SUNY Polytechnic Institute

NCS 450

Network Security

Lab 3: NAT

Author:
Jess Yanarella
Tony Perez

Professor:
Ronny Bull

February 26th 2015

1 Introduction

In this lab, we configured our Cisco router to allow for NAT functionality. Once NAT is set up, we can configure the switch to allow devices connected to it to have Internet access. If everything goes well in the lab, the pod PC should be able to connect to the Internet from the created internal LAN. NAT or Network Address Translation will allow our switch, on the 172.16.2.0/24 network, to be able to talk to anyone outside of the campus network.

2 Diagram:

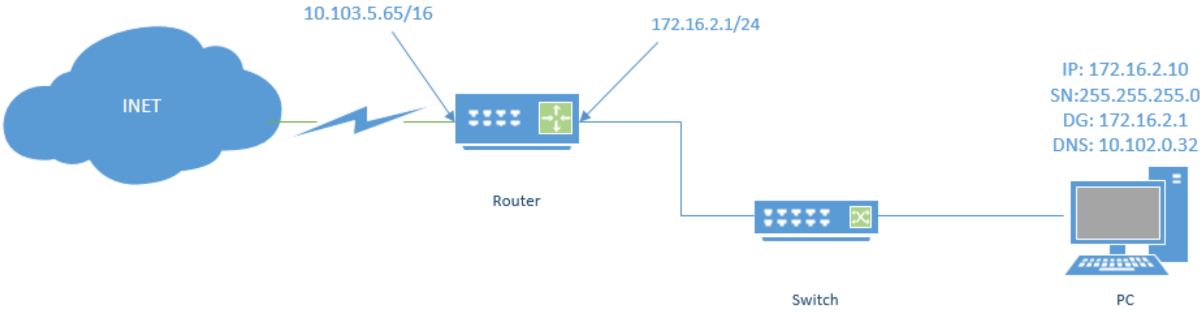


Figure 1: NAT Setup

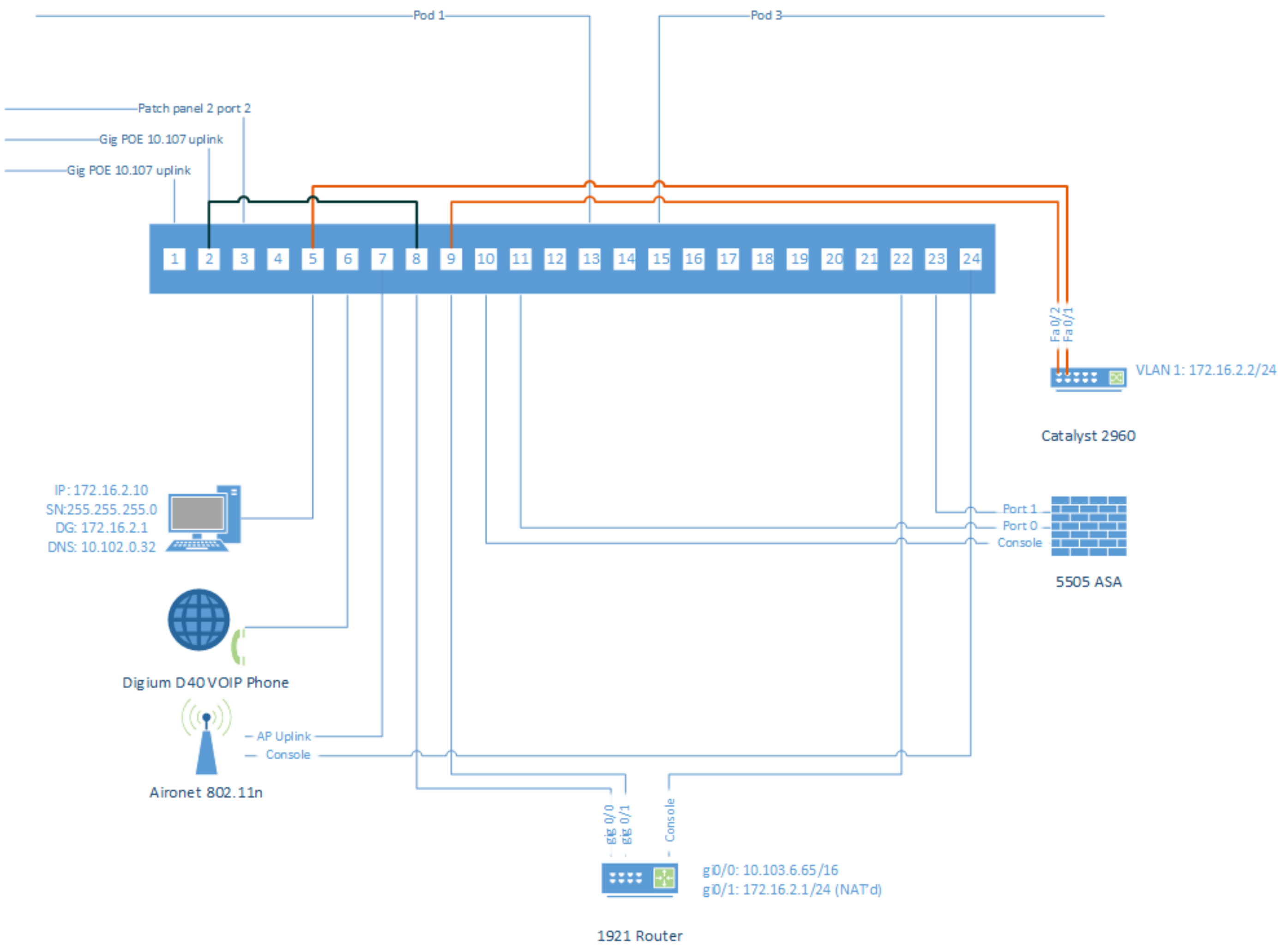


Figure 2: Updated Network Setup

3 Declare inside & outside NAT interfaces on the router:

On the router, we need to assign our network interfaces as inside or outside to configure NAT. Our outside interface is gi0/0 and our inside interface is gi0/1. To do this, go into config terminal mode then interface of the one you want. We started with configuring the outside first.

```
(config-if)# ip nat outside
(config-if)# ip nat inside
```

4 Define what IP addresses will be NAT'd:

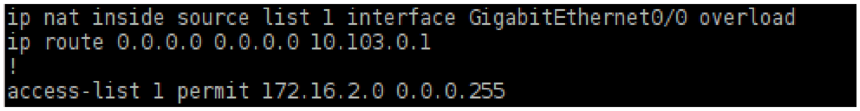
The router now needs to be configured so it knows what IP addresses should be NAT'd. This can be done by creating an access-list using a simple command.

```
(config)# access-list 1 permit 172.16.2.0 0.0.0.255
```

5 Enable NAT:

Next, we must enable NAT on the router. This can be done right after the access-list is added since we still are configuration mode.

```
(config)# ip nat inside source list 1 interface g0/0 overload
```



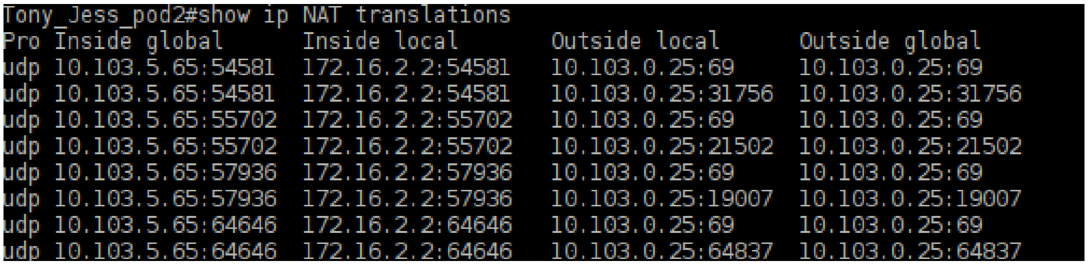
```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 10.103.0.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

Figure 3: NAT Config

6 Test NAT:

After all the previous steps, our router is now configured to perform NAT. Now we can test to see if it is working by doing a simple ping and showing the NAT translation table on the router. The ping it has us do is successful, but before we even configured NAT, we were able to reach the 10.103.0.25 network.

```
# ping 10.103.0.25
# show ip NAT translations
```



```
Tony_Jess_pod2#show ip NAT translations
Pro Inside global      Inside local       Outside local      Outside global
udp 10.103.5.65:54581  172.16.2.2:54581   10.103.0.25:69     10.103.0.25:69
udp 10.103.5.65:54581  172.16.2.2:54581   10.103.0.25:31756  10.103.0.25:31756
udp 10.103.5.65:55702  172.16.2.2:55702   10.103.0.25:69     10.103.0.25:69
udp 10.103.5.65:55702  172.16.2.2:55702   10.103.0.25:21502  10.103.0.25:21502
udp 10.103.5.65:57936  172.16.2.2:57936   10.103.0.25:69     10.103.0.25:69
udp 10.103.5.65:57936  172.16.2.2:57936   10.103.0.25:19007  10.103.0.25:19007
udp 10.103.5.65:64646  172.16.2.2:64646   10.103.0.25:69     10.103.0.25:69
udp 10.103.5.65:64646  172.16.2.2:64646   10.103.0.25:64837  10.103.0.25:64837
```

Figure 4: NAT Translations

7 Configure IP on your pod PC:

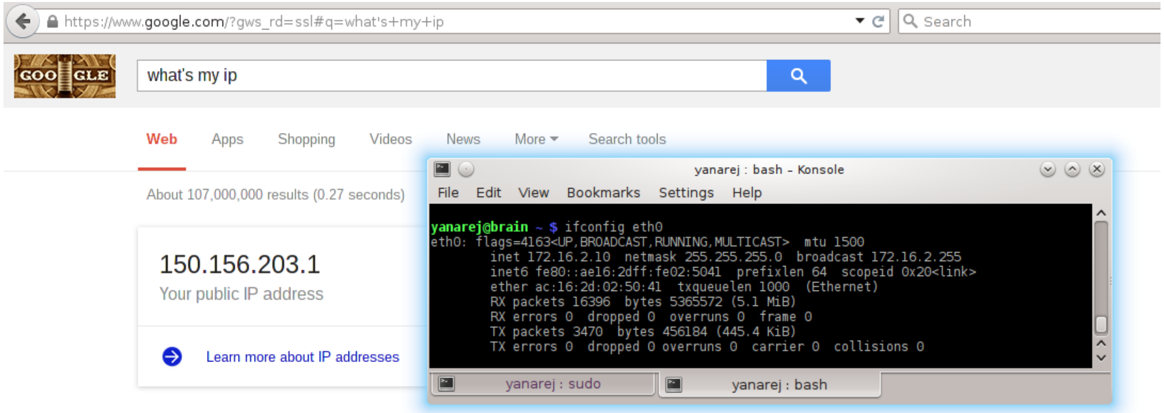
Since the NAT test was successful, we can now move onto the configuration on the pod PC. Since we just made changes to the router, the PC host must be changed so it can communicate with the Internet. First, we need to change the IP address in terminal.

```
# sudo ifconfig eth0 inet 172.16.2.10 255.255.255.0
```

Once that is changed, we must now add the default gateway. The address for this is the default gateway of our computer on the LAN side of the router.

```
# sudo route add default gw 172.16.2.1
```

The changes were successful and we can get an IP address along with connection to the Internet.



https://www.google.com/?gws_rd=ssl#q=what's+my+ip

what's my ip

About 107,000,000 results (0.27 seconds)

150.156.203.1
Your public IP address

Learn more about IP addresses

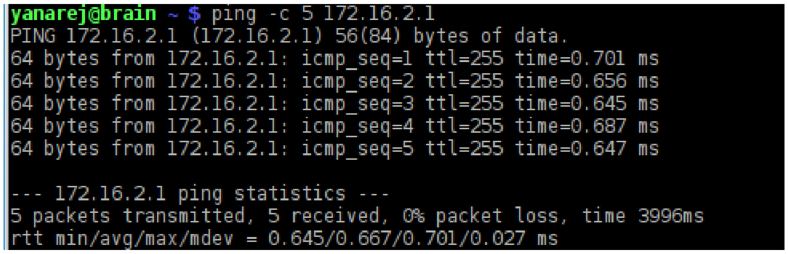
yanarej : bash - Konsole

```
yanarej@brain ~ $ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.2.10  netmask 255.255.255.0  broadcast 172.16.2.255
        inet6 fe80::ae16:2dff:fe02:5041  prefixlen 64  scopeid 0x20<link>
        ether ac:16:2d:02:50:41  txqueuelen 1000  (Ethernet)
        RX packets 16396  bytes 5365572 (5.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3470  bytes 456184 (445.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5: PC Test

8 Testing new LAN:

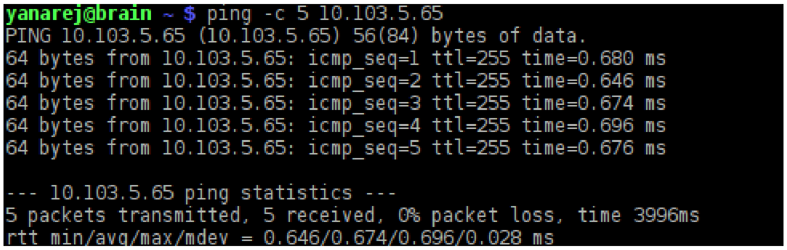
The PC is now connected to our new LAN and to verify this, we can perform different pings.



```
yanarej@brain ~ $ ping -c 5 172.16.2.1
PING 172.16.2.1 (172.16.2.1) 56(84) bytes of data.
64 bytes from 172.16.2.1: icmp_seq=1 ttl=255 time=0.701 ms
64 bytes from 172.16.2.1: icmp_seq=2 ttl=255 time=0.656 ms
64 bytes from 172.16.2.1: icmp_seq=3 ttl=255 time=0.645 ms
64 bytes from 172.16.2.1: icmp_seq=4 ttl=255 time=0.687 ms
64 bytes from 172.16.2.1: icmp_seq=5 ttl=255 time=0.647 ms

--- 172.16.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.645/0.667/0.701/0.027 ms
```

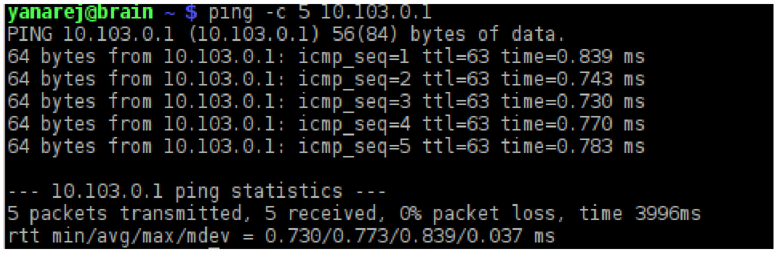
Figure 6: Ping IP address of our pod LAN's router Interface



```
yanarej@brain ~ $ ping -c 5 10.103.5.65
PING 10.103.5.65 (10.103.5.65) 56(84) bytes of data.
64 bytes from 10.103.5.65: icmp_seq=1 ttl=255 time=0.680 ms
64 bytes from 10.103.5.65: icmp_seq=2 ttl=255 time=0.646 ms
64 bytes from 10.103.5.65: icmp_seq=3 ttl=255 time=0.674 ms
64 bytes from 10.103.5.65: icmp_seq=4 ttl=255 time=0.696 ms
64 bytes from 10.103.5.65: icmp_seq=5 ttl=255 time=0.676 ms

--- 10.103.5.65 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.646/0.674/0.696/0.028 ms
```

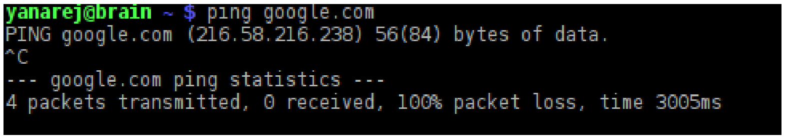
Figure 7: Ping external IP address for our LAN router



```
yanarej@brain ~ $ ping -c 5 10.103.0.1
PING 10.103.0.1 (10.103.0.1) 56(84) bytes of data.
64 bytes from 10.103.0.1: icmp_seq=1 ttl=63 time=0.839 ms
64 bytes from 10.103.0.1: icmp_seq=2 ttl=63 time=0.743 ms
64 bytes from 10.103.0.1: icmp_seq=3 ttl=63 time=0.730 ms
64 bytes from 10.103.0.1: icmp_seq=4 ttl=63 time=0.770 ms
64 bytes from 10.103.0.1: icmp_seq=5 ttl=63 time=0.783 ms

--- 10.103.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.730/0.773/0.839/0.037 ms
```

Figure 8: Ping next router beyond our LAN



```
yanarej@brain ~ $ ping google.com
PING google.com (216.58.216.238) 56(84) bytes of data.
^C
--- google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3005ms
```

Figure 9: Ping external host

9 Lab Questions:

1. Theorize what would happen if a host outside your network pinged one of your internal hosts. Will that ping be successful? Why or why not?

It would not be successful because our host is on the 172.16.2.0/16 network and so unless the router had the route to our network it would not know what to di with it. Packets would be sent but nothing will be received since no one is getting it.

2. In section III, step c, you were asked to ping fang.cs.sunyit.edu from the switch. Was it successful? Can you ping it now? Please explain what is happening.

It was successful because the router knew the 172.16.2.0/16 network and so the switch could send and receive the ping.

3. Does NAT make troubleshooting harder or easier? Justify your answer.

NAT would make troubleshooting harder because if a number of subnets are NAT'd then they would appear as a single IP and we would have to resort to using ports. Although we would not know exactly where an IP that has been NAT'd exactly is at least we would still be able to track it down but it would take more time.

4. What type of impacts does NAT have on security and complexity of a network?

NAT could hide the true identity of a host and so it could be used for privacy, unless the packet is inspected, but it bring more complexity to a network. Now one public IP address could be matched to many IP addresses internally. The router must add and remove headers which cause more overhead.