



# **Wireless 11g Cable/DSL Router**

## User Guide

WL-550

3CRWER101U-75  
3CRWER101E-75  
3CRWER101A-75

<http://www.3Com.com/>

Part No. 10016641 Rev. AA

Published March 2008

**3Com Corporation**  
**350 Campus Drive,**  
**Marlborough, MA**  
**USA 01752-3064**

Copyright © 2008, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

#### **UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. 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 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. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, and the 3Com logo are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

JavaScript is a trademark of Sun Microsystems

Wi-Fi and the Wi-Fi logo are registered trademarks of the Wi-Fi Alliance.

IEEE and 802 are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

#### **ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

#### **End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

#### **Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

#### **Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

---

## **ABOUT THIS GUIDE**

- Naming Convention 5
- Conventions 6
- Feedback About This User Guide 7
- Related Documentation 7

**1**

---

## **INTRODUCING THE ROUTER**

- Wireless 11g Cable/DSL Router 9
- Router Advantages 11
- Package Contents 11
- Minimum System and Component Requirements 12
- Physical Features 12

**2**

---

## **INSTALLING THE ROUTER**

- Introduction 17
- Positioning the Router 17
- Powering Up the Router 18
- Connecting the Router to the Internet 18
- Connecting the Router to LAN 18
- Setting up your computers for networking with the Router 20

**3**

---

## **SETTING UP YOUR COMPUTERS**

- Obtaining an IP Address Automatically 23
  - Windows 2000 23
  - Windows XP 23
  - Windows Vista 25

Macintosh	27
Disabling PPPoE and PPTP Client Software	28
Disabling Web Proxy	28

**4**

---

## **RUNNING THE SETUP WIZARD**

Accessing the Setup Wizard	29
Setup Wizard - Wireless Settings	31
Setup Wizard - Connection Settings	32

**5**

---

## **CONFIGURING THE ROUTER**

Navigating Through the Router Configuration screens	39
Main Menu	39
Network Settings	39
Status	39
LAN Settings	41
WAN Settings	43
Wireless	48
Firewall	57
Schedule Rule	58
Access Control	60
MAC Filter	62
URL Filtering	63
Intrusion Detection	64
DMZ	69
Maintenance	70
Configuration Tools	70
Firmware Upgrade	71
Restart Router	72
Advanced Settings	72
NAT	73



System	78
UPNP	82
DNS	83
DDNS	84
Routing	85
Static Routes	85
RIP	86
Routing Table	87

---

## **TROUBLESHOOTING**

Basic Connection Checks	89
Browsing to the Router Configuration Screens	89
Connecting to the Internet	90
Forgotten Password and Reset to Factory Defaults	90
Wireless Networking	91
Recovering from Corrupted Software	93
Frequently Asked Questions	94

---

## **IP ADDRESSING**

The Internet Protocol Suite	95
Managing the Router over the Network	95
IP Addresses and Subnet Masks	95
How does a Device Obtain an IP Address and Subnet Mask?	97
DHCP Addressing	97
Static Addressing	97
Auto-IP Addressing	97

**B**

---

**TECHNICAL SPECIFICATIONS**

Wireless 11g Cable/DSL Router 99  
    Standards 100  
    System Requirements 100

**C**

---

**END USER SOFTWARE LICENSE AGREEMENT**

**D**

---

**OBTAINING SUPPORT FOR YOUR PRODUCT**

---

**GLOSSARY**

---

**REGULATORY NOTICES**

---

**INDEX**

# ABOUT THIS GUIDE

This guide describes how to install and configure the 3Com Wireless 11g Cable/DSL Router (3CRWER101x-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 Wireless 11g Cable/DSL 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 Wireless 11g Cable/DSL 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

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

**Table 2** Text Conventions

Convention	Description
The words "enter" and "type"	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."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"> <li>■ Emphasize a point.</li> <li>■ Denote a new term at the place where it is defined in the text.</li> <li>■ Identify menu names, menu commands, and software button names. Examples: From the <i>Help</i> menu, select <i>Contents</i>. Click <i>OK</i>.</li> </ul>

---

## Feedback About This User Guide

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:

**pddtechpubs\_comments@3com.com**

Please include the following information when commenting:

- Document title
- Document part number (on the title page)
- Page number (if appropriate)

Example:

- 3Com Wireless 11g Cable/DSL Router User Guide
- Part Number 149100059700J Rev. AA
- Page 24



*Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to [Appendix C](#).*

---

## 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.



# 1

## 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.

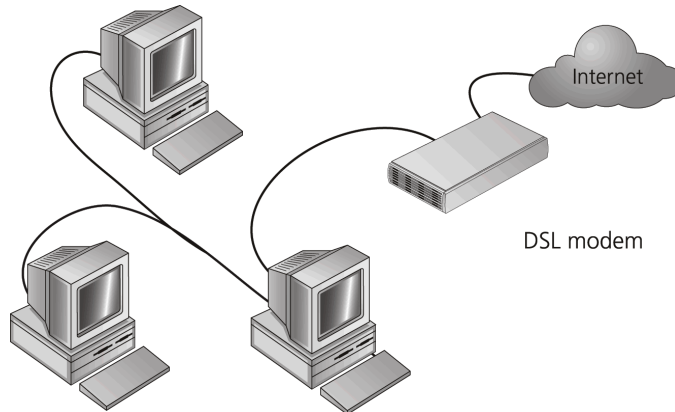
---

### **Wireless 11g Cable/DSL Router**

The Wireless 11g Cable/DSL 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.

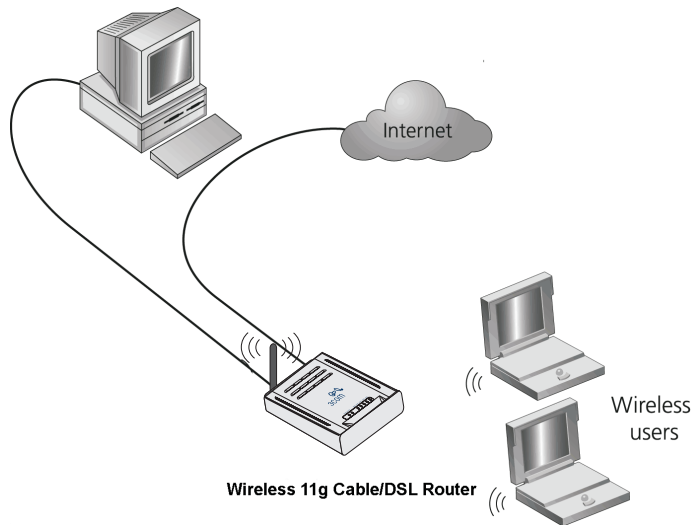
[Figure 1](#) shows an example network without a Router. In this network, only one computer is connected to the Internet. This computer must always be powered on for the other computers on the network to access the Internet.

**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, 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 Wireless 11g Cable/DSL Router
- One power adapter for use with the Router
- One Ethernet cable
- One Detachable antenna
- One CD-ROM containing this User Guide
- Installation Guide
- Support and Safety Information Sheet
- Warranty Flyer

If any of these items are missing or damaged, please contact your retailer.

---

## 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/Vista, 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.

OR

An 802.11b or 802.11g wireless NIC.

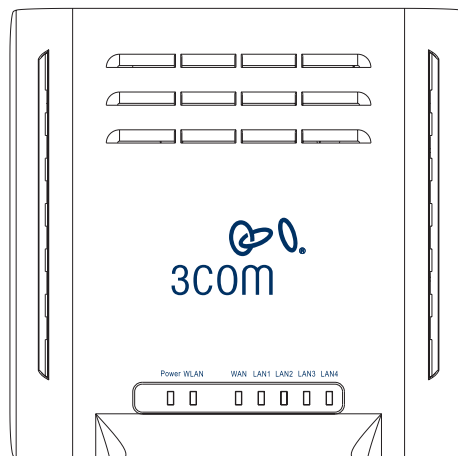
- Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem or cable modem.
- A Web browser that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

---

## Physical Features

The top 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 - Top View



### 1 Power LED

*Green*

Indicates that the Router is powered on, and the boot up is successful.

### 2 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"](#).

### 3 WAN Status LED

*Green*

If the LED is on it indicates that the WAN port has established a valid Ethernet network connection. If the LED is flashing, the link is OK and data is being transmitted or received. If the LED is off, the WAN has been disabled in the Router, or there is a problem. Refer to [Chapter 6 "Troubleshooting"](#).

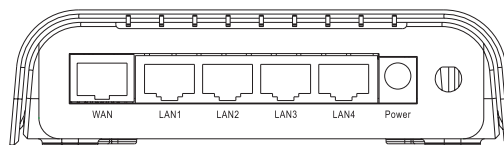
### 4 LAN Status LEDs

*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 one WAN port, four LAN ports, and a power adapter socket.

**Figure 4** Router - Rear Panel



### 5 WAN Port

Using the RJ-45 cable provided, you should connect your cable modem, DSL modem, or an Ethernet router to this port.

### 6 LAN 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.

### 7 Power Adapter Socket

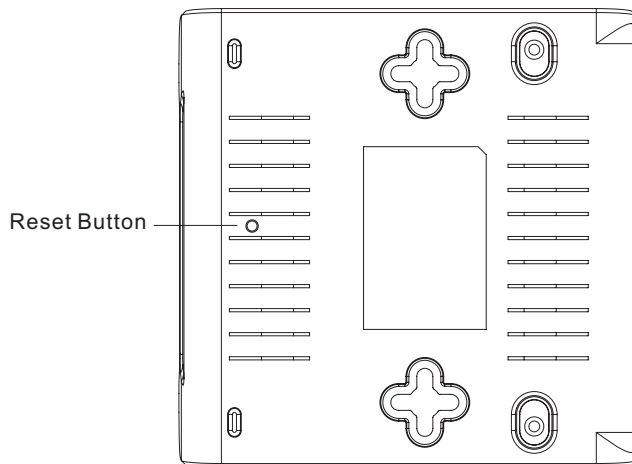
Only use the power adapter that is supplied with this Router. Do not use any other adapter.

### 8 Wireless Antenna

Be sure the detachable external antenna is connected to the Router before setting up your wireless LAN. Try to place the Wireless 11g Router in a position that is located in the center of your wireless network. The higher you place the antenna, the better the performance.

A reset bottom is located on the bottom of the Router ([Figure 5](#)).

**Figure 5** Router - Bottom Panel



## 9 Reset Button

The reset button allows you to reboot the Router, or to restore the default factory settings. Push for one second to perform a system reboot. All of your settings will remain upon restarting. Push for 8 seconds to reset the Router to the factory default settings.



*To perform a system reset without losing configuration settings, click the Restart Router button on the web management screen. The configurations that you have set previously will not be changed back to the factory default settings. Refer to ["Restart Router"](#).*



# 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.



**CAUTION:** *Be sure to attach the removable antenna to the Router before connecting to your wireless network.*

---

### Positioning the Router

You should place the Router in a location that:

- is conveniently located for connection to the cable or ADSL modem.
- 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 top 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.

---

## Powering Up the Router

To power up the Router:

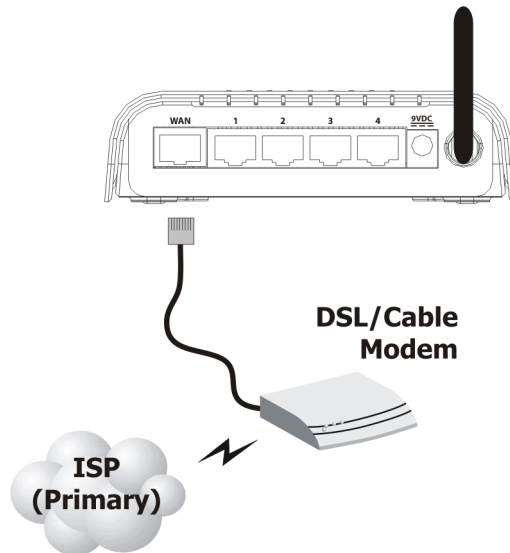
- 1 Plug the power adapter into the power adapter socket located on the back panel of the Router.
- 2 Plug the power adapter into a standard electrical wall socket.

---

## Connecting the Router to the Internet

Prepare an Ethernet cable for connecting the WAN port of the Wireless 11g Router to the RJ-45 port of the broadband xDSL or cable modem. See [Figure 6](#):

**Figure 6** Connecting the Router to the Internet




---

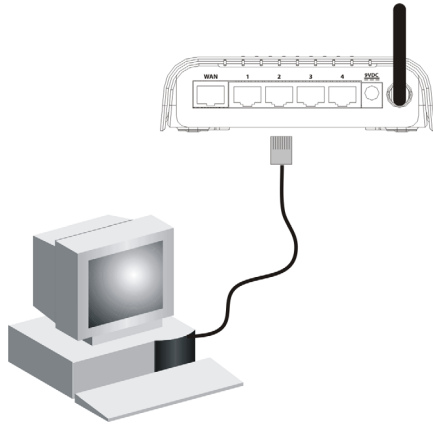
## Connecting the Router to LAN

The four LAN ports on the Router auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.



Use RJ-45 cables to connect any of the four LAN ports on the Router to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Router to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated. See [Figure 7](#):

**Figure 7** Connecting the LAN



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 — 6

---

**Setting up your computers for networking with the Router**

You may also connect the Router to your PC (using a wireless client adapter) via radio signals. Install a wireless network adapter in each computer that will be connected to the Internet or your local network via radio signals.

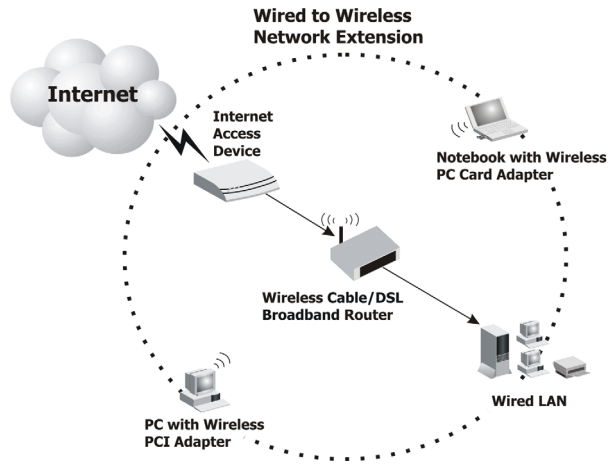
Place the Router in a position that gives it maximum coverage. Try to place the Router in a position that is located in the center of your wireless network. Normally, the higher you place the antenna, the better the performance. Ensure that the Router's location provides optimal reception throughout your home or office.

Computers equipped with a wireless adapter can communicate with each other as an independent wireless LAN by configuring each computer to the same radio channel. However, the Router can provide access to your wired/wireless LAN or to the Internet for all wireless workstations. Each wireless PC in this network infrastructure can talk to any computer in the wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure or over the Internet via the Router.

The wireless infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by retransmitting incoming radio signals through the Router.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, See [Figure 8](#):

Figure 8 WLAN Connections





# 3

## SETTING UP YOUR COMPUTERS

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:

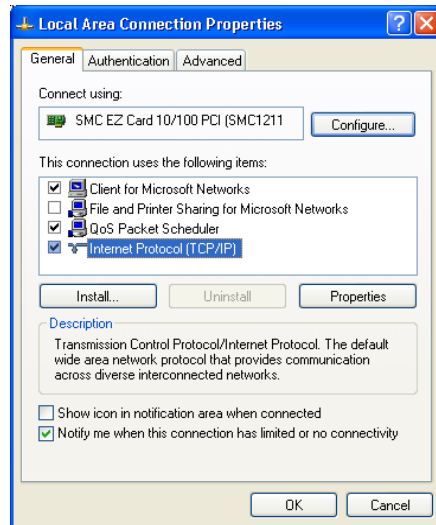
- 1 From the Windows *Start* Menu, select *Settings > Control Panel*.
- 2 Double click on *Network and Dial-Up Connections*.
- 3 Double click on *Local Area Connection*.
- 4 Click on *Properties*.
- 5 Select *Internet Protocol TCP/IP* and click on *Properties*.
- 6 Ensure that the options *Obtain an IP address automatically*, and *Obtain DNS server address automatically* are both selected. Click *OK*.
- 7 Restart your computer.

### Windows XP

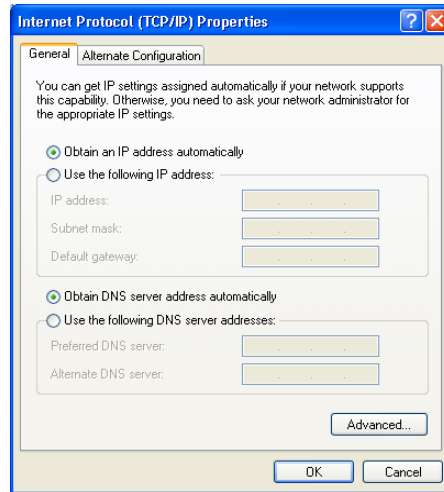
- 1 From the Windows *Start* Menu, select *Control Panel*.
- 2 Click on *Network and Internet Connections*.
- 3 Click on the *Network Connections* icon.

- 4 Double click on *LAN* or *High Speed Connection* icon. A screen titled *Local Area Connection Status* will appear.
- 5 A screen similar to [Figure 9](#) should be displayed. Select *Internet Protocol TCP/IP* and click on *Properties*.

**Figure 9** Local Area Connection Properties Screen



- 6 Ensure that the options *Obtain an IP address automatically*, and *Obtain DNS servers automatically* are both selected as shown in [Figure 10](#). Click *OK*.

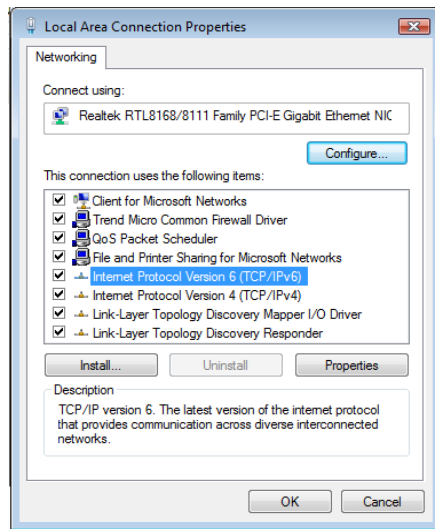
**Figure 10** Internet Protocol (TCP/IP) Properties Screen

7 Restart your computer.

## Windows Vista

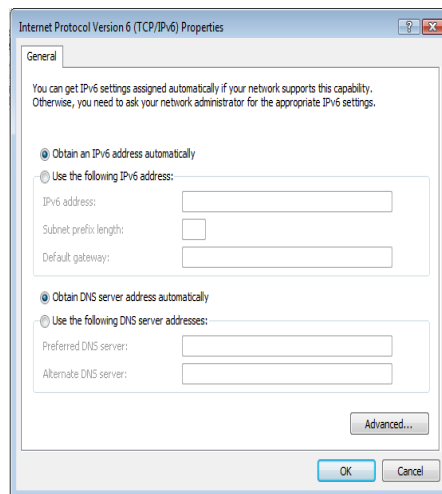
- 1 From the Windows *Start* Menu, select *Settings > Network*.
- 2 Click on *Organize*. Select *Properties*.
- 3 Click on *Manage network > Connections*.
- 4 Double click *Local Area Connection*. Select *Properties* and click *continue*.
- 5 A screen similar to [Figure 11](#) should be displayed. Select *Internet Protocol Version 6, Version 4 (TCP/IPv6, v4)* and click on *Properties*.

**Figure 11** Local Area Connection Properties Screen



- 6 Ensure that the options *Obtain an IPv6, v4 address automatically*, and *Obtain DNS servers address automatically* are both selected as shown in [Figure 12](#). Click **OK**.

**Figure 12** Internet Protocol Version 6 (TCP/IPv6) Properties Screen





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

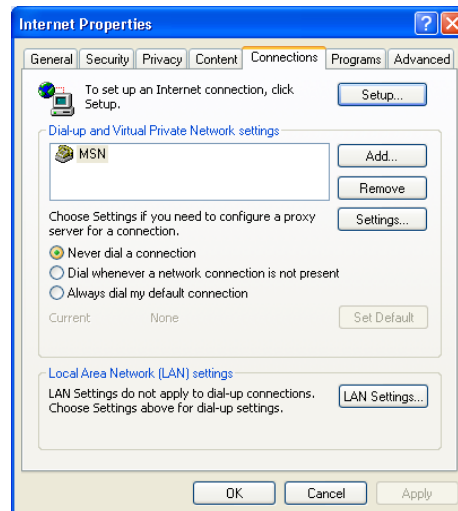
- 1 From the desktop, select *Apple Menu*, *Control Panels*, and *TCP/IP*.
- 2 In the *TCP/IP* control panel, set *Connect Via:* to *Ethernet*.
- 3 In the *TCP/IP* control panel, set *Configure:* to *Using DHCP Server*.
- 4 Close the *TCP/IP* dialog box, and save your changes.
- 5 Restart your computer.

## 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 *Control Panel > Network and Internet Connections*.
- 2 Double click on *Internet Options*.
- 3 Select the *Connections* Tab. A screen similar to [Figure 13](#) should be displayed.
- 4 Select the *Never dial a connection* option.

**Figure 13** 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.

# 4

## RUNNING THE SETUP WIZARD

---

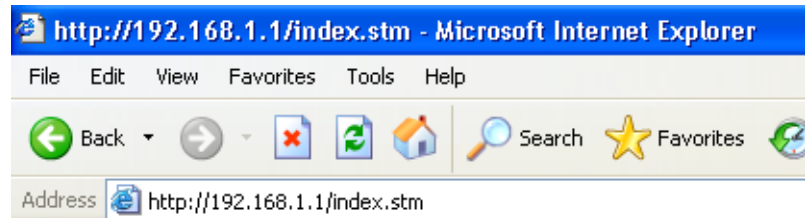
### Accessing the Setup Wizard

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 5.5 or higher, or Mozilla 1.2.1 or higher).

To use the Setup Wizard:

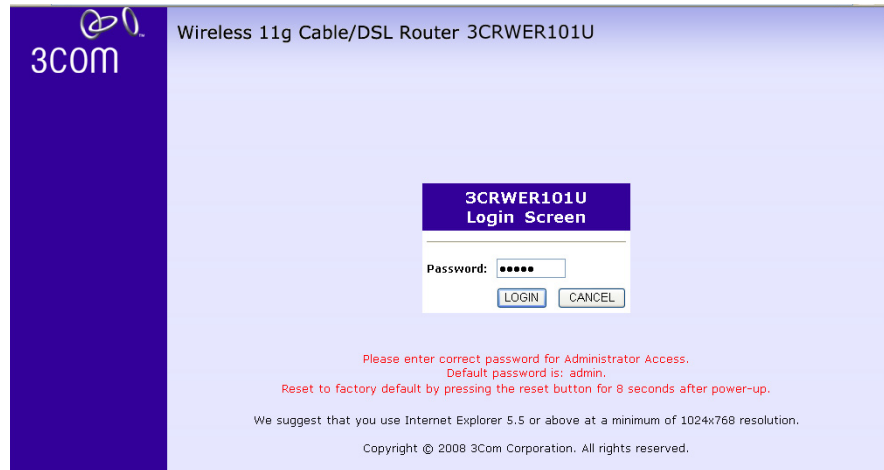
- 1 Ensure that you have at least one computer connected to the Router. Refer to [Chapter 2](#) for details on how to do this.
- 2 Launch your Web browser on the computer.
- 3 Enter the following URL in the location or address field of your browser: **http://192.168.1.1** ([Figure 14](#)). The Login screen displays.

**Figure 14** Web Browser Location Field (Factory Default)



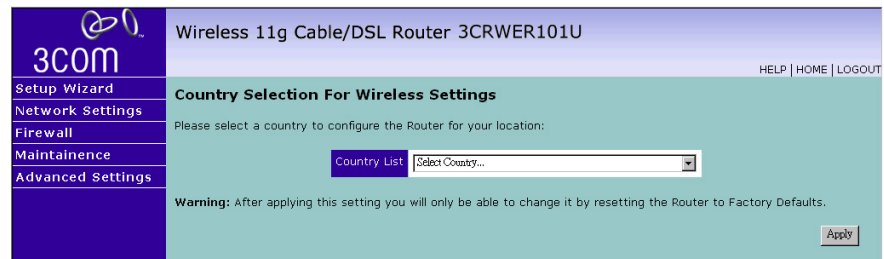
- 4 To log in as an administrator, enter the password (the default password is *admin*) in the *System Password* field and click *Log in* ([Figure 15](#)).

**Figure 15** 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 16](#)). Please select the country from the drop-down menu, and click *Apply*.

**Figure 16** Country Selection Screen



The Status page will then launch automatically (refer to [Figure 17](#)).

**Figure 17** Status Screen



Then click on *Setup Wizard* and you will be guided step by step through a basic setup procedure.

The first item in the Setup Wizard is *Getting Started*. Click *NEXT* to proceed to the following screen and configure your *Wireless Settings*.

**Setup Wizard - Wireless Settings**

The *Wireless Settings* screen allows you to set up your wireless network settings. You must specify a common radio channel and SSID (Service Set ID) to be used by the Router and all of its wireless clients. Be sure you configure all of its clients to the same value. For security purposes, you should change the default SSID immediately.

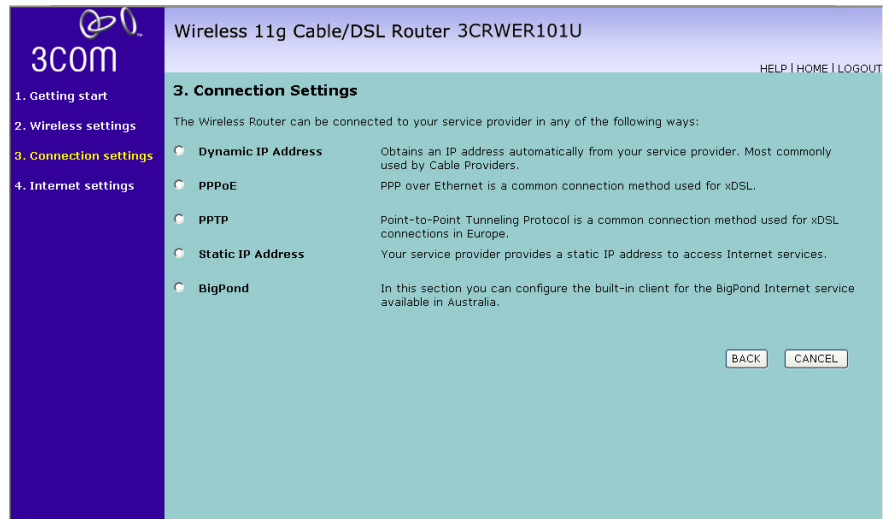
**Figure 18** Wireless Settings Screen

- **Wireless Network Name (SSID):** The Service Set ID (SSID) is the name of your wireless network. The SSID must be the same on the Router and all of its wireless clients. (Default: 3Com)
- **Broadcast Wireless Network Name:** Enable or disable the broadcasting of the SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. (Default: Enable)
- **Wireless Mode:** This device supports the following modes - 11g only, 11b only, and 11b/g mixed mode. (Default: 11b/g mixed mode)
- **Wi-Fi Channel Number:** The radio channel used by the Router and its clients to communicate with each other. This channel must be the same on the Router and all of its wireless clients. The Router will automatically assign itself a radio channel, or you may select one manually. (Default: 6)
- **Extend Range:** Increases the range of the Router. (Default: Disable)

### Setup Wizard - Connection Settings

The *Connection Settings* 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.

Select your connection type to proceed.

**Figure 19** Connection Settings Screen

Select a DSL mode from the following:

- *Dynamic IP Address*, automatically allocating IP addresses for all connected clients, see [page 33](#)
- *PPPoE* — PPP over Ethernet, providing routing for multiple PCs, see [page 34](#)
- *PPTP* — Point-to-Point Tunneling Protocol , providing virtual private networks, see [page 36](#)
- *Static IP Address*, manually assigning IP addresses for clients, see [page 37](#)
- *BigPond*, Australia's largest ISP, providing Internet access via ADSL/2+, Cable, Next G, and Dial-up. [page 37](#)

and click *Next*.



For further information on selecting a mode see [“WAN Settings”](#) on [page 43](#).

### **Dynamic IP Address Mode (For Multiple PCs)**

You can configure the Router to obtain an IP address automatically from a DHCP server.

**Figure 20** Dynamic IP Address Screen

The screenshot shows the 'Dynamic IP' configuration screen for a 3COM Wireless 11g Cable/DSL Router 3CRWER101U. The interface has a purple sidebar on the left with a navigation menu: 1. Getting start, 2. Wireless settings, 3. Connection settings, and 4. Internet settings (highlighted in yellow). The main content area has a light blue background and contains the following text:

**4. Internet settings**  
**Dynamic IP**  
 The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Wireless Router.  
 If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.  
 If necessary, you can use the "Renew" button on the Status page to renew the WAN IP address.

Below the text is a form with two fields:

- Host Name:** A text input field.
- MAC Address:** A field with six input boxes containing the values 00, 04, E2, 0D, 02, and FD.

At the bottom right of the form are three buttons: BACK, CANCEL, and NEXT.

If the ISP requires you to input a Host Name, type it in the Host Name field. The MAC Address field will be filled automatically.

Check all of your settings.

Click *NEXT* to proceed or *BACK* to change your settings.

### PPPoE Mode

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



Figure 21 PPPoE Mode Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

3COM

1. Getting start  
2. Wireless settings  
3. Connection settings  
4. Internet settings

#### 4. Internet settings

##### PPPoE

The WAN port is connected to an xDSL modem. Many service providers provide PPP over Ethernet (PPPoE) service. The Barricade supports Keep session, Auto connect and Manual connect features for PPPoE service.

To setup this connection type, enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped.

Keep session: If you enable this, the idle time setting is ignored. The connection will always be alive.

Auto Connect: When the connection is broken by the idle time, any Internet/WAN trigger will cause the router to re-establish the connection.

Manual Connect: Dial on demand is disabled in this mode. When the connection is broken by the idle time, you must press the Connect button to reconnect.

Do not change the MTU settings unless advised to by your Service Provider.

NOTE: If you are on a leased line or pay-per min. connection - please set your max idle time to 3 minutes. This will cause your internet connection to drop after 3 minutes of idle time so you won't be charged for extra online time from your ISP.

Use PPPoE Authentication

User Name :

---

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

3COM

1. Getting start  
2. Wireless settings  
3. Connection settings  
4. Internet settings

Manual Connect: Dial on demand is disabled in this mode. When the connection is broken by the idle time, you must press the Connect button to reconnect.

Do not change the MTU settings unless advised to by your Service Provider.

NOTE: If you are on a leased line or pay-per min. connection - please set your max idle time to 3 minutes. This will cause your internet connection to drop after 3 minutes of idle time so you won't be charged for extra online time from your ISP.

Use PPPoE Authentication

User Name :

Password :

Please retype your password :

Service Name :

MTU :  (576<=MTU Value<=1492)

Maximum Idle Time :  (min)

Keep session  
 Auto-connect  
 Manual-connect

BACK CANCEL NEXT

- 1 Enter your user name in the *User name* field.
- 2 Enter your password in the *Password* field.
- 3 Re-type your password in the *Please retype your password* field.
- 4 If your ISP has provided you with a Service Name enter it in the *Service Name* field, otherwise, leave it blank.
- 5 Leave the Maximum Transmission Unit (MTU) at the default value (1492) unless you have a particular reason to change it.

- 6 Enter the *Maximum Idle Time* for the Internet connection. After this time has been exceeded the connection will be terminated. Check *Keep session* to keep the session alive. Check the *Auto-connect* check box to automatically re-establish the connection as soon as you attempt to access the Internet again. Check the *Manual-connect* check box to manually re-establish the connection.
- 7 Check all of your settings.
- 8 Click *NEXT* to proceed or *BACK* to change your settings.

### PPTP Mode

To set up the Router for use with a PPTP connection, use the following procedure:

**Figure 22** PPTP Mode Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

1. Getting start

2. Wireless settings

3. Connection settings

4. Internet settings

#### 4. Internet settings

##### PPTP

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.

IP Address : 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

Default Gateway : 0 . 0 . 0 . 0

User ID: \_\_\_\_\_

Password: \_\_\_\_\_

PPTP Gateway: 0 . 0 . 0 . 0

Idle Time Out: 10 (min)

Manual-connect

Auto-connect

Keep session

\* If you have an ISP that charges by the time, change your idle time out value to 1 minute.

BACK CANCEL NEXT

- 1 Enter the IP Address information required by your ISP in the appropriate fields.
- 2 Enter the User ID and Password required by your ISP.
- 3 Enter the IP Address of the PPTP gateway as provided by your ISP
- 4 Enter the *Idle Time Out* for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. The default setting is 10 minutes. If your ISP charges you by the minute, you should change the Idle Time Out to one minute. After the

Idle Time Out has expired, set the action you wish the Router to take. You can tell the device to connect manually or automatically as soon as you try to access the Internet again, or to keep the session alive.

- 5 Check all of your settings.
- 6 Click *NEXT* to proceed or *BACK* to change your settings.

### Static IP Address Mode (For Multiple PCs)

If your Service Provider has assigned a fixed IP address, enter the assigned IP address information on the screen.

**Figure 23** Static IP Address Screen

To assign a fixed IP address:

- 1 Enter your Internet IP address in the *IP address* field.
- 2 Enter the subnet mask in the *Subnet Mask* field.
- 3 Enter the default gateway IP address in the *Gateway IP Address* field.
- 4 Check all of your settings.
- 5 Click *NEXT* to proceed or *BACK* to change your settings.

### BigPond (Australia)

BigPond is a service provider in Australia that uses a heartbeat system to maintain the Internet connection.

To set up the Router for use with BigPond connection, use the following procedure:

**Figure 24** BigPond Mode Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

3COM

1. Getting start  
2. Wireless settings  
3. Connection settings  
4. Internet settings

**4. Internet settings**

**BigPond**

In this section you can configure the built-in client for the BigPond Internet service available Australia.

User Name :

Password :

Please retype your password :

Authentication Service Name :

BACK CANCEL NEXT

- 1 Enter your user name in the *User name* field.
- 2 Enter your password in the *Password* field.
- 3 Re-type your password in the *Please retype your password* field.
- 4 Enter the Service Name provided by your ISP in the *Authentication Service Name* field.
- 5 Check all of your settings.
- 6 Click *NEXT* to proceed or *BACK* to change your settings.

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

Clicking the *Home* button at any time, returns you to this home page. The *Home* screen shows the current software information. The main menu is located on the left side, as shown in [Figure 25](#). When you click on an item from the main menu, the corresponding screen will then appear in the center.

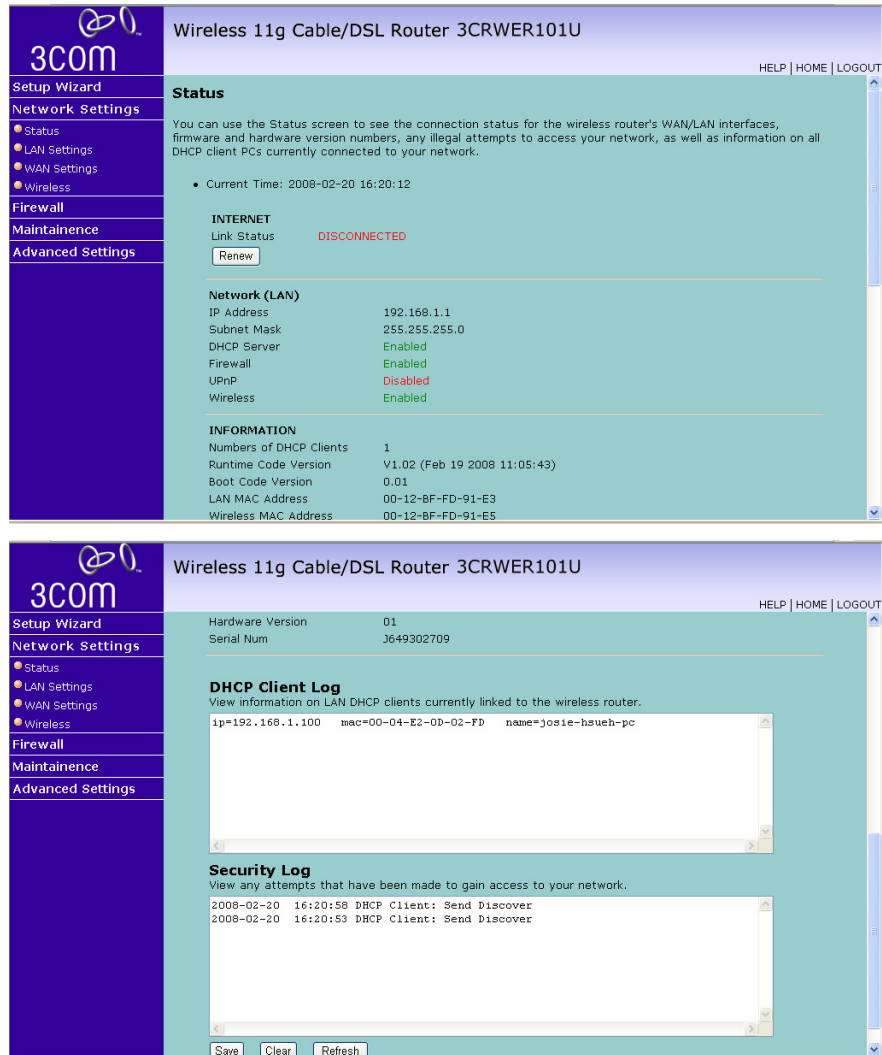
---

### Network Settings

#### Status

The Status screen displays WAN/LAN connection status, firmware and hardware version numbers, as well as information on DHCP clients connected to your network. You can also view the security Log. The security file, logfile.log, may be saved by clicking *Save* and choosing a location.

**Figure 25** Status Screen



- **Current Time:** Displays the current time.
- **INTERNET:** Displays WAN connection type and status.
  - **Release:** Click on this button to disconnect from the WAN.
  - **Renew:** Click on this button to establish a connection to the WAN.
- **Network (LAN):** Displays system IP settings, as well as DHCP Server, Firewall, UPnP and Wireless status.

- *INFORMATION*: Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface and for the Wireless 11g Router, as well as the hardware version and serial number.
- *DHCP Client Log*: Displays information on DHCP clients on your network.
- *Security Log*: Displays illegal attempts to access your network.
  - *Save*: Click on this button to save the security log file.
  - *Clear*: Click on this button to delete the access log.
  - *Refresh*: Click on this button to refresh the 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 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 One Day.
- Specify a local Domain Name.

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 26** LAN Settings Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

Setup Wizard

Network Settings

- Status
- LAN Settings
- WAN Settings
- Wireless

Firewall

Maintenance

Advanced Settings

### LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The wireless router must have an IP address for the local network.

#### Wireless Router IP Address

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

#### DHCP Server

DHCP Server:  Enabled  Disabled

DHCP Server ID:

#### DHCP IP Address Pool

Start IP: 192 . 168 . 1 . 100

End IP: 192 . 168 . 1 . 199

Domain Name:

Lease Time: One Day

- 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 *Enabled* in the *DHCP Server* field.
- 3 Enter the IP address range of *Start IP* and *End IP* in the *IP Address Pool* fields.
- 4 Specify the Local Domain Name for your network (this step is optional).
- 5 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.
- 6 Check all of your settings, and then click *SAVE SETTINGS*.



**WAN Settings** Specify the WAN connection type required by your Internet Service Provider.

You should see the first entry already contains information that's been configured using the Setup Wizard in the initial setup. If you want to change that information or set up other connection, select your connection type and click *Next* to set the detailed settings.

There are five options available for the DSL connection mode:

- *Dynamic IP Mode (for multiple PCs)* (see [page 43](#))
- *PPPoE* — PPP over Ethernet, providing routing for multiple PCs (see [page 44](#))
- *PPTP* — PPP, providing routing for multiple PCs (see [page 45](#))
- *Static IP Mode (for multiple PCs)* (see [page 46](#))
- *BigPond* — providing Internet access for Australian users (see [page 47](#))

### Dynamic IP (For Multiple PCs)

To configure the Dynamic IP Address function correctly, you should obtain the information on this screen from your ISP.

**Figure 27** Dynamic IP Mode Screen

3COM  
Wireless 11g Cable/DSL Router 3CRWER101U  
HELP | HOME | LOGOUT

Setup Wizard  
Network Settings  
Status  
LAN Settings  
WAN Settings  
Wireless  
Firewall  
Maintenance  
Advanced Settings

**Dynamic IP**

The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Wireless Router.

If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.

If necessary, you can use the "Renew" button on the Status page to renew the WAN IP address.

Host Name :

MAC Address : 00 - 12 - BF - FD - 91 - E4  
Clone MAC Address

SAVE SETTINGS CANCEL

- 1 The Host name is optional, but may be required by some Service Provider's. Enter the host name in the *Host Name* field.
- 2 If required by your Service Provider, you can use the Clone MAC Address button to copy the MAC address of the Network Interface Card (NIC) installed in your PC to replace the WAN MAC address.
- 3 If necessary, you can use the Renew button on the Status page to renew the WAN IP address.
- 4 Click *SAVE SETTINGS*.

### PPPoE

PPP over Ethernet, provides routing for multiple PCs. To configure this function correctly, you should obtain the information from your ISP.

**Figure 28** PPPoE Settings Screen

The screenshot shows the configuration interface for a 3COM Wireless 11g Cable/DSL Router 3CRWER101U. The left sidebar contains navigation options: Setup Wizard, Network Settings (selected), Firewall, Maintenance, and Advanced Settings. The main content area is titled 'Use PPPoE Authentication' and includes the following fields and options:

- User Name :
- Password :
- Please retype your password :
- Service Name :
- MTU :  (576<=MTU Value<=1492)
- Maximum Idle Time :  min
- Radio buttons:  Keep session,  Auto-connect,  Manual-connect

At the bottom right, there are two buttons: 'SAVE SETTINGS' and 'CANCEL'. A note at the top of the main area states: 'Do not change the MTU settings unless advised to by your Service Provider. NOTE: If your are on a leased line or pay-per min. connection - please set your max idle time to 3 minutes. This will cause your internet connection to drop after 3 minutes of idle time so you won't be charged for extra online time from your ISP.'

- 1 Enter the user name assigned to you by your ISP in the *User name* field. And enter the password assigned to you by your ISP in the *Password* field. Re-enter your password in the *Please retype your password* field.
- 2 If your ISP has provided you with a Service Name enter it in the *Service Name* field, otherwise, leave it blank.
- 3 Enter the *Maximum Transmission Unit (MTU)* value supplied by your ISP. If you do not know this, leave it at the default value.

- 4 Enter a *Maximum Idle Time* (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped.
- 5 Check *Keep session* to keep the session alive. Check the *Auto-connect* checkbox to automatically re-establish the connection as soon as you attempt to access the Internet again. Check the *Manual-connect* checkbox to manually re-establish the connection
- 6 Click *SAVE SETTINGS*.

### PPTP

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

**Figure 29** PPTP Settings Screen

The screenshot shows the PPTP configuration interface. On the left is a navigation menu with options: Setup Wizard, Network Settings (selected), Firewall, Maintenance, and Advanced Settings. The main content area is titled 'PPTP' and includes a brief description: 'Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.' Below this are several input fields: IP Address (four boxes), Subnet Mask (four boxes), Default Gateway (four boxes), User ID (text box), Password (text box), PPTP Gateway (four boxes), and Idle Time Out (a box with '10' and '(min)'). At the bottom of the form are three radio buttons: 'Manual-connect', 'Auto-connect' (which is selected), and 'Keep session'. A note at the bottom states: '\* If you have an ISP that charges by the time, change your idle time out value to 1 minute.' At the very bottom right are 'SAVE SETTINGS' and 'CANCEL' buttons.

- 1 Enter the IP Address information required by your ISP in the appropriate fields.
- 2 Enter the User ID assigned to you by your ISP in the *User ID* field. And enter the password assigned to you by your ISP in the *Password* field.
- 3 Enter the IP Address of the PPTP gateway as provided by your ISP
- 4 Enter the Idle Time Out for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. The default setting is 10 minutes. If your ISP charges you by the

minute, you should change the Idle Time Out to one minute. After the Idle Time Out has expired, set the action you wish the Router to take. You can tell the device to connect manually or automatically as soon as you try to access the Internet again, or to keep the session alive.

- 5 Click *SAVE SETTINGS*.

### Static IP (For Multiple PCs)

To configure the Static IP Address mode correctly, you should obtain the information on this screen from your ISP.

**Figure 30** Static IP Address Mode Screen

3COM Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

Setup Wizard

Network Settings

- Status
- LAN Settings
- WAN Settings
- Wireless

Firewall

Maintenance

Advanced Settings

### Static IP

If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.

Has your Service Provider given you an IP address and Gateway address?

IP address assigned by your Service Provider : 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

Service Provider Gateway Address : 0 . 0 . 0 . 0

SAVE SETTINGS CANCEL

- 1 If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address into the provided fields.
- 2 Click *SAVE SETTINGS*.

## BigPond

BigPond is a service provider in Australia that uses a heartbeat system to maintain the Internet connection.

**Figure 31** BigPond Mode Screen

The screenshot displays the configuration interface for a 3COM Wireless 11g Cable/DSL Router (model 3CRWER101U). The page title is 'BigPond' and it includes navigation links for 'HELP | HOME | LOGOUT'. A left-hand menu lists various settings categories: Setup Wizard, Network Settings (with sub-items: Status, LAN Settings, WAN Settings, and Wireless), Firewall, Maintenance, and Advanced Settings. The main content area is titled 'BigPond' and contains the following text: 'In this section you can configure the built-in client for the BigPond Internet service available Australia.' Below this text is a form with four input fields: 'User Name', 'Password', 'Please retype your password', and 'Authentication Service Name'. The 'Authentication Service Name' field is pre-filled with the text 'login-server'. At the bottom right of the form area, there are two buttons: 'SAVE SETTINGS' and 'CANCEL'.

- 1 Configure the built-in client with your user name, password and service name to get online.
- 2 Click *SAVE SETTINGS*.

**Wireless** The Wireless Settings screens allow you to turn on/ turn off the wireless function, and set up basic wireless settings.

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 32** Wireless Settings Screen



To use the wireless feature, check the *Enable* checkbox and click *SAVE SETTINGS*. After clicking *SAVE SETTINGS*, you will be asked to log in again.

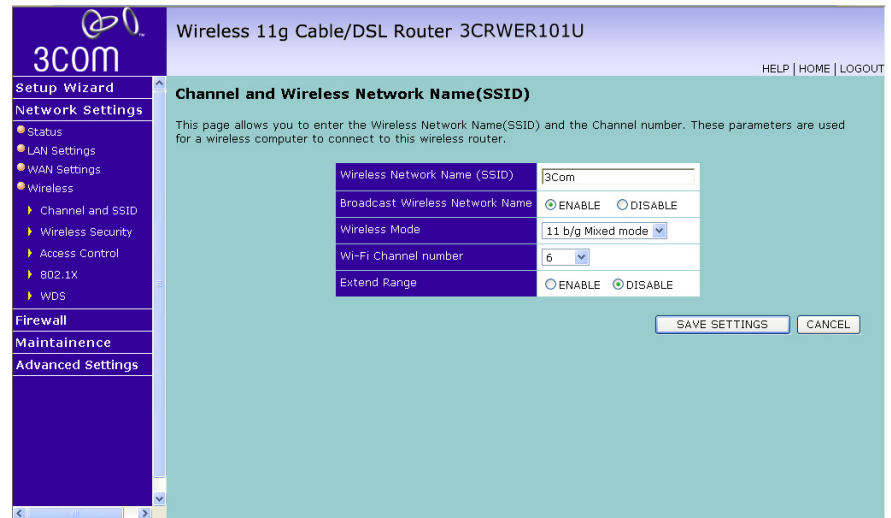
There are five items available:

- Channel and SSID
- Wireless Security
- Access Control
- 802.1X
- WDS

## Channel and SSID

Enter your wireless network settings on this screen. You must specify a common radio channel and SSID (Service Set ID) to be used by the Router and all of its wireless clients. Be sure you configure all of its clients to the same value. For security purposes, you should change the default SSID immediately.

**Figure 33** Channel and SSID Screen



To set up the wireless channel and SSID:

- 1 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.
- 2 Enable or disable *Broadcast Wireless Network Name*.

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 *Broadcast Wireless Network Name*, ensure that you know the name of your network first.

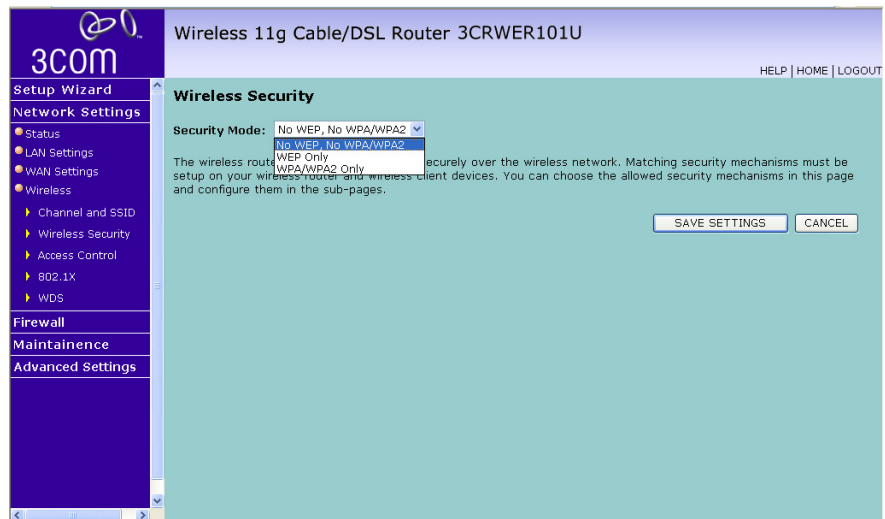
- 3 Select whether your Router will operate in 11b mode only, 11g mode only, or mixed 11b and 11g from the *Wireless Mode* drop-down menu.

- 4 Select the wireless channel you want to use from the *Wi-Fi Channel number* drop-down menu.
- 5 Enabling Extend Range extends the wireless radio range of the Router.
- 6 Click *SAVE SETTINGS*.

### Wireless Security

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

**Figure 34** Wireless Security Screen



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

- No WEP, No WPA/WPA2 (see [page 51](#))
- WEP Only (see [page 51](#))
- WPA/WPA2 (see [page 52](#))



**No WEP, No WPA/WPA2** 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.

**WEP Only** 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 35** WEP Only Screen

Wireless 11g Cable/DSL Router 3CRWER101U

3com

Setup Wizard

Network Settings

- Status
- LAN Settings
- WAN Settings
- Wireless
  - Channel and SSID
  - Wireless Security
  - Access Control
  - 802.1X
  - WDS
- Firewall
- Maintenance
- Advanced Settings

Wireless Security

Security Mode: WEP Only

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

WEP Mode:  64-bit  128-bit

Key Entry Method:  Hex  ASCII

Key Provisioning:  Static  Dynamic

Static WEP Key Setting

10/26 hex digits for 64-WEP/128-WEP

Default Key ID: 1

Passphrase:  (1~32 characters)

Key 1:

Key 2:

Key 3:

Key 4:

Clear

To enable 64-bit WEP:

- 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 to generate a hex key automatically 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 *SAVE SETTINGS*.

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 to generate a hex key automatically 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 *SAVE SETTINGS*.

**WPA/WPA2 Only** 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/WPA2 Only Screen

Wireless 11g Cable/DSL Router 3CRWER101U

3COM

Setup Wizard

Network Settings

- Status
- LAN Settings
- WAN Settings
- Wireless
  - Channel and SSID
  - Wireless Security
  - Access Control
  - 802.1X
  - WDS

Firewall

Maintenance

Advanced Settings

Wireless Security

Security Mode: WPA/WPA2 Only

WPA/WPA2 is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your wireless router and wireless client devices to use WPA/WPA2.

Cipher suite: TKIP+AES (WPA/WPA2)

Authentication:  802.1X  Pre-shared Key

Pre-shared key type:  Passphrase (8~63 characters)  Hex (64 digits)

Pre-shared Key:

Group Key Re\_Keying:  Per 1800 Seconds  Per 1000 K Packets  Disable

SAVE SETTINGS CANCEL

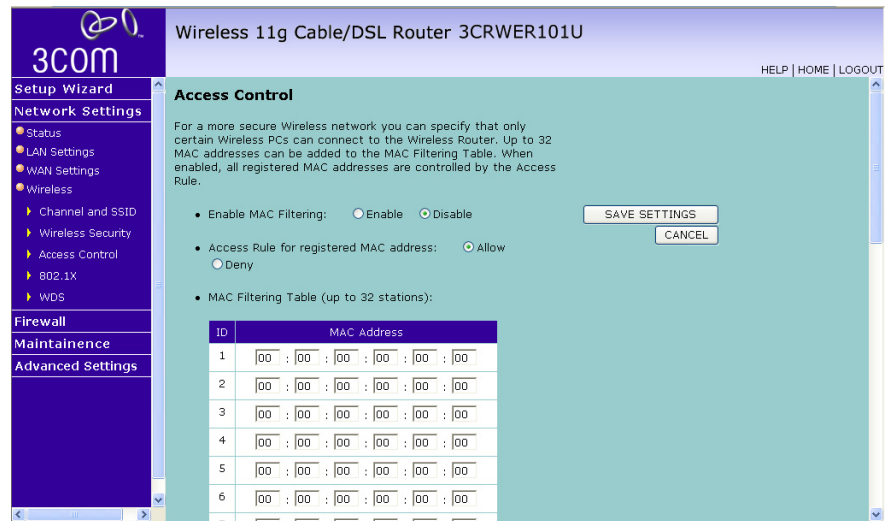
- 1 Select *WPA/WPA2 Only* from the *Security Mode* drop-down menu.
- 2 Select Encryption technique from the drop-down menu, two options are available: *TKIP+AES (WPA/WPA2)* or *AES WPA2 Only*.
- 3 Select *802.1X* or *Pre-shared Key* for the authentication method.
  - *802.1X*: for the enterprise network with a RADIUS server.
  - *Pre-shared key*: for the SOHO network environment without an authentication server.
- 4 Select the key type to be used in the *Pre-shared Key*.
- 5 Type the key in the *Pre-shared Key* field.
- 6 Set the period of renewing the broadcast/multicast key in the *Group Key Re\_Keying* field.
- 7 Click *SAVE SETTINGS*.

## Access Control

This feature is used to filter the clients based on their MAC addresses.

Check the *Enable MAC Address Filtering* checkbox on the Access Control screen.

**Figure 37** Access 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.

## 802.1X

If 802.1X is used in your network, then you should enable this function for the Router. 802.1X is a method of authenticating a client wireless connection. Enter the parameters below to connect the Router to the Authentication Server.

**Figure 38** 802.1X Screen

Wireless 11g Cable/DSL Router 3CRWER101U

802.1X

This page allows you to set the 802.1X, a method for performing authentication to wireless connection. These parameters are used for this wireless router to connect to the Authentication Server.

802.1X Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Session Idle Timeout	300 Seconds ( 0 for no timeout checking )
Re-Authentication Period	3600 Seconds ( 0 for no re-authentication )
Quiet Period	60 Seconds after authentication failed
Server Type	RADIUS

**RADIUS Server Parameters**

Server IP	192 . 168 . 2 . 1
Server Port	1812
Secret Key	
NAS-ID	

- 802.1X Authentication  
Enable or disable the authentication function.
- Session Idle Timeout  
This is the time (in seconds) that a session will sit inactive before terminating. Set to 0 if you do not want the session to timeout. (Default: 300 seconds)
- Re-Authentication Period  
The interval time (in seconds) after which the client will be asked to re-authenticate. For example, if you set this to 30 seconds, the client will have to re-authenticate every 30 seconds. Set to 0 for no re-authentication. (Default: 3600 seconds)
- Quiet Period  
This is the interval time (in seconds) for which the Router will wait between failed authentications. (Default: 60 seconds)
- Server Type  
Sets the authentication server type.

- RADIUS Server Parameters
  - Server IP  
Set the IP address of your RADIUS server.
  - Server Port  
Set the connection port that is configured on the radius server.
  - Secret Key  
The 802.1x secret key used to configure the Wireless 11g Router.
  - NAS-ID  
Defines the request identifier of the Network Access Server.

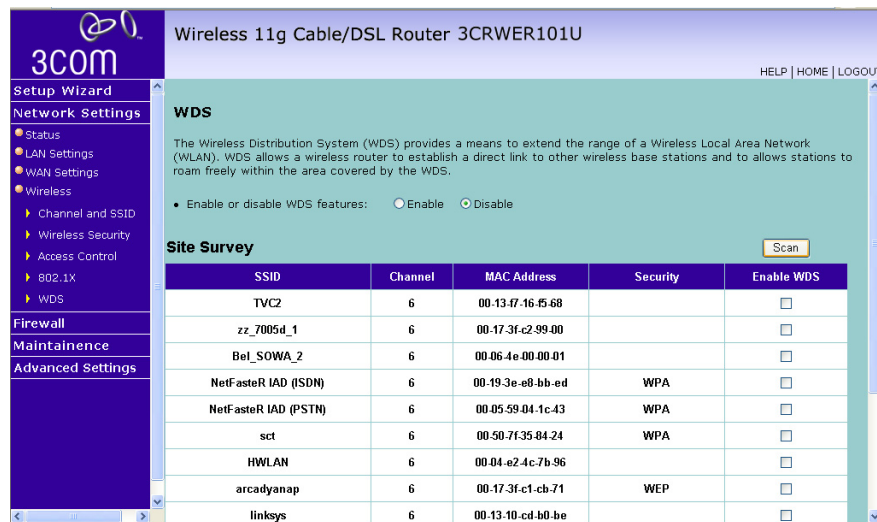
The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

Click *SAVE SETTINGS*.

## WDS

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 39** WDS Settings Screen



**WDS**

The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows a wireless router to establish a direct link to other wireless base stations and to allow stations to roam freely within the area covered by the WDS.

• Enable or disable WDS features:  Enable  Disable

**Site Survey**

SSID	Channel	MAC Address	Security	Enable WDS
TVC2	6	00-13-47-16-45-68		<input type="checkbox"/>
zz_7005d_1	6	00-17-3f-c2-99-00		<input type="checkbox"/>
Bel_SOWA_2	6	00-06-4e-00-00-01		<input type="checkbox"/>
NetFasteR IAD (ISDN)	6	00-19-3e-e8-bb-ed	WPA	<input type="checkbox"/>
NetFasteR IAD (PSTN)	6	00-05-59-04-1c-43	WPA	<input type="checkbox"/>
sct	6	00-50-7f-35-84-24	WPA	<input type="checkbox"/>
HWLAN	6	00-04-e2-4c-7b-96		<input type="checkbox"/>
arcadyanap	6	00-17-3f-c1-cb-71	WEP	<input type="checkbox"/>
linksys	6	00-13-10-cd-b0-be		<input type="checkbox"/>

- 1 Check the *Enable WDS Features* checkbox.
- 2 To refresh the list of available access points, click *Scan*.
- 3 Check the *Enable WDS* checkbox of the appropriate access points. (Default: Disable)

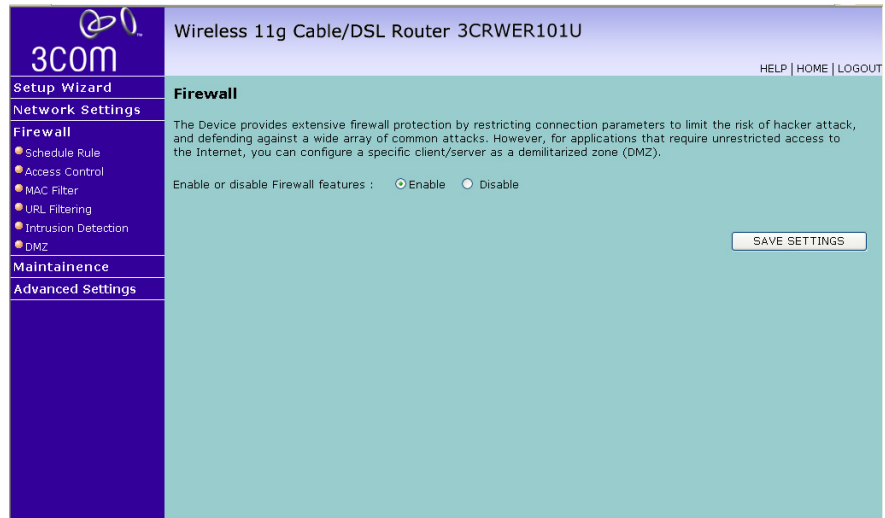


*WDS implementation varies from vendor to vendor. Hence there's no assured WDS interoperability with between all devices in the market.*

## Firewall

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.

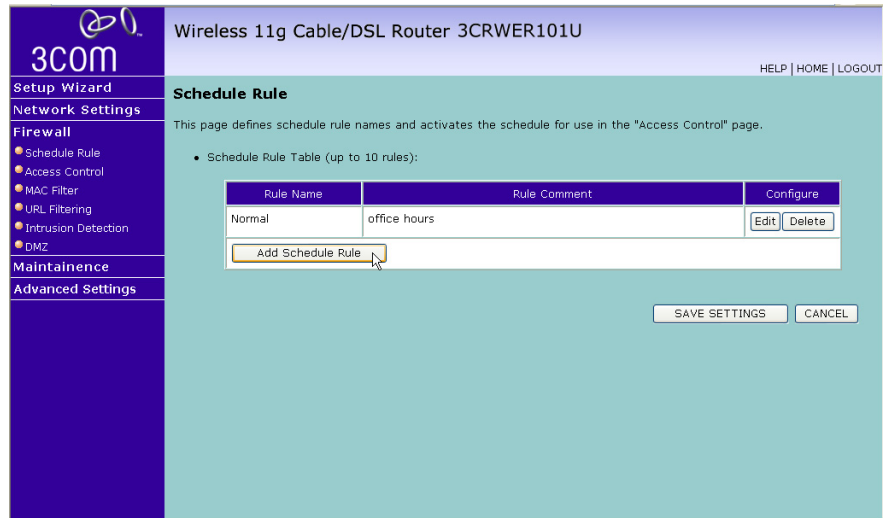
**Figure 40** Firewall Screen

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network.

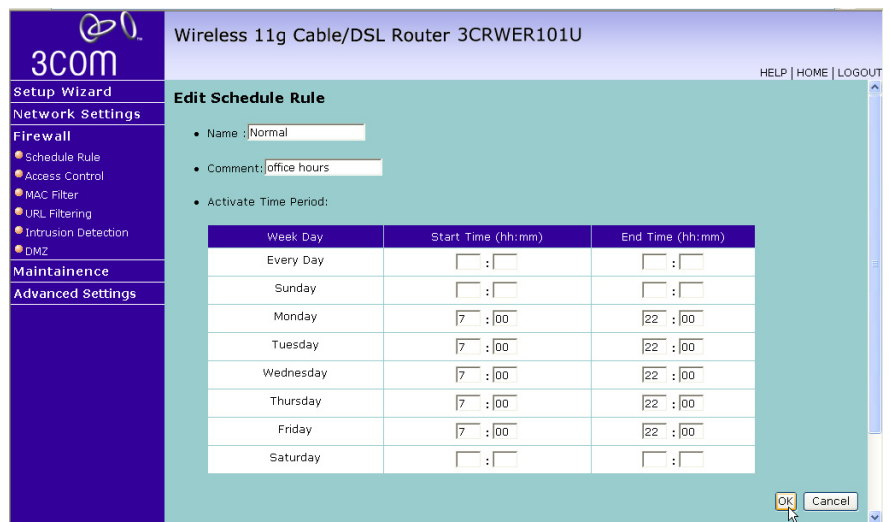
Enable the firewall feature, and click *SAVE SETTINGS* to proceed.

**Schedule Rule** The Router can be configured to restrict access to the Internet, email or other network services at specific days and times. Each access control rule may be activated at a scheduled time. First, define the schedule time on the Schedule Rule page, then apply the rule on the *Access Control* screen (see [page 60](#)).



**Figure 41** Schedule Rule Screen

- 1 Click *Add Schedule Rule* to add a schedule rule (a screen similar to [Figure 42](#) will appear).

**Figure 42** 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 *OK* and *SAVE SETTINGS*.

**Access 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 a single computer, a range of computers, or multiple computers.

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

**Figure 43** Access Control Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

Setup Wizard

Network Settings

Firewall

- Schedule Rule
- Access Control
- MAC Filter
- URL Filtering
- Intrusion Detection
- DMZ

Maintenance

Advanced Settings

**Access Control**

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

- Enable Filtering Function :  Enable  Disable
- Normal Filtering Table (up to 10 computers):

Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure
User 101-200	192.168.1.101 ~ 200	WWW with URL Blocking, News Forums, FTP, Telnet	Normal	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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 44](#) will appear).

Figure 44 Access Control Add PC Screen

Wireless 11g Cable/DSL Router 3CRWER101U

Setup Wizard **Access Control Add PC** HELP | HOME | LOGOUT

**Network Settings**

**Firewall**

- Schedule Rule
- Access Control
- MAC Filter
- URL Filtering
- Intrusion Detection
- DMZ

**Maintenance**

**Advanced Settings**

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL Filtering function, you need to configure the URL address first on the "URL Filtering" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

- Client PC Description:** User 101-200
- Client PC IP Address:** 192.168.1. 101 ~ 200
- Client PC Service:**

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Filtering	HTTP (Ref. URL Filtering Page)	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input checked="" type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input checked="" type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>

Wireless 11g Cable/DSL Router 3CRWER101U

Setup Wizard **Access Control Add PC** HELP | HOME | LOGOUT

**Network Settings**

**Firewall**

- Schedule Rule
- Access Control
- MAC Filter
- URL Filtering
- Intrusion Detection
- DMZ

**Maintenance**

**Advanced Settings**

E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input checked="" type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

**User Define Service**

Protocol:  TCP  UDP

Port Range: 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0

0 ~ 0

Clear

- Scheduling Rule (Ref. Schedule Rule Page):** Always Blocking

Always Blocking  
Normal

- Enter a description in the *Client PC Description* field, and the IP address or IP address range into the *Client PC IP Address* fields.
- 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 Service*.

- 5 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 58](#)).

- 6 Click *OK* to add the settings.

**MAC Filter** Use the MAC Filtering to block access to your network using MAC addresses.

**Figure 45** MAC Filter Screen

Wireless 11g Cable/DSL Router 3CRWER101U

Setup Wizard  
Network Settings  
Firewall  
Schedule Rule  
Access Control  
MAC Filter  
URL Filtering  
Intrusion Detection  
DMZ  
Maintenance  
Advanced Settings

MAC Filter

This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.

- MAC Address Control:  Enable  Disable
- MAC Filtering Table (up to 32 computers):

ID	MAC Address
1	00 : 04 : E2 : 00 : 02 : FD
2	: : : : : :
3	: : : : : :
4	: : : : : :
5	: : : : : :
6	: : : : : :
7	: : : : : :
8	: : : : : :
9	: : : : : :

SAVE SETTINGS  
CANCEL

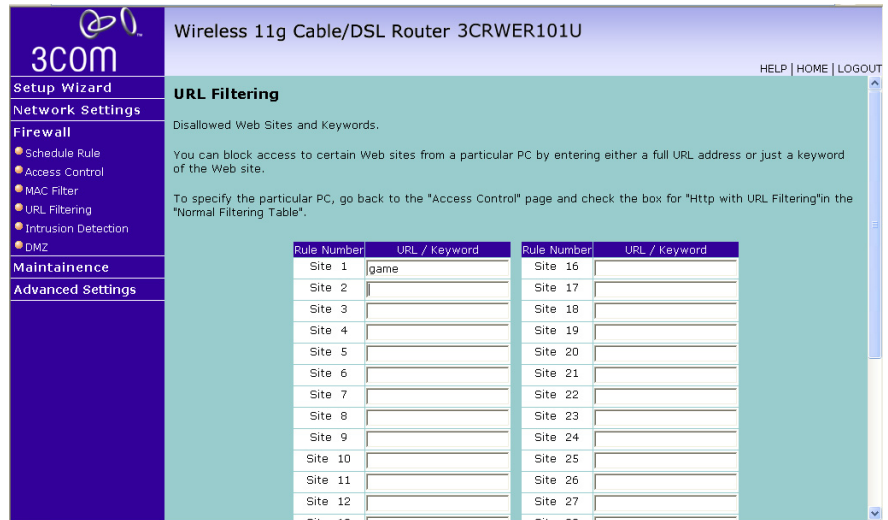
The Router can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Router to enter up to 32 MAC addresses that are allowed access to the WAN port. All other devices will be denied access. By default, this feature is disabled.

## URL Filtering

To configure the URL filtering feature, use the table on the URL Filtering screen to specify the Web sites (www.somesite.com) and/or keywords you want to filter on your network. This feature can be used to protect children from accessing violent or pornographic web sites.

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

**Figure 46** URL Filtering Screen



Enter the URL address or keywords in the *URL/Keyword* field. You can define up to 30 sites or keywords here.

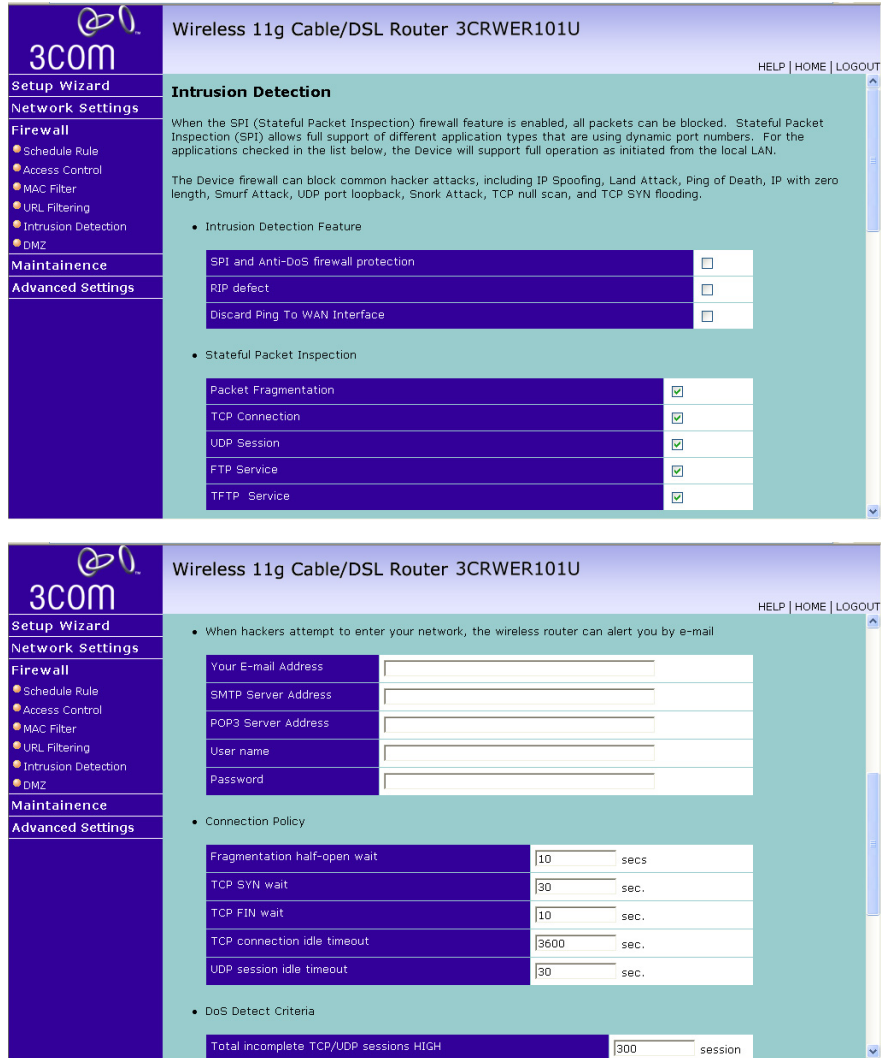
To complete this configuration, you will need to create or modify an access rule in "Access Control Add PC" on [page 60](#). To modify an existing rule, click the Edit option next to the rule you want to modify. To create a new rule, click on the Add PC option.

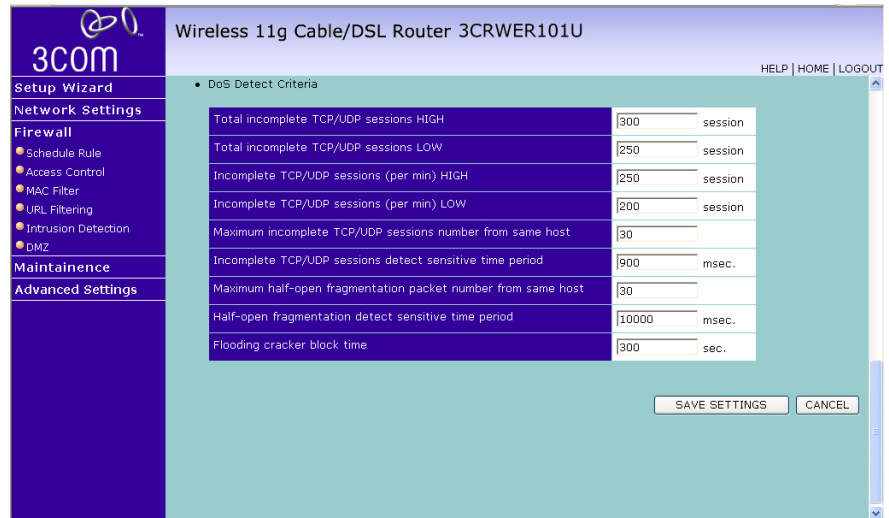
From the Access Control, Add PC section, check the option for WWW with URL Filtering in the Client PC Service table to filter out the web sites and keywords selected below, on a specific PC.

## Intrusion Detection

The Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as Denial-of-Service (DoS) attacks.

**Figure 47** Intrusion Detection Screen





Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Router protects against DoS attacks including: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack.



*The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.*

**Table 3** Intrusion Detection Parameters

Parameter	Defaults	Description
Intrusion Detection Feature		
SPI and Anti-DoS firewall protection	Yes	The Intrusion Detection feature of the Router limits the access of incoming traffic at the WAN port. When the Stateful Packet Inspection (SPI) feature is turned on, all incoming packets are blocked except those types marked with a check in the SPI section at the top of the screen.
RIP Defect	Disabled	If the router does not reply to an IPX RIP request packet, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets accumulating.
Discard Ping to WAN	Don't discard	Prevents a ping on the Router's WAN port from being routed to the network.
Stateful Packet Inspection	Enabled	<p>This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service and TFTP Service.</p> <p>It is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communication; 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 a connection to the specific port is requested.</p> <p>When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks FTP Service in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.</p>



Parameter	Defaults	Description
When hackers attempt to enter your network, we can alert you by email		
Your E-mail Address		Enter your email address.
SMTP Server Address		Enter your SMTP server address (usually the part of the email address following the "@" sign).
POP3 Server Address		Enter your POP3 server address (usually the part of the email address following the "@" sign).
User Name		Enter your email account user name.
Password		Enter your email account password.
Connection Policy		
Fragmentation half-open wait	10 secs	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 secs	Defines how long the software will wait for a TCP session to reach an established state before dropping the session.
TCP FIN wait	5 secs	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange.
TCP connection idle timeout	3600 secs (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 secs	The length of time for which a UDP session will be managed if there is no activity.
DoS Detect Criteria		
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>stop</i> deleting half-open sessions.
Incomplete TCP/UDP sessions (per min.) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min.) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.

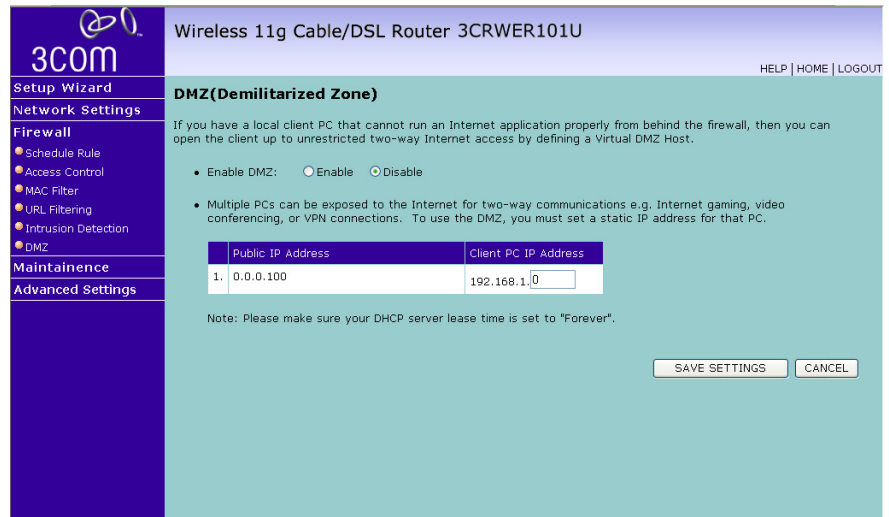
Parameter	Defaults	Description
Maximum incomplete TCP/UDP sessions number from same host	30 sessions	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/UDP sessions detect sensitive time period	900 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30 sessions	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	1 sec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 secs	Length of time from detecting a flood attack to blocking the attack.



*We do not recommend modifying the default parameters shown above.*

**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 48** DMZ Screen



Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort

## Maintenance

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

## Configuration Tools

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

**Figure 49** Configuration Tools Screen



- Backup Wireless Router Configuration — You can save your current configuration by clicking the *Backup Wireless Router Configuration* 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 from saved Configuration file (backup.bin) — The restore option will allow you to restore a previously saved configuration. Check the *Restore from saved Configuration file* radio button and click *NEXT* to restore the saved backup configuration file.
- Restore Wireless Router to Factory Defaults — 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, check *Restore Wireless Router to Factory Defaults* and click *NEXT*. You will be asked to confirm your decision.

## Firmware 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 50** Firmware Upgrade Screen

3Com  
Wireless 11g Cable/DSL Router 3CRWER101U  
HELP | HOME | LOGOUT

**Setup Wizard**  
**Network Settings**  
**Firewall**  
**Maintenance**  
• Configuration Tools  
• Firmware Upgrade  
• Reboot  
**Advanced Settings**

**Firmware Upgrade**

This tool allows you to upgrade the wireless router firmware. You can download the latest firmware from [3Com Support](#). The Product Model number is : 3CRWER101U.

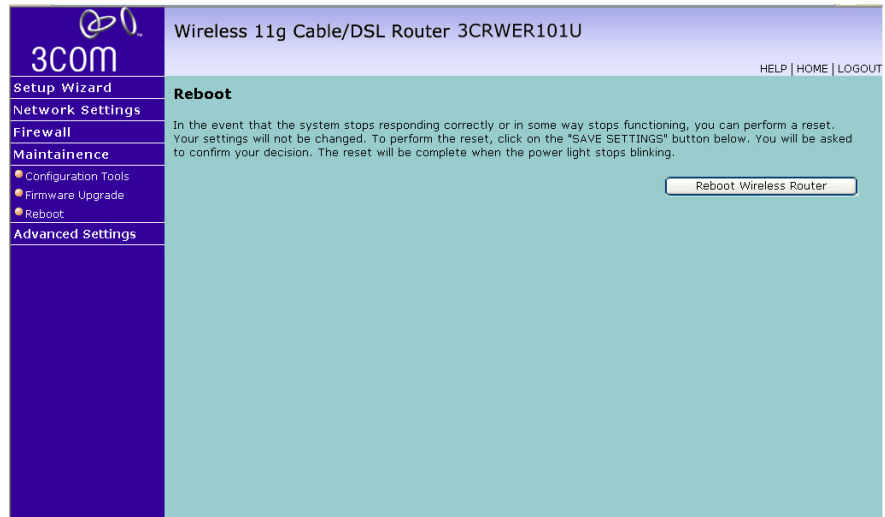
Enter the path and name, or browse to the location, of the upgrade file then click the BEGIN UPGRADE button. You will be prompted to confirm the upgrade to complete the process.

Firmware File

Please download the firmware file to your PC first, and then click *Browse* and select the firmware file. Click *BEGIN UPGRADE* to upload the firmware to the Router.

**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.

**Figure 51** Reboot Screen



Click the *Reboot Wireless Router* button to restart the Router.

---

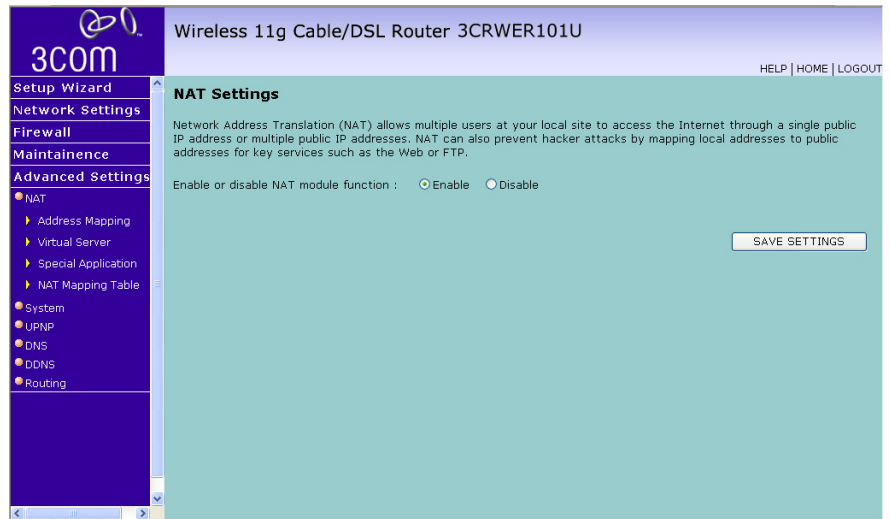
## Advanced Settings

From the Advanced Settings screen, you can configure:

- NAT: Shares a single ISP account with multiple users, sets up virtual servers.
- System: Sets the local time zone, the password for administrator access, the IP address of a PC that will be allowed to manage the Router remotely, and the IP address of a Domain Name Server.
- UPnP: Universal Plug and Play (UPnP) allows for simple and robust connectivity between external devices and your PC.
- DNS: Specify the IP address of your network domain name server.
- DDNS: Configures Dynamic DNS function.
- Routing: Sets routing parameters and displays the current routing table.

**NAT** The first menu item in the Advanced Settings section is Network Address Translation (NAT). This process allows all of the computers on your home network to use one IP address. Using the NAT capability of the Router, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

**Figure 52** NAT Screen



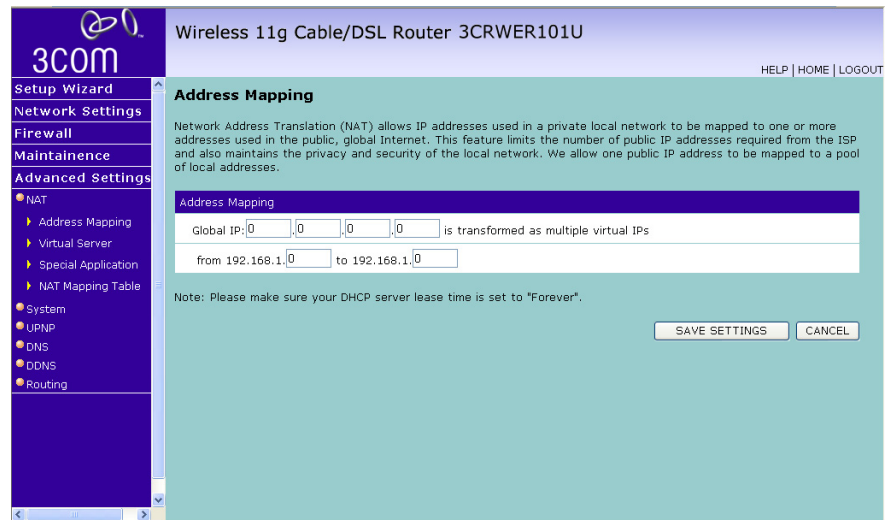
To use the NAT feature:

- 1 Check the *Enable* radio button.
- 2 Click *SAVE SETTINGS*.

## Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet.

**Figure 53** Address Mapping Screen



This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one public IP address to be mapped to a pool of local addresses.

## 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 54 Virtual Servers Screen

**3COM** Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

**Virtual Server**

You can configure the wireless router as a virtual server so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the wireless router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- Port Ranges: 100-150
- Multiple Ports: 25,110,80
- Combination: 25-100,80
- [All known port number](#)

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	Add	Clean
1	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
2	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
3	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
4	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
5	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
6	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
7	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean
8	192.168.1.	TCP			<input type="checkbox"/>	Add	Clean

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.

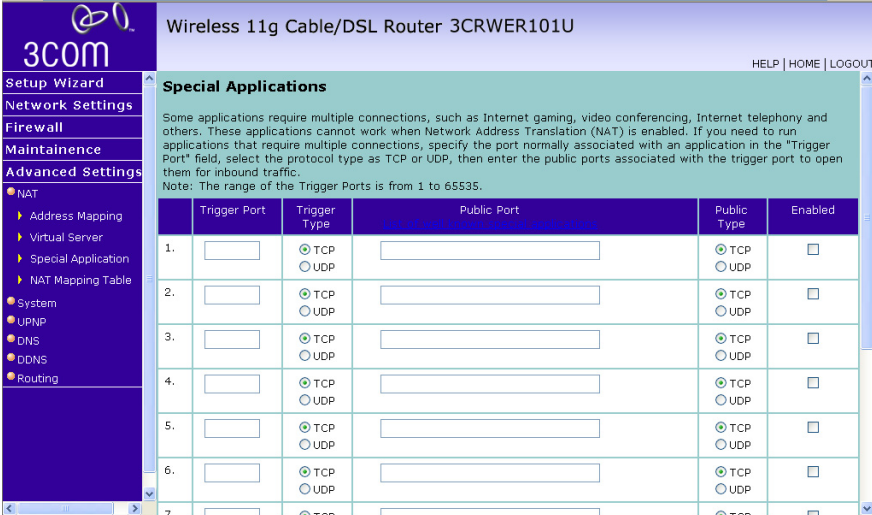
To manually configure your virtual servers:

- 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 *Enable* checkbox.
- 5 Click *Add* or *Clean* button to save the changes for each Virtual Server entry.

## Special Applications

Some applications, such as Internet gaming, video-conferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use the following screen to specify the additional public ports to be opened for each application.

**Figure 55** Special Applications Screen



Wireless 11g Cable/DSL Router 3CRWER101U

Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Note: The range of the Trigger Ports is from 1 to 65535.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

To put a computer in the DMZ:

- 1 Click the List of well known special applications link for more information.
- 2 Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, then enter the ports that the application requires. The ports may be in the format of a single port, or in a range, e.g., 72-96, or a combination of both.
- 3 Popular applications requiring multiple ports are listed in the Popular Applications field. From the drop-down list, choose the application and then choose a row number to copy this data into.
- 4 Click *SAVE SETTINGS*.



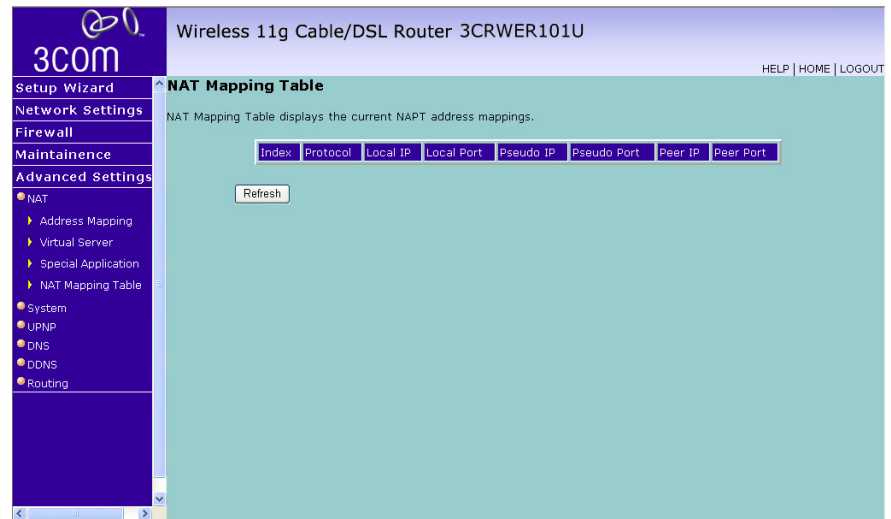
*Choosing a row that already contains data will overwrite the current settings.*

For a full list of ports and the services that run on them, see [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)

## NAT Mapping Table

This page displays the current NAPT (Network Address Port Translation) address mappings.

**Figure 56** NAT Mapping Table Screen



The NAT address mappings are listed 20 lines per page, click the control buttons to move forwards and backwards. As the NAT mapping is dynamic, a *Refresh* button is provided to refresh the NAT Mapping Table with the most updated values.

The content of the NAT Mapping Table is described as follows:

- Protocol - protocol of the flow.
- Local IP - local (LAN) host's IP address for the flow.
- Local Port - local (LAN) host's port number for the flow.
- Pseudo IP - translated IP address for the flow.
- Pseudo Port - translated port number for the flow.
- Peer IP - remote (WAN) host's IP address for the flow.
- Peer Port - remote (WAN) host's port number for the flow.

**System** This section includes all the basic configuration tools for the Router, such as time settings, password settings, remote management and Syslog server setup.

## Time Zone

You can set the time settings for the Router on this screen.

**Figure 57** Time Zone Screen

The figure displays two screenshots of the 3COM router's configuration interface, specifically the Time Settings page for a Wireless 11g Cable/DSL Router 3CRWER101U. The interface includes a navigation menu on the left and a main configuration area on the right.

**Top Screenshot:** The 'Set Time Zone' dropdown is set to '(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna'. The 'Enable Daylight Savings' checkbox is unchecked. The 'Start Daylight Savings Time' is set to January 1, and the 'End Daylight Savings Time' is also set to January 1. The 'Set Date and Time Manually' checkbox is checked. The date is set to February 20, 2008, and the time is set to 16:20:00. The 'Enable Automatic Time Server Maintenance' checkbox is unchecked.

**Bottom Screenshot:** The 'Set Date and Time Manually' checkbox is checked. The date is set to February 20, 2008, and the time is set to 16:20:00. The 'Enable Automatic Time Server Maintenance' checkbox is unchecked. The 'Configure Time Server (NTP)' section is visible, with the 'Primary Server' set to 129.132.2.21 - Europe and the 'Secondary Server' set to 130.149.17.8 - Europe. The 'SAVE SETTINGS' and 'CANCEL' buttons are visible at the bottom right.

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 Savings*. 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.

## Password Settings

Use this page to restrict access based on a password. For security you should assign one before exposing the Router to the Internet.

**Figure 58** Password Settings Screen

The screenshot shows the web interface of a 3COM Wireless 11g Cable/DSL Router 3CRWER101U. The left sidebar contains a navigation menu with the following items: Setup Wizard, Network Settings, Firewall, Maintenance, Advanced Settings (selected), NAT, System, Time Settings, Password Settings (highlighted), Remote Management, Syslog Server, UPNP, DNS, DDNS, and Routing. The main content area is titled 'Password Settings' and includes the following text: 'Set a password to restrict management access to the wireless router. If you want to manage the wireless router from a remote location (outside of the local network), you must also specify the IP address of the remote PC. You can do this in the System - Remote Management menu.' Below this text are four input fields: 'Current Password', 'New Password', 'Re-Enter Password for Verification', and 'Idle Time Out: 10 Min (Idle Time =0 : NO Time Out)'. At the bottom right of the main area are two buttons: 'SAVE SETTINGS' and 'CANCEL'.

Passwords can contain from 3 to 12 alphanumeric characters and are case sensitive.



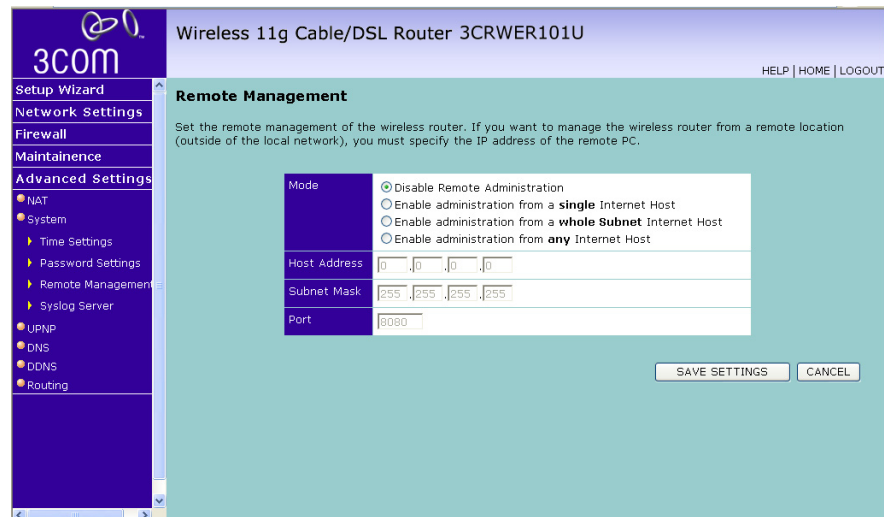
If your password is lost, or you cannot gain access to the user interface, press the reset button on the bottom of the device (holding it down for at least eight seconds) to restore the factory defaults. The default password is “admin”.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time an inactive login session will be maintained. If the connection is inactive for longer than the maximum idle time, it will be logged out, and you will have to log in to the web management system again. Setting the idle time to 0, will mean the connection never times out. (Default: 10 minutes)

## Remote Management

By default, management access is only available to users on your local network. However, you can also manage the Router from a remote host by entering the IP address of a remote computer on this screen.

**Figure 59** Remote Management Screen



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.

Click **SAVE SETTINGS**.

## Syslog Server

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

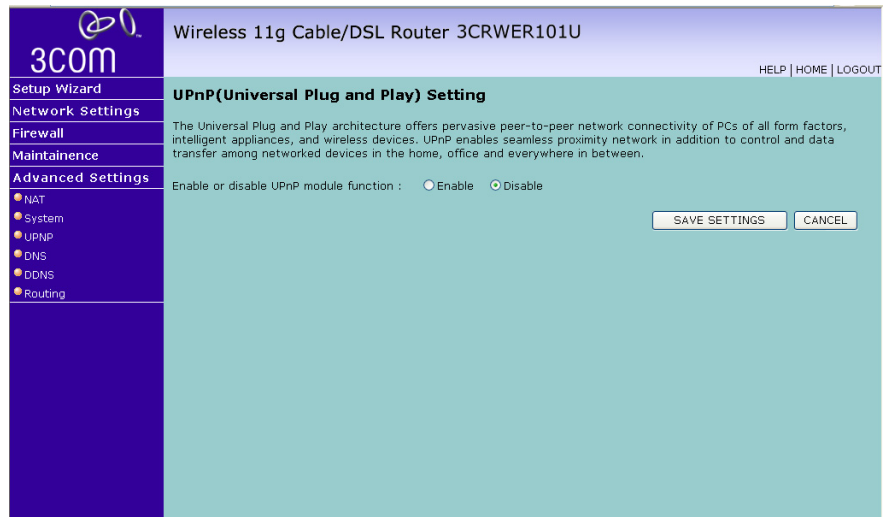
**Figure 60** Syslog Server Screen

The screenshot shows the configuration interface for the Syslog Server on a 3COM router. The page title is "Wireless 11g Cable/DSL Router 3CRWER101U". The left sidebar contains a navigation menu with the following items: Setup Wizard, Network Settings, Firewall, Maintenance, Advanced Settings (selected), NAT, System, Time Settings, Password Settings, Remote Management, Syslog Server (selected), UPNP, DNS, DDNS, and Routing. The main content area is titled "Syslog Server" and includes the following text: "Using third party syslog software, this Syslog Server tool will automatically download the router log to the server IP address specified below." Below this text are two input fields: "Server LAN IP Address" with a dotted IP address (0 . 0 . 0 . 0) and an "Enabled" checkbox. At the bottom right of the form are two buttons: "SAVE SETTINGS" and "CANCEL".

- 1 Enter the *Server LAN IP Address* in the space provided.
- 2 Check the *Enabled Syslog Server* checkbox.
- 3 Click **SAVE SETTINGS**.

**UPNP** Universal Plug and Play technology makes home networking simple and affordable. This architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP architecture leverages TCP/IP and the web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

**Figure 61** UPNP Screen



- 1 Click *Enable* to turn on the Universal Plug and Play function of the Router. This function allows the device to automatically and dynamically join a network.
- 2 Click *SAVE SETTINGS*.



**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 62** DNS Screen

Wireless 11g Cable/DSL Router 3CRWER101U

3com

HELP | HOME | LOGOUT

Setup Wizard

Network Settings

Firewall

Maintenance

Advanced Settings

• NAT

• System

• UPnP

• DNS

• DDNS

• Routing

**DNS**

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as `www.3com.com`, a DNS server will find that name in its index and find the matching IP address: `161.88.242.11`. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address

Secondary DNS Address (optional)

SAVE SETTINGS CANCEL

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

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, PPTP or PPPoE, it is likely that you do not have to enter a DNS address.

**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 two DDNS providers:

- DynDNS.org
- TZO.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 63** Dynamic Domain Name Server (DDNS) Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

Setup Wizard

Network Settings

Firewall

Maintenance

Advanced Settings

- NAT
- System
- UPnP
- DNS
- DDNS
- Routing

**DDNS (Dynamic DNS) Settings**

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Dynamic DNS  Enable  Disable

Provider

Domain Name

Account / E-mail

Password / Key

SAVE SETTINGS CANCEL

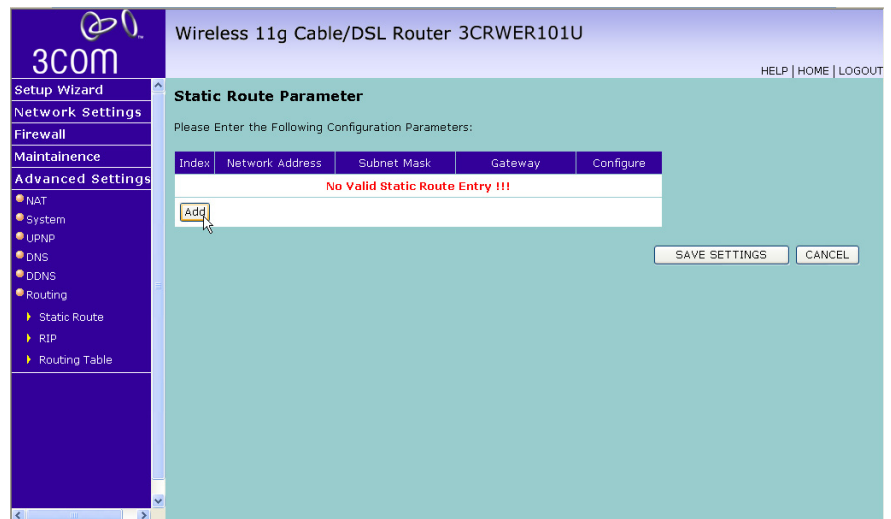
- 1 Check *Enable* Dynamic DNS.
- 2 Select the provider, and then enter the necessary information provided by your DDNS provider.
- 3 Click *SAVE SETTINGS*.

**Routing** This section defines routing related parameters, including static routes, RIP (Routing Information Protocol) parameters and routing table.

**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 64** 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.
- *Configure* — Allows you to edit existing routes.

After you have finished making changes to the table, click *SAVE SETTINGS*.

- RIP** 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 65** RIP Parameter Screen

Wireless 11g Cable/DSL Router 3CRWER101U

HELP | HOME | LOGOUT

**RIP Parameter**

The device supports Routing Information Protocol (RIP) v1 and v2 to dynamically exchange routing information with adjacent routers.

Please Enter the following Configuration Parameters:

- **General RIP parameter:**
  - RIP mode:  Enable  Disable
  - Auto summary:  Enable  Disable
- **Table of current interface RIP parameter:**

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
WAN	Disable	1	Enable	None	
WLAN_g	Enable	1	Enable	None	
WLAN_XR	Disable	1	Enable	None	
WDS-1	Disable	1	Enable	None	
WDS-2	Disable	1	Enable	None	
WDS-3	Disable	1	Enable	None	

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

- 1 Check the *Enable RIP Mode* 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.

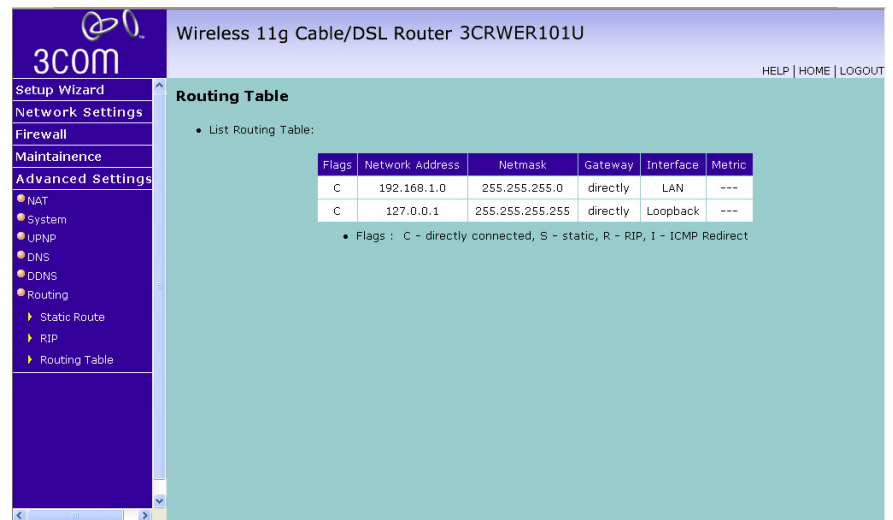


3Com recommends that you only use RIPv1 if there is an existing RIP-enabled device on your network that does not support RIPv2. In all other cases, you should use RIPv2.

- 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 *SAVE SETTINGS*.

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

**Figure 66** Routing Table Screen



The screenshot shows the web interface for a 3COM Wireless 11g Cable/DSL Router 3CRWER101U. The left sidebar contains navigation options: Setup Wizard, Network Settings, Firewall, Maintenance, and Advanced Settings. Under Advanced Settings, the following options are listed: NAT, System, UPnP, DNS, DDNS, Routing, Static Route, RIP, and Routing Table. The main content area is titled "Routing Table" and displays a table of routing entries. Below the table, a legend explains the flags: C - directly connected, S - static, R - RIP, I - ICMP Redirect.

Flags	Network Address	Netmask	Gateway	Interface	Metric
C	192.168.1.0	255.255.255.0	directly	LAN	---
C	127.0.0.1	255.255.255.255	directly	Loopback	---

• Flags : C - directly connected, S - static, R - RIP, I - ICMP Redirect



# 6

## TROUBLESHOOTING

---

### 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 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, Windows XP and Windows Vista, 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 WAN 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 PPTP 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 network 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 bottom of the device for 8 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”](#) on [page 48](#) 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 Antenna. 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.



*Check on [www.3com.com](http://www.3com.com) for the latest version of firmware.*

- 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:  
  
**http://192.168.1.1.**  
  
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

### How do I reset the Router to Factory Defaults?

See [“Forgotten Password and Reset to Factory Defaults”](#) on [page 90](#).

### How many computers on the LAN does the Router support?

A maximum of 253 computers on the LAN are supported.

### How many wireless clients does the Router support?

A maximum of 32 wireless clients are supported.



*Maximum practical number of users depends on speed of broadband connection and amount of traffic generated by users.*

### There are only 4 LAN ports on the Router. How are additional computers connected?

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 switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

<http://www.3com.com/>

### Does the Router support virtual private networks (VPNs)?

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.

# A

# IP ADDRESSING

---

## **The Internet Protocol Suite**

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.

---

## **Managing the Router over the Network**

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

- An IP address
- A Subnet Mask

## **IP Addresses and Subnet Masks**

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 4](#) for an example about how a network with three computers and a Router might be configured.

**Table 4** IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.255.0
PC 2	192.168.100.33	255.255.255.0
PC 3	192.168.100.188	255.255.255.0
Router	192.168.100.72	255.255.255.0

### 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 5](#) for an example about how a network (only four computers represented) and a Router might be configured.

**Table 5** IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Router	192.168.002.72	255.255.0.0

## 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.



# B

## TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the Wireless 11g Cable/DSL Router.

---

### Wireless 11g Cable/DSL Router

#### Interfaces

WAN connection — one 10 Mbps/100 Mbps dual speed Ethernet port

LAN connection — four 10 Mbps/100 Mbps dual speed Ethernet ports

#### 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/WPA2

Maximum clients: 32

O/P Power: 19.5dBm E.I.R.P.

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/WPA2

Maximum clients: 32

O/P Power 19.5dBm E.I.R.P.

**Operating Temperature**

0 °C to 40 °C (32 °F to 105 °F)

**Power**

9V 1A

**Humidity**

0% to 90% (non-condensing) humidity

**Dimensions**

- Width = 118 mm (4.6 in.)
- Depth = 120 mm (4.7 in.)
- Height = 30 mm (1.1 in.)

**Weight**

Approximately 550 g (1.1 lbs)

**Standards**

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

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
- Windows Vista
- 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).





# END USER SOFTWARE LICENSE AGREEMENT

***IMPORTANT: READ BEFORE YOU DOWNLOAD, INSTALL, OR USE THIS SOFTWARE***

## **3COM END USER SOFTWARE LICENSE AGREEMENT**

**YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING AND/OR USING THIS SOFTWARE, 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 THIS 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 THIS SOFTWARE AND DOCUMENTATION ON PHYSICAL MEDIA, PROMPTLY RETURN THE ENTIRE PRODUCT WITH THIS SOFTWARE AND DOCUMENTATION UNUSED TO THE SUPPLIER WHERE YOU OBTAINED IT.**

**IN THE EVENT THAT A SYSTEM INTEGRATOR, CONSULTANT, CONTRACTOR, OR OTHER PARTY DOWNLOADS THE SOFTWARE FOR YOU, AND/OR USES OR INSTALLS THE SOFTWARE OR DOCUMENTATION ON YOUR BEHALF PRIOR TO YOUR USE OF THE SOFTWARE OR DOCUMENTATION, SUCH SYSTEM INTEGRATOR, CONSULTANT, CONTRACTOR, OR OTHER PARTY WILL BE DEEMED TO BE YOUR AGENT ACTING ON YOUR BEHALF AND YOU WILL BE DEEMED TO HAVE ACCEPTED ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT AS IF YOU HAD DOWNLOADED, INSTALLED, OR USED THE SOFTWARE OR DOCUMENTATION.**

**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.

You may not derive or attempt to derive the source code of the Software by any means, nor permit any other party to derive or attempt to derive such source code. You may not reverse engineer, decompile,

disassemble, or translate the Software or any part thereof. 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.

**OPEN SOURCE SOFTWARE:** Certain items of independent code that are included with the Software hereunder may be subject to various open source or free software licenses (the "Open Source Software"). This Open Source Software is licensed under the terms of the end-user license(s) that are provided as part of the Documentation or upon request to 3Com. Nothing in this Agreement limits your rights under, or grants you rights that supersede, the terms and conditions of any applicable end-user license for such Open Source Software. The terms of this Agreement other than the Limited Warranties and Disclaimers and the Limitation of Liability will not apply to the Open Source Software.

**THIRD-PARTY APPLICATIONS.** Any third-party supplier of computer programs included in the Software is a third-party beneficiary of the provisions of this Section 1, and such third party may protect its rights in the Software against violations of this license.

**EXPORT:** The product, Software, Documentation and/or other technical data (collectively "Product") are subject to U.S. export control laws and regulations. Certain products made by 3Com are further controlled for export as encryption items and may be subject to additional export or import regulations in other countries. You agree that you will not export, reexport or transfer the Product (or any copies thereof) or any products utilizing the Product 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, reexport, transfer or import the Product.

You agree that you are not prohibited by the U.S. or other government export control regulations from receiving this Software, Documentation and/or other technical data.

In addition to the above, the Product may not be used by, or exported or reexported to (i) any U.S.- or EU- sanctioned or embargoed country, or to nationals or residents of such countries; or (ii) to any person, entity,

organization or other party identified on the U.S. Department of Commerce's Table of Denial Orders or the U.S. Department of Treasury's lists of "Specially Designated Nationals and Blocked Persons," as published and revised from time to time; (iii) to any party engaged in nuclear, chemical/biological weapons or missile proliferation activities, unless authorized by U.S. and local (as required) law or regulations.

**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 licensors. You agree to hold such trade secrets in confidence. You further acknowledge and agree that the Software is licensed and not sold to you and that all 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 licensors.

**UNITED STATES GOVERNMENT RESTRICTED RIGHTS:** The Software and Documentation are "Commercial Items(s)" as defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. § 12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227-7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Therefore, if you are licensing the Software and/or Documentation for acquisition by the U.S. Government or any contractor therefore, you will license consistent with the policies set forth in 48 C.F.R. §12.212 (for civilian agencies) and 48 C.F.R. §227-7202-1 and 227.7202-4 (for the Department of Defense), and their successors.

**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 any portions thereof 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 DISCLAIMER:** All warranties applicable to the Software are as stated on the Limited Warranty Sheet or in the product manual, whether in paper or electronic form, accompanying the Software. EXCEPT AS EXPRESSLY STATED ON SUCH LIMITED WARRANTY SHEET, THE SOFTWARE IS LICENSED TO YOU "AS IS," WITHOUT WARRANTY OF ANY KIND AND 3COM AND ITS LICENSORS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT OF THIRD-PARTY RIGHTS.

**LIMITATION OF LIABILITY:** 3COM AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION LOST PROFITS), EVEN IF 3COM OR SUCH LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NO 3COM LICENSOR SHALL HAVE ANY LIABILITY WHATSOEVER UNDER THIS AGREEMENT.

**GOVERNING LAW:** This Agreement shall be governed by the laws of the Commonwealth of Massachusetts, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

**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 want to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write: 3Com Corporation, 350 Campus Drive, Marlborough, MA 01752. (508) 323-5000. Alternatively, log onto [www.3Com.com](http://www.3Com.com) and click "Contact Us" at the bottom of your screen for topic-specific contact information.

Copyright © 2008 3Com Corporation. All rights reserved. 3Com is a registered trademark of 3Com Corporation.

# D

## OBTAINING SUPPORT FOR YOUR PRODUCT

---

For technical support, register your product and request service via our online support system at <http://www.3Com.com/esupport>



# 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 it's 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 be 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 be 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.

<b>Traffic</b>	The movement of data packets on a network.
<b>Universal Plug and Play</b>	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.
<b>URL Filter</b>	A URL Filter is a feature of a firewall that allows it to stop its clients from browsing inappropriate Web sites.
<b>WAN</b>	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.
<b>WDS</b>	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.
<b>WECA</b>	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)
<b>WEP</b>	Wired Equivalent Privacy. A shared key encryption mechanism for wireless networking. Encryption strength is 40/64 bit or 128 bit.
<b>Wi-Fi</b>	Wireless Fidelity. This is the certification granted by WECA to products that meet their interoperability criteria. (see also 802.11b, WECA)
<b>Wireless Client</b>	The term used to describe a desktop or mobile PC that is wirelessly connected to your wireless network.
<b>Wireless LAN Service Area</b>	Another term for ESSID (Extended Service Set Identifier).
<b>Wizard</b>	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 Wireless 11g Cable/DSL Router

---

### GENERAL STATEMENTS

The 3Com Wireless 11g Cable/DSL Router (WL-550) 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).

---

### BRAZIL ANATEL COMPLIANCE

Este produto está homologado pela ANATEL, de acordo com os procedimentos regulamentados pela Resolução 242/2000 e atende aos requisitos técnicos aplicados.

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

Para maiores informações, consulte o site da ANATEL – [www.anatel.gov.br](http://www.anatel.gov.br)





# INDEX

---

## Numbers

64-bit WEP Screen 47

---

## A

Access Control Screen 56

Add PC Screen 57

Add Schedule Rule Screen 55

Addresses

IP 91

Automatic Addressing 93

---

## C

Cable Specifications 97

Conventions

notice icons, About This Guide 6

text, About This Guide 6

---

## D

DDNS 80

DHCP 93

DHCP server 23

disabling 24

DNS 22

DNS Screen 79

DSL mode 29

Dynamic Domain Server (DDNS) Screen 80

Dynamic IP Mode Screen 30, 33, 39, 42, 43

---

## E

Encryption Screen 46

Encryption, disabling 47

---

## F

Firewall Screen 54

Forgotten Password 86

---

## I

Internet

addresses 91

Internet Properties Screen 24

Internet Protocol (TCP/IP) Properties Screen 22

IP Address 38, 91

---

## L

LAN Settings Screen 38

LED 12

LEDs 12

Local Area Properties Screen 22

---

## M

mode 30

---

## N

Network

addresses 91

Networking

wireless 87

NIC

wireless 12

---

## P

Password 26

Poison Reverse 83

PPPoE 24, 30, 32

PPPoE Screen 31

PPPoE Settings Screen 40

PPTP 32

PPTP Screen 32

PPTP Settings Screen 41

---

---

**R**

Reset to Factory Defaults 86  
RIP Parameter Screen 82  
Router Login Screen 26  
Routing Mode Screen 34

---

**S**

Schedule Rule Screen 55  
Setup Wizard 25  
Specifications  
    technical 95  
SSID 45  
Static Addressing 93  
Static Route Parameters Screen 81  
Subnet Mask 91

---

**T**

TCP/IP 21, 23, 91  
Technical  
    specifications 95  
    standards 95  
Time and Time Zone screen 74, 75

---

**U**

URL Blocking Screen 59, 60, 61

---

**V**

Virtual Servers Screen 71

---

**W**

WDS 53  
Web Browser Location Field 25  
Web Proxy 24  
WiFi Protected Access 48  
Wireless  
    networking 87  
    NIC 12  
Wireless Configuration Scree 45  
Wireless Settings Screen 44  
Wireless WDS Settings Screen 53  
WPA-PSK (no server) Screen 49