

# CN Lab: Week 1

Komal Mathur, CSE B2, 220905546

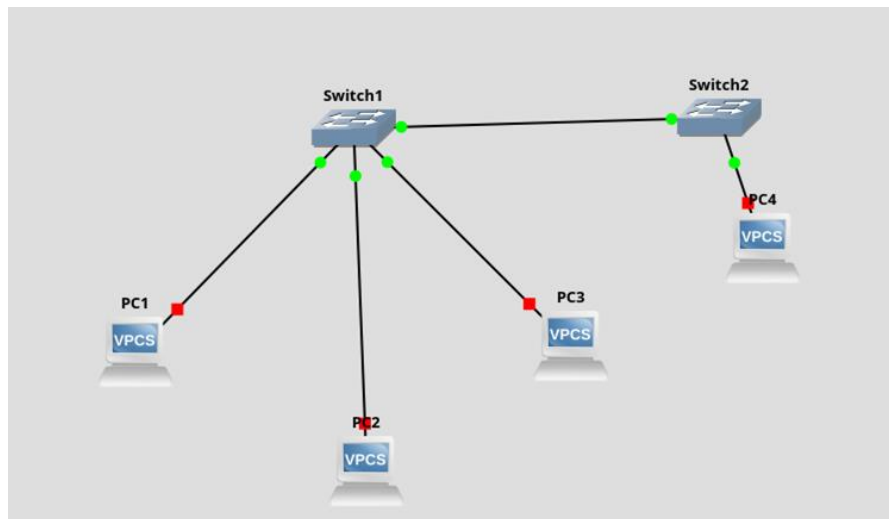
## Initial commands-

```
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)

```
PC1
IP/MASK      : 198.169.1.1/24
GATEWAY      : 255.255.255.0
DNS          :
MAC          : 00:50:79:66:68:00
LPORT        : 10000
RHOST:PORT   : 127.0.0.1:10001
MTU          : 1500

PC1> ip 198.169.1.1/24
Checking for duplicate address...
PC1 : 198.169.1.1 255.255.255.0

PC1> show ip

NAME        : PC1[1]
IP/MASK      : 198.169.1.1/24
GATEWAY      : 0.0.0.0
DNS          :
MAC          : 00:50:79:66:68:00
LPORT        : 10000
RHOST:PORT   : 127.0.0.1:10001
MTU          : 1500

PC1>
```

## 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

```
PC1
PC1> ip 198.169.1.1/24
Checking for duplicate address...
PC1 : 198.169.1.1 255.255.255.0

PC1> show ip

NAME        : PC1[1]
IP/MASK      : 198.169.1.1/24
GATEWAY      : 0.0.0.0
DNS          :
MAC          : 00:50:79:66:68:00
LPORT        : 10000
RHOST:PORT   : 127.0.0.1:10001
MTU          : 1500

PC1> ping 198.169.1.4

84 bytes from 198.169.1.4 icmp_seq=1 ttl=64 time=0.652 ms
84 bytes from 198.169.1.4 icmp_seq=2 ttl=64 time=0.821 ms
84 bytes from 198.169.1.4 icmp_seq=3 ttl=64 time=0.321 ms
84 bytes from 198.169.1.4 icmp_seq=4 ttl=64 time=0.989 ms
84 bytes from 198.169.1.4 icmp_seq=5 ttl=64 time=0.878 ms

PC1>
```

## 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.

Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	198.169.1.1	198.169.1.4	ICMP	98	Echo (ping) request id=0xc268, seq=1/256, ttl=64 (reply in 2)
2	0.000698	198.169.1.4	198.169.1.1	ICMP	98	Echo (ping) reply id=0xc268, seq=1/256, ttl=64 (request in 1)
3	1.002295	198.169.1.1	198.169.1.4	ICMP	98	Echo (ping) request id=0xc368, seq=2/512, ttl=64 (reply in 4)
4	1.002945	198.169.1.4	198.169.1.1	ICMP	98	Echo (ping) reply id=0xc368, seq=2/512, ttl=64 (request in 3)
5	2.003371	198.169.1.1	198.169.1.4	ICMP	98	Echo (ping) request id=0xc468, seq=3/768, ttl=64 (reply in 6)
6	2.003463	198.169.1.4	198.169.1.1	ICMP	98	Echo (ping) reply id=0xc468, seq=3/768, ttl=64 (request in 5)
7	3.004562	198.169.1.1	198.169.1.4	ICMP	98	Echo (ping) request id=0xc568, seq=4/1024, ttl=64 (reply in 8)
8	3.004819	198.169.1.4	198.169.1.1	ICMP	98	Echo (ping) reply id=0xc568, seq=4/1024, ttl=64 (request in 7)
9	4.005723	198.169.1.1	198.169.1.4	ICMP	98	Echo (ping) request id=0xc668, seq=5/1280, ttl=64 (reply in 10)
10	4.006290	198.169.1.4	198.169.1.1	ICMP	98	Echo (ping) reply id=0xc668, seq=5/1280, ttl=64 (request in 9)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on inter	0000	00 50 79 66 68 03 00 50	79 66 68 00 08 00 45 00	Pyrh..P yfh...E
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:	0010	00 54 68 c2 00 00 40 01	82 8f c6 a9 01 01 c6 a9	Th...@: .....
Internet Protocol Version 4, Src: 198.169.1.1, Dst: 198.169.1.4	0020	01 04 08 00 5d a2 c2 68	00 01 08 09 0a 0b 0c 0d	....].h .....
Internet Control Message Protocol	0030	0e 0f 10 11 12 13 14 15	16 17 18 19 1a 1b 1c 1d	..... .....
	0040	1e 1f 20 21 22 23 24 25	26 27 28 29 2a 2b 2c 2d	.. !"#\$\$% &'()*+,-
	0050	2e 2f 30 31 32 33 34 35	36 37 38 39 3a 3b 3c 3d	./012345 6789;<=
	0060	3e 3f		>?

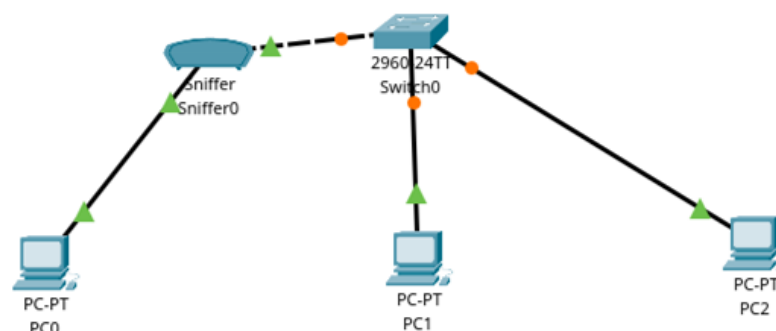
## Content of ICMP Packets

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 Configurations

The steps to follow 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 doesn't 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'.