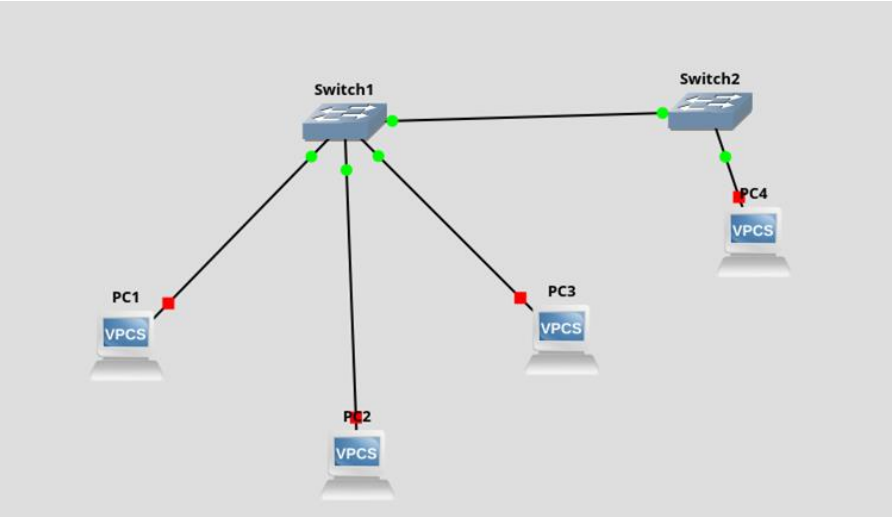
CN Lab: Week 1

Komal Mathur, CSE B2, 220905546

Initial commands-
python3 -m venv gns3env
source gns3/env/activate
pip install pyqt5
pip install gns3-server
pip install gns3-gui

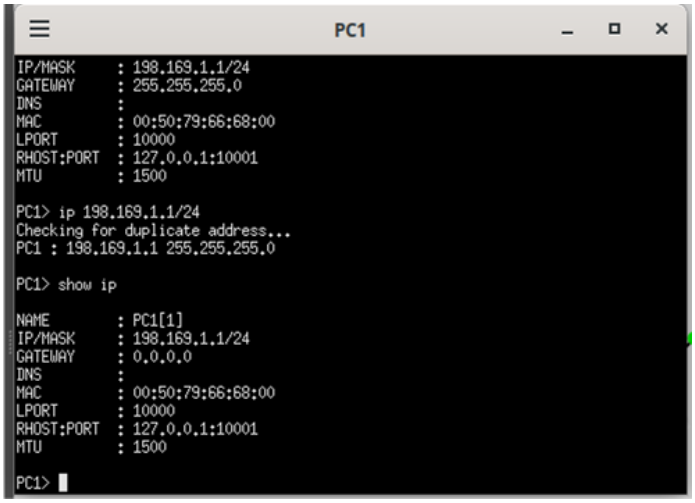
Commands to run to open gns3
source gns3/env/activate
gns3

GNS3 Sample Network:



Assigning ip addresses in console of each vpc:
There are 2 ways to assign ip addresses:
1. $ ip 192.168.1.1/24 (using slash notation for SUBNET MASK)
2. $ ip 192.168.1.1 255.255.255.0 (using dot notation for SUBNET MASK)

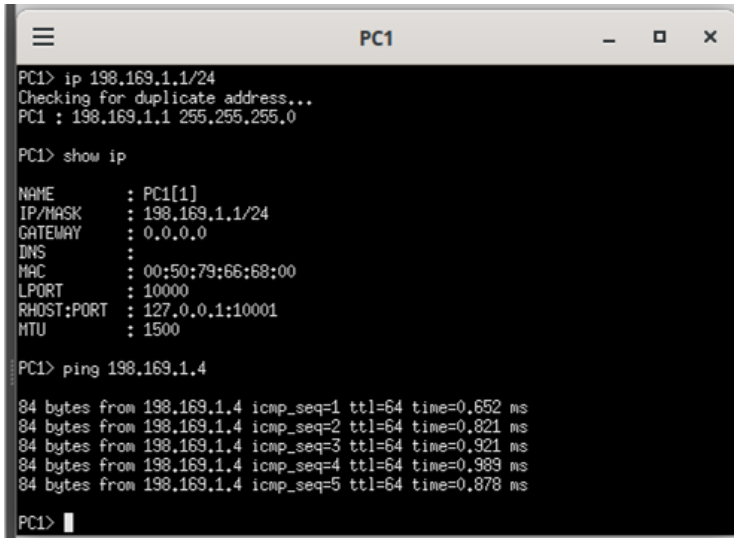
$ save (to save the configuration in each vpc)
$ show ip (to show the details of the ip address)



Ping Command
This sends a special packet to the assigned pc and we get a reply. It is used to check the correctness of the network, and to check for the speed of the network configuration.

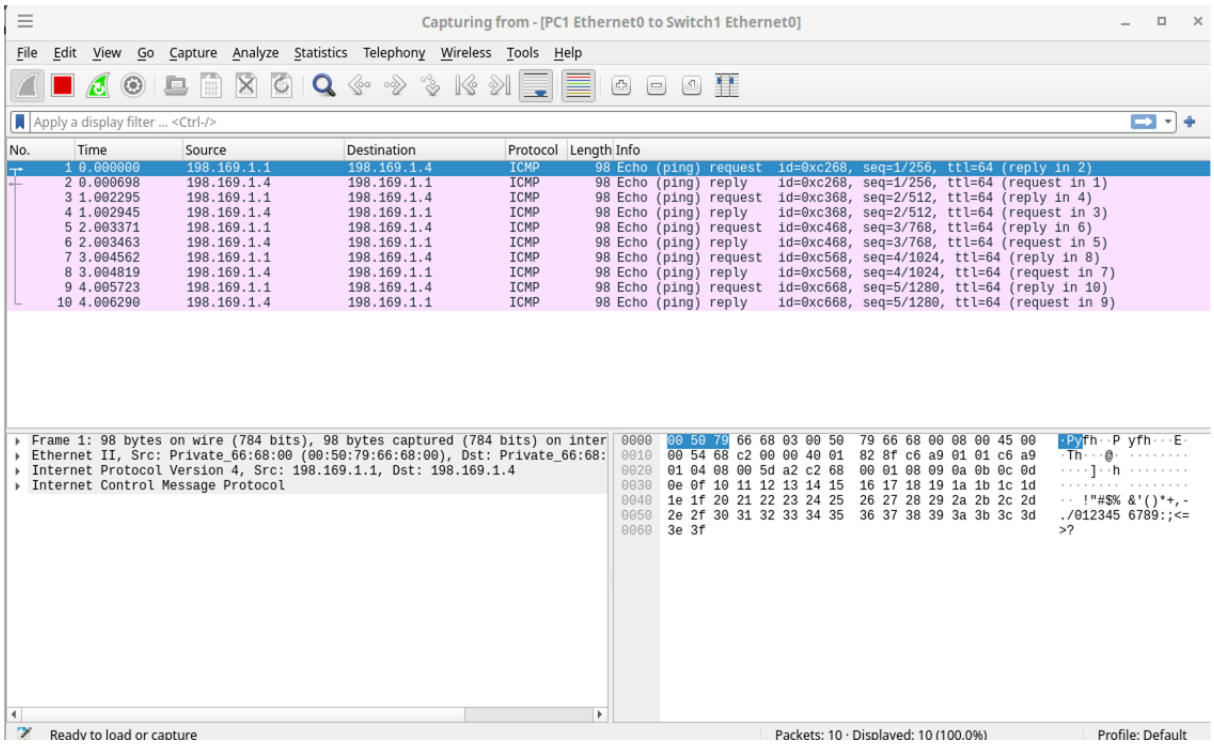
$ ping {ip address to ping} -c {number of packets to ping}

Note: by default the number of packets is 5



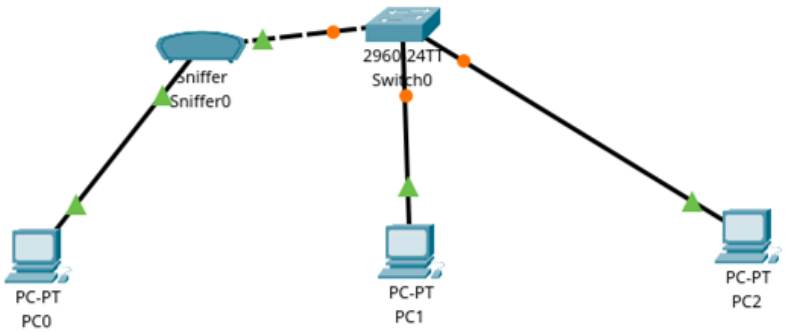
Wireshark tool
To visualize the data packets/ ping packets we use wireshark, on a given network connection.
To configure wireshark, rightclick on wire, and click on ‘Start Capture’.

Note: 1 ping generates 2 data packets- request + reply. Each is 98 bytes.



Content of ICMP Packets
ICMP: Internet Control Message Protocol
It is 98 bytes.
It uses Encapsulation ie. ICMP packet < IP Packet < Ethernet 2 which is converted to a dataframe to flow as electrical signals.

Cisco Packet Tracer Sample Network:



VPC Cofigurations
The steps to follwo to configure the Pcs are:
Click on PC > Desktop > ip configuration > follow commands as above

To ping another PC: Desktop > command prompt
Note: The count parameter doent work here. By default 4 packets are sent.

Monitoring using Sniffer

In place of wireshark, a sniffer is connected between 2 devices, to monitor the data flow.

Note: Sniffer is present under ‘End Devices’.