ECE/CS 4984: Wireless Networks and Mobile Systems

Pre-lab and In-class Laboratory Exercise 10 (L10)

Part I – Objectives and Lab Materials

Objective

The objectives of this lab are to:

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

After completing the assignment, the students should be able to:

- Understand the operations of VPNs, DHCP, and NAT; and
- Setup VPN connections in Windows 2000 Professional systems.

Hardware to be used in this lab assignment

Each group needs the following hardware.

- One (1) Dell Latitude C640 notebook computer (*with a fully charged battery*)
- One (1) Xircom 802.11b wireless Ethernet adapter
- One (1) crossover Ethernet cable (*comes with the Intel Wireless Gateway*)

Software to be used in this lab assignment

- Microsoft Windows 2000 Professional operating systems
- Ethereal network analyzer tool

Part II – Pre-lab Assignment

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

- Read the following overview of VPN in Windows 2000: "Virtual Private Networking in Windows 2000: An Overview," available at http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/vpnoverview.asp.

Part III – In-class Lab Assignment

Overview

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

Task A – Teams of three groups will conduct the following tasks together. Setup VPN connections between two Windows 2000 Professional computers and monitor the operation and overhead of the VPN using Ethereal. The network scenario is illustrated in Figure 1.

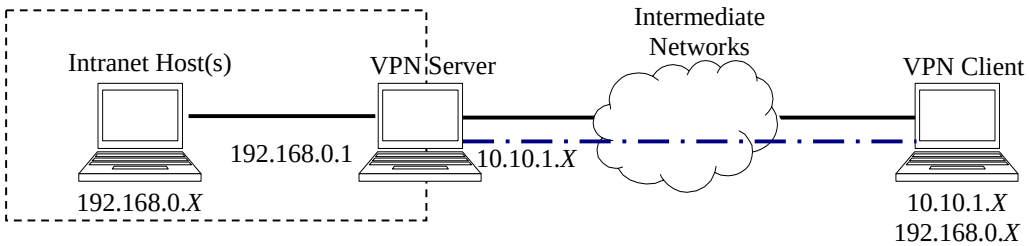


Figure 1. VPN network scenario.

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 with 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 hosts, the VPN server allows the VPN client to communicate with intranet hosts as if it is directly connected to the private network.

In this experiment, the VPN client will connect to the VPN server via an 802.11b access point that will be setup by the GTA. The intranet host will connect directly to the VPN server through an Ethernet interface. The intermediate networks are omitted in this experiment for simplicity. Each team will setup an intranet host, a VPN server and a VPN client.

Task B – Teams of two groups will conduct the following tasks together. Configure Internet Connection Sharing (ICS) and trace the operation of DHCP and NAT. The network scenario is illustrated in Figure 2.

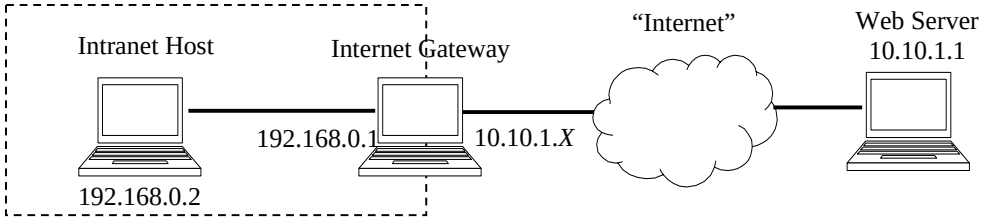


Figure 2. Network diagram for ICS.

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. Networking address translation (NAT) is used at the Internet gateway to provide connection to the Internet for hosts in the intranet. In Windows 2000, NAT and DHCP are used to enable Internet Connection Sharing (ICS).

In this lab experiment, the Internet gateway is connected to the public web server via an 802.11b access point. Each team will setup the intranet host and the Internet gateway. The GTA will setup the public web server and the access point.

Details of Task A – Configure a VPN and Monitor Operation and Overhead

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

1. On the notebook computer that will serve as the VPN server, boot into Windows 2000. If you have not done so, insert the Xircom 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 **ECECS4984** 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 **ABCDEF4984**.

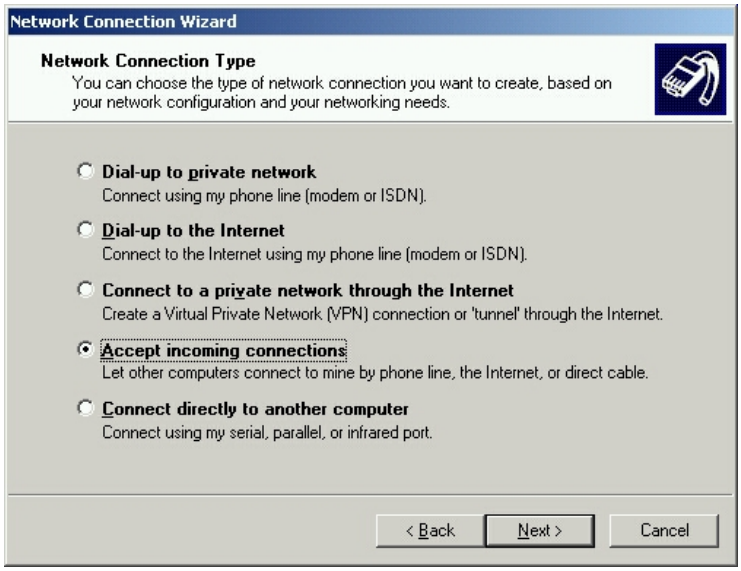
2. From the "Start" menu, open "Settings->Network and Dial-up Connections," right-click on "Wireless LAN," and then click "Properties." Highlight the item "Internet Protocol (TCP/IP)" and then click "Properties." In the "Internet Protocol Properties" dialog box, check "Obtain an IP address automatically" 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 and Dial-up Connections," right-click "Local Area Network" 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 “Settings->Network and Dial-up Connections,” click “Make New Connection**”** to start the Network 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 **Accept Incoming Connections** (as shown in the figure below), and then click “Next.”

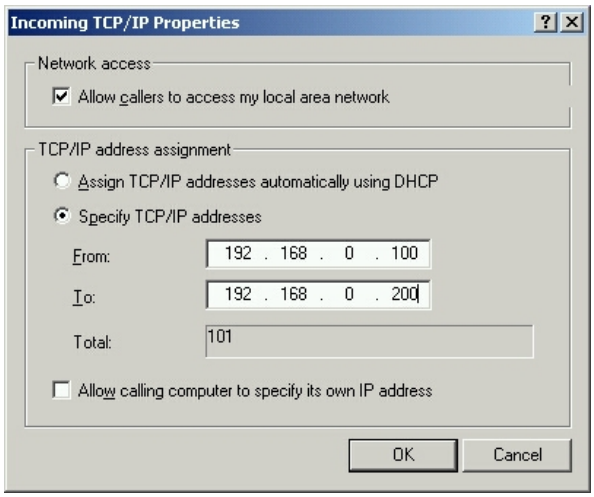


   On the “Devices for Incoming Connections” dialog box, do **NOT** select any device. Just click “Next.”

   On the “Incoming Virtual Private Connection” dialog box, click **Allow Private Connections**, and then click “Next”.

   On the “Allowed Users” dialog box, select **Administrator** to allow connection requests. Click “Next.”

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



   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.

The following two steps set up the **intranet host**.

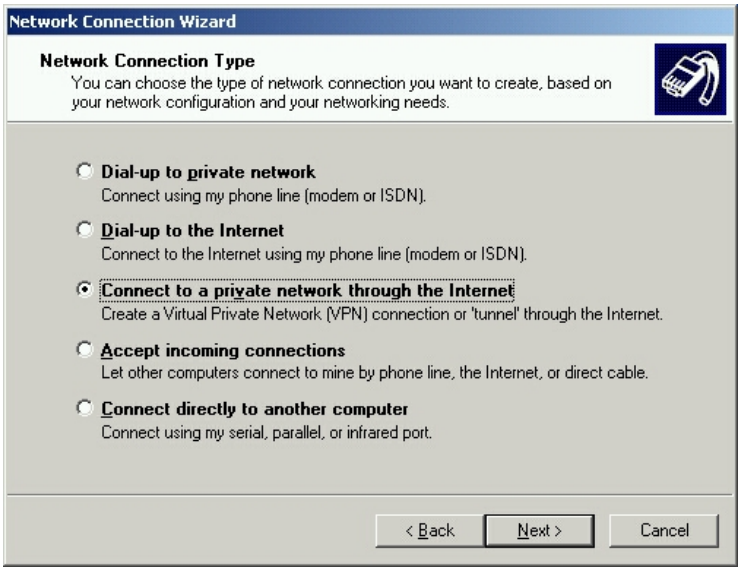
1. On the notebook computer that serves as the intranet host, remove any wireless 802.11b card from the PC card slots. Use the crossover Ethernet cable to connect the intranet host and the VPN server via the wired Ethernet interface on each computer.
2. Boot Windows 2000, open "Settings->Network and Dial-up Connections," right-click "Local Area Network," 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.

Setup the **VPN client** and create a VPN connection to the server according to the following four steps.

1. On the notebook computer that serves as the VPN client, boot Windows 2000. If you have not done so already, insert the Xircom 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 **ECECS4984** 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 **ABCDEF4984**.
2. Open "Settings->Network and Dial-up Connections," right-click "Wireless LAN," and then click "Properties." Highlight "Internet Protocol (TCP/IP)" and click "Properties." Configure TCP/IP to use DHCP. 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 and Dial-up Connections," double-click "Make New Connections" 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 Private Network through Internet** as shown below and then click "Next".



   If the "Public Network" dialog appears, select "Do not dial the initial connection" option and then click "Next."

   In the "Destination Address" 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 "Connection Availability" dialog box, check **Only for Myself** and the click "Next."

On the "Completing the Network Connection Wizard" dialog box, accept **Virtual Private Connection** as the default connection name and then click "Finish." The "Connect Virtual Private Connection" dialog will appear.

4. The "Connect Virtual Private Connection" dialog will appear. Click "Properties" to display the VPN settings dialog. In "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 in order to analyze the operations in the VPN with Ethereal.

Use Ethereal network analyzer to trace the operation and overhead of VPN according to the following four steps.

1. Launch Ethereal on the VPN client, use menu "Capture->Start" to open the "Capture Options" dialog box. Select the 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Disable the **Capture packets in promiscuous mode** and **Enable network name resolution** options. Click "OK" to start tracing packets.
2. In the "Connect Virtual Private Connection" dialog box, 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. Start Windows Explorer and enter "\\192.168.0.2\" in the address bar. You should be able to find the shared resources on that computer (printers, scheduled tasks, shared folders, etc.).
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.
   1) What tunneling protocol is used to establish the VPN connection, PPTP, L2TP, or IPSec?
   2) Identify the sequence of packet exchanges that establish the VPN connection.
   3) Examine some IP packets (such as ping request/reply) 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.

   Have the GTA verify your results.

Details of Task B – Configure ICS and Trace the Operations of DHCP and NAT

Two notebook computers are used in the following procedures.

1. On the notebook computer that will serve as the **Internet gateway**, boot into Windows 2000. Insert the Xircom 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 **ECECS4984** 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 **ABCDEF4984.**
2. Connect the **Internet gateway computer** to the **intranet host** via a crossover Ethernet cable. On the Internet gateway computer, open "Settings->Network and Dial-up Connections," click on "Local Area Network," 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 802.11b card from the PC card slots and configure the "Local Area Network" interface to use DHCP in the same way.

3. On the **Internet gateway**, open "Settings->Network and Dial-up Connections," right-click "Wireless LAN," and then click "Properties." Click on the "Sharing" tab in the "Wireless LAN Properties**"** dialog, check **Enable Internet Connection Sharing for this connection,** and then click "OK." When prompted for confirmation, 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 "Settings->Network and Dial-up Connections," right-click "Local Area Network," 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 Network" interface (3Com EtherLink PCI). On the **Internet gateway**, start Ethereal Network Analyzer and begin tracing packets on the 802.11b wireless interface (Cisco 340 Series Wireless LAN Adapter). Remember to enable the **Capture packets in promiscuous mode** and **Enable network name resolution** options.

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." Start Internet Explorer and browse 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.

   1) 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.

   2) 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.

8. One the internet gateway, stop tracing with Ethereal. Examine the packet trace and answer the following questions.

   1) 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?

   2) 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?

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