D-Link DI-704P

Express Ethernetwork™ Broadband Router

Manual

Rev. 061302

D-Link
Building Networks for People

Contents

Package Contents

Contents of Package:

- **D-Link DI-704P** Express Ethernetwork^{TM} Broadband Router
- AC Power Adapter, 5V/2A
- Ethernet (CAT5-UTP/Straight-Through) Cable
- Manual on CD
- Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the DI-704P will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

System Requirements:

- Computer with a Windows, Macintosh, or Unix based operating system with an installed Ethernet adapter
- Internet Explorer or Netscape Navigator, version 4.0 or above, with JavaScript enabled

Introduction

Congratulations on your purchase of this outstanding Broadband Router. The DI-704P is specifically designed for Small Office and Home Office needs. It provides a complete solution for Internet surfing and office resources sharing, and it is easy to configure and operate for even non-technical users. Instructions for installing and configuring the DI-704P can be found in the enclosed *Quick Install Guide*. Before you install and use the DI-704P, please read this manual carefully for more detailed information and to fully utilize its functions.

Features and Benefits

- **Broadband modem and IP sharing**
  Connects multiple computers to a broadband (cable or DSL) modem to surf the Internet.

- **Auto-sensing Ethernet Switch**
  Equipped with a 4-port auto-sensing Ethernet switch.

- **VPN Pass-Through supported**
  Supports pass-through PPTP sessions and allows you to setup VPN server and VPN clients.

- **Printer sharing (Optional)**
  Embeds a print server to allow all of the networked computers to share one printer.

- **Firewall**
  All unwanted packets from outside intruders are blocked to protect your network.

- **DHCP server supported**
  All of the networked computers can retrieve TCP/IP settings automatically from the DI-704P.

- **Web-based configuration**
  Configurable through any networked computer's web browser using Netscape or Internet Explorer.

- **Access Control supported**
  Allows you to assign different access rights for different users.

- **Packet filter supported**
  Packet Filter allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Virtual Server supported**
  Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.

- **User-Definable Application Sensing Tunnel**
  User can define the attributes to support special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on. The DI-704P can sense the application type and open a multi-port tunnel for it.

- **DMZ Host supported**
  Allows a networked computer to be fully exposed to the Internet; this function is used when the special "application-sensing tunnel feature" is insufficient to allow an application to function correctly.

Introduction to Broadband Router Technology

A router is a device that forwards data packets from a source to a destination. Routers forward data packets using IP addresses and not a MAC address. A router will forward data from the Internet to a particular computer on your LAN.

The information that makes up the Internet gets moved around using routers. When you click on a link on a web page, you send a request to a server to show you the next page. The information that is sent and received from your computer is moved from your computer to the server using routers. A router also determines the best route that your information should follow to ensure that the information is delivered properly.

A router controls the amount of data that is sent through your network by eliminating information that should not be there. This provides security for the computers connected to your router, because computers from the outside cannot access or send information directly to any computer on your network. The router determines which computer the information should be forwarded to and sends it. If the information is not intended for any computer on your network, the data is discarded. This keeps any unwanted or harmful information from accessing or damaging your network.

Introduction to Firewalls

A firewall is a device that sits between your computer and the Internet that prevents unauthorized access to or from your network. A firewall can be a computer using firewall software or a special piece of hardware built specifically to act as a firewall. In most circumstances, a firewall is used to prevent unauthorized Internet users from accessing private networks or corporate LAN's and Intranets.

A firewall watches all of the information moving to and from your network and analyzes each piece of data. Each piece of data is checked against a set of criteria that the administrator configures. If any data does not meet the criteria, that data is blocked and discarded. If the data meets the criteria, the data is passed through. This method is called packet filtering.

A firewall can also run specific security functions based on the type of application or type of port that is being used. For example, a firewall can be configured to work with an FTP or Telnet server. Or a firewall can be configured to work with specific UDP or TCP ports to allow certain applications or games to work properly over the Internet.

Introduction to Local Area Networking

Local Area Networking (LAN) is the term used when connecting several computers together over a small area such as a building or group of buildings. LAN's can be connected over large areas. A collection of LAN's connected over a large area is called a Wide Area Network (WAN).

A LAN consists of multiple computers connected to each other. There are many types of media that can connect computers together. The most common media is CAT5 cable (UTP or STP twisted pair wire.) On the other hand, wireless networks do not use wires; instead they communicate over radio waves. Each computer must have a Network Interface Card (NIC), which communicates the data between computers. A NIC is usually a 10Mbps network card, or 10/100Mbps network card, or a wireless network card.

Most networks use hardware devices such as hubs or switches that each cable can be connected to in order to continue the connection between computers. A hub simply takes any data arriving through each port and forwards the data to all other ports. A switch is more sophisticated, in that a switch can determine the destination port for a specific piece of data. A switch minimizes network traffic overhead and speeds up the communication over a network.

Networks take some time in order to plan and implement correctly. There are many ways to configure your network. You may want to take some time to determine the best network set-up for your needs.

Introduction to Virtual Private Networking

Virtual Private Networking (VPN) uses a publicly wired network (the Internet) to securely connect two different networks as if they were the same network. For example, an employee can access the corporate network from home using VPN, allowing the employee to access files and printers. Here are several different implementations of VPN that can be used.

Point-to-Point Tunneling Protocol (PPTP)

PPTP uses proprietary means of connecting two private networks over the Internet. PPTP is a way of securing the information that is communicated between networks. PPTP secures information by encrypting the data inside of a packet.

IP Security (IPSec)

IPSec provides a more secure network-to-network connection across the Internet or a Wide Area Network (WAN). IPSec encrypts all communication between the client and server whereas PPTP only encrypts the data packets.

Both of these VPN implementations are used because there is not a standard for VPN server software. Because of this, each ISP or business can implement its own VPN network making interoperability a challenge.

LEDS

M1&M2   System status indicators, Orange. M1 is flashed once per second to indicate an active system. When the system is busy, M2 lights up.

WAN & LAN   Ethernet port indicators, Green. The LED flickers when the LAN or WAN port is sending or receiving data.

Link/Act. Link status indicators, Green. The LED flickers when the corresponding port is sending or receiving data

10/100 10/100 status indicators, Green. The LED flickers when the corresponding port is transmitting or receiving data in 10 or 100Mbps.

CONNECTIONS
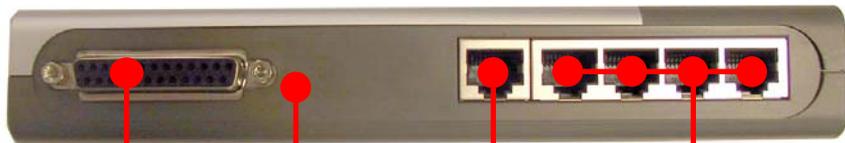
Printer Port   **Reset**   **WAN port**   **LAN ports (1-4)**

Getting Started

The **Infrastructure Network** example shown contains the following D-Link network devices:

Express Ethernetwork^{TM} Broadband Router - **D-Link DI-704P**
A laptop computer with an Ethernet adapter - **D-Link DFE-670TXD**
A desktop computer with an Ethernet adapter - **D-Link DFE-530TX+**
A Cable modem - **D-Link DCM-200**
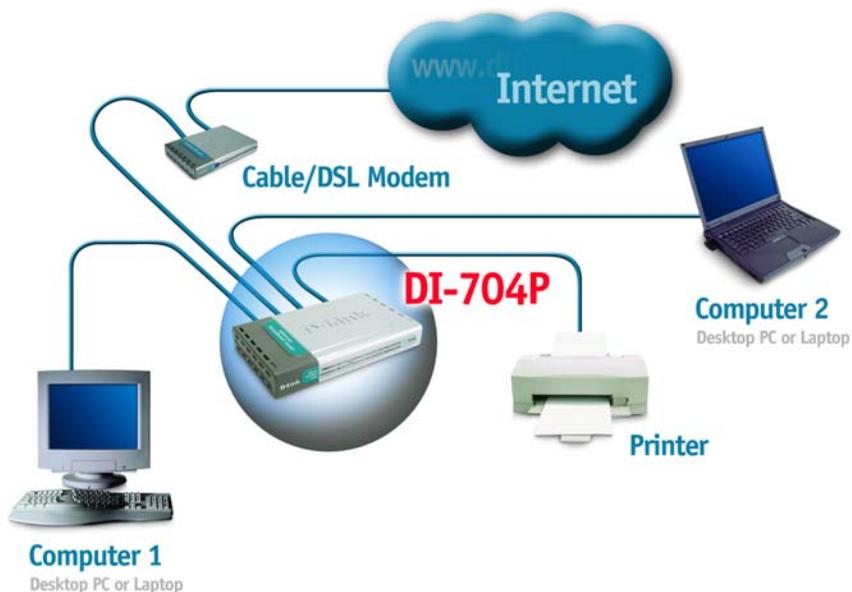
Using the Configuration Wizard

The DI-704P provides Web based configuration. You can configure your DI-704P through your Netscape Communicator or Internet Explorer browser in MS Windows, Macintosh or UNIX based platforms.

Activate your browser. Then type the IP address of the DI-704P into the *Location* (for Netscape) or *Address* (for IE) field and press "**Enter**." For example: **http://192.168.0.1**.

- Open the web browser
- Type in the **IP Address** of the DI-704P
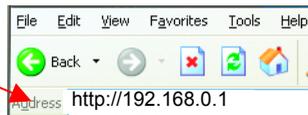
(The IP Address shown in the example above is the default setting. If you have changed the IP Address of the DI-704P to conform to a network, then input that IP Address in the web browser, instead of the default IP Address shown.)

- Type **admin** in the **User Name** field (lower case)
- Leave the **Password** blank
- Click **OK**

This screen will appear. Click **Run Wizard**.
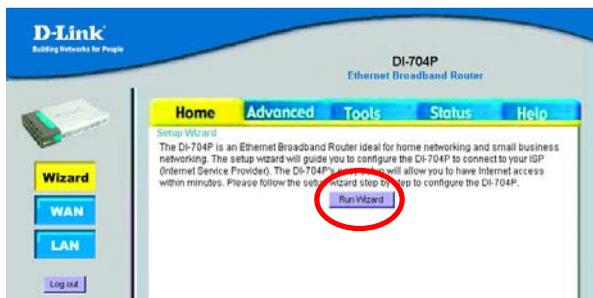
The **Setup Wizard** screen will appear. Follow the Wizard step by step to quickly configure the DI-704P.

Click **Next**

It is recommended that you change the admin password for security purposes. Enter in your new password. Enter it in a second time for verification.

Click Next

In the window below, select the method you use to connect to the Internet. This is called the WAN connection or WAN Type.

Static IP Address: *Select this option to manually input the IP address that your ISP assigned to you. (*Please see *Assigning a Static IP Address* in the **Troubleshooting** section of this manual.)

Dynamic IP Address: *(e.g., Cable users)*
Select this option to obtain an IP address automatically from your ISP. Please see Dynamic IP Address section.

Dynamic IP Address with Road Runner Session Management: (e.g., Telstra BigPond users) Choose this option if it is required by your ISP

PPP over Ethernet (PPPoE): *(e.g., DSL users) Select this option if your ISP requires the use of PPPoE to connect to their services.* Please see PPPoE section.

PPTP: Select this option if your ISP requires it
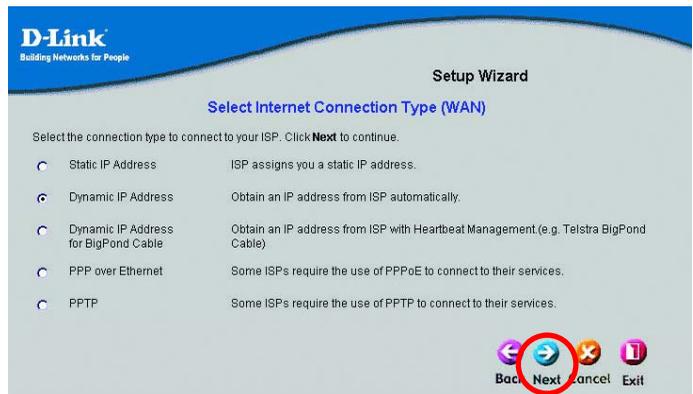
Once you have made the appropriate selection, click **Next**.

Static IP Address

If you selected **Static IP Address**, you will see the following page.

Enter in the IP address information provided to you by your ISP. You will need to enter in WAN IP Address, WAN Subnet Mask, WAN Gateway, and Primary DNS.

Click **Next**

Dynamic IP Address

If you selected **Dynamic IP Address**, you will see the following page.

If your ISP requires you to enter a specific host name or specific MAC address, please enter it in. The CLONE MAC Address button is used to copy the MAC address of your Ethernet adapter to the DI-704P WAN interface.

Click **Next**

Dynamic IP Address for BigPond Cable

If you selected **Dynamic IP Address with RoadRunner Session Management**, you will see the following page.

If your ISP requires you to enter a specific host name or specific MAC address, please enter it in. The CLONE MAC Address button is used to copy the MAC address of your Ethernet adapter to the DI-704P WAN interface.

Click **Next**

PPPoE

If you select PPP over Ethernet (PPPoE), you will see the following page.
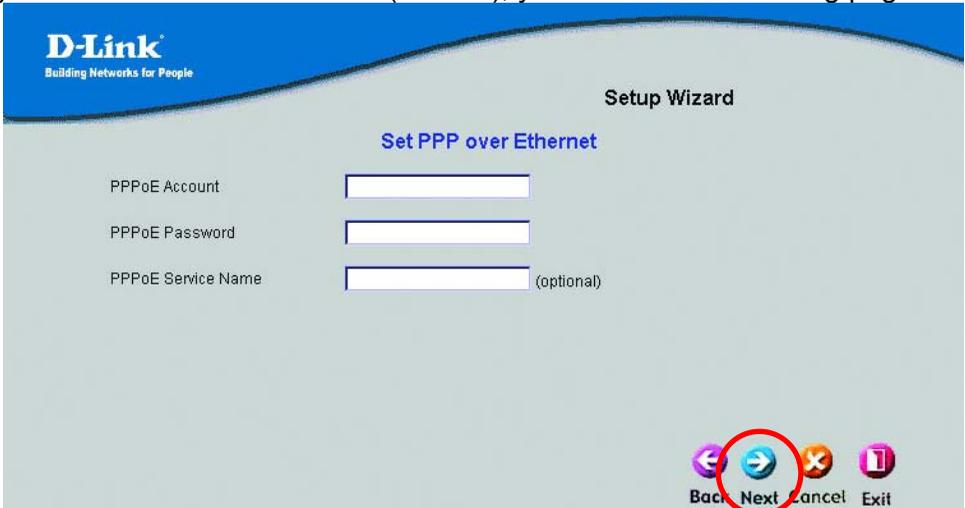
Enter in the username and password provided to you by your ISP.
Enter in the Service Name if your ISP uses a Service Name for the PPPoE connection.
Click **Next**

PPTP

If you selected PPTP, fill out the required information, provided to you by your ISP.
Click **Next**

At this point, the **Setup Wizard** has completed. Click **Restart** to save the settings and reboot the DI-704P.

The DI-704P will save the changes and reboot.

You have completed the Setup Wizard.
You can now access the Internet.

Whenever you choose to make changes or additions to the configuration of the DI-704P, you can access the Configuration menu by typing the IP Address of the DI-704P into the address line of your web browser and pressing "enter." Read more about the Configuration menu in the following chapter.

Using the Configuration Menu

Setup Wizard

The Setup Wizard page is the first page that appears when logging into the web-based management interface. The Setup Wizard is a utility used to quickly configure the DI-704P. It will guide you through three quick and basic steps to help you connect to your ISP. You will be connected to your ISP (Internet Service Provider) and have Internet access within minutes.
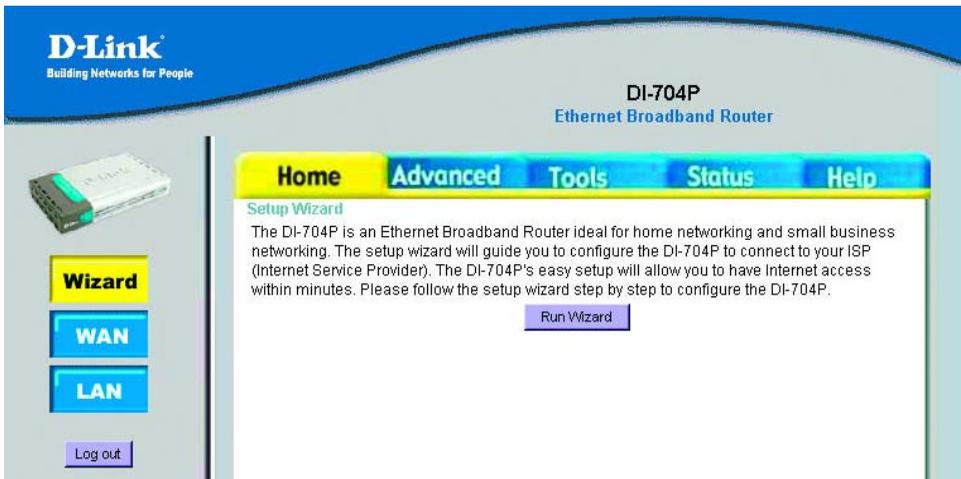
WAN

WAN is short for Wide Area Network. The WAN settings can be referred to as the Public settings. All IP information in the WAN settings are public IP addresses which are accessible on the Internet.

The WAN settings consist of these options: *Dynamic IP Address*, *Dynamic IP (w/RoadRunner,) Static IP Address*, *PPPoE, and PPTP*. Select the appropriate option and fill in the information needed to connect to your ISP.

Choose Dynamic IP Address to obtain IP address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

Host Name: The Host Name field is optional but may be required by some ISPs. The host name is the device name of the Broadband Router.

Click **Apply** if you have made changes.

Choose Static IP Address if all WAN IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

**WAN IP Address:** Public IP address provided by your ISP.

WAN Subnet Mask: Subnet mask provided by your ISP.

WAN Gateway Address: Public IP address of your ISP that you are connecting to.

Primary DNS Address: Primary DNS (Domain Name Server) IP provided by your ISP

Secondary DNS Address: optional

Click **Apply** if you have made changes.

HOME > WAN > PPPOE
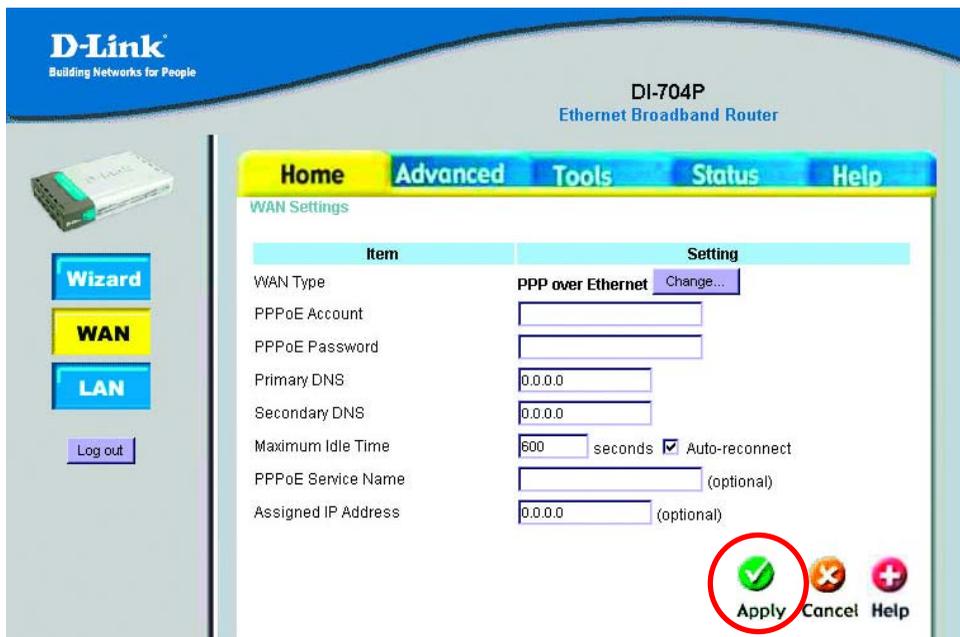
Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

PPPoE Account: Your PPPoE account is provided by your ISP

PPPoE Password: Your PPPoE password is provided by your ISP

**Primary DNS Address:** Primary DNS IP Address is provided by your ISP

Secondary DNS Address: optional

Maximum Idle Time: The amount of time of inactivity before disconnecting your PPPoE session. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then the connection will be dropped. Either set this to zero or enable Auto-reconnect to disable this feature.

PPPoE Service Name: *Enter the Service Name provided by your ISP. (optional)*

Assigned IP Address: This option is only available for Static PPPoE. Enter in the Static IP Address for the PPPoE connection.

Click **Apply** if you have made changes.
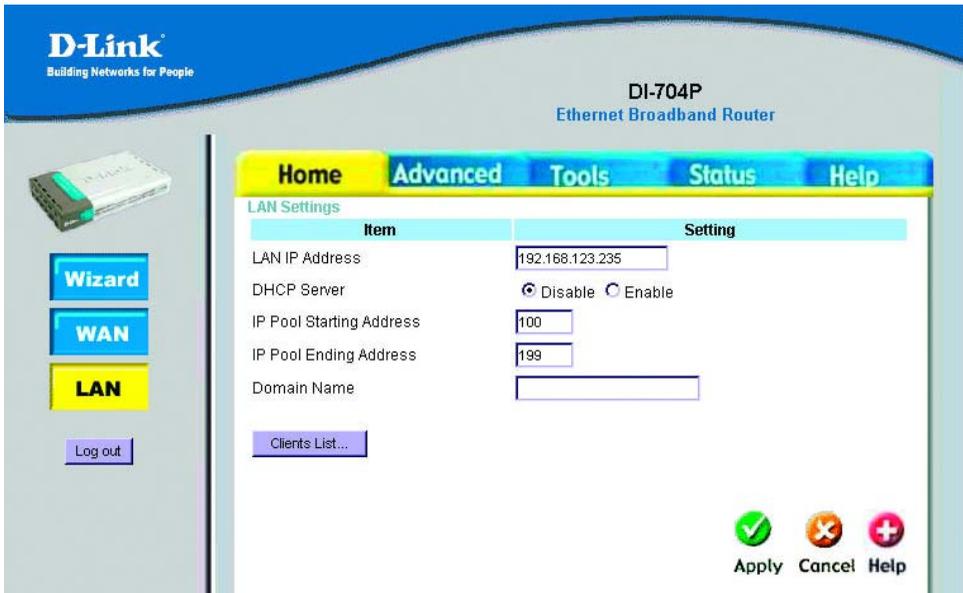
LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DI-704P. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

LAN IP Address: The IP address of the LAN interface. The default IP address is 192.168.0.1.

DHCP Server: Choose **Enable** or **Disable**

The range of the IP Address Pool: Whenever there is a request, the DHCP server will automatically allocate an unused IP Address from the *IP Address Pool* to the requesting computer. You must specify the starting and ending address of the IP Address pool.

Domain Name: This field is optional. Enter in the your local domain name.

Click **Apply** if you have made any changes.

DHCP stands for Dynamic Host Control Protocol. The DI-704P has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DI-704P. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

ADVANCED > VIRTUAL SERVER

The firewall filters out unrecognized packets to protect your LAN (local area network); so all computers networked with the DI-704P are invisible to the outside world. If you wish, you can make some of them accessible by enabling the *Virtual Server Mapping.*

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**.

For example, if you have an FTP server (port 21) at 192.168.0.1, a Web server (port 80) at 192.168.0.2, and a VPN server at 192.168.0.6, then you need to specify the following virtual server-mapping table:

Service Port	Server IP	Enable
21	192.168.0.1	V
80	192.168.0.2	V
1723	192.168.0.6	V

ADVANCED > APPLICATIONS

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony and so on. Due to the firewall function, these applications cannot work without some intervention. **Special Applications** makes some of these applications work with the DI-704P. If **Special Applications** is still insufficient to allow an application to function correctly, try the **DMZ Host** in the **Miscellaneous Items** options.

*Trigger*: the outbound port number the application issued first.

Incoming Ports: when the trigger packet is detected, the inbound packets to the specified port numbers are allowed to pass the firewall.

The DI-704P provides some predefined settings in the gray pad on the bottom of the web page. Select your application in the **Popular applications** pull-down menu and click **Copy to** in order to copy the predefined setting.

Note! At any time, only one PC can use each Special Application tunnel.

Click **Apply** if you have made any changes.

ADVANCED > FILTER
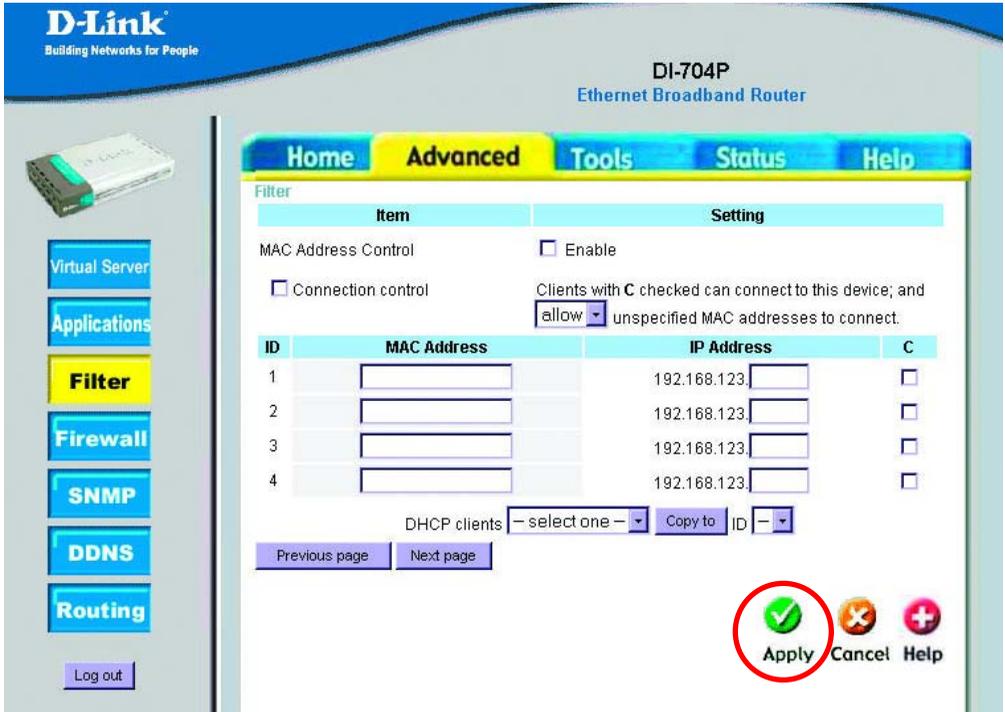
MAC Address Control allows you to assign different access rights for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control: Check **Enable** to enable the **MAC Address Control.** All of the settings in this page will take effect only when **Enable** is checked.

Connection control: Check **Connection control** to control what wired and wireless clients can connect to this device. If a client is denied connection to this device, it means the client can't access the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. You may choose to leave this field empty.
C	When "**Connection control**" is checked, check "**C**" to allow the corresponding client to connect to this device.

*Near the bottom of the **MAC Address Control** window, the following pull-down menu and button will help you to input the MAC address.*

DHCP clients — select one — ▼   Copy to   ID — ▼

Select a specific client in the **"DHCP clients"** pull-down menu.
Click on the **"Copy to"** button to copy the MAC address of the DHCP client you select to the ID selected in the **"ID"** pull-down menu.

Previous page and Next Page: At the bottom of the **MAC Address Control** window you will find these two buttons. Use them to navigate between the several pages of the **MAC Address Control** function.

Previous page   Next page

ADVANCED > FIREWALL

The **Firewall** enables you to control what packets are allowed to pass the router. **Outbound filter** applies on all outbound packets. However, **Inbound filter** applies on packets that are destined for Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. **Allow** all to pass except those that match the specified rules

2. **Deny** all to pass except those that match the specified rules

You can specify 8 rules for inbound or outbound. For each rule, you can define the following:

- Source IP address

- Source port address

- Destination IP address

- Destination port address

For source or destination IP address, you can define a single IP address (e.g., 4.3.2.1) or a range of IP addresses (e.g., 4.3.2.1-4.3.2.254). An empty fields implies all IP addresses.
For source or destination port, you can define a single port (e.g., 80) or a range of ports (e.g., 1000-1999).

Each rule can be enabled or disabled individually.

Inbound Filter:
To enable the **Inbound Packet Filter,** click the check box next to **Enable** in the **Inbound Packet Filter** field.

Outbound Firewall: (to access the Outbound Filter, click **Outbound Firewall** at the bottom of the window.)

To enable the **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

Follow the same procedure as for the Inbound Firewall. The IP addresses that you input will be blocked from the port activity that you input (e.g., browsing the internet, receiving mail etc.)

After **Outbound Packet Filter** setting is configured, click the **Apply** button.

ADVANCED > SNMP
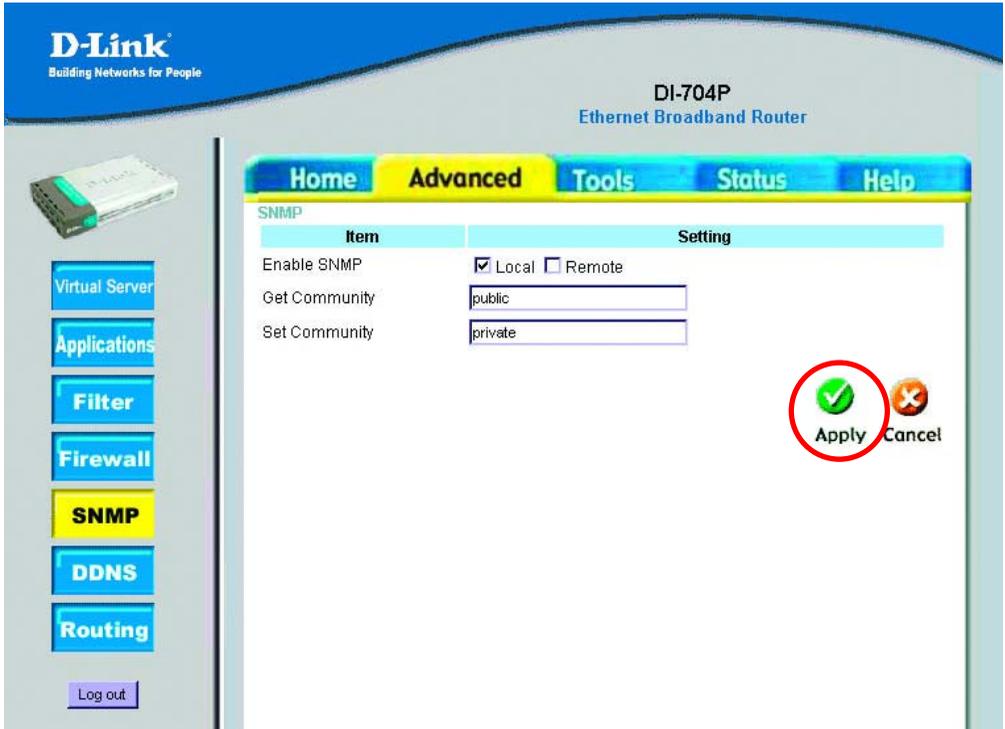
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

To enable **SNMP** click the check box next to **Local or Remote** in the **Enable SNMP** field.

Local: allow manager to access this device through LAN port

Remote: allow manager to access this device through WAN port

You can define:

Get Community: The **Get community** field is the name of your network. Your SNMP manager must have the same name in their **Get community** setting to get SNMP values from this device.

Set Community: The **Set community** field is the name of your network. Your SNMP manager must have the same name in their **Set community** setting to set this device's SNMP values.

Click **Apply** if you have made any changes.

ADVANCED > DDNS

Dynamic DNS
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

Anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect to your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in the **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server. Click **Apply** if you have made any changes.

ADVANCED > ROUTING

Routing allows you to determine which physical interface address to use for outgoing IP data grams. If you have more than one router and subnet, you will need to enable the routing table to allow packets to find the proper routing path and allow different subnets to communicate with each other.

To enable the **Routing Table,** click the check box next to **Enable** in the related field.

You have to define:
Destination
Subnet Mask
Gateway
Hop: router's position compared to this Device; if it is under this device, then input 2.

For example, if the host wanted to send an IP data gram to 192.168.3.88 (destination), it would use the above table to determine that it had to go via 192.168.1.33 (a gateway),

Each rule can be enabled or disabled individually.

After the **routing table** setting is configured, click **Apply**.

Installing the Print Server Software

Step 1: Insert the installation CD-ROM into the CD-ROM drive. The following window will be shown automatically. If it is not, please run "install.exe" on the CD-ROM.

Step 2: Click on the *Install Print Server Software* button. Wait until the following *Welcome* dialog appears, and click on the *Next* button.
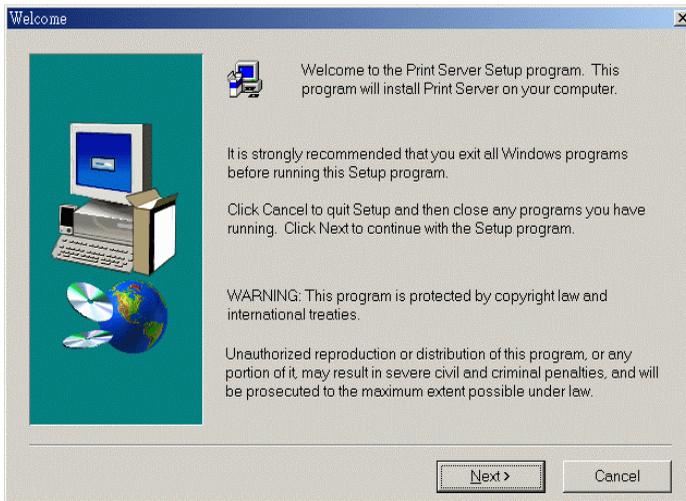
Step 3: Select the destination folder and click on the *Next* button. Then, the setup program will begin to install the programs into the destination folder.
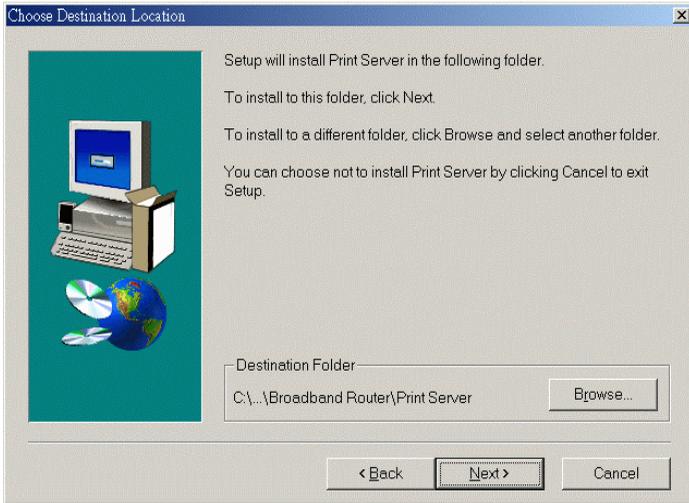
Step 4: When the following window is displayed, click on the *Finish* button.
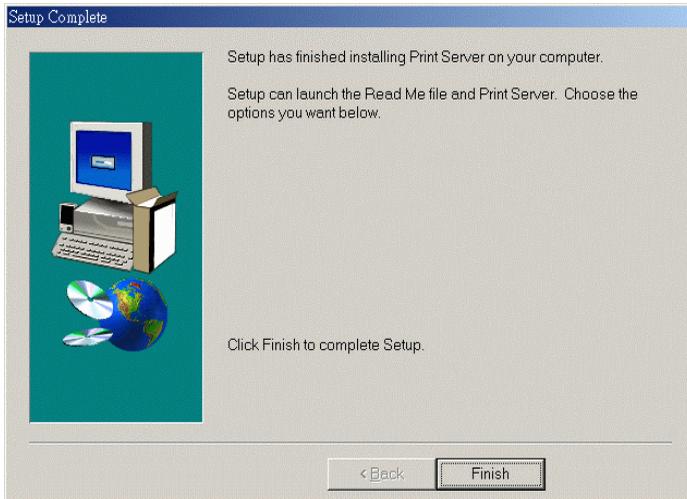
Step 5: Select the item to restart the computer and then click the *OK* button to reboot your computer.

```
reboot
    To make broadband router workable for you, please remember
    rebootingyour computer...



    ⊙ Yes, I want to restart my computer now.

    ○ No, I will restart my computer later.

                                              OK
```
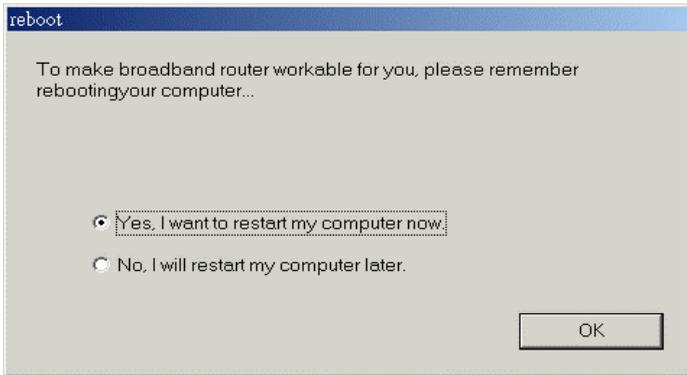
Step 6: After rebooting your computer, the software installation procedure is finished.

Configuring on Windows 98/ME Platforms

After you finish the software installation procedure, your computer will be capable of network printing provided by the DI-704P. For convenience, we call the printer connected to the printer port of the DI-704P a s*erver printer*. On a Windows 95/98 platform, open the *Printers* window in the *My Computer* menu:

```
Printers                              _ □ ×
File  Edit  View  Help

  🖨        🖨           🖨
Add Printer  HP LaserJet   HPLaserJet(...
             6L (PCL)      Chinese)


4 object(s)
```

Now, you can configure the print server of the DI-704P:
1. Find out the corresponding icon of your s*erver printer*, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the *Properties* item:

The following screen appears:
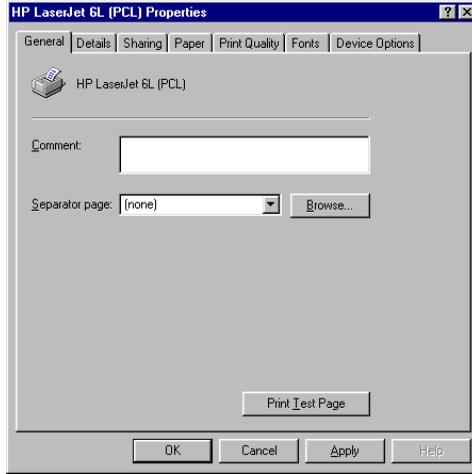
2. Click the *Details* item:
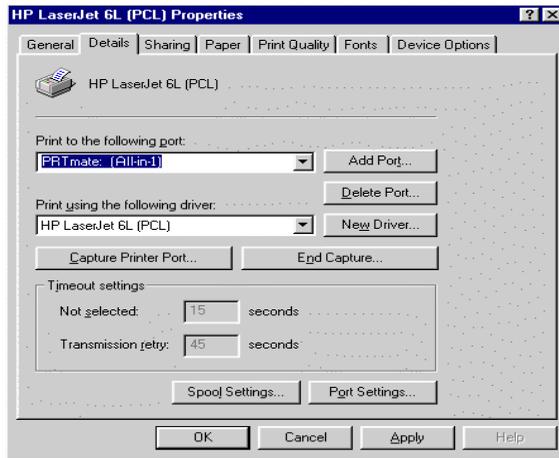
3. Choose the "PRTmate: (All-in-1)" from the list attached at the *Print To* item. Be sure that the *Printer Driver* item is configured to the correct driver of your *server printer*.
4. Click on the button of *Port Settings*:
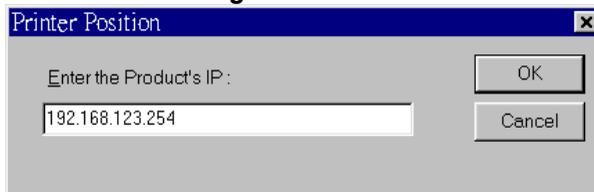
Type in the IP address of the DI-704P and then click the *OK* button.
5. Make sure that all settings mentioned above are correct and then click the *OK* button.

Configuring on Windows NT Platforms

The configuration procedure for a Windows NT platform is similar to that of Windows 95/98 except the screen of printer *Properties*:
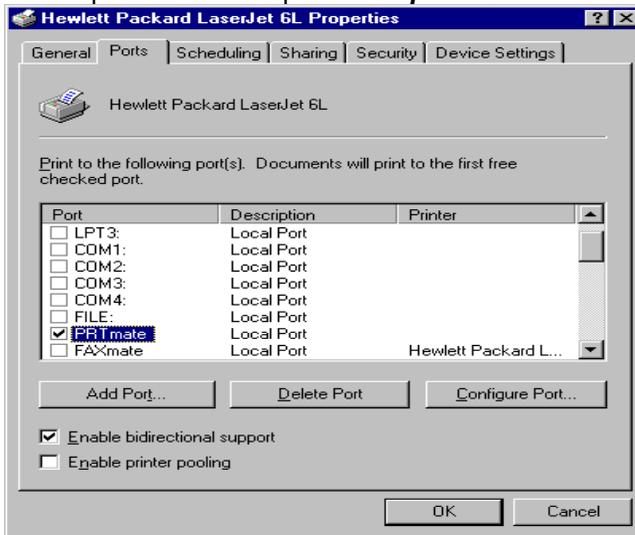

Compared to the procedure in last section, the selection of *Details* is equivalent to the selection of **Ports**, and *Port Settings* is equivalent to *Configure Port*.

Configuring on Windows 2000/XP Platforms

The configuration procedure for a Windows 2000/XP platform is similar to that of Windows 95/98 except the screen of printer *Properties*:
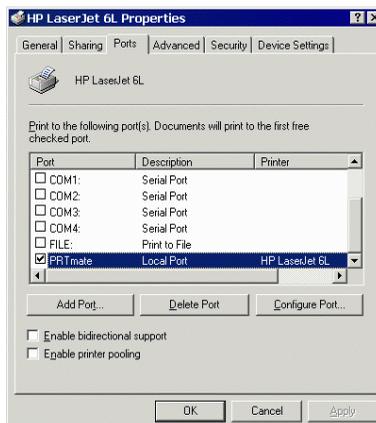
Compared to the procedure in last section, the selection of *Details* is equivalent to the selection of **Ports**, and *Port Settings* is equivalent to *Configure Port.*
(Note: Screen shots are taken in Windows 2000, similar screens will appear in Windows XP.)

Troubleshooting

If you **do not** wish to set the static IP address on your PC, you will need to configure your PC to request an IP address from the gateway.

Click the Start button, select Settings, and select Control Panel.
Double-click the Network icon.
In the configuration tab, select the TCP/IP protocol line that has been associated with your network card/adapter. If there is no TCP/IP line listed, you will need to install TCP/IP now.
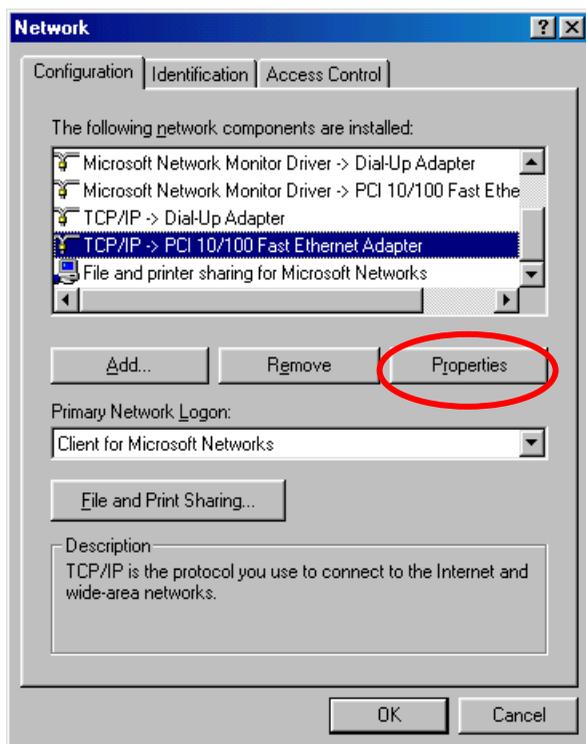
Click the **Properties** button.

Choose the **IP ADDRESS** tab. Select **Obtain an IP automatically**.
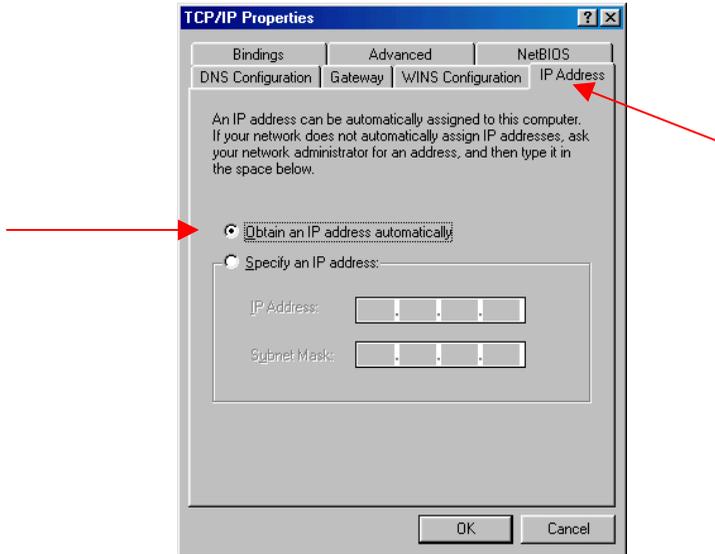
After clicking **OK**, windows might ask you to restart the PC. Click **Yes**.

There are two tools which are great for finding out a computer's IP configuration: MAC address and default gateway.

WINIPCFG (for Windows 95/98)

Inside the windows 95/98 Start button, select Run and type winipcfg. In the example below this computer has an IP address of 192.168.0.100 and the default gateway is 192.168.0.1. The default gateway should be the network device IP address. The MAC address in windows 95/98 is called the Adapter Address.

NOTE: You can also type **winipcfg** in the DOS command prompt.
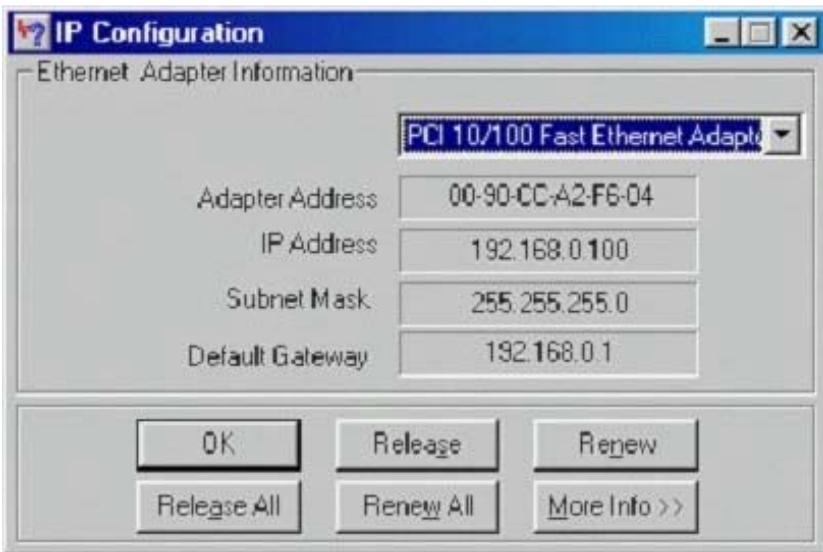
IPCONFIG (for Windows 2000/NT/XP)

At the command prompt type **IPCONFIG** and press **Enter**. Your PC IP information will be displayed as shown below.

Assigning a Static IP Address

Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

Go to **START**
Double-click on
Control Panel
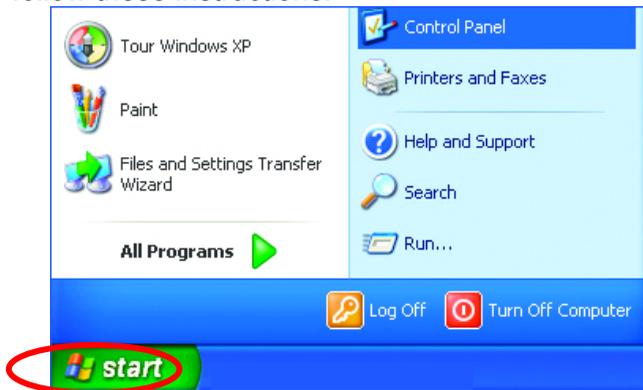
Double-click on
Network Connections
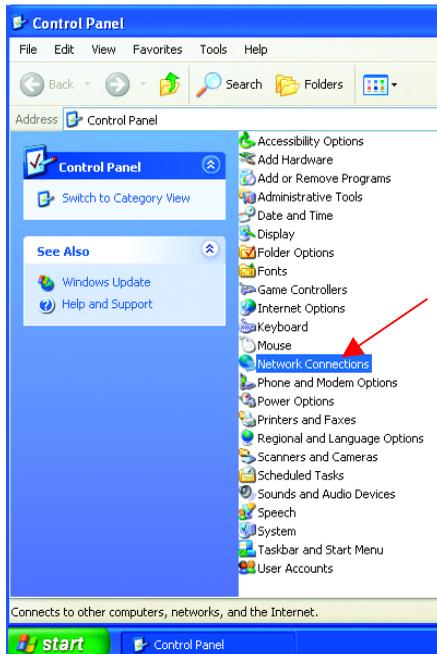
Right-click on **Local Area Connections**.

Click **Properties**
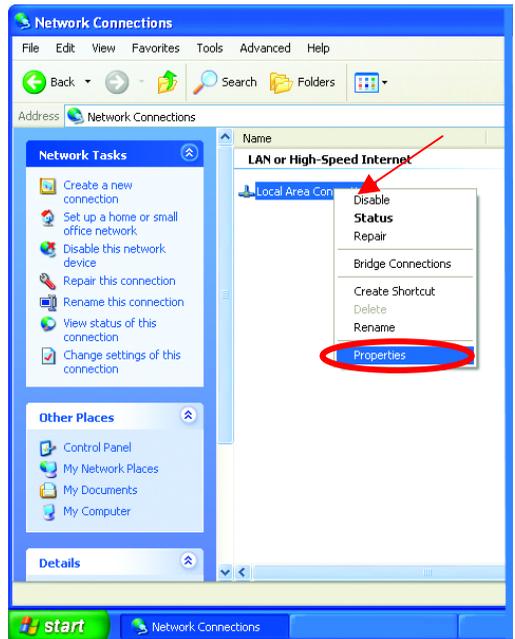
Highlight **Internet Protocol (TCP/IP)**
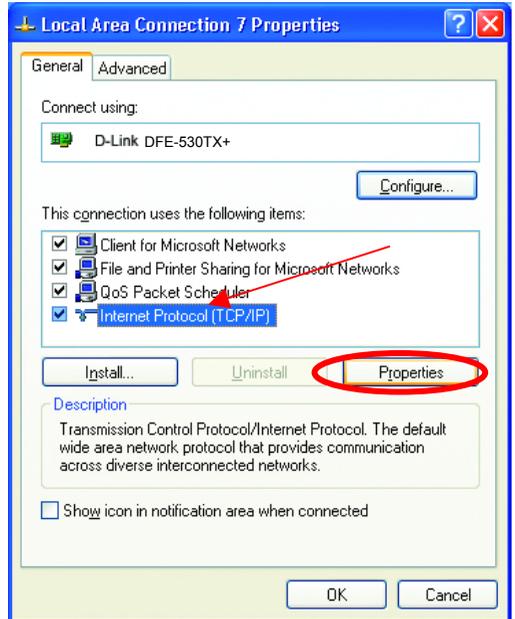
Click **Properties**

Select **Use the following IP address** in the Internet Protocol (TCP/IP) Properties window.

Input your IP address and subnet mask. (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)

- Input your DNS server addresses

The DNS server information will be provided by your ISP (Internet Service Provider.)
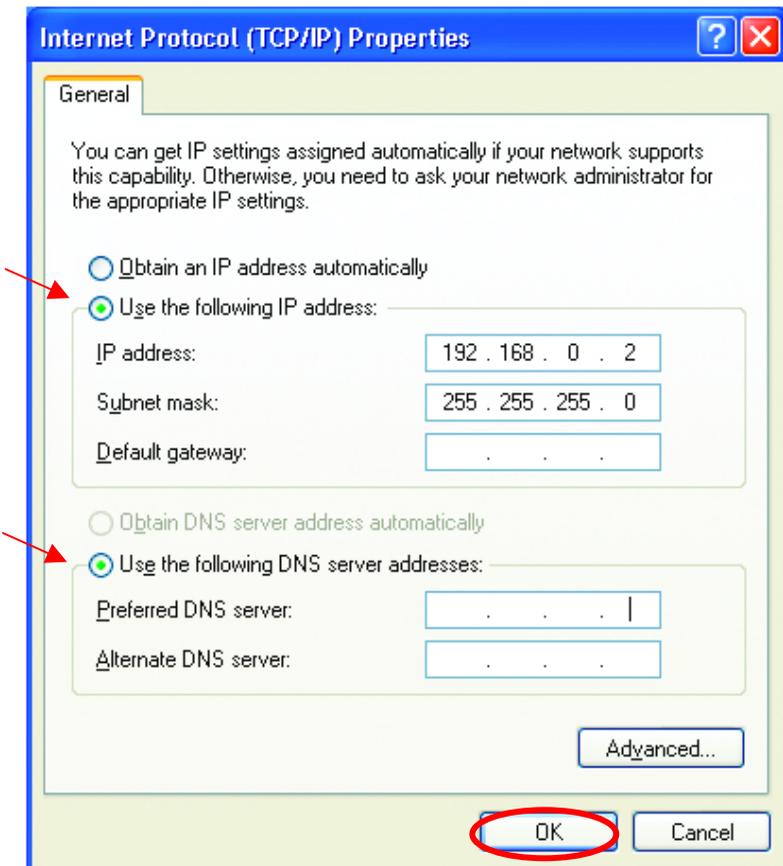
Click **OK**

You have completed the assignment of a Static IP Address. (You do not need to assign a Static IP Address if you have a DHCP-capable Gateway/Router.)

Networking Basics

Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP.**

Note: Please refer to websites such as http://www.homenethelp.com and http://www.microsoft.com/windows2000 for information about networking computers using Windows 2000, ME or 98.

Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**
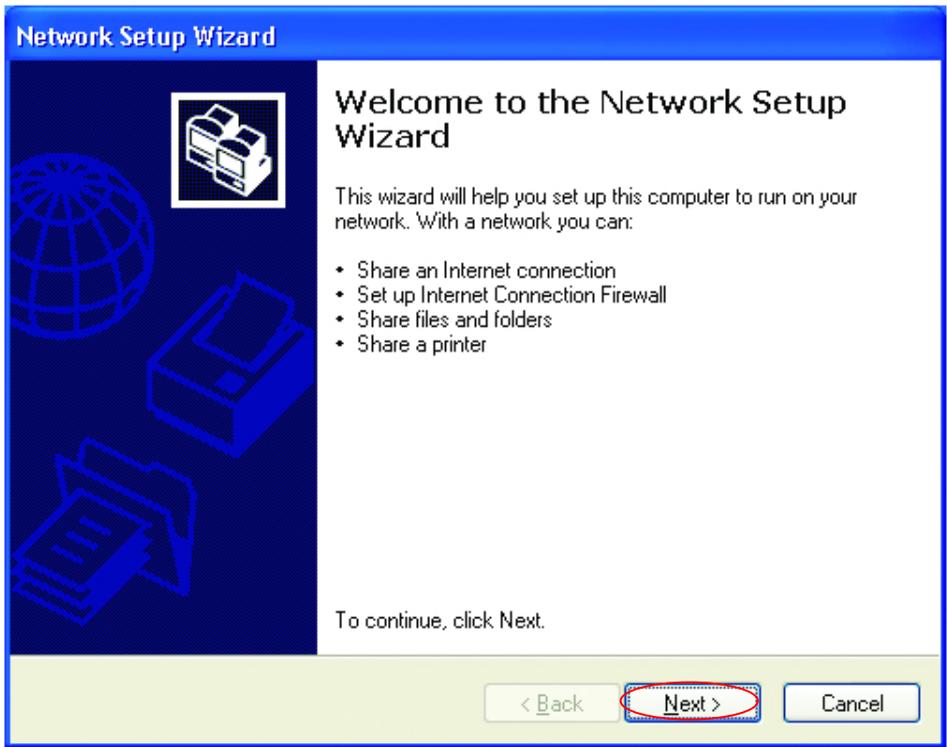
When this screen appears, click **Next.**

Networking Basics

Please follow all the instructions in this window:
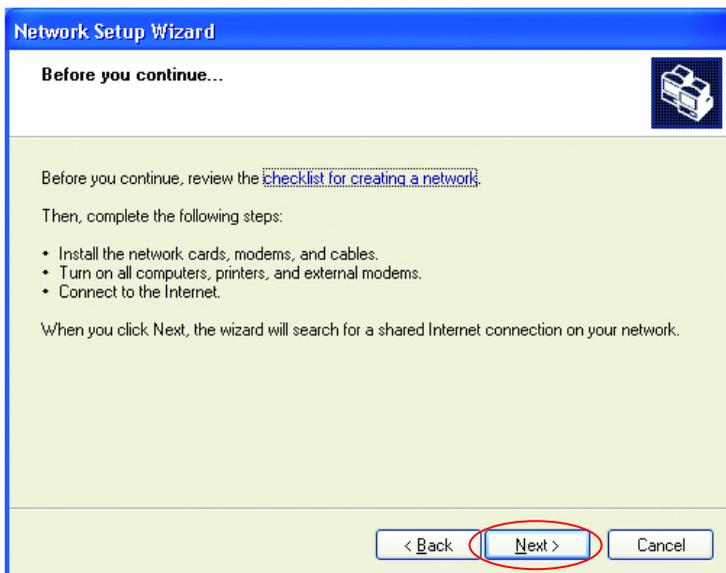
Click **Next**

In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.
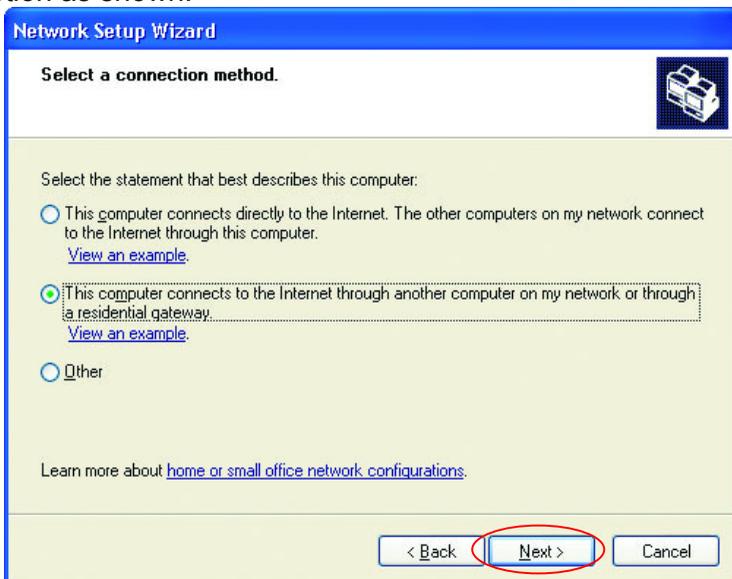
Click **Next**

Networking Basics

Enter a **Computer description** and a **Computer name** (optional.)

Click **Next**

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name.**

Click **Next**

Networking Basics

Please wait while the **Network Setup Wizard** applies the changes.
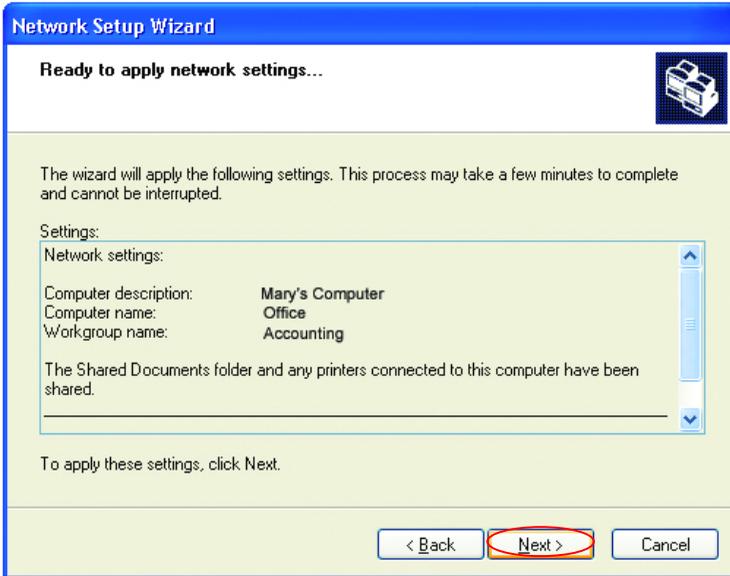
When the changes are complete, click **Next**.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.
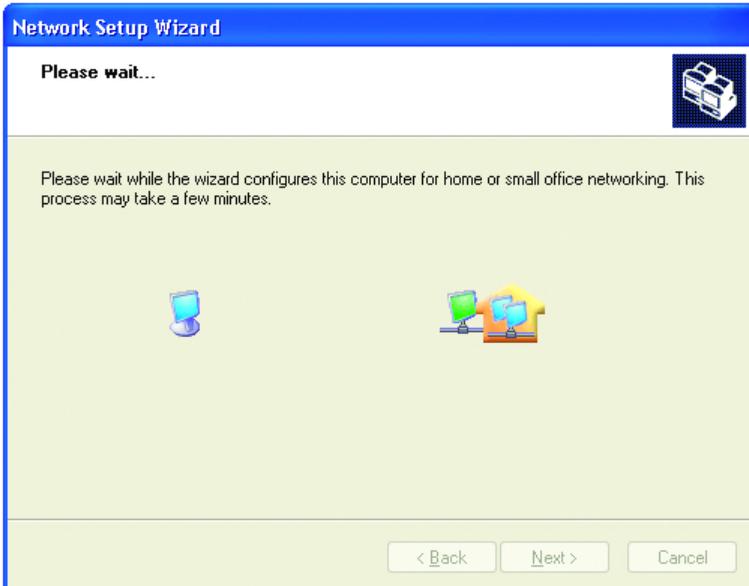
Networking Basics

In the window below, select the best option. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.
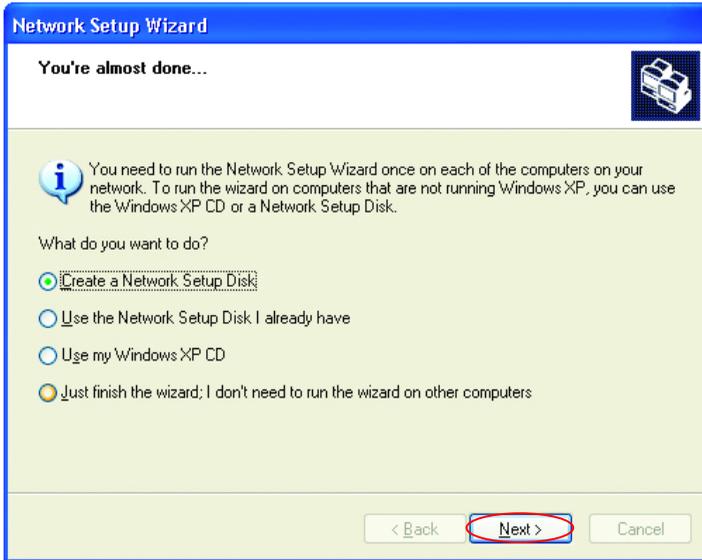
Insert a disk into the Floppy Disk Drive, in this case drive **A.**

Format the disk if you wish, and click **Next.**

Networking Basics

Please wait while the **Network Setup Wizard** copies the files.
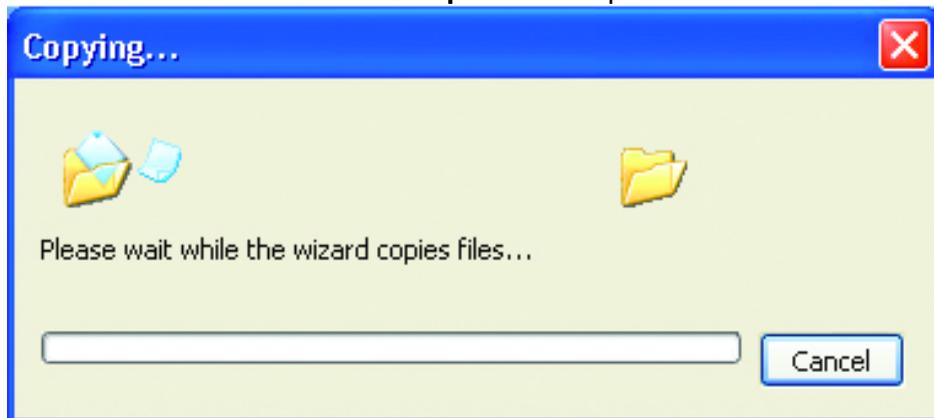
Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. To continue click **Next.**
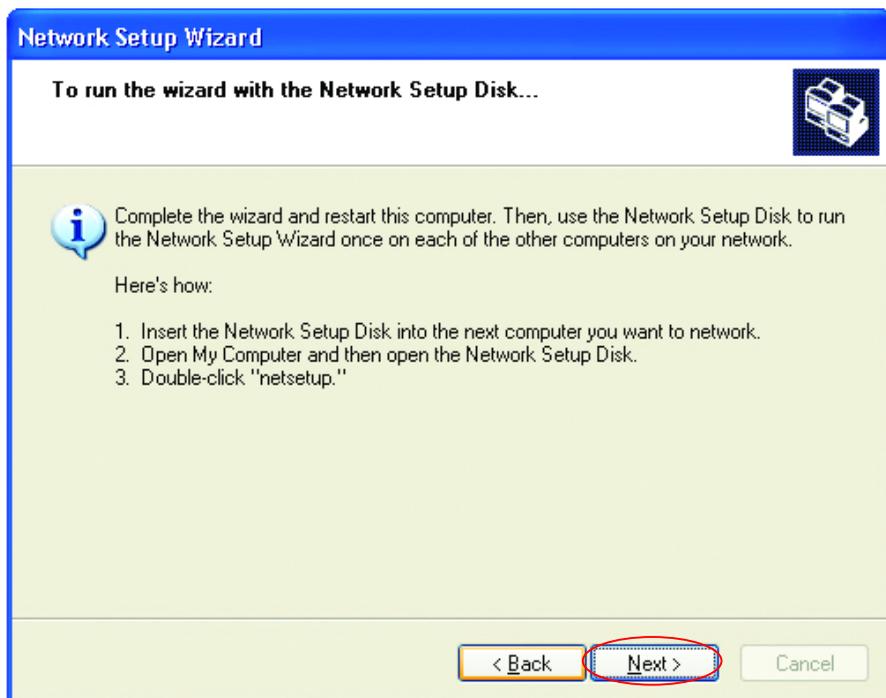
Networking Basics

Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.
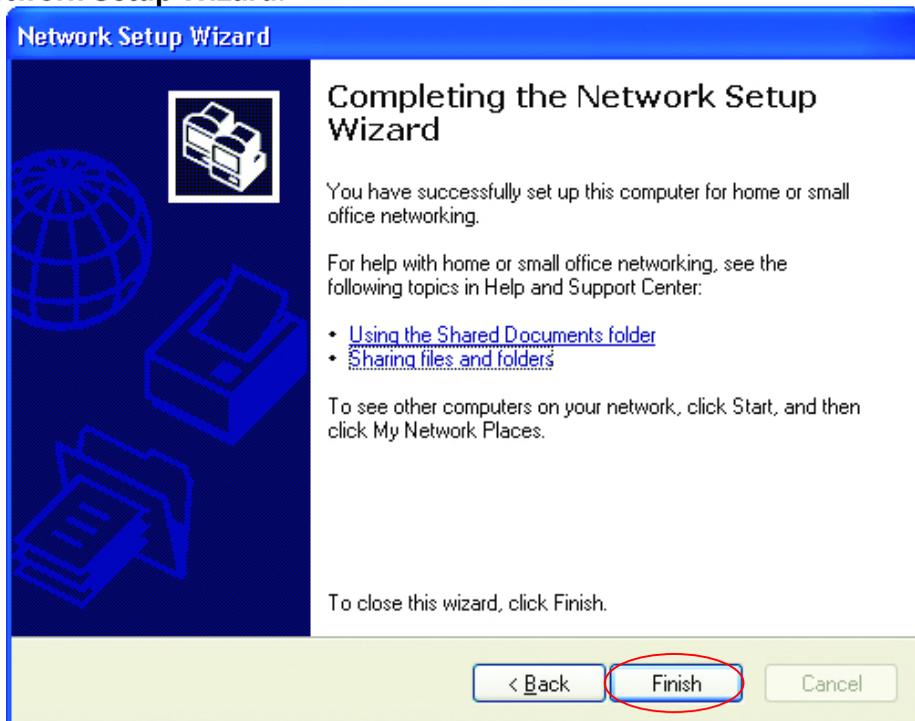
The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.
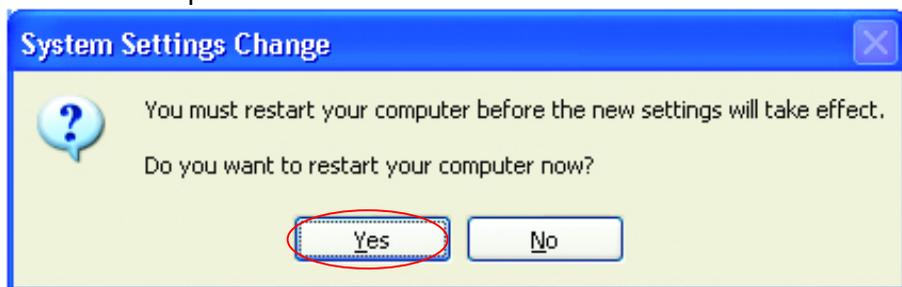
You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

Networking Basics
Naming your Computer

To name your computer, please follow these directions:

In **Windows XP**:

- Click **Start** (in the lower left corner of the screen)

- **Right-click** on **My Computer**

- Select **Properties** and click
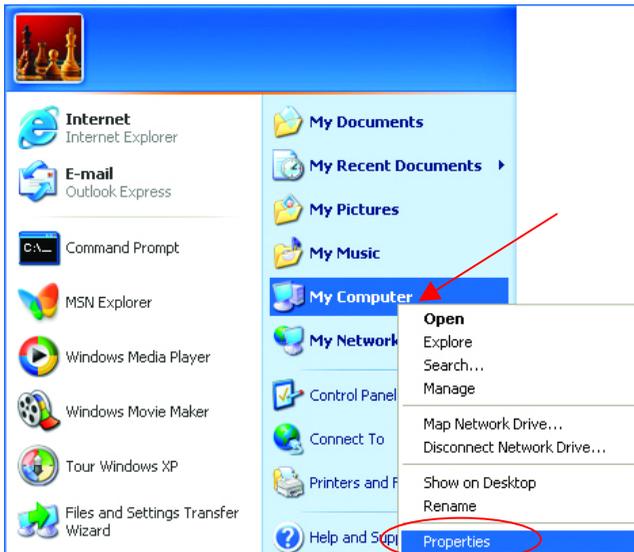
- Select the **Computer Name Tab** in the **System Properties** window.

You may enter a Computer description if you wish, this field is optional.

To rename the computer and join a domain,
- Click **Change**
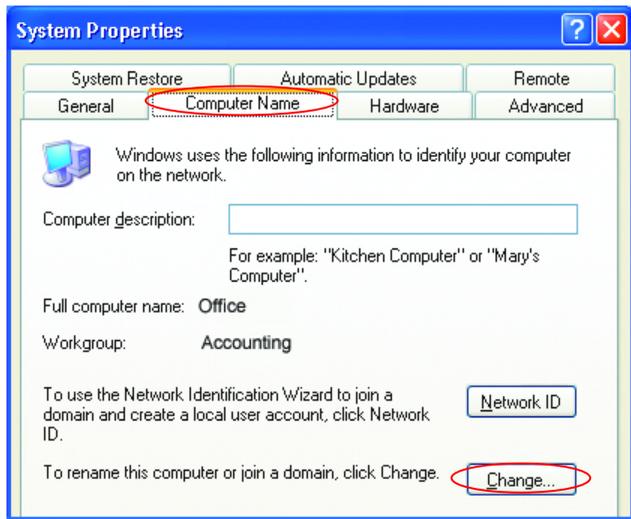
Networking Basics
Naming your Computer

- In this window, enter the **Computer name**.

- Select **Workgroup** and enter the name of the **Workgroup**.

- All computers on your network must have the same **Workgroup** name.

- Click **OK**
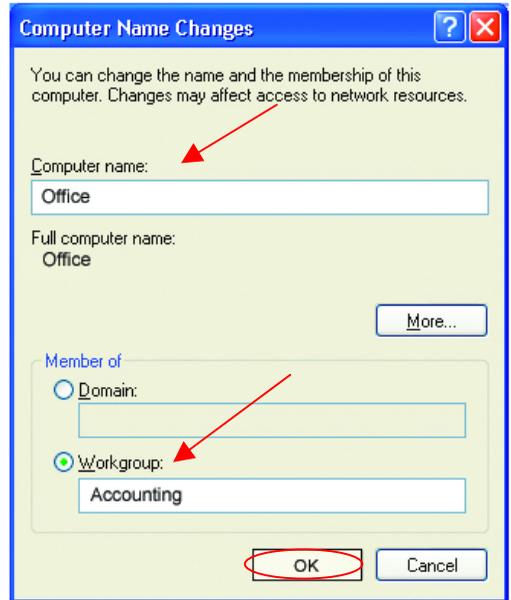
Checking the IP Address in Windows XP/2000

Go to Start > All Programs > Accessories > Command Prompt
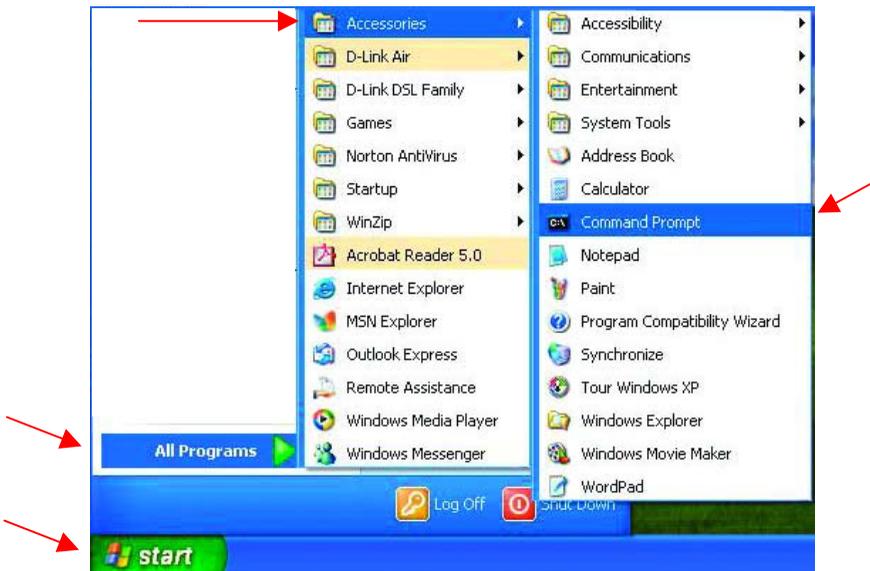
Networking Basics
Checking the IP Address in Windows XP/2000

Type **Command**
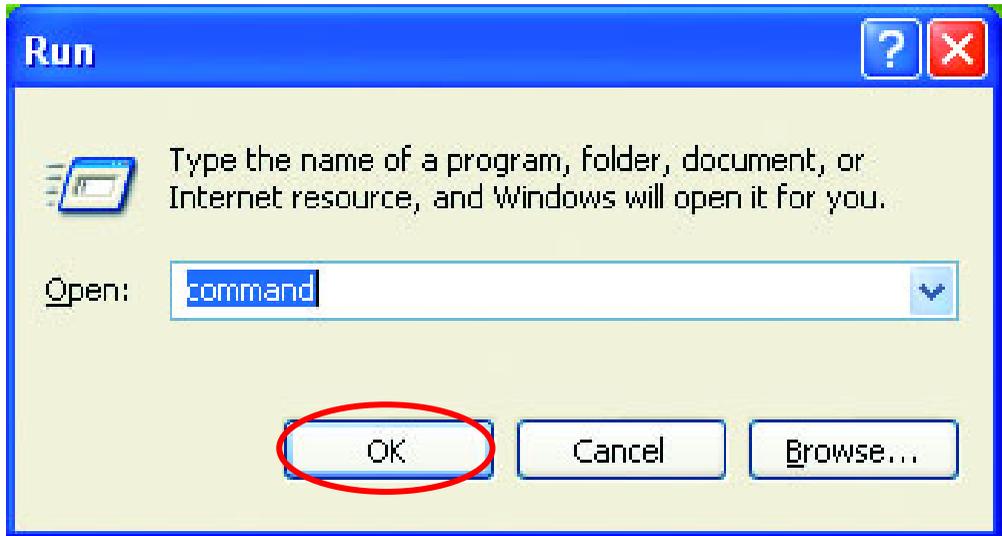
Click **OK**

Checking the IP Address in Windows XP/2000

Type **ipconfig /all** at the prompt. Click **Enter**. All the configuration settings are displayed as shown below.
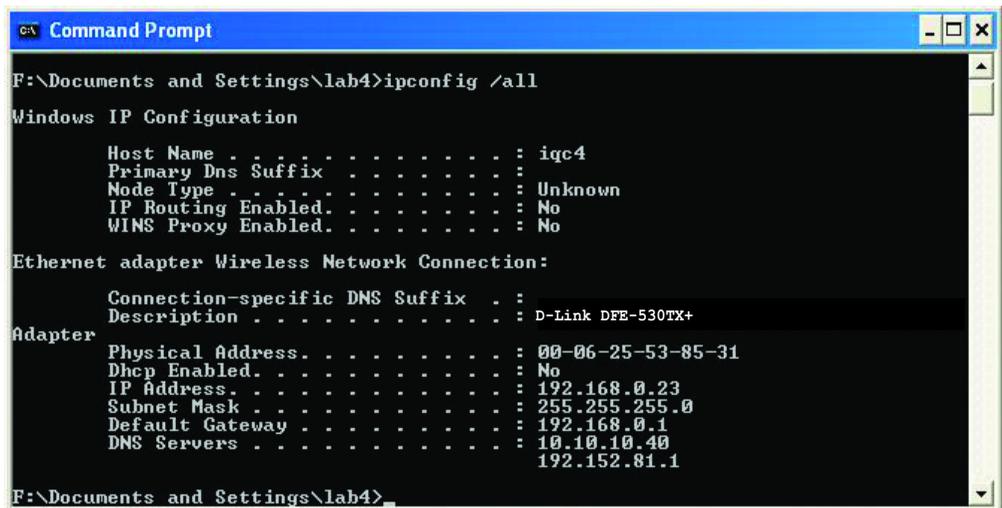
Networking Basics
Checking the IP Address in Windows XP/2000

Type **ipconfig /renew** at the prompt to get a new IP Address. Click **Enter**. The new IP Address is shown below.
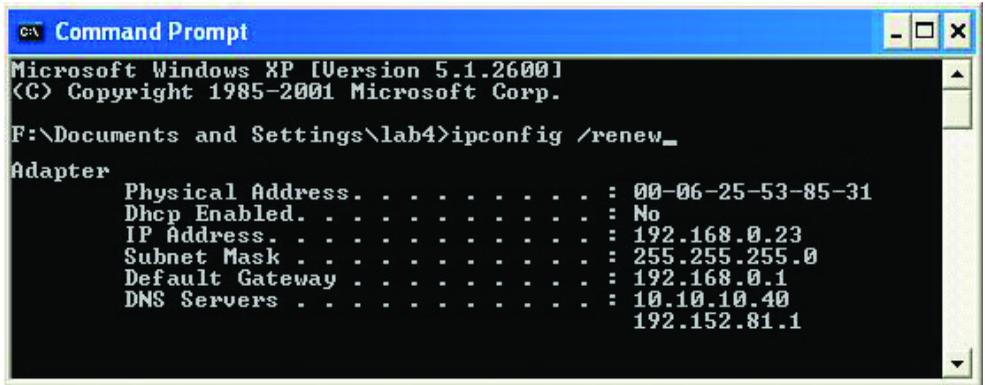

```
Command Prompt                                          - □ ×

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\lab4>ipconfig /renew_

Adapter
        Physical Address. . . . . . . . . . : 00-06-25-53-85-31
        Dhcp Enabled. . . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . . : 192.168.0.23
        Subnet Mask . . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . . : 10.10.10.40
                                              192.152.81.1
```

(**Windows 98/ME users:** go to **Start** > **Run**. Type **Command**. Type **winipcfg** at the prompt. Click **Release and Renew** to obtain a new IP Address.)

Assigning a Static IP Address

Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

- Go to **Start**

- **Double-click** on **Control Panel**
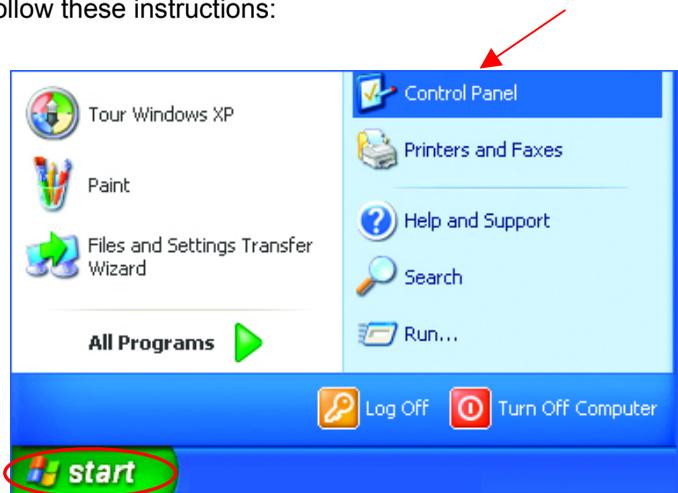
Networking Basics
Assigning a Static IP Address

- **Double-click** on **Network Connections**
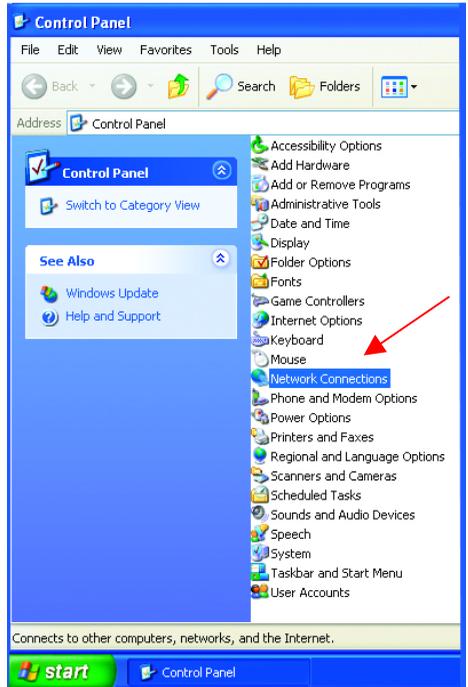
- **Right-click** on **Local Area Connections.**

- **Double-click Properties**
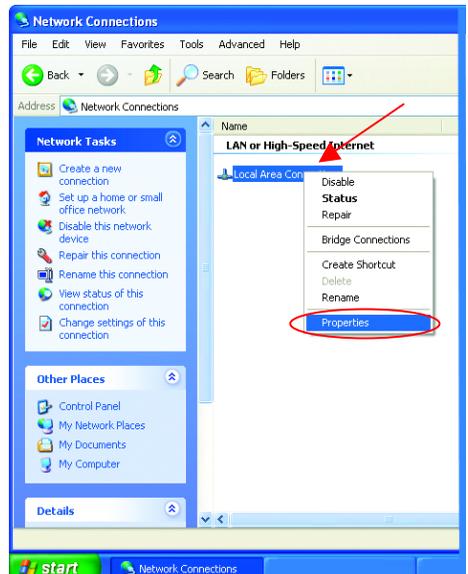
Networking Basics
Assigning a Static IP Address

- Highlight **Internet Protocol (TCP/IP)**

- Click **Properties**

- **Select Use the following IP address** in the **Internet Protocol (TCP/IP) Properties** window,
- Input your **IP address and subnet mask.** (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)
- Input your **DNS server addresses. (Note: If you are entering a DNS server, you must enter the IP Address of the Default Gateway.)**

The DNS server information will be provided by your ISP (Internet Service Provider.)
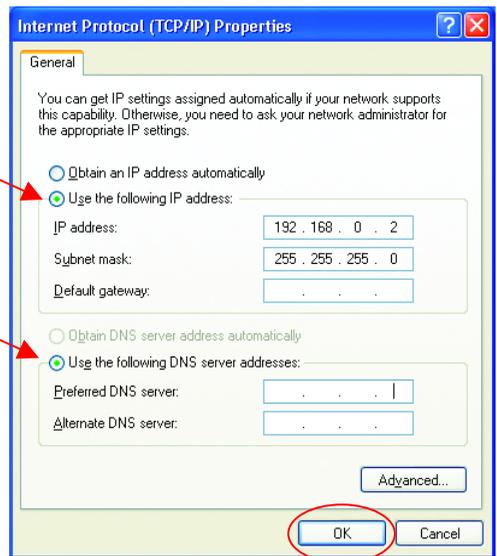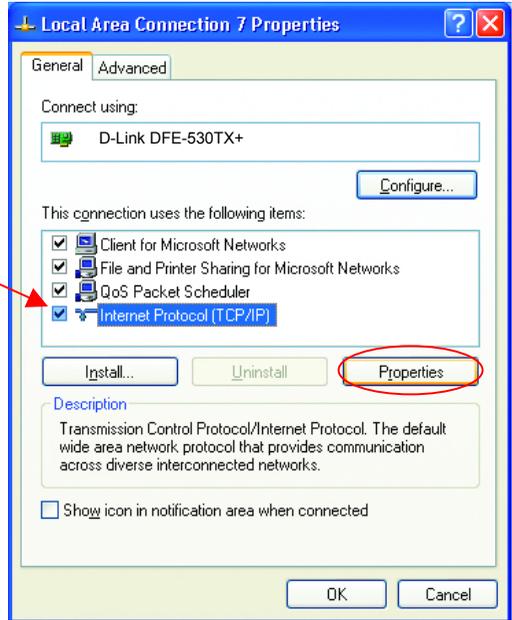
- Click **OK**

You have completed the assignment of a Static IP Address. *(You do not need to assign a Static IP Address if you have a DHCP-capable Gateway/Router.)*

Technical Specifications

Standards:

- IEEE 802.3 10BASET-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.1p Priority Queue
- ANSI/IEEE 802.3 NWay auto-negotiation

Management:
- Web-Based

VPN Pass Through Function*:
- PPTP
- L2TP
- IPSec

Ports:
- 4 x NWay 10BASE-T/100BASE-TX Fast Ethernet LAN (Media Auto Sensing)
- 1 x 10BASE-T WAN
- 1 Printer Port (Female DB-25)

LEDs:
- WAN Activity
- LAN Link Activity
- M1 – Status
- M2 – Status

Power:
- DC 5V 2A

Weight:
- 1.74 kg (3.83 lb)

Size:
- 300(W) x 142(D) x 40(H) mm

Operating Temperature:
- 5 C ~ 55 C

Humidity:
- 10% ~ 90%

Contacting Technical Support

You can find the most recent software and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States for the duration of the warranty period on this product.

U.S. customers can contact **D-Link** technical support through our web site or by phone.

D-Link Technical Support over the Internet:
http://support.dlink.com

D-Link Technical Support over the Telephone:
Phone: 877-453-5465
24 hours a day, seven days a week.

When contacting Technical Support, please provide the following information:

- Serial number of unit
- Model number or product name
- Software type and version number

Warranty and Registration

D-Link Systems, Inc. ("D-Link") provides this 1-Year warranty for its product only to the person or entity who originally purchased the product from:

- D-Link or its authorized reseller or distributor.
- Products purchased and delivered within the fifty United States, the District of Columbia, US Possessions or Protectorates, US Military Installations, addresses with an APO or FPO.

1-Year Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period").

1-Year Limited Warranty for the Product(s) is defined as follows

- Hardware (excluding power supplies and fans)
- Spare parts and spare kits Ninety (90) days.

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic

media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:
Registration is conducted via a link on our Web Site (http://www.dlink.com/). Each product purchased must be individually registered for warranty service within ninety (90) days after it is purchased and/or licensed.

FAILURE TO PROPERLY TO REGISTER MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

- The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package.
- The customer is responsible for all shipping charges to and from D-Link (No CODs allowed). Products sent COD will become the property of D-Link Systems, Inc. Products should be fully insured by the customer and shipped to **D-Link Systems Inc., 53 Discovery Drive, Irvine CA 92618**.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:
This limited warranty provided by D-Link does not cover: Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE 1-YEAR LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This 1-Year Warranty shall be governed by the laws of the state of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

CE Mark Warning
This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with a minimum of 20 cm (approximately 8 inches) between the radiator and your body.

Registration: Register your D-Link DI-704P online at http://support.dlink.com/register/