EET475L Lab #5

DNS Administration Lab

Goals: In this lab your group will produce a full working Windows network complete with DHCP, DNS, and routing services to the outside world ("Internet"). Each group will be in a separate collision domain (separate benches, or separate hubs/switches). You will be configuring the NAT firewall in this experiment.

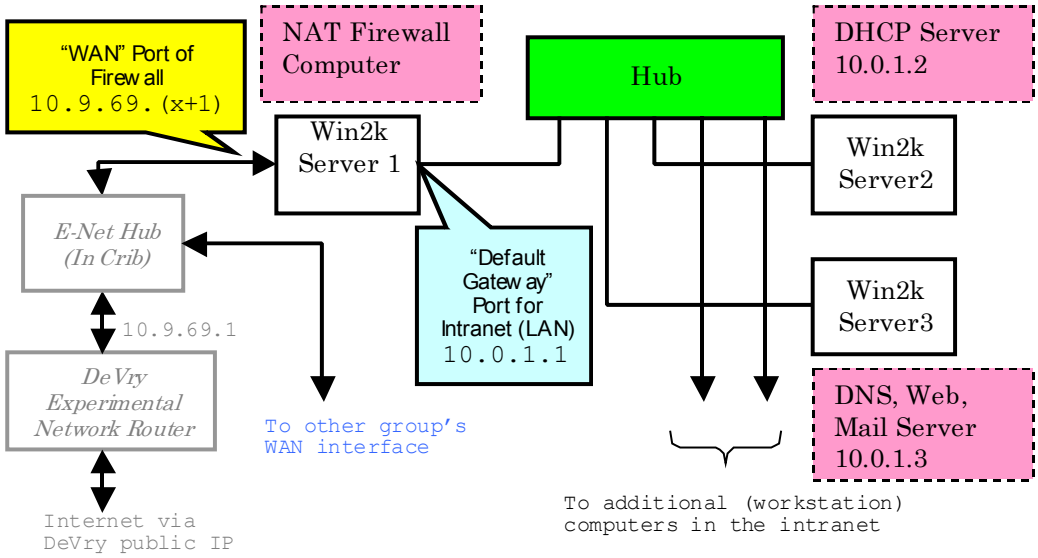
Follow all instructions carefully. Don't change any settings or procedures unnecessarily. If you feel the desire to be creative with your configuration, *first* get it working, *then* make the creative additions (one at a time.) You can lose much time (and hair!) over one "creative" setting choice made by a team member!

Please read this entire document before starting the experiment.

Resources Required: Windows 2000 Server; Windows 2000 Server configured as a router (requires two NIC cards); access to experimental network (for outside route); any other Windows computer running 95/NT4/98/2000/XP.

1. Study the network configuration below. You'll need to understand it before configuring any machines!

   It is strongly suggested that you name your network interfaces "WAN" and "INTRANET" (do this under Network and Dial-up Connections) before proceeding.



In the picture above, E-Net Hub is in the electronics laboratory stockroom. The jumpers at the end of your lab bench connect to this hub. *You have to request that the crib connect the bench to the experimental network*. Once this has been done, the bench connection that would normally go to the DeVry University intranet now connects to the experimental network.

The *experimental network* (E-Net) passes through an additional firewall and NAT before touching DeVry's Internet gateway. It has the following characteristics:

Network address: 10.9.69.0 /24
Available IP block: 10.9.69.2 - 10.9.69.254 (Each group must use a different IP)
Gateway: 10.9.69.1 (This is one port of a Cisco router administered by the DeVry IT department).

2. Configure the Windows 2000 NAT firewall, being careful to correctly administer its IP address on the "experimental" side of the network. This box will perform two functions:

   a) It will NAT Internet-destined packets from your groups "INTRANET" into an address acceptable to the "EXPERIMENTAL" network. Use your WAN address as the transformed IP address for NAT.

   b) It will route packets destined for the other groups' "INTRANET" networks to the appropriate group's WAN IP address.

   You should be able to ping the gateway (10.9.69.1) as well as the other group's router ports (10.9.69.2, 10.9.69.3, 10.9.69.4, etc.) It would be wise to check that this works at this point! Also, you should be able to ping external IP addresses from the router. If there's any problem here, fix it before proceeding!

3. Configure the DNS service on your Windows 2000 server. Use the FQDN (Fully-Qualified Domain Name) of your organization for the forward lookup zone. Create a reverse lookup zone based on the LAN address range of your "private" network. (Creating a reverse lookup zone in this manner is normally an incorrect practice, but in our case we have no direct connection to the Internet. There's no other way for incoming traffic to reach your network.)

   In order to work correctly, your DNS configuration must have a forward lookup zone with an address (A) record for the DNS host, and a pointer (PTR) record for the DNS host in the corresponding reverse lookup zone. There should be address and pointer records for each computer in your domain.

   You should be able to browse the web from your Windows 2000 server. If you can do this, it's a good sign that the DNS service is working correctly. Also, you should be able to "nslookup" your organization (and any hosts within it) by name.

4. Make sure that the DHCP server delivers the Windows 2000 DNS server address to workstations when it gives out DNS addresses. Otherwise, workstations on your network won't have any DNS services!

5. Last, you should add a forward lookup zone for the other groups in the class. Use the "pseudo-public" IP block (on the 10.9.69.0/24 subnet) allocated for each different group. This way, you can lookup any other group and its hosts by name.

Setting up a Windows 2000 Internetwork NAT/Router with Port Forwarding

Getting Started

1. Install two (or more) network interface cards in the Windows 2000 server box.

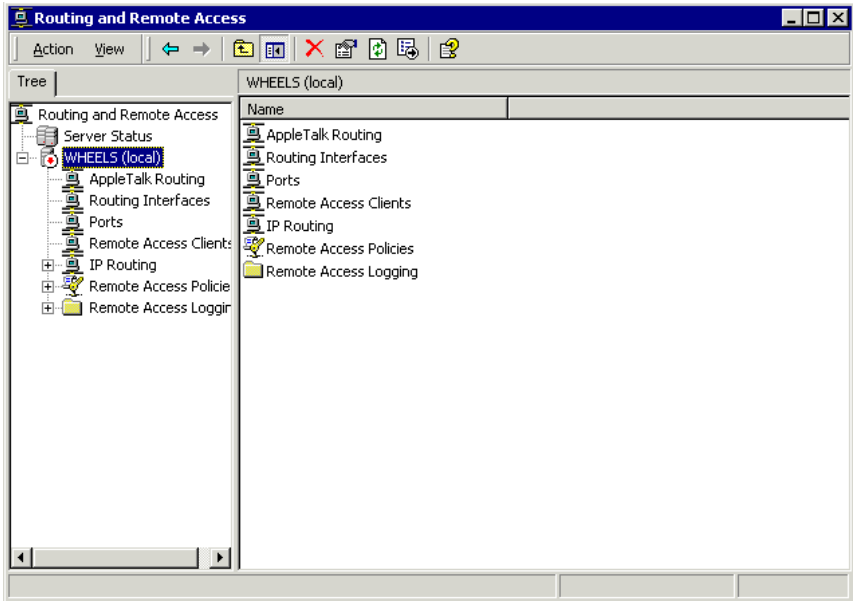
2. Configure the IP address of each card. You'll need to know the gateway address on the remote network, as well as its subnet mask and other information. Write this information down.

3. Under "Administrative Tools" start the "Routing and Remote Access" service manager.

Setting up NAT Services

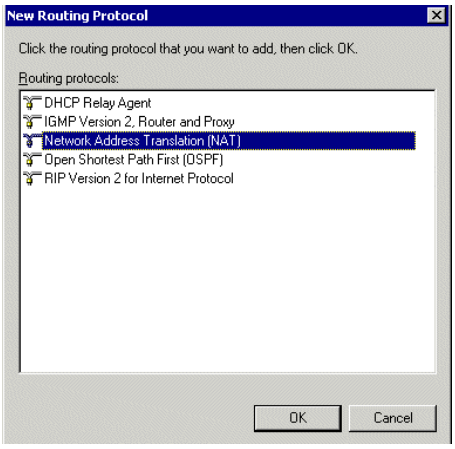
1. Under the Action menu, choose "Configure and Enable Routing and Remote Access." This will start the configuration wizard.

2. Choose the role of the computer to be a "Manually Configured Server" and click NEXT. Allow the service to start. You should now see something like this:



3. Expand "IP Routing" in the left-hand pane by clicking the [+]. A group of IP routing protocols will appear. Right-click on "**General**" and choose "New Routing Protocol..." from the pop-up menu.

4. In the “New Routing Protocol” dialog box choose “Network Address Translation (NAT)” and click OK. Note: Your dialog box may have a different number of protocols available.



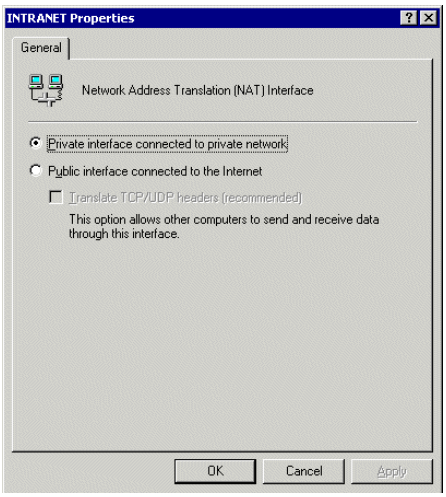
5. The new protocol (Network Address Translation) should now appear under “IP Routing” in the left-hand pane. Click on the new protocol. The right-hand pane should be blank, indicating that no interfaces are yet supporting NAT.

6. Two interfaces are needed for NAT to operate, since NAT translates the addresses in IP packets. Add a NAT interface for the LAN side of your network as follows:

   a) Right-click in the empty right pane and choose “New Interface...”

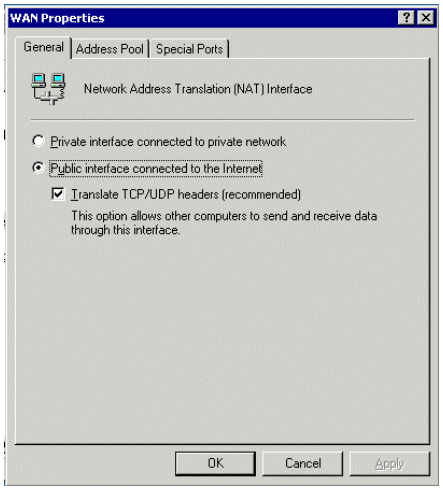
   b) Choose the LAN interface.

   c) The properties box below will appear. Set it as shown (this is the “private” side of the NAT transaction.)



7. Add the second NAT interface by again right-clicking in an empty portion of the right-hand pane and choosing “New Interface...”

a) Choose WAN as the new interface.
b) Choose “Public interface connected to the Internet” as well as “Translate TCP/UDP headers” in the properties box. (This option causes packets outbound on the WAN interface to be address-translated.)



c) Click on the “Address Pool” tab in the WAN Properties box, and add the single address of the WAN interface for *your* group.

NOTE: It is possible for you to use blocks of IP addresses for NAT operation on the WAN side of the router, but not necessary.

d) Click OK to close the WAN properties box. NAT is now correctly set up between the INTRANET and WAN for your group.

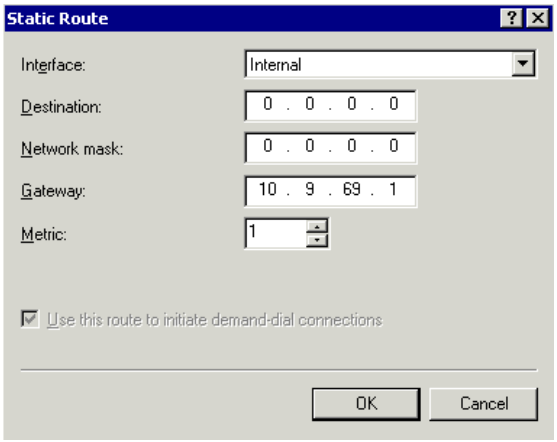
TIP: You may need to stop and restart the Routing and Remote Access Service (RRAS) after making configuration changes to ensure that they actually take effect.

Setting up IP Routing Services

1. Expand "IP Routing" in the left-hand pane (if needed) and add the static routes required. You'll need one default route so that packets are correctly routed to the default gateway at 10.9.69.1 on the E-Net.

   a) Right click on "Static Routes" and choose "New Static Route..."

   b) Fill in the information in the dialog box.



   In the figure above, the destination network is 0.0.0.0 (any), and the gateway is 10.9.69.1 (E-Net gateway). When the firewall computer receives a packet bound for an unknown network, it will automatically forward this packet to *its* default gateway at 10.9.69.1.

2. You can check on all routes available to the Windows 2000 router by using the "`route print`" command from a DOS window. You should see the default route entered in step 1.

Port Forwarding Services

Port forwarding allows specific traffic from the outside (Internet or "WAN") network to pass into your private network. The forwarding is based on the destination port number of the incoming IP packets, which specifies the services being requested from your organization.

You'll need to forward TCP traffic on port 80 to your web server machine so that the other groups can access your web site.

1. Under the "Routing and Remote Access" manager, right click on the NAT interface and choose "properties."

2. On the "Special Ports" tab, click the ADD button.

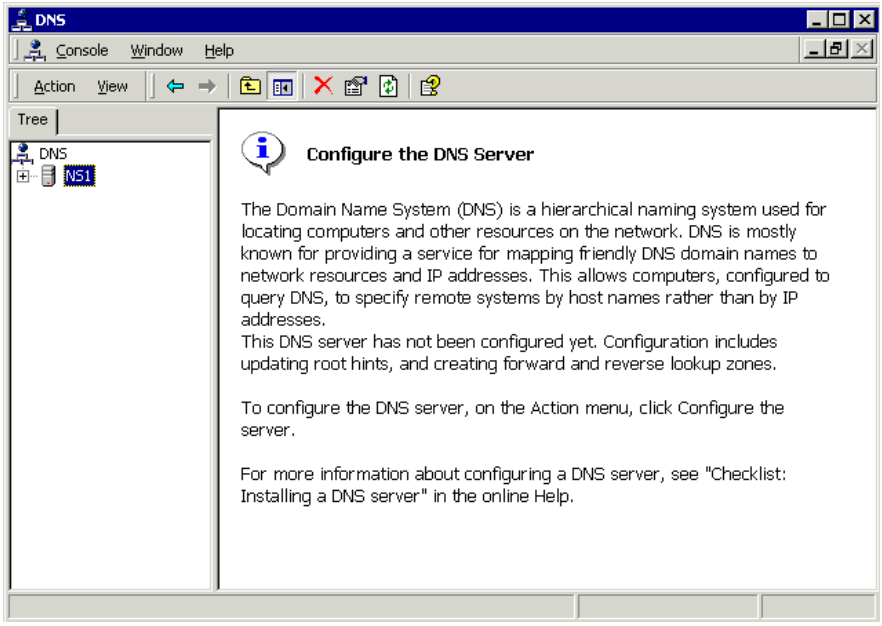
3. Enter 80 for incoming port, the IP address of the web server, and 80 for the outgoing port. Click OK to complete the setup.

How to Configure Windows 2000 DNS

0. Your computer must have a valid domain name before starting. To set this:

   a) Go to "My Computer" and choose "Properties."
   b) Click on the "Network Identification" tab and click the "Properties" button.
   c) A dialog box marked "Identification Changes" will appear. Click the MORE button to set the primary DNS suffix of the computer (set it equal to the FQDN of your organization.)
   d) Click OK to close these dialogs. Restart the computer to make the changes take effect.

1. Under "Administrative Tools" start the DNS manager. You should see the following screen:



2. Right-click on the server icon (shown as "NS1" in the figure above) and choose "Configure the server." This will start the DNS Configuration Wizard.

3. In the Wizard, choose the following options. (Each of the below represents one step of the wizard):

   a) Create a forward lookup zone.
   b) Set the zone as a standard primary type.
   c) The name of the zone should be the FQDN of your organization ("n0gsg.com", for example.)
   d) Allow the system to create a new zone file with the recommended name.
   e) Create a reverse lookup zone.
   f) The type of reverse lookup zone is standard primary.
   g) Type in the network ID of the zone. (You'll only be permitted as many octets as the subnet mask of your network permits.)
   h) Create a new zone file for reverse lookup.
   i) Click FINISH to close the Wizard.

4. For DNS to work correctly, the name of the DNS server computer must be properly configured in both forward and reverse lookup tables. Traditionally DNS hosts are given the names "ns1", "ns2", and so on. Using the name of *your* computer:

   a) Expand the folder for the Reverse Lookup Zones in the left-hand pane of the DNS control panel until you find the folder marked with your IP subnet.

   b) Open this folder and add a pointer record (right click in the right-hand pane and choose "New Pointer..."

   c) Enter the remaining octet(s) of the DNS host computer and the name prefix of the DNS host (NOT a fully qualified domain name.)

   d) If the DNS host has several IP addresses, each one should be in both a forward and reverse lookup zone.

5. To test DNS, issue a `nslookup` command on the DNS machine for a known host. If DNS is working correctly, should get a response like this:

```
F:\Documents and Settings\Administrator>nslookup swbell.net
Server:  ns1
Address:  192.168.1.4

Non-authoritative answer:
Name:    swbell.net
Address:  151.164.129.2
```

6. It is helpful to be able to view the DNS cache. To see it, click on the server name ("NS1" in the figure above), then choose "Advanced" from the VIEW menu.