

Microsoft Windows Network Administration Portfolio

CIS 196
Spring 2006

Rich Simms
May 30, 2006
Cabrillo College

Table of Contents

Lab 1 - Joining a Host to a Network
Lab 2 - Filters and Network Address Translation (NAT)
Lab 3 - Domain Name System
Lab 4 - Remote Access

Lesson 1 - Networking Overview
Lesson 2 - Network Protocols
Lesson 3 - TCP/IP Architecture
Lesson 4 - Routing and Subnetting
Lesson 5 - Dynamic Host Configuration Protocol
Lesson 6 - Name Resolution
Lesson 7 - Managing and monitoring DHCP
Lesson 8 - DNS
Lesson 9 - Security and Group Policy
Lesson 10 - IPSec
Lesson 11 - Software Update Service
Lesson 12 - Remote Access
Lesson 13 - Remote Access continued
Lesson 14 - Troubleshooting

Worksheets

Virtual Lab

March 6, 2006

Learn how to utilize multiple network interface cards on a single computer. A Windows Server 2003 computer with dual NIC's will be configured to be a member of two networks. On one NIC the computer will join a peer-to-peer network. On the other NIC it will join a different network and become a member of a domain.

The diagram illustrates a network topology where a central cloud, labeled "Cabrillo Net", connects several distinct local networks. On the left, a network with IP range 207.62.186.0 contains a server named "Opus" with IP .9. On the right, a network with IP range 207.62.187.0 contains a "DNS Server" with IP .54. These two external networks are connected to the central cloud. The cloud is then connected to a "Router" with IP .1. This router is part of a larger network that includes two switches. One switch is connected to a server named "Dovercorp.net" with IP .10. The other switch is connected to a network with IP range 172.30.4.0, labeled "The Shire" network, which contains a server named "Frodo" with IP .109. A third network, highlighted in green and labeled "Rivendell" network, has IP range 192.168.2.0 / 24. It contains three servers: "Arwen" (.108), "Celebrian" (.107), and "Legolas" (.105). A switch in this network is connected to a server named "Elrond" with IP .106. A blue arrow points from a text box stating "This connection configured on Elrond in Lab 1 so it can be a member of two networks" to the connection between the "Rivendell" network and "The Shire" network, indicating that Elrond is a member of both.

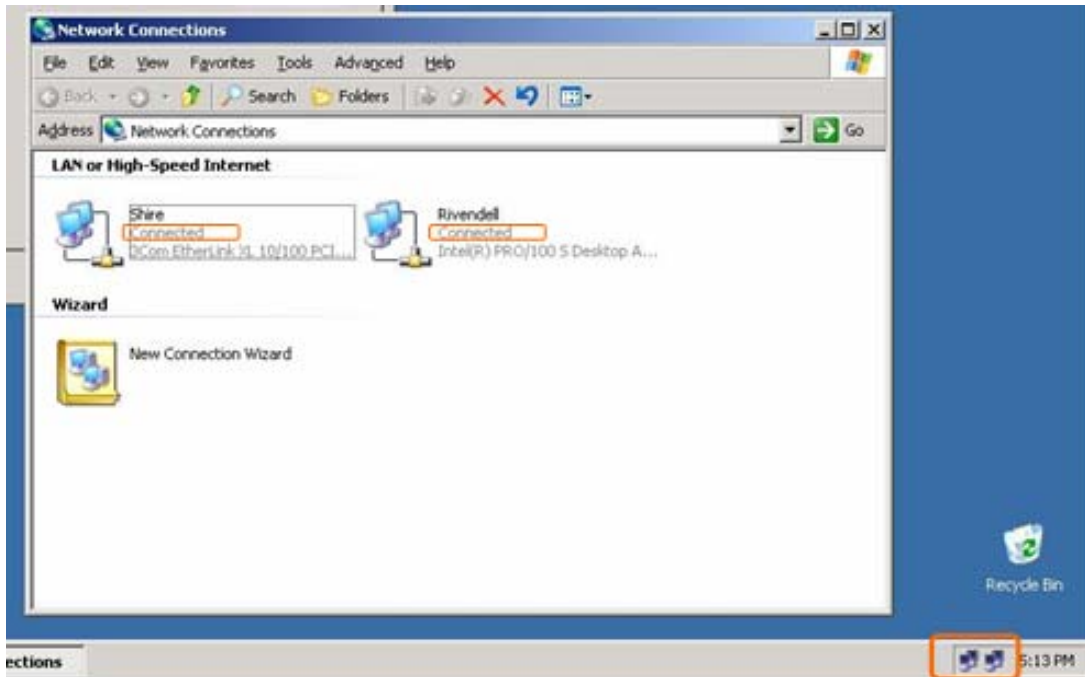
```
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
```

```
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
```

Ping statistics for 207.62.186.9:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Showing the system configured with two network interfaces up.



The correct values for IP addresses, Default Gateway and DNS Server.

Windows IP Configuration

```
Host Name . . . . . : elrond
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter **Rivendell:**

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/100 S Desktop Adapter
Physical Address. . . . . : 00-02-B3-4C-14-3F
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.2.106
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Ethernet adapter **Shire:**

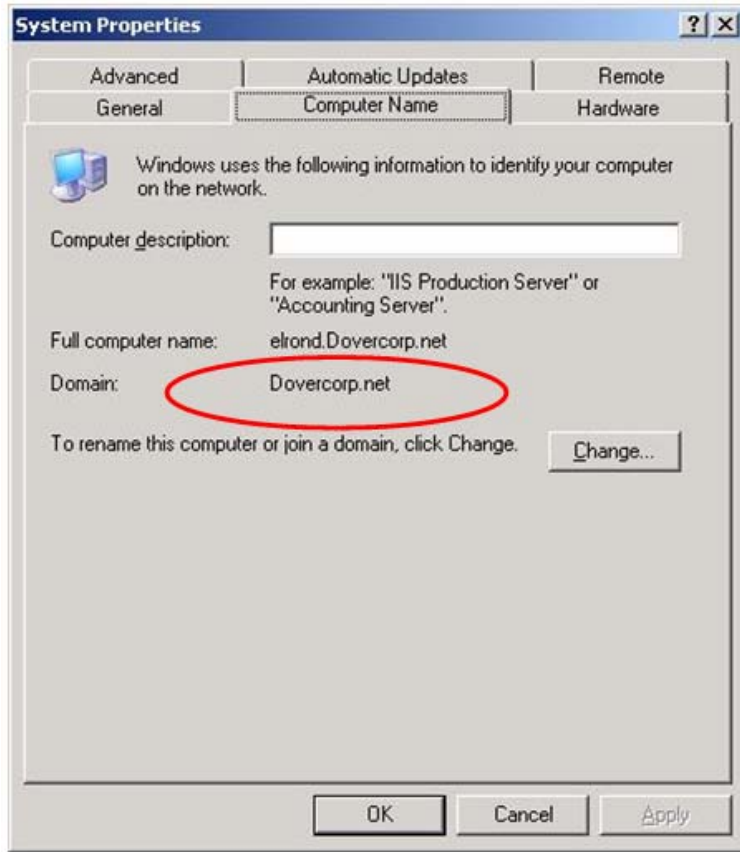
```
Connection-specific DNS Suffix . :
Description . . . . . : 3Com EtherLink XL 10/100 PCI TX NIC
(3C905B-TX)
```

```

Physical Address. . . . . : 00-50-DA-6E-7F-29
DHCP Enabled. . . . . : No
IP Address. . . . . : 172.30.4.106
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.30.4.1
DNS Servers . . . . . : 172.30.4.10

```

Showing the system configured as a member server to the Dovercorp.net domain.



Lessons Learned

I see, at last, the reason why someone would want to have more than one NIC to make a “multi-homed” computer. I understand now how a customer could configure separate management and production LANs for a set of dual NIC servers. (I also see now why HP ProLiant blade servers ship with two NICs already built in.) New skills I learned include the /all option on `ipconfig` which is valuable for capturing all the network configuration information. I also spent some time manually “discovering” the system networks in the lab by following cables and looking at network configurations. Finally I learned to verify uploads to my Yahoo Briefcase to make sure the results I saved were the right ones. Hopefully next time I won’t have to come back and set up the lab a second time again to get the screen shot!

Original Lab with Notes

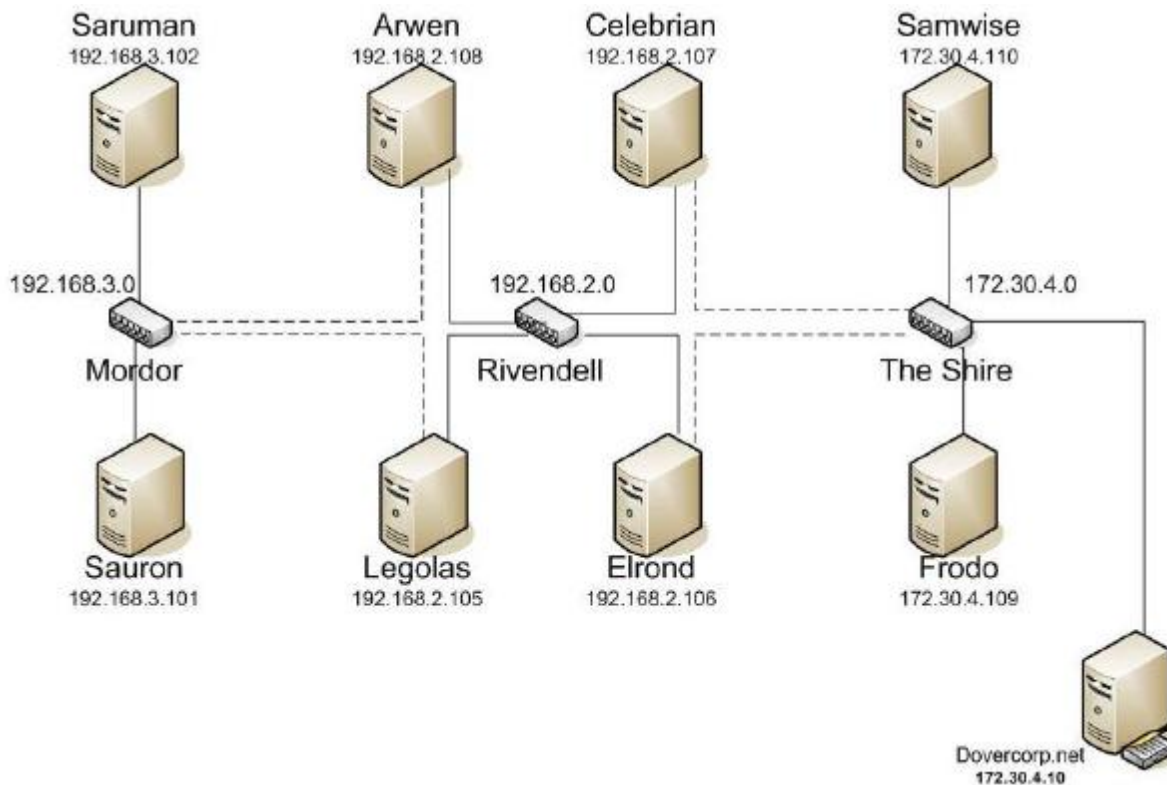
Text from Jim Griffin's original lab document in gray

Text added by student in black

The purpose of this lab is to join a Windows 2003 server to both a peer-to-peer and a domain network. It will involve configuring the network interface of a second NIC card, as well as configuring the identity of the computer to become a member server of an existing Domain.

Background

The computers in the lab, (Room 2504, or the CTC), are currently setup in separate peer-to-peer networks. The networks are hub based and there are three of them:



There is a domain controller on the Shire network that is serving the Domain:

Dovercorp.net

Joining a standalone server to a network involves 3 steps:

1. Installing the network adapter (NIC)
2. Installing the device driver for the network adapter.
3. Configuring the NIC

To join a Domain, an added step is required to change the identity, (name), of the computer and give it an account in the Domain.

You will be working with the computers in the Rivendell network, specifically, I suggest working with **Elrond** or Celebrian, as they are already cabled to the shire with the appropriate NIC.

Procedure

Part I

The first part of this lab assumes the first two steps have already been done. But let's verify this before we proceed.

1. Log on as Administrator using the password: *Cabrillo* ✓
2. Verify that the network adapters have been installed using the Device Manager. ✓
Note the names of the drivers by double-clicking on each adapter and checking the Drivers tab. ✓ **Note the two NICs are: 3Com Ethernet XL 10/100 PCI TX NIC (3C905B-TX) and Intel PRO/100 S Desktop Adapter**
How would you disable these devices if they were not working? **You can right-click enable/disable on these adapters in Device Manager**
3. Now From the Start -> Control Panel menu, check the Network Connections. You should have two. ✓ **(they are named Shire and Rivendell)**
Holding the mouse sprite over each connection will reveal the network adapter associated with that interface. This is useful for figuring out which interface goes with which NIC. ✓
4. Right-click each interface and note whether it is enabled or disabled.
Also note that you can rename the connection. ✓ **Shire (3Com) disabled, Rivendell (Intel) enabled**
5. The Intel 100 Pro adapter is the NIC joining you to the Rivendell network; Note its configuration by following the properties menu option. ✓ **ip 192.168.2.106, subnet mask 255.255.255.0, no default gateway, DNS 172.30.4.10**
Note that no Gateway or DNS nameserver is configured. ✓ **Note, the DNS was set so I removed it**
6. Verify that you can ping one or more of the other computers on the Rivendell network. Their IP addresses are as follows:

- Legolas: 192.168.2.105 ✓ **success**
- Elrond: 192.168.2.106 ✓ **success**
- Celebrian: 192.168.2.107 ✓ **success**
- Arwen: 192.168.2.108 ✓ **failed, being worked on by another student and temporarily not responding**

Part II

Now we will configure the interface for the second NIC card and connect our host to the Shire network.

1. The second NIC card is **not** the Intel Pro 100. It is most likely a 3Com card, but may be something else altogether. Enable this interface by right clicking on the interface from the Network Connections menu under Control Panel. ✓ **3Com NIC**
2. Using the TCP/IP Properties dialog box configure the following parameters:
 - IP Address: **172.30.4.XXX** where XXX is the same host id as the first interface. ✓
 - Network Mask: **255.255.255.0** ✓
 - Default Gateway: **172.30.4.1** ✓
 - DNS Nameserver: **172.30.4.10** ✓
3. Save this information by closing all open dialog boxes. ✓
4. Verify that you can now connect to computers on the Shire network by **pinging** both the Frodo machine (172.30.4.109) and your default Gateway: 172.30.4.1 ✓ **success**
5. Save the output of the following ping command to a file:
`ping opus.cabrillo.edu > results1` ✓ **see below**
6. Note that you are not a router, even though you are connected to two networks; packets will not travel through you from one network to another, but you have access to computers on both networks now. ✓
7. View and save this information by running the command:
`ipconfig /all` ✓
 from a command window and redirecting the output to the file: **results2** ✓

Part III

In this final procedure we will join our standalone server to the Dovercorp Domain. To join a domain, your computer needs to have an account in that Domain. An account will be created for you if you have access to sufficient privilege in the Domain. Such an account for this exercise has been created. The username is **gandalf** and the password is *Mithrandi1* (the final character of the password is a one.)

Note: this is an account on the domain controller, not on your local machine.

1. Bring up the System Properties dialog box and click on the Computer Name tab. Note the current name of your computer. ✓
2. Click the **Change** button, and note the you are currently a Workgroup member ✓
3. Click the *Member of Domain* radio button and type in the domain name you wish to join: **Dovercorp.net** ✓
4. When you click **OK** you will be asked for an account in the Domain that has the authority to join you to the Domain. Use the account/password mentioned above. It takes a minute or two, but you should soon be Welcomed to the domain. You must reboot the computer for the changes to take effect. ✓
5. The system may take a little longer than normal to reboot, since domain information will be downloaded to your member server. ✓
6. When you get the login dialog box, click the **Options** button and note that you can either log on to THIS COMPUTER (a local login) or you can log on to the Dovercorp domain. ✓
7. Log on to THIS COMPUTER as administrator, since you don't have a Domain account. ✓
8. Bring up the **System Properties** dialog box and note the new name of your computer. ✓
9. Take a screen shot of the **Computer Name** tab by pressing *alt-PrintScreen*, pasting the image into WordPad, and saving it to a file named: **results3** WordPad will append a **.rtf** extension to your file; remove this extension before submitting the file. ✓

Cleanup:

1. Once you have collected your results files, unjoin yourself from the domain by selecting the **Change** button and joining the Workgroup: WORKGROUP ✓
2. Set the Shire interface back to automatic DNS and IP addressing, and then disable the connection. ✓
3. Shut down the computer; the system will now be ready for the next student. ✓
4. Include your three results files in your lab document. Also include a network diagram showing how your computer is a member of two networks, and label the respective interfaces. ✓

Grading Rubric

20 Points possible

5 points for:

Showing a successful **ping** output between your system and the opus computer.

```
Pinging opus.cabrillo.edu [207.62.186.9] with 32 bytes of data:
```

```
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
Reply from 207.62.186.9: bytes=32 time<1ms TTL=63
```

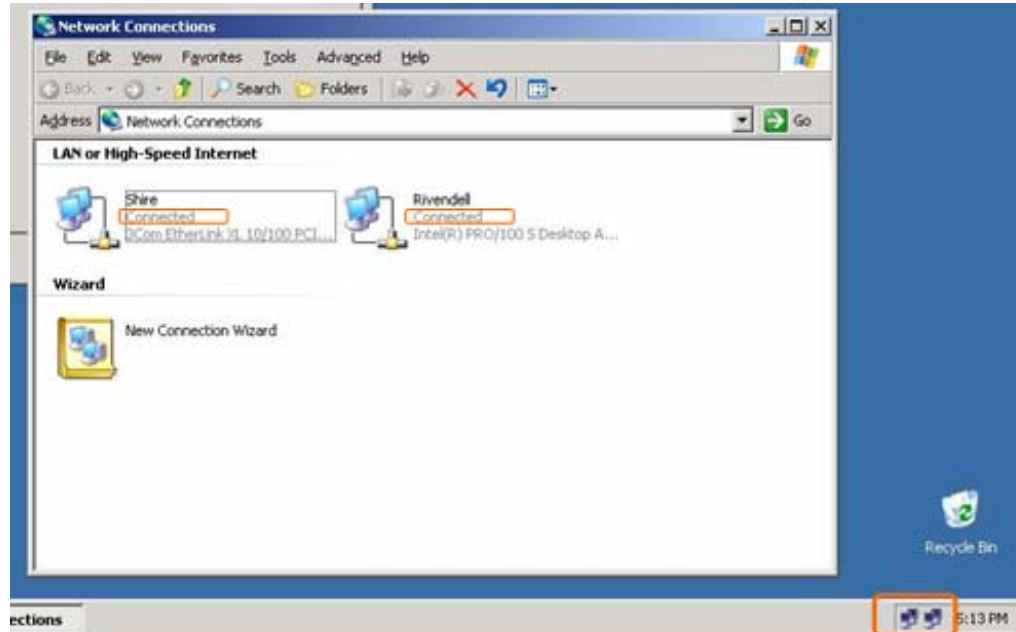
```
Ping statistics for 207.62.186.9:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

5 points for:

Showing the system configured with two network interfaces up.



5 points for:

The correct values for IP addresses, Default Gateway and DNS Server.

Windows IP Configuration

```
Host Name . . . . . : elrond
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Rivendell:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/100 S Desktop Adapter
Physical Address. . . . . : 00-02-B3-4C-14-3F
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.2.106
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

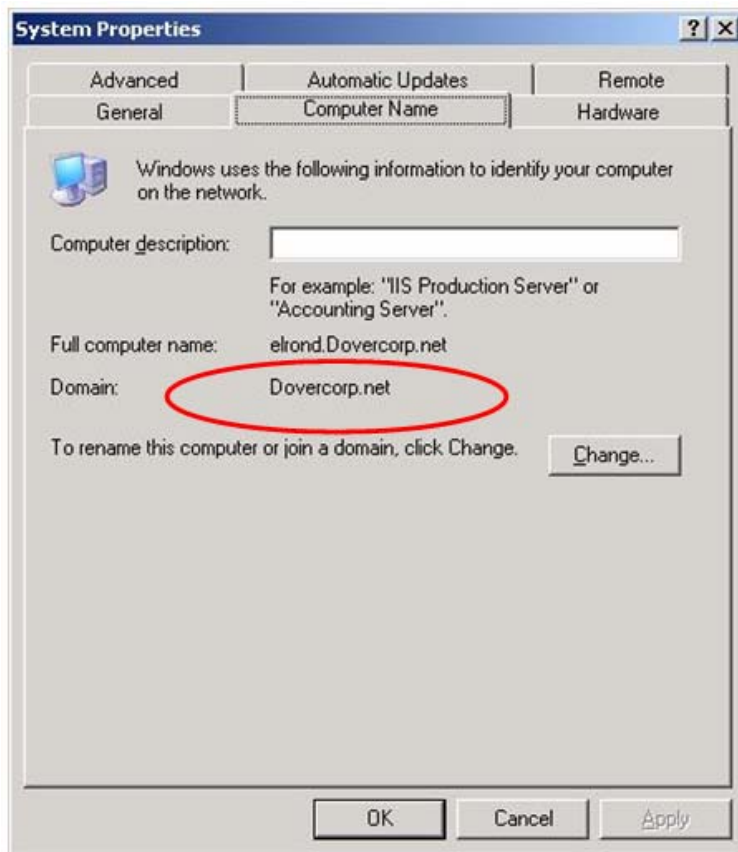
Ethernet adapter Shire:

```
Connection-specific DNS Suffix . :
Description . . . . . : 3Com EtherLink XL 10/100 PCI TX
NIC (3C905B-TX)
Physical Address. . . . . : 00-50-DA-6E-7F-29
DHCP Enabled. . . . . : No
IP Address. . . . . : 172.30.4.106
Subnet Mask . . . . . : 255.255.255.0
```

```
Default Gateway . . . . . : 172.30.4.1  
DNS Servers . . . . . : 172.30.4.10
```

5 points for:

Showing the system configured as a member server to the Dovercorp.net domain.



CIS 196 - Lab 2: Filters and Network Address Translation (NAT)

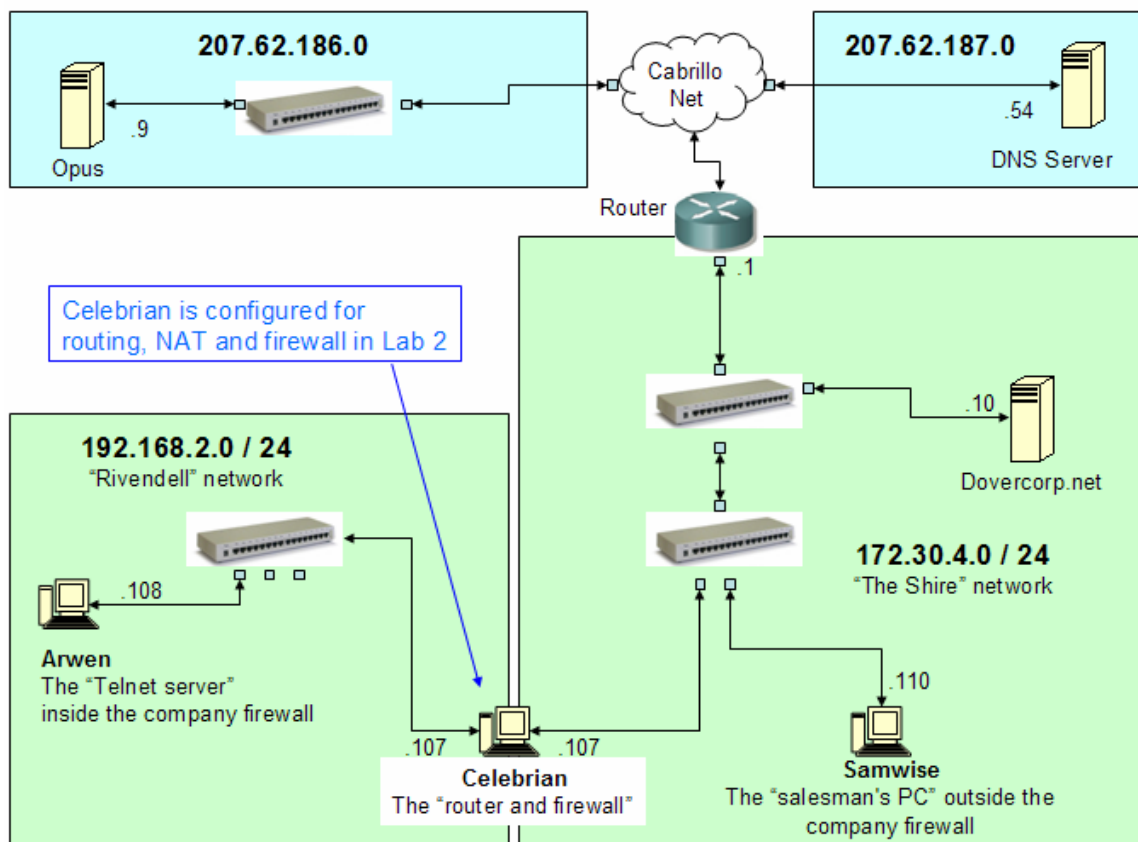
Rich Simms

March 27, 2006

Objective

Learn how to utilize the routing, firewall, filtering and NAT capabilities of a Windows 2003 server to allow selective access to resources inside a company firewall to employees working outside. Specifically in this lab we will configure Celebrian to provide access (routing, firewall, filtering and network address translation) to a specific Telnet Server (Arwen) from an “external” host in the Shire (Samwise).

Layout



Results

Showing a successful telnet session from the Shire client to the Rivendell telnet server:

```
*=====
Welcome to Microsoft Telnet Server.
*=====
C:\Documents and Settings\Administrator>hostname
arwen
```

Showing a successful ping from the telnet server to opus.cabrillo.edu:

```
C:\Documents and Settings\Administrator>ping opus.cabrillo.edu

Pinging opus.cabrillo.edu [207.62.186.9] with 32 bytes of data:

Reply from 207.62.186.9: bytes=32 time=2ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62

Ping statistics for 207.62.186.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Rivendell:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.108
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.107

C:\Documents and Settings\Administrator>exit

Connection to host lost.
```

and an unsuccessful ping from the Shire client to the Rivendell router:

```
C:\Documents and Settings\Administrator>hostname
Samwise

C:\Documents and Settings\Administrator>ping 172.30.4.107

Pinging 172.30.4.107 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.30.4.107:
```

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>

Lessons Learned

I learned a great deal in this lab. Before taking this class I had no idea Windows 2003 server could be configured to be a router, firewall and provide NAT services. I learned the key to this is to use the RRAS (Routing and Remote Access) MMC snap-in. There are some definite subtleties to configuring these capabilities and that though millions of configuration combinations are possible most don't do what you want! Attention to detail is very important when configuring this service. I learned that in Windows 2003 SP1 the Allow Incoming Sessions option **must** be enabled now as the Reserve Addresses does only that now. Jim mentioned prior to SP1 the Allow Incoming Sessions could be disabled and selectively opened using the Reserve Address capability. Additional filtering can be configured separately for incoming and outgoing packets down to the port level. One mistake I made when setting of a filter was to not notice the default action is to allow all packets except the telnet port 23 file I created. You must check the drop all packets except those meeting the filter criteria.

Text from Jim Griffin's original lab document in gray

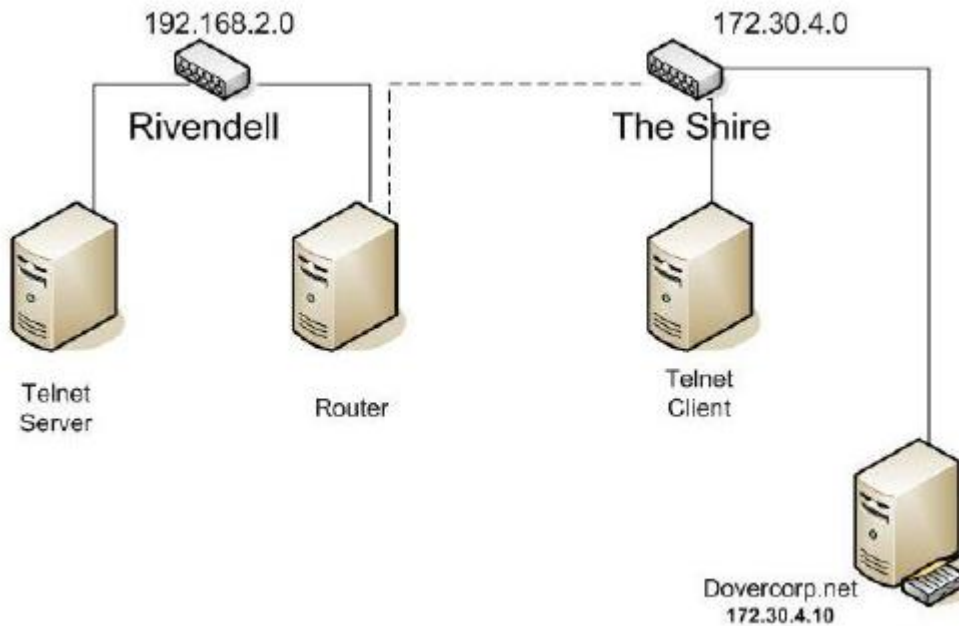
Text added by student in black

The purpose of this lab is to exercise the use of network filters, address translation, and routing to build a permissive firewall by selectively filtering packets based on protocol type. It also demonstrates how addresses may be translated from private addresses to public and vice versa as they pass in and out of the firewall. The goal of this lab is to allow internet access to the hosts in Rivendell, and to allow hosts in the Shire only telnet access, and no other, to a single host in Rivendell. Celebrian or Elrond may act as the gateway/firewall between Rivendell and the Shire.

Background

Note that the current state of the Rivendell network is that Celebrian and Elrond are the only hosts that have access to the Internet. That is because Celebrian and Elrond have a network interface directly onto the 172.30.4.0 network. For the sake of this lab, we will treat the 172. IP addresses as if they were public and the 192. addresses as private. To the world outside of the firewall, your gateway provides the public address of 172.30.4.XXX. The Rivendell telnet server will appear to have a public address of

172.30.4.105/108



The mmc consoles we will be using for this lab are:

- RRAS
- Services

Procedure

Part I

In this step, you will setup the above network with no firewall and verify connectivity in both directions through the gateway (router).

1. Log in to your chosen gateway, Celebrian or Elrond, and join the Shire (172.30.4.0) subnet as your public interface. ✓ **using Celebrian**
2. Set the default gateway to 172.30.4.1 (the Internet) and DNS Nameserver to 207.62.187.54 ✓
3. Turn on Routing using the RRAS console. Simple LAN routing will do. ✓
4. Log in to a Rivendell host such as Arwen or Legolas, and enable and start the telnet service using Administrative Tools -> Services. ✓
5. Ensure that the default route has been configured to be the gateway you are using, and that the nameserver is set to 207.62.187.54. ✓
6. Log in to one of the Shire machines, and verify that it can ping your router. ✓
ping 172.30.4.107 ok
7. Can you ping the telnet server from the Shire? Why or why not? ✓ **no, samwise has no route to 192.168.2.0**

8. Provide a route for 192.168.2.0 packets that goes to your Rivendell gateway. ✓
route add 192.168.2.0 mask 255.255.255.0 172.30.4.107
9. Can the Rivendell telnet server ping the Shire side of the router? ✓ no, ping 172.30.4.110 fails, need to enable IP forwarding on Celebrian using RRAS MMC snap-in and configure LAN routing. This results in a "green" light for Celebrian in RRAS,
10. Verify that your router can run a telnet session on the Rivendell telnet server. ✓
yes, note: you can log in without having to provide credentials!

Part II

In this procedure we will configure Network Address Translation and a basic one-way firewall that will allow Rivendell hosts to contact the SHire host and the Internet.

1. On your gateway server, open up the RRAS console and expand the Server/IP Routing menu. ✓
2. Under **IP Routing** should be a **NAT/Basic Firewall** menu. If **it is not there**, right-click the **General** menu and select **New Routing Protocol**. and then select **NAT/Basic Firewall**. ✓
3. Right-click the **NAT/Basic Firewall** menu and use the **New Interface** submenu to configure your public (Shire) and private (Rivendell) interfaces:
 - In the Network Address Translation Properties dialog box for the Shire interface
 - select **Public interface connected to the Internet** ✓
 - select **Enable NAT on this Interface** ✓
 - and **Enable a basic Firewall** ✓
 - In the Network Address Translation Properties dialog box for the Rivendell interface
 - select **Private interface connected to private network** ✓
4. We should now be blocking all network traffic initiated from the outside world into our router/firewall, but our telnet server should now be able to ping the shire host and to surf the web. Verify this. ✓

Samwise:

Ping 172.30.4.107 fails

Ping 192.168.2.107 fails

Ping 192.168.2.108 fails

Arwen:

Ping 172.30.4.110 succeeds

Ping www.google.com succeeds

Can the Shire (Samwise) host ping the router? No the telnet server? No

Part III

Now we will further configure our firewall to allow outside hosts to use our telnet server, we will allow only telnet packets to be forwarded through our firewall from the outside world. To do this, we will have to allocate a public IP address that will translate to the telnet server's private IP address.

1. On the router/firewall, use the **RRAS** console to bring up the **Network Address Translation Properties** dialog box for the **public** (Shire) interface. ✓
2. Click the **Address Pool** tab and add a range of "public" IP address that includes both your router's host address and your telnet server's host address, e.g.
172.30.4.107 – 172.30.4.108 (**Celebrian – Arwen**) ✓ or 172.30.4.105 – 172.30.4.106
3. Once you have set up the pool, make a reservation for the telnet server. This will map the public address of 172.3.4.10? to the private address of your telnet server. In the **Reserve Address** dialog box, provide the:
 - Public address and netmask ✓
 - Private address ✓
 - Select the **Allow Incoming Sessions** checkbox, (we will specify telnet traffic in the next step.) ✓ **Note: I did have to check this for it to work correctly. Confirmed with Jim that that is how it works now with SP1.**
4. In the **Service and Ports** tab, click the **Telnet** checkbox and fill out the following information:
 - **On this address pool entry** ✓ 172.30.4.108
 - **Private address** ✓ 192.168.2.108
5. You should now be able to access the internal telnet service from the public IP address from a client in the Shire. ✓
6. For completeness, look at the **ICMP** tab in the **NAT Properties** dialog box. Is any ICMP traffic allowed? ✓ **no, note: I temporarily enabled incoming echo requests and could successfully ping Celebrian, then I disabled it again so pings would fail.**

Congratulations! You have created a secure network in Rivendell with all machines having access to the Internet! Only your telnet server is accessible from the outside.

Your Results

For this lab assignment, I want to see:

1. a telnet session to the telnet server where the following three commands are run:
 - **hostname** ✓
 - **ping opus.cabrillo.edu** ✓
 - **exit** ✓
2. an unsuccessful ping from the Shire computer to your router. ✓

To collect this data, bring up a command line window on the Shire computer in which to execute the telnet session:

```
telnet 172.30.4.10?
```

Use the *administrator* account with the password: *Cabrillo* to log on.

You should get a screen with the banner:

```
Welcome to Microsoft Telnet Server
```

Execute the commands requested above, and capture the screen output into a text file. To do this, right-click on the title bar of the System Command window and select Edit/Select All. Hit the Enter key and this will copy the text data to the clipboard. You can then paste it into Notepad to create your lab2 text file.

Grading Rubric

10 Points possible

5 points for:

showing a successful telnet session from the Shire client to the Rivendell telnet server

```
*=====
Welcome to Microsoft Telnet Server.
*=====
C:\Documents and Settings\Administrator>hostname
arwen
```

5 points for:

showing a successful ping from the telnet server to opus.cabrillo.edu,

```
C:\Documents and Settings\Administrator>ping opus.cabrillo.edu

Pinging opus.cabrillo.edu [207.62.186.9] with 32 bytes of data:

Reply from 207.62.186.9: bytes=32 time=2ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62
Reply from 207.62.186.9: bytes=32 time=1ms TTL=62
```

```
Ping statistics for 207.62.186.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\Documents and Settings\Administrator>ipconfig
```

Windows IP Configuration

Ethernet adapter Rivendell:

```
Connection-specific DNS Suffix  . :
IP Address. . . . . : 192.168.2.108
Subnet Mask . . . . . : 255.255.255.0
```

```
Default Gateway . . . . . : 192.168.2.107
```

```
C:\Documents and Settings\Administrator>exit
```

```
Connection to host lost.
```

and an unsuccessful ping from the Shire client to the Rivendell router

```
C:\Documents and Settings\Administrator>hostname
```

```
Samwise
```

```
C:\Documents and Settings\Administrator>ping 172.30.4.107
```

```
Pinging 172.30.4.107 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 172.30.4.107:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Documents and Settings\Administrator>
```

CIS 196 - Lab 3: DHCP and DNS

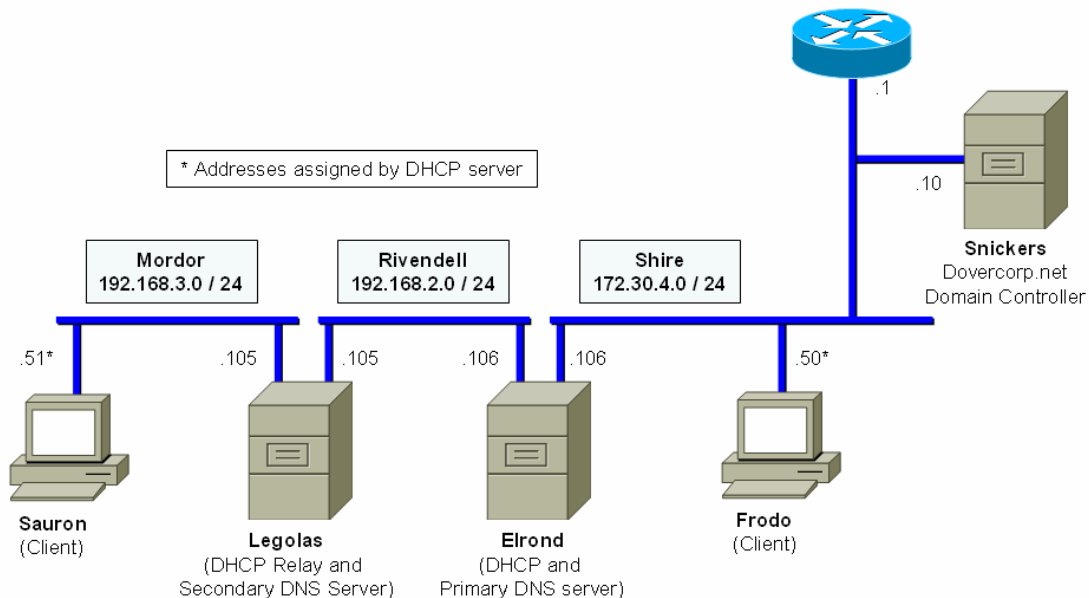
Rich Simms

May 1, 2006

Objective

The objective of this lab is to show how a Windows 2003 server can function as a DHCP and DNS server in a domain environment. Elrond will be configured as both a DHCP server and a primary DNS server. Legolas will be configured as a DHCP relay and a secondary DNS server. Elrond will provide DHCP service for the Rivendell and Shire networks. Legolas will provide DHCP service for the Mordor network. Snickers will provide DHCP service for the Mordor network.

Layout



Results

The audit log for the DHCP Server (Elrond):

DhcpSrvLog-Wed (on Elrond)

Microsoft DHCP Service Activity Log						
Event ID	Meaning					
00	The log was started.					
01	The log was stopped.					
02	The log was temporarily paused due to low disk space.					
10	A new IP address was leased to a client.					
11	A lease was renewed by a client.					
12	A lease was released by a client.					
13	An IP address was found to be in use on the network.					
14	A lease request could not be satisfied because the scope's address pool was exhausted.					
15	A lease was denied.					
16	A lease was deleted.					
17	A lease was expired.					
20	A BOOTP address was leased to a client.					
21	A dynamic BOOTP address was leased to a client.					
22	A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.					
23	A BOOTP IP address was deleted after checking to see it was not in use.					
24	IP address cleanup operation has begun.					
25	IP address cleanup statistics.					
30	DNS update request to the named DNS server					
31	DNS update failed					
32	DNS update successful					
50+	Codes above 50 are used for Rogue Server Detection information.					
ID	Date	Time	Description	IP Address	Host Name	MAC Address
00	04/19/06	08:10:12	Started			
50	04/19/06	08:10:12	Unreachable Domain		dovercorp.net	8240
56	04/19/06	08:10:12	Authorization failure, stopped servicing		dovercorp.net	
50	04/19/06	08:10:12	Unreachable Domain		dovercorp.net	8240
55	04/19/06	08:34:56	Authorized(servicing)		dovercorp.net	
30	04/19/06	09:00:51	DNS Update Request	50.4.30.172	frodo	
10	04/19/06	09:00:51	Assign	172.30.4.50	frodo	0003FF9D8E68
31	04/19/06	09:01:13	DNS Update Failed	172.30.4.50	frodo	2
30	04/19/06	09:01:13	DNS Update Request	50.4.30.172	frodo	
11	04/19/06	09:01:13	Renew	172.30.4.50	frodo	0003FF9D8E68
24	04/19/06	09:10:13	Database Cleanup Begin			
31	04/19/06	09:10:13	DNS Update Failed	172.30.4.50	frodo	2
30	04/19/06	09:10:13	DNS Update Request	50.4.30.172	frodo	
25	04/19/06	09:10:13	0 leases expired and 0 leases deleted			
25	04/19/06	09:10:13	0 leases expired and 0 leases deleted			
01	04/19/06	09:14:17	Stopped			
00	04/19/06	09:14:30	Started			
55	04/19/06	09:14:30	Authorized(servicing)		dovercorp.net	
30	04/19/06	10:14:28	DNS Update Request	51.3.168.192	sauron	
10	04/19/06	10:14:28	Assign	192.168.3.51	sauron	0003FF868E68
24	04/19/06	10:14:34	Database Cleanup Begin			
30	04/19/06	10:14:34	DNS Update Request	50.4.30.172	frodo	
31	04/19/06	10:14:34	DNS Update Failed	192.168.3.51	sauron	2
30	04/19/06	10:14:34	DNS Update Request	51.3.168.192	sauron	
25	04/19/06	10:14:34	0 leases expired and 0 leases deleted			
25	04/19/06	10:14:34	0 leases expired and 0 leases deleted			
31	04/19/06	10:25:24	DNS Update Failed	192.168.3.51	sauron	2
30	04/19/06	10:25:24	DNS Update Request	51.3.168.192	sauron	
11	04/19/06	10:25:24	Renew	192.168.3.51	sauron	0003FF868E68
31	04/19/06	10:28:53	DNS Update Failed	172.30.4.50	frodo	-1
31	04/19/06	10:35:14	DNS Update Failed	192.168.3.51	sauron	2
30	04/19/06	10:35:14	DNS Update Request	51.3.168.192	sauron	
12	04/19/06	10:35:14	Release	192.168.3.51	sauron	0003FF868E68

```

31,04/19/06,10:35:28,DNS Update Failed,192.168.3.51,sauron.,2,
30,04/19/06,10:35:28,DNS Update Request,51.3.168.192,sauron.,,
10,04/19/06,10:35:28,Assign,192.168.3.51,sauron.,0003FF868E68,
30,04/19/06,10:35:52,DNS Update Request,50.4.30.172,frodo.,,
12,04/19/06,10:35:52,Release,172.30.4.50,frodo.,0003FF9D8E68,
32,04/19/06,10:35:52,DNS Update Successful,172.30.4.50,frodo.,,
30,04/19/06,10:35:57,DNS Update Request,50.4.30.172,frodo.,,
10,04/19/06,10:35:57,Assign,172.30.4.50,frodo.,0003FF9D8E68,
32,04/19/06,10:35:57,DNS Update Successful,172.30.4.50,frodo.,,
31,04/19/06,10:49:44,DNS Update Failed,192.168.3.51,sauron.,-1,
24,04/19/06,11:14:37,Database Cleanup Begin,,,,
30,04/19/06,11:14:37,DNS Update Request,51.3.168.192,sauron.,,
25,04/19/06,11:14:37,0 leases expired and 0 leases deleted,,,,
25,04/19/06,11:14:37,0 leases expired and 0 leases deleted,,,,
32,04/19/06,11:14:37,DNS Update Successful,192.168.3.51,sauron.,,
24,04/19/06,12:14:39,Database Cleanup Begin,,,,
25,04/19/06,12:14:39,0 leases expired and 0 leases deleted,,,,
25,04/19/06,12:14:39,0 leases expired and 0 leases deleted,,,,
01,04/19/06,12:21:56,Stopped,,,,

```

The DNS database secondary zone files (on Legolas) that came from the zone transfer.

Dovercorp.net.dns (on Legolas secondary DNS server)

```

;
; Database file Dovercorp.net.dns for Dovercorp.net zone.
; Zone version: 12
;

@                IN  SOA  elrond.  hostmaster.dovercorp.net. (
                        12          ; serial number
                        900          ; refresh
                        600          ; retry
                        86400         ; expire
                        3600          ) ; default TTL

;
; Zone NS records
;

@                NS    legolas.dovercorp.net.
@                NS    elrond.

;
; Zone records
;

arwen             A      192.168.2.108
celebrian         A      172.30.4.107
elrond            A      192.168.2.106
                  A      172.30.4.106
frodo             A      172.30.4.50
lab-router        A      172.30.4.1
legolas           A      192.168.2.105
samwise           A      172.30.4.110
saruman           A      192.168.3.102
sauron            A      192.168.3.51
snickers          A      172.30.4.10

```

2.168.192.in-addr.arpa.dns (on Legolas secondary DNS server)

```

;
; Database file 2.168.192.in-addr.arpa.dns for 2.168.192.in-addr.arpa zone.
; Zone version: 7
;
@           IN SOA elrond.dovercorp.net. hostmaster.dovercorp.net. (
        7           ; serial number
        900         ; refresh
        600         ; retry
        86400       ; expire
        3600        ) ; default TTL

;
; Zone NS records
;
@           NS      elrond.dovercorp.net.
@           NS      legolas.dovercorp.net.

;
; Zone records
;
105         PTR     legolas.dovercorp.net.
108         PTR     arwen.dovercorp.net.

```

3.168.192.in-addr.arpa.dns (on Legolas secondary DNS server)

```

;
; Database file 3.168.192.in-addr.arpa.dns for 3.168.192.in-addr.arpa zone.
; Zone version: 8
;
@           IN SOA elrond.dovercorp.net. hostmaster.dovercorp.net. (
        8           ; serial number
        900         ; refresh
        600         ; retry
        86400       ; expire
        3600        ) ; default TTL

;
; Zone NS records
;
@           NS      elrond.dovercorp.net.
@           NS      legolas.dovercorp.net.

;
; Zone records
;
102         PTR     saruman.dovercorp.net.
51          900     PTR     sauron.
            PTR     sauron.dovercorp.net.

```


4.30.172.in-addr.arpa.dns (on Legolas secondary DNS server)

```

;
; Database file 4.30.172.in-addr.arpa.dns for 4.30.172.in-addr.arpa zone.
;   Zone version: 25
;
@                               IN   SOA  elrond.dovercorp.net.
hostmaster.dovercorp.net. (
                                25      ; serial number
                                900     ; refresh
                                600     ; retry
                                86400   ; expire
                                3600    ) ; default TTL
;
; Zone NS records
;
@                               NS  elrond.dovercorp.net.
@                               NS  legolas.dovercorp.net.
;
; Zone records
;
1                               PTR   lab-router.dovercorp.net.
10                              PTR   snickers.dovercorp.net.
110                             PTR   samwise.dovercorp.net.
50                               900   PTR   frodo.dovercorp.net.

```

Successful pings by name of a Shire client from a Mordor client.

```
C:\Documents and Settings\Administrator>ipconfig /all
```

```
Windows IP Configuration
```

```
Host Name . . . . . : sauron
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Dovercorp.net
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : Dovercorp.net
Description . . . . . : Intel 21140-Based PCI Fast Ethernet Adapter (Generic)
Physical Address. . . . . : 00-03-FF-86-8E-68
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.3.51
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.3.105
DHCP Server . . . . . : 172.30.4.106
DNS Servers . . . . . : 192.168.3.105
Lease Obtained. . . . . : Wednesday, April 19, 2006 10:35:18 AM
Lease Expires . . . . . : Thursday, April 27, 2006 10:35:18 AM
```

```
C:\Documents and Settings\Administrator>
```

```
C:\Documents and Settings\Administrator>hostname
sauron
```

```
C:\Documents and Settings\Administrator>ping frodo
```

```
Pinging frodo.Dovercorp.net [172.30.4.50] with 32 bytes of data:
```

```
Reply from 172.30.4.50: bytes=32 time=143ms TTL=126
Reply from 172.30.4.50: bytes=32 time=4ms TTL=126
Reply from 172.30.4.50: bytes=32 time=4ms TTL=126
Reply from 172.30.4.50: bytes=32 time=4ms TTL=126
```

```
Ping statistics for 172.30.4.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 143ms, Average = 38ms
```

```
C:\Documents and Settings\Administrator>
```

Lessons Learned

Never take a Microsoft error message at face value! When attempting to authorize the DHCP server I got stuck at a misleading error message saying “The DHCP server could not contact Active Directory”. The TCP/IP network DNS setting on Elrond was configured for Snickers so it didn’t seem possible that it was not able to find the Domain Controller. I was expecting to get a dialog box asking for a domain administrators credentials like you get when you add a computer to a domain or try to access a restricted file server. The work around was to log again, this time as a domain administrator (Gandalf). A more accurate error message would be “current operation can only be performed by a domain administrator”.

I continued expanding my virtual MiddleEarth to do this lab. This lab is made up of virtual machines using MS Virtual Server 2005 R2. I increased RAM size on the physical host server to 2 GB to handle the Windows 2003 server VMs. They require more memory than the minimal Linux VMs used for CIS 192. Frodo, Elrond, Legolas and Sauron are all Windows 2003 Standard Edition systems. I also had to create Snickers as the virtual Domain Controller for a real domain environment. I could operate the VMs without problem directly on the physical host machine. However, when using a remote desktop connection to the physical host machine it was necessary to add the special Virtual Machine Additions. Without the VM Additions it was extremely difficult to control the mouse over the remote connection.

Original Lab with notes

Text from Jim Griffin's original lab document in gray

Text added by student in black

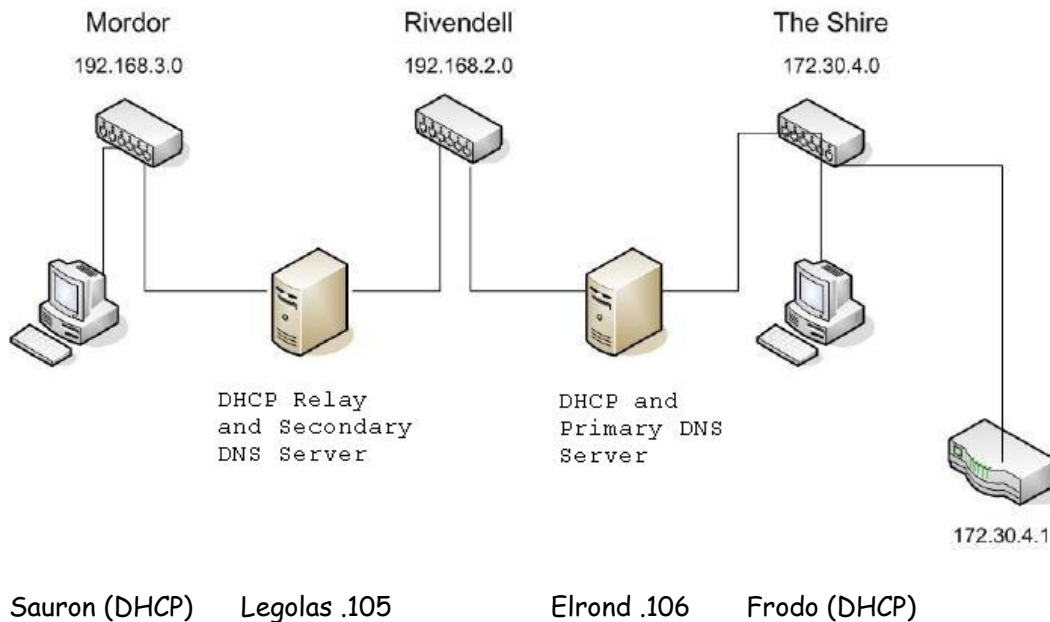
Lab 3: DHCP and the Domain Name System

The purpose of this lab is to configure a DHCP server in a domain environment that will supply IP information to two different subnets with client computers.

You will include default gateways, a static route, Domain names and the DNS servers in the DHCP options.

You will also configure a DNS primary and secondary server to handle hostname resolution. Read through the entire lab before proceeding with the individual steps so that you know what the big picture is.

Lab 3



Procedure

Part I

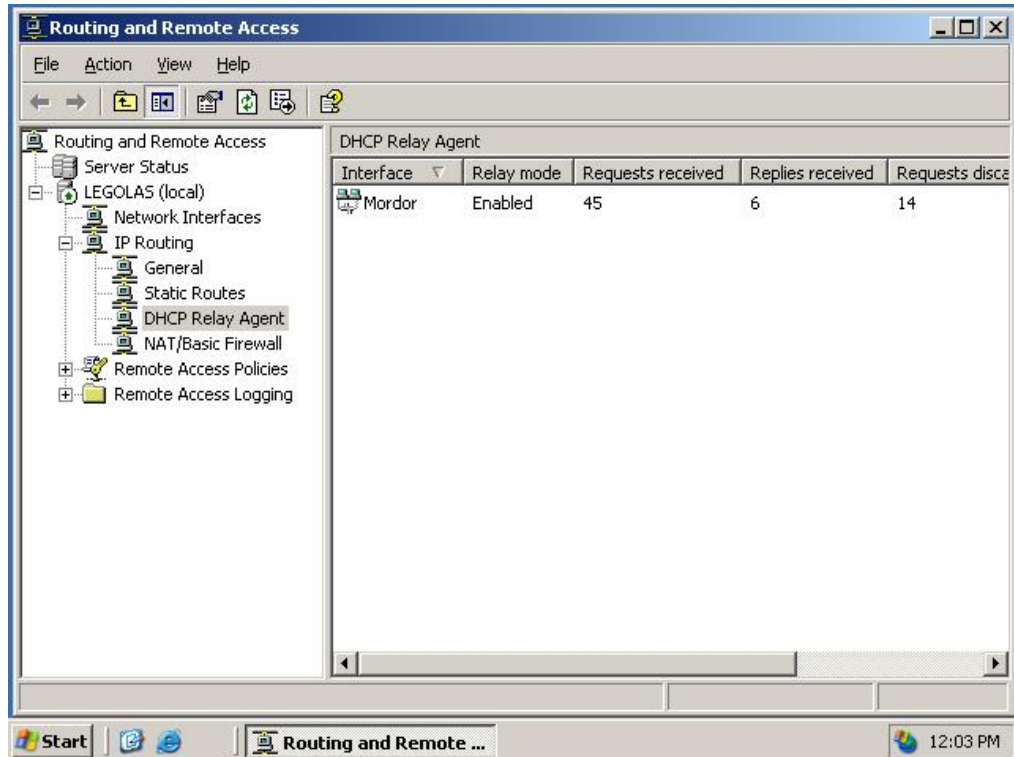
Configure two routers to route packets between Mordor and the Shire. The Routers will have their usual static IP addresses, the Shire and Mordor machines will be the DHCP clients.

1. Configure Elrond or Celebrian to route packets between Rivendell and the Shire. The default route should be set to 172.30.4.1 **using Elrond**
A static route will need to be set to the Mordor/Rivendell router configured in the steps below. **route add 192.168.3.0 mask 255.255.255.0 192.168.2.105**
2. Configure Arwen or Legolas to route packets between Mordor and Rivendell. The default route should be set to the Rivendell/Shire router above.
3. For the Shire computer to communicate with the Mordor client, it will need a static route configured for packets destined for 192.168.3.0. You will configure this as a DHCP scope option. **using Frodo and Sauron**
4. Be aware that the Shire XP Client may have a firewall turned on.

Part II

Install and Authorize DHCP on the Rivendell-Shire router, and configure two scopes for the clients in the Shire and Mordor.

1. Make sure there are no DHCP servers active in Rivendell.
2. Your Rivendell/Shire router will be the DHCP server and the primary DNS server. The Rivendell/Shire router must join the Dovercorp.net domain. (Recall that you have an account in this domain. The Gandalf (Mithrandi1) account has Domain Admin rights.)
3. Install the DHCP package from Windows components of the **Add/Remove Programs** applet.
Note: You may need a Distribution folder - look for a Source folder on the D: drive. note, Virtual Server lets you mount a ISO image of a Windows 2003 SE CD as just another drive.
4. Authorize the DHCP server using it's static IP address. This only worked if you were logged in as Gandalf (a domain administrator). If not you got a totally misleading error message saying "The DHCP server could not contact Active Directory"
5. Activate two scopes, one for Mordor: 192.168.3.50 to 192.168.3.99 and one for the Shire: 172.30.4.50 to 172.30.4.99 also changed /16 to /24
6. Configure scope options to allocate the appropriate default routes to clients on these subnets. The Shire clients should obtain a DNS server option pointing to the Primary DNS server; the Mordor clients' DNS server should be the Secondary DNS Server. Shire: GW=172.30.4.1, DNS=172.30.4.106 Mordor: GW=192.168.3.105, DNS=192.168.3.105
7. In the Shire scope, set Scope Option Classless Routing Table (the last scope option in the list) to the static route needed to send packets to the 192.168.0.0 networks. 192.168.3.0 255.255.255.0 172.30.4.106
8. Add a Server Option that will apply to both scopes. That Server Option is #15 - Domain Name.
The Domain name is: **Dovercorp.net**
9. Log in to the Mordor-Rivendell router and add the DHCP Relay Agent routing protocol.
Enable just the Mordor interfaces of the Relay Agent, keeping the default configuration values.
Using the Relay Agent Properties dialog box, assign the IP address of the DHCP server.

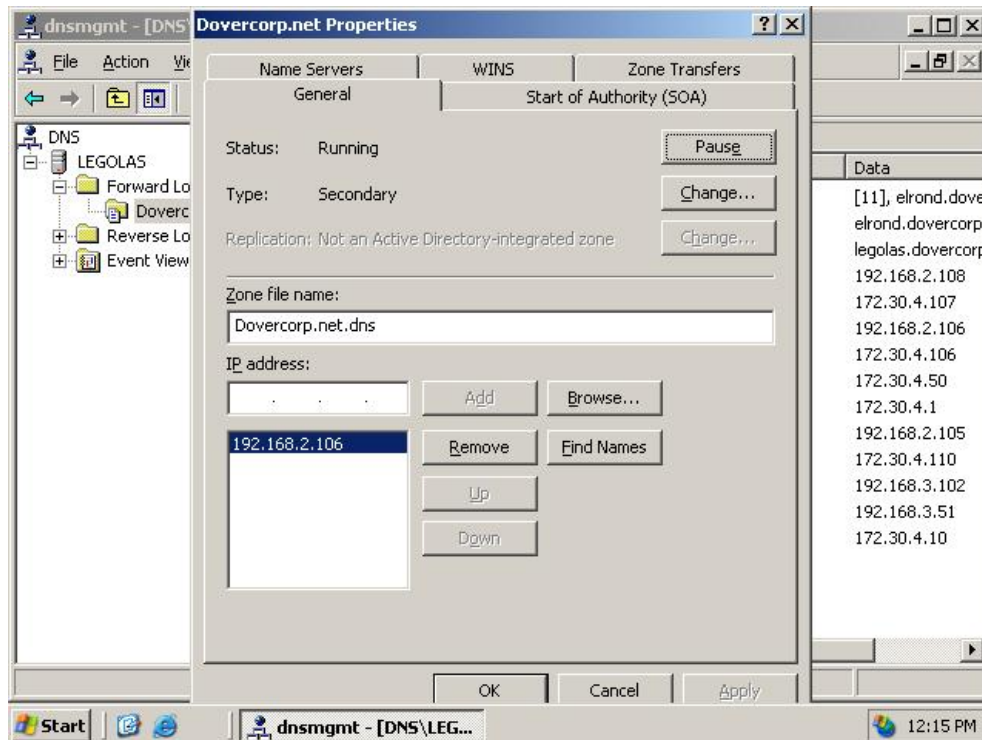


10. Verify that the Mordor client and a Shire client get their network identities from the DHCP server. Do this by setting their network interface to automatic.

Part III

Note that even though the Mordor client computer can now ping the shire computer, you must use the IP addresses of the computers, because no name resolution is being done. In Network Places, computers are aware only of the other computers on the local subnet. In this final procedure, you will install and configure a DNS server that will resolve names for all three networks: Shire, Rivendell and Mordor.

1. Log into the Rivendell-Shire computer and install DNS from the Windows Components of **Add/Remove Programs**.
2. Configure both forward and reverse lookup zone files for the Dovercorp.net domain.
Note: Since you have addresses from three different subnets, you will need three reverse lookup zone files - one for each subnet.
3. Add A and Ptr records for all the machines in the lab and for Snickers (172.30.4.10).
4. Log into the Rivendell-Mordor computer and install DNS.
5. Configure this server as a Secondary server with the Primary server as the Master.



6. Don't forget to allow the Secondary server to receive a zone transfer from the Primary server.
(hint: look in the zone properties Name Server tab of the Primary DNS server.)
7. You should now be able to ping all machines on your network by name.

Results

I want to see three files for this lab:

- The audit log for the DHCP Server: `%SystemRoot%\system32\dhcp\DhcpSrv-DDD.log` **see results section above**
- The DNS database secondary zone file that came from the zone transfer. **see results section above**
- Successful pings by name of a Shire client from a Mordor client. **see results section above**

To clean up for this lab:

1. Unauthorize and uninstall the DHCP server package from the Shire machine.
2. Uninstall the DNS package
3. Disable routing from the Rivendell-Shire and the Rivendell-Mordor routers.

Grading Rubric

20 Points possible

5 points for:

Properly authorized and configured DHCP server

5 points for:

Properly configured DHCP Relay agent

5 points for:

A Primary DNS server database with A and PTR records for clients from both subnets.

5 points for:

A Secondary DNS server database a successful zone transfer of the Primary server's zone file.

CIS 196 - Lab 4: Remote Access – Dial-up

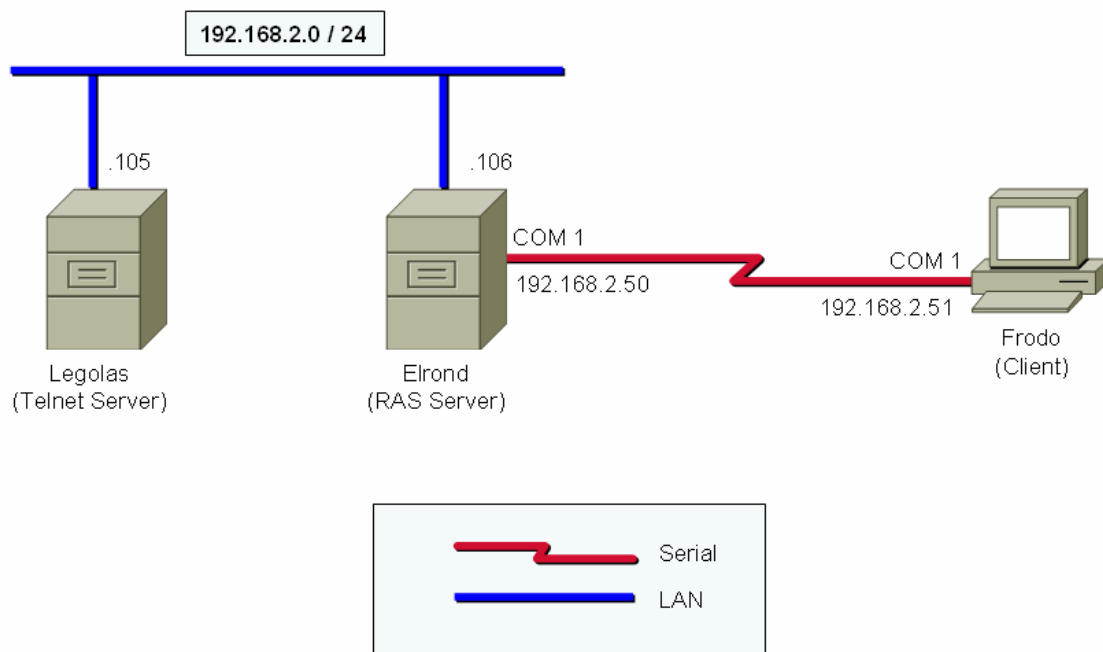
Rich Simms

May 22, 2006

Objective

The purpose of this lab is to connect a standalone computer (Frodo) to a LAN using a serial connection with PPP. The serial connection gets established using a null modem cable connecting the COM port between Frodo and the LAN RAS server (Elrond). Once the connection is made the client will connect to a third server (Legolas) using Telnet.

Layout



Results

The output of the **ipconfig** command for both the client and the server, before and after the connection.

RAS Server (Elrond)

Before	<pre> C:\Documents and Settings\Administrator>ipconfig /all Windows IP Configuration Host Name : elrond Primary Dns Suffix : Node Type : Unknown IP Routing Enabled. : No WINS Proxy Enabled. : No Ethernet adapter Rivendell: Connection-specific DNS Suffix . : Description : Intel 21140-Based PCI Fast Ethernet Adapter (Generic) Physical Address. : 00-03-FF-9A-8E-68 DHCP Enabled. : No IP Address. : 192.168.2.106 Subnet Mask : 255.255.255.0 Default Gateway : </pre>
After	<pre> C:\Documents and Settings\Administrator>ipconfig /all Windows IP Configuration Host Name : elrond Primary Dns Suffix : Node Type : Unknown IP Routing Enabled. : Yes WINS Proxy Enabled. : Yes PPP adapter RAS Server (Dial In) Interface: Connection-specific DNS Suffix . : Description : WAN (PPP/SLIP) Interface Physical Address. : 00-53-45-00-00-00 DHCP Enabled. : No IP Address. : 192.168.2.50 Subnet Mask : 255.255.255.255 Default Gateway : Ethernet adapter Rivendell: Connection-specific DNS Suffix . : Description : Intel 21140-Based PCI Fast Ethernet Adapter (Generic) Physical Address. : 00-03-FF-9A-8E-68 DHCP Enabled. : No IP Address. : 192.168.2.106 Subnet Mask : 255.255.255.0 Default Gateway : </pre>

Client (Frodo)

Before	<pre> C:\Documents and Settings\Administrator>ipconfig /all Windows IP Configuration C:\Documents and Settings\Administrator> </pre>
After	<pre> C:\Documents and Settings\Administrator>ipconfig /all Windows IP Configuration Host Name : frodo Primary Dns Suffix : Node Type : Unknown IP Routing Enabled. : No WINS Proxy Enabled. : No PPP adapter Elrond: Connection-specific DNS Suffix . : Description : WAN (PPP/SLIP) Interface Physical Address. : 00-53-45-00-00-00 DHCP Enabled. : No IP Address. : 192.168.2.51 Subnet Mask : 255.255.255.255 Default Gateway : 192.168.2.51 C:\Documents and Settings\Administrator> </pre>

Telnet session (from Frodo to Legolas)

Legolas	<pre> Welcome to Microsoft Telnet Client Escape Character is 'CTRL+]' You are about to send your password information to a remote computer in Internet zone. This might not be safe. Do you want to send anyway(y/n): *===== Welcome to Microsoft Telnet Server. *===== C:\Documents and Settings\Administrator>hostname LEGOLAS C:\Documents and Settings\Administrator>ping elrond Pinging elrond [192.168.2.50] with 32 bytes of data: Reply from 192.168.2.50: bytes=32 time=10ms TTL=128 Reply from 192.168.2.50: bytes=32 time<1ms TTL=128 Reply from 192.168.2.50: bytes=32 time=1ms TTL=128 Reply from 192.168.2.50: bytes=32 time=1ms TTL=128 Ping statistics for 192.168.2.50: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 3ms C:\Documents and Settings\Administrator> C:\Documents and Settings\Administrator>ping 192.168.2.51 Pinging 192.168.2.51 with 32 bytes of data: Reply from 192.168.2.51: bytes=32 time=19ms TTL=127 Reply from 192.168.2.51: bytes=32 time=6ms TTL=127 Reply from 192.168.2.51: bytes=32 time=5ms TTL=127 Reply from 192.168.2.51: bytes=32 time=6ms TTL=127 </pre>
---------	--

```

Ping statistics for 192.168.2.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 19ms, Average = 9ms

C:\Documents and Settings\Administrator>ping frodo
Ping request could not find host frodo. Please check the name and try
again.

C:\Documents and Settings\Administrator>nbtstat -c

Mordor:
Node IpAddress: [192.168.3.105] Scope Id: []

    No names in cache

Rivendell:
Node IpAddress: [192.168.2.105] Scope Id: []

NetBIOS Remote Cache Name Table

    Name                Type                Host Address        Life [sec]
    -----
    ELROND                <00> UNIQUE            192.168.2.50         240
    FRODO                 <20> UNIQUE            192.168.2.51         192

C:\Documents and Settings\Administrator>

```

Lessons Learned

It was interesting to compare this lab to the CIS 192 PPP lab. Microsoft has made it quite simple to quickly set up a PPP connection for providing remote access to a LAN. This lab took a lot less time to do because of it.

The “enable broadcast name resolution” option on the Elrond RAS configuration did not perform as expected. The remote computer Frodo could not access Legolas by name using NetBIOS name resolution. Jim mentioned this in class as apparently it happened to others doing this lab. At least the behavior is consistent. In the last section below there are some Ethereal captures showing the failed NetBIOS name request for Legolas going as far as Elrond but no further.

I did this lab on my virtual MiddleEarth lab using Virtual Server 2005 R2. At first I didn’t think it would be possible because of the need for a serial connection. However, after a little research on the Microsoft TechNet web site I found the following information which shows how to connect a virtual null modem cable between two virtual COM ports:

Select this option to connect the virtual serial port to a Windows named pipe on the host operating system or between virtual machines on the same virtual network. A named pipe is a portion of memory that can be used by one process to pass information to a second local process, so that the output of one is the input of the other. An example of a local named pipe path could be \\.\pipe\my pipe name.

Named pipes can be used to create a virtual null modem cable between two virtual machines, or between a virtual machine and a debugging program on the host operating system that supports the use of named pipes. By connecting two virtual serial ports to the same named pipe, you can create a virtual null modem

cable connection. Named pipes are useful for debugging or for any program that requires a null modem connection.

http://www.microsoft.com/technet/prodtechnol/virtualserver/2005/proddocs/vs_operate_using_config_add_RemCOM.msp?mfr=true

Other lessons learned are the seemingly strange PPP IP network established. For Frodo, the subnet mask is 255.255.255.255 which implies no host bits. It seems this is more of a genmask specifying a specific host. Frodo's default gateway is also itself which is strange. The following is the routing table on Frodo after the PPP connection is established:

```
C:\Documents and Settings\Administrator>route print

IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x40003 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
      0.0.0.0              0.0.0.0        192.168.2.51      192.168.2.51         1
      127.0.0.0            255.0.0.0        127.0.0.1         127.0.0.1         1
    192.168.2.50      255.255.255.255    192.168.2.51      192.168.2.51         1
    192.168.2.51      255.255.255.255    127.0.0.1         127.0.0.1        50
    192.168.2.255  255.255.255.255    192.168.2.51      192.168.2.51        50
      224.0.0.0            240.0.0.0        192.168.2.51      192.168.2.51         1
Default Gateway:          192.168.2.51
=====
Persistent Routes:
    None
```

Given the serial connection is a pipe where everything that goes in one end pops out the other end I can see how this might work. It does indeed work too!

Original Lab with notes

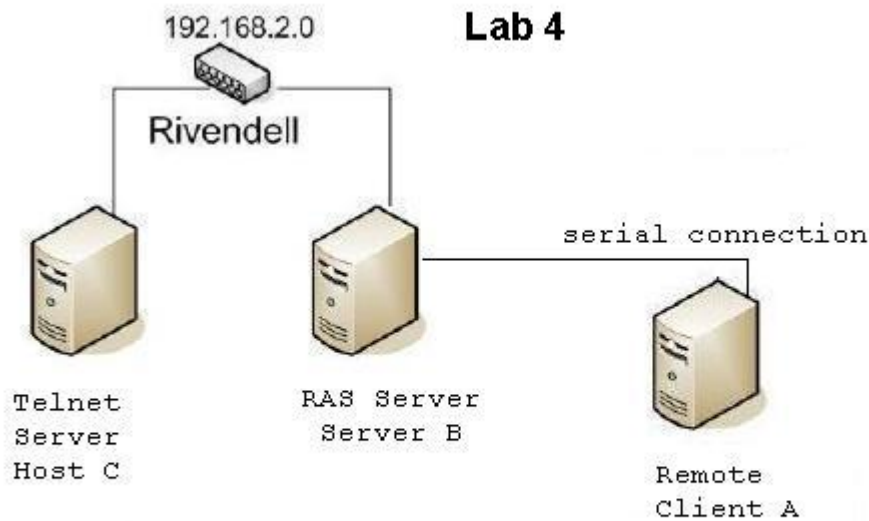
Text from Jim Griffin's original lab document in gray

Text added by student in black

Lab 4: Remote Access - Dial-up

The purpose of this lab is to connect a standalone computer to a LAN using a serial connection with PPP. Whereas the serial connection is usually established with analog modems, in this lab, you will have your choice of using modems or a serial null-modem cable connecting the serial ports of two computers. Your goal is to connect to a Rivendell Remote Access Server from an isolated client and telnet to one of the other hosts on the Rivendell LAN through the RAS server. In the following discussion, Client A will refer to the isolated client, Server B will refer to the computer acting as the RAS server, and

Host C will refer to one of the other computers on the 192.168.2.0 LAN.



Background

PPP has replaced SLIP as the preferred method for establishing serial connections between computers that emulate a network connection. Operating at the network interface layer of the TCP/IP stack, PPP relies on an external component for establishing the serial link and then manages that connection to act as an IP connection so that network applications will work transparently across the link. In this lab, the external component is the null-modem wire connecting the two serial ports; more commonly, it would be two modems connecting through a PSTN. Once a connection is established and a PPP interface built, Windows Server manages the connection allowing connectivity between the client and the LAN.

The snapins we will be using for this lab are:

- *Phone and Modem Options applet*
- *New Network Connection Wizard*
- *Computer Management console*
- *Routing and Remote Access (RRAS)*

You will also need to check out from the Lab Assistant on duty the serial null-modem cable, (or two modems), used to connect the client and server machines. Connect Client A with Server B using the null-modem cable plugged into the serial (COM 1) port of each computer, and disconnect the network cable from the computer that will be the client.

Read the instructions for each Part before doing them; that way you will know what is coming. Note that although you will be using three machines, you don't need the 172.30.4.0 network.

Procedure

Part I

Configure the RAS Server for dial-up connections

1. After you have connected Client A with Server B with the cable, boot up Server B and log in as administrator. **A=Frodo, b=Elrond**
2. Save a copy of the output of the `ipconfig /all` command to document your "before" condition.

```
C:\Documents and Settings\Administrator>ipconfig /all
```

```
Windows IP Configuration
```

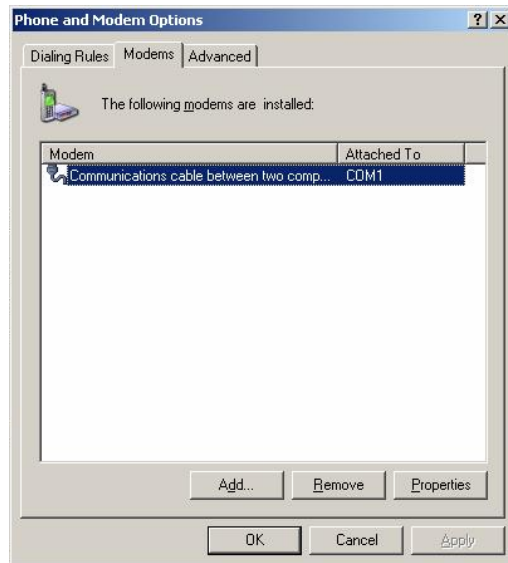
```
Host Name . . . . . : elrond
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

```
Ethernet adapter Rivendell:
```

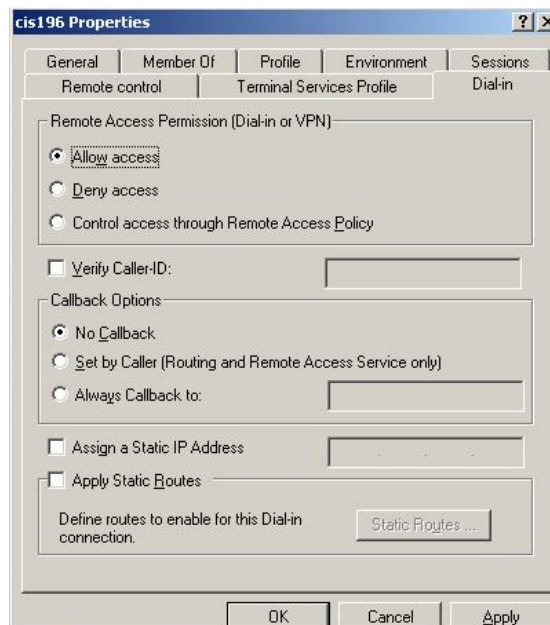
```
Connection-specific DNS Suffix . :
Description . . . . . : Intel 21140-Based PCI Fast Ethernet Adapter (Generic)
Physical Address. . . . . : 00-03-FF-9A-8E-68
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.2.106
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

```
C:\Documents and Settings\Administrator>
```

3. Use the *Control Panel / Phone and Modem Options* applet to configure the communication link between two serial ports:
 - If asked, specify the Area code as 831
 - Rather than let Windows try to detect a nonexistent modem, choose the "Communication cable between two computers" from the modem models list.
 - Choose COM1 as the selected port.

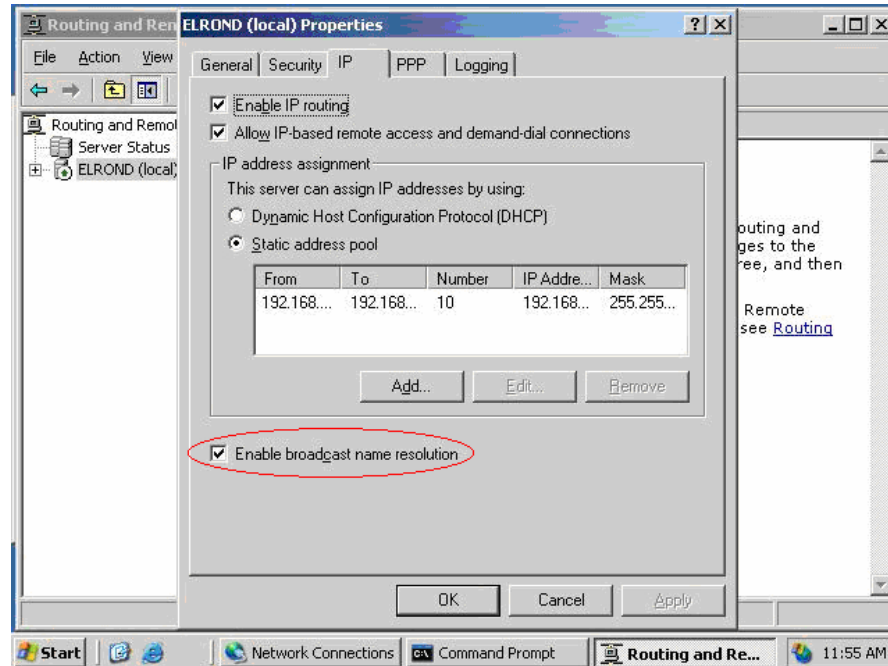


4. Use the *Computer Management* console to create a new user account for the remote client to log into:
 - Select a name and password of your choosing for the account
cis196/cis196
 - Uncheck the box that requires the user to change their password at the first login.
 - When the account is created, edit the properties of that user and change the *Dial-in* permission to "Allow access".



5. Use the RRAS snapin to configure Remote Dial-up Access:
 - Select the Rivendell interface for your remote access clients

- Assign IP addresses from a statically defined list of 10 addresses starting with 192.168.2.50.
Note: there is no DHCP server on the Rivendell LAN
- Do not attempt to work with a RADIUS server



Note the "Enable broadcast name resolution" is checked. See more discussion on this option later.

Part II

Bring up another Rivendell host and enable the telnet service

1. Boot up another Rivendell computer as Host C **C=Legolas**
2. Enable and start the **Telnet** service using the *Administrative Tools / Services* menu:
 - Double-click the Telnet service in the alphabetized list of services.
 - Change the state from *Disabled* to *Manual*, applying the changes
 - Start the service.

Part III

Bring up the client and configure it to "dial" a connection..

1. On Client A, disable the network interfaces that may be configured. We want a stand-alone machine here.
2. Run the ipconfig command and save the output to a file showing that you have no network interfaces

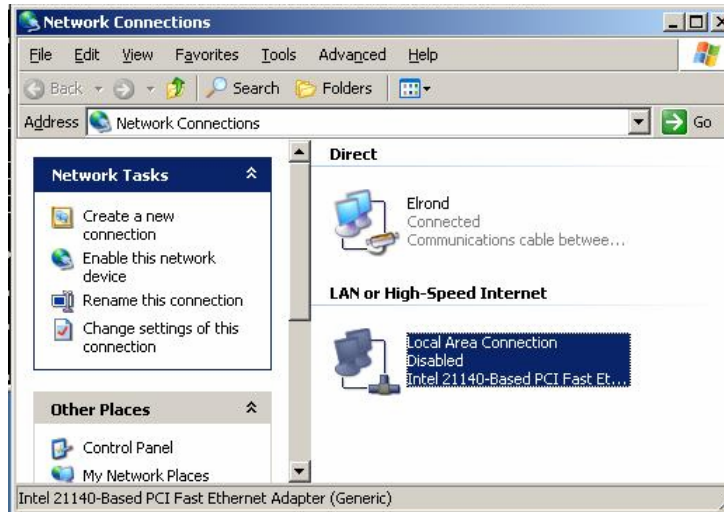
```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
C:\Documents and Settings\Administrator>
```

3. Configure the Modem as a Communication wire between two serial ports in the same way as you did for the server.
4. Run the "New Connection Wizard" from the *Control Panel / Network Connections* menu:
 - o Setup an Advanced Connection by connecting directly to another computer as a guest.
 - o Use the name of your RAS server as the name of your connection interface.
 - o Make the connection available for anyone's use.
5. When presented with the login screen, login to the account you created on the server by providing the name, password and clicking on the "Connect" button. Within a few seconds you should see that you have established a point-to-point network connection with Server B by a network-connection icon in your system tray.





Part IV

Now that you have successfully established a PPP connection to the server, let's gather a few statistics and then connect to another computer in Rivendell.

1. Run `ipconfig /all` to see your PPP connection and note your IP address and your default route. The IP address should be one from your static list, and the default route should be set to yourself. What does that mean? Save the output of this command to collect for this lab as part of your "after" condition.

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : frodo
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

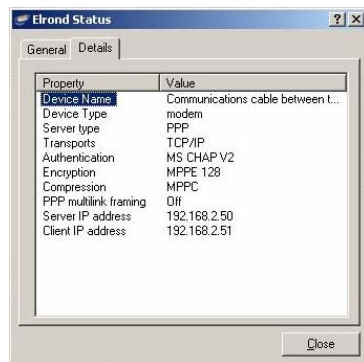
PPP adapter Elrond:

```
Connection-specific DNS Suffix . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.2.51
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 192.168.2.51
```

```
C:\Documents and Settings\Administrator>
```

2. Click on the network-connection icon in the system tray to bring up your connection status. Click on the **Details** tab and note the following:
 - o the Server's **192.168.2.50** and your IP addresses **192.168.2.51**
 - o the authentication protocol being used **MS CHAP V2**

- the encryption type **MPPE 128**
- is compression being used? **Yes, MPPC**



RFC 3078 - Microsoft Point-To-Point Encryption (MPPE) Protocol
RFC 2118 - Microsoft Point-To-Point Compression (MPPC) Protocol

3. Ping your RAS server from your client using the IP address obtained above.

```
C:\Documents and Settings\Administrator>ping 192.168.2.50
```

```
Pinging 192.168.2.50 with 32 bytes of data:
```

```
Reply from 192.168.2.50: bytes=32 time=49ms TTL=128
Reply from 192.168.2.50: bytes=32 time=5ms TTL=128
Reply from 192.168.2.50: bytes=32 time=3ms TTL=128
Reply from 192.168.2.50: bytes=32 time=3ms TTL=128
```

```
Ping statistics for 192.168.2.50:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 49ms, Average = 15ms
```

4. Ping your RAS server by name. Does it work? **Yes** What IP address was the name resolved to? **192.168.2.50**

```
C:\Documents and Settings\Administrator>ping elrond
```

```
Pinging elrond [192.168.2.50] with 32 bytes of data:
```

```
Reply from 192.168.2.50: bytes=32 time=15ms TTL=128
Reply from 192.168.2.50: bytes=32 time=3ms TTL=128
Reply from 192.168.2.50: bytes=32 time=3ms TTL=128
Reply from 192.168.2.50: bytes=32 time=3ms TTL=128
```

```
Ping statistics for 192.168.2.50:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 15ms, Average = 6ms
```

5. Ping the Host C machine using the IP address.

```
C:\Documents and Settings\Administrator>ping 192.168.2.105
```

```
Pinging 192.168.2.105 with 32 bytes of data:
```

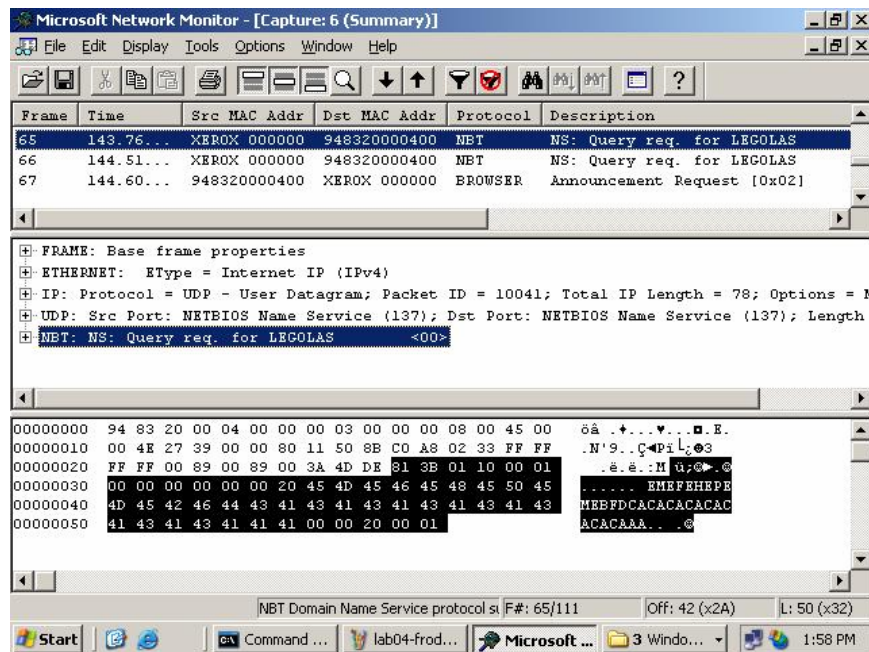
```
Reply from 192.168.2.105: bytes=32 time=33ms TTL=127
Reply from 192.168.2.105: bytes=32 time=5ms TTL=127
Reply from 192.168.2.105: bytes=32 time=4ms TTL=127
Reply from 192.168.2.105: bytes=32 time=4ms TTL=127
```

```
Ping statistics for 192.168.2.105:
```

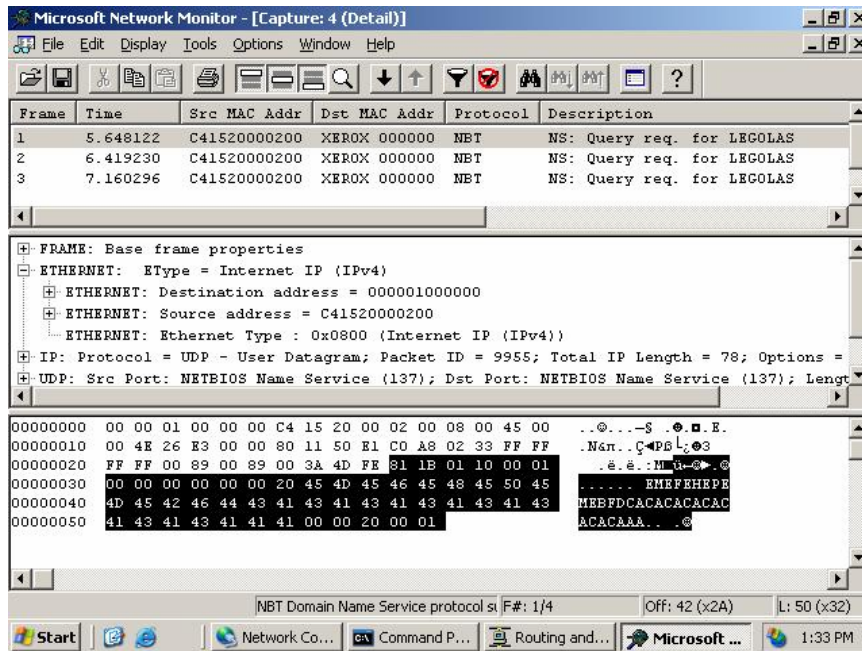
```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 33ms, Average = 11ms
```

6. Ping Host C by name. Does it work? No Why? NetBIOS requests for Legolas never make it to 192.168.2.0 network. The IP destination is 255.255.255.255 but the MAC destination is not a broadcast. This happens even when the RRAS configuration on Elrond has "enable broadcast name resolution" checked on properties IP tab.

Frodo capture of NetBIOS Legolas name request.



Elrond capture of NetBios Legolas name request.



And it stops there, the sniffer on the 192.168.2.0 network didn't record any packets from the Legolas request

```
C:\Documents and Settings\Administrator>ping legolas
Ping request could not find host legolas. Please check the name and try again.
```

7. Use the command `nbtstat -c` to view your NetBIOS cache.

```
C:\Documents and Settings\Administrator>nbtstat -c
```

Elrond:

```
Node IpAddress: [192.168.2.51] Scope Id: []
```

NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
ELROND	<00> UNIQUE	192.168.2.50	500

```
C:\Documents and Settings\Administrator>
```

8. Now let's verify that we have access to other services on the Rivendell LAN.
telnet to Host C and log in as administrator. **C=Legolas**
9. Capture the output of the following commands from the telnet session window:
 - o Enter the command `hostname`

```
C:\Documents and Settings\Administrator>hostname
LEGOLAS
```

- o Ping your RAS server by name.

```
C:\Documents and Settings\Administrator>ping elrond

Pinging elrond [192.168.2.50] with 32 bytes of data:

Reply from 192.168.2.50: bytes=32 time=10ms TTL=128
Reply from 192.168.2.50: bytes=32 time<1ms TTL=128
Reply from 192.168.2.50: bytes=32 time=1ms TTL=128
Reply from 192.168.2.50: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

- Ping your Client by IP address.

```
C:\Documents and Settings\Administrator>ping 192.168.2.51

Pinging 192.168.2.51 with 32 bytes of data:

Reply from 192.168.2.51: bytes=32 time=19ms TTL=127
Reply from 192.168.2.51: bytes=32 time=6ms TTL=127
Reply from 192.168.2.51: bytes=32 time=5ms TTL=127
Reply from 192.168.2.51: bytes=32 time=6ms TTL=127

Ping statistics for 192.168.2.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 19ms, Average = 9ms
```

10. Ping your Client by name. Does it work? No Why? NetBIOS requests are not getting through the serial connection. This is not what I expected given the "enable broadcast name resolution" is checked on Elrond.

○

```
C:\Documents and Settings\Administrator>ping frodo
Ping request could not find host frodo. Please check the name and try again.
```

11. What does `nbtstat -c` tell you?

<00> = Workstation service, <20> = File Server Service

```
C:\Documents and Settings\Administrator>nbtstat -c
```

```
Mordor:
Node IpAddress: [192.168.3.105] Scope Id: []
```

No names in cache

```
Rivendell:
Node IpAddress: [192.168.2.105] Scope Id: []
```

NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
ELROND	<00> UNIQUE	192.168.2.50	240
FRODO	<20> UNIQUE	192.168.2.51	192

12. Can your RAS Server ping your Client by name? **Yes** Why the difference?
Maybe this is the only thing that really happens with the "enable broadcast name resolution" option.

```
C:\Documents and Settings\Administrator>ping frodo
```

```
Pinging frodo [192.168.2.51] with 32 bytes of data:
```

```
Reply from 192.168.2.51: bytes=32 time=6ms TTL=128
```

```
Reply from 192.168.2.51: bytes=32 time=3ms TTL=128
```

```
Reply from 192.168.2.51: bytes=32 time=4ms TTL=128
```

```
Reply from 192.168.2.51: bytes=32 time=5ms TTL=128
```

```
Ping statistics for 192.168.2.51:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

```
C:\Documents and Settings\Administrator>nbtstat -c
```

```
Rivendell:
```

```
Node IpAddress: [192.168.2.106] Scope Id: []
```

NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
LEGOLAS	<20> UNIQUE	192.168.2.105	300

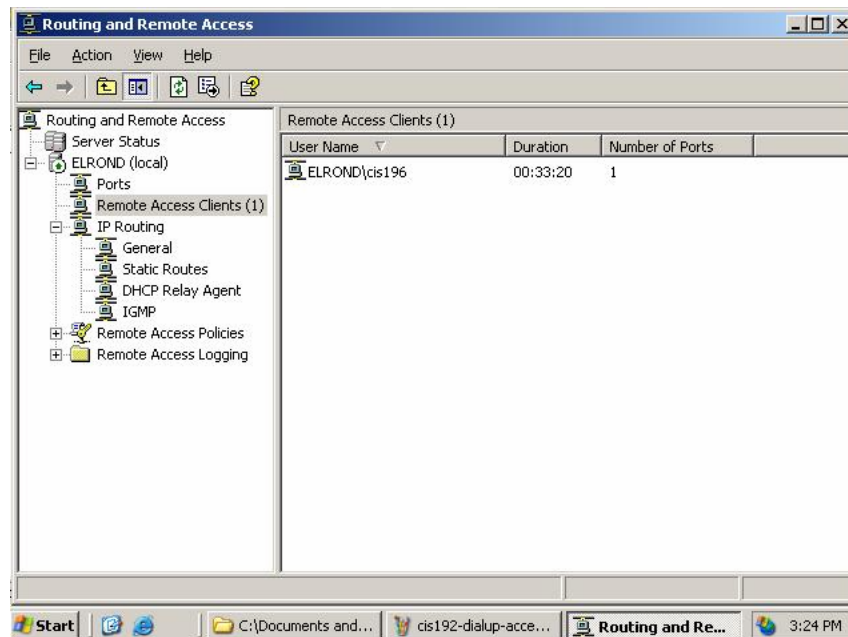
```
RAS Server (Dial In) Interface:
```

```
Node IpAddress: [192.168.2.50] Scope Id: []
```

NetBIOS Remote Cache Name Table

Name	Type	Host Address	Life [sec]
FRODO	<00> UNIQUE	192.168.2.51	592

```
C:\Documents and Settings\Administrator>
```



Results and Cleanup

To collect for this assignment, I want to see the output of the `ipconfig` command for both the client and the server, before and after the connection. **See results section above**

I also want to see the output of the telnet session with Host C **See results section above**

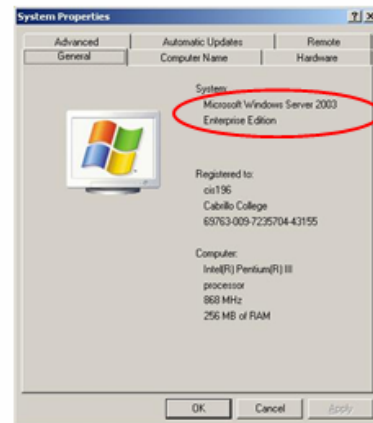
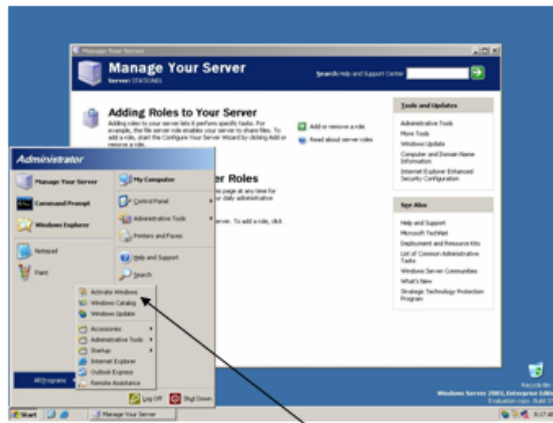
To clean up for the next user please do the following:

- Disconnect the client and remove the Network Connection
- Deconfigure the Modem configuration of both server and client
- Disable the RAS service on the Server
- Remove the account created on the RAS Server
- Disable the Telnet service on host C
- Remove the null-modem cable and return it to whomever checked it out to you.

Lesson 1 - Networking Overview

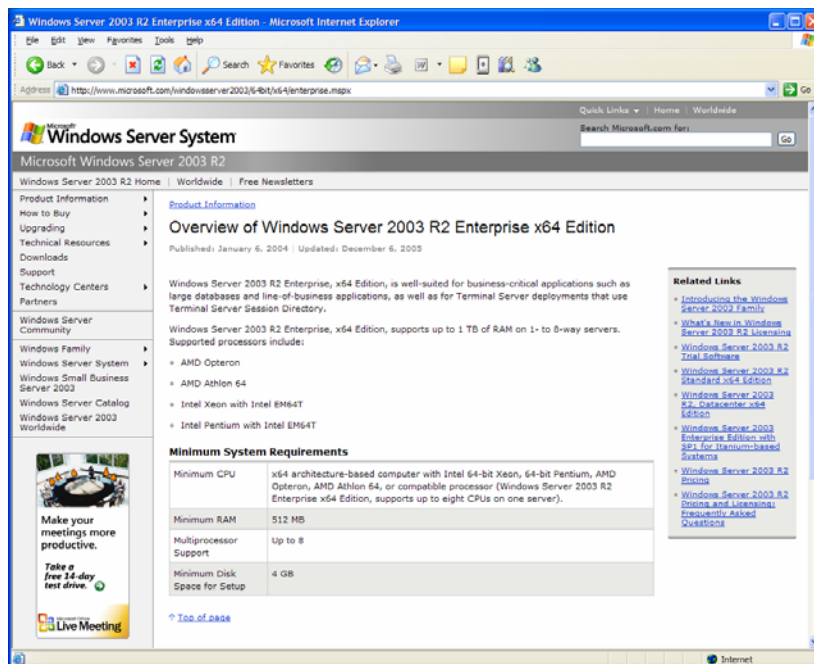
- Screenshot: *Start-Programs* menu, and the General tab of *System Properties* dialog.

C: XP	Contents of the Win 2003 EE CD have been copied to c:\source\ In XP, the command line installation of Win 2003 EE to drive D:
D: 2003 EE	<code>winnt32 /s:c:\source\i386 /tempdrive:d</code>



Note: activation required after installing

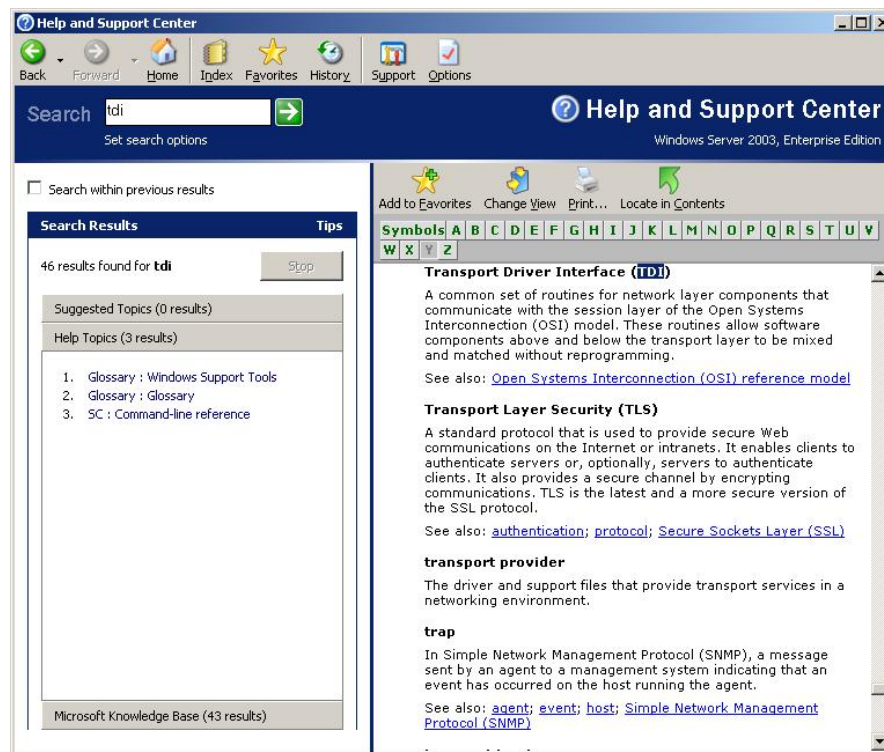
- Screenshot: Minimum system requirements of the Enterprise x64 Edition



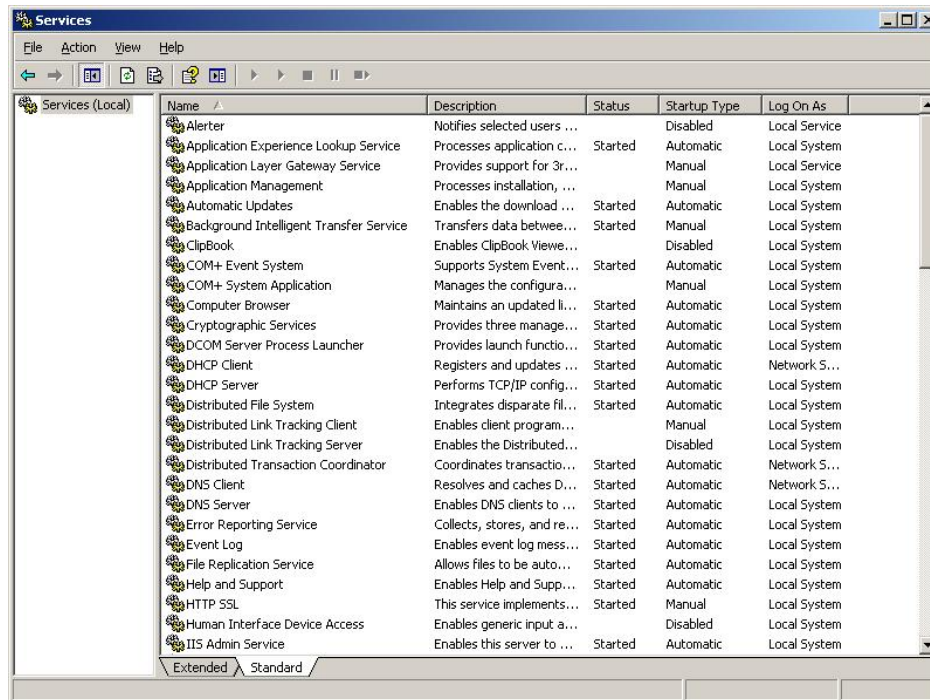
- Verify the various network protocols available for installation.
Screenshot: *Select Network Protocol* dialog box.



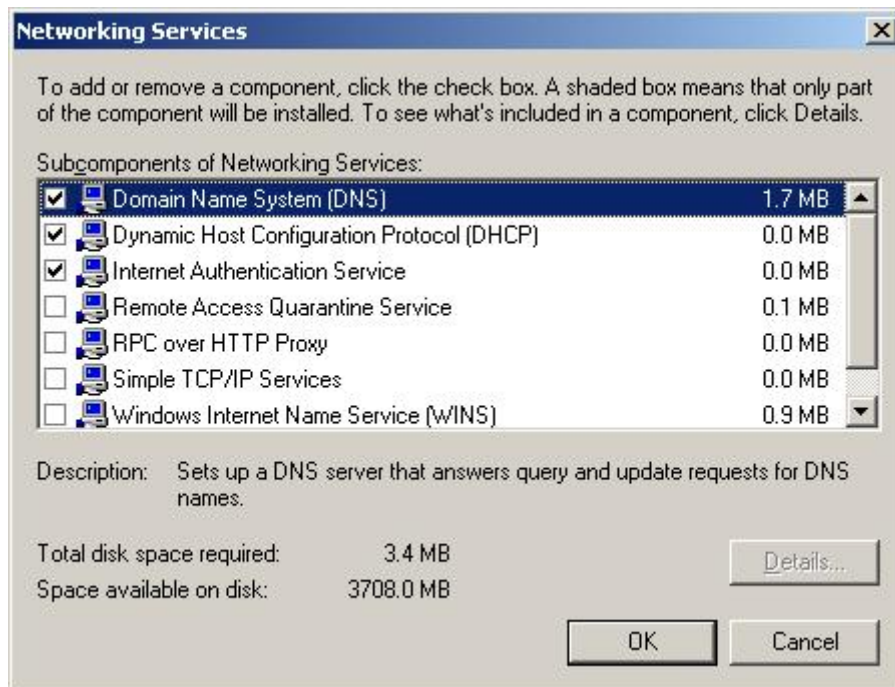
- Screenshot: *Help and Support* glossary page showing either NDIS or TDI



- View the status of services installed on the installed operating system.
Screenshot: Standard view of the *Services* dialog box



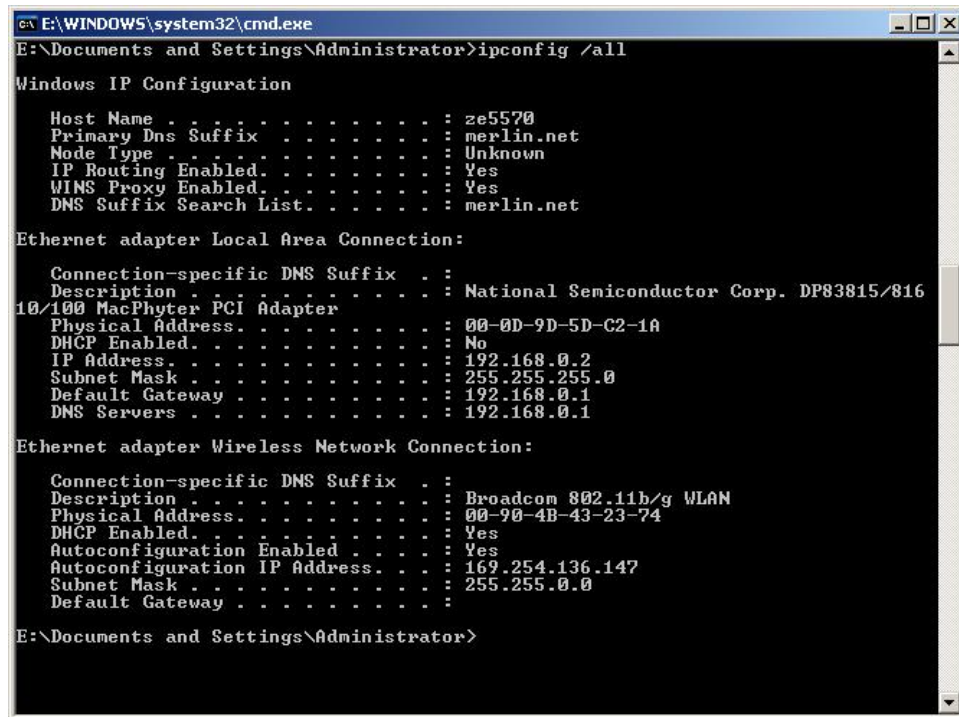
- View what networking services are available for installation.
Screenshot: *Networking Services* dialog box.



Lesson 2 - Configuring Network Protocols

- Use *ipconfig* to view IP configuration

Screenshot: output of *ipconfig /all*



```
E:\WINDOWS\system32\cmd.exe
E:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : ze5570
    Primary Dns Suffix . . . . . : merlin.net
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : Yes
    WINS Proxy Enabled. . . . . : Yes
    DNS Suffix Search List. . . . . : merlin.net

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : National Semiconductor Corp. DP83815/816
10/100 MacPhyter PCI Adapter
    Physical Address. . . . . : 00-0D-9D-5D-C2-1A
    DHCP Enabled. . . . . : No
    IP Address. . . . . : 192.168.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
    DNS Servers . . . . . : 192.168.0.1

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . : 
    Description . . . . . : Broadcom 802.11b/g WLAN
    Physical Address. . . . . : 00-90-4B-43-23-74
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IP Address. . . : 169.254.136.147
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

E:\Documents and Settings\Administrator>
```

- Finding valid hosts for a given subnet

Complete worksheet [handout](#).

Lesson 3 - TCP/IP Architecture

- **Screenshot:** Displayed capture of DNS TCP and HTTP packets

Microsoft Network Monitor - [Capture: 1 (Detail)]

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type
968	758.18...	0002B34C16CF	*BROADCAST	ARP	Request, Target IP: 172.30.1.102			
969	763.43...	LOCAL	*BROADCAST	BROWSER	Host Announcement (0x01) STATION01	STATION01	172.30.1.255	IP
970	764.32...	INTEL 427F12	*BROADCAST	BROWSER	Workgroup Announcement (0x0c) DOVERCORP	STATION01	172.30.1.255	IP
971	768.16...	LOCAL	00B064534201	DNS	0x3F08:Std Qry for www.google.com. of type ...	STATION01	207.62.187.53	IP
972	768.16...	00B064534201	LOCAL	DNS	0x3F08:Std Qry Resp. Auth. NS is www.google...	207.62.187.53	STATION01	IP
973	768.16...	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:140714...	STATION01	66.102.7.104	IP
974	768.17...	00B064534201	LOCAL	TCP	Control Bits: ...S... len: 0, seq:297015...	66.102.7.104	STATION01	IP
975	768.17...	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:140714...	STATION01	66.102.7.104	IP
976	768.17...	LOCAL	00B064534201	HTTP	GET Request from Client	STATION01	66.102.7.104	IP
977	768.18...	00B064534201	LOCAL	TCP	Control Bits: ...S... len: 0, seq:297015...	66.102.7.104	STATION01	IP
978	768.18...	00B064534201	LOCAL	TCP	Control Bits: ...S... len: 0, seq:297015...	66.102.7.104	STATION01	IP
979	768.19...	00B064534201	LOCAL	HTTP	Response to Client; HTTP/1.1; Status Code =...	66.102.7.104	STATION01	IP
980	768.19...	00B064534201	LOCAL	HTTP	Continuation Response Packet	66.102.7.104	STATION01	IP
981	768.19...	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:140714...	STATION01	66.102.7.104	IP
982	768.40...	LOCAL	00B064534201	HTTP	GET Request from Client	STATION01	66.102.7.104	IP
983	768.42...	00B064534201	LOCAL	HTTP	Response to Client; HTTP/1.1; Status Code =...	66.102.7.104	STATION01	IP
984	768.42...	00B064534201	LOCAL	HTTP	Continuation Response Packet	66.102.7.104	STATION01	IP
985	768.42...	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:140714...	STATION01	66.102.7.104	IP
986	768.42...	00B064534201	LOCAL	HTTP	Continuation Response Packet	66.102.7.104	STATION01	IP

FRAME: Base frame properties

ETHERNET: EType = Internet IP (IPv4)

IP: Protocol = UDP - User Datagram; Packet ID = 32969; Total IP Length = 224; Options = No Options

UDP: Src Port: Domain Name Server (53); Dst Port: Unknown (1026); Length = 204 (0xCC)

UDP: Source Port = Domain Name Server

UDP: Destination Port = 0x0402

UDP: Total length = 204 (0xCC)

UDP: UDP Checksum = 0x95FA

Internet Domain Name System Pack F#: 972/1600 Off: 42 (x2A) L: 196 (x4C)

Creating a display filter for DNS packets:

Microsoft Network Monitor - [Capture: 2 (Summary)]

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type
3	5.868438	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:149059...	STATION01	207.62.187.7	IP
4	5.868438	00B064534201	LOCAL	TCP	Control Bits: ...S... len: 0, seq:297431...	207.62.187.7	STATION01	IP
5	5.868438	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:149059...	STATION01	207.62.187.7	IP
6	5.868438	00B064534201	LOCAL	HTTP	GET Request from Client	STATION01	207.62.187.7	IP
7	5.868438	00B064534201	LOCAL	TCP	Control Bits: ...S... len: 0, seq:297431...	207.62.187.7	STATION01	IP
8	5.868438	LOCAL	00B064534201	HTTP	Response to Client; HTTP/1.1; Status Code =...	207.62.187.7	STATION01	IP
9	5.868438	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:149059...	STATION01	207.62.187.7	IP
10	5.878453	00B064534201	LOCAL	TCP	Control B...			IP
11	5.878453	LOCAL	00B064534201	TCP	Control B...			IP
12	5.878453	00B064534201	LOCAL	TCP	Control B...			IP
17	45.375246	LOCAL	00B064534201	DNS	0x3F08:Std Q...			IP
18	45.475390	00B064534201	LOCAL	DNS	0x3F08:Std Q...			IP
19	45.485405	LOCAL	00B064534201	TCP	Control B...			IP
20	45.565520	00B064534201	LOCAL	TCP	Control B...			IP
21	45.565520	LOCAL	00B064534201	TCP	Control B...			IP
22	45.565520	LOCAL	00B064534201	HTTP	GET Reque...			IP
23	45.825894	00B064534201	LOCAL	TCP	Control B...			IP
27	49.811625	00B064534201	LOCAL	HTTP	Response t...			IP
28	49.821640	LOCAL	00B064534201	TCP	Control B...			IP
29	49.851683	00B064534201	LOCAL	HTTP	Continuat...			IP
30	49.851683	LOCAL	00B064534201	TCP	Control B...			IP
31	49.901755	00B064534201	LOCAL	TCP	Control B...			IP
32	49.901755	LOCAL	00B064534201	TCP	Control B...			IP
33	49.901755	LOCAL	00B064534201	HTTP	GET Reque...			IP
34	49.971856	00B064534201	LOCAL	HTTP	Continuat...			IP
35	50.011913	00B064534201	LOCAL	HTTP	Continuat...			IP
36	50.011913	LOCAL	00B064534201	TCP	Control B...			IP
37	50.041957	00B064534201	LOCAL	HTTP	Continuat...			IP
38	50.041957	LOCAL	00B064534201	HTTP	GET Reque...			IP
39	50.082014	00B064534201	LOCAL	HTTP	Response t...			IP
40	50.122072	00B064534201	LOCAL	HTTP	Continuat...			IP
41	50.122072	LOCAL	00B064534201	TCP	Control B...			IP
42	50.162129	00B064534201	LOCAL	HTTP	Response t...			IP
43	50.182158	00B064534201	LOCAL	HTTP	Continuation response packet	67.100.3.196	STATION01	IP
44	50.182158	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:103630...	STATION01	67.100.3.196	IP
45	50.182158	LOCAL	00B064534201	HTTP	GET Request from Client	STATION01	67.100.3.196	IP
46	50.242245	00B064534201	LOCAL	HTTP	Continuation Response Packet	67.100.3.196	STATION01	IP
47	50.272288	00B064534201	LOCAL	HTTP	Continuation Response Packet	67.100.3.196	STATION01	IP
48	50.272288	LOCAL	00B064534201	TCP	Control Bits: ...S... len: 0, seq:177832...	67.100.3.196	STATION01	IP
49	50.312345	00B064534201	LOCAL	HTTP	Continuation Response Packet	67.100.3.196	STATION01	IP

Display Filter

UDP & TCP.Destination Port == 80 & TCP.Source Port == 80 & UDP.Source Port == 53 & UDP.Destination Port == 53

Load... Save... OK Cancel Help

TCP protocol summary F#: 3/81 Off: 34 (x22) L: 28 (x1C)

Network Monitor Capture window and summary views:

The image displays two windows from a Windows XP environment. The top window is a command prompt showing the output of the `ipconfig /all` command. The bottom window is Microsoft Network Monitor, showing a capture window and a summary view of the captured data.

Windows IP Configuration

```
E:\WINDOWS\system32\cmd.exe
E:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : ze5570
Primary Dns Suffix . . . . . : merlin.net
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : Yes
MAC Address . . . . . : 00-15-5D-00-00-00
```

Microsoft Network Monitor

Local Area Connection Capture Window (Station Stats)

% Network Utilization: 0
Frames Per Second: 0
Bytes Per Second: 0

Time Elapsed: 00:00:17.214754

Network Statistics

- # Frames: 27
- # Broadcasts: 2
- # Multicasts: 0
- # Bytes: 12312
- # Frames Dropped: 0
- Network Status: Normal

Network Address: 1
LOCAL 1
ZYXEL E1C9A8 1

Capture: 1 (Summary)

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr
1	4.005760	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 192.168.0.1		
2	4.005760	ZYXEL E1C9A8	LOCAL	ARP_RARP	ARP: Reply, Target IP: 192.168.0.2 Target H...		
3	4.005760	LOCAL	ZYXEL E1C9A8	DNS	0xF0F9:Std Qry for www.google.com. of type...	ZE5570	15
4	4.025789	ZYXEL E1C9A8	LOCAL	DNS	0xF0F9:Std Qry Resp. Auth. NS is www.google...	192.168.0.1	28
5	4.025789	LOCAL	ZYXEL E1C9A8	TCP	Control Bits:S., len: 0, seq:339922...	ZE5570	66

Network Address: 12
LOCAL 12
ZYXEL E1C9A8 15

Network Address: 0
BROADCAST 0

FRAME: Base frame properties

- ETHERNET: EType = Internet IP (IPv4)
- IP: Protocol = UDP - User Datagram; Packet ID = 10125; Total IP Length = 60; Options = No Options
- UDP: Src Port: Unknown (1029); Dst Port: Domain Name Server (53); Length = 40 (0x28)
- DNS: 0xF0F9:Std Qry for www.google.com. of type Host Addr on class INET addr.

00000000 00 A0 C5 F1 C9 A8 00 0D 9D 5D C2 1A 08 00 45 00 .4+0F...H...S.E.
00000010 00 3C 27 8D 00 00 80 11 91 D0 C0 A8 00 02 C0 A8 .<1..C...L...S.L.
00000020 00 01 04 05 00 35 00 28 FA 6E F0 F9 01 00 00 01 .0+...S...H...S...G...G
00000030 00 00 00 00 00 00 03 77 77 77 06 67 6F 67 6CWuuu@googl

Lesson 4 - Routing

- Configure a static route
Save the output of the *route print* command

```
D:\Documents and Settings\Administrator>route print

IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x30003 ...00 60 08 96 4a 63 ..... 3Com 3C905TX-based Ethernet Adapter (Generic
) #2
0x30004 ...00 02 b3 4c 15 8a ..... Intel(R) PRO/100 S Desktop Adapter
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.1.1.100       10.1.1.101       30
0.0.0.0                    0.0.0.0          10.1.1.100       192.168.1.101    30
10.1.1.0                   255.255.255.0    10.1.1.101       10.1.1.101       30
10.1.1.101                 255.255.255.255  127.0.0.1        127.0.0.1        30
10.255.255.255             255.255.255.255  10.1.1.101       10.1.1.101       30
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
192.168.1.0                255.255.255.0    192.168.1.101    192.168.1.101    30
192.168.1.101              255.255.255.255  127.0.0.1        127.0.0.1        30
192.168.1.255              255.255.255.255  192.168.1.101    192.168.1.101    30
224.0.0.0                  240.0.0.0        10.1.1.101       10.1.1.101       30
224.0.0.0                  240.0.0.0        192.168.1.101    192.168.1.101    30
255.255.255.255            255.255.255.255  10.1.1.101       10.1.1.101       1
255.255.255.255            255.255.255.255  192.168.1.101    192.168.1.101    1
Default Gateway:          10.1.1.100
=====
Persistent Routes:
None

D:\Documents and Settings\Administrator>
```


Lesson 5 - DHCP

- Configuring a DHCP Relay
Save the output of *netsh dhcp show all* for the DHCP server you configure in class.

```
netsh dhcp server>show all

MIBCounts:
    Discovers = 10.
    Offers = 5.
    Requests = 7.
    Acks = 2.
    Naks = 0.
    Declines = 0.
    Releases = 0.
    ServerStartTime = Thursday, March 30, 2006 8:24:44 AM
    Scopes = 1.
    Subnet = 192.168.0.0.
        No. of Addresses in use = 5.
        No. of free Addresses = 0.
        No. of pending offers = 3.

Server Database Properties :

    DatabaseName           = dhcp.mdb
    DatabasePath            = E:\WINDOWS\System32\dhcp
    DatabaseBackupPath     = E:\WINDOWS\System32\dhcp\backup
    DatabaseBackupInterval = 60 mins.
    DatabaseLoggingFlag    = 1
    DatabaseRestoreFlag    = 0
    DatabaseCleanupInterval = 60 mins.

Server Status:
    Server Attrib - Rogue Authorization Succeeded :TRUE
    Server Attrib - Dynamic BootP Support Enabled :TRUE
    Server Attrib - DHCP Server Part Of DS       :TRUE
    Server Attrib - DHCP Server Bindings Aware   :TRUE
    Server Attrib - Administrative Rights        :TRUE
netsh dhcp server>show audit log

The Audit log setting for the current server :
    Audit File Path       : E:\WINDOWS\System32\dhcp
    Disk Check Interval   : 50 Min
    Maximum Log File Size : 70 MB
    Minimum Space on Disk : 20 MB

Command completed successfully.

netsh dhcp server>
```

Lesson 6 - Name Resolution

- Viewing and purging the DNS cache
Save the output of: *nbtstat -c* and *ipconfig /displaydns*

```
E:\WINDOWS\system32\cmd.exe
E:\Documents and Settings\Administrator>nbtstat -c

Local Area Connection:
Node IpAddress: [192.168.0.2] Scope Id: []

          NetBIOS Remote Cache Name Table

      Name                Type          Host Address      Life [sec]
-----
HP9795C      <20>    UNIQUE        192.168.0.23      562
HPA250N      <20>    UNIQUE        192.168.0.21      500

Wireless Network Connection:
Node IpAddress: [169.254.136.147] Scope Id: []

      No names in cache

E:\Documents and Settings\Administrator>_
```

```
E:\Documents and Settings\Administrator>ipconfig /displaydns
```

Windows IP Configuration

1.0.0.127.in-addr.arpa

```
-----
Record Name . . . . . : 1.0.0.127.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 600875
Data Length . . . . . : 4
Section . . . . . : Answer
PTR Record . . . . . : localhost
```

hphqglobal.112.2o7.net

```
-----
Record Name . . . . . : hphqglobal.112.2o7.net
Record Type . . . . . : 1
Time To Live . . . . . : 1612
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 216.52.17.236
```

```
Record Name . . . . . : hphqglobal.112.2o7.net
Record Type . . . . . : 1
Time To Live . . . . . : 1612
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 216.52.17.116
```

```
Record Name . . . . . : hphqglobal.112.2o7.net
Record Type . . . . . : 1
Time To Live . . . . . : 1612
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 216.52.17.206
```

```
Record Name . . . . . : hphqglobal.112.2o7.net
```

Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Answer
A (Host) Record . . . : 216.52.17.213

Record Name : hphgglobal.112.2o7.net
Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Answer
A (Host) Record . . . : 216.52.17.216

Record Name : ns1.omniture.com
Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Additional
A (Host) Record . . . : 216.52.17.51

Record Name : ns2.omniture.com
Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Additional
A (Host) Record . . . : 216.52.17.52

net-server

Record Name : net-server.merlin.net
Record Type : 1
Time To Live : 77477
Data Length : 4
Section : Answer
A (Host) Record . . . : 69.45.6.90

Record Name : udns1.ultradns.net
Record Type : 1
Time To Live : 77477
Data Length : 4
Section : Additional
A (Host) Record . . . : 204.69.234.1

Record Name : udns2.ultradns.net
Record Type : 1
Time To Live : 77477
Data Length : 4
Section : Additional
A (Host) Record . . . : 204.74.101.1

_ldap._tcp.default-first-site-name._sites.dc._msdcs.merlin.net

No records of type SRV

ns1.omniture.com

Record Name : ns1.omniture.com
Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Answer
A (Host) Record . . . : 216.52.17.51

udns2.ultradns.net

Record Name : udns2.ultradns.net
Record Type : 1
Time To Live : 77479
Data Length : 4
Section : Answer
A (Host) Record . . . : 204.74.101.1

ns2.omniture.com

Record Name : ns2.omniture.com
Record Type : 1
Time To Live : 1612
Data Length : 4
Section : Answer
A (Host) Record . . . : 216.52.17.52

udns1.ultradns.net

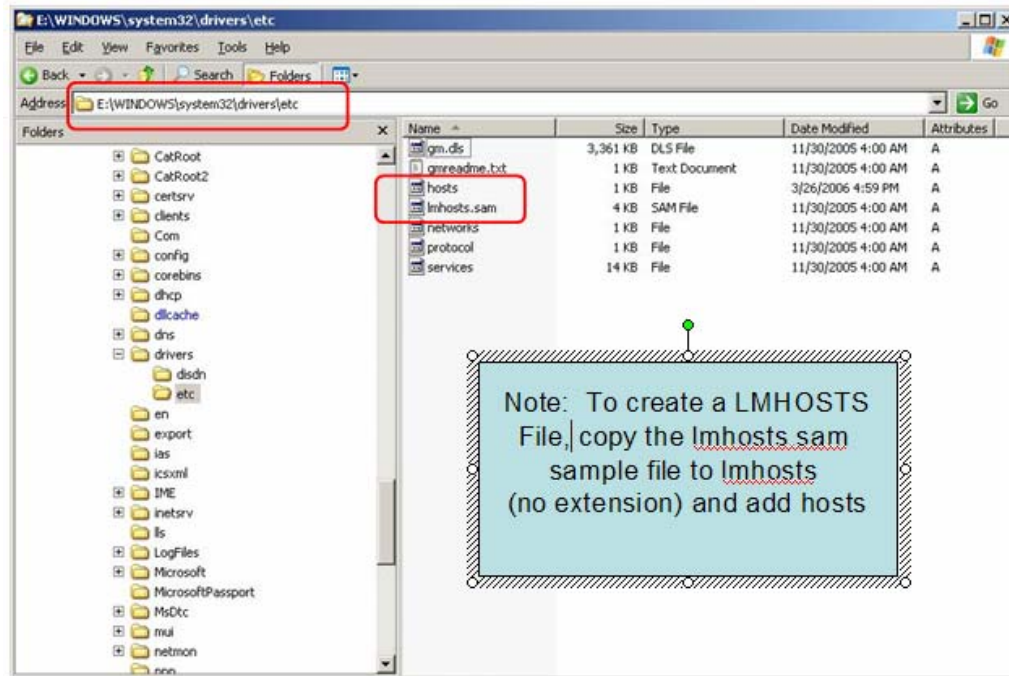
Record Name : udns1.ultradns.net
Record Type : 1
Time To Live : 77479
Data Length : 4
Section : Answer
A (Host) Record . . . : 204.69.234.1

localhost

Record Name : localhost
Record Type : 1
Time To Live : 600875
Data Length : 4
Section : Answer
A (Host) Record . . . : 127.0.0.1

E:\Documents and Settings\Administrator>

- Creating an LMHOSTS file
Save a copy of: *hosts* file and *LMHOSTS* file.



The hosts file (Home LAN)

```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com             # x client host
127.0.0.1       localhost
192.168.0.1     router
192.168.0.5     wap

```

The LMHOSTS file:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names. Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#       #PRE
#       #DOM:<domain>
#       #INCLUDE <filename>
#       #BEGIN_ALTERNATE
#       #END_ALTERNATE
#       \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addition the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
#
\machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshar
es
# in the registry. Simply add "public" to the list found there.
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97      rhino          #PRE #DOM:networking  #net group's DC
# 102.54.94.102     "appname  \0x14"  #special app server
# 102.54.94.123     popular        #PRE                #source server
# 102.54.94.117     localsrv        #PRE                #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
```

```
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.
```

Lesson 7 - Managing and Monitoring DHCP

No snapshots required

Lesson 8 - Domain Name System

- Creating Primary and Secondary zones
Save a copy of a Forward and Reverse lookup zone file.

Forward lookup zone file: station01.MiddleEarth.net

```
;
; Database file station01.MiddleEarth.net.dns for station01.MiddleEarth.net zone.
; Zone version: 4
;

@                IN  SOA station01.dovercorp.net.
hostmaster.dovercorp.net. (
                        4           ; serial number
                        900         ; refresh
                        600         ; retry
                        86400       ; expire
                        3600        ) ; default TTL

;
; Zone NS records
;

@                NS   station01.dovercorp.net.

;
; Zone records
;

Keith            A    10.1.1.102
www              CNAME keith.
Zeb              A    10.1.1.105
```

Reverse lookup zone file: 1.1.10.in-addr.arpa

```
;
; Database file 1.1.10.in-addr.arpa.dns for 1.1.10.in-addr.arpa zone.
; Zone version: 5
;

@                IN  SOA station01.dovercorp.net.
hostmaster.dovercorp.net. (
                        5           ; serial number
                        900         ; refresh
                        600         ; retry
                        86400       ; expire
                        3600        ) ; default TTL

;
; Zone NS records
;

@                NS   station01.dovercorp.net.

;
; Zone records
;

102              PTR  keith.
105              PTR  zeb.
```

- Performing zone transfers
Save a zone file that came from a zone transfer.

Transfer from station02.MiddleEarth.net

```
;
; Database file station02.MiddleEarth.net.dns for station02.MiddleEarth.net zone.
; Zone version: 1
;

@                IN SOA station02.dovercorp.net.
hostmaster.dovercorp.net. (
                        1          ; serial number
                        900        ; refresh
                        600        ; retry
                        86400      ; expire
                        3600       ) ; default TTL

;
; Zone NS records
;

@                NS    station02.dovercorp.net.

;
; Zone records
;
```

Lesson 9 - Security and Group Policy

- Create a custom security template
Save this template's .inf file

```
; Copyright (c) Microsoft Corporation. All rights reserved.
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name: lowsecws.inf
; Template Version: 1
```

```
[version]
signature="$CHICAGO$"
Revision=1
```

```
[System Access]
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 10
LockoutDuration = 10
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableGuestAccount = 0
```

```
;-----
;Local Policies - Security Options
;-----
;DC Only
;ForceLogoffWhenHourExpire = 1

;NewAdministratorName =
;NewGuestName =
;SecureSystemPartition
```

```
;-----
;Event Log - Log Settings
;-----
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)
```

```
[System Log]
MaximumLogSize = 5056
RestrictGuestAccess = 1
```

```
[Security Log]
MaximumLogSize = 16384
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
```

```
[Application Log]
RestrictGuestAccess = 1
```

```
;-----
; Local Policies\Audit Policy
;-----
[Event Audit]
AuditSystemEvents = 0
AuditLogonEvents = 3
AuditObjectAccess = 0
AuditAccountManage = 3
```

```
AuditProcessTracking = 0
AuditAccountLogon = 3
```

```
;-----
;Registry Values
;-----
```

```
[Strings]
SceInfAdministrator = "Administrator"
SceInfAdmins = "Administrators"
SceInfAccountOp = "Account Operators"
SceInfAuthUsers = "Authenticated Users"
SceInfBackupOp = "Backup Operators"
SceInfDomainAdmins = "Domain Admins"
SceInfDomainGuests = "Domain Guests"
SceInfDomainUsers = "Domain Users"
SceInfEveryone = "Everyone"
SceInfGuests = "Guests"
SceInfGuest = "Guest"
SceInfPowerUsers = "Power Users"
SceInfPrintOp = "Print Operators"
SceInfReplicator = "Replicator"
SceInfServerOp = "Server Operators"
SceInfUsers = "Users"
SceSecureWSPProfileDescription = "Provides enhanced local account policies, limits the use
of LanMan authentication, enables server-side SMB signing, and provides further
restrictions on anonymous users. To apply to a domain member, all DC's that contain
accounts of all users that logon to that member must be running NT4 SP4 or higher. See
online help for further info."
[Registry Values]
```

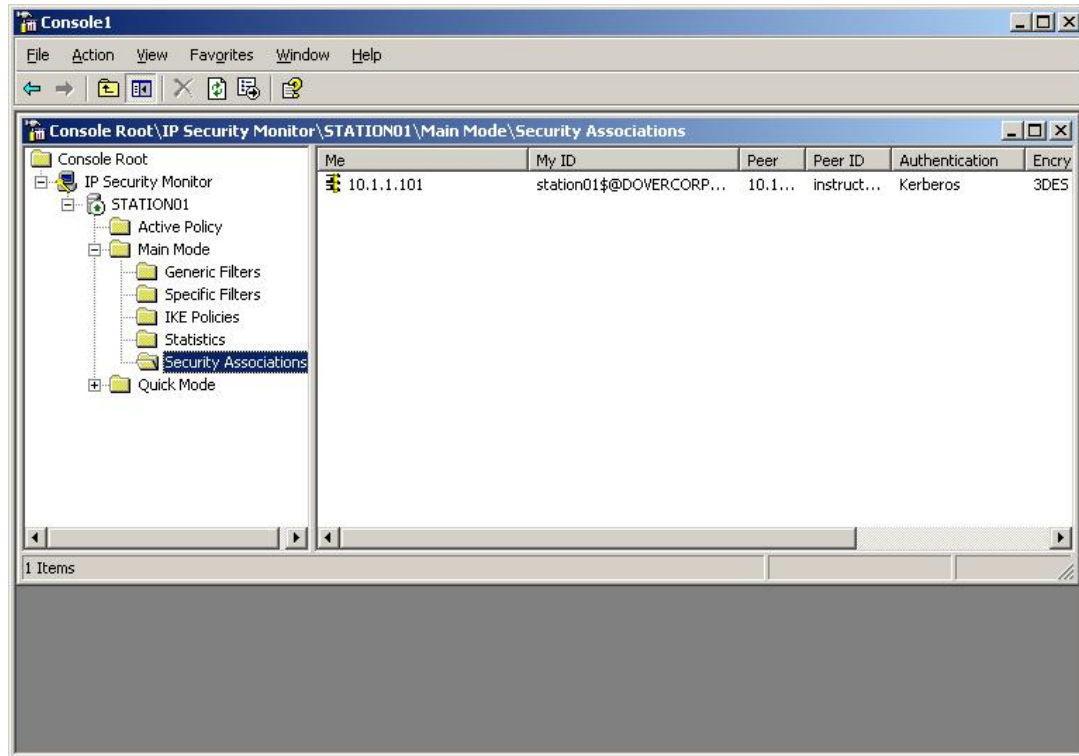
```
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,
1
```

```
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon>PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"10"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,"0"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"0"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,"0"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1," "
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName
=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge=4,30
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange=4,0
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPas
sword=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySig
nature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySign
ature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=
4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignatur
e=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature
=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
```

MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMInServerSec=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMInClientSec=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,0
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
[Privilege Rights]
SeMachineAccountPrivilege = *S-1-5-11
[Service General Setting]
"Messenger",3,""
[Profile Description]
Description=Provides enhanced local account policies, limits the use of LanMan
authentication, enables server-side SMB signing, and provides further restrictions on
anonymous users. To apply to a domain member, all DC's that contain accounts of all users
that logon to that member must be running NT4 SP4 or higher. See online help for further
info.

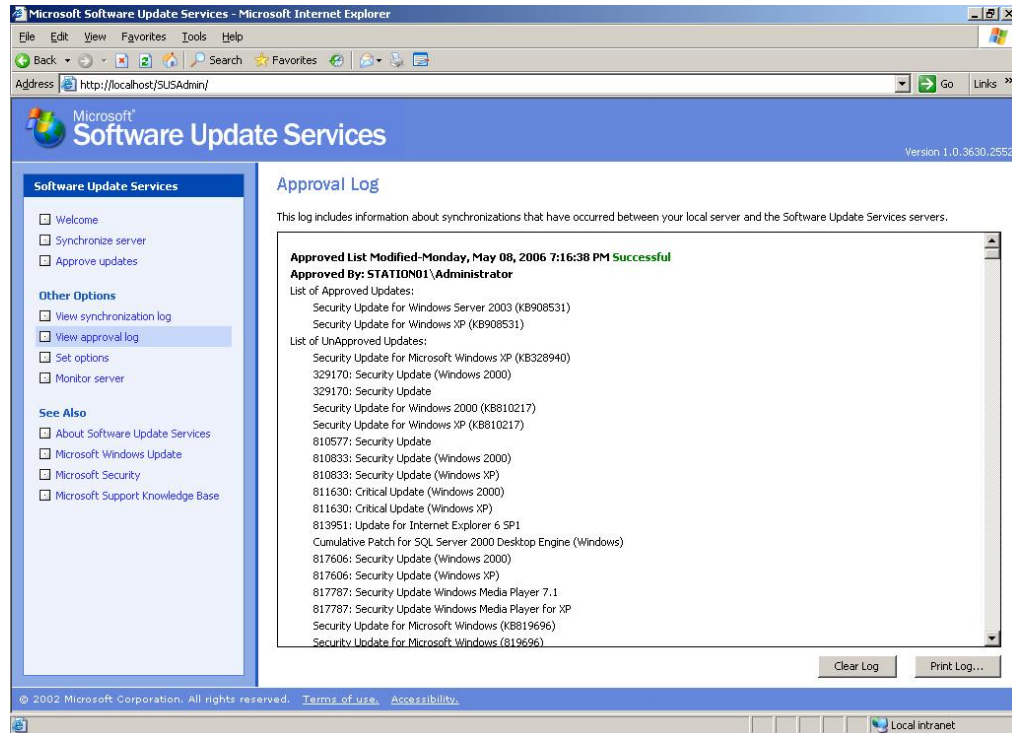
Lesson 10 - Securing Network Traffic Using IPSec

- Creating an IPSec policy using a customized filter list and filter action
Screenshot: of a Security Association from the IP Security Monitor



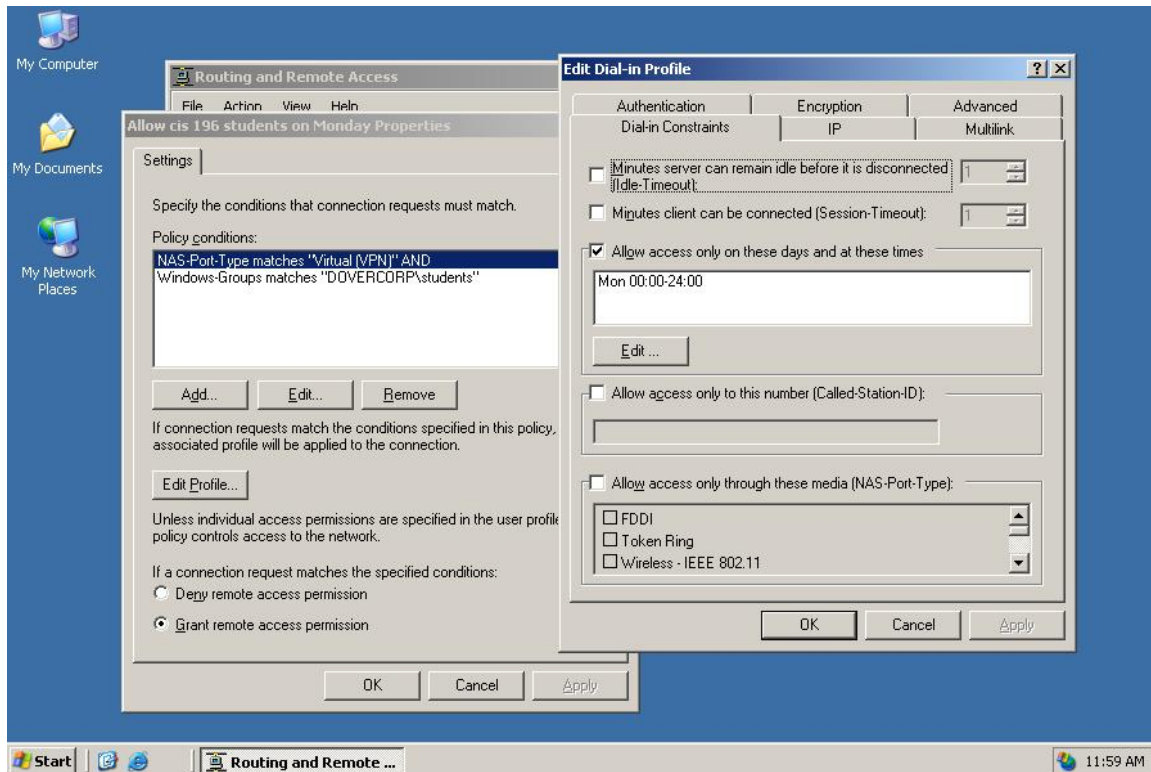
Lesson 11 - Software Update Services (SUS and WSUS)

- Synchronize and Approve Updates
Screenshot: SUS Approval log.



Lesson 12 – Remote Access

Connecting to Cabrillo network from home using RAS




```
C:\Documents and Settings\rsimms>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : ovwpc097
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cup.hp.com
```

Ethernet adapter {A5210777-7B46-4586-980E-1334051E0A1E}:

```
Connection-specific DNS Suffix . :
Description . . . . . : Nortel IPSECSHM Adapter
Physical Address. . . . . : 44-45-53-54-42-00
Dhcp Enabled. . . . . : No
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
```

Ethernet adapter Wireless Network Connection:

```
Media State . . . . . : Media disconnected
Description . . . . . : Broadcom 802.11b/g WLAN
Physical Address. . . . . : 00-90-4B-43-23-74
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : cup.hp.com
Description . . . . . : National Semiconductor Corp.
```

DP83815

/816 10/100 MacPhyter PCI Adapter

```
Physical Address. . . . . : 00-0D-9D-5D-C2-1A
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.0.25
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.1
Lease Obtained. . . . . : Wednesday, May 10, 2006
```

8:20:50 AM

```
Lease Expires . . . . . : Saturday, May 13, 2006
```

8:20:50 AM

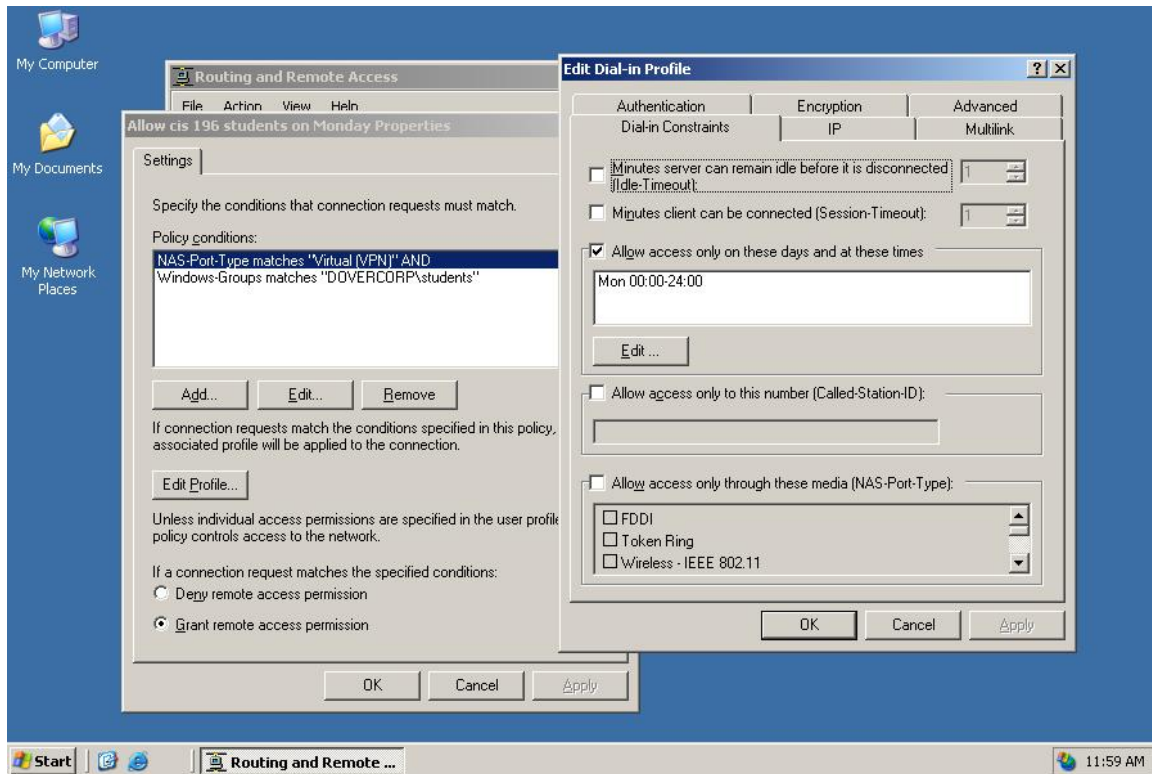
PPP adapter Cabrillo 196 class :

```
Connection-specific DNS Suffix . :
Description . . . . . : WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
Dhcp Enabled. . . . . : No
IP Address. . . . . : 172.30.1.202
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 172.30.1.202
```

```
C:\Documents and Settings\rsimms>
```

Lesson 13 – Remote Access (continued)

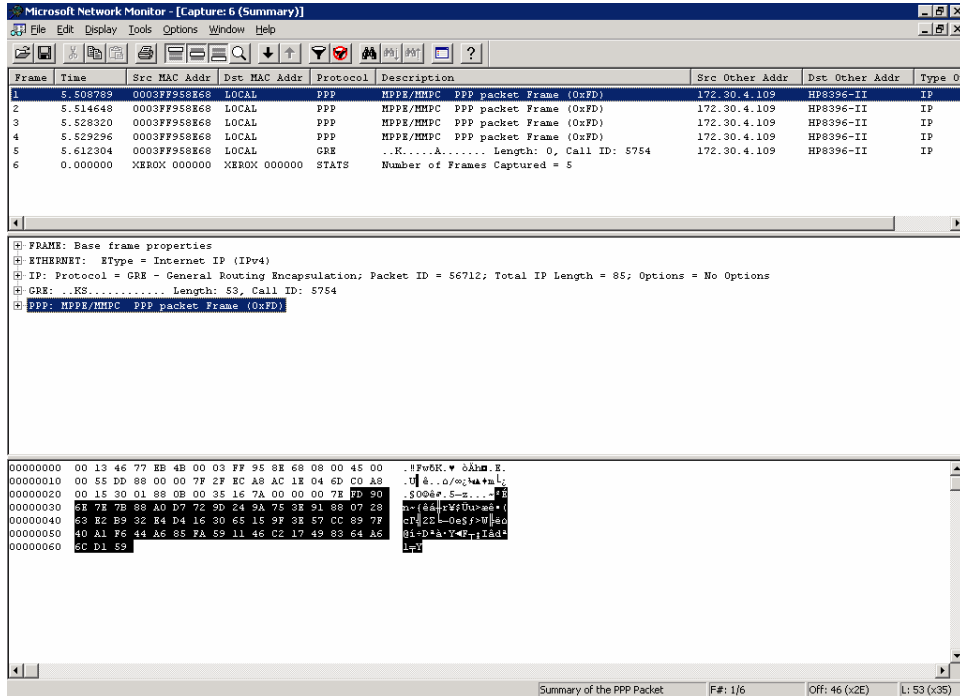
RAS policy to only allow CIS 196 students on Monday



Lesson 14 –Troubleshooting

Capturing Point-to-Point Tunneling Protocol (PPTP) packets used by RAS connection

Network Monitor (Frodo VM to Host)



Microsoft Network Monitor - [Capture: 6 (Summary)]

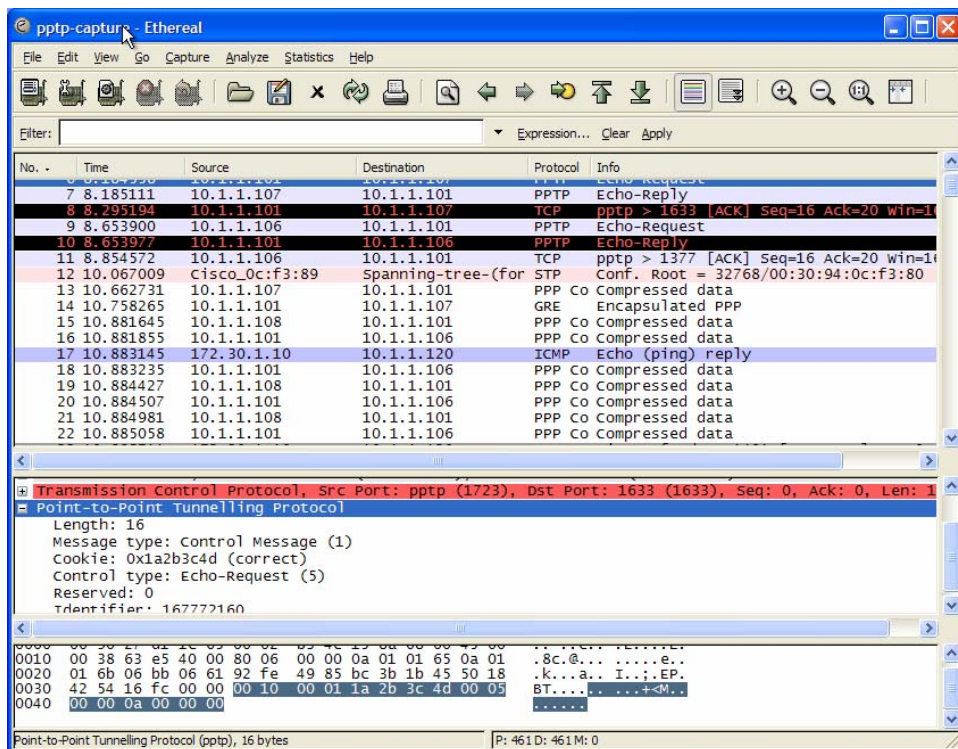
Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type
1	5.508789	0003FF958868	LOCAL	PPP	MPPE/MMPC PPP packet Frame (0x7D)	172.30.4.109	HP8396-II	IP
2	5.514648	0003FF958868	LOCAL	PPP	MPPE/MMPC PPP packet Frame (0x7D)	172.30.4.109	HP8396-II	IP
3	5.528320	0003FF958868	LOCAL	PPP	MPPE/MMPC PPP packet Frame (0x7D)	172.30.4.109	HP8396-II	IP
4	5.529296	0003FF958868	LOCAL	PPP	MPPE/MMPC PPP packet Frame (0x7D)	172.30.4.109	HP8396-II	IP
5	5.612304	0003FF958868	LOCAL	GRE	..K.....A..... Length: 0, Call ID: 5754	172.30.4.109	HP8396-II	IP
6	0.000000	XEROX 000000	XEROX 000000	STATS	Number of Frames Captured = 5			

FRAME: Base frame properties

- ETHERNET: EType = Internet IP (IPv4)
- IP: Protocol = GRE - General Routing Encapsulation; Packet ID = 56712; Total IP Length = 85; Options = No Options
- GRE: ..KS..... Length: 53, Call ID: 5754
- PPP: MPPE/MMPC PPP packet Frame (0x7D)

Summary of the PPP Packet F#: 1/6 Off: 46 (x2E) L: 53 (x35)

Ethereal (from class)



pptp-capture - Ethereal

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
7	8.185111	10.1.1.101	10.1.1.107	PPTP	Echo-Request
8	8.295194	10.1.1.101	10.1.1.107	PPTP	Echo-Reply
9	8.653900	10.1.1.106	10.1.1.101	TCP	pptp > 1633 [ACK] Seq=16 Ack=20 win=1
10	8.653977	10.1.1.101	10.1.1.106	PPTP	Echo-Request
11	8.854572	10.1.1.106	10.1.1.101	PPTP	Echo-Reply
12	10.067009	Cisco_0c:f3:89	Spanning-tree-(for	STP	Conf. Root = 32768/00:30:94:0c:f3:80
13	10.662731	10.1.1.107	10.1.1.101	PPP	Co Compressed data
14	10.758265	10.1.1.101	10.1.1.107	GRE	Encapsulated PPP
15	10.881645	10.1.1.108	10.1.1.101	PPP	Co Compressed data
16	10.881855	10.1.1.101	10.1.1.106	PPP	Co Compressed data
17	10.883145	172.30.1.10	10.1.1.120	ICMP	Echo (ping) reply
18	10.883235	10.1.1.101	10.1.1.106	PPP	Co Compressed data
19	10.884427	10.1.1.108	10.1.1.101	PPP	Co Compressed data
20	10.884507	10.1.1.101	10.1.1.106	PPP	Co Compressed data
21	10.884981	10.1.1.108	10.1.1.101	PPP	Co Compressed data
22	10.885058	10.1.1.101	10.1.1.106	PPP	Co Compressed data

Transmission Control Protocol, Src Port: pptp (1723), Dst Port: 1633 (1633), Seq: 0, Ack: 0, Len: 1

Point-to-Point Tunneling Protocol

Length: 16

Message type: Control Message (1)

Cookie: 0x1a2b3c4d (correct)

Control type: Echo-Request (5)

Reserved: 0

Identifier: 167772160

Point-to-Point Tunneling Protocol (pptp), 16 bytes P: 461D: 461M: 0

Virtual Lab for CIS 192 & 196

Rich Simms

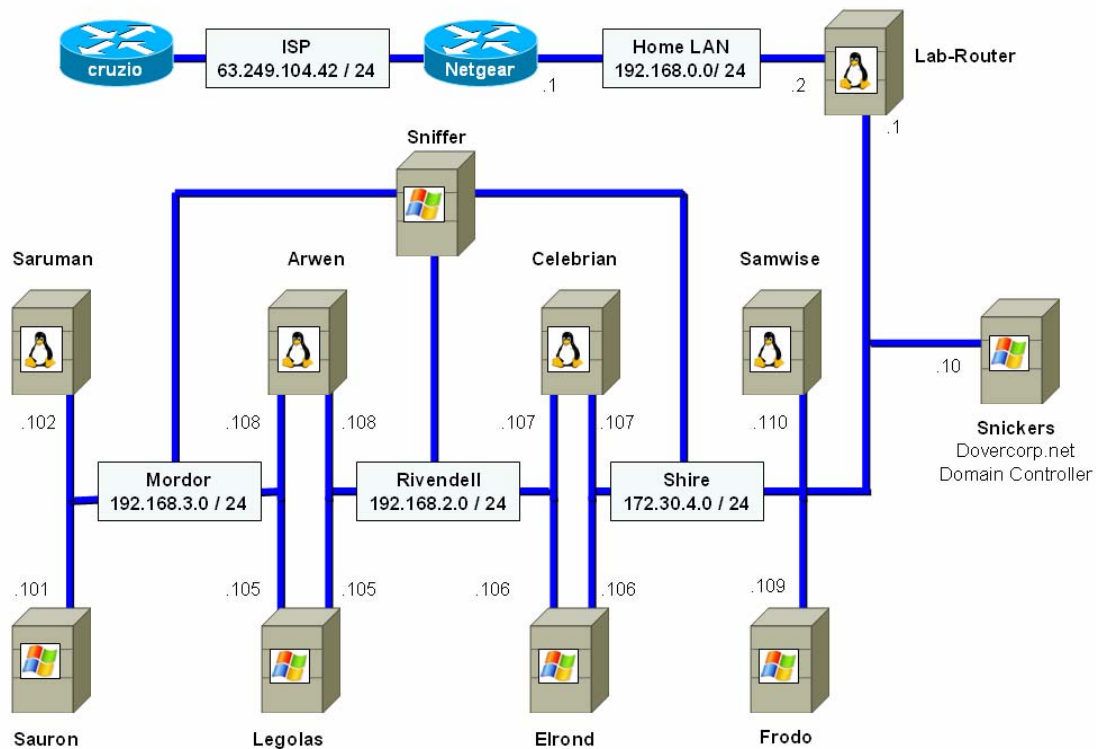
May 27, 2006

Overview

Microsoft's virtualization technology has been available as a product called Virtual Server. Microsoft recently announced two major changes for Virtual Server 2005 R2. It is now a free download and Linux is supported.

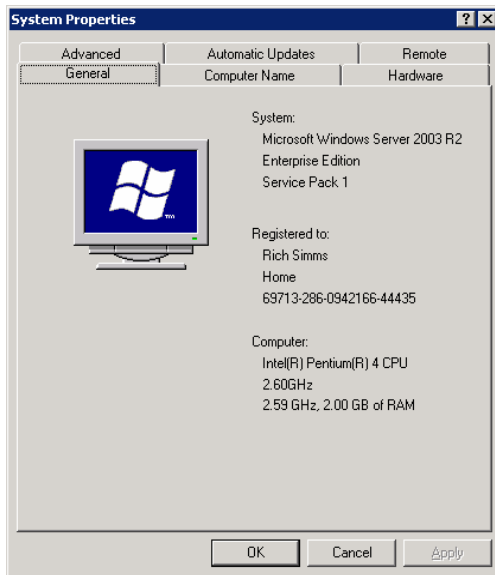
A virtual MiddleEarth lab was created using Virtual Server on one physical host computer running Windows 2003 Enterprise Edition R2. It is a virtual replica of the physical MiddleEarth lab running at Cabrillo College. There are some differences from the real lab in that the version of Linux is different and the VMs created are not dual boot. Each VM was either loaded with Windows or Linux as shown in the diagram below. The *lab-router* server was a virtual machine running Linux that bridged the virtual world with the physical world. The Sniffer VM had three interfaces with Ethereal loaded for troubleshooting purposes.

Layout



Physical Host

The Host computer supporting all these VMs had a single 2.6 GHz Pentium 4 CPU with 2 GB of RAM installed as shown in the following System Properties summary.



Lab-Router configuration

The VM named *lab-router* is a Linux server that connects the virtual lab to the home LAN. Eth0 is connected to the home LAN and eth1 is connected to virtual Shire network. Routes were added so MiddleEarth VMs could communicate with PCs on the home LAN. A destination NAT was added so VM's would still think the Cabrillo DNS server was available. The Cabrillo DNS addresses was translated to my home Netgear router which provide DNS services.

Commands used:

```
iptables -t nat -A PREROUTING -d 207.62.187.54 -j DNAT --to-destination 192.168.0.1
route add -net 192.168.2.0 netmask 255.255.255.0 gw 172.30.4.107
route add -net 192.168.3.0 netmask 255.255.255.0 gw 172.30.4.107
```

Routing Table:

```
[root@lab-router root]# route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
172.30.4.0     0.0.0.0        255.255.255.0   U        0      0        0 eth1
192.168.3.0    172.30.4.107   255.255.255.0   UG        0      0        0 eth1
192.168.2.0    172.30.4.107   255.255.255.0   UG        0      0        0 eth1
192.168.0.0    0.0.0.0        255.255.255.0   U        0      0        0 eth0
169.254.0.0    0.0.0.0        255.255.0.0     U        0      0        0 eth1
127.0.0.0      0.0.0.0        255.0.0.0       U        0      0        0 lo
0.0.0.0        192.168.0.1    0.0.0.0         UG        0      0        0 eth0
[root@lab-router root]#
```

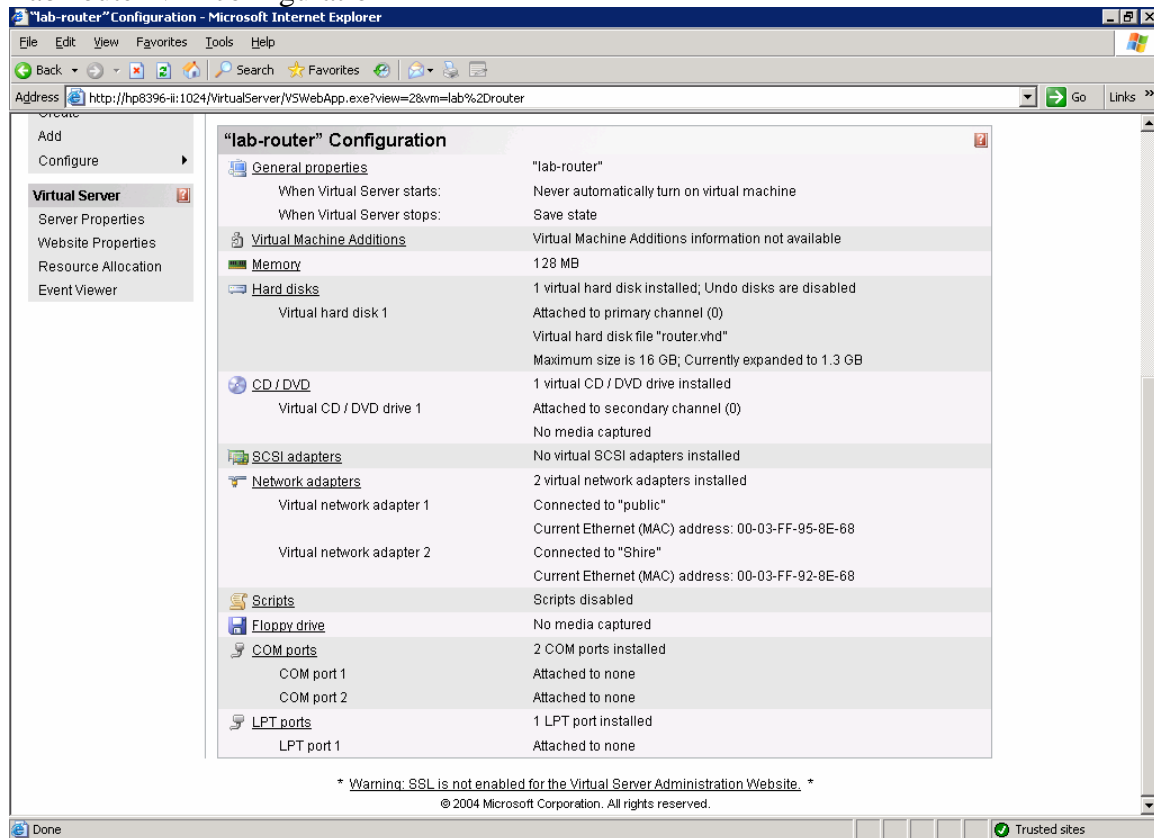
NAT table:

```
[root@lab-router root]# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT       all  --  anywhere              buttercup.cabrillo.eduto:192.168.0.1

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination

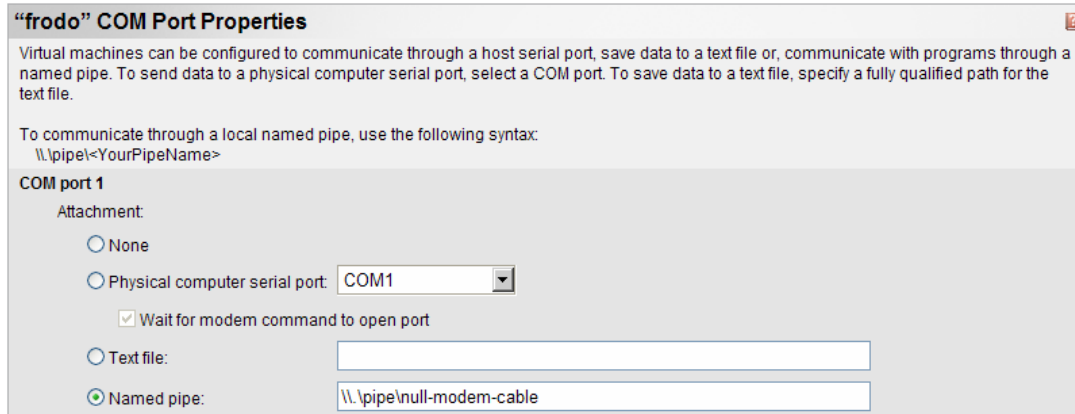
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@lab-router root]#
```

Lab-router VM configuration



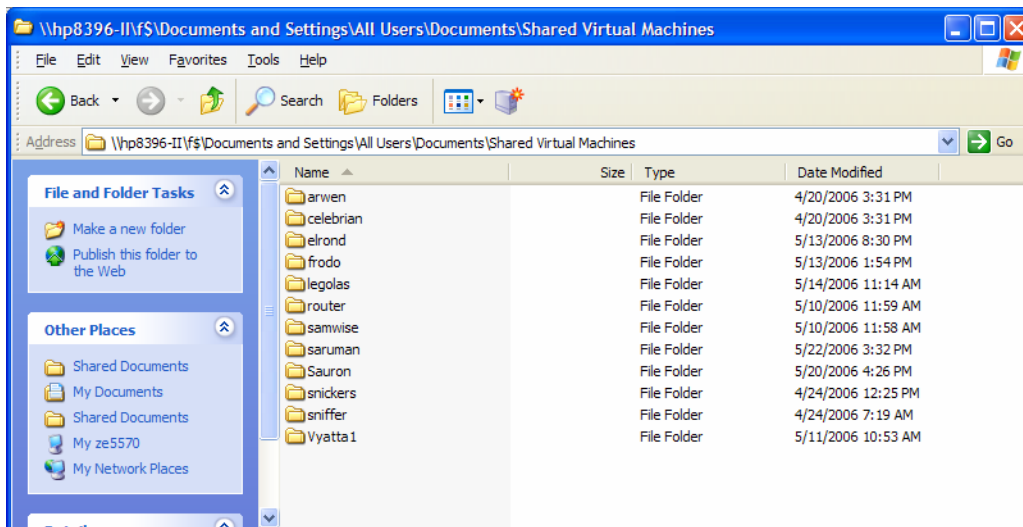
Serial Connections

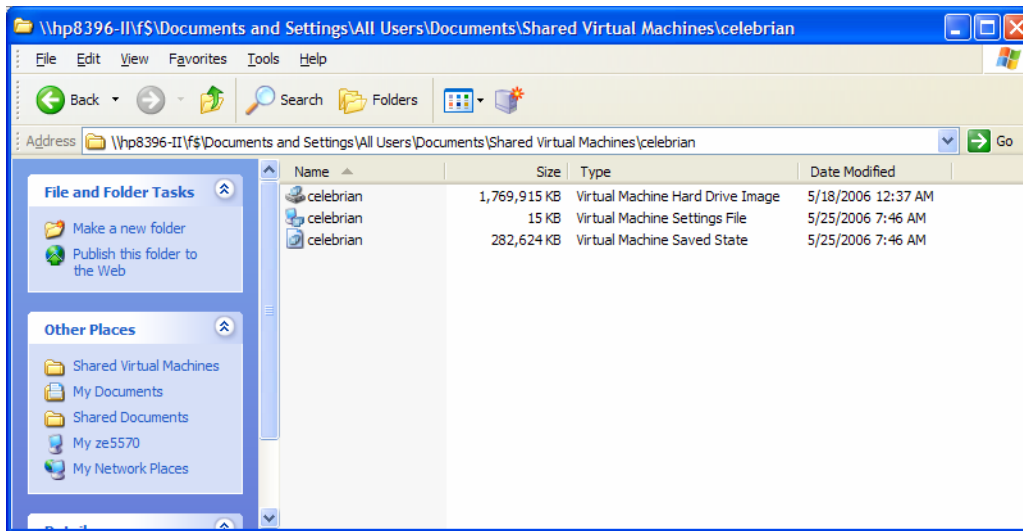
Some of the lab assignments required serial connections between computers. There is a way to have a virtual serial cable running between the COM ports of the VMs. This is done by specifying a named pipe as the COM port setting. For example the Com 1 ports on *Frodo* and *Elrond* are both set to [\\.\pipe\null-modem-cable](#) to enable a serial connection between the two of them.



Physical Disk Space

Each VM occupies about 2 GB of physical disk space. They are kept in the folder shown below on the host machine:





The virtual machines

The screenshot shows the 'hp8396-ii Status' page in Microsoft Internet Explorer. The browser's address bar shows the URL 'http://hp8396-ii:1024/VirtualServer/VSWebApp.exe?view=1'. The page title is 'hp8396-ii Status'. The main content area displays a table of virtual machines with columns for 'Virtual Machine Name', 'Status', 'Running Time', and 'CPU Usage'. The table lists 13 VMs: arwen, celebrian, elrond, frodo, lab-router, legolas, samwise, saruman, sauron, snickers, sniffer, and vyatta1. The status of each VM is indicated by a small icon and a status label (e.g., 'Saved', 'Running', 'Off'). The running time is shown for running VMs, and the CPU usage is shown as a percentage (e.g., 'n/a', '1 minute, 29 seconds').

Virtual Machine Name	Status	Running Time	CPU Usage
arwen	Saved	n/a	n/a
celebrian	Saved	n/a	n/a
elrond	Running	1 minute, 29 seconds	
frodo	Running	1 minute, 49 seconds	
lab-router	Running	2 minutes, 22 seconds	
legolas	Running	1 minute, 6 seconds	
samwise	Saved	n/a	n/a
saruman	Saved	n/a	n/a
sauron	Saved	n/a	n/a
snickers	Running	2 minutes, 0 seconds	
sniffer	Running	38 seconds	
vyatta1	Off	n/a	n/a

The page also includes a 'Navigation' sidebar on the left with links to 'Master Status', 'Virtual Machines', 'Virtual Disks', 'Virtual Networks', and 'Virtual Server'. The 'Virtual Machines' section is currently selected. At the bottom of the page, there is a section for 'hp8396-ii Recent Events'.

The Windows VMs were loaded with Windows 2003 Standard Edition and the Linux VMs were loaded with Redhat Enterprise Linux AS3.

Typical Linux VM configuration:

The screenshot displays the 'celebrian' Configuration page in Microsoft Internet Explorer. The browser's address bar shows the URL: `http://hp8396-it:1024/VirtualServer/VSWebApp.exe?view=2&vm=celebrian`. The page is divided into a left navigation pane and a main content area.

Navigation Pane:

- Master Status
- Virtual Server Manager
- Virtual Machines
 - Create
 - Add
 - Configure
- Virtual Disks
 - Create
 - Inspect
- Virtual Networks
 - Create
 - Add
 - Configure
- Virtual Server
 - Server Properties
 - Website Properties
 - Resource Allocation
 - Event Viewer

“celebrian” Status

celebrian ▶ Click the thumbnail to restore this virtual machine from saved state

Virtual machine status	Saved
Running time	n/a
Physical CPU utilization	n/a
Heartbeat	n/a
Disk I/O	n/a
Network I/O	n/a
Guest operating system	n/a
Virtual Machine Additions	Additions information not available
.vmc file	F:\Documents and Settings\All Users\Documents\Shared Virtual Machines\celebrian\celebrian.vmc

“celebrian” Configuration

General properties	
When Virtual Server starts:	Never automatically turn on virtual machine
When Virtual Server stops:	Save state
Virtual Machine Additions	
Virtual Machine Additions information not available	
Memory	
256 MB	
Hard disks	
1 virtual hard disk installed; Undo disks are disabled	
Attached to primary channel (0)	
Virtual hard disk file "celebrian.vhd"	
Maximum size is 4 GB; Currently expanded to 1.7 GB	
CD / DVD	
1 virtual CD / DVD drive installed	
Attached to secondary channel (0)	
ISO image "rhel-3-i386-as-disc3.iso"	
SCSI adapters	
No virtual SCSI adapters installed	
Network adapters	
2 virtual network adapters installed	
Virtual network adapter 1	
Connected to "Rivendell"	
Current Ethernet (MAC) address: 00-03-FF-94-8E-68	
Virtual network adapter 2	
Connected to "Shire"	
Current Ethernet (MAC) address: 00-03-FF-91-8E-68	
Scripts	
Scripts disabled	
Floppy drive	
Host drive "A"	
COM ports	
2 COM ports installed	
COM port 1	
Attached to none	
COM port 2	
Attached to none	
LPT ports	
1 LPT port installed	
LPT port 1	
Attached to none	

The status bar at the bottom shows "Done" and "Local intranet".

Typical Windows VM configuration

The screenshot shows a web-based interface for configuring a virtual machine named "elrond". The interface is displayed in a Microsoft Internet Explorer browser window. The address bar shows the URL: `http://hp8396-it:1024/VirtualServer/VSWebApp.exe?view=2&vm=elrond`.

Navigation Panel (Left):

- Master Status
- Virtual Server Manager
- Virtual Machines
 - Create
 - Add
 - Configure
- Virtual Disks
 - Create
 - Inspect
- Virtual Networks
 - Create
 - Add
 - Configure
- Virtual Server
 - Server Properties
 - Website Properties
 - Resource Allocation
 - Event Viewer

"elrond" Status Panel:

elrond Click the thumbnail to restore this virtual machine from saved state

Virtual machine status	Saved
Running time	n/a
Physical CPU utilization	n/a
Heartbeat	n/a
Disk I/O	n/a
Network I/O	n/a
Guest operating system	n/a
Virtual Machine Additions	Additions information not available
.vmc file	F:\Documents and Settings\All Users\Documents\Shared Virtual Machines\elrond\elrond.vmc

"elrond" Configuration Panel:

General properties

- When Virtual Server starts: Never automatically turn on virtual machine
- When Virtual Server stops: Save state

Virtual Machine Additions

- Virtual Machine Additions information not available

Memory

- 256 MB

Hard disks

- 1 virtual hard disk installed; Undo disks are disabled
- Attached to primary channel (0)
- Virtual hard disk file "elrond.vhd"
- Maximum size is 4 GB; Currently expanded to 1.8 GB

CD / DVD

- 1 virtual CD / DVD drive installed
- Attached to secondary channel (0)
- No media captured

SCSI adapters

- No virtual SCSI adapters installed

Network adapters

- 2 virtual network adapters installed
- Virtual network adapter 1: Connected to "Rivendell"
- Current Ethernet (MAC) address: 00-03-FF-9A-8E-68
- Virtual network adapter 2: Connected to "Shire"
- Current Ethernet (MAC) address: 00-03-FF-98-8E-68

Scripts

- Scripts disabled

Floppy drive

- No media captured

COM ports

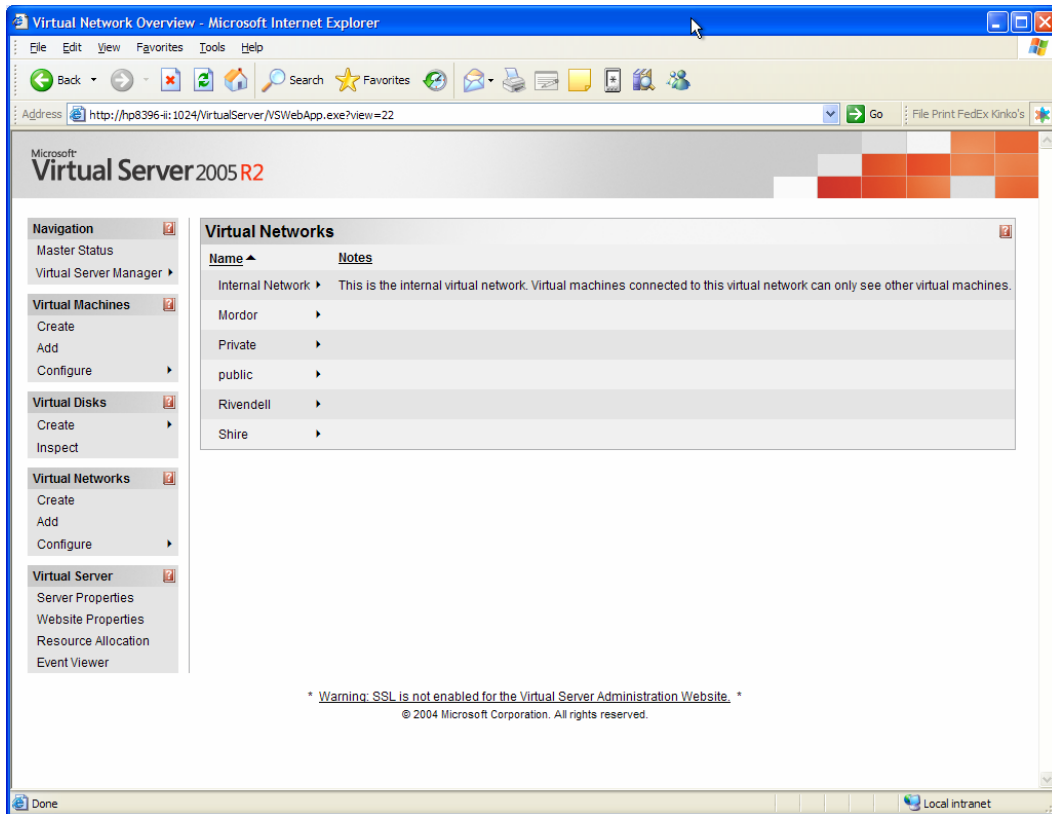
- 2 COM ports installed
- COM port 1: Attached to named pipe "\\pipe>null-modem-cable"
- COM port 2: Attached to none

LPT ports

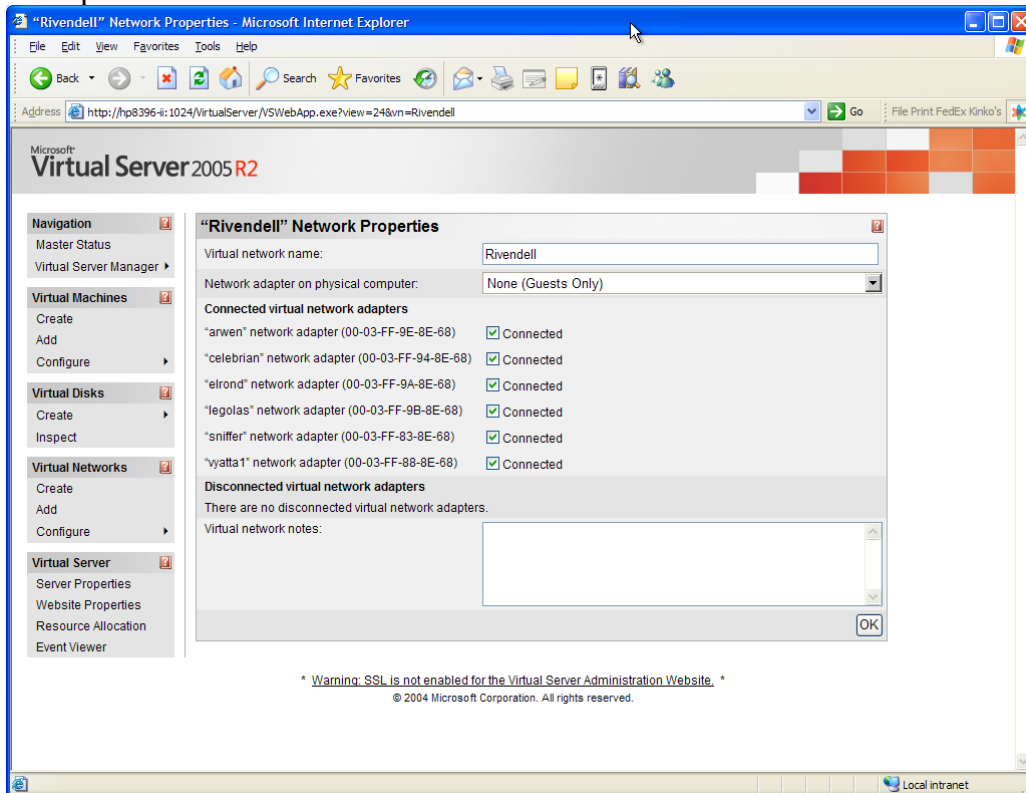
- 1 LPT port installed
- LPT port 1: Attached to none

The status bar at the bottom shows "Done" and "Local intranet".

Virtual Networks:



Example network:



Resource Allocation:

hp8396-ii CPU Resource Allocation - Microsoft Internet Explorer

Address: http://hp8396-ii:1024/VirtualServer/VSIWebApp.exe?view=34

Microsoft
Virtual Server 2005 R2

Navigation

- Master Status
- Virtual Server Manager

Virtual Machines

- Create
- Add
- Configure

Virtual Disks

- Create
- Inspect

Virtual Networks

- Create
- Add
- Configure

Virtual Server

- Server Properties
- Website Properties
- Resource Allocation**
- Event Viewer

hp8396-ii CPU Resource Allocation

You can allocate CPU resources to virtual machines currently configured on Virtual Server. In most cases, you will only need to configure the Relative Weight of the virtual machines. You can also configure absolute limits. For more information, click the help button.

Virtual Machine	Relative Weight	Reserved Capacity (% of one CPU)	Maximum Capacity (% of one CPU)	Reserved Capacity (% of system)	Maximum Capacity (% of system)	CPU Usage
Virtual Machines Currently Running						
elrond	100	0%	100%	0%	100%	
frodo	100	0%	100%	0%	100%	
lab-router	100	0%	100%	0%	100%	
legolas	100	0%	100%	0%	100%	
snickers	100	0%	100%	0%	100%	
sniffer	100	0%	100%	0%	100%	
Total Capacity Reserved				0%		
Available Capacity Remaining				100%		
Virtual Machines Not Currently Running						
arwen	100	0%	100%	0%	100%	
celebrian	100	0%	100%	0%	100%	
samwise	100	0%	100%	0%	100%	
saruman	100	0%	100%	0%	100%	
sauron	100	0%	100%	0%	100%	
vyatta1	100	0%	100%	0%	100%	

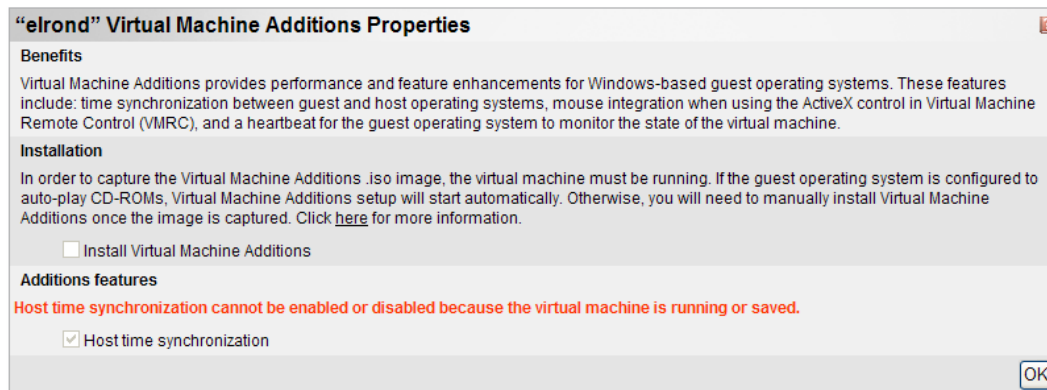
OK

* Warning: SSL is not enabled for the Virtual Server Administration Website. *

Done Local intranet

Issues with Virtual Server 2005 R2

Most issues that arose were resolved. The first issue I ran into was effective mouse control on a VM when using a Remote Desktop Connection. For example if you had a remote connection into the server hosting the VM's it was just about impossible to control the mouse using the Virtual Machine Remote Control Client. The resolution was to install the Virtual Machine Additions on each Windows VM.

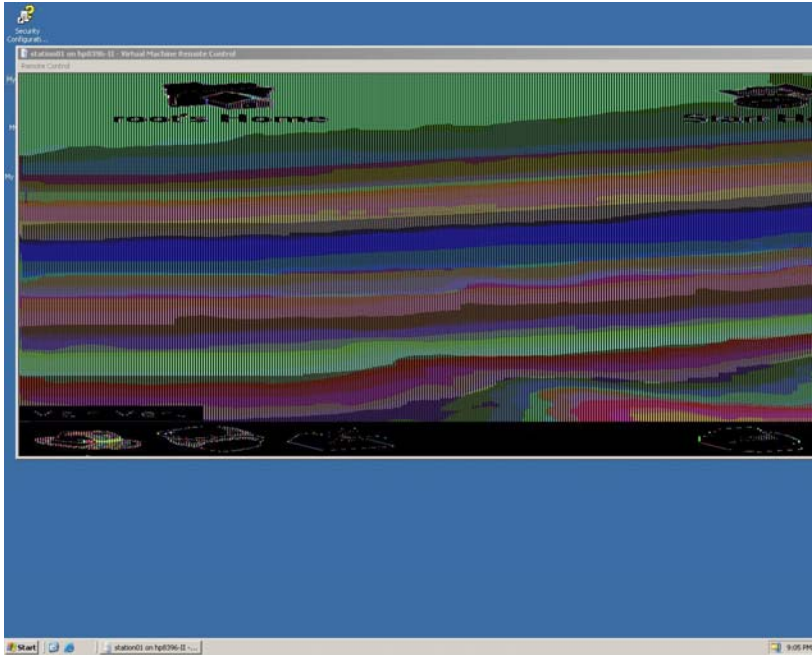


With Linux I still have two unresolved issues. One is an annoyance and the other is a serious limitation. The annoyance was that randomly on the Linux VM's you will get the following message:

```
i8253 count too high! Resetting..
```

It seems to have no impact at all so I have just ignored it.

The more serious issue is that I cannot get Linux to run in Graphics mode correctly. The display configuration is wrong resulting in a very stretched out screen. There is no ability to scroll to the right side and the GUI tools are too unreadable to be useful. I thought the "not so easy to install" VM Additions for Linux would help, especially the vmadd-x11-0.0.1-1.i386.rpm. While they improved mouse control there were no improvements to the display issue.



I had a similar problem in the past trying to install Linux on my laptop. The solution then was to fiddle with the boot and configuration files till it worked correctly. The Linux VMs work fine in text mode so it is a good way to learn how to do everything from the command line.

Summary

This has been a very useful tool and the price is right. VMs are very flexible and useful for doing lab assignments. Being able to save the state of a VM allows you to save of multiple configurations that can be brought back online whenever needed.