OfficeConnect®
ADSL Wireless 54 Mbps 11g Firewall Router
User Guide
WL-552

3CRWDR101A-75
3CRWDR101B-75
CONTENTS

ABOUT THIS GUIDE
Naming Convention  7
Conventions  8
Feedback About This User Guide  8
Related Documentation  9

1 INTRODUCING THE ROUTER
OfficeConnect ADSL Wireless 54 Mbps 11g Firewall Router  11
Router Advantages  13
Package Contents  13
Minimum System and Component Requirements  14
Physical Features  14

2 INSTALLING THE ROUTER
Introduction  17
   Safety Information  17
Positioning the Router  17
      Using the Rubber Feet  18
Wall Mounting  18
Powering Up the Router  19
Connecting the Router  19

3 SETTING UP YOUR COMPUTERS
Obtaining an IP Address Automatically  23
   Windows 2000  23
   Windows XP  25
   Windows 98/ME  25
   Macintosh  25
Disabling PPPoE and PPTP Client Software  26
Disabling Web Proxy  26
4 Running the Setup Wizard

Accessing the Setup Wizard 27
Setup Wizard - Change Password 30
Setup Wizard - Time and Time Zone 30
Setup Wizard - Connection Type 31
Setup Wizard - LAN Settings 36
Setup Wizard - Wireless Settings 37
Setup Wizard - Configuration Summary 38

5 Configuring the Router

Navigating Through the Router Configuration screens 39
Main Menu 39
Welcome Screen 39
Status 39
LAN Settings 40
LAN Settings 40
DHCP Clients List 41
Wireless Settings 43
Configuration 44
Encryption 45
Connection Control 50
Client List 51
WDS Settings 51
Advance 52
Profile 53
Internet Settings 54
ATM PVC 54
DNS 65
Hostname & Clone MAC address 66
Firewall 67
SPI 67
Special Applications 71
Virtual Servers 72
DMZ 73
6 TROUBLESHOOTING

Basic Connection Checks 103
Browsing to the Router Configuration Screens 103
ABOUT THIS GUIDE

This guide describes how to install and configure the 3Com OfficeConnect© ADSL Wireless 54 Mbps 11g Firewall Router (3CRWDR101A-75/3CRWDR101B-75).

This guide is intended for use by those responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks) and Internet Routers.

If a release note is shipped with the 3Com OfficeConnect ADSL Wireless 54 Mbps 11g Firewall Router and contains information that differs from the information in this guide, follow the information in the release note.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) on the 3Com World Wide Web site:

http://www.3Com.com

Naming Convention

Throughout this guide, the 3Com OfficeConnect© ADSL Wireless 54 Mbps 11g Firewall Router is referred to as the “Router”.

Category 3 and Category 5 Twisted Pair Cables are referred to as Twisted Pair Cables throughout this guide.
Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1  Notice Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Information note icon]</td>
<td>Information note</td>
<td>Information that describes important features or instructions.</td>
</tr>
<tr>
<td>![Caution icon]</td>
<td>Caution</td>
<td>Information that alerts you to potential loss of data or potential damage to an application, system, or device.</td>
</tr>
<tr>
<td>![Warning icon]</td>
<td>Warning</td>
<td>Information that alerts you to potential personal injury.</td>
</tr>
</tbody>
</table>

**Table 2  Text Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The words “enter” and “type”</td>
<td>When you see the word “enter” in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says “type.”</td>
</tr>
<tr>
<td>Keyboard key names</td>
<td>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del.</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Italics are used to:</td>
</tr>
<tr>
<td></td>
<td>■ Emphasize a point.</td>
</tr>
<tr>
<td></td>
<td>■ Denote a new term at the place where it is defined in the text.</td>
</tr>
<tr>
<td></td>
<td>■ Identify menu names, menu commands, and software button names. Examples: From the Help menu, select Contents. Click OK.</td>
</tr>
<tr>
<td>Feedback About This User Guide</td>
<td>Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong><a href="mailto:pddtechpubs_comments@3com.com">pddtechpubs_comments@3com.com</a></strong></td>
</tr>
<tr>
<td></td>
<td>Please include the following information when commenting:</td>
</tr>
<tr>
<td>■</td>
<td>Document title</td>
</tr>
<tr>
<td>■</td>
<td>Document part number (on the title page)</td>
</tr>
<tr>
<td>■</td>
<td>Page number (if appropriate)</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>■</td>
<td>3Com OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router User Guide</td>
</tr>
<tr>
<td>■</td>
<td>Part Number 10015091 Rev. AA</td>
</tr>
<tr>
<td>■</td>
<td>Page 24</td>
</tr>
<tr>
<td><strong>Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to Appendix C.</strong></td>
<td></td>
</tr>
</tbody>
</table>

| Related Documentation | In addition to this guide, each Router document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Router. |
INTRODUCING THE ROUTER

Welcome to the world of networking with 3Com®. In the modern business environment, communication and sharing information is crucial. Computer networks have proved to be one of the fastest modes of communication but, until recently, only large businesses could afford the networking advantage.

OfficeConnect ADSL Wireless 54 Mbps 11g Firewall Router

The OfficeConnect ADSL Wireless 54 Mbps 11g Firewall Router is designed to provide a cost-effective means of sharing a single broadband Internet connection amongst several wired and wireless computers. The Router also provides protection in the form of an electronic “firewall” preventing anyone outside of your network from seeing your files or damaging your computers. The Router can also prevent your users from accessing Web sites which you find unsuitable.

Figure 1 shows an example network without a Router. In this network, only one computer is connected to the Internet. This computer must always be powered on for the other computers on the network to access the Internet.
**Figure 1**  Example Network Without a Router

When you use the Router in your network (Figure 2), it becomes your connection to the Internet. Connections can be made directly to the Router, or to an OfficeConnect Switch or Hub, expanding the number of computers you can have in your network.

**Figure 2**  Example Network Using a Firewall Router
**Router Advantages**
The advantages of the Router include:
- Shared Internet connection for both wired and wireless computers
- High speed 802.11g wireless networking
- No need for a dedicated, “always on” computer serving as your Internet connection
- Cross-platform operation for compatibility with Windows, Unix and Macintosh computers
- Easy-to-use, Web-based setup and configuration
- Provides centralization of all network address settings (DHCP)
- Acts as a Virtual server to enable remote access to Web, FTP, and other services on your network
- Security — Firewall protection against Internet hacker attacks and encryption to protect wireless network traffic

**Package Contents**
The Router kit includes the following items:
- One OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router
- One power adapter for use with the Router
- Four rubber feet
- One Telephone Cable
- One CD-ROM containing this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer

If any of these items are missing or damaged, please contact your retailer.
CHAPTER 1: INTRODUCING THE ROUTER

Minimum System and Component Requirements

Your Router requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10 Mbps or 10/100 Mbps NIC for each computer to be connected to the four-port switch on your Router.
- An 802.11b or 802.11g wireless NIC.
- An active ADSL subscription and connection.
- A Web browser that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

Physical Features

The front panel of the Router contains a series of indicator lights (LEDs) that help describe the state of various networking and connection operations.

**Figure 3** Router - Front Panel

1 Alert LED

*Orange*

Fast flash during self test. If self test fails the LED will remain on.
Fast flash during software upgrade.
Fast flash for software reset to the factory defaults.
Fast flash for hardware reset to the factory defaults.
The LED is on for 2 seconds when the firewall detects a hacker attack.
2 Power LED
   Green
   Indicates that the Router is powered on, and the boot up is successful.

3 SYNC LED
   Green
   If the LED is on it indicates that DSL connection is present. This LED flashes during configuration at power up.

4 Online LED
   Green
   If this LED is on, your username/password has been authenticated successfully with your ISP.

5 Wireless LAN (WLAN) Status LED
   Green
   If the LED is on it indicates that wireless networking is enabled. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, the Wireless LAN has been disabled in the Router, or there is a problem. Refer to Chapter 6 “Troubleshooting”.

6 LAN Status LEDs
   Green
   If the LED is on, the link between the port and the next piece of network equipment is OK. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, nothing is connected, or the connected device is switched off, or there is a problem with the connection (refer to Chapter 6 “Troubleshooting”). The port will automatically adjust to the correct speed and duplex.
The rear panel (Figure 4) of the Router contains four LAN ports, one ADSL port, a reset button, a power OK LED, and a power adapter socket.

Figure 4  Router - Rear Panel

7 Wireless Antennae
The antennae should be placed in a ‘V’ position when initially installed.

CAUTION: Do not force the antennae beyond their mechanical stops. Rotating the antennae further may cause damage.

8 ADSL Port
Using the RJ-11 cable provided, you should connect your Router to the telephone socket via a splitter.

9 Power OK LED
Indicates the Router is powered on, the power adapter is working properly.

10 Power Adapter Socket
Only use the power adapter that is supplied with this Router. Do not use any other adapter.

11 Reset Button
If you want to reset your Router to factory default settings, and cannot access the web management interface (for example, due to a lost password), then you may use this button. Refer to “Forgotten Password and Reset to Factory Defaults” on page 104 for further details.

12 Ethernet Ports
Using suitable RJ-45 cables, you can connect your Router to a computer, or to any other piece of equipment that has an Ethernet connection (for example, a hub or a switch). These ports have an automatic MDI/MDIX feature, which means either straight-through or a crossover cable can be used.
2

INSTALLING THE ROUTER

Introduction
This chapter will guide you through a basic installation of the Router, including:

■ Connecting the Router to the Internet.
■ Connecting the Router to your network.
■ Setting up your computers for networking with the Router.

Safety Information
Please note the following:

WARNING: Please read the “Safety Information” section in Appendix C before you start.

VORSICHT: Bitte lesen Sie den Abschnitt “Wichtige Sicherheitshinweise” sorgfältig durch, bevor Sie das Gerät einschalten.

AVERTISSEMENT: Veuillez lire attentivement la section “Consignes importantes de sécurité” avant de mettre en route.

Positioning the Router
You should place the Router in a location that:

■ is conveniently located for connection to the telephone socket.
■ is centrally located to the wireless computers that will connect to the Router. A suitable location might be on top of a high shelf or similar furniture to optimize wireless connections to computers in both horizontal and vertical directions, allowing wider coverage.
■ allows convenient connection to the computers that will be connected to the four LAN ports on the rear panel, if desired.
■ allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.
When positioning your Router, ensure:

- It is out of direct sunlight and away from sources of heat.
- Cabling is away from power lines, fluorescent lighting fixtures, and sources of electrical noise such as radios, transmitters and broadband amplifiers.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. 3Com recommends you provide a minimum of 25 mm (1 in.) clearance.

**Using the Rubber Feet**

Use the four self-adhesive rubber feet to prevent your Router from moving around on your desk or when stacking with flat top units. Only stick the feet to the marked areas at each corner of the underside of your Router.

**Wall Mounting**

There are two slots on the underside of the Router that can be used for wall mounting.

*When wall mounting the unit, ensure that it is within reach of the power outlet.*

You will need two suitable screws to wall mount the unit. To do this:

1. Ensure that the wall you use is smooth, flat, dry and sturdy and make two screw holes which are 150 mm (5.9 in.) apart.
2. Fix the screws into wall, leaving their heads 3 mm (0.12 inch) clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.

*When making connections, be careful not to push the unit up and off the wall.*

**CAUTION:** Only wall mount single units, do not wall mount stacked units.
Powering Up the Router

To power up the Router:

1. Plug the power adapter into the power adapter socket located on the back panel of the Router.
2. Plug the power adapter into a standard electrical wall socket.
3. Press the power button located on the back of the Router.

Connecting the Router

The first step for installing your Router is to physically connect it to the telephone socket and then connect it to a computer in order to be able to access the Internet. See Figure 5:

**Figure 5** Connecting the Router

1. Run the provided telephone cable from the wall jack providing ADSL service to the ADSL port on your Router. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. If you are using splitterless ADSL service, add low-pass filters between the ADSL wall jack and your telephones. (These filters pass voice signals through but filter data signals out.)

2. Then:
   - If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case
you can connect your phones and computer directly to the splitter as shown below (Figure 6):

or

- If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system. In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below (Figure 7).

Figure 6  Installing with a splitter
You have now completed the hardware installation of your Router. Next you need to set up your computers so that they can make use of the Router to communicate with the Internet.

3Com recommends that you perform the initial Router configuration from a computer that is directly connected to one of the LAN ports.

If you configure the Router from a wireless computer, note that you may lose contact with the Router if you change the wireless configuration.

To communicate wirelessly with your Router, your wireless NIC should be set as follows:

- Encryption — none
- SSID — 3Com
- Channel — 11
The Router has the ability to dynamically allocate network addresses to the computers on your network, using DHCP. However, your computers need to be configured correctly for this to take place. To change the configuration of your computers to allow this, follow the instructions in this chapter.

### Obtaining an IP Address Automatically

**Windows 2000**

If you are using a Windows 2000-based computer, use the following procedure to change your TCP/IP settings:

1. From the Windows Start Menu, select Settings > Control Panel.
2. Double click on Network and Dial-Up Connections.
3. Double click on Local Area Connection.
4. Click on Properties.
5. A screen similar to Figure 8 should be displayed. Select Internet Protocol TCP/IP and click on Properties.
6 Ensure that the options *Obtain an IP address automatically*, and *Obtain DNS server address automatically* are both selected as shown in Figure 9. Click OK.

7 Restart your computer.
Obtaining an IP Address Automatically

Windows XP

1. From the Windows Start Menu, select Control Panel.
2. Click on Network and Internet Connections.
3. Click on the Network Connections icon.
4. Double click on LAN or High Speed Connection icon. A screen titled Local Area Connection Status will appear.
5. Select Internet Protocol TCP/IP and click on Properties.
6. Ensure that the options Obtain an IP address automatically, and Obtain DNS servers automatically are both selected. Click OK.
7. Restart your computer.

Windows 98/ME

1. From the Windows Start Menu, select Settings > Control Panel.
2. Double click on Network. Select the TCP/IP item for your network card and click on Properties.
3. In the TCP/IP dialog, select the IP Address tab, and ensure that Obtain IP address automatically is selected. Click OK.

Macintosh

If you are using a Macintosh computer, use the following procedure to change your TCP/IP settings:

1. From the desktop, select Apple Menu, Control Panels, and TCP/IP.
2. In the TCP/IP control panel, set Connect Via: to Ethernet.
3. In the TCP/IP control panel, set Configure: to Using DHCP Server.
4. Close the TCP/IP dialog box, and save your changes.
5. Restart your computer.
Disabling PPPoE and PPTP Client Software

If you have PPPoE client software installed on your computer, you will need to disable it. To do this:

1. From the Windows Start Menu, select Settings > Control Panel.
2. Double click on Internet Options.
3. Select the Connections Tab. A screen similar to Figure 10 should be displayed.
4. Select the Never dial a connection option.

**Figure 10** Internet Properties Screen

You may want to remove the PPPoE client software from your computer to free resources, as it is not required for use with the Router.

Disabling Web Proxy

Ensure that you do not have a web proxy enabled on your computer.

Go to the Control Panel and click on Internet Options. Select the Connections tab and click LAN Settings at the bottom. Make sure that the Use Proxy Server option is unchecked.
Accessing the Setup Wizard  

The Router setup program is Web-based, which means that it is accessed through your Web browser (Netscape Navigator 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher).

To use the Setup Wizard:

1. Ensure that you have at least one computer connected to the Router. Refer to Chapter 2 for details on how to do this.
2. Launch your Web browser on the computer.
3. Enter the following URL in the location or address field of your browser: [http://192.168.1.1](http://192.168.1.1) (Figure 11). The Login screen displays.

Figure 11  Web Browser Location Field (Factory Default)
4 To log in as an administrator, enter the password (the default password is *admin*) in the *System Password* field and click *Log in* (Figure 12).

**Figure 12** Router Login Screen

5 When you have logged in,
  - if you are logging in for the first time, the Country Selection screen will appear (Figure 13). Please select the country form the drop-down menu, and click *Apply*.

**Figure 13** Country Selection Screen

The Wizard will then launch automatically (refer to Figure 16). You will be guided step by step through a basic setup procedure.

  - if the Router has been configured previously, the *Welcome* screen will appear (Figure 14). There are three tabs: Notice Board, Password and Wizard.
Go to the Notice Board tab to see the current software information. To view the Web help, click the Help button.

Go to the Password tab to change the password (Figure 15).

Go to the Wizard tab to do a quick setup of the Router (Figure 16).

The password screen allows you to change the current password and set the login time limit to the Router's management interface.

1. To change the current password, enter the password in the Current Password field.
2. Enter the new password in the New Password field, and enter it again in the Confirm New Password field.
3 Enter the time period in Login Timeout to set a maximum period of time for which the login session is maintained during inactivity (Default: 10 minutes).

Setup Wizard - Change Password

To ensure the security of your Router, it is recommended that you choose a new password - this should be a mix of letters and numbers, and not easily guessed by others. To leave the current password unchanged, leave the fields blank and click Next.

Figure 16  Change Password Screen

Setup Wizard - Time and Time Zone

The Time and Time Zone screen allows you to set up the time for the Router.

Figure 17  Time and Time Zone Screen

1 If you want to automatically synchronize the Router with a public time server, check the Enable box in the Using Time Server NTP field.
2 Select the time zone in the Set Time Zone drop-down menu.
3 Select the desired servers from the Time Server drop-down menu.
4 Check the Enable box in the Daylight Savings field, if daylight savings applies to your area.

5 Click Next.

**Setup Wizard - Connection Type**

The Connection Type screen allows you to set up the Router for the type of Internet connection you have. Before setting up your connection type, have your account information from your ISP ready.

**Figure 18** Connection Type Screen

Select a DSL mode from the following:

- **PPPoE** — PPP over Ethernet, providing routing for multiple PCs, see page 32
- **PPPoA** — PPP over ATM, providing routing for multiple PCs, see page 33
- **Bridge Mode (for a single PC)** — RFC1483 Bridged Mode, for single PCs only, see page 34
- **Routing Mode over ATM** — RFC1483 Routed Mode, for multiple PCs, see page 34
- **Dynamic/Fixed IP in 1483 Bridge Mode (for multiple PCs)**, see page 35

and click Next.

For further information on selecting a mode see “Internet Settings” on page 54.
PPPoE Mode

To set up the Router for use with a PPP over Ethernet (PPPoE) connection, use the following procedure:

1. Enter your user name in the Username field.
2. Enter your password in the Password field.
3. Re-type your password in the Retype Password field.
4. Enter your VPI and VCI information in the VPI/VCI fields.
5. Select the encapsulation type (LLC or VC MUX) in the Encapsulation drop-down menu. This information should be provided to you by your ISP.
6. Check all of your settings, and then click Next.

The LAN Settings screen will then be displayed (refer to Figure 24).
PPPoA Mode
To set up the Router for use with a PPP over ATM (PPPoA) connection, use the following procedure:

Figure 20  PPPoA Screen

1. Enter your user name in the **Username** field.
2. Enter your password in the **Password** field.
3. Re-type your password in the **Retype Password** field.
4. Enter your VPI and VCI information in the **VPI/VCI** fields.
5. Select the encapsulation type (LLC or VC MUX) in the **Encapsulation** drop-down menu. This information should be provided to you by your ISP.
6. Check all of your settings, and then click **Next**. The LAN Settings screen will then be displayed (refer to Figure 24).
**Bridge Mode (for a single PC)**

To set up the Router for use with an RFC1483 bridged connection, use the following procedure:

1. Enter your VPI and VCI information in the VPI/VCI fields.
2. Select the encapsulation type (LLC or VC MUX) in the Encapsulation drop-down menu. This information should be provided to you by your ISP.
3. Check all of your settings, and then click Next. The LAN Settings screen will then be displayed (refer to Figure 24).

**Routing Mode over ATM**

To set up the Router for use with an RFC1483 routed connection, use the following procedure:

1. Enter your VPI and VCI information in the VPI/VCI fields.
2. Select the encapsulation type (LLC or VC MUX) in the Encapsulation drop-down menu. This information should be provided to you by your ISP.
3. Check all of your settings, and then click Next. The LAN Settings screen will then be displayed (refer to Figure 24).
1. Enter your Internet IP address in the **WAN IP** field.
2. Enter the subnet mask in the **Subnet Mask** field.
3. Enter the default gateway IP address in the **Default Gateway** field.
4. Enter the DNS address in the **DNS** field.
5. Enter your VPI and VCI information in the **VPI/VCI** fields.
6. Select the encapsulation type (LLC or VC MUX) in the **Encapsulation** drop-down menu. This information should be provided to you by your ISP.
7. Check all of your settings, and then click **Next**. The LAN Settings screen will then be displayed (refer to Figure 24).

**Dynamic/Fixed IP in 1483 Bridge Mode (For Multiple PCs)**

For bridge mode to work, you need to assign an IP address to the Router. You can either configure the Router to obtain an IP address automatically from a DHCP server or assign a fixed or static IP address to it.

**Figure 23**  Dynamic/Fixed IP for Bridge Mode Screen

To obtain an IP address automatically from a DHCP server:
Check the Get **WAN IP By DCHP** checkbox, and then click **Next**. The LAN Settings screen will then be displayed (refer to Figure 24).
CHAPTER 4: RUNNING THE SETUP WIZARD

To assign a fixed IP address:

1. Enter your Internet IP address in the **WAN IP** field.
2. Enter the subnet mask in the **Subnet Mask** field.
3. Enter the default gateway IP address in the **Default Gateway** field.
4. Enter the DNS address in the **DNS** field.
5. Enter your VPI and VCI information in the **VPI/VCI** text boxes.
6. Select the encapsulation type (LLC or VC MUX) in the **Encapsulation** drop-down menu. This information should be provided to you by your ISP.
7. Check all of your settings, and then click **Next**. The LAN Settings screen will then be displayed (refer to Figure 24).

**Setup Wizard - LAN Settings**

The LAN Settings screen allows you to set the default IP address and DHCP client IP range for the Router.

**Figure 24** The LAN Settings Screen

1. To change the Router's default IP address, enter the new IP address in the **IP Address** field, and then enter the subnet mask in the **Subnet Mask** field.
2. Select the **On/Off** button to turn on/turn off the DHCP function in the **DHCP Server** field.
3. Enter the client IP address range in the **IP Pool Start Address** and **IP Pool End Address** fields.
4. Click **Next**. The Wireless Settings screen will be displayed (refer to Figure 25).
**Setup Wizard - Wireless Settings**

The Wireless Settings screen allows you to set up the SSID and radio channel used for the wireless connection.

**Figure 25** Wireless Settings Screen

1. Select the channel you want to use from the **Channel** drop-down menu.

2. Specify the SSID to be used by your Wireless Network in the **SSID** field. If there are other wireless networks in your area, you should give your wireless network a unique name.
CHAPTER 4: RUNNING THE SETUP WIZARD

**Setup Wizard - Configuration Summary**

When you have completed the Setup Wizard, a configuration summary will appear. Verify the configuration information of the Router and then click **Apply** to save your settings. 3Com recommends that you print out this page for your records.

**Figure 26** Configuration Summary Screen

![Configuration Summary Screen](image)

Your Router is now configured and ready for use.

See **Chapter 5** for a detailed description of the Router configuration.
5 CONFIGURING THE ROUTER

Navigating Through the Router Configuration screens
This chapter describes all the screens available through the Router configuration screens, and is provided as a reference. To get to the configuration screens, enter the Router’s default IP in the location bar of your browser. The default IP is http://192.168.1.1.

However, if you changed the Router LAN IP address during initial configuration, use the new IP address instead. Enter your password to login to the management interface. (The default password is admin).

Main Menu
The main menu is located on the left side, as shown in Figure 27. When you click on an item from the main menu, the corresponding screen will then appear in the center.

Welcome Screen
The Welcome screen shows the current software information.

Status
Figure 27 Welcome Screen
LAN Settings

Your Router is equipped with a DHCP server that will automatically assign IP addresses to each computer on your network. The factory default settings for the DHCP server will work with most applications. If you need to make changes to the settings, you can do so.

The LAN settings screen allows you to:

- Change the default IP address of the Router. The default IP is 192.168.1.1
- Change the Subnet Mask. The default setting is 255.255.255.0
- Enable/Disable the DHCP Server Function. The default is ON (Enabled).
- Specify the Starting and Ending IP Pool address. The default is Starting: 2 / Ending: 254.
- Specify the IP address Lease Time. The default is Half day.
- Specify a local Domain Name. The default is NONE.
- Specify the IP address of 3Com NBX call processor.

The Router will also provide a list of all client computers connected to the Router.

LAN Settings

The LAN Settings screen is used to specify the LAN IP address of your Router, and to configure the DHCP server.

Figure 28  LAN Settings Screen
1 Enter the Router’s IP Address and Subnet Mask in the appropriate fields. The default IP address is 192.168.1.1.

2 If you want to use the Router as a DHCP Server, select On in the DHCP Server field.

3 Enter the IP address range in the IP Pool Start Address and IP Pool End Address fields.

4 Specify the DHCP Lease time by selecting the required value from the Lease Time drop-down menu. The lease time is the length of time the DHCP server will reserve the IP address for each computer.

5 Specify the Local Domain Name for your network (this step is optional).

6 Enter the IP address of the NBX Call Processor in the 3Com NBX Call Processor field (this step is optional).

7 Check all of your settings, and then click Apply.

**DHCP Clients List**

The DHCP Clients List provides details on the devices that have received IP addresses from the Router. The list is only created when the Router is set up as a DHCP server. A maximum of 253 clients can be connected to the Router.

![DHCP Clients List Screen](image)

For each device that is connected to the LAN, the following information is displayed:

- **IP address** — The Internet Protocol (IP) address issued to the client machine.
- **Host Name** — The client machine’s host name, if configured.
- **MAC Address** — The Media Access Control (MAC) address of the client’s network card.
- **Client Type** — Whether the client is connected to the Router by wired or wireless connection.
- Check the *Fix* checkbox to permanently fix the IP address.
- Click *Release* to release the displayed IP address.
- Click *New* to allocate an IP address to a MAC address (refer to Figure 30). Enter the required details and click *Apply* to save your settings.

**Figure 30** Fixed Mapping Clients List Screen

The DHCP server will give out addresses to both wired and wireless clients.
The Wireless Settings screens allow you to configure the settings for the wireless connections.

You can enable or disable the wireless connection for your LAN. When disabled, no wireless PCs can gain access to either the Internet or other PCs on your wired or wireless LAN through this Router.

**Figure 31** Wireless Settings Screen

There are seven tabs available:

- Configuration
- Encryption
- Connection Control
- Client List
- WDS
- Advance
- Profile
Configuration

The Wireless Configuration Screen allows you to turn on/turn off the wireless function, and set up basic wireless settings.

Figure 32  Wireless Configuration Screen

To enable the wireless function:

1. Check Enable Wireless Networking checkbox.
2. Select the wireless channel you want to use from the Channel drop-down menu.
3. Specify the SSID to be used by your wireless network in the SSID field. If there are other wireless networks in your area, you should give your wireless network a unique name.
4. Enable or disable SSID Broadcast.

A feature of many wireless network adapters is that a computer's SSID can be set to ANY, which means it looks randomly for any existing wireless network. The available networks are then displayed in a site survey, and your computer can select a network. By clicking Disable, you can block this random search, and set the computer’s SSID to a specific network (for example, WLAN). This increases network security. If you decide to enable SSID Broadcast, ensure that you know the name of your network first.

5. Select whether your Router will operate in 11b mode only, 11g mode only, or mixed 11b and 11g from the Wireless Mode drop-down menu.
6. Click Apply.
**Encryption**

This feature prevents any non-authorized party from reading or changing your data over the wireless network.

**Figure 33** Encryption Screen

Select the wireless security mode that you want to use from the drop-down menu, and click **Apply**. There are five selections:

- Disabled (see page 45)
- 64-bit WEP (see page 46)
- 128-bit WEP (see page 47)
- WPA-PSK (no server) (see page 48)
- WPA (with RADIUS Server) (see page 49)

**Disabled**

In this mode, wireless transmissions will not be encrypted, and will be visible to everyone. However, when setting up or debugging wireless networks, it is often useful to use this security mode.
64-bit WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your Router and wireless client devices to use WEP.

Figure 34  64-bit WEP Screen

To enable 64-bit WEP:

1 You can enter the 64-bit WEP key manually:
   - enter the WEP key as 5 pairs of hex digits (0-9, A-F).

Or you can generate the 64-bit WEP key automatically:
   - enter a memorable passphrase in the Passphrase box, and then click Generate to generate the hex keys from the passphrase.

For 64-bit WEP, you can enter up to four keys, in the fields Key 1 to Key 4. The radio button on the left hand side selects the key that is used in transmitting data.

Note that all four WEP keys on each device in the wireless network must be identical.

2 Click Apply.
128-bit WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be set up on your Router and wireless client devices to use WEP.

**Figure 35** 128-bit WEP Screen

To enable 128-bit WEP:

1. You can enter the 128-bit WEP key manually:
   - enter your WEP key as 13 pairs of hex digits (0-9, A-F).

   Or you can generate the 128-bit WEP key automatically:
   - enter a memorable passphrase in the *Passphrase* box, and then click *Generate* to generate the hex keys from the passphrase.

   *The WEP keys on each device on the wireless network must be identical.*

   *In 128-bit WEP mode, only one WEP key can be specified.*

2. Click *Apply.*
WPA-PSK (no server)

WPA (Wi-Fi Protected Access) provides dynamic key changes and constitutes the best security solution. If your network does not have a RADIUS server. Select the no server option.

Figure 36  WPA-PSK (no server) Screen

1 Select WPA-PSK (no server) from the WPA drop-down menu.
2 Select WPA mode from the drop-down menu, three modes are supported: WPA, WPA2, and Mixed mode.
3 Select Encryption technique from the drop-down menu, four options are available: TKIP, AES, Auto for WPA AES for WPA2, and AES for both WPA and WPA2.
4 Enter the pre-shared key in the Pre-shared Key (PSK) field. The pre-shared key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between 8 and 63 characters long and can include spaces and symbols. Each client that connects to the network must use the same key.
5 If you want the key that you enter to be shown on the screen as a series of asterisks (*), then check the Hide PSK checkbox.
6 Click Apply.
WPA (with RADIUS Server)

WPA (Wi-Fi Protected Access) provides dynamic key changes and constitutes the best security solution. This function requires that a RADIUS server is running on the network.

**Figure 37** WPA (with RADIUS Server) Screen

1. Select WPA with RADIUS server from the *Security Mode* drop-down menu.
2. Select WPA mode from the drop-down menu, three modes are supported: WPA, WPA2, and Mixed mode.
3. Select Encryption technique from the drop-down menu, four options are available: TKIP, AES, Auto for WPA AES for WPA2, and AES for both WPA and WPA2.
4. Enter the IP address of the RADIUS server on your network into the *RADIUS Server* field.
5. Enter the port number that the RADIUS server is operating on in the *RADIUS Port* field.
6. Enter the key for the RADIUS server in the *RADIUS Key* field.
7. By default, the WPA keys are changed every hour, but if you want to change this setting, you can do so by specifying the required time in the *Re-key Interval* field.
8. Click *Apply*. 
Connection Control  This feature is used to filter the clients based on their MAC addresses.

Check the *Enable MAC Address Filtering* checkbox, the Connection Control screen will appear.

**Figure 38**  Connection Control Screen

There are two options available in the *Access rule for registered MAC address* field:

- if you click *Allow*, this means only the MAC addresses registered here in the list will be allowed to access the Router via wireless link.
- if you click *Deny*, this means the registered MAC addresses will not be able to access the Router via wireless link.

Use the *MAC Address Filtering List* to quickly copy the MAC addresses of the current wireless clients into the list table. You can define up to 32 MAC addresses to the list.

You can click *Clear* to delete the current entry in the list.
**Client List**  You can view the list of all wireless clients that are connected to the Router.

**Figure 39**  Client List Screen

Click *Refresh* to update the list.

**WDS Settings**  The Router supports WDS (Wireless Distribution System). WDS enables one or more Access Points to rebroadcast received signals to extend range and reach, though this can affect the overall throughput of data.

**Figure 40**  Wireless WDS Settings Screen

1. Check the *Enable WDS Function* checkbox.
2. To refresh the list of available access points, click *Rescan Wireless Networking*. 
Click **Add** to add the MAC address of the AP to the list, the add WDS screen will appear (refer to Figure 41).

**Figure 41**  Add WDS screen

Enter the MAC address(es) of one or more access points in the **AP MAC Address** table, and click **Apply**.

**Advance**  The Advance screen allows you to configure detailed settings for your wireless connection.

**Figure 42**  Wireless Advanced Setting screen

There are six parameters that you can configure:

- **Beacon Interval**: this represents the amount of time between beacon transmissions.
Wireless Settings

- **DTIM Interval**: A DTIM (Delivery Traffic Indication Message) is a countdown mechanism used to inform your wireless clients of the next window for listening to broadcast and multicast messages.

- **Fragmentation Threshold**: this is the maximum size for directed data packets transmitted. The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur.

- **RTS Threshold**: RTS stands for Request to Send, this parameter controls what size data packet the low level RF protocol issues to an RTS packet.

- **CTS Protection Mode**: CTS stands for Clear to Send. CTS Protection Mode boosts the Router's ability to intercept 802.11b/802.11g transmissions. Conversely, CTS Protection Mode decreases performance. Leave this feature disabled unless you encounter severe communication difficulties between the Router and your wireless clients.

- **WMM Mode**: Wireless Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard.

**Profile**

This feature is used to quickly set up the configuration parameters and save them into one profile for easy connection.

**Figure 43** Profile Screen
Internet Settings

You can configure the settings for your DSL connection.

ATM PVC

This feature is used to configure the parameters for your DSL connection. The information necessary to complete these screens should be obtained from your ISP. Check with your ISP first to find out what type of connection you should choose.

Figure 44  ATM PVC Screen

You should see the first entry already contains information that’s been configured using the Wizard in the initial setup. If you want to change that information or set up other connection, click Edit.

There are six options available for the DSL connection mode:

- **PPPoE** — PPP over Ethernet, providing routing for multiple PCs (see page 55)
- **PPPoA** — PPP over ATM, providing routing for multiple PCs (see page 57)
- **Bridge Mode** — RFC1483 Bridged Mode, for single PCs only (see page 59)
- **Routing Mode over ATM** — RFC1483 Routed Mode, for multiple PCs (see page 61)
- **Dynamic/Fixed IP in 1483 Bridge Mode (for multiple PCs)** (see page 63)
- **Disable** — To disable the Internet connection function (see page 64)

Click Edit to set the detailed settings.
PPP over Ethernet, provides routing for multiple PCs. To configure this function correctly, you should obtain the information from your ISP.

**Figure 45**  PPPoE Settings Screen

1. Select **PPPoE** from the Protocol drop-down menu.
2. Enter the IP address and Subnet Mask information provided by your ISP into the IP address and Subnet Mask fields.
3. Enter the user name assigned to you by your ISP in the Username field. And enter the password assigned to you by your ISP in the Password field. Re-enter your password in the Confirm Password field.
4. Select the connection type from the Connect Type drop-down menu.
   - **Always Connected** means that Internet connection to your ISP is always on.
   - **Auto - Triggered by Traffic** means your Router will automatically connect to your ISP every time a PC needs to access the Internet.
   - **Manual - Start in Disconnected** means that after re-booting the Router, the Internet connection will need to be re-established manually by the user.
   - **Manual - Start in Connected** means that after re-booting the Router, it will automatically establish a connection to your ISP.
CHAPTER 5: CONFIGURING THE ROUTER

- **Manual - Start in Last State** means that after re-booting the Router, the Internet connection will stay in the previous condition before the reboot.

5 If you want your Router to automatically disconnect from the Internet after a period of inactivity, specify a time in the **Idle Time (Minutes)** field. (Enter a value of 0 to disable this timeout).

6 Enter the **Maximum Transmission Unit (MTU)** value supplied by your ISP. If you do not know this, leave it at the default value.

7 The Router supports the IP Control Protocol (IPCP) Subnet Mask Support feature, check the **IPCP subnet** checkbox to enable it.

8 To use the IPCP Subnet Mask Support for the DHCP clients, check the **IPCP Subnet Populate DHCP Server** checkbox.

9 Enter the VPI and VCI values provided by your ISP in the **VPI** and **VCI** fields. You can click **Auto Search** to automatically find out this information.

10 Select the encapsulation type (LLC or VC MUX) in the **Encapsulation** field. This information should be provided to you by your ISP.

11 Select the type of Quality of Service (CBR, UBR or VBR) in the **QoS** field.

   - **CBR (constant bit rate):** the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.

   - **VBR (variable bit rate):** QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

   - **UBR (unspecified bit rate):** the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer communications applications. The UBR service may be considered as "best effort service".

12 Enter the PCR/SCR/MBS values. This information should be provided to you by your ISP.
13 Click Apply.

**PPPoA**

PP over ATM, this is a popular choice among European DSL providers. To configure this function correctly, you should obtain the information from your ISP.

**Figure 46** PPPoA Settings Screen

1 Select **PPPoA** from the *Protocol* drop-down menu.

2 IP assigned by ISP:
   - Select **Yes**, if your ISP assigns your IP address dynamically, and proceed to next step.
   - If your ISP has assigned you a fixed or static IP address, select **No** in the *IP assigned by ISP* field. Then enter the IP address and Subnet Mask information provided by your ISP into the *IP address* and *Subnet Mask* fields.

3 Enter the user name assigned to you by your ISP in the *Username* field. And enter the password assigned to you by your ISP in the *Password* field. Re-enter your password in the *Confirm Password* field.
Select the connection type from the Connect Type drop-down menu.

- **Always Connected** means the Internet connection to your ISP is always on.
- **Auto - Triggered by Traffic** means your Router will automatically connect to your ISP every time a PC needs to access the Internet.
- **Manual - Start in Disconnected** means that after re-booting the Router, the Internet connection will need to be re-established manually by the user.
- **Manual - Start in Connected** means that after re-booting the Router, it will automatically establish connection to your ISP.
- **Manual - Start in Last State** means that after re-booting the Router, the Internet connection will stay in the previous condition before the reboot.

If you want your Router to automatically disconnect from the Internet after a period of inactivity, specify a time in the Idle Time (Minutes) field. (Enter a value of 0 to disable this timeout).

Enter the MTU value supplied by your ISP. If you do not know this, leave it at the default value.

The Router supports the IP Control Protocol (IPCP) Subnet Mask Support feature, check the IPCP subnet checkbox to enable it.

To use the IPCP Subnet Mask Support for the DHCP clients, check the IPCP Subnet Populate DHCP Server checkbox.

Enter the VPI and VCI parameters provided to you by your ISP in the VPI and VCI fields. You can click Auto Search to automatically find out this information.

Select the encapsulation type (LLC or VC MUX) in the Encapsulation Type field. This information is provided to you by your ISP.

Select the type of Quality of Service (CBR, UBR or VBR) in the QoS field.

- **CBR (constant bit rate)**: the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.
- **VBR (variable bit rate)**: QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is
used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

- UBR (unspecified bit rate): the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer communications applications. The UBR service may be considered as “best effort service”.

12 Enter the PCR/SCR/MBS values.
13 Click Apply.

**Bridge Mode**

If your ISP limits access to the Internet to specific computers, this means that traffic to/from these computers only will be forwarded. In this case, Bridge Mode is used to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet. Check with your ISP to determine if this mode is used for your DSL connection. To configure the settings correctly, you should obtain the information from your ISP.

**Figure 47** Bridge Mode Screen

1 Select **Bridge Mode** from the **Protocol** drop-down menu.
2 Enter the VPI and VCI parameters in the **VPI** and **VCI** fields. You can click **Auto Search** to automatically find out this information.
3 Select the encapsulation type (LLC or VC MUX) in the **Encapsulation Type** field. This information should be provided to you by your ISP.
4 Select the type of Quality of Service that you want from the QoS Class drop-down menu.

- CBR (constant bit rate): the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.

- VBR (variable bit rate): QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

- UBR (unspecified bit rate): the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer communications applications. The UBR service may be considered as "best effort service".

5 Enter the PCR/SCR/MBS values.

6 Click Apply.
Routing Mode over ATM (RFC 1483 Routed Mode)

This mode is commonly used with either dynamic or static IP addressing. In this mode the WAN ADSL port will be configured with an IP address provided by the ISP. To configure the settings correctly, you should obtain the information on this screen from your ISP.

**Figure 48**  Routing Mode over ATM Screen

1. Select *Routing Mode over ATM* from the *Protocol* drop-down menu.
2. Enter the IP address, Subnet Mask and Default Gateway information provided by your ISP into the *IP address*, *Subnet Mask* and *Default Gateway* fields.
3. Check the *DNS Automatic from ISP* checkbox, if your ISP automatically configure DNS. However, if you need to configure DNS manually, enter the IP address in the *DNS Address* field. (If your ISP uses a secondary DNS, enter the IP address in the *Secondary DNS Address* field).
4. Enter the host name in the *Host Name* field.
5. If your ISP uses DHCP to automatically assign IP addresses, check the *DHCP Client* checkbox.
6. Enter the VPI and VCI parameters provided to you by your ISP in the *VPI* and *VCI* fields. You can click *Auto Search* to automatically find out this information.
7. Select the encapsulation type (LLC or VC MUX) in the *Encapsulation* field. This information should be provided to you by your ISP.
Select the type of Quality of Service that you want from the **QoS Class** drop-down menu.

- **CBR (constant bit rate):** the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.

- **VBR (variable bit rate):** QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

- **UBR (unspecified bit rate):** the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer communications applications. The UBR service may be considered as "best effort service".

Enter the PCR/SCR/MBS values.

Click **Apply**.
Dynamic/Fixed IP in 1483 Bridge Mode (For Multiple PCs)

In this example, the ISP uses fixed/dynamic IP to provide the Internet connection. To configure this function correctly, you should obtain the information on this screen from your ISP.

**Figure 49** Dynamic/Fixed IP for Bridge Mode Screen

1. Select *Dynamic/Fixed IP in 1483 Bridge Mode* from the *Protocol* drop-down menu.

2. Enter the IP address, Subnet Mask and Default Gateway information provided by your ISP into the *IP address*, *Subnet Mask* and *Default Gateway* fields.

3. Check the *DNS Automatic from ISP* checkbox, if your ISP automatically configures DNS. However, if you need to configure DNS manually, enter the IP address in the *DNS Address* field. (If your ISP uses a secondary DNS, enter the IP address in the *Secondary DNS Address* field).

4. Enter the host name in the *Host Name* field.

5. If your ISP uses DHCP to automatically assign IP addresses, check the *DHCP Client* checkbox.

6. Enter the VPI and VCI parameters provided by your ISP in the *VPI* and *VCI* fields. You can click *Auto Search* to automatically find out this information.

7. Select the encapsulation type (LLC or VC MUX) in the *Encapsulation* field. This information will have been provided to you by your ISP.
Select the type of Quality of Service that you want from the QoS Class drop-down menu.

- CBR (constant bit rate): the CBR service class is intended for real-time applications, for example, those requiring tightly constrained delay and delay variation, such as voice and video applications. The consistent availability of a fixed quantity of bandwidth is considered appropriate for CBR service.

- VBR (variable bit rate): QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QoS. Compare with ABR, CBR, and UBR.

- UBR (unspecified bit rate): the UBR service class is intended for delay-tolerant or non-real-time applications, for example, those which do not require tightly constrained delay and delay variation, such as traditional computer communications applications. The UBR service may be considered as "best effort service".

Enter the PCR/SCR/MBS values.

Click Apply.

Disable

Selecting this option means that you do not want your Router to connect to the Internet.

Figure 50  Disable Internet Connection Screen
DNS

Domain Name Service (or Server) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they’re easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

Check with your ISP for information on this screen.

Figure 51  DNS Screen

If the DNS information is automatically provided by your ISP every time you connect to it, check the Automatic from ISP checkbox.

If your ISP provided you with specific DNS addresses to use, enter them into the appropriate fields on this screen and click Apply.

Many ISPs do not require you to enter this information into the Router. If you are using a Static IP connection type, you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is Dynamic, PPPoA or PPPoE, it is likely that you do not have to enter a DNS address.
Hostname & Clone MAC address

To configure the Hostname and Clone MAC Address information for your Router, select Internet Settings, then go to the Clone MAC address tab. The Hostname and MAC Address screen displays.

**Figure 52  Hostname and MAC Address Screen**

1. Some ISPs require a host name. If your ISP has this requirement, enter the host name in the Host Name field.

2. Three different ways to configure the WAN MAC Address:
   - If your ISP requires an assigned MAC address, enter the values in the WAN MAC address field.
     
     or
   
     - If the computer you are now using is the one that was previously connected directly to the cable modem, click Clone.

     or
   
     - To reset the MAC Address to the default, click Reset MAC.

3. Click Apply to save the settings.
From these screens, you can configure settings for the firewall.

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but 3Com recommends that you leave the firewall enabled whenever possible.

**SPI**

Stateful Packet Inspection (SPI) - The Intrusion Detection Feature of the Router limits access for incoming traffic at the WAN port.

This feature is called a "stateful" packet inspection, because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

To enable the firewall function:

1. Select the level of protection (High, Medium, or Low) that you desire from the *Firewall level* drop-down menu.
2. Click *Apply*. 
For low and medium levels of firewall protection, refer to Figure 54.

For high level of firewall protection, refer to Figure 55.

**Figure 54  Low and Medium Level Firewall Protection Screen**

When abnormal network activity occurs, an alerting email will be sent out to you. Enter the following information to receive the email:

- Your E-mail Address
- SMTP Server Address
- User name
- Password
If you select high level of protection, you will need to configure additional parameters for the firewall.

- **Fragmentation half-open wait** - Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the Router drops the un-assembled packet, freeing that structure for use by another packet.
- **TCP SYN wait** - Defines how long the software will wait for a TCP session to synchronize before dropping the session.
- **TCP FIN wait** - Specifies how long a TCP session will be maintained after the firewall detects a FIN packet.
- **TCP connection idle timeout** - The length of time for which a TCP session will be managed if there is no activity.
- **UDP session idle timeout** - The length of time for which a UDP session will be managed if there is no activity.
- **H.323 data channel idle timeout** - The length of time for which an H.323 session will be managed if there is no activity.
- Total incomplete TCP/UDP sessions HIGH - Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
- Total incomplete TCP/UDP sessions LOW - Defines the rate of new unestablished sessions that will cause the software to stop deleting half-open sessions.
- Incomplete TCP/UDP sessions (per min) HIGH - Maximum number of allowed incomplete TCP/UDP sessions per minute.
- Incomplete TCP/UDP sessions (per min) LOW - Minimum number of allowed incomplete TCP/UDP sessions per minute.
- Maximum incomplete TCP/UDP sessions number from same host - Maximum number of incomplete TCP/UDP sessions from the same host.
- Incomplete TCP/UDP sessions detect sensitive time period - Length of time before an incomplete TCP/UDP session is detected as incomplete.
- Maximum half-open fragmentation packet number from same host - Maximum number of half-open fragmentation packets from the same host.
- Half-open fragmentation detect sensitive time period - Length of time before a half-open fragmentation session is detected as half-open.
- Flooding cracker block time - Length of time from detecting a flood attack to blocking the attack.
Special Applications

Special Applications let you choose specific ports to be open for specific applications to work properly with the Network Address Translation (NAT) feature of the Router.

Figure 56 Special Applications Screen

A list of popular applications has been included to choose from. Select your application from the Popular Applications drop-down menu. Then select the row that you want to copy the settings to from the Copy To drop-down menu, and click Copy To. The settings will be transferred to the row that you specified. Click Apply to save the setting for that application.

If your application is not listed, you will need to check with the application vendor to determine which ports need to be configured. You can manually enter the port information into the Router.

To manually enter the port information:

1. Specify the trigger port (the one used by the application when it is initialized) in the Trigger Port column, and specify whether the trigger is TCP or UDP.

2. Specify the Public Ports used by the application, that will need to be opened up in the firewall for the application to work properly. Also specify whether these ports are TCP or UDP.

3. Check the Enabled checkbox, then click Apply.
Virtual Servers  

The Virtual servers feature allows you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, machines from the Internet cannot get to them because they cannot be 'seen'.

If you need to configure the Virtual Server function for a specific application, you will need to contact the application vendor to find out which port settings you need.

The maximum number of virtual servers that can be configured is 20.

Figure 57  Virtual Servers Screen

A list of popular servers has been included to choose from. Select the server from the Popular servers drop-down menu. Then click Add, your selection will be added to the table.

If the server that you want to use is not listed in the drop-down menu, you can manually add the virtual server to the table.

To manually configure your virtual servers:

1. Enter the IP address, and the description in the spaces provided for the internal machine.
2. Select the protocol type (TCP, UDP, or both TCP and UDP) from the drop-down menu.
3. Specify the public port that will be seen by clients on the Internet, and the LAN port which the traffic will be routed to.
4 You can enable or disable each Virtual Server entry by checking or unchecking the appropriate Enabled checkbox.

5 Click Apply to save the changes for each Virtual Server entry.

**DMZ**

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. This may be necessary if the NAT feature is causing problems with an application such as a game or video conferencing application.

**Figure 58  DMZ Screen**

Use this feature on a temporary basis. The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ:

1 Check the Enable 1-to-1 NAT checkbox.

2 Enter the last digits of the LAN IP address in the Client PC IP Address field. Enter the IP address (if known) that will be accessing the DMZ PC into the Public IP Address field, so that only the computer on the Internet at this address can access the DMZ PC without firewall protection. If the IP address is not known, or if more than one PC on the Internet will need to access the DMZ PC, then set the Public IP Address to 0.0.0.0.

3 Click Apply.
**Schedule Rule**  The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Define the time in this screen, and define the rules in the *PC Privileges* screen (see page 75).

**Figure 59  Schedule Rule Screen**

1. **Click** *Add Rule* to add a schedule rule (a screen similar to Figure 60 will appear).

**Figure 60  Add Schedule Rule Screen**

2. Enter a name and comment for the schedule rule in the *Name* and *Comment* fields.

3. Specify the schedule rules for the required days and times - note that all times should be in 24 hour format.

4. **Click** *Apply*.
PC Privileges

The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

You can define the traffic type permitted or not-permitted to the Internet.

Figure 61  PC Privileges Screen

To edit or delete specific existing filtering rules, click on Edit or Delete for the appropriate filtering rule.

To configure a new filtering rule:

1 Check the Enable Filtering Function checkbox.
2 Click Add PC (a screen similar to Figure 62 will appear).

Figure 62  PC Privileges Add PC Screen
3 Enter a description in the Client PC Description field, and the IP address or IP address range into the Client PC IP Address fields.

4 To bypass the URL Filter and Content Filter, check the corresponding Bypass checkbox.

If you check the two options: Bypass URL Filter, and Bypass Content Filter, then the Web sites and keywords defined in this screen will not be filtered out.

5 Select the services to be blocked. A list of popular services is given on this screen, to block a particular service, check the appropriate Blocking checkbox.

If the service to be restricted is not listed here, you can enter a custom range of ports at the bottom of the screen, under User Defined Blocked Ports.

6 If you want the restriction to apply only at certain times, select the schedule rule to apply from the Schedule Rule drop-down menu.

Note that schedule rules are defined on the Schedule Rules screen (see page 74).

7 Click Apply to add the settings.
**URL Filter**

To configure the URL filter feature, use the table on the URL Filter screen to specify the Web sites (www.somesite.com) and/or keywords you want to filter on your network.

For example, entering a keyword of *xxx* would block access to any URL that contains the string *xxx*.

**Figure 63**  URL Filter Screen

1. Check the *Enable URL Filtering Function* checkbox.
2. Enter the URL address or keywords in the *URL/Keyword* field.
3. Select *Denied or Allowed* from the *Mode* drop-down menu.

To complete this configuration, you will need to create or modify the filtering rule in the PC Privileges screen (see page 75).

From the *PC Privileges Add PC* screen (Figure 62), if you check the two options: *Bypass URL Filter*, and *Bypass Content Filter*, then the Web sites and keywords defined in this screen will not be filtered out.
Content Filter
You can use the list on the Content Filter screen to specify the type of content that you want to filter out.

*The Router comes with a 14-day free trial of the 3Com Content Filter Service (3CSBCFS). To activate the 14-day free trial of the service, you must first register your Router at www.3com.com. To continue using the service after the trial period, you must purchase the 12-month subscription license.*

**Figure 64** Content Filter Screen

To configure the Content Filter feature:

1. Check the *Enable Content Filtering Function* checkbox.
2. Select the server that you want to use from the *Content Filter Server* drop-down menu. If the server you want to use is not listed, enter the server address manually.
3. Define the time in the *Server Timeout* field (the default value is 3000ms). If the Content Filter Server does not respond within this time period, the Router will use the default content filter rule. The default rule is either *Allow* or *Deny None of the above (Uncategorized URL)*. You can configure this rule at the bottom of the Content Filter screen.
4 If you are not sure about your subscription status, click **CHECK** in **Subscription Filtering Status** to find out if you have a current, valid subscription.

5 Subjects are listed under **Core Categories** and **Productivity Categories**. You can define what content should be viewed/blocked using the **Allow/Deny** option. The **Deny** option is used to filter out the content that contains the specific subject matter. Content with a specific subject matter will not be filtered out if the **Allow** option is checked.

6 Click **Apply** for the changes to take effect.

**Server Control**

The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Restriction can be set for the servers.

You can define the traffic type permitted or not-permitted to the Internet.

**Figure 65  Server Control Screen**

In the **Service Filtering Mode**, select one option:

- Denied except listed below.
- All Allowed.

Click **Add** to add a new entry to the table (see **Figure 66**).
1 Enter a description in the **Server Description** field, and the IP address or IP address range into the **Server IP Address** fields.

2 Select the services that will be allowed. A list of popular services is given on this screen, to unblock a particular service, check the appropriate **Allowed** checkbox. If the service to be allowed is not listed here, you can enter a custom range of ports at the bottom of the screen, under **User Defined Service Ports**.

3 Select the time that the rule will be enforced from the **Scheduling Rule** drop-down menu.

4 Click **Apply** to save the settings.
Quality of Service

The QoS (Quality of Service) function allows you to differentiate your network traffic and provide it with high-priority forwarding service.

QoS Settings

The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. This QoS function allows you to classify traffic of applications and provides them with differentiated services (Diffserv).

Figure 67 QoS Settings Screen

Define the minimum percentage of bandwidth for each type of traffic.

Traffic Mapping

You can define up to 16 rules to classify traffic into Diffserv forwarding groups and outgoing VCs in this screen.

Figure 68 Traffic Mapping screen
Click Add to add a new traffic class rule (see Figure 69).

**Figure 69** Add New Traffic Class Rule Screen

**Traffic Statistics** This screen shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours. This screen automatically updates every 5 minutes.

**Figure 70** Traffic Statistics Screen
From the Advanced screen, you can configure:

- Security
- Static Routes
- RIP
- DDNS
- SNMP
- Syslog
- Proxy Arp

**Security**

Use the Security screen to set the advanced security settings for the Router.

Figure 71 Security Screen

- **NAT** — Before you enable NAT (Network Address Translation), make sure you have changed the administrator password. NAT is the method by which the Router shares the single IP address assigned by your ISP with the computers on your network.

  This function should only be disabled by advanced users, and if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and
you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur.

■ IPSEC NAT-T Pass-through — NAT-T (NAT Traversal) is an Internet Draft proposed to IETF in order to help the problems associated with passing IPsec traffic through NAT Routers. For NAT-T to work, both ends of the connection need to support this function. Ensure that you select NAT-T only if it is needed as it will reduce LAN-WAN throughput. This Router supports NAT-T draft 2 implementation.

■ Universal Plug and Play — This is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are Universal Plug and Play compliant. Some applications require the Router’s firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports and in some instances setting trigger ports. An application that is Universal Plug and Play compliant has the ability to communicate with the Router, basically “telling” the Router which way it needs the firewall configured. The Router ships with the Universal Plug and Play feature disabled. If you are using any applications that are Universal Plug and Play compliant, and want to take advantage of the Universal Plug and Play features, you can enable this feature. Simply check the Enable Universal Plug and Play checkbox. Click Apply to save the change.

■ WAN Ping Blocking — Computer hackers use what is known as “Ping” to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an Internet Control Message Protocol (ICMP) Ping from the outside. This heightens the level of security of your Router. To turn off the ping response, check Block ICMP Ping and click Apply; the Router will not respond to an ICMP ping from the Internet.

■ MSS Clamping — You might not be able to browse some Web sites or to send email messages that contain attachments from an Internet Connection Sharing client computer if your outbound connection is through a Windows XP-based Internet Connection Sharing host computer that uses Point-to-Point Protocol over Ethernet (PPPoE). This issue may occur if the Windows XP-based Internet Connection Sharing host computer uses a smaller Maximum Transmission Unit (MTU) size on the WAN interface (the PPPoE connection to the Internet) than it uses on the private interface (the Ethernet connection to the Internet Connection Sharing client). If a packet is larger than
the MTU size on the WAN interface, the client sends an Internet Control Message Protocol (ICMP) error to the external server to request that the server negotiate the TCP Maximum Segment Size (MSS). However, this message may be blocked by some firewalls. When this occurs, the packet is dropped. To allow the message to go through the firewall, enable MSS Clamping. MSS clamping will make Internet Connection Sharing set the MSS value low enough to match the external interface.

- Remote Administration — This feature allows you to make changes to your Router's settings from anywhere on the Internet. Four options are available:
  - If you do not want to use this feature, select Disable Remote Administration.
  - Select Enable administration from a single Internet Host, and enter the IP address, to allow only one computer to use the remote administration. This is more secure, as only the specified IP address will be able to manage the Router.
  - Select Enable administration from a whole Subnet Internet Host, and enter the IP address and subnet mask, to allow PCs from that specific subnet group to use the remote administration.
  - Select Enable administration from any Internet Host, this allows any computer to access the Router remotely.

*Before you enable this function, ensure that you have set the Administration Password.*
Static Routes

You can configure static routes in this screen.

To add a static route entry to the table, click Add.

To change an existing entry, click Edit. To delete an entry, click Delete.

**Figure 72  Static Routes Screen**

This screen shows a list of current static route entries. For each entry, the following information is displayed:

- **Index** — the index of the entry.
- **Network Address** — the network address of the route.
- **Subnet Mask** — the subnet mask of the route.

*A network address of 0.0.0.0 and a subnet mask of 0.0.0.0 indicates the default route.*

- **Gateway** — the router used to route data to the network specified by the network address.

After you have finished making changes to the table, click Apply.
RIP  (Routing Information Protocol) - RIP allows the network administrator to set up routing information on one RIP-enabled device and send that information to all RIP-enabled devices on the network.

Figure 73  RIP Parameter Screen

You can set up RIP independently on both LAN and WAN interfaces.

1  Check the *Enable RIP* checkbox.

2  Check the *Enable Auto summary* checkbox. Auto summarization sends simplified routing data to other RIP-enabled devices rather than full routing data.

3  Select the *Operation Mode*:

   ■  *Disabled* — RIP is not enabled for the WAN or LAN interface.

   ■  *Enabled* — RIP is enabled for the WAN or LAN interface. The router will transmit RIP update information to other RIP-enabled devices.

   ■  *Silent* — RIP is enabled, however the Router only receives RIP update messages, it will not transmit any messages itself.

4  In the *Version* field, select 1 or 2.

   3Com recommends that you only use RIPv1 if there is an existing RIP-enabled device on your network that does not support RIPv2. In all other cases, you should use RIPv2.
5 Use the Poison Reverse drop-down menu to enable or disable Poison Reverse on the Router. Enabling Poison Reverse on your Router allows it to indicate to other RIP-enabled devices that they have both routes that point to each other, preventing data loops.

6 Use the Authentication Required field to choose the mode of authentication:
   - None — Switches off authentication on the specified interface.
   - Password — An unencrypted text password that needs to be set on all RIP-enabled devices connected to this Router. RIP information is not shared between devices whose passwords do not match.

7 In the Authentication Code field, enter the password that is required if the Password option has been selected.

8 Click Apply.

DDNS

The Router provides a list of dynamic DNS providers for you to choose from. Dynamic Domain Name Server (DDNS) enables you to map a static domain name to a dynamic IP address.

The Router supports five DDNS providers:

- DynDNS.org
- TZO.com
- Dt DNS.com
- No-IP.com
- Zoneedit.com
Before you set up DDNS, you must obtain an account, password or key and static domain name from your DDNS provider.

DDNS is disabled by default.

**Figure 74**  Dynamic Domain Name Server (DDNS) Screen

1. Check *Enable DDNS*.
2. Select the provider, and then enter the necessary information provided by your DDNS provider.
3. Click *Apply*. 
SNMP (Simple Network Management Protocol) allows remote management of your Router by a PC that has an SNMP management agent installed.

Figure 75  SNMP Screen

To Configure SNMP Community:

1. In the Community column, enter the name of the SNMP communication channel. Your SNMP management agent needs to be configured with this name so that it can communicate with your Router.

2. In the Access column, select Read to allow the management agent to collect data (for example, bandwidth usage) from your Router. Select Write to allow the management agent to change the configuration of your Router.

3. Check the appropriate Valid checkbox to enable the communication channel.
You can configure your Router to send status messages to the SNMP management agent if a problem occurs on the network. To configure SNMP traps:

1. In the *IP Address* field, enter the IP address of the PC to which you want your Router to send status messages.
2. In the *Community* field, enter the name of the SNMP communication channel to which you want your Router to send status messages.
3. Set the *Version* field to match the version of trap messaging that your SNMP management agent supports. The Router supports V1 and V2c trap messaging.

**Syslog**

Using third party syslog software, this Syslog Server tool will automatically download the Router log to the specified server IP address.

**Figure 76** Syslog Server Screen

1. Check the *Enable Syslog Server* checkbox.
2. Enter the *Server LAN IP Address* in the space provided.
3. Click *Apply*. 
Proxy ARP

Proxy ARP is the technique in which one host, usually a Router, answers ARP requests intended for another machine. By "faking" its identity, the Router accepts responsibility for routing packets to the "real" or intended destination. This heightens the security for your network.

**Figure 77** Proxy ARP Screen

Enter the corresponding IP address in the *IP Address From* and *IP Address To* fields.
System Tools

These screens allow you to manage different parameters of the Router and perform certain administrative functions.

Restart Router

Sometimes it may be necessary to restart (or reboot) the Router. Restarting the Router from this screen will not delete any of your configuration settings.

Click the Restart the Router button to restart the Router.

Figure 78 Restart Router Screen

Configuration

Use this configuration screen to backup, restore or reset the configuration details of the Router.

Figure 79 Configuration Screen
Backup Configuration — You can save your current configuration by clicking the **Backup** button. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you backup your current configuration before performing a firmware update.

- **Restore Configuration Data** — The Restore Settings option will allow you to restore a previously saved configuration. Please select the configuration file using the **Browse** button and click **Restore**.

- **Reset to Factory Default** — Using this option will reset all of the settings in the Router to the factory default settings. It is recommended that you backup your settings before you restore all of the defaults. To restore the factory default settings, click **Reset**.

**Upgrade**

From time to time 3Com may release new versions of the Router’s firmware. Firmware updates contain improvements and fixes to problems that may have existed.

**Figure 80** Upgrade Screen

Please download the firmware file to your PC first, and then click **Browse** and select the firmware file. Click **Upgrade** to upload the firmware to the Router.
**Time Zone**  You can set the time settings for the Router on this screen.

**Figure 81  Time Zone Screen**

The Router keeps time by connecting to a Network Time Protocol (NTP) server. This allows the Router to synchronize the system clock to the Internet. The synchronized clock in the Router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes Daylight Saving, then check the checkbox for **Enable Daylight Saving**. The system clock may not update immediately. Allow at least 15 minutes for the Router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

You can specify which NTP servers the Router will use to update the system clock, although doing this should only be necessary if you are experiencing difficulty.
Ping  The ping tool is used to test if the network is working properly.

**Figure 82** Ping Screen

1. Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Ping*.
2. Select from the *Number of times to Ping* drop-down menu.
3. The Router keeps a log of the ping test, click *Clear Log* to delete the records.
**Traceroute**

Traceroute is the program that shows you the route over the network between two systems, listing all the intermediate routers a connection must pass through to get to its destination. It can help you determine why your connections to a given server might be poor, and can often help you figure out where exactly the problem is. It also shows you how systems are connected to each other, letting you see how your ISP connects to the Internet as well as how the target system is connected.

**Figure 83**  Traceroute Screen

1. Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Traceroute*.
2. The Router keeps a log of the traceroute test, click *Clear Log* to delete the records.
DNS Lookup

DNS Lookup is the process of resolving an IP address (i.e. 192.168.11.137) to a host name (i.e. xxxcompany.net).

**Figure 84** DNS Lookup Screen

1. Enter the IP address or domain name in the *IP Address or Domain Name* field, and click *Dns lookup*.

2. The Router keeps a log of the DNS lookup test, click *Clear Log* to delete the records.
You can use the Status Screen to view version numbers for your Router's software and hardware and check the status of connections to WAN, LAN and WLAN interfaces.

This screen shows Router status and statistics.

This screen shows ADSL modem status and statistics.
**ATM PVC Status**  
*Figure 87  ATM PVC Status Screen*

This screen shows ATM PVC status and statistics.

- Click *Release* to release the IP address from your ISP.
- Click *Renew* to obtain the IP address from your ISP.

**Routing Table**  
This screen displays details for the default routing used by your Router and any routing created using Static Routing or RIP.

*Figure 88  Routing Table Screen*
**Logs**  This screen shows any attempts that have been made to gain access to your network as well as the system activities.

**Figure 89  Logs Screen**

- Click **Help** to view the help file.
- Click **Save** to save the log to the hard disk as a text file. When prompted for a location to save the file to, specify a filename and location, and then click **OK**.
- Click **Clear** to clear the log (note that all current entries will be erased).
- Click **Refresh** to update the record.
Support/Feedback  
You can use the Support/Feedback screen to obtain support and help, and also provide feedback to 3Com.

Support  
Figure 90  Support Screen

This screen shows support information.

Feedback  
To provide feedback to 3Com, please click Provide Feedback, and this will connect you to the 3Com Web site.

Figure 91  Feedback Screen

This screen shows feedback information.
Basic Connection Checks

- Check that the Router is connected to your computers and to the telephone line, and that all the equipment is powered on. Check that the LAN Status and SYNC LEDs on the Router are illuminated, and that any corresponding LEDs on the NIC are also illuminated.

- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.

- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Router Configuration Screens

If you have connected your Router and computers together but cannot browse to the Router configuration screens, check the following:

- Confirm that the physical connection between your computer and the Router is OK, and that the LAN Status LEDs on the Router and network adapter are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.

- Ensure that you have configured your computer as described in Chapter 3. Restart your computer while it is connected to the Router to ensure that your computer receives an IP address.

- When entering the address of the Router into your web browser, ensure that you use the full URL including the http:// prefix (e.g. http://192.168.1.1).

- Ensure that you do not have a Web proxy enabled on your computer. Go to the Control Panel and click on Internet Options. Select the Connections tab and click on the LAN Settings button at the bottom. Make sure that the Proxy Server option is unchecked.
If you cannot browse to the Router, use the `winipcfg` utility in Windows 98/ME to verify that your computer has received the correct address information from the Router. From the Start menu, choose Run and then enter `winipcfg`. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Router is 192.168.1.1 (the address of the Router). If these are not correct, use the Release and Renew functions to obtain a new IP address from the Router. Under Windows 2000 and Windows XP, use the `ipconfig` command-line utility to perform the same functions.

Connecting to the Internet

If you can browse to the Router configuration screens but cannot access Web sites on the Internet, check the following:

- Confirm that the physical connection between the Router and the telephone line is OK, and that the DSL LED on the Router is illuminated.
- Ensure that you have entered the correct information into the Router configuration screens as required by your Internet Service Provider. Use the Internet Settings screen to verify this.
- Check that the PPPoE or PPPoA user name and password are correct.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under Control Panel > Internet Options > Connections.

Forgotten Password and Reset to Factory Defaults

If you can browse to the Router configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Router to its factory default configuration.

**CAUTION:** All your configuration changes will be lost, and you will need to run the configuration wizard again before you can re-establish your Router connection to the Internet. Also, other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.

1. Power off the Router.
2. Disconnect all your computers and the telephone line from the Router.
3. Re-apply power to the Router, and wait for it to finish booting up.
4 Press and hold the Reset button on the rear panel (see “The rear panel (Figure 4) of the Router contains four LAN ports, one ADSL port, a reset button, a power OK LED, and a power adapter socket.” on page 16) for 5 seconds.

5 The Router will restart, and when the start-up sequence has completed, browse to:

http://192.168.1.1

and run the configuration wizard. You may need to restart your computer before you attempt this.

6 When the configuration wizard has completed, you may reconnect your network as it was before.

Wireless Networking

- Ensure that you have an 802.11b or 802.11g wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each wireless computer has either Windows 98 or higher or MAC OS 8.5 or higher.
- Verify that your wireless computers are configured to work in Infrastructure mode and not Ad Hoc mode. The Router contains an Access Point that is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Router.
- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the WLAN LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to “Wireless Settings” on page 43 and enable wireless networking.
- Ensure that the TCP/IP settings for all devices are correct.
- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Router. The SSID is case-sensitive.
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Router. The Router cannot simultaneously support WPA and WEP encryption.
- Ensure that you have the wireless computer enabled in the list of allowed MAC addresses if you are using MAC Address Filtering on the Router.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Router.
For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage. Additionally consider moving the wireless computer closer to the Router to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the wireless computer or the Router, or trying a different channel on the Router.

- Sources of interference: The 2.4Ghz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices, like microwave ovens for example, close to the Router or wireless computers as this could affect receiver sensitivity and reduce the performance of your network. If you are unsure try relocating both the wireless computers and the Router to establish whether this problem exists.

- Most wireless computer adapters will scan the channels for the wireless Router. If a wireless computer has not located the Router then try initiating a search manually if the client software supports this feature or manually set the channel on your wireless computer to correspond to the Router channel number. Please refer to your wireless computer adapter documentation and vendor to do this.

- Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Router the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Router or moving the wireless computer closer to the Router. In an ideal network the Router should be located in the centre of the network with wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.
Recovering from Corrupted Software

If the system software has become corrupted, the Router will enter a “recovery” state; DHCP is enabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Router unit in this state.

Ensure that one of your computers has a copy of the new software image file stored on its hard disk or available on CD-ROM.

The latest software is available on 3Com’s Web site at:

www.3com.com

1 Remove power from the Router and disconnect the telephone line and all your computers, except for the one computer with the software image.

2 You will need to reconfigure this computer to obtain an IP address automatically (see “Obtaining an IP Address Automatically” on page 23).

3 Restart the computer, and re-apply power to the Router.

4 Using the Web browser on the computer, enter the following URL in the location bar:


This will connect you to the Recovery utility in the Router.

5 Follow the on-screen instructions. Enter the path and filename of the software image file.

6 When the upload has completed, the Router will restart, run the self-test and, if successful, resume normal operation.

7 Refer to the Installation Guide to reconnect your Router to the telephone line and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

If the Router does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.
### Frequently Asked Questions

<table>
<thead>
<tr>
<th><strong>How do I reset the Router to Factory Defaults?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>See “Forgotten Password and Reset to Factory Defaults” on page 104.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>How many computers on the LAN does the Router support?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A maximum of 253 computers on the LAN are supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>How many wireless clients does the Router support?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A maximum of 128 wireless clients are supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>There are only 4 LAN ports on the Router. How are additional computers connected?</strong></th>
</tr>
</thead>
</table>
| You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Router. 3Com wireless access points and hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:  
http://www.3com.com/ |

<table>
<thead>
<tr>
<th><strong>Does the Router support virtual private networks (VPNs)?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Router supports VPN passthrough, which allows VPN clients on the LAN to communicate with VPN hosts on the Internet. It is also possible to set up VPN hosts on your LAN that clients elsewhere on the Internet can connect to, but this is not a recommended configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Where can I download software updates for the Router?</strong></th>
</tr>
</thead>
</table>
| Updates to the Router software are posted on the 3Com support Web site, accessible by visiting:  
http://www.3com.com |
The Internet Protocol Suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

To manage a device over the network, the Router must be correctly configured with the following IP information:

- An IP address
- A Subnet Mask

Each device on your network must have a unique IP address to operate correctly. An IP address identifies the address of the device to which data is being sent and the address of the destination network. IP addresses have the format n.n.n.x where n is a decimal number between 0 and 255 and x is a number between 1 and 254 inclusive.

However, an IP address alone is not enough to make your device operate. In addition to the IP address, you need to set a subnet mask. All networks are divided into smaller sub-networks and a subnet mask is a number that enables a device to identify the sub-network to which it is connected.
For your network to work correctly, all devices on the network must have:

- The same sub-network address.
- The same subnet mask.

*The only value that will be different is the specific host device number. This value must always be unique.*

An example IP address is ‘192.168.100.8’. However, the size of the network determines the structure of this IP address. In using the Router, you will probably only encounter two types of IP address and subnet mask structures.

**Type One**

In a small network, the IP address of ‘192.168.100.8’ is split into two parts:

- Part one (‘192.168.100’) identifies the network on which the device resides.
- Part two (’.8’) identifies the device within the network.

This type of IP address operates on a subnet mask of ‘255.255.255.0’.

See **Table 3** for an example about how a network with three computers and a Router might be configured.

**Table 3** IP Addressing and Subnet Masking

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC 1</td>
<td>192.168.100.8</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC 2</td>
<td>192.168.100.33</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>PC 3</td>
<td>192.168.100.188</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Router</td>
<td>192.168.100.72</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**Type Two**

In larger networks, where there are more devices, the IP address of ‘192.168.100.8’ is, again, split into two parts but is structured differently:

- Part one (‘192.168’) identifies the network on which the device resides.
- Part two (’.100.8’) identifies the device within the network.
This type of IP Address operates on a subnet mask of ‘255.255.0.0’.

See Table 4 for an example about how a network (only four computers represented) and a Router might be configured.

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC 1</td>
<td>192.168.100.8</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>PC 2</td>
<td>192.168.201.30</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>PC 3</td>
<td>192.168.113.155</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>PC 4</td>
<td>192.168.002.230</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Router</td>
<td>192.168.002.72</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

How does a Device Obtain an IP Address and Subnet Mask?

There are three different ways to obtain an IP address and the subnet mask. These are:

- Dynamic Host Configuration Protocol (DHCP) Addressing
- Static Addressing
- Automatic Addressing (Auto-IP Addressing)

**DHCP Addressing**

The Router contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

DHCP will work on any client Operating System such as Windows 95, Windows 98, Windows NT 4.0, Windows 2000 and Windows XP. Also, using DHCP means that the same IP address and subnet mask will never be duplicated for devices on the network. DHCP is particularly useful for networks with large numbers of users on them.

**Static Addressing**

You must enter an IP Address and the subnet mask manually on every device. Using a static IP and subnet mask means the address is permanently fixed.

**Auto-IP Addressing**

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves
an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000 and Windows XP.
This section lists the technical specifications for the OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router.

### Interfaces
- **DSL connection**
- **LAN connection** — four 10 Mbps/100 Mbps dual speed Ethernet ports (10BASE-T/100BASE-TX)

### WLAN Interfaces

Standard IEEE 802.11g, Direct Sequence Spread Spectrum (DSSS)

- Transmission rate: 54 Mbps, automatic fallback to 48, 36, 24, 18, 12, or 6 Mbps
- Maximum channels: 13
- Range up to 304.8m (1000ft)
- Sensitivity: 6, 12, 18, 24, 36, 48 Mbps: -85 dBm; 54 Mbps -66 dBm typical
- Modulation: CCK, BPSK, QPSK, OFDM
- Encryption: 40/64 bit WEP, 128 bit WEP, WPA
- Maximum clients: 128
- O/P Power: 18dBm

Standard IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)

- Transmission rate: 11Mbps, automatic fallback to 5.5, 2, or 1 Mbps
- Maximum channels: 13
- Range up to 304.8m (1000ft)
- Sensitivity: 1, 2, 5.5 Mbps: -85 dBm; 11 Mbps -82 dBm typical
- Modulation: CCK, BPSK, QPSK
- Encryption: 40/64 bit WEP, 128 bit WEP, WPA
- Maximum clients: 128
- O/P Power 16dBm
Operating Temperature
0 °C to 40 °C (32 °F to 105 °F)

Power
8VA, 25 BThU/hr

Humidity
0% to 90% (non-condensing) humidity

Dimensions
- Width = 220 mm (8.7 in.)
- Depth = 133 mm (5.2 in.)
- Height = 38 mm (1.5 in.)

Weight
Approximately 550 g (1.1 lbs)

Standards
Functional:
ISO 8802/3
IEEE 802.3
IEEE 802.11b, 802.11g

Safety:
EN 60950-1: 2001
UL 60950-1
IEC 60950-1: 2001

EMC:
FCC Part 15 B
EN 55022
EN 55024
EN 61000
EN 301 489-1
ICES-003

Radio
FCC Part 15 C
RSS-210
EN 300 328

Environmental: EN 60068 (IEC 68)

*See “Regulatory Notices” for conditions of operation.
System Requirements  Operating Systems
The Router will support the following Operating Systems:
- Windows 98Se
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Mac OS 8.5 or higher
- Unix

Ethernet Performance
The Router complies to the IEEE 802.3i, u and x specifications.

Cable Specifications
The Router supports the following cable types and maximum lengths:
- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).
WARNING: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.
You must read the following safety information carefully before you install or remove the unit:

WARNING: The Router generates and uses radio frequency (rf) energy. In some environments, the use of rf energy is not permitted. The user should seek local advice on whether or not rf energy is permitted within the area of intended use.

WARNING: Exceptional care must be taken during installation and removal of the unit.

WARNING: To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.

WARNING: The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

WARNING: This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

WARNING: There are no user-replaceable fuses or user-serviceable parts inside the Router. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.

WARNING: Disconnect the power adapter before moving the unit.
**WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.

---

**Wichtige Sicherheitshinweise**

**VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.

Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Gerät installieren oder ausbauen:

**VORSICHT:** Der Router erzeugt und verwendet Funkfrequenz (RF). In manchen Umgebungen ist die Verwendung von Funkfrequenz nicht gestattet. Erkundigen Sie sich bei den zuständigen Stellen, ob die Verwendung von Funkfrequenz in dem Bereich, in dem der Bluetooth Access Point eingesetzt werden soll, erlaubt ist.

**VORSICHT:** Bei der Installation und beim Ausbau des Geräts ist mit höchster Vorsicht vorzugehen.

**VORSICHT:** Aufgrund von internationalen Sicherheitsnormen darf das Gerät nur mit dem mitgelieferten Netzadapter verwendet werden.

**VORSICHT:** Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden.

**VORSICHT:** Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.
**VORSICHT:** Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Router haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.

**VORSICHT:** Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.


---

**Consignes importantes de sécurité**

**AVERTISSEMENT:** Les avertissements présentent des consignes que vous devez respecter pour garantir votre sécurité personnelle. Vous devez respecter attentivement toutes les consignes. Nous vous demandons de lire attentivement les consignes suivantes de sécurité avant d’installer ou de retirer l’appareil:

**AVERTISSEMENT:** La Router fournit et utilise de l’énergie radioélectrique (radio fréquence -rf). L’utilisation de l’énergie radioélectrique est interdite dans certains environnements. L’utilisateur devra se renseigner sur l’autorisation de cette énergie dans la zone prévue.

**AVERTISSEMENT:** Faites très attention lors de l’installation et de la dépose du groupe.

**AVERTISSEMENT:** Pour garantir le respect des normes internationales de sécurité, utilisez uniquement l’adaptateur électrique remis avec cet appareil.

**AVERTISSEMENT:** La prise secteur doit se trouver à proximité de l’appareil et son accès doit être facile. Vous ne pouvez mettre l’appareil hors circuit qu’en débranchant son cordon électrique au niveau de cette prise.

**AVERTISSEMENT:** L’appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 60950. Ces
conditions ne sont maintenues que si l’équipement auquel il est raccordé fonctionne dans les mêmes conditions.

AVERTISSEMENT: Il n’y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l’intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.

AVERTISSEMENT: Débranchez l’adaptateur électrique avant de retirer cet appareil.

END USER SOFTWARE LICENSE AGREEMENT

3Com Corporation

END USER SOFTWARE LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND USING THIS PRODUCT, THE USE OF WHICH IS LICENSED BY 3Com CORPORATION (“3Com”) TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. DOWNLOADING, INSTALLING OR OTHERWISE USING ANY PART OF THE SOFTWARE OR DOCUMENTATION INDICATES THAT YOU ACCEPT THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR OTHERWISE USE THE SOFTWARE OR DOCUMENTATION, DO NOT CLICK ON THE “I AGREE” OR SIMILAR BUTTON. AND IF YOU HAVE RECEIVED THE SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, RETURN THE ENTIRE PRODUCT WITH THE SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.

LICENSE:
3Com grants you a nonexclusive, nontransferable (except as specified herein) license to use the accompanying software program(s) in executable form (the “Software”) and accompanying documentation (the “Documentation”), subject to the terms and restrictions set forth in this Agreement. You are not permitted to lease, rent, distribute or sublicense (except as specified herein) the Software or Documentation or to use the Software or Documentation in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights with respect to the Software or Documentation.

Subject to the restrictions set forth herein, the Software is licensed to be used on any workstation or any network server owned by or leased to you, for your internal use, provided that the Software is used only in connection with this 3Com product. You may reproduce and provide one (1) copy of the Software and Documentation for each such workstation or network server on which the Software is used as permitted hereunder. Otherwise, the Software and Documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. Each copy of the Software and Documentation must contain 3Com’s and its licensors’ proprietary rights and copyright notices in the same form as on the original. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation delivered to you under this Agreement.

ASSIGNMENT; NO REVERSE ENGINEERING:
You may transfer the Software, Documentation and the licenses granted herein to another party in the same country in which you obtained the Software and Documentation if the other party agrees in writing to accept and be bound by the terms and conditions of this Agreement. If you transfer the Software and Documentation, you must at the same time either transfer all copies of the Software and Documentation to the party or you must destroy any copies not transferred. Except as set forth above, you may not assign or transfer your rights under this Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Union (“EU”) resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EU Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

EXPORT RESTRICTIONS:
The Software, including the Documentation and any other technical data provided hereunder is commercial in nature subject to United States Export control laws and may be subject to export or import regulations in other countries. In addition, the Technical Data covered by this Agreement may contain data encryption code which is unlawful to export or transfer from the United States or country where you legally obtained it without an approved U.S. Department of Commerce export license and appropriate foreign export or import license, as required. You agree that you will not export or re-export the Technical Data (or any copies thereof) or any products utilizing the Technical Data in violation of any applicable laws or regulations of the United States or the country where you legally obtained it. You are responsible for obtaining any licenses to export, re-export or import the Technical Data.

In addition to the above, the Product may not be used, exported or re-exported (i) into or to a national or resident of any country to which the U.S. has embargoed; or (ii) to any one on the U.S. Commerce Department’s Table of Denial Orders or the U.S. Treasury Department’s list of Specially Designated Nationals.

TRADE SECRETS; TITLE: You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and Documentation and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature.
and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable.

TERM AND TERMINATION: The licenses granted hereunder are perpetual unless terminated earlier as specified below. You may terminate the licenses and this Agreement at any time by destroying the Software and Documentation together with all copies and merged portions in any form. The licenses and this Agreement will also terminate immediately if you fail to comply with any term or condition of this Agreement. Upon such termination you agree to destroy the Software and Documentation, together with all copies and merged portions in any form.

LIMITED WARRANTIES AND LIMITATION OF LIABILITY: All warranties and limitations of liability applicable to the Software are as stated on the Limited Warranty Card or in the product manual, whether in paper or electronic form, accompanying the Software. Such warranties and limitations of liability are incorporated herein in their entirety by this reference.


SEVERABILITY: In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties. Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation, 350 Campus Drive, Marlborough, MA. USA 01752-3064
# Obtaining Support for Your Product

## Register Your Product

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

Warranty and other service benefits are enabled through product registration. Register your product at [http://eSupport.3com.com/](http://eSupport.3com.com/).

3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request. If you have trouble registering your product, please contact 3Com Global Services for assistance.

## Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services like 3Com ExpressSM and GuardianSM can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com maintenance and Professional Services is available at [www.3com.com](http://www.3com.com).

Contact your authorized 3Com reseller or 3Com for a complete list of the value-added services available in your area.
APPENDIX E: OBTAINING SUPPORT FOR YOUR PRODUCT

Troubleshoot Online

You will find support tools posted on the 3Com Web site at www.3com.com.

3Com Knowledgebase helps you troubleshoot 3Com products. This query-based interactive tool is located at http://knowledgebase.3com.com and contains thousands of technical solutions written by 3Com support engineers.

Access Software Downloads

Software Updates are the bug fix/maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com Web site at http://eSupport.3com.com/

First time users will need to apply for a user name and password. A link to software downloads can be found at http://eSupport.3com.com/, or under the Product Support heading at www.3com.com.

Software Upgrades are the feature releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Telephone Technical Support and Repair

To enable telephone support and other service benefits, you must first register your product at http://eSupport.3com.com/

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- Proof of purchase, if you have not pre-registered your product
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable
To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at http://eSupport.3com.com/. First time users will need to apply for a user name and password.

### Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below.

Telephone numbers are correct at the time of publication. Find a current directory of contact information posted on the 3Com Web site at http://csoweb4.3com.com/contactus/

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia, Pacific Rim</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>1 800 678 515</td>
<td>Philippines</td>
<td>1235 61 266 2602 or 1800 61 266 2602</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>800 933 486</td>
<td></td>
<td>1800 1 888 9469</td>
</tr>
<tr>
<td>India</td>
<td>+61 2 9424 5179 or 00800 650 1111</td>
<td>P.R. of China</td>
<td>800 810 3033</td>
</tr>
<tr>
<td>Indonesia</td>
<td>001 803 61009</td>
<td>S. Korea</td>
<td>800 616 463</td>
</tr>
<tr>
<td>Japan</td>
<td>00531 616 439 or 03 3507 5984</td>
<td>Taiwan</td>
<td>00801 611 261</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1800 801 777</td>
<td>Thailand</td>
<td>001 800 611 2000</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800 446 398</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td>+61 2 9937 5083</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can also obtain support in this region using the following e-mail: apr_technical_support@3com.com

Or request a repair authorization number (RMA) by fax using this number: + 65 543 6348

### Europe, Middle East, and Africa

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>From anywhere in these</td>
<td>+44 (0)1442 435529</td>
</tr>
<tr>
<td>regions, call:</td>
<td></td>
</tr>
</tbody>
</table>

From the following countries, you may use the numbers shown:
## Appendix E: Obtaining Support for Your Product

### Europe

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>0800 297 468</td>
<td>Luxembourg</td>
<td>800 23625</td>
</tr>
<tr>
<td>Belgium</td>
<td>0800 71429</td>
<td>Netherlands</td>
<td>0800 0227788</td>
</tr>
<tr>
<td>Denmark</td>
<td>800 17309</td>
<td>Norway</td>
<td>800 11376</td>
</tr>
<tr>
<td>Finland</td>
<td>0800 113153</td>
<td>Poland</td>
<td>00800 4411 357</td>
</tr>
<tr>
<td>France</td>
<td>0800 917959</td>
<td>Portugal</td>
<td>800 831416</td>
</tr>
<tr>
<td>Germany</td>
<td>0800 182 1502</td>
<td>South Africa</td>
<td>0800 995 014</td>
</tr>
<tr>
<td>Hungary</td>
<td>06800 12813</td>
<td>Spain</td>
<td>900 938 919</td>
</tr>
<tr>
<td>Ireland</td>
<td>1 800 553 117</td>
<td>Sweden</td>
<td>020 795 482</td>
</tr>
<tr>
<td>Israel</td>
<td>1800 945 3794</td>
<td>Switzerland</td>
<td>0800 553 072</td>
</tr>
<tr>
<td>Italy</td>
<td>800 879489</td>
<td>U.K.</td>
<td>0800 096 3266</td>
</tr>
</tbody>
</table>

You can also obtain support in this region using the following URL:

http://emea.3com.com/support/email.html

### Latin America

#### Telephone Technical Support and Repair

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antigua Barbuda</td>
<td>AT&amp;T +800 988 2112</td>
<td>Guadalupe</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Argentina Local Number</td>
<td>54 11 5556 3200</td>
<td>Guatemala</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Argentina</td>
<td>0 810 444 3COM</td>
<td>Guyana</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Argentina</td>
<td>810 44 32 66</td>
<td>Haiti</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Aruba</td>
<td>AT&amp;T +800 988 2112</td>
<td>Honduras</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Bahamas</td>
<td>AT&amp;T +800 988 2112</td>
<td>Jamaica</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Barbados</td>
<td>AT&amp;T +800 988 2112</td>
<td>Mexico Local Number</td>
<td>52 55 52 01 00 04</td>
</tr>
<tr>
<td>Belize</td>
<td>AT&amp;T +800 988 2112</td>
<td>Mexico</td>
<td>01 800 849CARE</td>
</tr>
<tr>
<td>Bermuda</td>
<td>AT&amp;T +800 988 2112</td>
<td>Mexico</td>
<td>01 800 849 2273</td>
</tr>
<tr>
<td>Bolivia</td>
<td>AT&amp;T +800 988 2112</td>
<td>Monserrat</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Brazil Local Number</td>
<td>55 11 5643 2700</td>
<td>Nicaragua</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Brazil</td>
<td>800 133 286</td>
<td>Panama</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>British Virgin Islands</td>
<td>AT&amp;T +800 988 2112</td>
<td>Paraguay</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>AT&amp;T +800 988 2112</td>
<td>Paraguay</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Chile</td>
<td>AT&amp;T +800 988 2112</td>
<td>Puerto Rico</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Columbia Local Number</td>
<td>57 1 592 5000</td>
<td>Saba Anquila</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Colombia</td>
<td>800 011 3266</td>
<td>St. Kitts Neives</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>AT&amp;T +800 988 2112</td>
<td>St. Lucia</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Curacao</td>
<td>AT&amp;T +800 988 2112</td>
<td>St. Vincent</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Dominica</td>
<td>AT&amp;T +800 988 2112</td>
<td>Suriname</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Dominique</td>
<td>AT&amp;T +800 988 2112</td>
<td>Trinidad and Tobago</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Equador</td>
<td>AT&amp;T +800 988 2112</td>
<td>Turks and Caycos</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>El Salvador</td>
<td>AT&amp;T +800 988 2112</td>
<td>Uruguay - Montevideo</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>French Guiana</td>
<td>AT&amp;T +800 988 2112</td>
<td>Venezuela</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
<tr>
<td>Grenada</td>
<td>AT&amp;T +800 988 2112</td>
<td>Virgin Islands</td>
<td>AT&amp;T +800 988 2112</td>
</tr>
</tbody>
</table>

You can also obtain support in this region using the following:

Spanish speakers, enter the URL:

http://lat.3com.com/lat/support/form.html

Portuguese speakers, enter the URL:

http://lat.3com.com/br/support/form.html

English speakers in Latin America should send e-mail to:

lat_support_anc@3com.com
<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>US and Canada Telephone Technical Support and Repair</td>
<td>1 800 876 3266</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Glossary

802.11b  The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11g  The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.

10BASE-T  The IEEE specification for 10 Mbps Ethernet over Category 3, 4 or 5 twisted pair cable.

100BASE-TX  The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

Access Point  An access point is a device through which wireless clients connect to other wireless clients and which acts as a bridge between wireless clients and a wired network, such as Ethernet. Wireless clients can be moved anywhere within the coverage area of the access point and still connect with each other. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless client radio traffic and forwarding wireless client messages to the Ethernet LAN.

Ad Hoc mode  Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the router uses. (see also Infrastructure mode.)
**Auto-negotiation**  Some devices in the range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE 802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

**Bandwidth**  The information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. The bandwidth for 802.11b wireless is 11Mbps.

**Category 3 Cables**  One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 3 is voice grade cable and can only be used in Ethernet networks (10BASE-T) to transmit data at speeds of up to 10 Mbps.

**Category 5 Cables**  One of five grades of Twisted Pair (TP) cabling defined by the EIA/TIA-586 standard. Category 5 can be used in Ethernet (10BASE-T) and Fast Ethernet networks (100BASE-TX) and can transmit data up to speeds of 100 Mbps. Category 5 cabling is better to use for network cabling than Category 3, because it supports both Ethernet (10 Mbps) and Fast Ethernet (100 Mbps) speeds.

**Channel**  Similar to any radio device, the Wireless Cable/DSL router allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Router operates.

**Client**  The term used to describe the desktop PC that is connected to your network.

**DHCP**  Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.
**DNS Server Address**  
DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing “3com.com” into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

**DSL modem**  
DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

**Encryption**  
A method for providing a level of security to wireless data transmissions. The Router uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.

**ESSID**  
Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the Router and each of its wireless clients.

**Ethernet**  
A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks use CSMA/CD to transmit packets at a rate of 10 Mbps over a variety of cables.

**Ethernet Address**  
See MAC address.

**Fast Ethernet**  
An Ethernet system that is designed to operate at 100 Mbps.

**Firewall**  
Electronic protection that prevents anyone outside of your network from seeing your files or damaging your computers.

**Full Duplex**  
A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

**Half Duplex**  
A system that allows packets to transmitted and received, but not at the same time. Contrast with full duplex.
**Hub** A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

**IEEE** Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

**IETF** Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

**Infrastructure mode** Infrastructure mode is the wireless configuration supported by the Router. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Router. (see also Ad Hoc mode)

**IP** Internet Protocol. IP is a Layer 3 network protocol that is the standard for sending data through a network. IP is part of the TCP/IP set of protocols that describe the routing of packets to addressed devices. An IP address consists of 32 bits divided into two or three fields: a network number and a host number or a network number, a subnet number, and a host number.

**IP Address** Internet Protocol Address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with periods (full-stops), and is made up of a network section, an optional subnet section and a host section.

**IPsec** IP Security. Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication. When setting up an IPSec connection between two devices, make sure that they support the same encryption method.

**ISP** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.
LAN  Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

MAC  Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC Address  Media Access Control Address. Also called the hardware or physical address. A Layer 2 address associated with a particular network device. Most devices that connect to a LAN have a MAC address assigned to them as they are used to identify other devices in a network. MAC addresses are 6 bytes long.

NAT  Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Router allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Network  A network is a collection of computers and other computer equipment that is connected for the purpose of exchanging information or sharing resources. Networks vary in size, some are within a single room, others span continents.

Network Interface Card (NIC)  A circuit board installed into a piece of computing equipment, for example, a computer, that enables you to connect it to the network. A NIC is also known as an adapter or adapter card.

Protocol  A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

PPPoE  Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP  Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the Internet.
**RJ-45** A standard connector used to connect Ethernet networks. The “RJ” stands for “registered jack”.

**Router** A device that acts as a central hub by connecting to each computer’s network interface card and managing the data traffic between the local network and the Internet.

**Server** A computer in a network that is shared by multiple end stations. Servers provide end stations with access to shared network services such as computer files and printer queues.

**SSID** Service Set Identifier. Some vendors of wireless products use SSID interchangeably with ESSID.

**Subnet Address** An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.

**Subnet Mask** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must assigned by InterNIC).

**Subnets** A network that is a component of a larger network.

**Switch** A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

**TCP/IP** Transmission Control Protocol/Internet Protocol. This is the name for two of the most well-known protocols developed for the interconnection of networks. Originally a UNIX standard, TCP/IP is now supported on almost all platforms, and is the protocol of the Internet.

TCP relates to the content of the data travelling through a network — ensuring that the information sent arrives in one piece when it reaches its destination. IP relates to the address of the end station to which data is being sent, as well as the address of the destination network.
Traffic  The movement of data packets on a network.

Universal Plug and Play  Universal Plug and Play is a system which allows compatible applications to read some of their settings from the Router. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter  A URL Filter is a feature of a firewall that allows it to stop its clients from browsing inappropriate Web sites.

WAN  Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

WDS  Wireless Distribution System. WDS enables one or more access points to rebroadcast received signals to extend range and reach, though this can affect the overall throughput of data.

WECA  Wireless Ethernet Compatibility Alliance. An industry group formed to certify cross vendor interoperability and compatibility of 802.11b and 802.11g wireless networking products and to promote the standard for enterprise, small business and home environments. (see also 802.11b, 802.11g, Wi-Fi)

WEP  Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.

Wi-Fi  Wireless Fidelity. This is the certification granted by WECA to products that meet their interoperability criteria. (see also 802.11b, WECA)

Wireless Client  The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network.

Wireless LAN Service Area  Another term for ESSID (Extended Service Set Identifier).

Wizard  A Windows application that automates a procedure such as installation or configuration.
**WLAN**  Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

**WPA**  Wi-Fi Protected Access. A dynamically changing encryption mechanism for wireless networking. Encryption strength is 256 bit.
# REGULATORY NOTICES

For The OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router

## GENERAL STATEMENTS

The 3Com OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router (WL-552) must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

This product contains encryption. It is unlawful to export out of the U.S. without obtaining a U.S. Export License.

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate 3Com's warranty and all applicable regulatory certifications and approvals.

This product can only be used with the supplied antenna(s).

## EXPOSURE TO RADIO FREQUENCY RADIATION

This device generates and radiates radio-frequency energy. In order to comply with FCC radio-frequency exposure guidelines for an uncontrolled environment, this equipment must be installed and operated while maintaining a minimum body to antenna distance of 20 cm (approximately 8 in.).

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's website www.hc-sc.gc.ca/rpb.

This product must maintain a minimum body to antenna distance of 20 cm. Under these conditions this product will meet the Basic Restriction limits of 1999/519/EC [Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)].

## US - RADIO FREQUENCY REQUIREMENTS

This device must not be co-located or operated in conjunction with any other antenna or transmitter.

## US FEDERAL COMMUNICATIONS COMMISSION (FCC) EMC COMPLIANCE

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 communications. 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.

The user may find the following booklet prepared by the Federal Communications Commission helpful: The Interference Handbook


3Com is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this 3Com OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router (WL-552), or the substitution or attachment of connecting cables and equipment other than specified by 3Com.

The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

Changes or modifications not expressly approved by 3Com could void the user's authority to operate this equipment.

## US MANUFACTURER'S FCC DECLARATION OF CONFORMITY

3Com Corporation  
350 Campus Drive  
Marlborough, MA 01752-3064, USA  
(508) 323-5000  
Date: March 8, 2006  
Declares that the Product:  
Brand Name: 3Com Corporation  
Model Number: WL-552  
Equipment Type: 3Com OfficeConnect ADSL Wireless 54Mbps 11g Firewall Router
Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

3Com OfficeConnect ADSL Wireless
54Mbps 11g Firewall Router
Model WL-552

INDUSTRY CANADA - RF COMPLIANCE
This device complies with RSS 210 of Industry Canada.
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.

L’ utilisation de ce dispositif est autorisée seulement aux conditions suivantes: (1) il ne doit pas produire de brouillage et (2) l’utilisateur du dispositif doit être prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term “IC” before the equipment certification number only signifies that the Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication. To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Pour empêcher que cet appareil cause du brouillage au service faisant l’objet d’une licence, il doit être utilisé à l’intérieur et devrait être place loin des fenêtres afin de Fournir un écran de blindage maximal. Si le matériau (ou son antenne d’émission) est installé à l’extérieur, il doit faire l’objet d’une licence.

INDUSTRY CANADA - EMISSIONS COMPLIANCE STATEMENT
This Class B digital apparatus complies with Canadian ICES-003.

AVIS DE CONFORMITÉ À LA RÉGLEMENTATION D’INDUSTRIE CANADA
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

SAFETY COMPLIANCE NOTICE
This device has been tested and certified according to the following safety standards and is intended for use only in Information Technology Equipment which has been tested to these or other equivalent standards:

- UL Standard 60950-1
- CAN/CSA C22.2 No. 60950-1
- IEC 60950-1
- EN 60950-1

EU COMPLIANCE

Usage restrictions apply. See documentation
For connection to ADSL networks
This equipment may be operated in:
Intended use: ADSL 802.11g/b Firewall Router

For connection to ADSL networks

NOTE: To ensure product operation is in compliance with local regulations, select the country in which the product is installed. Refer to 3CRWDR101A-75 User Guide.
A copy of the signed Declaration of Conformity can be downloaded from the Product Support web page for the 3Com OfficeConnect ADSL Wireless 54 Mbps 11g Firewall Router at http://www.3Com.com. Also available at http://support.3com.com/doc/WL-552_EU_DOC.pdf.

### EU - Restrictions for Use in the 2.4GHz Band

This device may be operated indoors in all countries of the European Community using the 2.4GHz band: Channels 1 - 13, except where noted below.

- In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors.
- In Belgium outdoor operation is only permitted using the 2.46 - 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.4835 GHz band: Channel 13.

### Brazil RF Compliance

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não causar interferência a sistema operando em caráter primário.

### DGT Statement

注意！

本设备未涉及射頻頻譜管理法

第十一條 本設備其對無線電波頻譜之使用不影響飛航安全及干擾合法使用；並符合電波法例及 功能。

第十二條 在臺灣地區，低功率射頻電機之使用應經申請及核發許可證後方得使用。
前項合法通信，指合法通信所作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

RTTE01:

1. 本機限在不干擾合法電台與不受被干擾保障條件下於室內使用
2. 為減少電波干擾，請妥適使用
INDEX

Numbers
128-bit WEP  46
128-bit WEP Screen  46
1483 Bridge Mode  55
64-bit WEP Screen  47

A
Access Control Screen  62
Add PC Screen  63
Add Schedule Rule Screen  65
Addresses
IP  85
Admin Password Screen  75
ADSL Status Screen  77
Advanced Screen  68
Automatic Addressing  87

B
Backup/Restore Settings Screen  74
Bridge Mode for Single PC Screen  53
Bridged Mode Configuration Screen  33

C
Cable Specifications  91
Channels  111
Configuration Summary Screen  37
Connection Type Screen  29, 50
Conventions
notice icons, About This Guide  8
text, About This Guide  8

D
DDNS  70
DHCP  87
DHCP Clients List  42
DHCP server  25, 42
disabling  26
DMZ Screen  67
DNS  24

DNS Screen  55
DSL mode  29
Dynamic Domain Server (DDNS) Screen  70
Dynamic IP Address  34
Dynamic/Fixed IP for Bridge Mode Screen  35, 55
DYNDNS  70

E
Editing DHCP Clients List Screen  42
Encryption Screen  44
Encryption, disabling  45

F
Firewall Screen  59
Forgotten Password  80

H
Hostname
configuring  56
Hostname and MAC Address Screen  56

I
Internet
addresses  85
Internet Properties Screen  26
Internet Protocol (TCP/IP) Properties Screen  24
IP Address  41, 85
IPSEC  68

L
LAN Settings Screen  41
LED  14
LEDs  14
Local Area Properties Screen  24
Logs Screen  77

M
MAC Address  56
configuring 56
MAC Address Filtering Screen 66
mode 30

N
NAT (Network Address Translation) 68
NAT-T (NAT Traversal) 68
Network addresses 85
Networking wireless 81
NIC wireless 14

P
Password 27, 75
Poison Reverse 58
PPPoA 31
PPPoA Screen 31
PPPoA Settings Screen 52
PPPoE 26, 30, 31
PPPoE Screen 30
PPPoE Settings Screen 51

R
Remote Admin 68
Reset to Factory Default Screen 73
Reset to Factory Defaults 80
Restart Router Screen 73
RFC 1483 Bridged Mode 32, 53
RFC 1483 Routed Mode 34
RIP (Routing Information Protocol) 57
RIP Parameter Screen 58
Router Login Screen 28
Routing Mode Screen 34
Routing Table Screen 59

S
Schedule Rule Screen 65
Setup Wizard 27
SNMP Community Screen 71
SNMP Trap Screen 72
Special Applications Screen 60
Specifications technical 89
SSID 31, 32, 33, 35, 36, 43
Static Addressing 87
Static Route Parameters Screen 57
Status Screen 28, 40

Subnet Mask 85

T
TCP/IP 23, 25, 85
Technical
   specifications 89
   standards 89
Time and Time Zone screen 76
TZO.com 70

U
Universal Plug and Play 68
Upgrade Screen 74
URL Blocking Screen 64

V
Virtual Servers Screen 61
VPI/VCI 30, 32, 33, 34, 36

W
WAN Ping Blocking 68
WDS 49
Web Browser Location Field 27
Web Proxy 26
WiFi Protected Access 45, 48
Wireless
   networking 81
   NIC 14
Wireless Configuration Screen 43
Wireless Settings Screen 31, 32, 33, 35, 36, 43
Wireless WDS Settings Screen 49
WPA (with RADIUS Server) Screen 48
WPA-PSK (no server) Screen 45