CHAPTER 5

Networking

Networking Resources

Overview

Windows 2000 Server includes a variety of network protocols and technologies to extend the capabilities of your server.

DHCP with DNS and Active Directory

Dynamic Host Configuration Protocol (DHCP) works with DNS and Active Directory on IP networks, helping to free you from assigning and tracking static IP addresses. DHCP dynamically assigns IP addresses to computers or other resources connected to an IP network.

Internet Connection Sharing

With the Internet connection sharing feature of Network and Dial-up Connections, you can use Windows 2000 to connect your home network or small office network to the Internet. For example, you might have a home network that connects to the Internet by using a dial-up connection. By enabling Internet connection sharing on the computer that uses the dial-up connection, you are providing network address

translation, addressing, and name resolution services for all computers on your home network.

Network Address Translation

Network Address Translation (NAT) hides internally managed IP addresses from external networks by translating private internal addresses to public external addresses. This reduces IP address registration costs by letting you use unregistered IP addresses internally, with translation to a small number of registered IP addresses externally. It also hides the internal network structure, reducing the risk of attacks against internal systems.

Virtual Private Networking

You can allow users ready access to the network even when they're out of the office, and reduce the cost of such access, by implementing a Virtual Private Network (VPN). VPNs enable users to easily and securely connect to the corporate network. The connection is through a local ISP, which reduces connect-time charges.

With Windows 2000 Server, you can use several new, more secure protocols for creating Virtual Private Networks, including:

- Layer 2 Tunneling Protocol (L2TP), a more secure version of Point-to-Point Tunneling Protocol (PPTP). L2TP is used for tunneling, address assignment, and authentication.
- Internet Protocol Security (IPSec), a standard-based protocol that provides the highest levels of VPN security. Using IPSec, virtually everything above the networking layer can be encrypted.

Routing and Remote Access service

Routing and Remote Access service is a single integrated service that terminates connections from either dial-up or VPN clients, or provides routing (IP, IPX, and AppleTalk), or both. With Routing and Remote Access service, your Windows 2000 server can function as a remote access server, a VPN server, a gateway, or a branch-office router.

When providing remote access, Routing and Remote Access service supports PPP (the standard dial-up protocol). It also supports the new Extensible Authentication Protocol to enable vendor-provided authentication methods for remote clients (such

as retina scan).

When working as a router, Routing and Remote Access service supports both local (LAN-to-LAN) routing and remote (demand-dial) routing. In addition to physical dial-up, frame relay, ISDN, or X.25 connections, the connection can be in the form of a direct connection to the corporate network or a point-to-point, branch office VPN connection through the Internet. Routing and Remote Access service supports the OSPF and RIP2 routing control protocols for IP networks and both RIP and SAP for IPX networks. The range of routing and gateway services included in Windows 2000 Server allow you to create flexible connections between branch offices (or perimeter networks) and the corporate network.

Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a high-speed connection-oriented protocol designed to transport multiple types of traffic across a network. It is applicable to both LANs and WANs. Using ATM, your network can simultaneously transport a wide variety of network traffic: voice, data, image, and video.

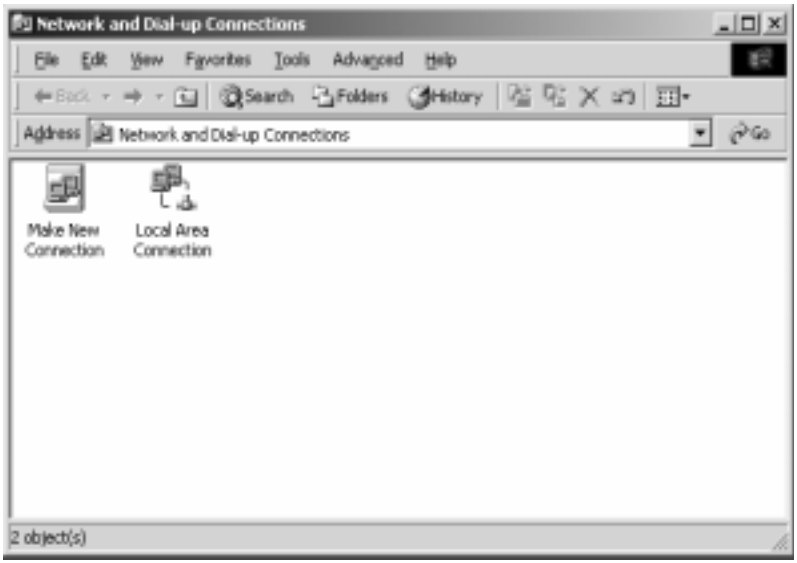
Fibre Channel

Fibre Channel is a technology for 1-gigabit-per-second data transfer that maps common transport protocols such as SCSI and IP, merging networking and high-speed I/O into a single connectivity technology. Fibre Channel technology gives you a way to address the distance and the address-space limitations of conventional channel technologies.

General Configuration

Setting up Windows 2000 to work in our network is becoming less complicated. Our campus is moving to DHCP which will require less configuration on our part to make computers communicate with one another. It is this environment that we will explore through the following examples.

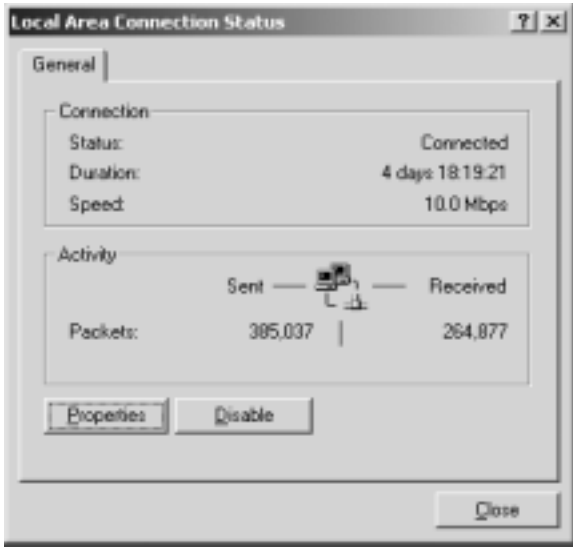
To get to your network configuration go to Start > Settings > Network and Dialup connections. You will see the following window displayed:



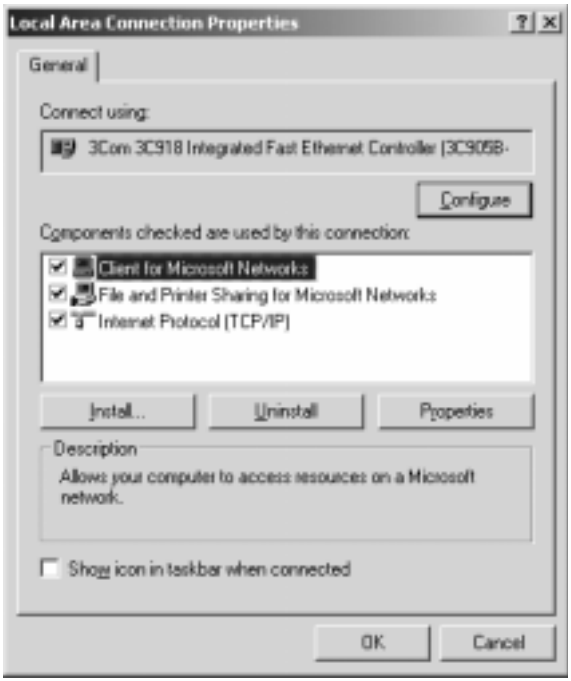
At this point the two options available to you are:

1. Create a new connection
2. Configure the current network connection

We will not look at creating a new connection at this point. Lets look at the current configuration.



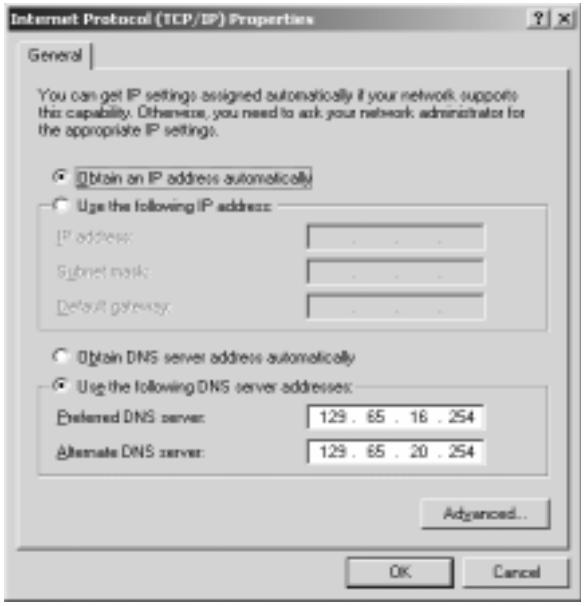
This window is valuable for checking the current condition of your connection. You can tell if you are connected, how long you've been connected, at what speed your connected, and how many packets have been sent and received. These are all of the basic vital statistics that help you to determine if you need to adjust the configuration of your network settings.



Within the properties settings you will find the basic components that make up your network connection. In this example you will see that we are using the Default Microsoft client with file and print sharing with TCP/IP as the protocol[11]. If we added Novell's Netware client, this would be the place you would see changes made. The client would be changed to the Novell Netware client and possibly IPX/SPX would be added to the protocol stack.

11. In information technology, a protocol (pronounced PROH-tuh-cahl, from the Greek *protocollon*, which was a leaf of paper glued to a manuscript volume, describing its contents) is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard.

There is one other item on this window you should be made aware of -- the check-mark box at the bottom of the window “Show icon in the taskbar when connected”. This is a very useful icon on your taskbar -- it lets you know the condition of your network connection.



Selecting the TCP/IP Properties will open this window. The window is broken down into two main groups:

1. IP
2. DNS

The IP address in this example is gained by accessing the DHCP server (who then grants an IP address if one is available at that time). Otherwise you would have to order an IP address through NetAdmin. NetAdmin would then render you an IP address, subnet mask and gateway. Prior to calling NetAdmin, you will have to get

the hardware address for your system (referred to as the Mac[12] Address). To do so you will have to run the IPCONFIG /ALL command from the command prompt.

Open the command prompt through the START menu:

START > RUN

Type in CMD and hit the return key.

In this example, you can find the Mac address labeled “Physical Address”. This number is unique for every NIC[13]. You will notice that there is other information displayed here as well as the physical address. It is a good idea to record all of this information. Using DHCP will change your IP address but not the other information.

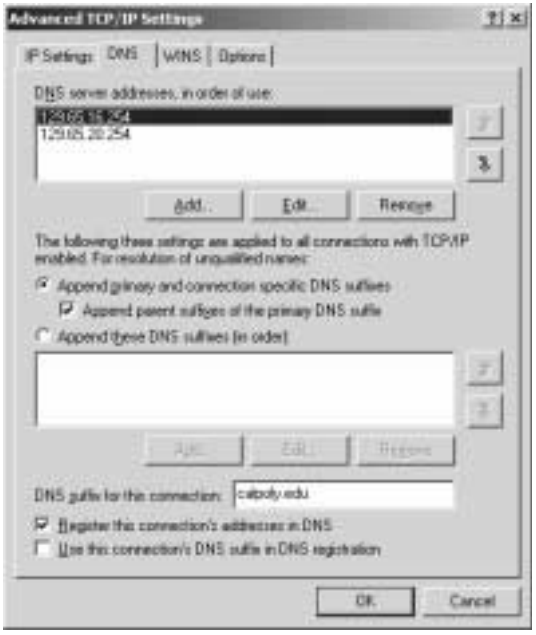
Type exit at the c:\> propmt to close this window.

12.Mac - Machine

If you click on the Advanced button you will get the next window example:

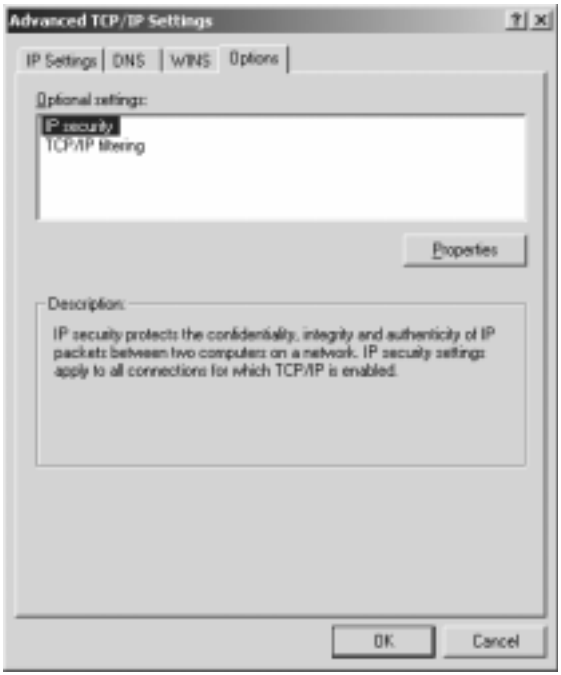
13.A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or token ring. Network interface cards provide a dedicated, full-time connection to a network. Most home and portable computers connect to the Internet through as-needed dial-up connection. The modem provides the connection interface to the Internet service provider.

You will notice that your IP settings are, in fact, DHCP Enabled. No other information is needed here for the network connection to function. Click on DNS to continue.



The information in DNS may not be required in order for DNS to work. DHCP, when set properly, will provide all of the information (including DNS). In this example we have physically set DNS.

WINS is not required for Windows 2000 and should be disabled. However, there may be times when you need to activate your LMHost file in order to connect with servers or workstations that may not be in your DNS scope. Adding their addresses to the LMHost file will give you the ability to see IP Hosts not registered by your DNS server. We will not go into how to edit you LMHost file here.



In the options tab you will find that we have IPSecurity enabled as well as TCP/IP filtering.