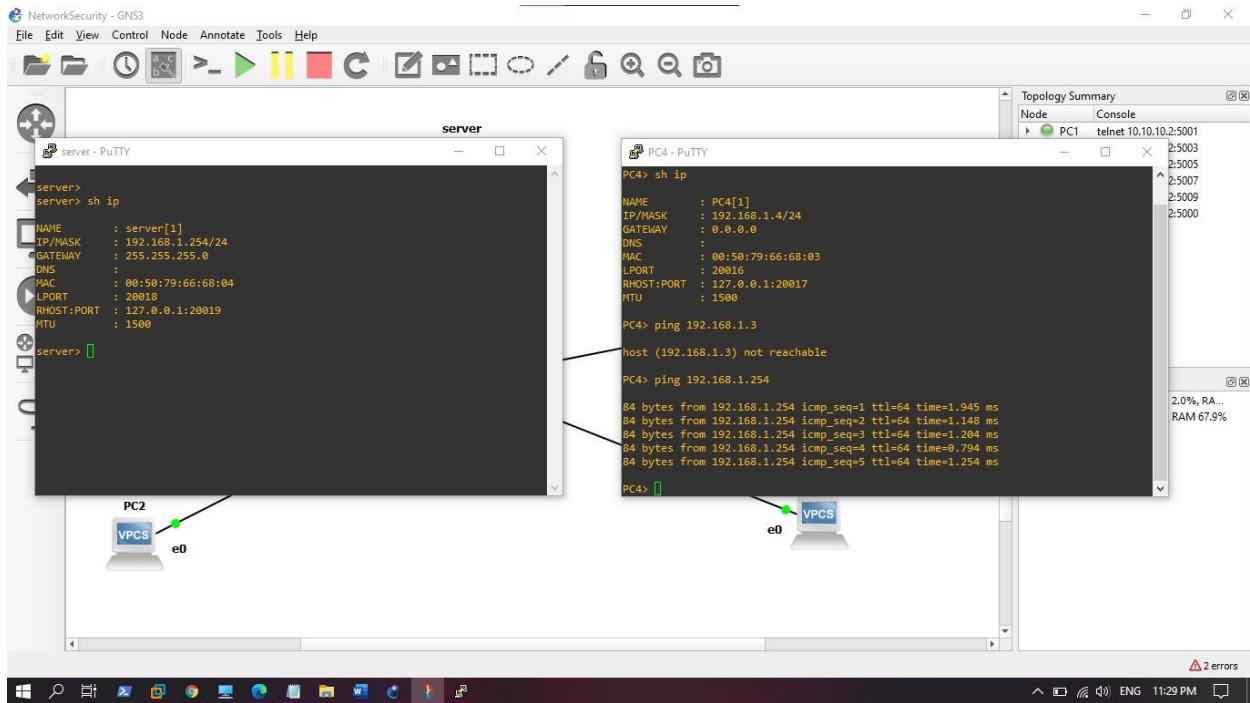
## Isolated VLAN

```
vlan 202
private-vlan isolated
vlan 200
private-vlan primary
private-vlan association add 202
interface range eth 0/2-3
switchport mode private-vlan host
switchport private-vlan host-association 200 202
interface eth 1/0
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 202
```









In summary, our network setup showcases the effective utilization of VLANs, VACLs, and PVLANS to achieve enhanced network segmentation, security, and traffic control. This configuration allows network administrators to design and manage intricate network e