NETWORK + LAB SERIES

Lab 04: Understanding Network and Port Address Translation

Document Version: 2024-05-06

Material in this Lab Aligns to the Following	
CompTIA Network+ (N10-009) Exam Objectives	2.1 Explain characteristics of routing technologies. 3.1 Explain the purpose of organizational processes and procedures. 3.5 Compare and contrast network access and management methods.

Contents

Introduction

This lab is part of a series of lab exercises designed to supplement coursework and provide students with a hands-on training experience based on real-world applications. This series of lab exercises is intended to support courseware for CompTIA Network+® certification.

Due to the exponential growth of the Internet and the numerous devices being added, IPv4 addresses depleted quite rapidly in the late 1980s to early 1990s. IPv6 was not a viable solution during this time as devices and operating systems were not yet compatible. One of the greatest solutions to the IPv4 address crisis was the development and implementation of Network Address Translation (NAT) and private IPv4 addresses. A block of IPv4 addresses from each class (A, B and C) was excluded from the public range by the Internet Assigned Numbers Authority (IANA). These addresses were labeled as private, and published in the Request for Comment #1918 (RFC1918) document by the IETF in February 1996. The table below displays the range of private addresses from each class.

Class	Address Range	Prefix Length
A	10.0.0.0 - 10.255.255.255	8
B	172.16.0.0 - 172.31.255.255	12
C	192.168.0.0 - 192.168.255.255	16

You may recognize the 192.168.X.X address in use inside your home network. This range is normally used in Small Office, Home Office (SOHO) networks.

Prior to the development of private addresses, all addresses were public, and all devices on a network had to be assigned a public address. Private addresses are designed to be used on inside networks only and cannot be routed through the Internet. This means that these private addresses can be used on any internal network, thus minimizing the need for public addresses. However, how does a device configured with a private address reach the Internet? These private addresses must be translated into a public address using NAT. NAT is a protocol that converts private IPv4 addresses into public IPv4 addresses by modifying the IP header in a packet. Translation can be performed by a router or by a device dedicated to NAT services. There are several types of NAT implementations in IPv4 networks today. Source NAT is also known as Port Address Translation (PAT) or NAT Overload. Destination NAT is also known as Port Forward and is mainly used to redirect outside traffic into a private network. The other type of NAT is known as 1-to-1 NAT, where both DNAT and SNAT (bidirectional NAT) are used. NAT has been the lifesaver to the IPv4 address crisis and still is widely deployed today.

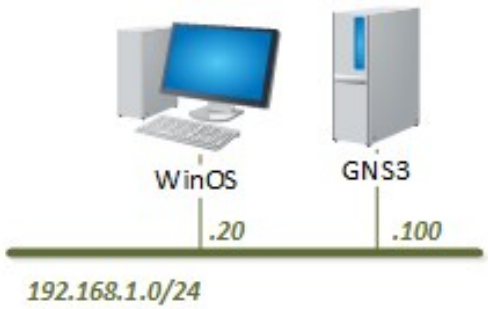
Objective

This lab will utilize the Windows Server (WinOs) and GNS3 to be able to configure NAT. GNS3 is a powerful Graphical Network Simulator used to emulate end user and networking devices. The commands used in this lab are based on the Linux OS utilizing a Vyos router and an Exos multi-layer switch within the GNS3 environment. Testing and verification commands will be used to validate successful configuration.

In this lab, students will:

1. Configure Source NAT (SNAT), also known as PAT or NAT Overload
2. Verify SNAT Configuration
3. Configure Destination NAT (DNAT), also known as Port Forward
4. Verify DNAT Configuration
5. Configure 1-to-1 NAT
6. Verify 1-to-1 NAT

Lab Topology



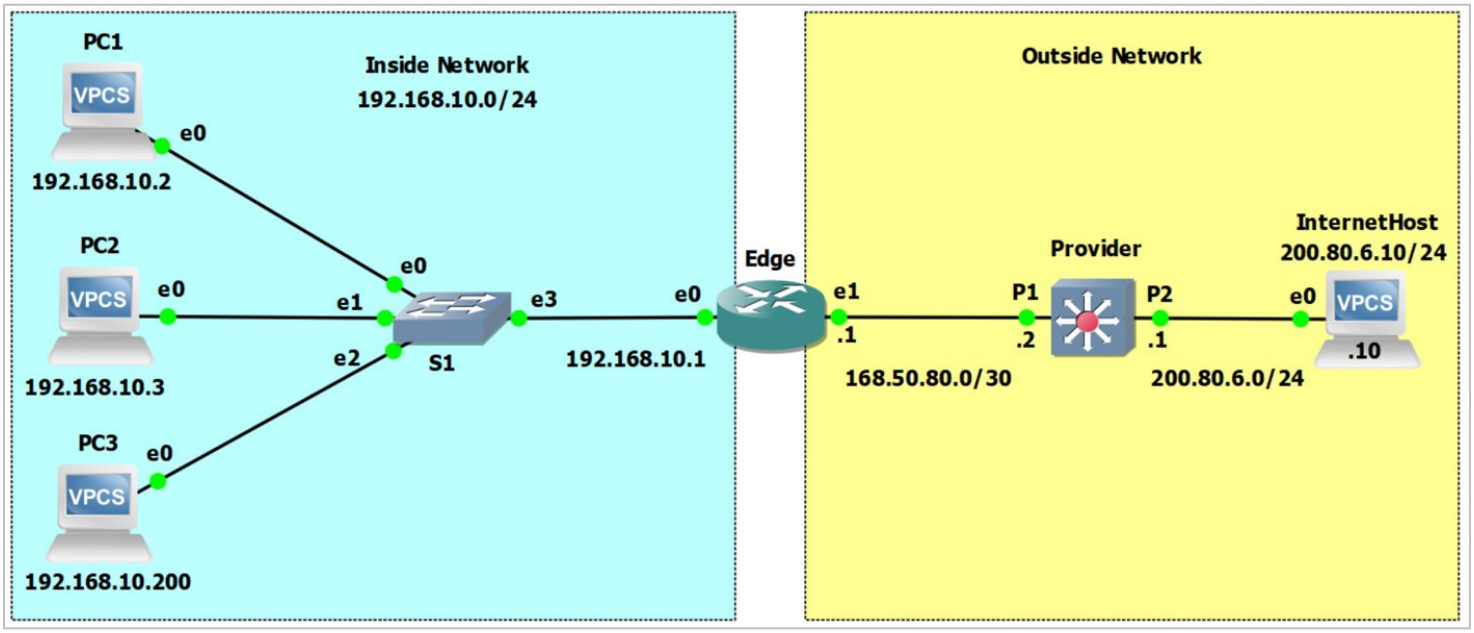
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
GNS3	192.168.1.100/24	**gns3**	gns3
WinOS	192.168.1.20/24	**Administrator**	NDGlabpass123!
EXOS		**admin**	<no password>
VyOS		**vyos**	vyos

1 Topology and Addressing Table

NAT Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	e0 NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC2	e0 NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC3	e0 NIC	192.168.10.200	255.25.255.0	192.168.10.1
InternetHost	e0 NIC	200.80.6.10	255.255.255.0	200.80.6.1
Edge	e0	192.168.10.1	255.255.255.0	N/A
	e1	168.50.80.1	255.255.255.252	N/A

2 Network Address Translation (NAT)

The most common type of NAT implementation is Bidirectional NAT, where both SNAT and DNAT are configured on a router. DNAT or 1-to-1 NAT provides one-to-one address mapping. It is used when an external public host needs to access an internal private host. An example is when a customer needs to access a private host behind a router's public IP address.

SNAT is the most widely used form of NAT. Devices inside a network with private addresses are dynamically assigned a public address from a predefined pool as needed for translation. PAT overloads a single public IP address from a pool or from a single interface address. This overloading is also known as masquerading. With PAT, each private-to-public translation is assigned a unique source port number. There are 65,536 port numbers (0 to 65,535). The use of these dynamically assigned port numbers for each translation provides many-to-one NAT mapping. Therefore, a single public address can be overloaded with many private addresses. Theoretically, approximately 65,536 private addresses can be translated to a single public address with PAT; however, because each translation demands RAM usage, the number of translations possible is limited by the memory available. The Vyos router used in this lab recommends 1 public IP address for every 256 private addresses.

The device doing the actual translation is normally a router in most networks. This device builds a table known as the NAT table, which keeps a temporary record of each dynamic translation. NAT time out is the term used to describe how long a translation will stay in the NAT table before aging out. This time can be configured by a network administrator. The default for most is 30 seconds. Since the NAT router is the only device that knows the true private address of devices in a LAN, end-to-end reachability is lost. However, this is actually good in hiding (masquerading) the actual private IP address of devices inside a LAN. Accessing the NAT table is the only way to view the mapping of private-to-public addresses.

There are four types of NAT addresses to be familiar with. There are:

- **Inside Local** – This is the private IP address assigned to hosts inside a LAN
- **Inside Global** – This is the public address a private address is translated to
- **Outside Local** – This is normally the IP address assigned to the outside interface of the NAT router
- **Outside Global** – This is the destination device outside on another network or the Internet

In this lab, you will be using the following topology and addressing table to configure and verify SNAT, DNAT, and 1-to-1 NAT (static or bi-directional). Some configurations have already been done, which you will learn how to do in subsequent labs. In this lab, the Provider multi-layer switch is already configured. You will be configuring the IP addressing of the host devices, the Edge router interface addresses, and several types of NAT. The host name for the Linux Vyos router is Edge in the topology. Rules will be created for both SNAT and DNAT. SNAT modifies the Source IP Address field in a packet, and DNAT modifies the Destination IP Address.

3 Basic Device Configurations

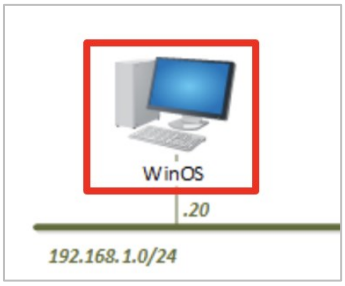
Before network services and protocols can be configured in network devices, basic configuration tasks must be done. Interfaces need to be properly addressed and enabled. End user devices must also be configured and enabled. Of course, all physical connections must be correct between the devices. You will be using the NAT topology diagram as well as the addressing table to complete these steps.

- Configure the PCs in the Inside Network
- Configure the Edge Router (Vyos) inside and outside interfaces
- Verify Connectivity between devices

3.1 End User Device and Basic Router Configuration

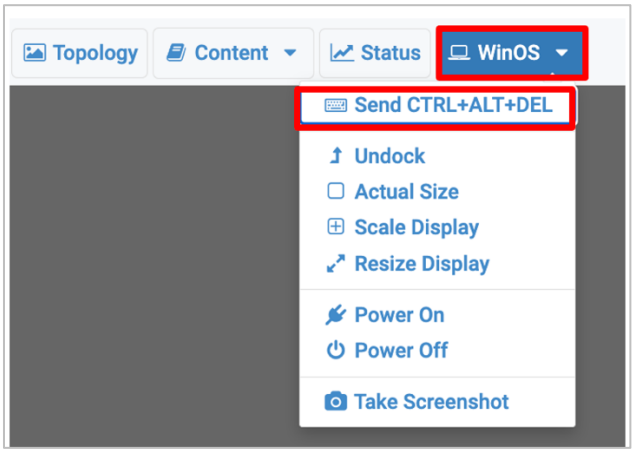
In the following steps, you will use WinOS to launch the GNS3 Application and load the network for NAT. We will first have to configure addressing on the host devices and the Edge router. Refer to the NAT topology and addressing table to complete the following steps.

1. Open a console connection to the **WinOS** system.



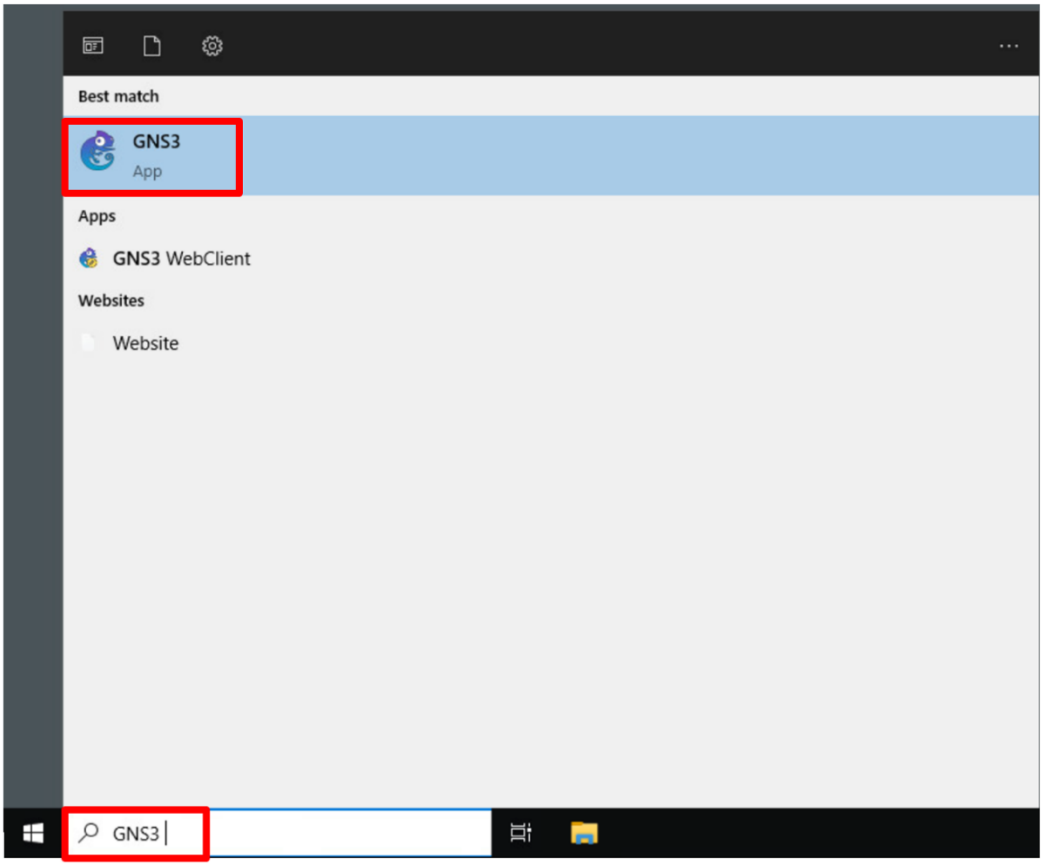
You can open a console connection by clicking on the device tab or the device icon in the topology image.

2. Next, click the **down arrow** next to the **WinOS** tab, and then click **Send CTRL+ALT+DEL** to the get to the log in screen.



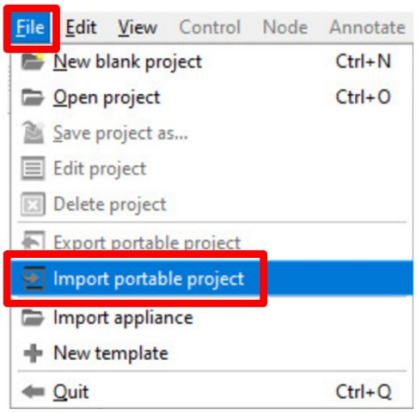
3. Log in to the WinOS machine using the following credentials:
   Username: `Administrator` Password: `NDGlabpass123!`

4. In the Windows search bar, type `GNS3`, and then click the **GNS3** App.

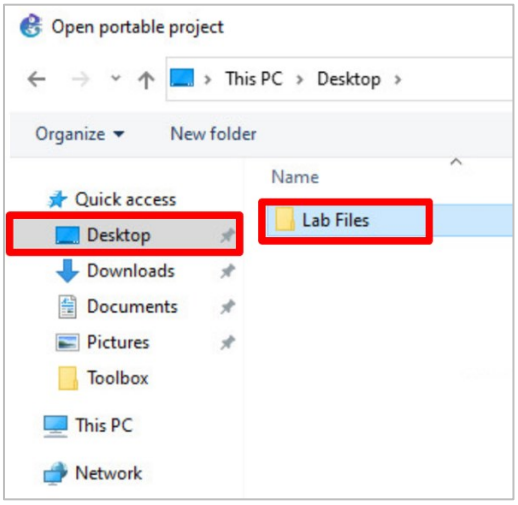


5. The GNS3 Emulator opens. In the Project window, click **Cancel.**

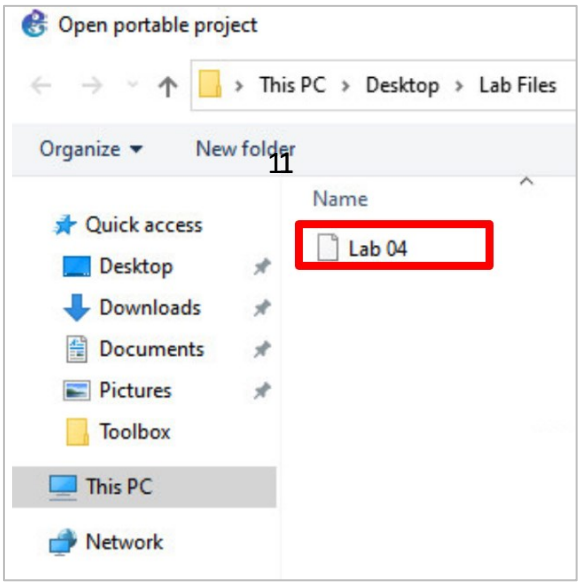
6. In the GNS3 App window, click **File**, and then click **Import portable project**.



7. In the Open portable project window, click **Desktop**, and then double-click the **Lab Files** folder.

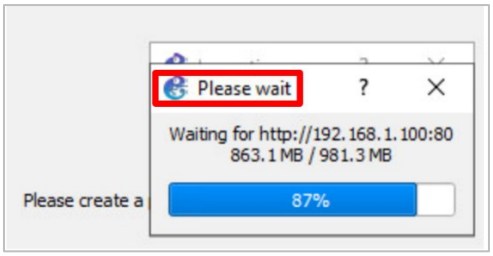


8. Double-click **Lab 04.**

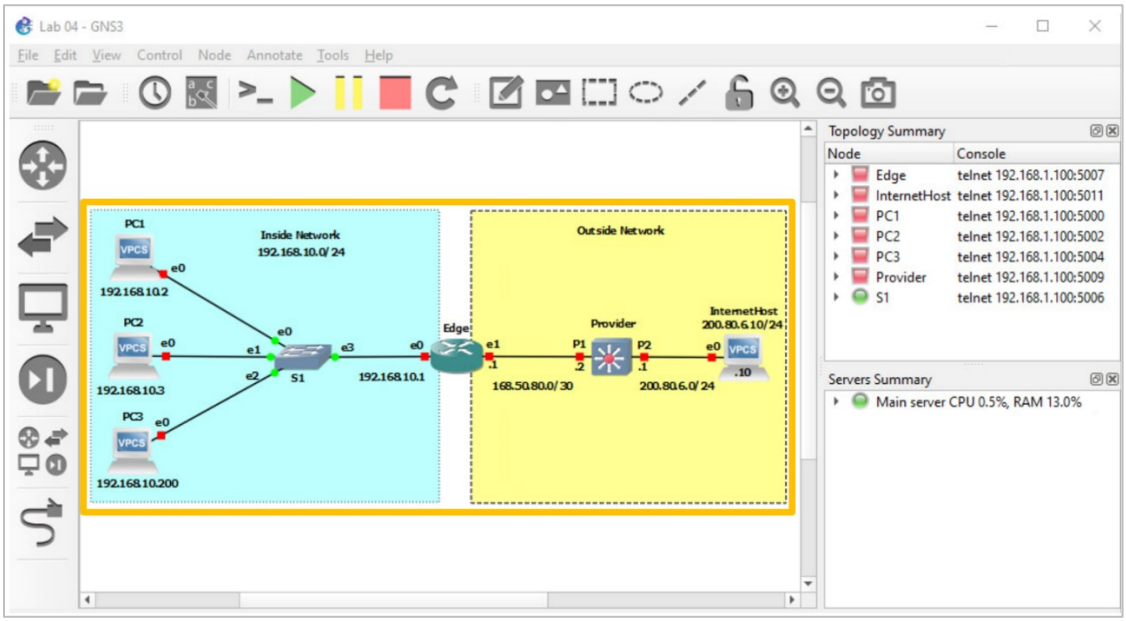


9. The Project window opens with **Lab 04** in the *Name* field. Click **OK** to open Lab 04.

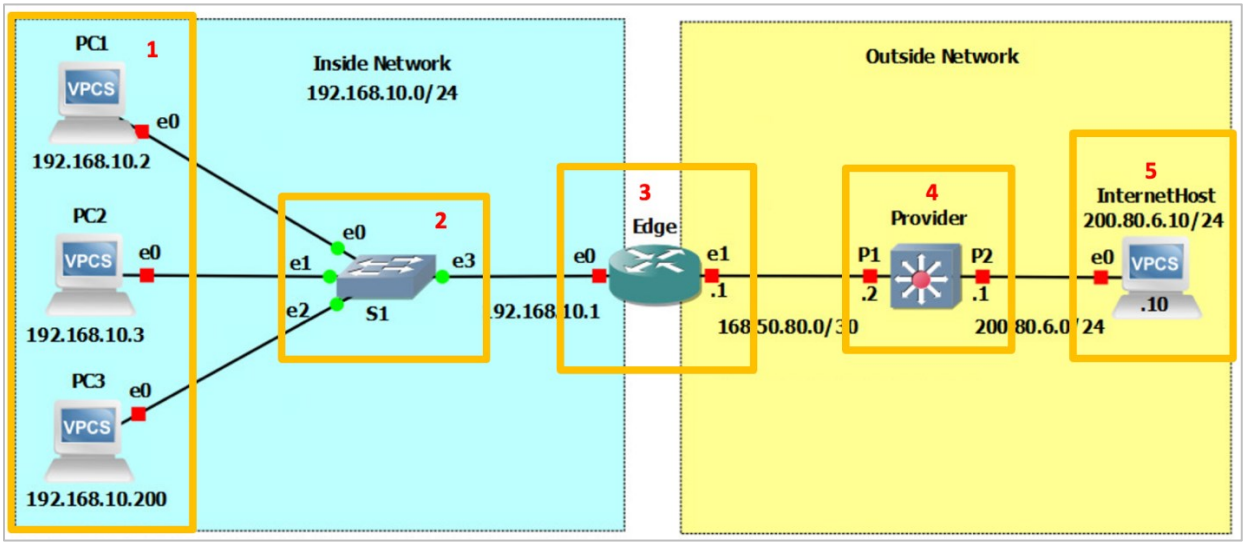
10. It will take about 1 minute for Lab 04 to load. You will see the **Please wait** screen displaying the progress.



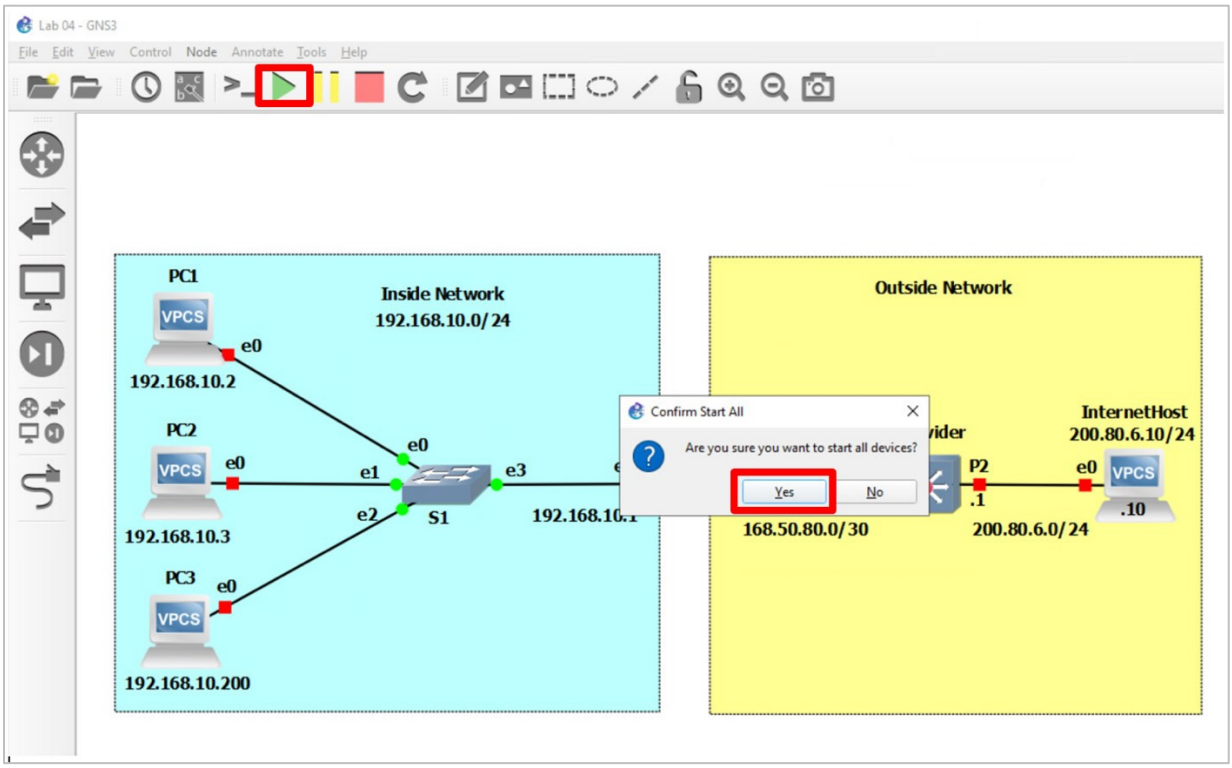
11. The Lab 04 GNS3 network topology is now visible and matches the NAT topology on page 7.



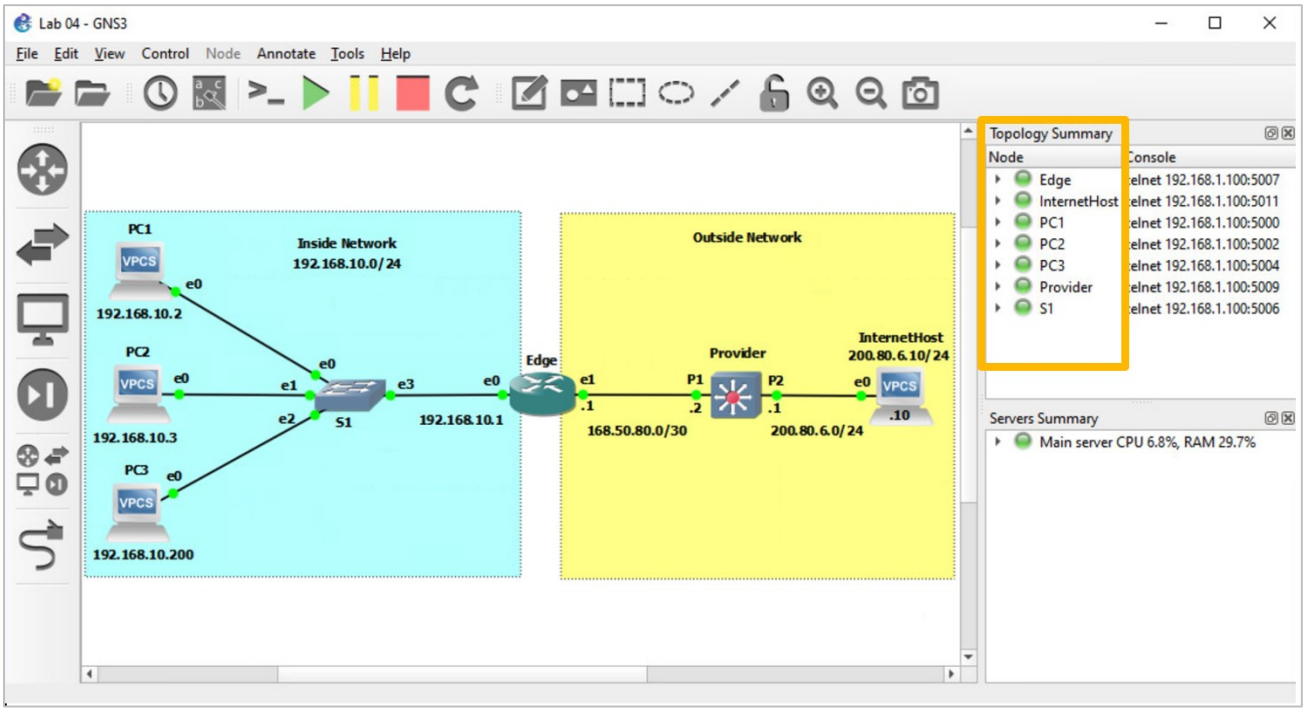
12. The network consists of an **Inside Network** (highlighted in blue) and an **Outside Network** (highlighted in yellow). The inside network consists of **3 PCs** (1), a layer 2 switch, **S1** (2), and a router, **Edge** (3). The outside network consists of the same router (3), a layer 3 multi-layer switch, **Provider** (4), and a PC representing an outside host, I**nternetHost** (5). All devices have host names and are labeled in the topology. Also notice that most devices have a red square box indicating that these devices are not powered on except switch S1.



13. Next, we need to start the devices in the network. In the top menu bar, click the big **green arrow** to start all nodes. In the Confirm Start All window, click **Yes**.



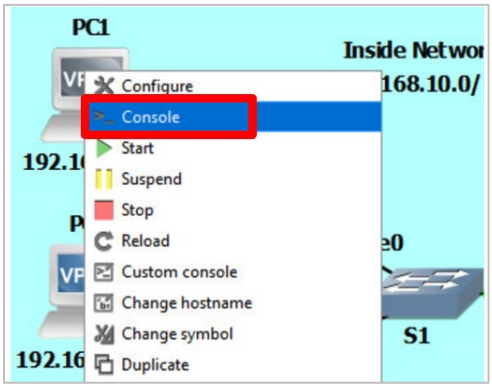
14. All connections between devices are now green, indicating all devices have started. Notice that in the Topology Summary, all nodes have also turned from red to green.



The GNS3 network is now ready for configuration. In the next steps, we will configure IP addressing parameters on PC1, PC2, PC3, and the InternetHost. We will then configure IP addressing on the interfaces of the Edge router, and finally we will configure and verify SNAT and DNAT. Use the topology and addressing table on page 7 for reference.

15. Configure the PCs.

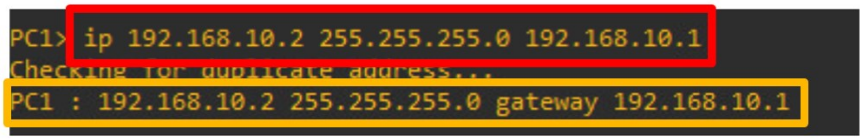
    a. Right-click **PC1**, and then click the **Console** icon.



b. The PC1 **solarwinds** console window opens. Press **Enter** to access the PC1 prompt.

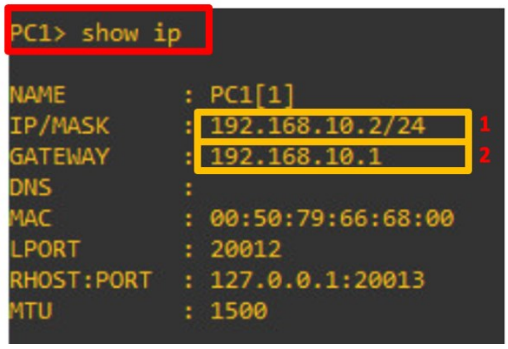
c. Next, we will configure an IPv4 address, subnet mask, and default gateway on PC1. Referencing the topology, PC1 is assigned the IP address of 192.168.10.2, with a subnet mask of 255.255.255.0 or /24, and a default gateway of 192.168.10.1. Notice that the default gateway is the e0 IP address of Edge. In the PC1 console, enter the following command.

PC1> `ip 192.168.10.2 255.255.255.0 192.168.10.1`



Notice that after checking for duplicate addresses, the IP address assigned to PC1 is: **192.168.10.2**, the subnet mask is **255.255.255.0**, and the default **gateway** is **192.168.10.1**.

d. To verify these parameters, type `show ip` at the PC1 prompt. Notice the **IP/MASK** (1) and **GATEWAY** (2).



e. Repeat steps 15a through 15d to configure PC2, PC3, and the InternetHost. Use the addressing table or topology for the proper configuration parameters for these devices. Use the **show ip** command on PC2 and PC3 to verify correct addressing.

```
PC2> ip 192.168.10.3/24 192.168.10.1
Checking for duplicate address...
shPC2 : 192.168.10.3 255.255.255.0 gateway 192.168.10.1

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 192.168.10.3/24
GATEWAY     : 192.168.10.1
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 20014
RHOST:PORT  : 127.0.0.1:20015
MTU         : 1500
```

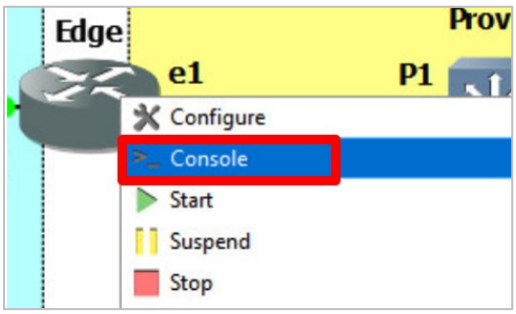
```
PC3> ip 192.168.10.200/24 192.168.10.1
Checking for duplicate address...
PC3 : 192.168.10.200 255.255.255.0 gateway 192.168.10.1

PC3> show ip

NAME        : PC3[1]
IP/MASK     : 192.168.10.200/24
GATEWAY     : 192.168.10.1
DNS         :
MAC         : 00:50:79:66:68:02
LPORT       : 20016
RHOST:PORT  : 127.0.0.1:20017
MTU         : 1500
```

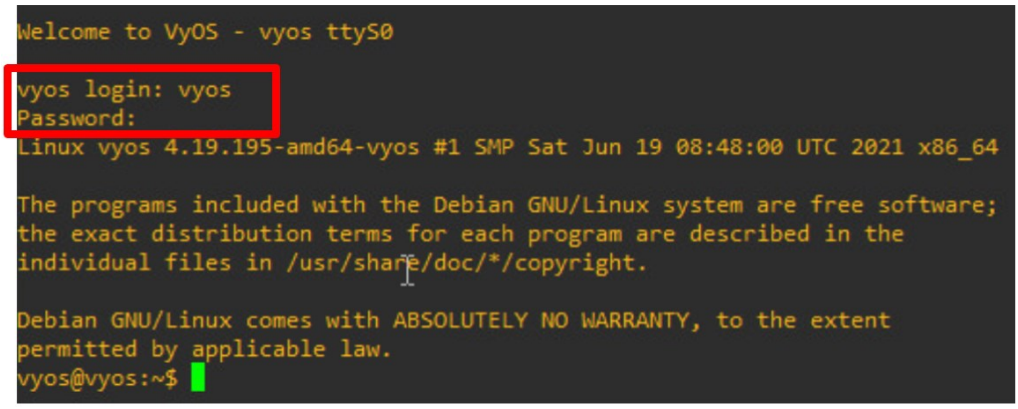
16. Configure the interfaces on Edge.

a. The Edge router has two interfaces, e0 and e1. The e0 interface is the inside interface and is the default gateway for the internal hosts PC1, PC2 and PC3. The e1 interface is the outside interface, which connects to the Provider network. In this lab, the Provider multi-layer switch is already configured. In the real world, you would not have access to your service provider network. To configure Edge, we need to open a console as we did with the PCs. Right-click on the **Edge** router, and then click **Console**.

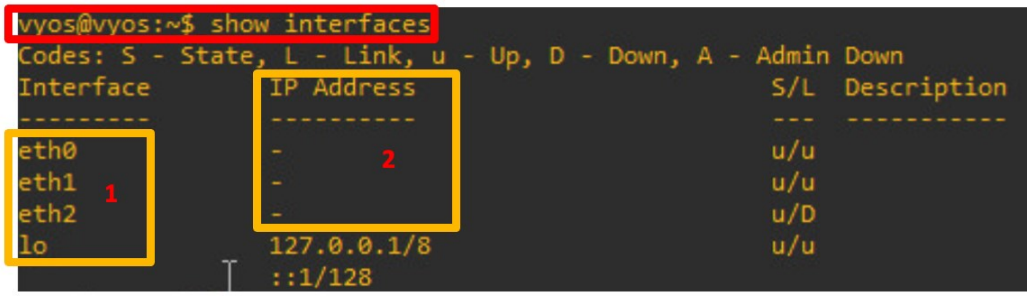


b. The console displays the **Welcome to Vyos** banner and prompts you to login. In this lab, the Vyos router is named Edge in the topology.

c. Login to the Vyos router (Edge) using the following credentials:
Username: `vyos` Password: `vyos`



d. At the vyos@vyos:~$ prompt, type `show interfaces` to see the currently installed interfaces and their IP address. Notice there are three Ethernet interfaces (1): **eth0**, **eth1**, **eth2**, and one loopback interface **lo**. Also notice that the three Ethernet interfaces have no **IP address** (2) assigned to them.



e. To configure anything on Vyos, we need to enter configuration mode. At the Vyos prompt, type `configure`. Notice the prompt changed from a **$** to a **#**.

f. Next, we will configure IP parameters on interface eth0 and eth1. To configure eth0, type `set interfaces ethernet eth0 address 192.168.10.1/24`, and then press **Enter**. Next, set an interface description. Type `set interfaces ethernet eth0 description 'Inside Network'`, and then press **Enter**. Interface descriptions are not mandatory but are useful reminders of what an interface is connected to or used for.

```
vyos@vyos# set interfaces ethernet eth0 address 192.168.10.1/24
[edit]
vyos@vyos# set interfaces ethernet eth0 description 'Inside Network'
[edit]
vyos@vyos#
```

g. Next repeat the same commands to configure eth1 using the address shown in the addressing table and topology. Use the description `'Outside Network'`.

```
vyos@vyos# set interfaces ethernet eth1 address 168.50.80.1/30
[edit]
vyos@vyos# set interfaces ethernet eth1 description 'Outside Network'
[edit]
vyos@vyos#
```

h. To accept the configurations you just made, type `commit`.

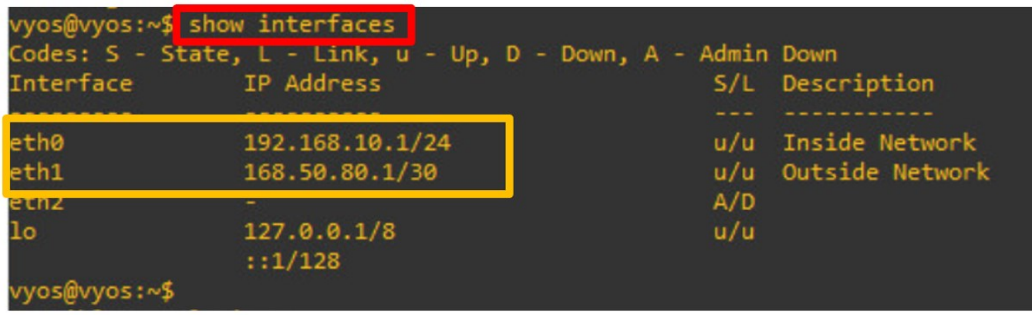
```
vyos@vyos# commit
[edit]
vyos@vyos#
```

i. Next, we will verify that eth0 and eth1 were properly configured. To do this, we must first exit configure mode. Type `exit` at the prompt.

```
vyos@vyos# exit
Warning: configuration changes have not been saved. 2
exit
vyos@vyos:~$ 1
```

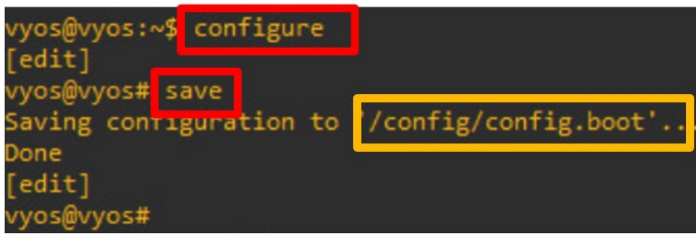
j. Notice that the prompt changes back to the **$** (1). Also observe the **Warning:** (2) message stating that **configuration changes have not been saved**. We will save the configuration later.

k. To verify that eth0 and eth1 are correctly configured, type **`show interfaces`** at the **`$`** prompt.



l. Notice that interface eth0 is assigned the IP Address /mask of 192.168.10.1/24, and eth1 is assigned 168.50.80.1/30. Validate that they are correct by referring to the addressing table and/or topology.

m. Whenever you configure networking devices, it is a good habit to save the active configuration often. To save the Edge router configuration, navigate back to configuration mode. Type **`configure`** at the prompt. Next, to save the configuration, type **`save`**. Using Vyos, you must be in configuration mode to be able to save.



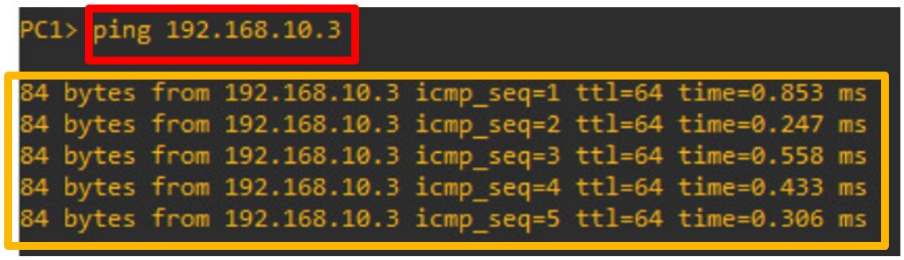
n. Notice that the configuration was saved to '/config/config.boot' (1). This backup configuration is given the name config.boot by default. If Edge has to be rebooted for any reason, this saved configuration will be reloaded into the router.

3.2 Verify Network Connectivity

In the previous steps, we configured the internal hosts PC1, PC2, PC3, and the Edge router with IP addressing parameters to match the network design topology. Next, we will verify connectivity between these devices on the inside network of 192.168.10.0/24. We will be using the ICMP ping command from PC1 to verify reachability to PC2, PC3 and the Edge router interfaces, eth0 and eth1.

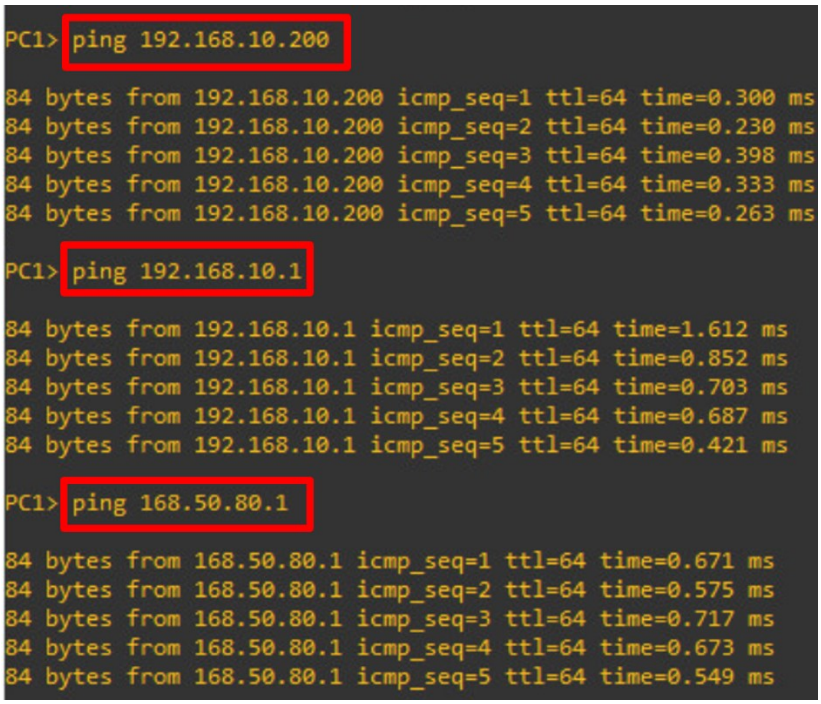
1. Click **PC1s console tab** to access its console.

2. At the PC1> prompt, ping the IP address of PC2. Type `ping 192.168.10.3`, and then press **Enter**.

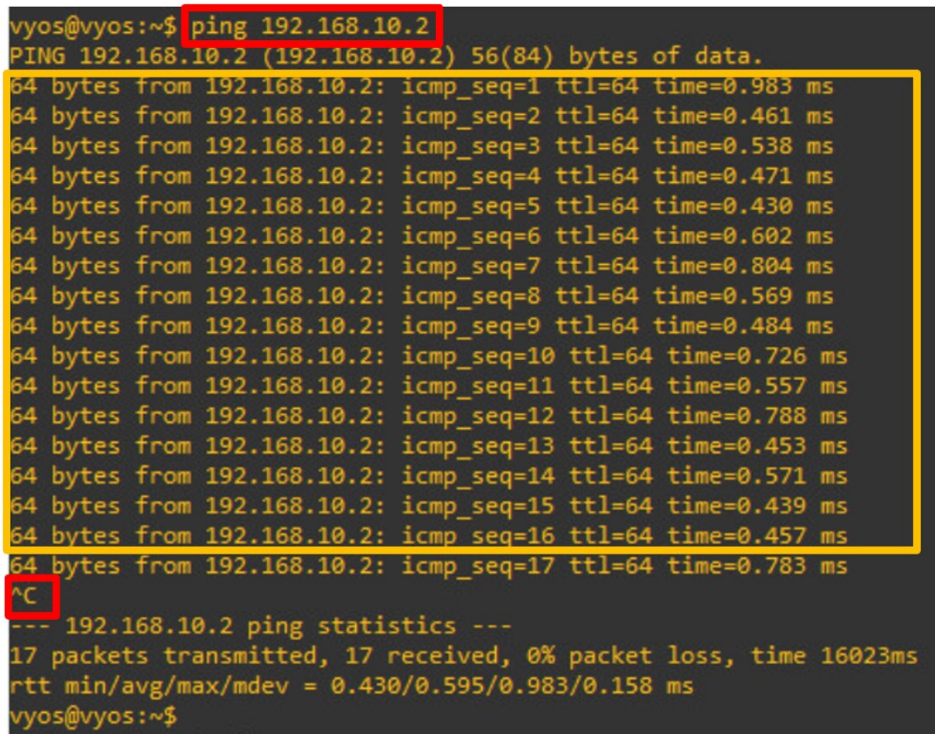


3. Notice that 5 icmp ping packets were sent to and returned from the PC2 IP address of 192.168.10.3.

4. From PC1, ping the PC3 IP address (192.168.10.200), and then the e0 interface IP address of the Edge router (192.168.10.1), and ping the eth1 interface of the Edge router (168.50.80.1). Pings should all be successful.

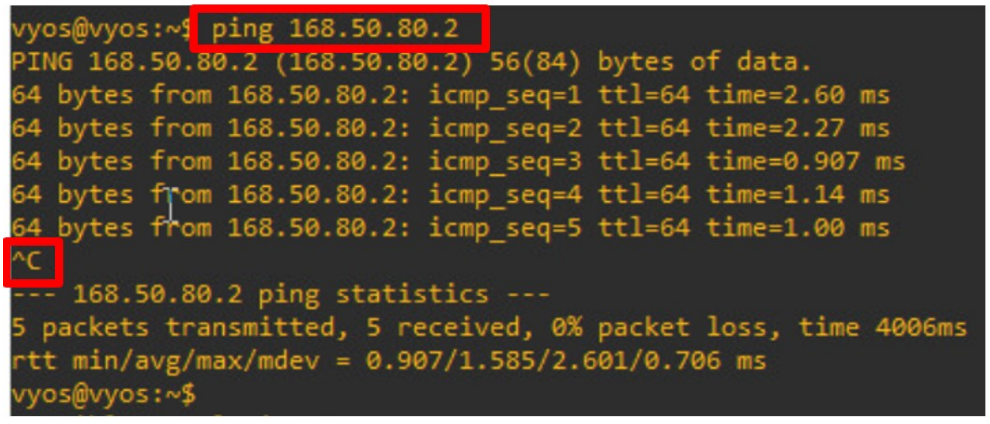


5. Now we will verify connectivity from the Edge router to PC1 and also to the Provider P1 IP address interface. Click the Edge console tab. At the vyos prompt, type `ping 192.168.10.2` to test connectivity to PC2.



6. Notice that the pings do not stop. To interrupt and stop the pings, press **CTRL + C**. In Linux, when a ping command is entered, continuous pings are sent.

7. Repeat the ping command to verify Edge can reach the Provider P1 interface. Type `ping 168.50.80.2`. Pings should be successful. Press **CTRL + C** to stop the pings.



3.3 Conclusion

Basic end device configuration, as well as configuring interfaces on a router, are some of the basic tasks that must be done prior to enabling other network services and protocols. These device configurations must also be validated to match the network design topology using show commands. Connectivity between

devices is also important. Network reachability between devices is done using ICMP. As you may recall from previous labs, ping is a basic network test that verifies layer 3 (network layer) connectivity between a source and destination device. In the next section, you will be configuring NAT.

4 Source NAT (SNAT)

SNAT, or many-to-one NAT, is the translation of many private (inside local) addresses from internal hosts into one or several public (inside global) address(es). To configure SNAT, rules need to be created. NAT is configured as a series of NAT rules. Each rule tells the NAT router to perform a network address translation that you require. These rules are numbered and are executed in numerical order. You will need to know:

- The private internal addresses we want to translate - this will be the inside network of 192.168.10.0/24
- The outgoing (outbound) interface used for the outside traffic
- The external device IP address to translate to

4.1 Configure SNAT

NAT is always configured on a border router or firewall that connects an internal network to the outside world. In our network, the Edge router is the bordering device between the inside and outside networks on which we will configure NAT. We will start with SNAT, the most popular implementation of NAT, and then verify that it works. Again, refer to the topology as we go through the steps.

1. In the Edge (vyos) device console prompt, type **`configure`** to enter configuration mode.

```
vyos@vyos:~$ configure
[edit]
vyos@vyos#
```

2. To configure SNAT, source rules are created and applied as follows:
   i. **#set nat source rule 10 description 'SNAT'** (Describe NAT purpose)
   ii. **#set nat source rule 10 outbound-interface 'eth1'** (Specify outbound interface)
   iii. **#set nat source rule 10 source address '192.168.10.0/24'** (Translate only traffic from private network 192.168.10.0/24)
   iv. **#set nat source rule 10 translation address 'masquerade'** (Use and overload IP address on outbound interface eth1 which is 168.50.80.1)

3. Enter the bolded commands on Edge. Press **Enter** after each line.

```
vyos@vyos# set nat source rule 10 description 'SNAT'
[edit]
vyos@vyos# set nat source rule 10 outbound-interface 'eth1'
[edit]
vyos@vyos# set nat source rule 10 source address '192.168.10.0/24'
[edit]
vyos@vyos# set nat source rule 10 translation address 'masquerade'
[edit]
vyos@vyos#
```

4. Type **commit** to accept the configurations you just made, and then type **save** to save the configuration.

```
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos#
```

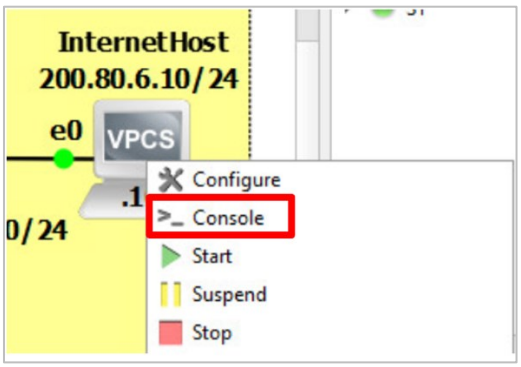
5. Type **exit** to leave configuration mode.

```
vyos@vyos# exit
exit
vyos@vyos:~$
```

4.2 Verify and Test SNAT

Now it is time to verify and test our SNAT configuration. We will first configure the InternetHost with IP parameters, and then view the current configuration running on the Edge router. Next, we will generate some traffic from the internal network, and view the SNAT translation in the NAT table in the Edge router. We will use PC1 as source host, and the destination will be the InternetHost. PC1 has a private IP address which will be translated into a public IP Address by the Edge router (inside local to inside global translation). Remember that SNAT is also known as NAT overload or many-to-one NAT. Many private (inside local) addresses can be translated into a single public (inside global) address by using the masquerade command, will use the IP address of the eth1 interface of the Edge router.

1. Configure the InternetHost (outside global) IP parameters. On the GNS3 topology, right-click **InternetHost**, and then click **Console**.



2. In the *solarwinds* list of device consoles, click the **InternetHost** tab, and then press **Enter**.

```
InternetHost>
```

3. At the InternetHost prompt, type `ip 200.80.6.10/24 200.80.6.1` to enter the IP address/Mask and Default Gateway. Press **Enter**.

```
InternetHost> ip 200.80.6.10/24 200.80.6.1
Checking for duplicate address...
InternetHost : 200.80.6.10 255.255.255.0 gateway 200.80.6.1
```

4. At the Edge router prompt, type `show configuration commands`, and then press **Enter.**

```
vyos@vyos:~$ show configuration commands
set interfaces ethernet eth0 address '192.168.10.1/24'
set interfaces ethernet eth0 description 'Inside Network'
set interfaces ethernet eth1 address '168.50.80.1/30'
set interfaces ethernet eth1 description 'Outside Network'
set nat source rule 10 description 'SNAT'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '192.168.10.0/24'
set nat source rule 10 translation address 'masquerade'
```

5. Look at the command output to locate the following. Your output may have additional commands. The output below reflects what we have configured in the Edge router. The first four lines (1) represents eth0 and eth1 interface configurations, and the last four lines (2) are the SNAT configurations.

```
vyos@vyos:~$ show configuration commands
set interfaces ethernet eth0 address '192.168.10.1/24'
set interfaces ethernet eth0 description 'Inside Network'
set interfaces ethernet eth1 address '168.50.80.1/30'
set interfaces ethernet eth1 description 'Outside Network'
set nat source rule 10 description 'SNAT'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '192.168.10.0/24'
set nat source rule 10 translation address 'masquerade'
```

1

2

6. View the NAT table in Edge. Type `show nat source translations` to view the SNAT table.

```
vyos@vyos:~$ show nat source translations
Pre-NAT               Post-NAT              Prot   Timeout
vyos@vyos:~$
```

7. Notice that there are no translations. The NAT table is empty. Why? Because we have not generated any traffic from the inside private network to be translated yet.

8. Now let's generate some traffic from the inside network to the outside network, and view SNAT translations. Navigate to the PC1s console. From the PC1> prompt, type **`ping 200.80.6.10`**.

```
PC1> ping 200.80.6.10

84 bytes from 200.80.6.10 icmp_seq=1 ttl=62 time=3.457 ms
84 bytes from 200.80.6.10 icmp_seq=2 ttl=62 time=3.040 ms
84 bytes from 200.80.6.10 icmp_seq=3 ttl=62 time=2.022 ms
84 bytes from 200.80.6.10 icmp_seq=4 ttl=62 time=1.721 ms
84 bytes from 200.80.6.10 icmp_seq=5 ttl=62 time=2.221 ms
```

9. Notice the pings are successful. PC1 was able to access the InternetHost (an outside global address) on a completely different network.

10. Navigate back to the Edge console and type **`show nat source translations`** again. View the NAT table in Edge.

```
vyos@vyos:~$ show nat source translations
Pre-NAT              Post-NAT             Prot  Timeout
192.168.10.2         168.50.80.1          icmp  19
192.168.10.2         168.50.80.1          icmp  16
192.168.10.2         168.50.80.1          icmp  18
192.168.10.2         168.50.80.1          icmp  20
192.168.10.2         168.50.80.1          icmp  17
vyos@vyos:~$
```

11. The NAT table now displays active translations. Notice the Pre-NAT (1) address is the PC1 private IP address, and the Post-NAT (2) address is the Edge eth1 public IP address, and the Protocol (Prot) (3) is icmp.

12. SNAT translations do not permanently stay in the NAT table. They age or timeout after 30 seconds. From the Edge prompt, type **`show nat source translations`** again.

```
vyos@vyos:~$ show nat source translations
Pre-NAT              Post-NAT             Prot  Timeout
vyos@vyos:~$
```

13. Notice there are no visible translations. They have aged or timed out.

4.3 Conclusion

SNAT is a widely used NAT solution in today's networks. Because many private IP addresses can be translated to a single public IP address (many-to-one NAT), NAT has been the most popular solution to the IPv4 address depletion and crisis. Until IPv6 is fully implemented, NAT with private IP addressing will continue to be deployed in IPv4 networks.

5 Destination NAT (DNAT)

Destination NAT (DNAT) is used to allow an outside host (outside global) access to a host inside a private network. DNAT is typically ussed when an external (public) host needs to initiate a session with an internal (private) host on a specific port or protocol. DNAT changes the destination address of packets. A customer needs to access a private service behind the routers public IP. A connection is established with the router's public IP address on a well-known port, and thus all traffic for this port is rewritten to address the internal (private) host. This is also known as Port Forwarding. In this step, the InternetHost will access PC3 specifically inside the private network. Like SNAT, DNAT will be configured on the border router Edge. We will first configure DNAT, and then verify it works using connectivity tests and show commands. Again, refer to the topology as we go through the steps.

5.1 Configure DNAT

In this step, The InternetHost is the outside global device whose IP address will need translation so it can reach the internal private device IP address of PC3.

1. In the Edge (vyos) device console prompt, type `configure` to enter configuration mode.

```
vyos@vyos:~$ configure
[edit]
vyos@vyos#
```

2. To configure SNAT, destination rules are created and applied as follows:

   i. **#set nat destination rule 20 description ' DNAT'** (Describe NAT purpose)
   ii. **#set nat destination rule 20 inbound-interface 'eth1'** (Specify inbound interface)
   iii. **#set nat destination rule 20 protocol 'icmp'** (Protocol that will be forwarded)
   iv. **#set nat destination rule 20 translation address '192.168.10.200'** (Internal host address that traffic will be forwarded to - this command replaces the destination address of an inbound packet with 192.168.10.200)

3. Enter the bolded commands above on Edge. Press **Enter** after each line.

```
vyos@vyos# set nat destination rule 20 description 'DNAT Port Forward'
[edit]
vyos@vyos# set nat destination rule 20 inbound-interface 'eth1'
[edit]
vyos@vyos# set nat destination rule 20 protocol 'icmp'
[edit]
vyos@vyos# set nat destination rule 20 translation address '192.168.10.200'
[edit]
vyos@vyos#
```

4. Type **commit** to accept the configurations you just made, and then type **save** to save the configuration.

```
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos#
```

5. Type **exit** to leave configuration mode.

```
vyos@vyos# exit
exit
vyos@vyos:~$
```

5.2 Verify and Test DNAT

Now we will verify and test our DNAT configuration. This time, traffic will be generated from the outside to a specific internal private host. We will use the InternetHost, the source host, and the destination will be PC3. The InternetHost is assigned a public IP address which will be translated into a PC3 private IP Address by the Edge router (outside global to inside local translation). Remember that DNAT is also known as 1-to-1 NAT or port forward. It is used to translate a single public (outside global) address to a single private (inside local) address. Traffic will now be coming into Edge eth1 interface. With DNAT, is important to note that the DNAT translation occurs *before* traffic traverses the router. In this example, the destination address has already been translated to 192.168.10.200, so the Pre-NAT and Post-NAT addresses in the table will be the same.

1. At the Edge router prompt, type **show configuration commands**, and then press **Enter.**

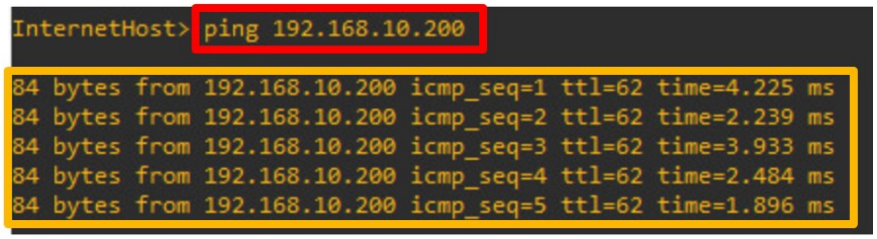
```
vyos@vyos:~$ show configuration commands
set interfaces ethernet eth0 address '192.168.10.1/24'
set interfaces ethernet eth0 description 'Inside Network'
set interfaces ethernet eth0 duplex 'auto'
set interfaces ethernet eth0 hw-id '0c:e3:91:0a:00:00'
set interfaces ethernet eth0 smp-affinity 'auto'
set interfaces ethernet eth0 speed 'auto'
set interfaces ethernet eth1 address '168.50.80.1/30'
set interfaces ethernet eth1 description 'Outside Network'
set interfaces ethernet eth1 duplex 'auto'
set interfaces ethernet eth1 hw-id '0c:e3:91:0a:00:01'
set interfaces ethernet eth1 smp-affinity 'auto'
set interfaces ethernet eth1 speed 'auto'
set interfaces ethernet eth2 hw-id '0c:e3:91:0a:00:02'
set nat destination rule 20 description 'DNAT'
set nat destination rule 20 inbound-interface 'eth1'
set nat destination rule 20 protocol 'icmp'
set nat destination rule 20 translation address '192.168.10.200'
set nat source rule 10 description 'SNAT'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '192.168.10.0/24'
set nat source rule 10 translation address 'masquerade'
```

1

2

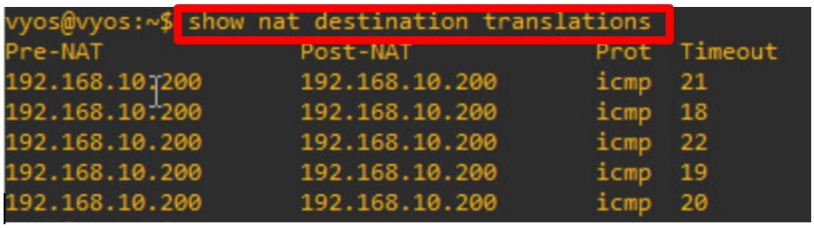
The output displays the NAT configuration. Notice both the DNAT (1) and SNAT (2) configurations.

2. Now let's generate some traffic from the InternetHost (outside) to PC3 (inside). Navigate to the InternetHost console. From the InternetHost> prompt, type **`ping 192.168.10.200`**.



3. There are five icmp echo replies displayed, indicating successful pings from 192.168.10.200. The InternetHost was able to access the private internal host PC3.

4. Navigate back to the Edge console, and type **`show nat destination translations`**. View the NAT table in Edge.



5. Notice that the Pre-NAT and Post-NAT addresses in the table are the same.

5.3 Conclusion

DNAT is used to redirect traffic to an internal private network or host from outside public devices. The outside interface on the router or firewall will be the inbound interface for traffic. DNAT rules can specify protocols and ports to forward, and the IP address of the internal private device to forward traffic to.

6 1-to-1 NAT

1-to-1 NAT is a combination of configuring both DNAT and SNAT. 1-to-1 NAT is used to translate all ip traffic between an external IP address to an internal IP address. 1-to-1 NAT will translate in both directions by creating rules, like before. One rule for DNAT to translate an outside host IP address, and then a corresponding SNAT rule to translate outgoing traffic from an internal host IP address to a reserved external IP. This 1-to-1 mapping is used for NAT protocols and not specific ports. DNAT is used for port forwarding.

6.1 Configure 1-to-1 NAT

In this step, we will configure both SNAT and DNAT on the vyos (Edge) router, creating 2-way mapping between PC3 and the InternetHost.

1. In the Edge (vyos) device console prompt, type `configure` to enter configuration mode.

```
vyos@vyos:~$ configure
[edit]
vyos@vyos#
```

2. First, we will configure DNAT. Destination rules are created and applied as follows:

   i. **#set nat destination rule 30 description ' 1-to-1 NAT'** (Describe NAT purpose)
   ii. **#set nat destination rule 30 destination address '168.50.80.1'** (Outside eth0 IP address)
   iii. **#set nat destination rule 30 inbound-interface 'eth1'** (Specify inbound interface)
   iv. **#set nat destination rule 30 translation address '192.168.10.200'** (Internal host address that traffic will be forwarded to - this command replaces the destination address of an inbound packet with 192.168.10.200)

3. Enter the bolded commands above on Edge. Press **Enter** after each line.

```
vyos@vyos# set nat destination rule 30 description '1-to-1 NAT'
[edit]
vyos@vyos# set nat destination rule 30 destination address '168.50.80.1'
[edit]
vyos@vyos# set nat destination rule 30 inbound-interface 'eth1'
[edit]
vyos@vyos# set nat destination rule 30 translation address '192.168.10.200'
[edit]
vyos@vyos#
[edit]
```

4. Next, we will configure SNAT. Source rules are created and applied as follows:

    i. **#set nat source rule 30 description '1-to-1 NAT'** (Describe NAT purpose)
    ii. **#set nat source rule 30 outbound-interface 'eth1'** (Specify outbound interface)
    iii. **#set nat source rule 30 source address '192.168.10.200'** (Translate only traffic from host 192.168.10.200)
    iv. **#set nat source rule 30 translation address '168.50.80.1'** (Use the IP address on outbound interface eth1 which is 168.50.80.1)

```
vyos@vyos# set nat source rule 30 description '1-to-1 NAT'
[edit]
vyos@vyos# set nat source rule 30 outbound-interface 'eth1'
[edit]
vyos@vyos# set nat source rule 30 source address '192.168.10.200'
[edit]
vyos@vyos# set nat source rule 30 translation address '168.50.80.1'
[edit]
vyos@vyos#
[edit]
```

5. Type **`commit`** to accept the configurations you just made, and then type **`save`** to save the configuration.

```
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos#
```

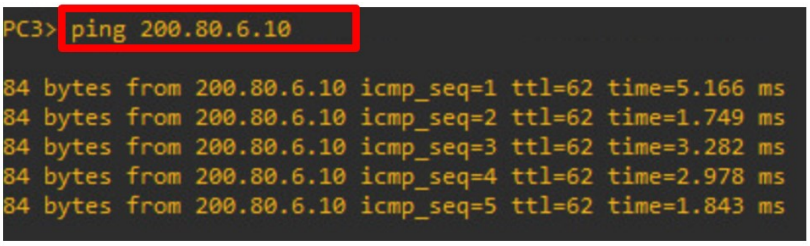
6. Type **`exit`** to leave configuration mode.

```
vyos@vyos# exit
exit
vyos@vyos:~$
```

6.2 Verify and Test 1-to-1 NAT

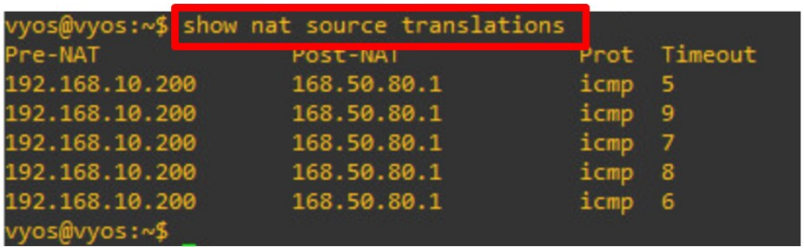
Now we will verify and test our 1-to-1 NAT configuration. Remember 1-to-1 NAT is bi-directional, so we need to look at both SNAT and DNAT translations. To verify SNAT, we will use the PC3, the source host, and the destination will be the InternetHost. To verify DNAT, we will use the InternetHost as the source host, and the destination will be PC3.

1. To test SNAT, generate some traffic from PC3 to the InternetHost. Navigate to the PC3 console. From the PC3> prompt, type `ping 200.80.6.10`.



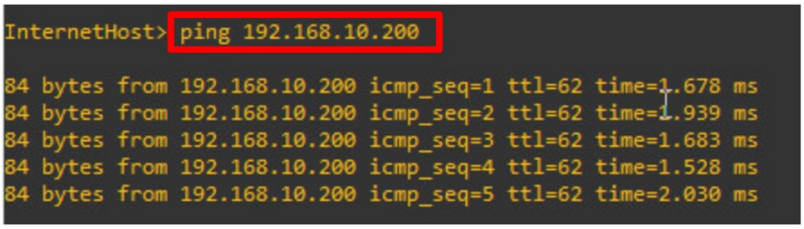
2. There are five icmp echo replies displayed, indicating successful pings from 200.80.6.10.

3. Navigate back to the Edge console, and type **`show nat source translations`**. View the NAT table in Edge.



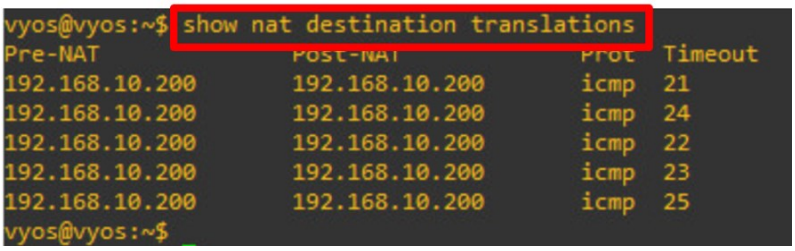
4. Notice that the Pre-NAT and Post-NAT addresses in the table display the SNAT translation.

5. To test DNAT, generate some traffic from the InternetHost to PC3. Navigate to the InternetHost console. From the InternetHost> prompt, type `ping 192.168.10.200`.



6. There are five icmp echo replies displayed, indicating successful pings from 192.168.10.200.

7. Navigate back to the Edge console, and type **`show nat destination translations`**. View the NAT table in Edge.



8. Close the main console window and the GNS3 application.

6.3 Conclusion

NAT is still very important in IPv4 networks today. In this lab, we explored the three types of NAT using the Linux Vyos router. SNAT is used to translate many private addresses from inside a network/subnet to a single public IP address to reach hosts outside. DNAT is used to redirect traffic using specific ports and protocols to an internal private network or host from outside public devices. 1-to-1 NAT is similar to DNAT, but is used to translate for all IP protocols and not specific ports. 1-to-1 NAT is a combination of both SNAT and DNAT for bi-directional traffic translations.

References

1. The Internet Engineering Task Force (IETF) https://www.ietf.org/rfc/rfc1918.txt
2. The Internet Assigned Numbers Authority (IANA) https://www.iana.org/numbers
3. Vyos Configuration Guide https://docs.vyos.io/en/equuleus/configuration/index.html

