CET442L Lab #2

IP Configuration and Network Traffic Analysis Lab

Goals: In this lab you will plan and implement the IP configuration for the Windows server computers on your group's network. You will use PING to verify connectivity between the various units. You will also learn how to monitor a network using *Ethereal*, a protocol analyzer program.

WARNING:

Failure to disconnect your group's network from DeVry's network may cause severe disruption to the school network. Your installation will also not work correctly.

Each group must be in a separate collision domain; in other words, each group must have its own hub or switch that is not connected to any other group's system.

IP Planning

There are two types of IP addresses on any network, *static* and *dynamic*. A static address never changes. Servers, printers, routers, and other important devices are always assigned a static IP address when the network is being planned. This way everyone on the network knows where important services can be found.

Dynamic IP addresses are usually assigned to client workstations. The dynamic host configuration protocol (DHCP) assigns dynamic IP addresses -- and you guessed it, a server must provide DHCP services to the network. In a later experiment you'll set up DHCP so that clients can connect to your network and automatically obtain the IP configuration information. Your network will look very similar to Figure 1.

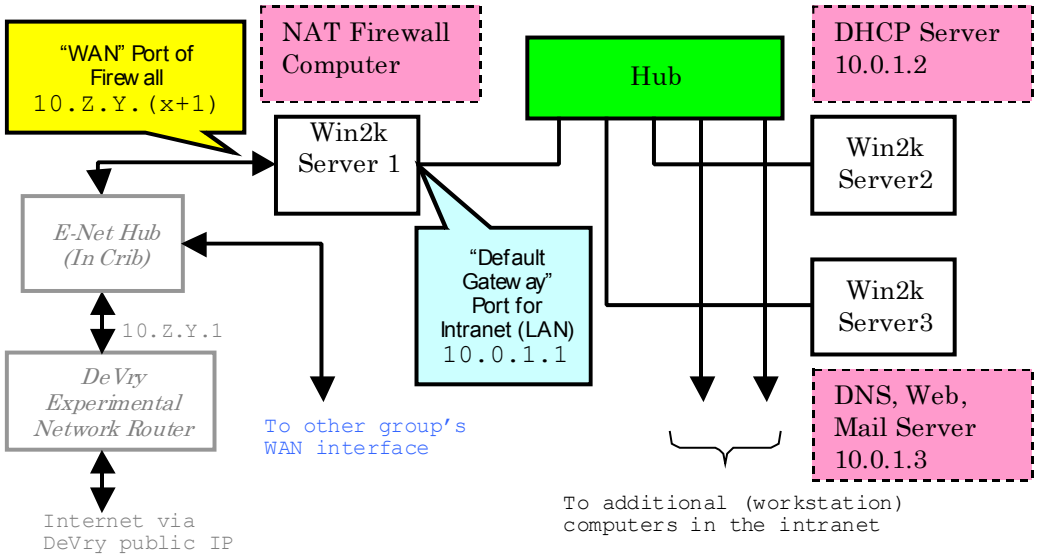


Figure 1: Network configuration diagram

Your network will consist of the following parts:

- HUB (or SWITCH): This component connects all the devices on your network. If possible, use a switch for better performance. The hub is located on the north end of the bench.

- Server 1: NAT Firewall: This computer will be your company's bridge to the open Internet. *It must have two NIC cards (the computers at the ends of the benches have dual NIC cards).* This computer insulates the "internal" network of your company from the Internet, effectively controlling external access to your organizations resources.

  Note that this unit will have two IP addresses, one for the "internal" interface, and one for the "external" (Internet) interface.

  For the "internal" interface, use 10.0.1.1 for the IP address. For the "external" interface (NOT YET CONNECTED IN THIS EXPERIMENT), use 10.Z.Y.(*X+1)*, where *X* is your group number. The subnet mask for both firewall interfaces should be 255.255.255.0, and the "default gateway" value should be 10.Z.Y.1 (the next-hop router in the DeVry experimental network). You learned the values for Z and Y in Step 9 of Lab 1; they depend on what part of the E-NET your lab is stationed in.

TIP:

You can name network interfaces in Windows. It is very helpful to give the names "WAN" and "LAN" to the two interfaces on your firewall computer.

- Server 2: DHCP Server: This unit will parcel out IP addresses to workstations within your network using the dynamic host configuration protocol. (Note that you can let this function be taken up by another server on the network, but for the purpose of this lab, we want you to use a separate computer.) Use 10.0.1.2 for the DHCP server.

- Server 3: DNS, Web and Mail Server: The "face" of your company will be the web site it provides to the outside world. It will host the web pages that people will see when they look for your organization, and it will also provide POP/SMTP services for your employees. In order to provide web and other Internet services to the world, you must also supply DNS service (or use a third-party to provide it). Use 10.0.1.3 for this computer.

TIP:

The default gateway for all computers in your LAN is the firewall computer. Therefore, set the default gateway value for LAN computers to the IP address of the LAN interface of the firewall.

Static and Dynamic IP Block Allocation

Before building a network, it's a good idea to the have IP parceling plan in hand. Our network has only three static IP devices so far, and an unknown number of DHCP clients. Table 1 shows a pretty safe way of resolving this, at least for a small (Class C subnetted) network.

IP Address (or Range)	Usage
10.0.1.1	Server 1 "LAN" port and "Default Gateway" for all devices on the LAN
10.0.1.2	Server 2 (DHCP service)
10.0.1.3	Server 3 (DNS, Web, Mail)
10.0.X.4 - 10.0.X.15	Reserved for future static IP devices such as printers, servers, etc.
10.0.X.16 - 10.0.X.254	Workstations and other DHCP clients

Table 1: Suggested IP Allocation Plan for the Network

Traffic Analysis on a Network

Networks are generally very reliable systems. Most trouble on them is caused by one or more of the following factors:

- Physical failure of cables, fiber optics, and other components.
- Failure of hosts that are are needed by the network.
- Excessive traffic load (leading to high collisions and congestion).
- Willful damage caused by crackers and other intruders.

You can easily check the physical layer of a network by looking for the activity lights on interfaces, but what about the data link and network layers? The way to check for bona-fide activity on a network is to use a *protocol analyzer*. A protocol analyzer (sometimes called a "sniffer") lets you monitor the traffic on a network, and thus verify the operation of the network and the hosts attached to it.

In order to monitor the traffic on a network segment, a protocol analyzer program sets the network interface card (NIC) in the computer into a special mode called "promiscuous mode." In this mode the NIC responds to messages (frames, or layer 2 packet datagram units) from all computers on the network, even when the messages aren't addressed to it.

⇒ *The "Network Monitor" that is supplied with Windows 2000 Server is crippleware. It doesn't utilize the promiscuous mode of the network interface adapter, therefore it can only view traffic to and from the computer on which it is installed.*

The physical connection of the monitoring computer to the network being monitored is important. Computers are usually networked together using either *hubs* or *switches*. There is a critical difference between these two types of devices. *Hubs* electrically tie all the network interfaces on the network together into one shared connection (like a party line telephone.) *Switches* isolate the individual computers, electronically analyzing and directing the traffic only to the connection wired to the destination computer.

You may not be able to effectively monitor traffic through a switch because of the selective switching of the traffic. Often you may see just one half of a network "conversion." If you need to verify what's going on, substitute a hub for the components involved. Many networking people carry one or two small "pocket" hubs in their toolkit for exactly this purpose.

Ethereal, an Open-Source Analyzer

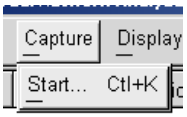
Ethereal is a free network traffic analyzer available for Windows, UNIX, and Linux. It is a very effective program for traffic analysis and troubleshooting. It can be downloaded from `http://www.ethereal.com`. To use the software on a Windows box you must install the following packages (in order):

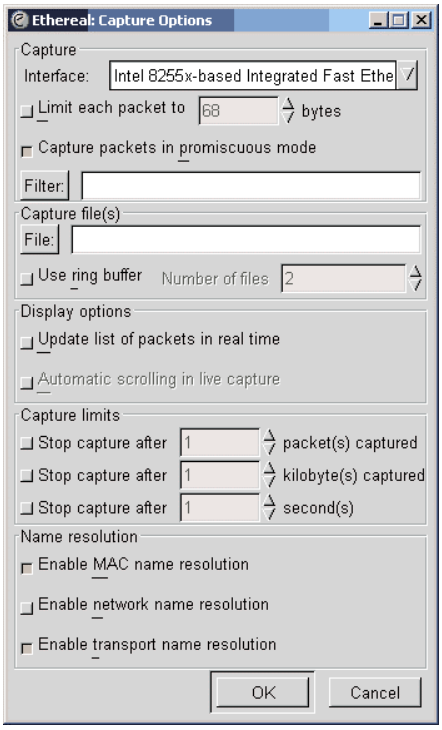
- WinPcap32 packet capture driver. This driver lets Ethereal access the NIC card in promiscuous mode. **Make sure you get the latest version of this driver!**
- Ethereal.

Ethereal should be installed on a laptop or workstation (not a server). Laptop installation is optimal since it allows portability and gives you the ability to freely connect to various parts of a network as needed.

Using Ethereal

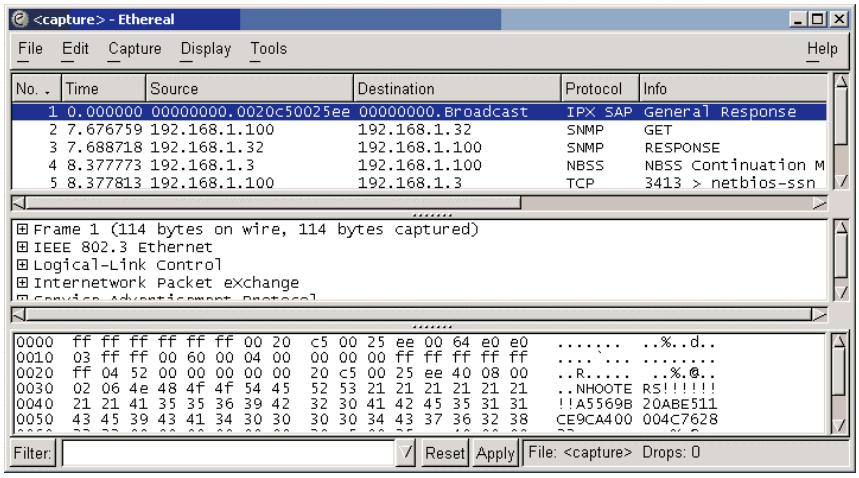
To use Ethereal, simply double-click its icon. Connect the computer to the network being analyzed, then use the "Capture - > Start" command (CTRL-K) to begin the capture:





Once you issue this command, Ethereal pops up a dialog box with a few options. Pay attention to the "Interface" setting. You should choose the interface corresponding to the NIC card connected to the network being inspected. Also notice the "Capture limits" section. These tell Ethereal when to stop collecting data. Leaving them all unchecked (as shown) will cause Ethereal to collect data until you manually stop it. Finally, the "promiscuous mode" option must be checked to see traffic from any host on the network.

Once you click OK, Ethereal begins collecting *all* the packets it sees on the network. When the traffic collection is complete (capture limit is reached or you manually stop it), it displays the data in the main window:



In the main window display, the top portion shows the packet summary (each packet is numbered in the order it was captured). The middle portion shows the parsed or disassembled version of the packet. The bottom window shows the raw data. Ethereal knows how to decipher more than 110 different network protocols, so there's rarely a need to utilize the raw data in the bottom window.

Just like in most Windows applications, clicking the [+] icon for items expands them so that you can read the details.

You can learn a great deal by trying the various options available with the software. The documentation is also available online at the Ethereal web site.

CAUTION: Ethereal will let you see *all* traffic on a network segment. This may include messages containing the private information of other network users. Therefore, you should not allow just anyone to use *Ethereal* or any other sniffer on your network. Furthermore, if you are not the administrator of the network you need to troubleshoot, you should obtain permission before connecting the protocol analyzer.

DO NOT CONNECT YOUR PACKET ANALYZER TO THE DEVRY UNIVERSITY NETWORK WITHOUT PERMISSION. THIS WOULD BE CONSIDERED A VIOLATION OF THE COMPUTER ACCEPTABLE USE POLICY.

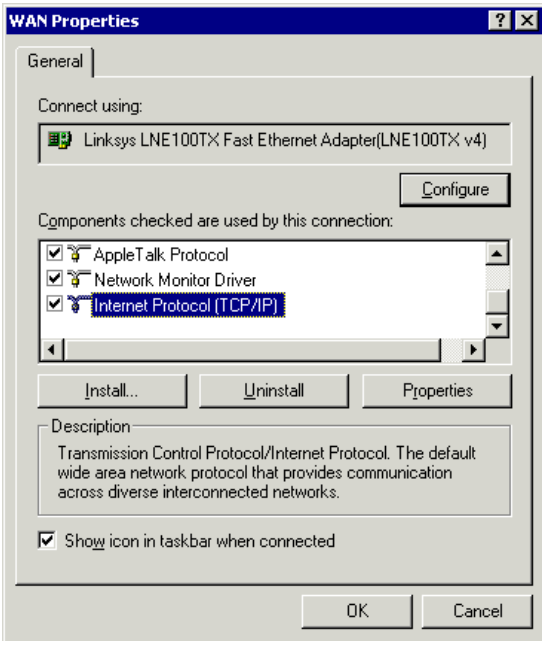
Laboratory Procedure:

1. Connect the three Windows 2000 servers as shown in Figure 1. Construct the IP plan of your network using the method previously shown.

2. To configure the IP address of each device (according to your plan), proceed as follows:

   a) Under the Start Menu, under "Settings -> Network and Dial-Up Connections" choose the LAN interface that you wish to configure.

   b) A "Status" dialog box for the network interface should appear. Click the PROPERTIES button to begin making changes to the IP configuration for the interface. The following should appear:

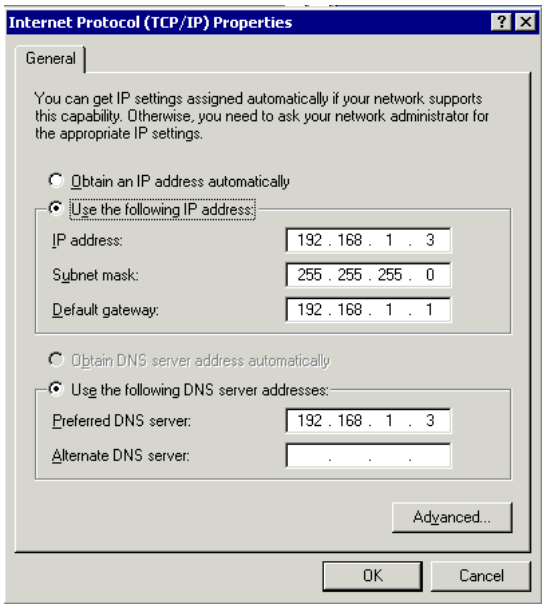


   c) Highlight "Internet Protocol (TCP/IP)" and click PROPERTIES.

   Note: If TCP/IP doesn't appear in the list, you need to install the TCP/IP networking component from the installation CD-ROM or image.

   Note: It is recommended that you check "Show icon in taskbar when connected." This makes it easier to access the dialog when working with the computer.

d) The following dialog box will appear:



Fill in the correct information for each computer. (Don't forget to enter the address of server #3 for the "Preferred DNS server" for each unit.)

Don't forget that server #1 is the default gateway to the Internet (it will be providing a NAT firewall), so all devices on your network should have server #1 as the gateway.

e) Click OK to close this dialog box, then click OK to close the "Status" dialog box. The IP configuration of the interface is now complete.

f) To verify the configuration, open a command line prompt and type the following:

```
IPCONFIG /ALL
```

This should "dump" all the information about the interface to the display. Make sure to include the IPCONFIG "dump" for each workstation in your documentation for this experiment!

3. Once all devices are configured, they should all be able to communicate with each other. A tool that is typically used for this purpose is PING. PING is issued from a command line prompt like this:

```
ping <host IP>
```

For example:

```
ping 10.0.1.1
```

Should ping the LAN interface of the NAT server in your network.

(Step 3, Continued):

You should test connectivity between all devices on the network by providing PING results in your laboratory report.

Please note that PING does *not* guarantee that the *correct* host is responding to the echo requests. In other words, if you have the wrong IP address configured for a host, then it will respond on that address. There's no way to know this directly from the results of a PING.

Figure out a working procedure for overcoming this limitation, and document it in your report.

4. Load *Ethereal* and the necessary supporting driver onto a workstation or laptop.

5. Use Ethereal to capture the PING session between two hosts. Provide the following information about the capture in your report:

   a) The IP addresses and MAC addresses of the hosts as reported by Ethereal.

   b) Any other activity that occurred when the PING was issued (for example, did an ARP occur?)

   c) Include the raw Ethereal capture data in your report. (To do this, capture the data, then use the "Print" command from within Ethereal, selecting a format of "Plain Text" and output of "File.")

6. See if you can PING any addresses outside of your LAN (the gateway at 10.9.69.1, for example). What happens when you do this, and why? Document this by capturing the attempt with Ethereal.

Laboratory Report Checklist:

The following contents are required in the laboratory report for this experiment:

- A drawing of your network, showing on each device the manufacturer's model number, and label of each port connected. For servers, give the station number of the server (on the bench below the box), and the hard drive number installed in the server.
- An inventory of the equipment needed to build your network (some of this information will duplicate the drawing information; that's expected.)
- A map (similar to Figure 1) giving the IP address allocation plan for your network.
- Results of IPCONFIG and PING tests with appropriate explanations.
- Procedure developed to ensure that PING is testing the proper hosts.
- Results of the Ethereal captures of Steps 5 and 6.
- A conclusion based upon the data you collected in the experiment.