Virginia Tech ■ ECE/CS 4570: Wireless Networks and Mobile Systems ■ Spring 2006

In-class Laboratory Exercise 10 (L10)

Part I – Objectives and Laboratory Materials

Objectives

The objectives of this in-class laboratory are to:

- ❑ Introduce you the operation of virtual private networks (VPN); and
- ❑ Introduce you to the operation of the Dynamic Host Configuration Protocol (DHCP) and IP masquerading, which is also known as network address translation (NAT).

After completing this assignment, you should be able to:

- ❑ Describe, in detail, the operation of VPNs, DHCP, and NAT; and
- ❑ Setup VPN connections in Windows XP systems.

Hardware to be used in this laboratory assignment

- ❑ One Dell Latitude C640 notebook computer (with a *fully charged* battery)
- ❑ One Xircom IEEE 802.11b wireless adapter
- ❑ One crossover Ethernet cable (this cable comes with the Intel Wireless Gateway)

In addition, the laboratory instructor will set up an access point for IEEE 802.11b and a notebook computer acting as a web server, as discussed below.

Software to be used in this laboratory assignment

- ❑ Microsoft Windows XP operating system
- ❑ Ethereal network analyzer tool

Part II – Pre-laboratory Assignment

This portion of the assignment should be completed ***prior*** to the in-class laboratory session.

- ❑ Read the following overview of VPNs: "Virtual Private Networking: An Overview," available at http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp.

Part III – In-class Laboratory Assignment

Overview

The in-class laboratory assignment includes the following two tasks, Task A and Task B.

Task A – Teams of three groups will work together on this task. Set up VPN connections between two Windows XP computers and monitor the operation and overhead of the VPN using Ethereal.

The network scenario is illustrated in Figure 1. The VPN server is connected to a private intranet (192.168.0.0/24) and a "public" intermediate network (10.10.1.0/24). To access resources in the private network, the VPN client must connect to the VPN server using a secured tunnel through the public network. When connected, the VPN client is assigned a private IP address of 192.168.0.*X*. By forwarding IP packets between the VPN clients and the intranet host, the VPN server allows the VPN client to communicate with intranet hosts as if it is directly connected to the private network.

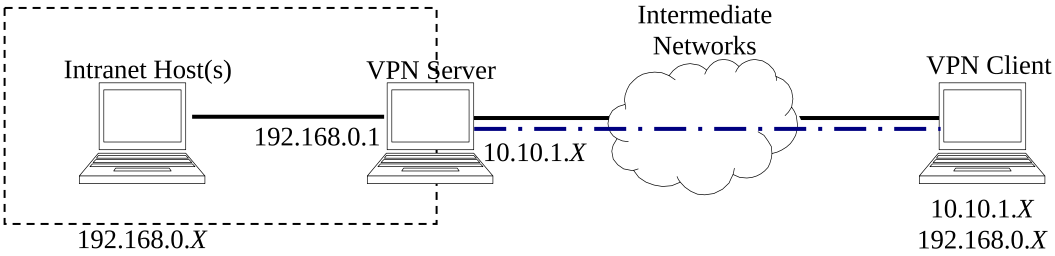


Figure 1. Network configuration for VPN experiment (Task A).

In this experiment, the VPN client will connect to the VPN server via an IEEE 802.11b access point that will be setup by the laboratory instructor. The intranet host will connect directly to the VPN server through an Ethernet interface using a crossover cable. The intermediate networks are omitted in this experiment for simplicity. Each team of three groups will setup an intranet host, a VPN server and a VPN client. Details are provided below.

Task B – Teams of two groups will work together on this task. Configure Internet Connection Sharing (ICS) and trace the operation of DHCP and NAT. The network configuration is illustrated in Figure 2.

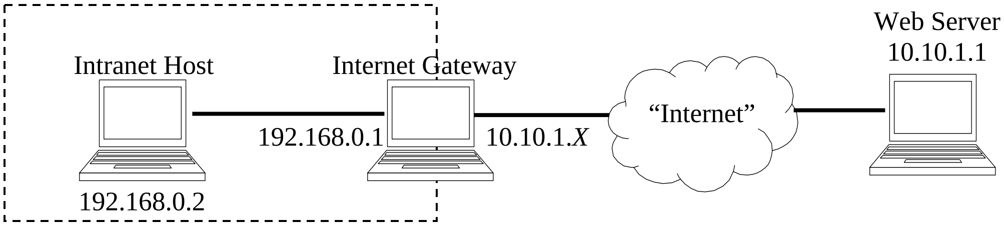


Figure 2. Network configuration for ICS experiment (Task B).

In this scenario, the Internet gateway and the Web server are connected to the pubic "Internet" (the 10.10.1.0/24 network is assumed to be public in this experiment). The intranet (192.168.0.0/24) cannot access the "internet" directly and the private addresses 192.168.0.*X* are not reachable from the public Internet. Network address translation (NAT) is used at the Internet gateway to provide connection to the Internet for hosts in the intranet. In Windows XP, NAT and DHCP are used to enable Internet Connection Sharing (ICS).

In this laboratory experiment, the Internet gateway is connected to the public web server via an IEEE 802.11b access point. Each team of two groups will setup the intranet host and the Internet gateway. The laboratory instructor will setup the public web server and the access point.

Details of Task A – Configuring a VPN and Monitoring the Operation and Overhead

VPN Server: First, configure the network interfaces and setup an incoming connection on the VPN server. This is done using the following three steps.

1. On the notebook computer that will serve as the VPN server, boot into Windows XP. If you have not done so, insert the Xircom IEEE 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet Client Utility*, choose the "Commands->Edit Properties" menu. In the "System Parameters" tab, fill in **ECECS4570** as SSID1 and select **Infrastructure** as the network type. In the "Network Security" tab, check the **Enable WEP** option and enable **Shared Key Authentication**.

   Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4570**.

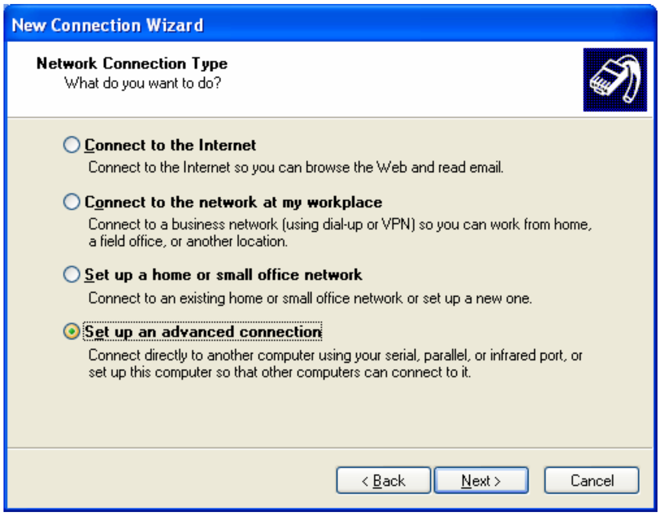
2. From the "Start" menu, open "Control Panel->Network Connections," right-click on "Wireless Network Connection," and then click "Properties." Highlight the item "Internet Protocol (TCP/IP)" and then click

“Properties.” In the “Internet Protocol Properties” dialog box, check “Obtain an IP address automatically” to enable DHCP. Then click “OK” to apply the changes. Open a command console, use the **“**ipconfig /all” command to verify that the “Wireless LAN” interface is properly configured. Check and record the assigned IP address, which will be the public address for your VPN server. Test the connection to the access point at IP address **10.10.1.1**.

In “Network Connections,” right-click “Local Area Connection” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Set the IP address as **192.168.0.1** and the subnet mask as **255.255.255.0**.

3. The following steps setup an incoming connection on the VPN server. In “Control Panel->Network Connections,” click “Create a new connection” under “Network Tasks” menu to start the New Connection Wizard. Click “Next.” (Note that if this is the first time for creating a VPN or dial-up connection, a “Location Information” dialog may appear. Input your area code to create the default location settings.)

   On the “Network Connections Type” dialog box, select **Set up an advanced connection** (as shown below) and then click **Next**.



New Connection Wizard

Network Connection Type
What do you want to do?

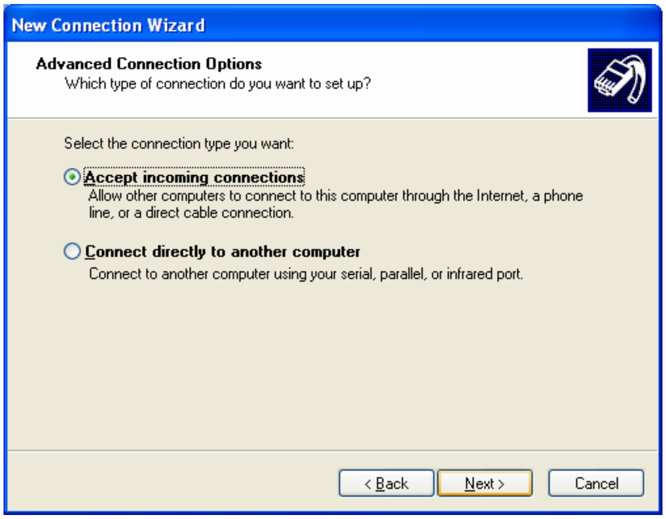
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

● **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

   On the “Advanced Connection Options” dialog box, select **Accept incoming connections** (as shown below) and then click **Next**.



New Connection Wizard

Advanced Connection Options
Which type of connection do you want to set up?

Select the connection type you want:

● **Accept incoming connections**
Allow other computers to connect to this computer through the Internet, a phone line, or a direct cable connection.

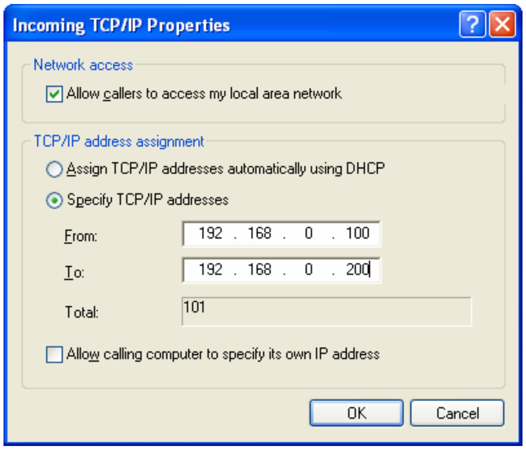
○ **Connect directly to another computer**
Connect to another computer using your serial, parallel, or infrared port.

On the “Devices for Incoming Connections” dialog box, do ***not*** select any device. Just click **Next**.

On the “Incoming Virtual Private Network (VPN) Connection” dialog box, select **Allow Private Connections**, and then click **Next**.

On the “User Permissions” dialog box, select **Administrator** to allow connection requests and then click **Next**.

On the “Networking Software” dialog box, select **Internet Protocol (TCP/IP)** and then click **Properties**. Setup TCP/IP as shown in the following figure.



Incoming TCP/IP Properties

Network access

☑ Allow callers to access my local area network

TCP/IP address assignment

○ Assign TCP/IP addresses automatically using DHCP

● Specify TCP/IP addresses

From: 192 . 168 . 0 . 100

To: 192 . 168 . 0 . 200

Total: 101

□ Allow calling computer to specify its own IP address

On the “Completing the Network Connection Wizard” dialog box, the default connection name is “Incoming Connections” and the name cannot be changed. Click **Finish** to close the dialog.

Intranet Host: The following two steps set up the intranet host.

1. On the notebook computer that serves as the intranet host, remove any wireless IEEE 802.11b card from the PC card slots. Use the crossover Ethernet cable to connect the intranet host and the VPN server via the wired Ethernet interface on each computer.

2. Boot Windows XP, open “Control Panel->Network Connections,” right-click “Local Area Connection,” and then click “Properties.**”** Highlight “Internet Protocol (TCP/IP)” and then click “Properties.” Setup the IP address as **192.168.0.2**, the default gateway as **192.168.0.1**, and the subnet mask as **255.255.255.0**. Click “OK” and close the dialog.

VPN Client: Setup the VPN client and create a VPN connection to the server using the following four steps.

1. On the notebook computer that serves as the VPN client, boot Windows XP. If you have not done so already, insert the Xircom IEEE 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet Client Utility*, choose the “Commands->Edit Properties” menu. In the “System Parameters” tab, fill in **ECECS4570** as SSID1 and choose **Infrastructure** as the network type. In the “Network Security” tab, check the “Enable WEP” option and enable **Shared Key Authentication**.

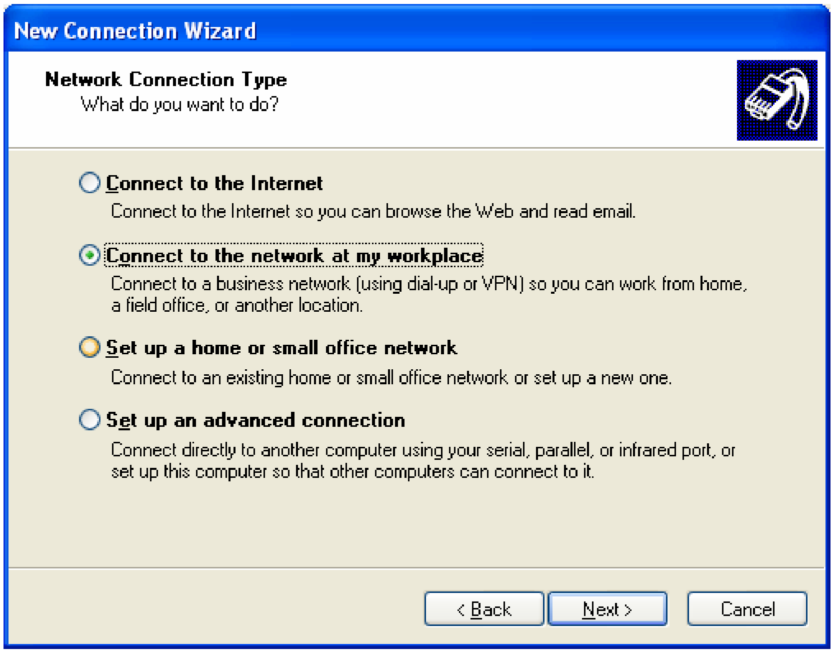
   Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4570**.

2. Open “Control Panel->Network Connections,” right-click “Wireless Network Connection,” and then click “Properties.” Highlight “Internet Protocol (TCP/IP)” and click “Properties.” Configure TCP/IP to use DHCP. From a command prompt, use the “*ipconfig /all*” command to verify that the “Wireless LAN” interface is properly configured and record the assigned IP address. Use the *ping* command to test the connection to the VPN server (10.10.1.*X*) of your team.

3. In “Network Connections,” click “Create a new connection” under the “Network Tasks” menu to start the “New Connection Wizard.” Click “Next.” (Note that if this is the first time creating a VPN or dial-

up connection on this computer, a “Location Information” dialog may appear. If so, input your area code to create the default location settings.)

On the “Network Connection Type” dialog box, select **Connect to the network at my workplace** as shown below and then click “Next”.



Network Connection Type

What do you want to do?

○ **Connect to the Internet**

Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**

Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**

Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**

Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

On the “Network Connection” dialog box, check **Virtual Private Network connection** and the click **Next**.

If the “Connection Name” dialog appears, type in your connection name and then click **Next**.

In the “VPN Server Selection” dialog box, type in the public IP address of the VPN server (10.10.1.*X*) to which you are attempting to connect and then click **Next**.

On the “Completing the Network Connection Wizard” dialog box, click **Finish**. The connection window will appear.

4. The “Connect XXX” dialog will appear. Click **Properties** to display the “VPN Properties” dialog. In the “Security” tab, check **Advanced (custom settings)** and click **Settings**. Select **No encryption allowed** for the “Data encryption” options. Click **OK** to close the dialog boxes. Encryption is an essential feature of a VPN, but we are disabling encryption here to allow us to use Ethereal to analyze the operation of the VPN.

After the three hosts are properly configured, use the Ethereal network analyzer to trace the operation and overhead of VPN using the following four steps.

1. Launch Ethereal on the VPN client, use menu “Capture->Start” to open the “Capture Options” dialog box. Select the IEEE 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Disable the **Capture packets in promiscuous mode** option and the **Enable network name resolution** option. Click **OK** to start tracing packets.

2. In the connection window, enter **Administrator** as the user name and **wireless** as the password. Then click **Connect** to establish the VPN connection. An icon for the VPN connection will appear in the system tray when connected.

   Use the “*ipconfig /all*” command to check the assigned IP address for the VPN client. The VPN client will have a virtual interface with a private IP address in the range of 192.168.0.100–192.168.0.200. Test the connection to the intranet gateway (with IP address 192.168.0.1) and the intranet host (with IP address 192.168.0.2).

3. Open a command prompt and ping host 192.168.0.2 to ensure the VPN is correctly configured.
4. Close the VPN connection. Stop tracing with Ethereal. Examine the packets transferred between the VPN client and the intranet host and answer the following questions.
    a) What tunneling protocol is used to establish the VPN connection, PPTP, L2TP, or IPSec?
    b) Identify the sequence of packet exchanges that establish the VPN connection.
    c) Examine some IP packets (such as ping request and reply messages) between the VPN client and the intranet host. Explain how these IP packets are encapsulated. Calculate the overhead (total bytes of the extra headers) of the VPN connection.

   Record your answers on the form at the end of this document and submit to the laboratory instructor. Have a laboratory instructor verify your results.

Details of Task B – Configuring ICS and Tracing the Operations of DHCP and NAT

Two notebook computers are used in this experiment.

1. On the notebook computer that will serve as the **Internet gateway**, boot into Windows XP. Insert the Xircom IEEE 802.11b adapter into one of the PC Card slots. Launch the *Xircom Wireless Ethernet Client Utility*, choose the "Commands->Edit Properties" menu. In the "System Parameters" tab, fill in **ECECS4570** as SSID1 and select **Infrastructure** as the network type. In the "Network Security" tab, check the **Enable WEP** option and enable **Shared Key Authentication.**

   Use the *Xircom Client Encryption Manager* to enter the default WEP key **ABCDEF4570.**
2. Connect the **Internet gateway computer** to the **intranet host** via a crossover Ethernet cable. On the Internet gateway computer, open "Control Panel->Network Connections," click on "Local Area Connection," and select "Properties." In the settings dialog, highlight "Internet Protocol (TCP/IP)" and then click "Properties." Check **Obtain an IP address automatically** to enable DHCP. Click **OK** to close the dialog boxes. Reboot the computers if prompted. On the **intranet host**, remove any wireless IEEE 802.11b card from the PC Card slots and configure the "Local Area Connection" interface to use DHCP in the same way.
3. On the **Internet gateway**, open "Control Panel->Network Connections," right-click "Wireless Network Connection," and then click "Properties." Click on the "Advanced" tab in the "Wireless Network Connection Properties**"** dialog, check **Allow other network users to connect through this computer's Internet connection** under **"**Internet Connection Sharing" menu**,** and then click **OK**.

   The wizard will automatically setup the wired Ethernet interface with IP address 192.168.0.1. DHCP and NAT will be enabled on this interface at the same time.
4. On the **Internet gateway**, open "Control Panel->Network Connections," right-click "Local Area Connection," and then click "Properties." Highlight "Internet Protocol (TCP/IP)" and then click "Properties." Verify that the interface was assigned a fixed IP address of **192.168.0.1** and a subnet mask of **255.255.255.0**.
5. On the **intranet host**, start Ethereal and begin tracing packets on the "Local Area Connection" interface (3Com EtherLink PCI). On the **Internet gateway**, start Ethereal and begin tracing packets on the IEEE 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Remember to disable the **Capture packets in promiscuous mode** option and the **Enable network name resolution** option.
6. On the **intranet host**, open a command console and execute the "*ipconfig /renew*" command to send a DHCP request to the internet gateway. Test the connection to the web server (with IP address 10.10.1.1) in the "Internet." Do this by start Internet Explorer and browsing the web page **http://10.10.1.1**.

7. On the **intranet host**, stop tracing with Ethereal. Examine the packet trace to locate and examine the following messages from the packet trace.

    a) The DHCP request message and the corresponding reply message. Record the fields in the reply message, such as client IP address, subnet mask, router, DNS server, lease time, etc.

    b) The TCP connections for the HTTP session. Record the source and destination IP addresses. What are the source and destination ports used for this HTTP session? Note that there may be multiple TCP connections.

    Record your responses on the form that is provided and submit your responses to the laboratory instructor.

8. On the **Internet gateway**, stop tracing with Ethereal. Examine the packet trace and answer the following questions.

    a) Locate the TCP connection for the HTTP session. Record the source and destination IP addresses. What are the source and destination ports used for this HTTP session?

    b) Compare the TCP packets from the intranet host and the TCP packets captured on the internet gateway. How does NAT work for the HTTP session?

    Record your responses on the form that is provided and submit your responses to the laboratory instructor.

Hint: You may want to repeat steps 5, 6 and 7 to understand the operation of NAT. Clear Internet Explorer's cache before you repeat these steps.

Virginia Tech ■ ECE/CS 4570: Wireless Networks and Mobile Systems ■ Spring 2006

In-class Laboratory Exercise 10 (L10)

Summary of Results

Group Members: ____ ID: ____________________________

____ ID: ____________________________

Group Number: ______

Task A, VPN Experiment

a) What tunneling protocol is used to establish the VPN connection, PPTP, L2TP, or IPSec?

b) Identify the sequence of packet exchanges that establish the VPN connection.

c) Examine some IP packets between the VPN client and the intranet host. Explain how these IP packets are encapsulated. Calculate the overhead (total bytes of the extra headers) of the VPN connection.

Task B, ICS Experiment

For the <u>intranet host</u> (step 7):

a) From the DHCP request message and the corresponding reply message, record the following fields in the reply message.

Client IP address: ______________________________________

Subnet mask: ______________________________________

Gateway router: ______________________________________

DNS server: ______________________________________

Lease time: ______________________________________

L10 Summary of Results (continued)

b) From one TCP connection request for the HTTP session, record the following information.

Source IP address: ____

Destination IP address: ____

Source port: ____

Destination port: ____

For the <u>Internet gateway</u> (step 8)

a) For the TCP connection request corresponding the one examined above, record the following information.

Source IP address: ____

Destination IP address: ____

Source port: ____

Destination port: ____

b) Compare the TCP packets from the intranet host and the TCP packets captured on the internet gateway. How does NAT work for the HTTP session?