Lab 08 – Network Address Translation

# What you will do:

* Learn about the network layer
* Learn about how NAT works
* Use Wireshark to receive IP Packets
* Use a router to forward packets between two networks

# Things that you will need to know or learn:

* How to configure IP addresses and subnet masks, both statically and dynamically, using the GUI, under Windows 7/8(see References below)
* How to use Wireshark to see actual network traffic
* How to reset a Linksys E2500 router.
* How to configure a Linksys router running Tomato firmware for routing and NAT operations

# What you need to submit and when:

* Complete the Pre-lab quiz on Blackboard before 8am on the day of your lab
* Complete the in-lab part of the exercise (see below) before the end of your lab period.
* Complete the Post-lab exercise on Blackboard before 8am on the day of your next lab

# Required Equipment:

* Network cables, available in lab
* A Linksys E2500 router running Tomato firmware (supplied in lab)
* Two PCs, one with VMware 10 Workstation installed

# Marks:

* Each of the three lab parts identified above are weighted equally, even though they may have a different number of points assigned to them.
* 20% of your final mark is for labs done during the course of the semester.

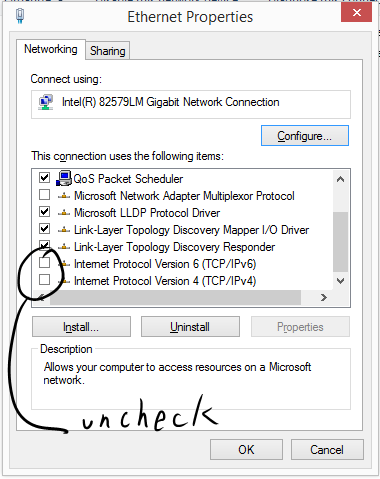
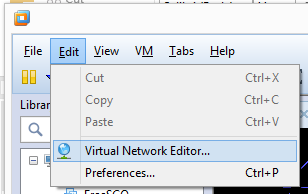
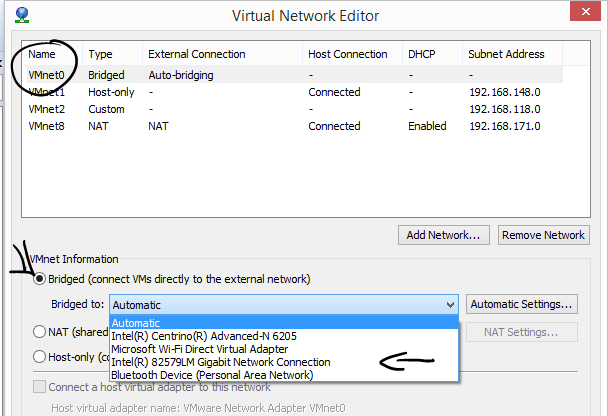
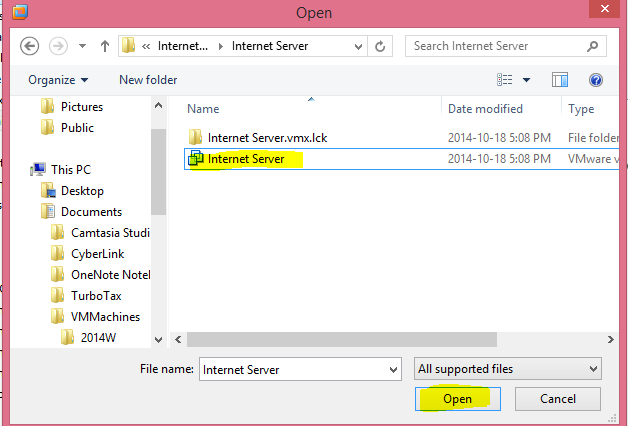
# References and Resources:

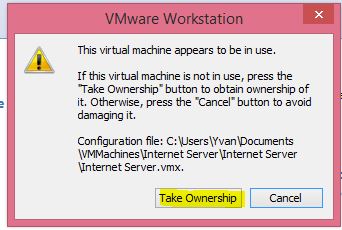
* Packet Tracer (for help on correct cabling; view of packets similar to Wireshark)
* How IP in Windows 7 (on Blackboard, Labs -> Lab 03)
* How to Wireshark (on Blackboard, Labs -> Lab 03)
* How to Cable (on Blackboard, Labs -> Lab 03)

# Task 0 – **Overview and setup instructions**

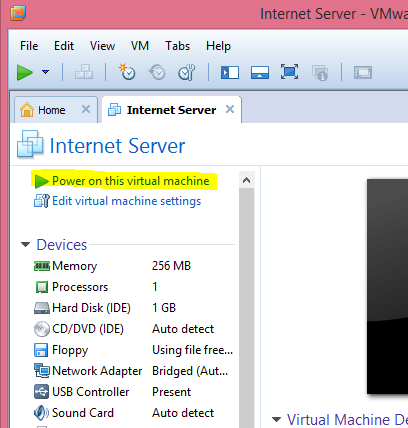
1. You will work is groups of 2 for this lab.
2. In this lab PC1 will be the simulate a server on the Internet and PC2 will be a client on the internal LAN
3. The lab will be divided into two parts. In the first part you will setup the router much like you do at home using NAT. PC2 will then access a few services on PC1. In the second part you will configure the router as a router and turn off NAT. You will access the same services and see what the differences are between the two modes of operation.
4. There are separate steps below for PC1 and PC2, you can do them at the same time but it would be wise to observe the steps take on each PC.

**PC1 – (needs VMWare)**

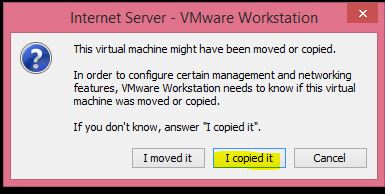
1. Download the VMWare “Internet Server” image from Blackboard
2. Extract the file to a known location, normally VMs are stored in Documents\Virtual Machines.
3. You now need to configure your real Ethernet adapter to limit traffic. We are going to setup the adapter so only the virtual machine can use the IP protocol stack on it.
4. Use ncpa.cpl and locate your Ethernet adapter. “Right Click” the adapter and select “Properties”. Locate “Internet Protocol Version 6 (TCP/IPv6)” and “Internet Protocol Version 4 (TCP/IPv4)” and uncheck the boxes next each. Be sure to carefully document what you disabled so you may restore your settings back to their original configuration when the lab is over.
5. Now setup VMware to bridge VMNet0 to your Ethernet adapter. Start VMware, on the VMware menu select “Edit” -> “Virtual Network Editor”
6. Now highlight “VMnet0”. Under “VMnet Information” select “Bridged”. Using the “Bridged to:“ drop down list, select your Ethernet Adapter. Click “Apply” and then “OK”. The VMnet0 NIC is now bridged to your real Ethernet adapter and it will see all traffic your real NIC sees.
7. From the VMWare Workstation File/Open menu option you will browse to the location where you unzipped the VM in step 2. Specifically you want to open the file named Internet Server as shown below.
8. Soon after clicking the Open button as shown above, you will be prompted with yet another question as shown below. Press the Take Ownership button.



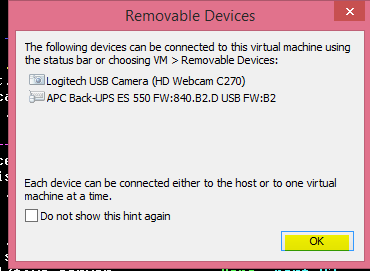
1. You are now ready to start the VM machine. To do so, press the “Power on this virtual machine” button as shown below.



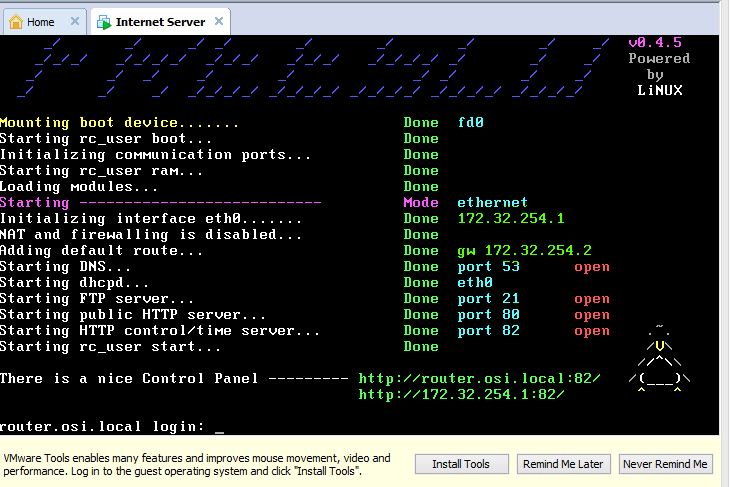
1. The final prompt to appear before the machine starts will be the following. Simply click “I copied it”.

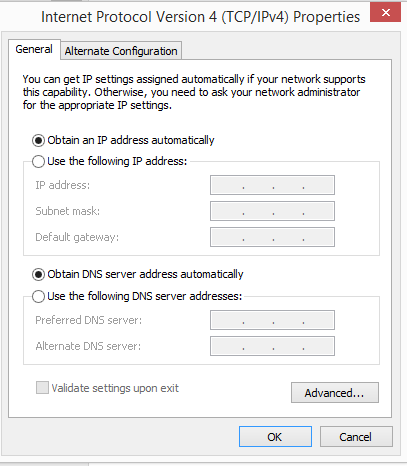


1. The Internet Server should now be in the process of booting. Note that you may receive a Removable Devices message (please see below) which can be ignored.



1. The boot up process should not take more than 2 to 3 minutes. The Internet Server is booted up and ready to go when the screen below appears in the Internet Server’s VM window. The machine is completely configured and ready to use. Note that you may ignore the VMWare Tools message. Remember that you will need to click Ctrl+Alt to return mouse control from your VM to your computer. You are now ready to move to the next setup task.



**PC2 – (Configures the router and acts as a client)**

1. Perform a 30/30/30 reset on the router.
2. Configure your PC2’s Ethernet card to “Obtain an IP address automatically” and “Obtain DNS server address automatically”.
3. You should now connect your PCs to the router. PC1 connects to the “Internet” port and PC2 connects to one of the Ethernet ports
4. Check the IP addresses on PC2 (via ipconfig) it should be 192.168.1.x – x could be any number between 2 and 51

DO NOT PROCEED UNLESS YOU HAVE AN ADDRESS.

1. Confirm you have connectivity.
   1. On PC2 type in:
      1. ping 172.32.254.1

Do not proceed until your Ping requests and replies are successful!!

1. From PC2, logon to the router <http://192.168.1.1> (admin/admin). On the “Overview” page locate and record the following:
   1. WAN IP
   2. Subnet mask
   3. gateway address
   4. MAC address.
2. Under Advanced -> Firewall check “respond to ICMP ping”
3. Record PC2’s (ipconfig)
   1. IP address,
   2. subnet mask,
   3. gateway address and
   4. MAC address.

Task 1 – Observe NATed traffic.

1. You are now going to complete three different captures. You generate the traffic from PC2 but capture it on both computers. In each case start the captures on both machines at the same time, generate the traffic from PC2, stop and save the captures.
2. ICMP traffic
   1. Start captures, from PC2 ping 172.32.254.1, allow the ping to stop, stop and save the captures as Task1\_1(PC*x*).pcapng. *x= 1 or 2 to indicate which PC captured the traffic*
3. HTTP traffic
   1. Start captures, on PC2 open the web page <http://172.32.254.1>, when the page displays, stop and save the captures as Task1\_2(PC*x*).pcapng. *x= 1 or 2 to indicate which pc captured the traffic*
4. DNS traffic
   1. Start captures, on PC2 ping [www.osi.loca](http://www.osi.loca)l, when the ping completes stop and save the captures as Task1\_3 PC*x*).pcapng. *x= 1 or 2 to indicate which pc captured the traffic*

**Checkpoint 1 – open all three captures on both PCs, filter the captures as follows: Capture 1 by ICMP, Capture 2 by TCP and Capture 3 by DNS. Show the captures to your instructor. You will need to point out the HTTP traffic that was sent from PC2 (capture) and how it was received at PC1 (PC1 capture). Make note of what is different**

Task 2 – Routing no NAT

1. You are now going to change the router from NATing to routing and repeat the steps above. On PC2 logon to the router. Click on the “Advanced” menu item and select “Routing”. Under Miscellaneous change the “Mode” from “Gateway” to “Router”. Uncheck “DHCP Routes”
2. Save the configuration.
3. On PC2 open an Administrator command prompt and enter “ipconfig /flushdns”. This will clear your DNS cache
4. Repeat the steps from 2, 3 and 4 from Task 1. Changed the saved file names to “Task2 …… .pcap”

Checkpoint 2 – open all three captures on both PCs, filter the captures as follows: Capture 1 by ICMP, Capture 2 by TCP and Capture 3 by DNS. Show the captures to your instructor

Task 3 – Cleanup

1. Stop the VM “Internet Server”
2. Restore your Ethernet adapter’s IPv4 and IPv6’s settings to their pre task 0 step 4 value. Note that you may also need to re-enable some Microsoft features such as Client for Microsoft Network and File and Printer Sharing for Microsoft Networks. Note that you only want to re-enable the properties that were disabled by task 0 step 4.
3. Return router and cables to their correct locations
4. Share your captures with you partner, you will need both sets of Wireshark captures to answer the post-lab questions.
5. Don’t forget to do the post lab
6. Re-enable wireless and firewall