A NAT is a system that connects a private address space to the Internet on a one-way basis. Use of NATs is inspired by shortage of IPv4 addresses.

![Diagram of a normal routed subnet](image1)

Referring to figure 1: in the Internet architecture, every interface has an Internet address in addition to its physical address. Under normal circumstances, all addresses on a LAN have the same subnet number. Thus B and C might be part of the GMU NETLAB subnet, in which case their addresses might be B = 129.174.65.1 and C = 129.174.65.2 on the 129.174.65/24 subnet, part of the GMU 129.174/16 address space. NETLAB is configured as a /24 subnet, so the last octet of C might be anything from 2 to 254 (1 being already taken by B and 255 being reserved for broadcast). Packets can be routed to/from C from/to anywhere in the Internet.

![Diagram of a NAT subnet](image2)

But suppose instead C is part of a subnet that can't get new IPv4 addresses (perhaps a home network). See figure 2. We could use B = 192.168.0.1 and C = 192.168.0.2. These addresses have been set aside as private, that is they will never be assigned to any Internet subnet. Thus they can be used over and over again, provided the NAT does something that is not quite legitimate under the Internet architecture: it substitutes its own address B for C in the source ('from') address of the outgoing packets, and substitutes C's address in the destination ('to') address of the response packets. It is even possible for D also to share address A if the NAT can determine whether reply packets are intended for C or D. If, like most Internet traffic, the packets are carrying a TCP payload, there will be a TCP port number that can be used to identify which connection (and therefore which host) is involved. In this case, the NAT also will
swap sending port number if C and D happen to be using the same number.

Given this understanding of NAT, in this project part you will work to connect a computer with a private address and a NAT to the Internet. *This lab must be done in the computer lab at the Prince William campus.*

**Lab Steps:**

**PART I: linux NAT**

1. Confirm that the lab computers are set up using a hub LAN as shown in Figure 2. First work with a linux system that has been set up as a NAT (C and D can be either Windows or linux). Check that B = 192.168.0.1 and C = 192.168.0.2. On a Windows system, use command `ipconfig` on a command-line window to do this. On linux use `ifconfig eth0` and `ifconfig eth1` to check the two interfaces (the IP address will be on the top line of the resulting output). Report on the IP addresses you find.

2. Use any computer (address X) in the lab except the NAT, C or D, to confirm that ping gives no response from outside the NAT subnet. Write an explanation why this is so.

3. Run a ping to address X from C. Unlike ping to C from X, this should work. Explain why it works when the other does not.

4. Run a Web browser on C and confirm that you can access [http://www.gmu.edu](http://www.gmu.edu). What protocols are used over IP by the browser?

**PART II: WINDOWS NAT**

1. Change the NAT computer over to Windows. With A and B set to addresses from a 129.174 subnet, confirm that C (still 192.168.0.2) cannot ping X. Now set up a NAT on the Windows system as follows:
   - Open the Control Panel through the Start prompt.
   - Click on Network Connections
   - Right click on the Local Area Connection for B (Local Area Connection 1)
   - Click Properties->Internet Protocol(TCP/IP)->Advanced. Then check the top box under Internet Connection Sharing and click OK. (Note: this box will not appear if you select Local Area Connection 2).

2. Repeat steps 2, 3 and 4 and report on your results.

3. Remove the NAT by returning to the Advanced tab, unchecking the box, and clicking OK.

**To Learn More**

More information about NAT can be found at the following locations: