Configuration Manual

MSc Research Project
MSc in Cyber Security

Anurag Nitin Mhatre
Student ID: X19236042

School of Computing
National College of Ireland

Supervisor: Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. Anurag Nitin Mhatre ……

Student ID: ……X19236042……..…

Programme: …MSc Cybersecurity…… **Year:** ……2021 ...

Module: ……MSc Research Project……..……

Lecturer: …… Vanessa Ayala-Rivera
……..……

Submission Due Date: ……16/08/21……..……

Project Title: ... Securing Home Automation against distributed denial of service attack.....……

Word Count: …… **Page Count:** ……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Anurag Nitin Mhatre……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Anurag Mhatre
Student ID: X19236042

The research study included a configuration Manual presenting a walkthrough of methodology that demonstrated a way to prevent Distributed Denial of Service attacks by building adaptive Routers to secure Home Automation. The configuration guide outlines the features and functioning of the software, devices as it is utilized throughout the research. This research will offer a brief overview of each step used in order to acquire findings.

1. System Requirements

To minimize the time consumption when executing the software and to execute the results, we must adhere to several critical software and hardware requirements.

1.1 Host System Specification

- Device name: LAPTOP-FJ6H38AB
- Processor: Intel(R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
- Installed RAM: 16.0 GB
- Product ID: 00327-35905-95214-AAOEM
- System type 64-bit operating system, x64-based processor

1.2 Virtual Machines

- Operating System: Kali-Linux-2021.3 (Debian- 64 bit)
- Processors: 2
- Storage: 80 GB
- RAM: 4GB

2. Software's Used.

The software and technologies that are used in the research implementation process.

- GNS3- Network engineers utilize graphical network stimulators to show network architecture, create network topology, test the topology, and debug physical and virtual networks. GNS3 supports Virtual machine deployment to connect with virtual networks. As this software is open source, through this stimulator we are able to illustrate the actual smart home automation. (Getting Started with GNS3, 2021)

- HPing3 – It is a Network Tool which is used to transmit customizable TCP, ICMP and UDP packets in order to perform DOS attack. This tool is use to test the network performance in our research. Through this tool we are able to perform DOS attack in cisco router in GNS3 Stimulator.

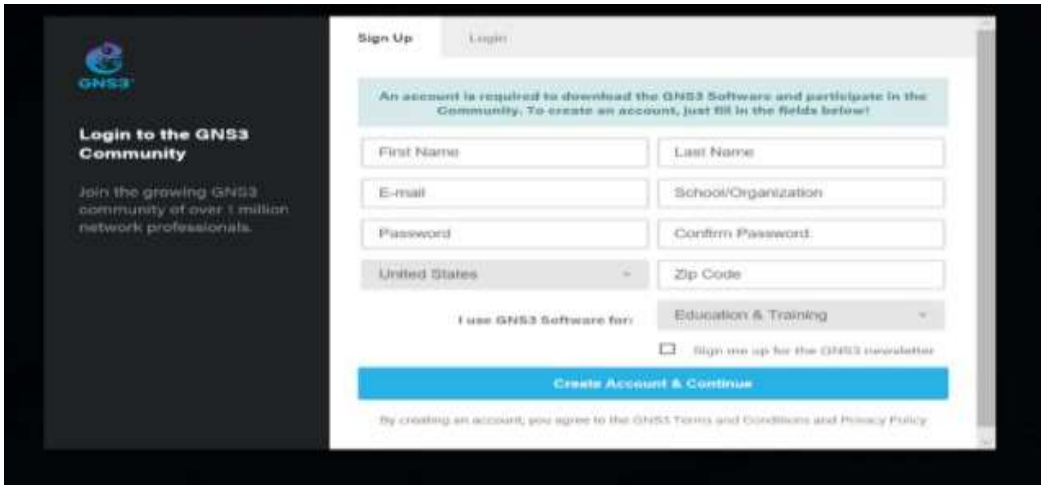
3. Software Configuration

- The instructions below demonstrate how to deploy GNS3 Stimulator step by step.

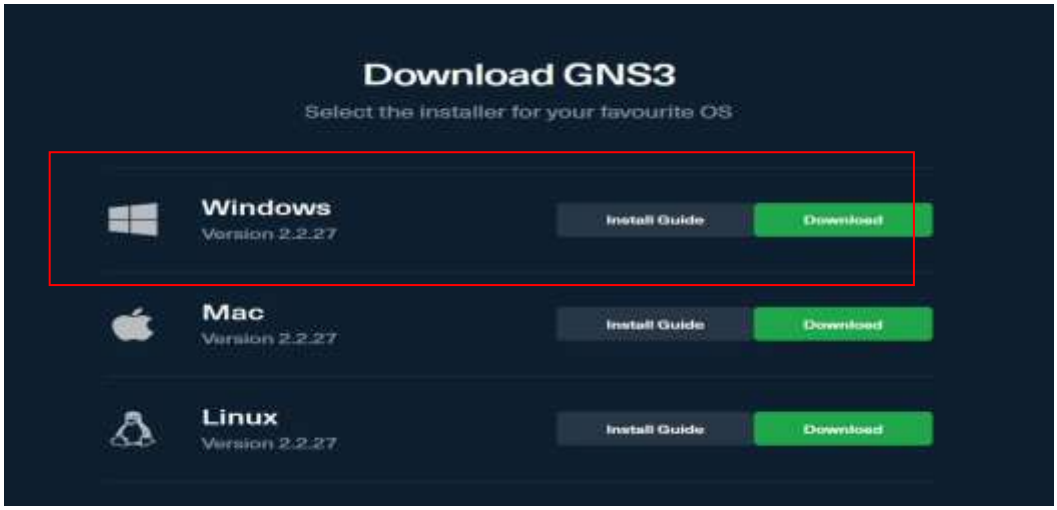
The attached link can be used to download GNS3
[https://www.gns3.com/software/download]

3.1 Installing **GNS3**

- The User installing for first time need to registered in GNS3 site and to create an account.

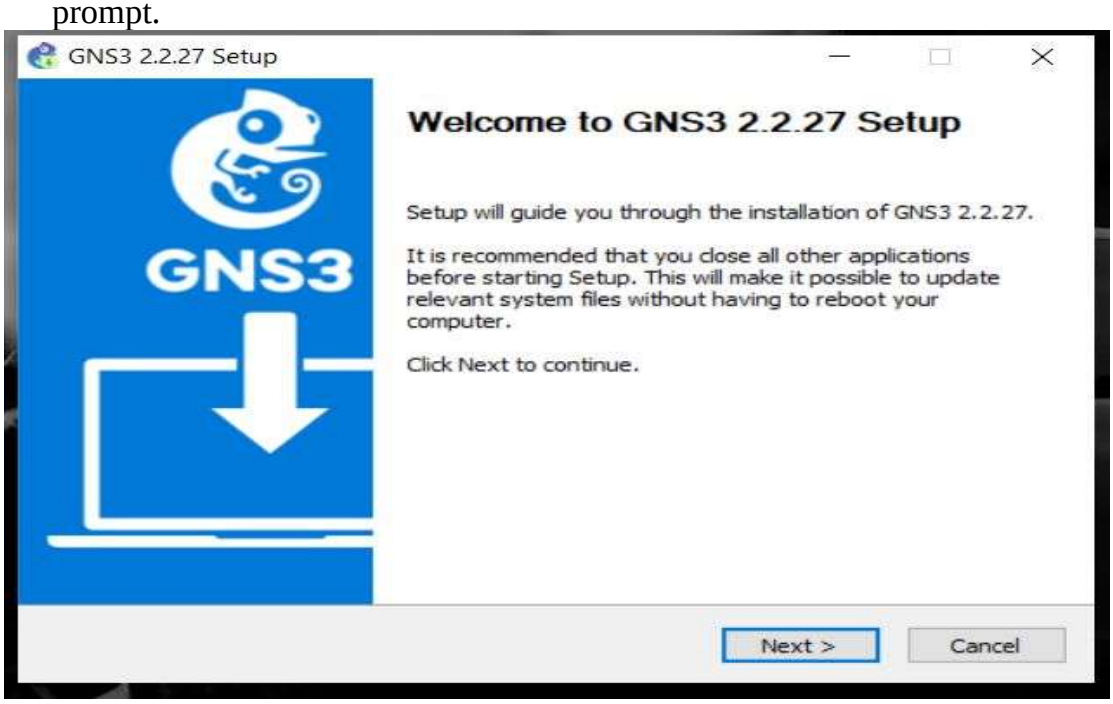


- GNS3 site will prompt user to select the version of GNS3 and to download the version for windows.

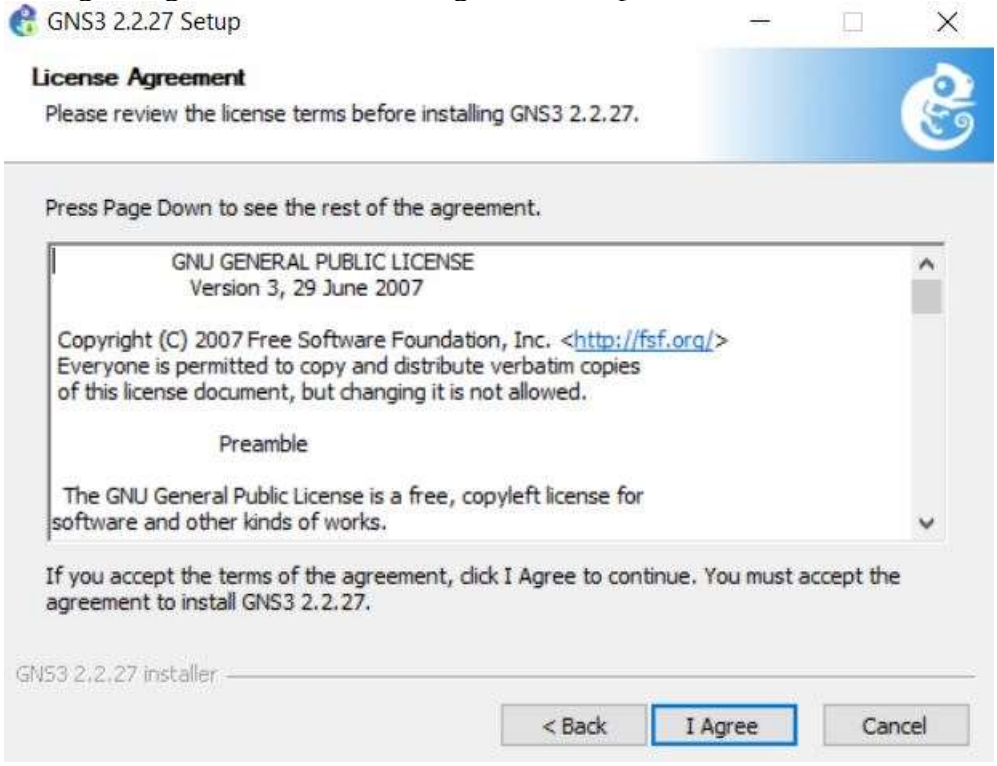


- Installing GNS3-all-in-one package will start automatic download with 85MB file in Size.

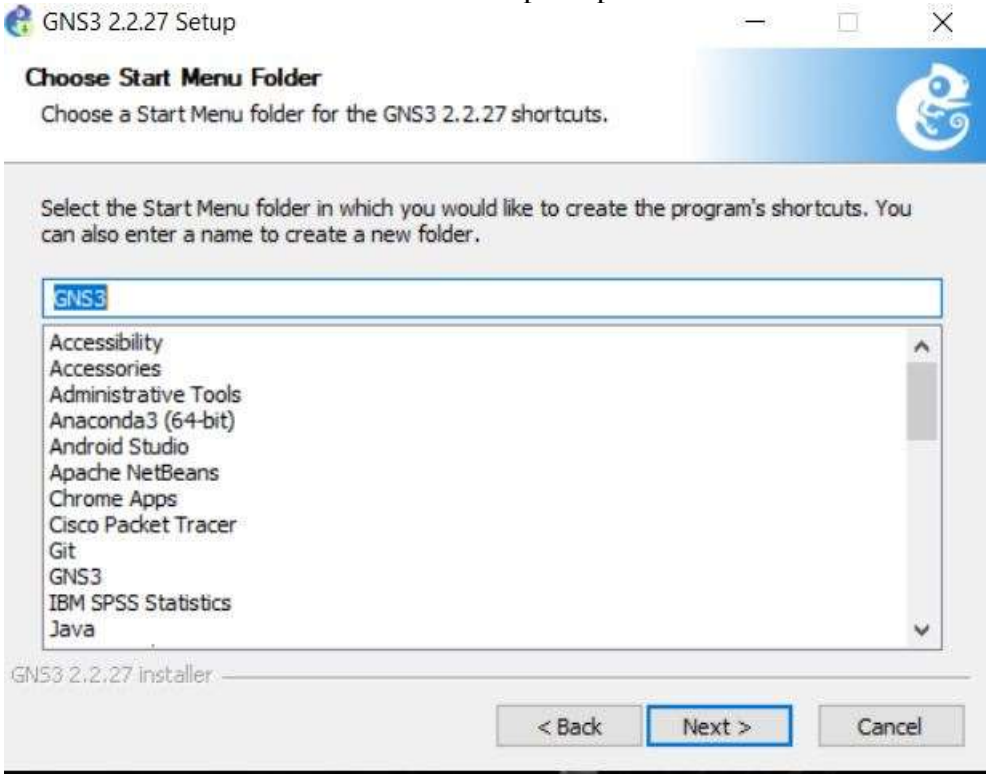
- Navigating to GNS3 folder file, by clicking on GNS3 setup file the below screen is prompt.



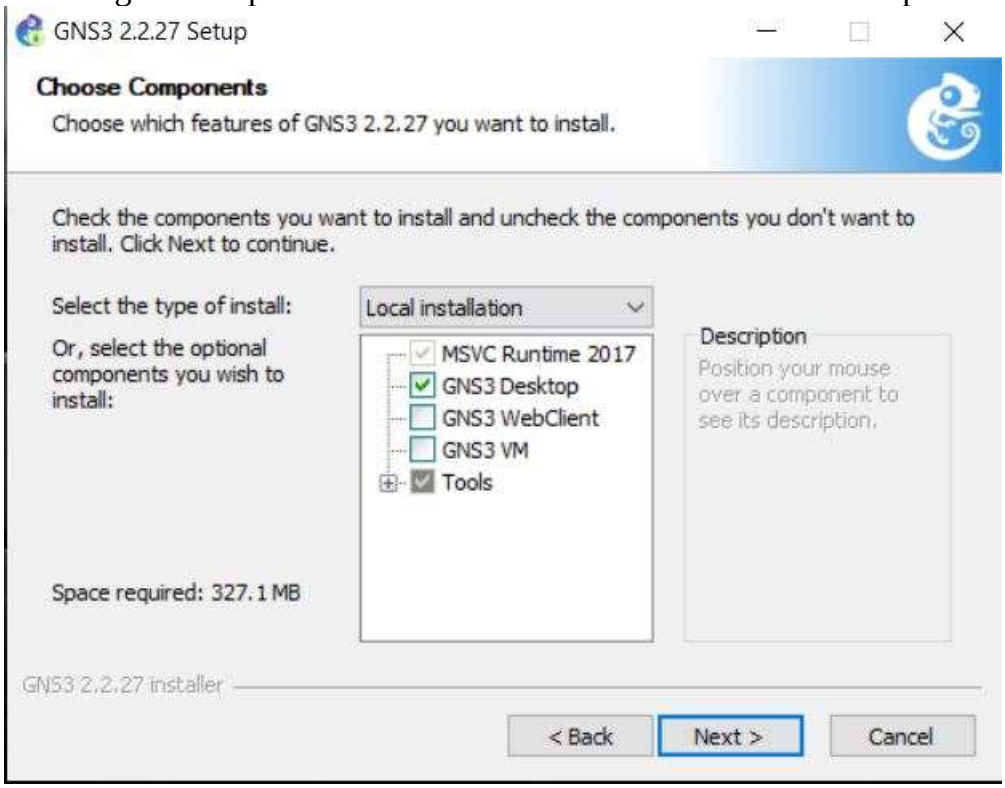
- Agreeing to GNS3 License agreement it proceed to further installation.



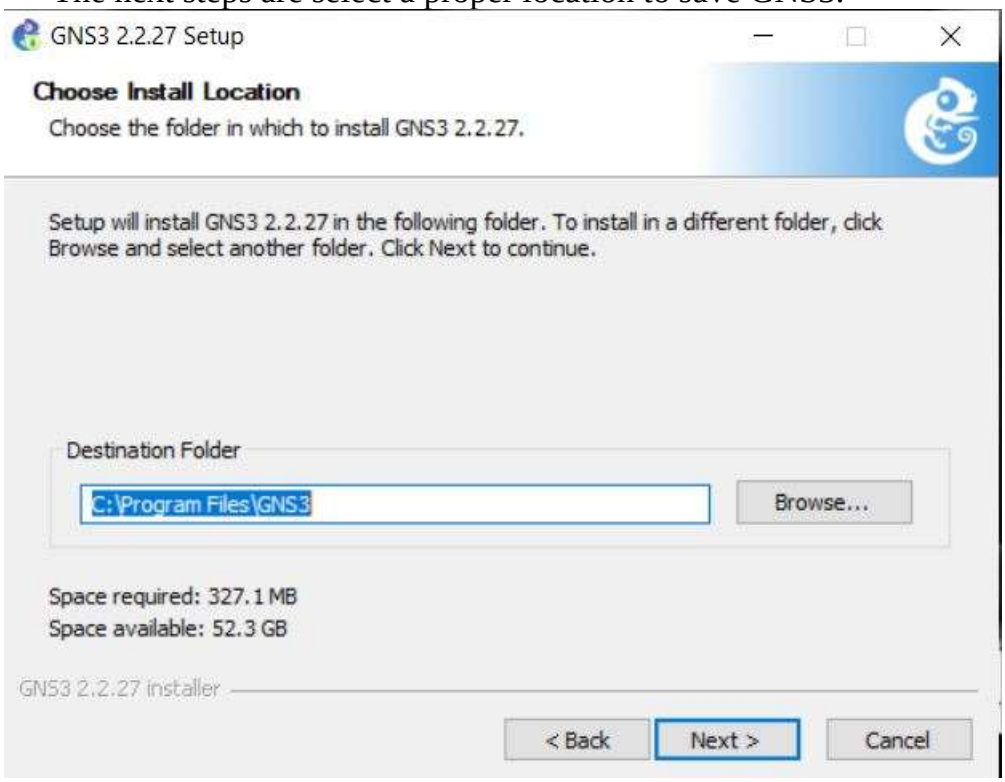
- User can check Start menu folder prompt or user can continue the installation.



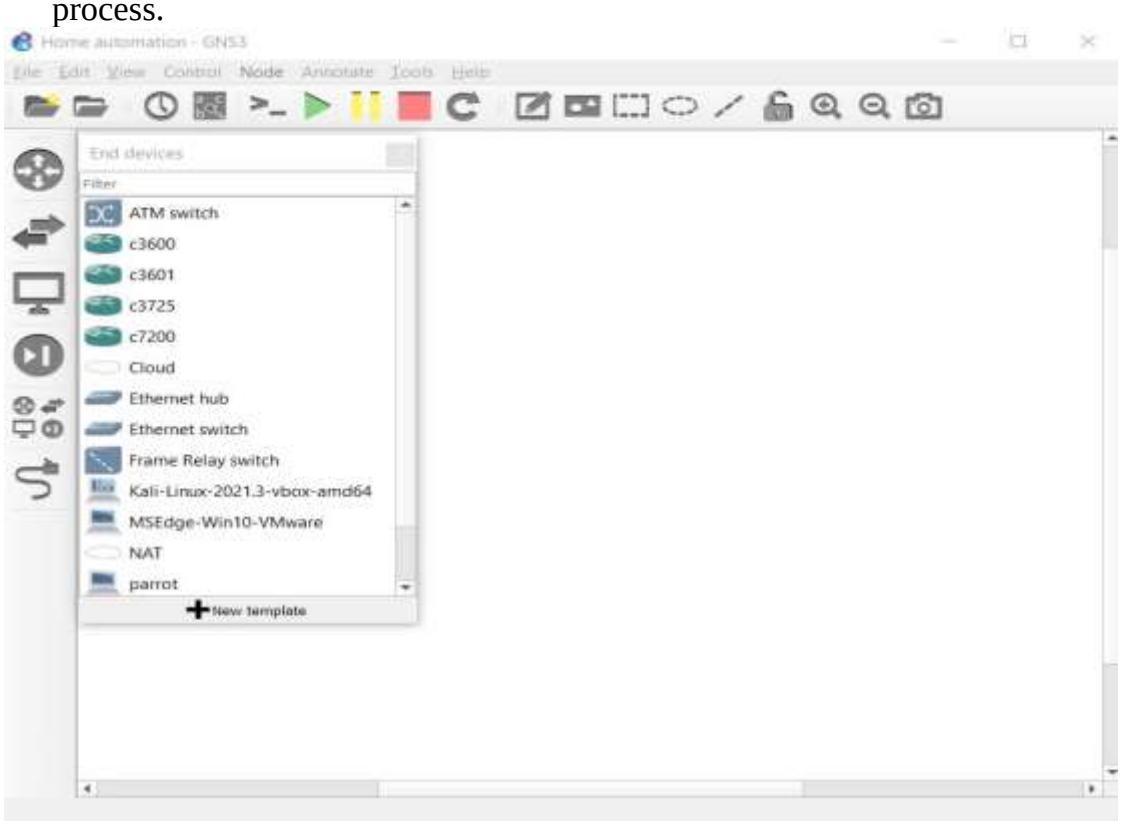
- The gns3 component allows user to select need software components or continue.



- The next steps are select a proper location to save GNS3.

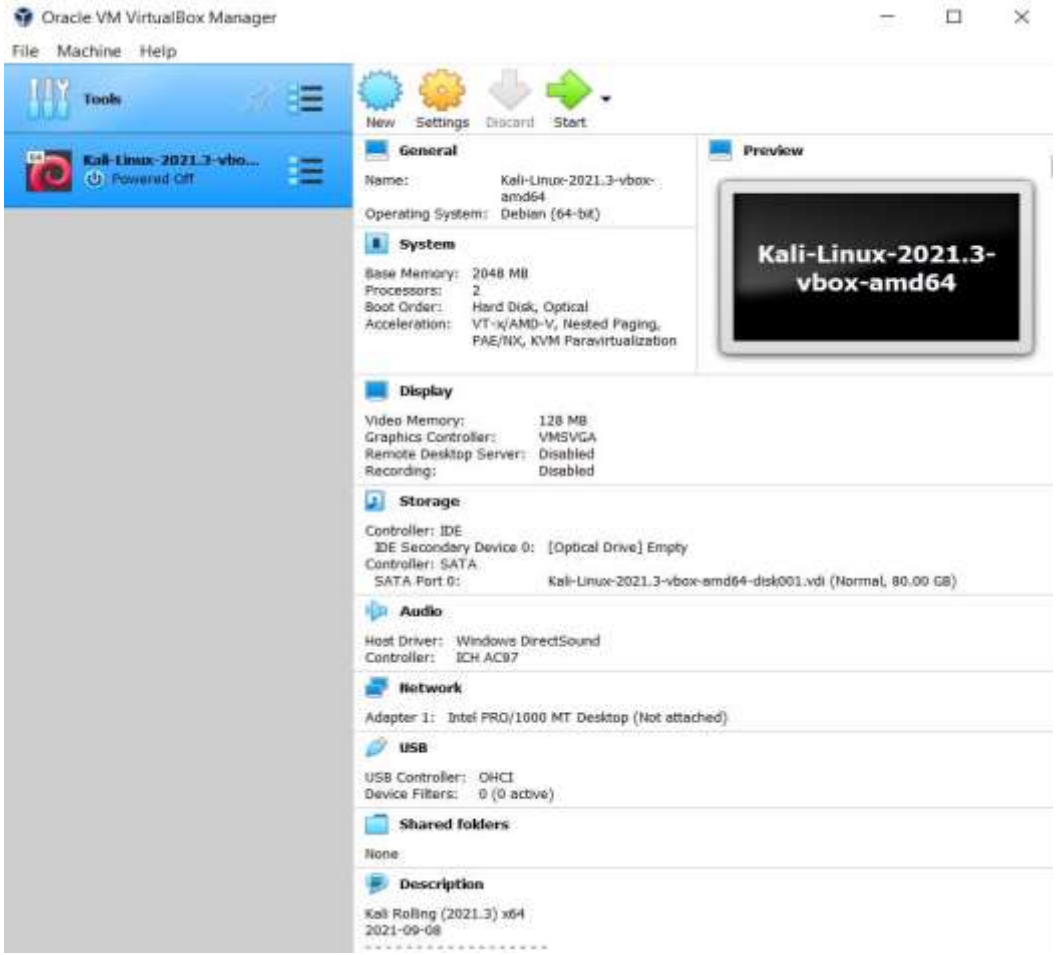


- Once GNS3 software is installed we can **Click Next** and complete the installation process.

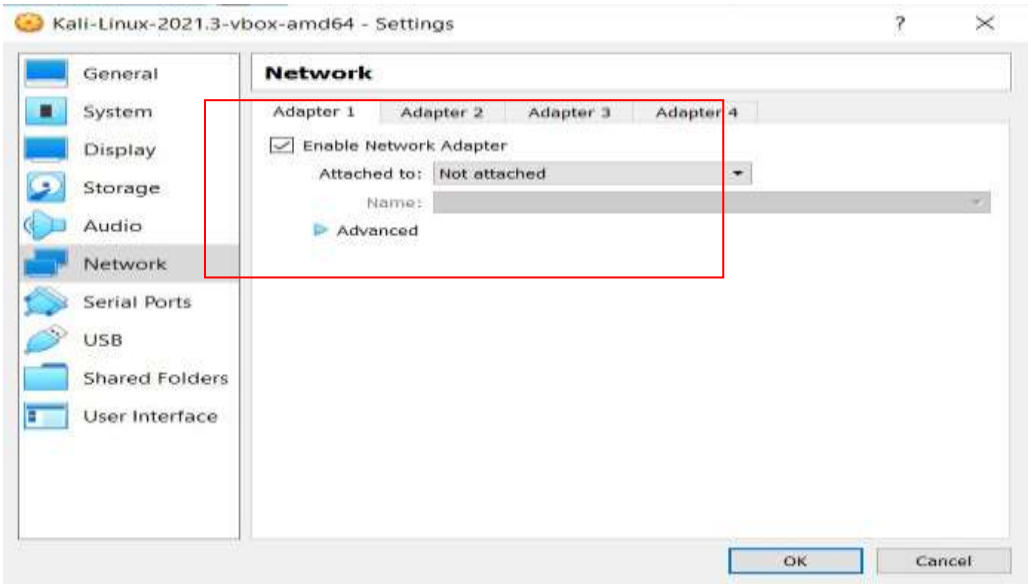


3.2 **Configuring Virtual Box**

- Assuming that users have kali Linux already installed in virtual Box.

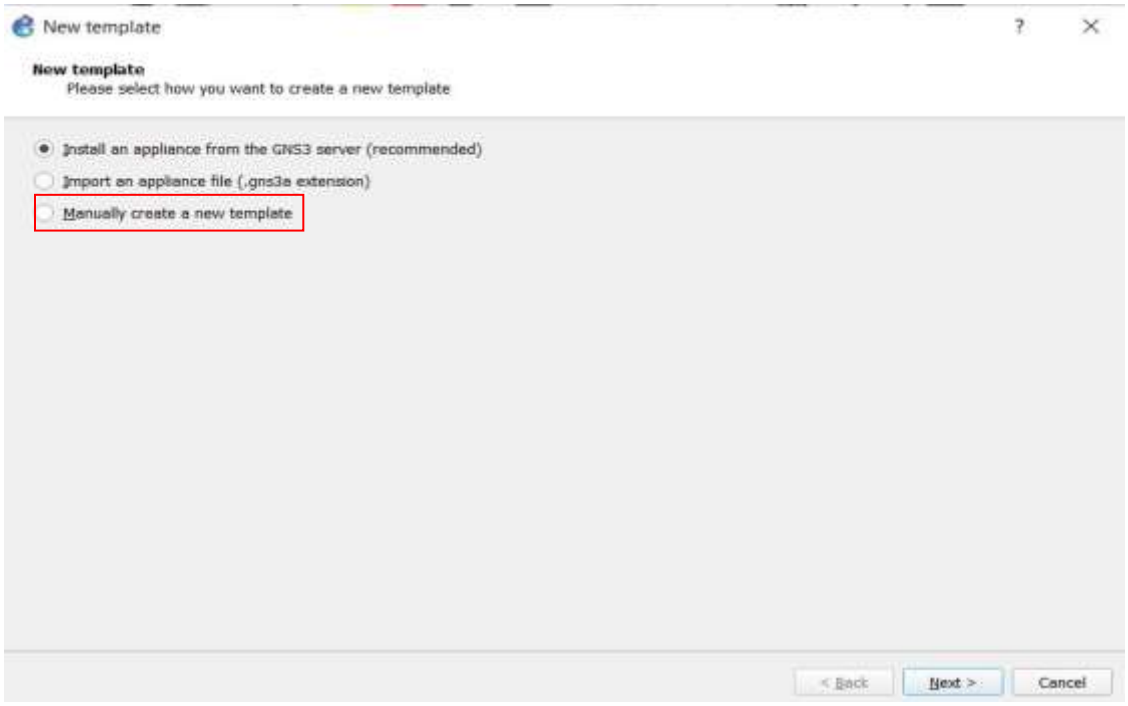


- After installing kali Linux, the network adapter should **not be Attached** to Network such as NAT, Bridge Adapter and so on.

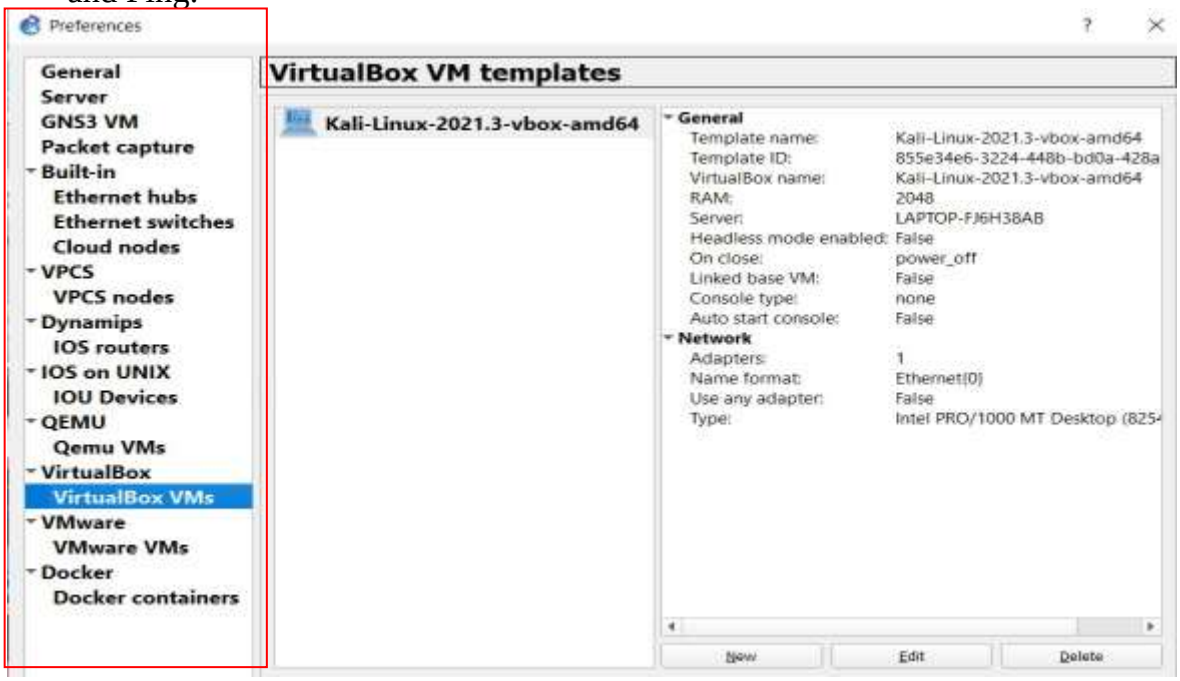


3.3 Configuring VPCS in GNS3

- In Gns3 there is inbuilt option for choosing End devices, selecting Option end devices option prompts.



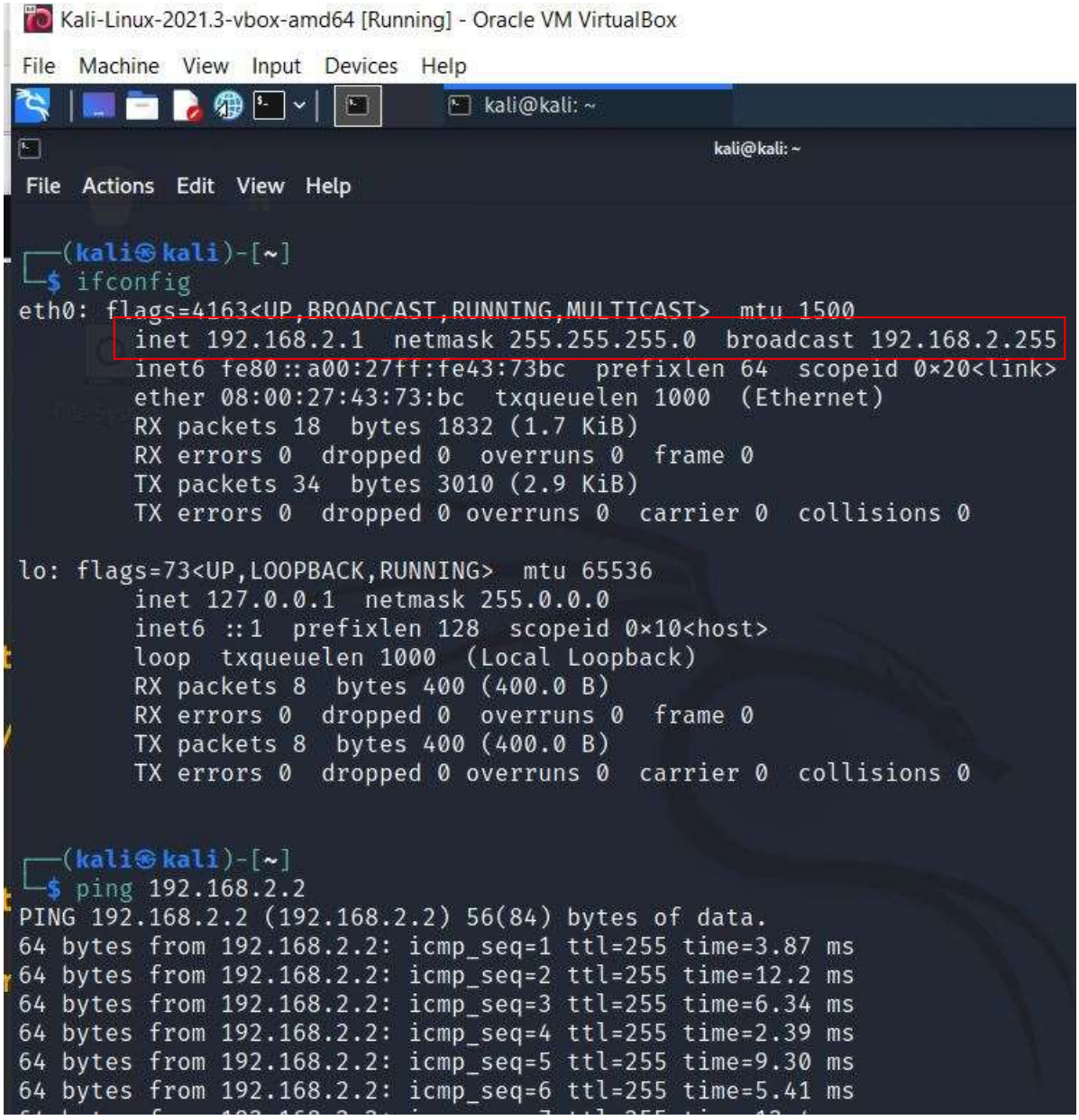
- Gns3 enables users to Import Multiple new appliances template file in-order to add virtual PC simulator which allow user to add lightweight PC which support DHCP and Ping.



- As GNS3 is connected to Virtual Box and VMware to our local host, user can choose different installed machine in virtual box using drop down menu.

- Selecting kali Linux will direct appear as VPCS in end devices.

3.4 Configuring IP Address to Kali in Order to Ping each other in GNS3 topology. (Setting a IP address)



4. Installing Command Line tool in kali Linux to perform Distributed denial of Service attack.

```
┌──(root💀kali)-[~]
└─# sudo apt install -y hping3
Reading package lists... Done
Building dependency tree
Reading state information... Done
hping3 is already the newest version (3.a2.ds2-10).
hping3 set to manually installed.
The following packages were automatically installed and are no longer required:
  libpython3.8-dev python3.8-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1300 not upgraded.
```

```
┌──(root💀kali)-[/home/kali]
└─# hping3 -1 --flood 192.168.2.2
HPING 192.168.2.2 (eth0 192.168.2.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

5. Configuring VRRP Protocol on cisco router.

```
Main-Router1(config)#int e2/1
Main-Router1(config-if)#ip add 10.0.254.20 255.255.255.0
Main-Router1(config-if)#vrrp 1 priority 200
Main-Router1(config-if)#vrrp 1 authentication text cisco
Main-Router1(config-if)#vrrp 1 timers  advertise 3
Main-Router1(config-if)#vrrp 1 timers learn
Main-Router1(config-if)#vrrp 1 ip 10.0.254.10
Main-Router1(config-if)#no shu
Main-Router1(config-if)#no shutdown
Main-Router1(config-if)#
*Mar  1 00:10:31.723: %VRRP-6-STATECHANGE: Et2/1 Grp 1 st
ate Init -> Backup
Main-Router1(config-if)#ex
*Mar  1 00:10:33.711: %LINK-3-UPDOWN: Interface Ethernet2
/1, changed state to up
*Mar  1 00:10:34.711: %LINEPROTO-5-UPDOWN: Line protocol
on Interface Ethernet2/1, changed state to up
Main-Router1(config-if)#exit
*Mar  1 00:10:40.943: %VRRP-6-STATECHANGE: Et2/1 Grp 1 st
ate Backup -> Master
Main-Router1(config-if)#exit
```

- **Checking VRRP Status in order to check priority of master router, Authentication, and advertise interval time.**

```
Main-Router1#show vrrp int e2/1
Ethernet2/1 - Group 1
  State is Master
  Virtual IP address is 10.0.254.10
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 200
  Authentication text "cisco"
  Master Router is 10.0.254.20 (local), priority is 200
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.218 sec
```

- **Configuring Backup router in order to check VRRP Status to check priority of Backup router, Authentication, and advertise interval time.**

```
Backup-Router(config)#int f0/0
Backup-Router(config-if)#ip add 10.0.254.30 255.255.255.0
Backup-Router(config-if)#vrrp 1 priority 100
Backup-Router(config-if)#vrrp 1 authentication text cisco
Backup-Router(config-if)#vrrp 1 timers advertise 3
Backup-Router(config-if)#vrrp 1 timers learn
Backup-Router(config-if)#vrrp 1 ip 10.0.254.10
Backup-Router(config-if)#no shu
Backup-Router(config-if)#no shutdown
Backup-Router(config-if)#
*Mar  1 00:21:01.199: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state I
nit -> Backup
```

```
Backup-Router#sho vrrp int f0/0
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 10.0.254.10
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 100
  Authentication text "cisco"
  Master Router is 10.0.254.20, priority is 200
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.609 sec (expires in 8.645 sec) Lea
rning
```

- **Setting up IP-route command on main router in order to communicate with another virtual router.**

```
Main-Router(config)#ip route 10.10.12.0 255.255.255.252 10.0.254.10
Main-Router(config)#end
Main-Router#pi
*Mar  1 00:34:42.387: %SYS-5-CONFIG_I: Configured from console by console
Main-Router#ping 10.10.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.12.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 60/66/76 ms
Main-Router#
```

6. Configuring load balancer on virtual router on cisco router.

- IP address is already configured, now setting up static route on master router.

```
Main-Router1(config)#ip route 2.2.2.2 255.255.255.255 e1/0 10.10.12.2
Main-Router1(config)#ip route 2.2.2.2 255.255.255.255 e2/0 10.10.13.2
Main-Router1(config)#exit
Main-Router1#
*Mar  1 01:30:22.375: %SYS-5-CONFIG_I: Configured from console by console
Main-Router1#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/30 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, Loopback1
     2.0.0.0/32 is subnetted, 1 subnets
S       2.2.2.2 [1/0] via 10.10.13.2, Ethernet2/0
                [1/0] via 10.10.12.2, Ethernet1/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.10.12.0 is directly connected, Ethernet1/0
C       10.10.13.0 is directly connected, Ethernet2/0
C       10.0.254.0 is directly connected, Ethernet2/1
Main-Router1#
```

- IP address is already configured, now setting up static route on Backup router

```
Backup-Router(config)#ip route 1.1.1.1 255.255.255.255 e1/0 10.10.12.1
Backup-Router(config)#ip route 1.1.1.1 255.255.255.255 e2/0 10.10.13.1
Backup-Router(config)#exit
Backup-Router#sh
*Mar  1 01:40:43.811: %SYS-5-CONFIG_I: Configured from console by console
Backup-Router#sho ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
S       1.1.1.1 [1/0] via 10.10.13.1, Ethernet2/0
                [1/0] via 10.10.12.1, Ethernet1/0
     2.0.0.0/30 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback1
     10.0.0.0/24 is subnetted, 3 subnets
C       10.10.12.0 is directly connected, Ethernet1/0
C       10.10.13.0 is directly connected, Ethernet2/0
C       10.0.254.0 is directly connected, FastEthernet0/0
Backup-Router#
```

- Checking the load balancer working from transmitting ICMP Packet from Main router to backup router.

```
Main-Router1#ping 2.2.2.2  repeat 1 source loopback 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 68/68/68 ms
Main-Router1#
*Mar  1 01:55:19.227: IP: s=10.0.254.20 (local), d=224.0.0.18 (Ethernet2/1), len 40, sending broad/multicast
Main-Router1#
*Mar  1 01:55:20.627: IP: tableid=0, s=1.1.1.1 (local), d=2.2.2.2 (Ethernet1/0), routed via RIB
*Mar  1 01:55:20.631: IP: s=1.1.1.1 (local), d=2.2.2.2 (Ethernet1/0), len 100, sending
*Mar  1 01:55:20.695: IP: tableid=0, s=2.2.2.2 (Ethernet1/0), d=1.1.1.1 (Loopback1), routed via RIB
*Mar  1 01:55:20.695: IP: s=2.2.2.2 (Ethernet1/0), d=1.1.1.1, len 100, rcvd 4
Main-Router1#
```

- Again, transmitting ICMP packet from main router in order to check change in interface.

```
Main-Router1#ping 2.2.2.2  repeat 1 source loopback 1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 68/68/68 ms
Main-Router1#
*Mar  1 01:55:54.931: IP: s=10.0.254.20 (local), d=224.0.0.18 (Ethernet2/1), len 40, sending broad/multicast
*Mar  1 01:55:55.315: IP: tableid=0, s=1.1.1.1 (local), d=2.2.2.2 (Ethernet2/0), routed via RIB
*Mar  1 01:55:55.319: IP: s=1.1.1.1 (local), d=2.2.2.2 (Ethernet2/0), len 100, sending
*Mar  1 01:55:55.379: IP: tableid=0, s=2.2.2.2 (Ethernet1/0), d=1.1.1.1 (Loopback1), routed via RIB
*Mar  1 01:55:55.383: IP: s=2.2.2.2 (Ethernet1/0), d=1.1.1.1, len 100, rcvd 4
```

- Configuring load balancer on interface e1/0

```
Main-Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Main-Router1(config)#int e1/0
Main-Router1(config-if)#ip ?
Interface IP configuration subcommands:
  access-group         Specify access control for packets
  accounting           Enable IP accounting on this interface
  address              Set the IP address of an interface
  admission            Apply Network Admission Control
  auth-proxy           Apply authentication proxy
  authentication       authentication subcommands
  bandwidth-percent    Set EIGRP bandwidth limit
  bgp                  BGP interface commands
  broadcast-address    Set the broadcast address of an interface
  cef                  Cisco Express Forwarding interface commands
  cgmp                 Enable/disable CGMP
  ddns                 Configure dynamic DNS
  dhcp                 Configure DHCP parameters for this interface
  directed-broadcast   Enable forwarding of directed broadcasts
  dvmrp                DVMRP interface commands
  flow                 NetFlow related commands
  hello-interval       Configures IP-EIGRP hello interval
  helper-address       Specify a destination address for UDP broadcasts
  hold-time            Configures IP-EIGRP hold time
  idle-group           Specify interesting packets for idle-timer
  igmp                 IGMP interface commands
  information-reply    Enable sending ICMP Information Reply messages
  inspect              Apply inspect name
  ips                  Create IPS rule
  irdp                 ICMP Router Discovery Protocol
  load-sharing         Style of load sharing
```

- Selecting load-sharing per-packet

```
Main-Router1(config-if)#ip lo
Main-Router1(config-if)#ip load
Main-Router1(config-if)#ip load-sharing ?
  per-destination  Deterministic distribution
  per-packet       Random distribution

Main-Router1(config-if)#ip load-sharing per
Main-Router1(config-if)#ip load-sharing per-packet
```

- Checking the result in order to check load distribution working on per packet

```
Main-Router1#u
*Mar  1 02:10:27.583: IP: s=10.0.254.20 (local), d=224.0.0.18 (Ethernet2/1), len 40, sending broad/multicast
*Mar  1 02:10:27.947: IP: tableid=0, s=10.10.12.1 (local), d=2.2.2.2 (Ethernet1/0), routed via RIB
*Mar  1 02:10:27.951: IP: s=10.10.12.1 (local), d=2.2.2.2 (Ethernet1/0), len 100, sending
*Mar  1 02:10:28.015: IP: tableid=0, s=2.2.2.2 (Ethernet1/0), d=10.10.12.1 (Ethernet1/0), routed via RIB
*Mar  1 02:10:28.015: IP: s=2.2.2.2 (Ethernet1/0), d=10.10.12.1 (Ethernet1/0), len 100, rcvd 3
Main-Router1#u all
All possible debugging has been turned off
Main-Router1#
*Mar  1 02:10:30.347: IP: s=10.0.254.20 (local), d=224.0.0.18 (Ethernet2/1), len 40, sending broad/multicast
```

- Second result Clearly showcase load balancer working

```
Main-Router1#
*Mar  1 02:10:46.919: IP: s=10.0.254.20 (local), d=224.0.0.18 (Ethernet2/1), len 40, sending broad/multicast
*Mar  1 02:10:47.131: IP: tableid=0, s=10.10.13.1 (local), d=2.2.2.2 (Ethernet2/0), routed via RIB
*Mar  1 02:10:47.135: IP: s=10.10.13.1 (local), d=2.2.2.2 (Ethernet2/0), len 100, sending
*Mar  1 02:10:47.195: IP: tableid=0, s=2.2.2.2 (Ethernet2/0), d=10.10.13.1 (Ethernet2/0), routed via RIB
*Mar  1 02:10:47.199: IP: s=2.2.2.2 (Ethernet2/0), d=10.10.13.1 (Ethernet2/0), len 100, rcvd 3
Main-Router1#u all
```

References

- GNS3 Documentation. 2021. *Getting Started with GNS3*. [online] Available at: <https://docs.gns3.com/docs/> [Accessed 15 December 2021].