OfficeConnect®

Wireless 11g Access Point User Guide

3CRWE454G72

The Standard for Wireless Fidelity.

http://www.3com.com/

Part No. DUA0045-4AAA01
Rev. 01
Published July 2003

3Com Corporation
5500 Great America Parkway
Santa Clara, California
95052-8145

Copyright © 2003, 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 Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies 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, OfficeConnect 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 trademarks of WECA (Wireless Ethernet Compatibility 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.

CONTENTS

ABOUT THIS GUIDE

Naming Convention 7
Conventions 8
Feedback about this User Guide 8
Related Documentation 9
Product Registration 9

1 INTRODUCING THE ACCESS POINT

OfficeConnect Wireless 11g Access Point 12
Access Point Advantages 13
Package Contents 13
Minimum System and Component Requirements 14
Front Panel 14
Rear Panel 16

2 HARDWARE INSTALLATION

Introduction 17
Safety Information 17
Positioning the Access Point 17
Using the Rubber Feet 18
Wall Mounting 18
Powering Up the Access Point 19
Connecting the Access Point 19

3 RUNNING THE SETUP WIZARD

Accessing the Wizard 21
Password 26
LAN Settings 26
Wireless Settings 28
Summary 30

4 ACCESS POINT CONFIGURATION

Navigating Through the Access Point Configuration Pages 31
Main Menu 31
Option Tabs 32
Welcome Screen 32
Notice Board 33
Password 33
Wizard 34
LAN Settings 34
Unit Configuration 34
DHCP Clients List 38
Wireless Settings 39
Configuration 39
Encryption 41
Configuring WPA Encryption 41
Configuring WEP Encryption 42
Connection Control 44
Client List 47
Profile 48
System Tools 50
Restart 50
Configuration 50
Upgrade 51
Status and Logs 53
Status 54
Logs 54
Support and Feedback 54

5 CLIENT BRIDGE MODE CONFIGURATION

What is Client Bridge Mode? 57
Switching to Client Bridge Mode 57
Configuring Client Bridge Mode 58
Welcome Menu 58
LAN Settings 59
Wireless Settings 59
Configuration 60
Encryption 60

Restart 63
Status and Logs 63
Support and Feedback 63

6 TROUBLESHOOTING

Basic Connection Checks 65
Browsing to the Access Point Configuration Screens 65
Forgotten Password and Reset to Factory Defaults 66
Wireless Networking 66
Alert LED 68
Recovering from Corrupted Software 68
Frequently Asked Questions 69

A USING DISCOVERY

Running the Discovery Application 71
Windows Installation (95/98/2000/Me/NT) 71

B IP ADDRESSING

The Internet Protocol Suite 73
Managing the Access Point over the Network 73
IP Addresses and Subnet Masks 73
How does a Device Obtain an IP Address and Subnet Mask? 75
DHCP Addressing 75
Static Addressing 75
Auto-IP Addressing 75

C TECHNICAL SPECIFICATIONS

Standards 78

D SAFETY INFORMATION

E END USER SOFTWARE LICENSE AGREEMENT

GLOSSARY

INDEX

REGULATORY NOTICES FOR THE WIRELESS 11G ACCESS POINT

About This Guide

This guide describes how to install and configure the OfficeConnect Wireless 11g Access Point (3CRWE454G72).

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).

If a release note is shipped with the OfficeConnect Wireless 11g Access Point 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 OfficeConnect Wireless 11g Access Point is referred to as the "Access Point".

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

The PC used to configure the Access Point is referred to as the "admin computer". 3Com recommends that during the initial configuration that this is connected to the same switch or hub as the Access Point.

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 *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

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:

- OfficeConnect Wireless 11g Access Point User Guide
- Part Number DUA0045-4AAA01
- Page 24

Do not use this e-mail address for technical support questions. For information about contacting Technical Support, please refer to the Support and Safety Information sheet.

Related Documentation

In addition to this guide, each Access Point document set includes one Installation Guide. This guide contains the instructions you need to install and configure your Access Point.

Product Registration

You can now register your Access Point on the 3Com web site and receive up-to-date information on your product:

`http://www.3com.com/register/`

1 INTRODUCING THE ACCESS POINT

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. The OfficeConnect® product range from 3Com has changed all this, bringing networks to the small office.

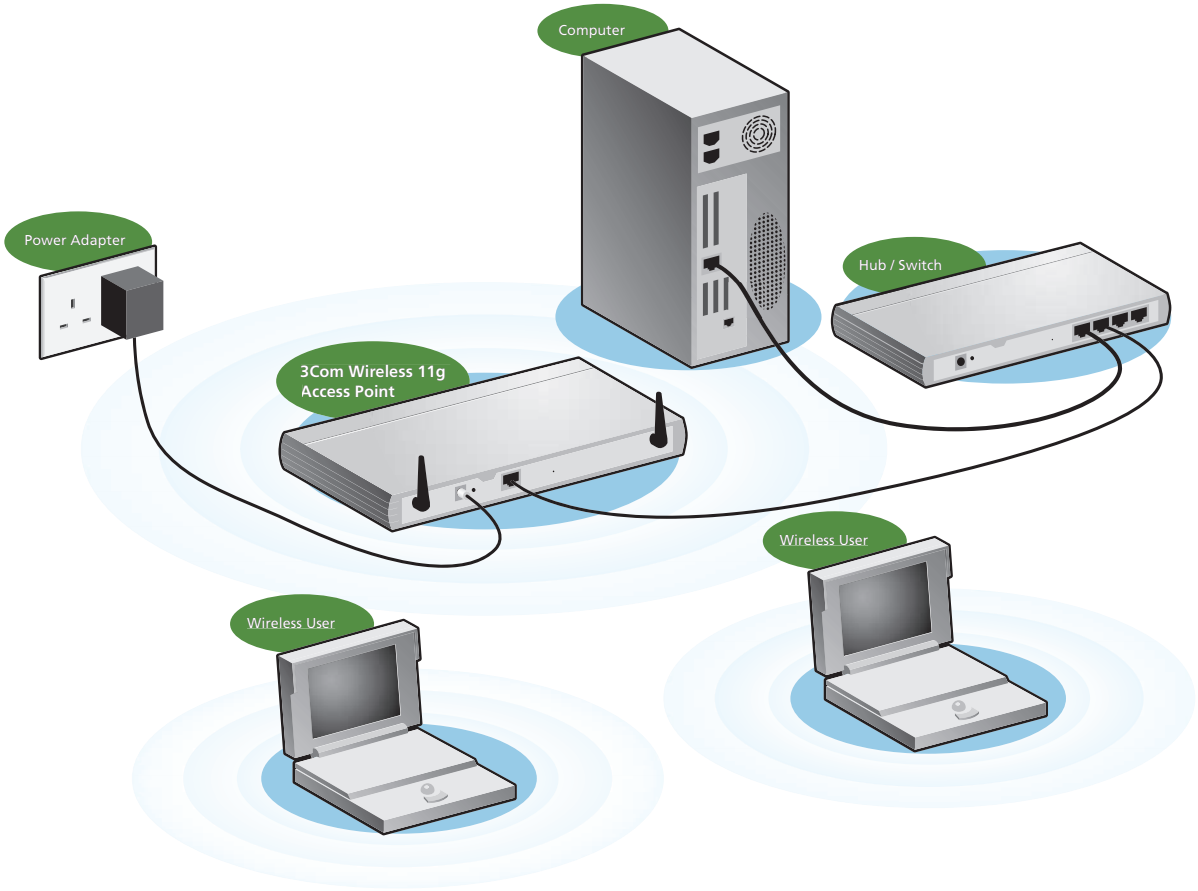
The products that compose the OfficeConnect range give you, the small office user, the same power, flexibility, and protection that has been available only to large corporations. Now, you can harness the benefits of wireless networking.

OfficeConnect Wireless 11g Access Point

The OfficeConnect Wireless 11g Access Point is designed to provide a cost-effective means of connecting wired and wireless networks.

A single Access Point makes the Internet, e-mail and network resources, such as printers, available to dozens of wireless clients. Because the Access Point is a WI-FI certified device, you can be sure it will work reliably with certified equipment from other manufacturers.

Figure 1 Example Network



Access Point Advantages

The advantages of the Access Point include:

- 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)
- Shares network resources between both wired and wireless computers
- Operates as either:
  - an Access Point (providing networking for wireless clients)
  - a Client Bridge (providing access to a wireless network for a single client)
- Support for Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access® (WPA) encryption methods.

Package Contents

The Access Point kit includes the following items:

- One OfficeConnect Wireless 11g Access Point
- One power adapter for use with the Access Point
- Four rubber feet
- One Ethernet cable
- One CD-ROM containing the Access Point Discovery program and this User Guide
- Installation Guide
- One Support and Safety Information Sheet
- One Warranty Flyer

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

Minimum System and Component Requirements

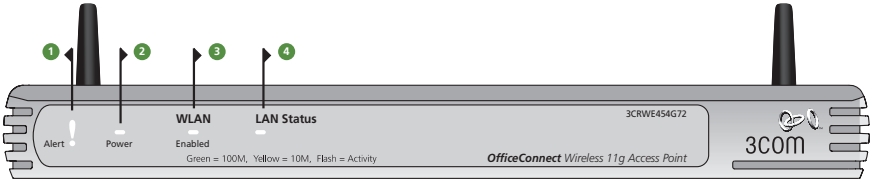
Your Access Point requires that the computer(s) and components in your network be configured with at least the following:

- A computer with an operating system that supports TCP/IP networking protocols (for example Windows 95/98/NT/Me/2000/XP, Unix, Mac OS 8.5 or higher).
- An Ethernet 10Mbps or 10/100 Mbps or 10/100/1000 Mbps NIC.
- An 802.11b or 802.11g wireless NIC.
- A Web browser program that supports JavaScript, such as Netscape 4.7 or higher, Internet Explorer 5.0 or higher, or Mozilla 1.2.1 or higher.

Front Panel

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

Figure 2 Access Point - Front Panel



1 Alert LED

Orange

Indicates a number of different conditions, as described below.

Off - The Access Point is operating normally.

Flashing quickly - Indicates one of the following conditions:

- The Access Point has just been started up and is running a self-test routine, or
- The administrator has invoked the *Reset to Factory Defaults* command, or
- The system software is in the process of being upgraded

In each of these cases, wait until the Access Point has completed the current operation and the alert LED is Off.

Flashing slowly - The Access Point has completed the *Reset to Factory Defaults* process, and is waiting for you to release the reset button. The Access Point will then enter the start-up sequence and resume normal operation.

If you have used the reset button to reset the unit to Factory Defaults, follow steps 5 to 6 in "Forgotten Password and Reset to Factory Defaults" *on* page 66.

Continuously on - A fault has been detected with your Access Point during the start-up process. Refer to Chapter 6 "Troubleshooting".

2 Power LED

Green

Indicates that the Access Point is powered on.

3 LAN Status LED

Green (100Mbps link) / yellow (10Mbps link)

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, 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.

4 Wireless LAN (WLAN) Status LED

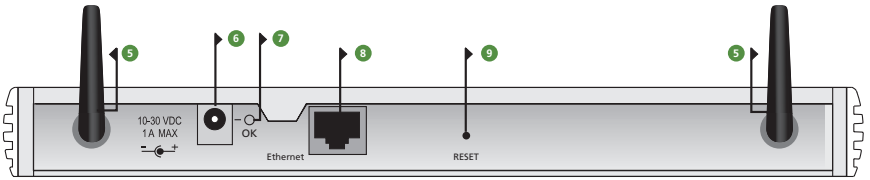
Yellow

If the LED is on it indicates that wireless networking is enabled. If the LED is flashing, data is being transmitted or received. If the LED is off, the Wireless LAN has been disabled in the Access Point, or there is a problem. Refer to Chapter 6 "Troubleshooting".

Rear Panel

The rear panel (Figure 3) of the Access Point contains one LAN port, a reset button, a power adapter OK LED and a power adapter socket.

Figure 3 Access Point - Rear Panel



5 Wireless Antennae

The antennae on the product should be placed in a 'V' position when initially installed.

CAUTION: *Do not force the antennae round further than 90 degrees in either direction.*

6 Power Adapter Socket

Only use the power adapter supplied with this Access Point. Do not use any other adapter.

7 Power Adapter OK LED

Green

Indicates that the power adapter is supplying Power to the Access Point. If the LED is off, there may be a problem with the power adapter or adapter cable.

8 Ethernet Port

Use the supplied patch cable to connect the Access Point to the LAN. The port will automatically adjust to the correct speed and duplex.

9 Reset Button

This button allows you to reset the unit to factory defaults.

2 HARDWARE INSTALLATION

Introduction

This chapter will guide you through a basic installation of the Access Point, including:

- Connecting the Access Point to your network.
- Setting up your computers for networking with the Access Point.

Safety Information

WARNING: *Please read the "Safety Information" section in Appendix D before you start.*

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

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

Positioning the Access Point

You should place the Access Point in a location that:

- allows convenient connection to the computer or other ethernet device that will be connected to the LAN port on the rear panel.
- allows easy viewing of the front panel LED indicator lights, and access to the rear panel connectors, if necessary.
- is centrally located to the wireless computers that will connect to the Access Point. 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.

When positioning your Access Point, ensure:

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

Using the Rubber Feet

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

Wall Mounting

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

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

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

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

CAUTION: *Only wall mount single units, do not wall mount stacked units.*

Powering Up the Access Point

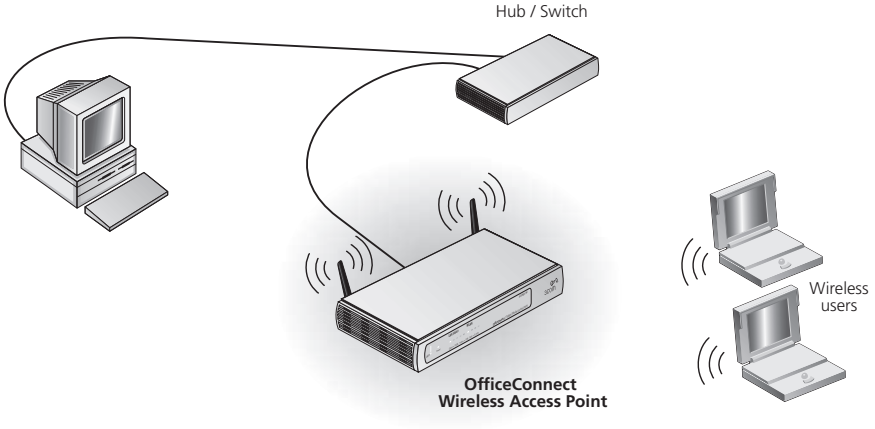
To power up the Access Point:

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

Connecting the Access Point

The first step for installing your Access Point is to physically connect it to a switch or hub. See Figure 4.

Figure 4 Connecting the Access Point



To use your Access Point to connect to the wireless LAN to the wired LAN:

1. Insert one end of the supplied Ethernet (RJ-45 Category 5) cable into the LAN port on the rear panel of the Access Point.
2. Insert the other end of the cable into the RJ-45 port on switch or hub. Check that the LAN status LED lights on the Access Point.

You have now completed the hardware installation of your Access Point. Next you need to set up your computers so that they connect to the Access Point.

3 RUNNING THE SETUP WIZARD

Accessing the Wizard

3Com recommends that you perform the initial Access Point configuration from a computer that is directly connected to the LAN port and not from a wireless connection.

However, you may configure the Access Point from a wireless admin computer but, note that you may lose contact with the Access Point if you change the wireless configuration. To communicate with the Access Point, your wireless NIC should be set as follows:

- Encryption — none
- Service Area Name/SSID — 3Com

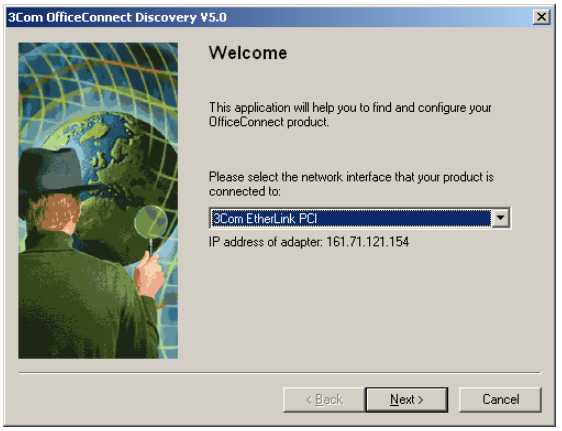
The Access Point setup program is Web-based, which means that it is accessed through your Web browser (Netscape Navigator, Internet Explorer or Mozilla).

To use the Setup Wizard:

1. Ensure that you have at least one computer connected to the Access Point. Refer to Chapter 2 for details on how to do this.
2. Insert the Access Point CD-ROM in the CD-ROM drive on your computer. A menu will appear; select *Discovery*.

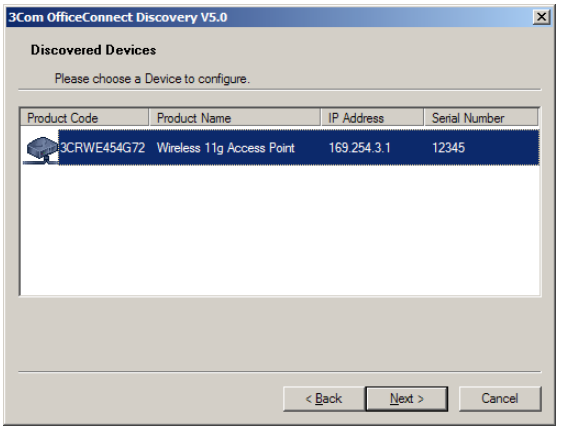
Discovery will find the Access Point even if it is unconfigured or misconfigured.

Figure 5 Discovery Welcome Screen



3 When the *Welcome* screen is displayed, select the NIC from which the Access Point will be discovered. Then click on *Next* and wait until the application discovers the Access Points connected to your LAN.

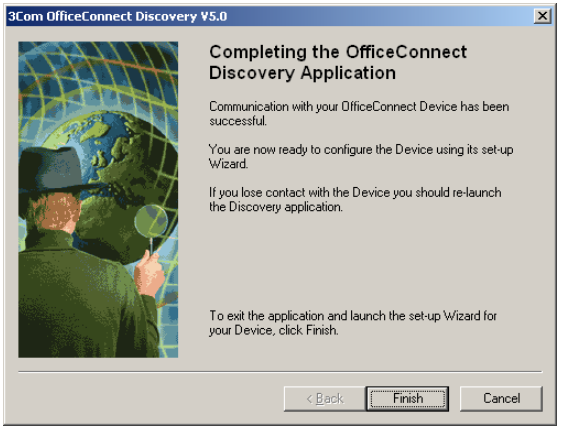
Figure 6 Discovered Access Point Screen



4 Figure 6 shows an example Discovered Devices screen. Highlight the *Wireless 11g Access Point* by clicking on it, and press *Next*.

If the discovery application finds multiple Access Points compare the serial number on the Discovered Devices Screen with the serial number on the base of your Access Point.

Figure 7 Discovery Finish Screen



5 Click on *Finish* to launch a web browser and display the login page for the Access Point as shown in Figure 8.

6 To log in, enter the password (the default setting is **`admin`**) in the *System Password* field and click *Log in* (Figure 8).

Figure 8 Access Point Login Screen

7 If the password is correct, the *Country & Mode Selection* screen appears. (Figure 9)

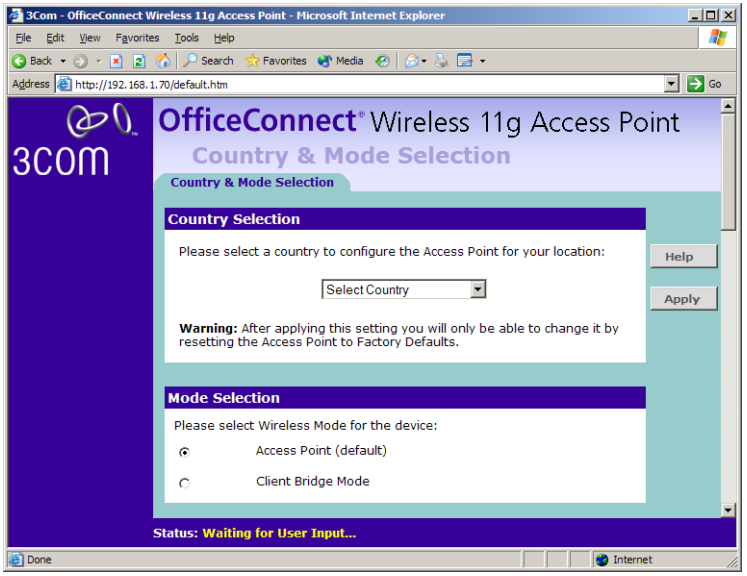
a Select the country in which the Access Point is to operate.

b Select the wireless mode for the Access point:

- Select *Access Point (default)* if the Access Point is to be used to provide networking for wireless clients. See Chapter 4 for configuration information.
- Select *Client Bridge Mode* if the Access Point is to be used to provide access to a wireless network for a single client. See Chapter 5 for configuration information.

The Country & Mode Selection *screen is only displayed on initial configuration of the Access Point.*

Figure 9 Country Selection Screen



8 When you have logged in and selected a country and operating mode either:

- The *Welcome* screen will appear (Figure 10). Select the *Wizard* tab and click *Wizard.*

  or

- If your Access Point has not been configured before, the Wizard will launch automatically (refer to Figure 11).

9 Click *Next*.

10 You will be guided step by step through a basic setup procedure.

Figure 10 Welcome Screen

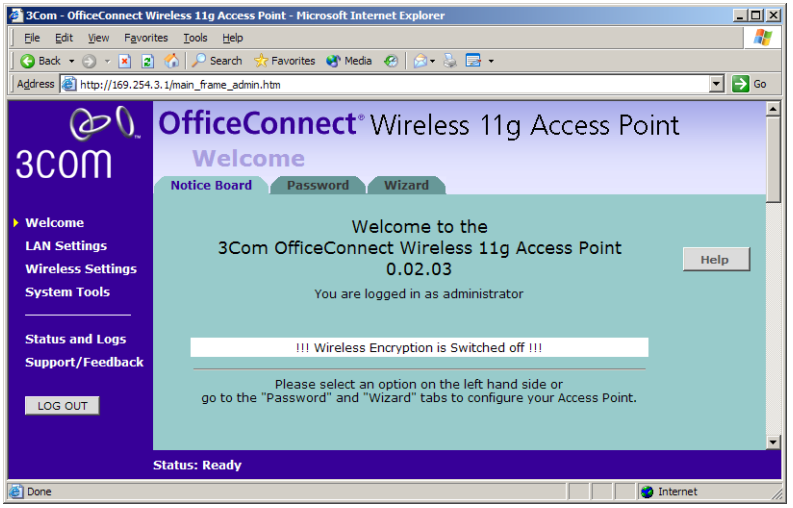
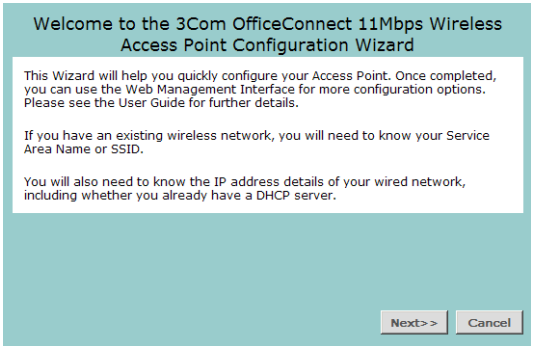
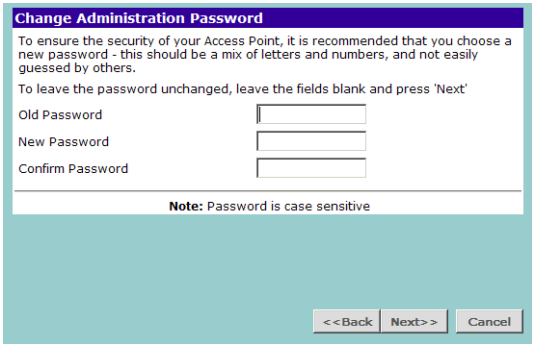


Figure 11 Wizard Screen



Password

Figure 12 Change Administration Password Screen



When the *Change Administration Password* screen (Figure 12) appears, type the *Old Password*, then a new password in both the *New Password* and *Confirm Password* boxes.

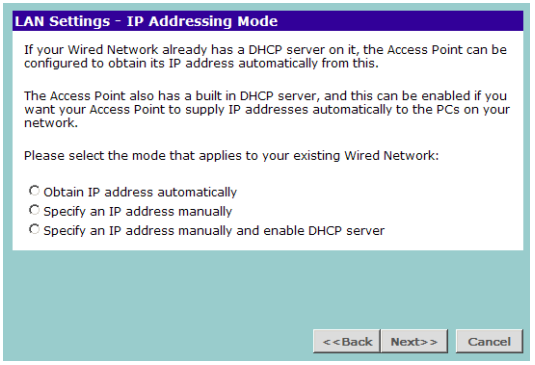
3Com recommends entering a new password when setting up the Access Point for the first time. The Access Point is shipped from the factory with a default password, **`admin`**.

1. *Password is case sensitive.*
2. *Write the new password down and keep it in a safe place, so that you can change your settings in the future.*

Click *Next*.

LAN Settings

Figure 13 LAN Settings Screen



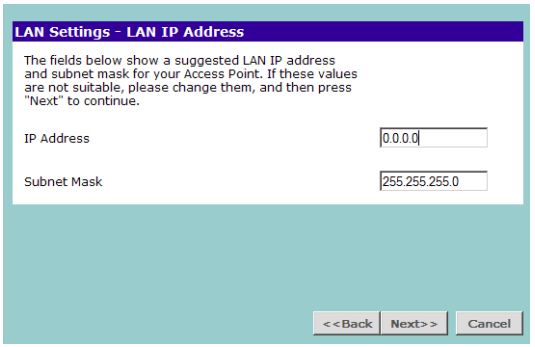
This screen determines how the Access Point obtains its IP address. There are three options.

Obtain IP Address automatically - The Access Point will obtain an IP address from a DHCP server already operating on your network.

Specify an IP address manually - Select this option to manually configure the IP address of the Access Point. The screen shown in Figure 14 is displayed. This screen displays a suggested LAN IP address and subnet mask of the Access Point. It also allows you to change the IP address and subnet mask.

3Com recommends that you manually assign your Access Point a static IP address.

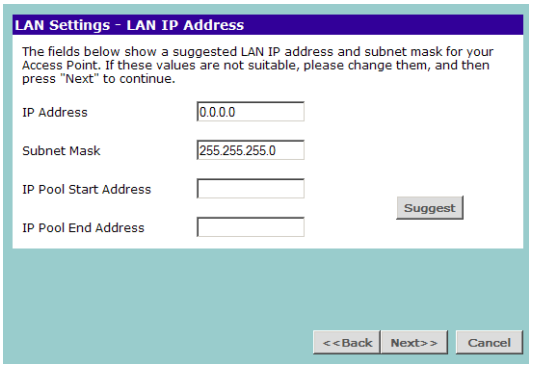
Figure 14 LAN IP Address Screen



Specify an IP address manually and enable DHCP server - The Access Point contains a Dynamic Host Configuration (DHCP) server that can automatically configure the TCP/IP settings of every computer on your network.

To activate the DHCP Server option, select *Specify an IP Address manually and Enable DHCP server.* The screen shown in Figure 15 opens.

Figure 15 DHCP Server Setup Screen



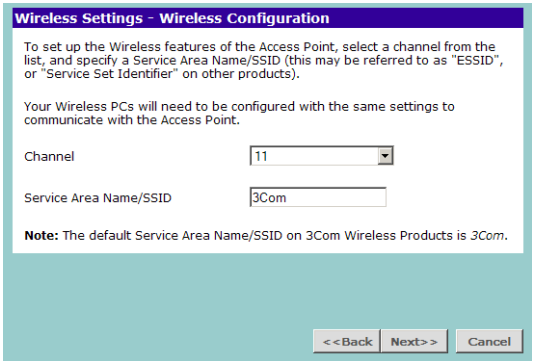
This screen displays a suggested LAN IP address and subnet mask of the Access Point. It also allows you to change the IP address and subnet mask.

Two further fields are available for you to enter the *Start* address of an address pool and an *End* address. The largest available continuous IP pool will be automatically entered; if this is not appropriate, make your required changes.

Before enabling the DHCP Server, ensure that there are no other DHCP servers running on your network.

Wireless Settings

Figure 16 Wireless Configuration Screen



This screen displays the current *Channel* and *Service Area Name*. It also allows you to change these settings. There are a maximum of 14 channels,

the number available to you is dependent on the country in which you reside.

1. Select a channel for the Access Point to use or Clear Channel Select if you want the Access Point to choose an unused channel on start-up.
2. Enter a Service Area Name/SSID.

   The *Service Area Name* default for 3Com products is "3Com". Up to 32 (case sensitive) characters can be entered for the *Service Area Name*.

   3Com strongly recommends that you change the *SSID* to something other than the default.

For information on improving your Wireless network security see "Wireless Settings" *on* page 39.

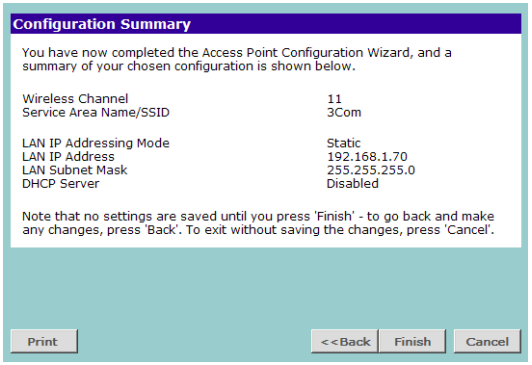
If you are configuring the Access Point from a wireless computer any changes you make to the wireless configuration will result in communication between the Access Point and your computer being lost. This is why 3Com strongly recommends that you configure the Access Point from a wired computer.

It is very important that you set up your wireless clients to use the same Service Area Name or SSID as the one you use on this screen. If your clients use a different Service Area Name then they will not be able to communicate with the Access Point.

The choice of channel is less important as Clients will generally search all of the available channels. You should however make a note of the channel you select as this may be useful if you experience problems with your clients.

Summary

Figure 17 Configuration Summary Screen



When you complete the Setup Wizard, a configuration summary will display. Verify the configuration information of the Access Point and then click *Finish* to save your settings. 3Com recommends that you print this page for your records.

If you have made changes to the LAN Settings or wireless configuration options, you may need to reconfigure the computer you are using in order to make contact with the Access Point again.

Your Access Point is now configured and ready for use.

See Chapter 4 for a detailed description of the Access Point configuration screens.

See Chapter 5 for a detailed description of the Client Bridge Mode configuration screens.

4 ACCESS POINT CONFIGURATION

Navigating Through the Access Point Configuration Pages

This chapter describes all the screens available through the Access Point configuration pages, and is provided as a reference. To get to the configuration pages, browse to the Access Point by entering the URL in the location bar of your browser. The URL is **`http://<IP Address of the Access Point>`**, for example **`http://192.168.1.1`**. When you have browsed to the Access Point, log in using your system password (default **`admin`**).

If your Access Point is set up in Client Bridge Mode*, see* Chapter 5 *to configure your Access Point.*

Main Menu

At the left side of all screens is a main menu, as shown in Figure 18 on page 32. When you click on a topic from the main menu, that page will appear in the main part of the screen.

- Welcome - displays the firmware version of the Access Point, allows you to change your password, and launch the Wizard
- LAN Settings - allows you to configure IP address and subnet mask information, setup DHCP server parameters, and display the DHCP client list.
- Wireless Settings - enables /disables access from wireless computers, and provides facilities for improving the security of the wireless network.
- System Tools - allows the administrator to perform maintenance activities on the Access Point.
- Status and Logs - displays the current status and activity logs of the Access Point.
- Support - contains a comprehensive online help system

Option Tabs

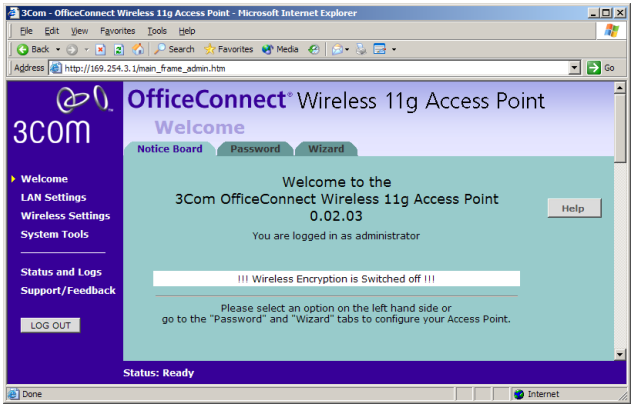
Each corresponding menu page may also provide sub-sections which are accessed through the use of tabs (see Figure 18 for example). To access a sub-section, simply click on the required tab.

Getting Help

On every screen, a Help button is available which provides access to the context-sensitive online help system. Click *Help* for further assistance and guidance relating to the current screen.

Welcome Screen

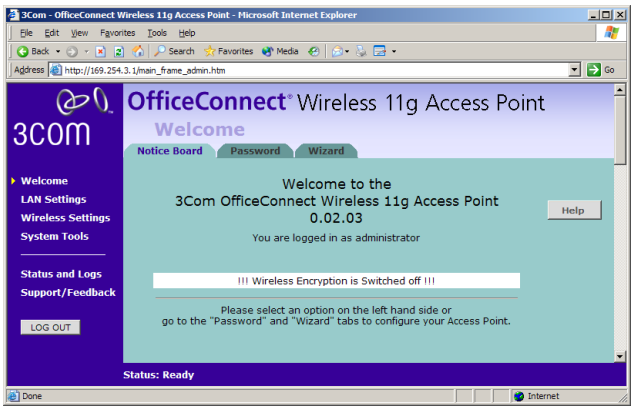
Figure 18 Access Point Welcome Screen



The *Welcome* section allows you to view the Notice board and to change your Password. You can also gain access to the Configuration Wizard. (See "Accessing the Wizard" on page 21 for details).

Notice Board

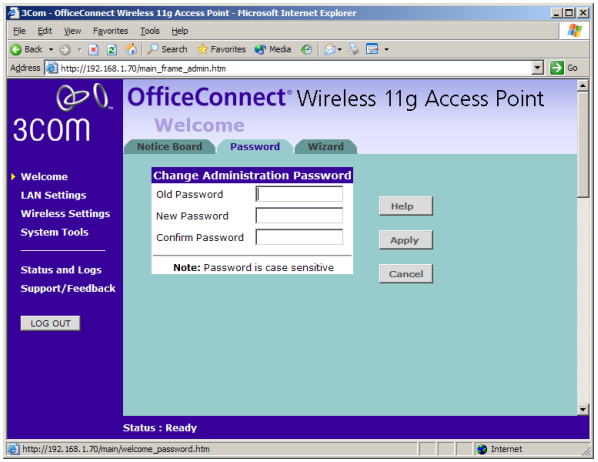
Figure 19 Notice Board Screen



The Notice Board is used to display configuration warning messages.

Password

Figure 20 Password Screen



Changing the Administration Password

You can change the password to prevent unauthorized access to the Administration System. To do this:

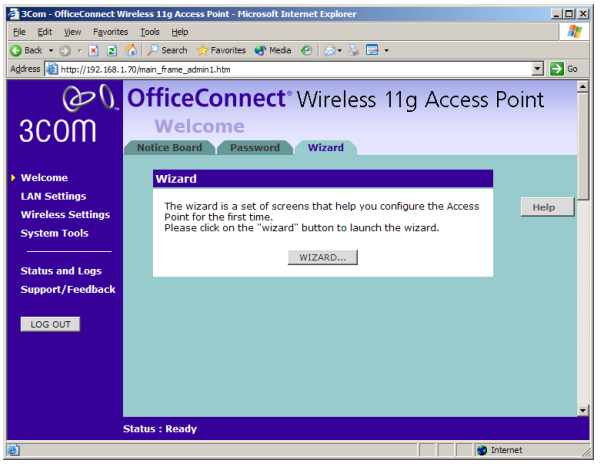
1. Enter the current password in the *Old Password* field
2. Enter the new password in the *New Password* field
3. Enter the new password again in the *Confirm Password* field
4. Click *Apply* to save the new password

The password is case sensitive.

If you have forgotten your password you need to reset the Access Point. See "Forgotten Password and Reset to Factory Defaults" on page 66

Wizard

Figure 21 Wizard Screen



Click *WIZARD...* to launch the configuration wizard. Refer to Chapter 3 for information on how to run the wizard.

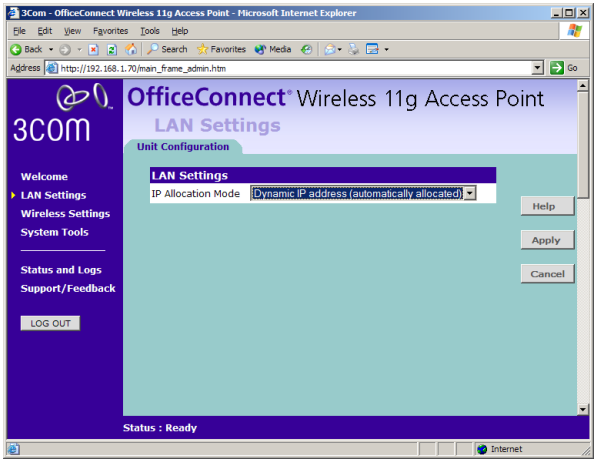
LAN Settings

The LAN Settings menu provides the following options:

Unit Configuration

The LAN Settings screen is used to determine how the LAN IP address of your Access Point is obtained. It can be obtained automatically or you can manually configure the IP address and optionally configure the DHCP server.

Figure 22 Unit Configuration Screen



Dynamic IP Address

3Com recommends that you manually assign your Access Point a static IP address.

Select *Dynamic IP Address (automatically allocated)* and the screen shown in Figure 22 is displayed. Check all your settings and click *Apply*.

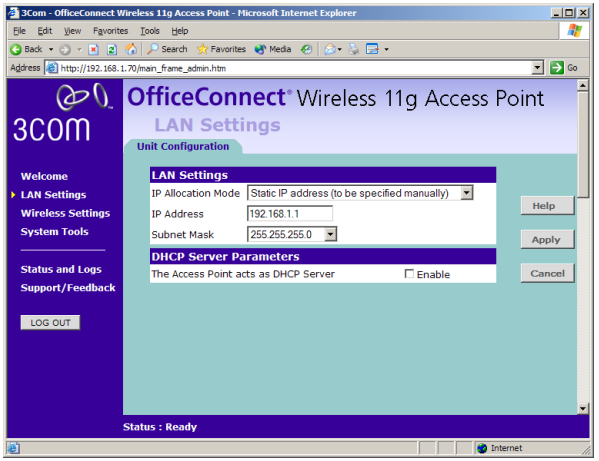
If the Access Point is set to obtain an IP address automatically and is unable to contact a DHCP server then it will allocate itself an address in the 169.254.xxx.xxx range.

Manually setting the IP address

3Com recommends that you assign your Access Point a static IP address.

1 Select *Unit Configuration* and then select *Static IP Address (to be specified manually)*. The screen shown in Figure 23 is displayed.

Figure 23 Unit Configuration Screen For Static IP Address



2 Enter the Access Point *IP Address* and *Subnet Mask* in the LAN Settings field. The default static IP address of the Access Point is 192.168.1.1.

3 If you want to use the Access Point as a DHCP Server, click in the *Enable* check box. See "DHCP Server" for more information about configuring the DHCP server.

4 Check all of your settings, and then click *Apply*.

DHCP Server

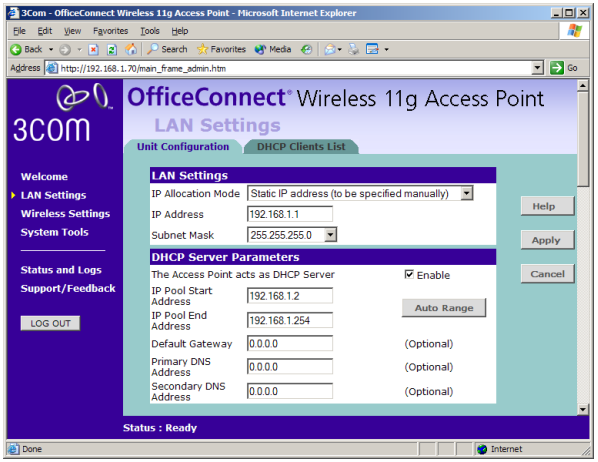
The DHCP server will give out addresses to both wired and wireless clients.

Before enabling the DHCP Server, ensure that there are no other DHCP servers running on your network.

If you want the Access Point to function as a DHCP server on your network, carry out the following:

1. Select *Unit Configuration* and then select *Static IP Address (to be specified manually)*. The screen shown in Figure 23 is displayed.
2. Enter the IP address details as described in "Manually setting the IP address" and click *Enable* against *The Access Point acts as a DHCP Server*. The screen shown in Figure 24 is displayed.

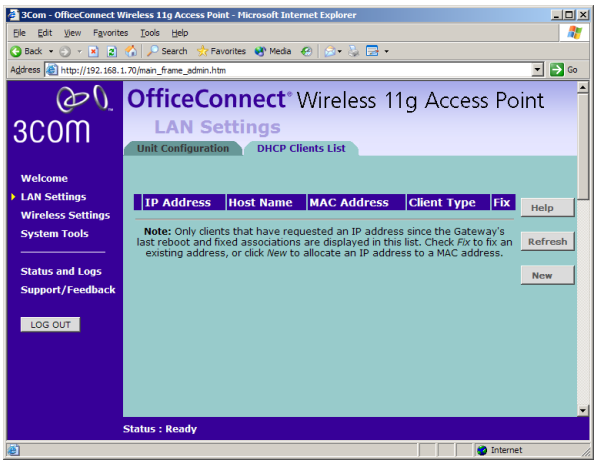
Figure 24 DHCP Server Configuration Screen



3. Clicking *Auto Range* automatically selects the largest range of addresses available for your network. Alternatively you can manually enter *Start* and *End* addresses for the IP address pool. The DHCP server supports up to a maximum of 253 addresses.
4. Enter any *Default Gateway* and *DNS* (Domain Name Server) addresses if required.
5. Check your settings and click *Apply*.

DHCP Clients List

Figure 25 DHCP Clients List Screen



The DHCP Clients List provides details on the devices that are connected to the LAN. The list is only created when the Access Point is set up as a DHCP server. For each device that is connected to the LAN the following information is displayed:

- IP address — The Internet Protocol (IP) address issued to the client machine.
- Host Name — The client machine's host name, if configured.
- MAC Address — The Media Access Control (MAC) address of the client's network card.
- Client Type — Whether the client is connected to the access point by wired or wireless connection.
- Fix — This box is checked if the IP address is fixed to the MAC address of the client's network card. Clients that have fixed addresses will get the same IP address each time they connect.

As you connect more devices, the client list will grow to a maximum number of 253 clients.

The *Release* button allows the lease time for the IP address that has been issued to a device to be cleared. The lease time is set at 12 hours. If a PC has been switched off, using the *Release* button would allow the 12 hour lease time to be cleared. The IP address would then be available for another device if there were no other IP addresses available.

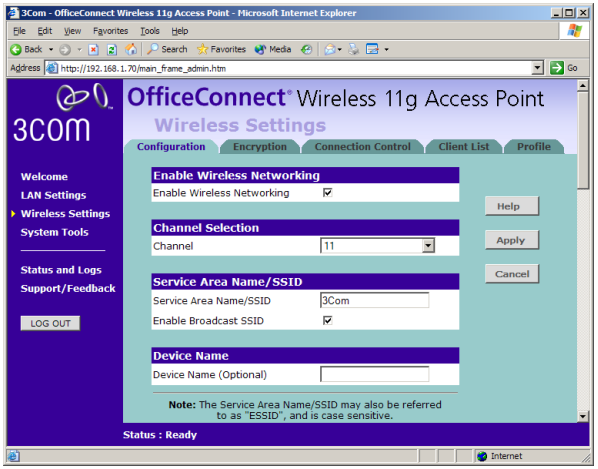
Wireless Settings

To improve the security of your wireless network, 3Com recommends that you:

1. *Change the SSID from its default value - see* page 40
2. *Enable Encryption - see* page 41
3. *Enable Connection Control - see* page 44

Configuration

Figure 26 Configuration Screen



Enable Wireless Networking

Allows you to enable/disable the wireless section of your LAN. When disabled, no wireless PCs can gain access to your Wired or Wireless LAN through this Access Point.

Channel Selection

The Channel Selector allows you to specify which channel the Access Point will transmit and receive on. If another Access Point nearby is using the same channel as you, there will be a reduction in the performance of your network. If this seems to be the case, you should select a different channel number. Usually the Wireless computers will scan to find the correct channel, but if they don't you must configure them to use the same channel number as the Access Point.

Valid channels are country dependent. See "Channels" on page 97 *for a list of channels approved by each country.*

Clear Channel Select allows the Access Point to automatically select an available channel when first powered on.

Service Area Name/SSID

This allows you to name your Wireless network. The field will accept any alphanumeric string and has a maximum length of 32 characters. Your Wireless computers must be configured with exactly the same name or you will not be able to establish a connection. The Service Area Name may also be referred to as "ESSID" depending on your networking vendor. By default the Access Point uses the name "3Com". 3Com recommends that you change the default name.

In order that your wireless computers can connect to the Access Point, you must:

- *Use Infrastructure Mode not Adhoc Mode.*
- *Have the same Service Area Name as the Access Point.*
- *Use the same encryption type and keys as the Access Point.*
- *Ensure that the PC is included in the authorized Wireless PCs list if Connection Control is enabled. See* page 44.

Disable Broadcast SSID

This feature can be used to improve the security of your wireless network. When the tickbox is checked, the Access Point will not broadcast the Service Area Name/SSID of your wireless network. This will prevent unauthorized clients from detecting your SSID and attempting to connect to your network.

If you have a wireless client that can detect all the available SSIDs in your area, your client will not list the Access Point SSID when this feature is enabled.

3Com recommends that you install your wireless network with this feature disabled and then enable it once you have set up the Access Point and wireless clients.

If you set the Access Point to Disable Broadcast SSID, *the Access Point will not allow access to clients with the SSID field set to "*any*".*

Access Point Name

This option allows you to name the Access Point. The field accepts any alphanumeric string upto a maximum of 32 characters. This option is useful if you have several Access Point units and want to be able to easily identify them. For example, you may name them *Marketing*, *Research*, *Admin*.

Encryption

When setting up wireless networks, it is important to remember that with encryption disabled, anyone with a Wireless PC can eavesdrop on your network. 3Com recommends that you get the network working with encryption disabled first and then enable it as the last step. This will simplify setting up your network.

The Access Point supports two types of encryption:

- WPA — Wi-FI Protected Access (WPA) is a 256 bit encryption method with keys that change over time.
- WEP — Wireless Equivalent Privacy (WEP) is a 64 bit or 128 bit encryption method with user configurable fixed keys.

WPA provides a higher level of security, provided by its longer key and dynamic changes made to the key over time. 3Com recommends that you use WPA with any clients which support it.

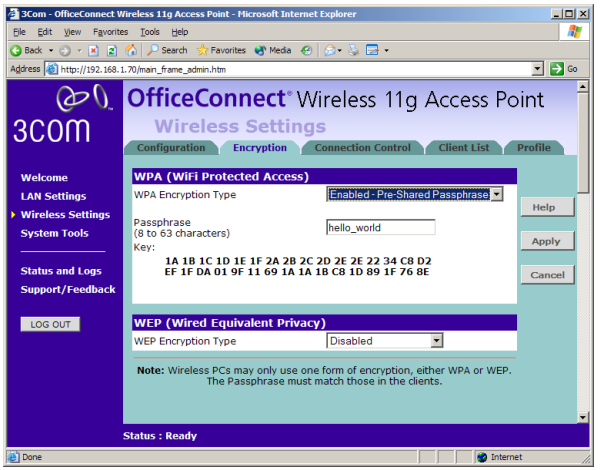
If you enable encryption on the Access Point, you must reconfigure your wireless PCs to use exactly the same Encryption Type and Keys otherwise the devices will not understand each other.

The encryption methods used by the Access Point secure data transmitted through wireless communications between the Access Point and its wireless clients. Enabling encryption has no security effect on data transmitted through wired (Ethernet) connections or through your connections to the Internet.

Configuring WPA Encryption

The only configuration that is needed for WPA is to enter the pre-shared key. This key is used to start the dialog between the Access Point and the client. During this dialog, a new key is agreed, making it more difficult to eavesdrop on wireless networks encrypted using WPA, than those encrypted using WEP. The pre-shared key can be entered as a 256 bit series of hexadecimal digits or as a pass-phrase.

Figure 27 Encryption Keys Screen showing WPA configuration



To enter the pre-shared key as hexadecimal digits:

1. Select *Enabled - Manual Pre-shared Key* from the *WPA Encryption Type* drop-down box.
2. Enter a pair of hexadecimal digits in each of the 32 *Key* fields. Each field can contain a hexadecimal number from 00 to ff, for example 1a.
3. Click *Apply* to generate the key.

To enter the pre-shared key as a pass-phrase:

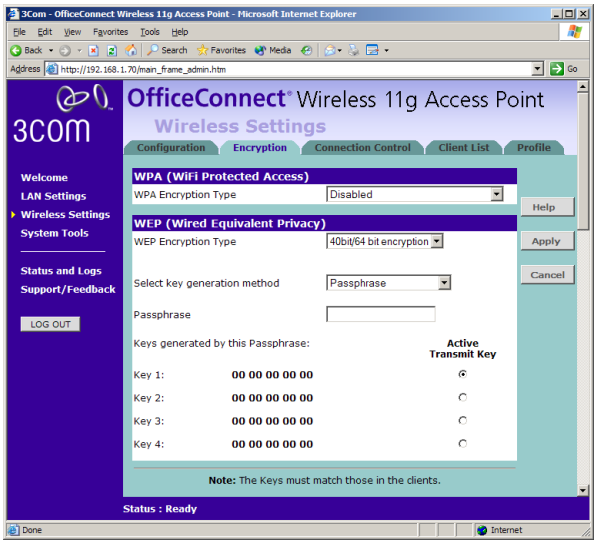
1. Select *Enabled - Pre-Shared Passphrase* from the *WPA Encryption Type* drop-down box.
2. Enter a phrase of between 8 and 63 characters in length in the *Passphrase* field. This passphrase will be used to generate a 256 bit key.
3. Click *Apply* to generate the key.

Configuring WEP Encryption

There are two levels of WEP encryption available, 64 bit (sometimes referred to as 40 bit) and 128 bit. 128 bit will result in a higher level of security, but may cause a slight decrease in performance. Use the *Wireless Encryption Type* box to select the desired level.

Encryption Keys

Figure 28 Encryption Keys Screen showing WEP configuration



A Key is a hexadecimal (0-9, A-F) number used to encrypt and decrypt the data. There can be up to 4 keys and each key can be as long as 26 digits. The Access Point also offers a number of methods for converting plain text into hex keys. The text is much easier to remember than hex keys but it relies on your wireless adapters also supporting this feature. Different manufacturers have developed different ways of converting plain text and so interoperability is not guaranteed. If you are experiencing difficulty, the Manual Hex Key method is supported by most vendors.

There are four methods available to generate the encryption keys:

- Manual Key Entry - This method allows you to manually enter hex keys. Virtually all manufacturers support this scheme. Enter a two digit hexadecimal number in every box. Hexadecimal numbers are formed from 0-9 and A-F.
- 3Com Encryption String - This method is supported by 3Com Wireless products. The string can contain any alphanumeric characters and must be between 6 and 30 characters long. A single string will automatically generate 4 unique keys for 64 or 128 bit WEP.
- ASCII - This method is supported by some adapter cards running under Windows XP. The string must be exactly 5 characters for 64 bit

WEP and 13 characters for 128 bit WEP. You must enter a separate string for each of the 4 Keys. You can leave a string blank provided this Key is not selected as the Active Transmit Key.

- Passphrase - This is another common method and similar to the 3Com Encryption string. In 64 bit WEP, the passphrase will generate 4 different keys. However, in 128 bit WEP, this method only generates 1 key which is replicated for all 4 keys. The passphrase can be up to 31 characters long and may contain any alphanumeric characters.

Select from the drop down list the key generation method you wish to use. If you have other wireless products choose the scheme that is compatible with these, then enter the appropriate information.

If you encounter any difficulty when you enable WEP ensure that you check that each key on your wireless computer is exactly the same as each key on your Access Point. In other words, Key number 1 on the Wireless computer must have the same Hex number as Key number 1 on the Access Point, Key 2 on the Wireless computer must match Key 2 on the Access Point and so on.

The *Active Transmit Key* selects which of the 4 Keys the Access Point uses when it transmits. You can change the selected key periodically to increase the security of your network.

Some wireless adapters have only one key available on their WEP configuration page. If this is the case ensure it is the same as Key 1 on the Access Point and that it is selected as the active transmit key.

Connection Control

This screen allows you to determine if all Wireless PCs or just authorised Wireless PCs can use the Access Point. Select Connection Control to display the screen shown in Figure 29.

Figure 29 Connection Control Screen

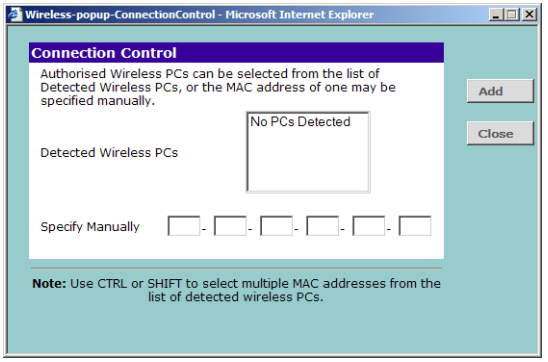
A higher level of security can be achieved for your wireless network if you use both encryption and you specify only certain wireless computers can connect to the Access Point. By default, any wireless computer that has the same Service Area Name/SSID, channel and encryption settings as the Access Point can connect to it.

Select *Only Authorised Wireless PCs can connect to the Access Point* to enable and configure this feature.

If you enable this feature from a Wireless PC, it will automatically be added to the Authorised Wireless PC list.

Authorised Wireless PCs

Figure 30 Connection Control Detail Screen



To create a list of Wireless computers that can access the Access Point:

1 Press *New*. The screen shown in Figure 30 opens.

2 Select one or more MAC addresses of the Wireless PCs that you want to allow to connect to the Access Point.

To select multiple MAC addresses, hold down the Ctrl *key while clicking on the addresses.*

3 Click *Add*.

The list on the Connection Control *window contains the MAC addresses of all Wireless PCs that are in range, currently operating, and have the same Service Area Name/SSID, channel and encryption settings as the Access Point. You will find this screen easier to use if you set up and make a note of all of your wireless PCs on your network first. You may also add the entries manually if you know the MAC address.*

To add a MAC address that is not in the list, enter the MAC address in the appropriate fields. A MAC address consists of 12 characters. Valid characters are '0-9', and 'A-F'.

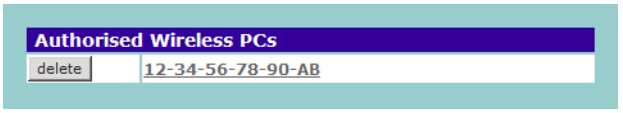
Modifying a MAC Address

1 Click on the MAC address to be modified in the table (Figure 31).

2 Modify the MAC address in the pop-up window. The MAC address can only be edited manually.

3 Press *Apply* to accept the changes.

Figure 31 MAC Address Table



Click Close *to discard all changes.*

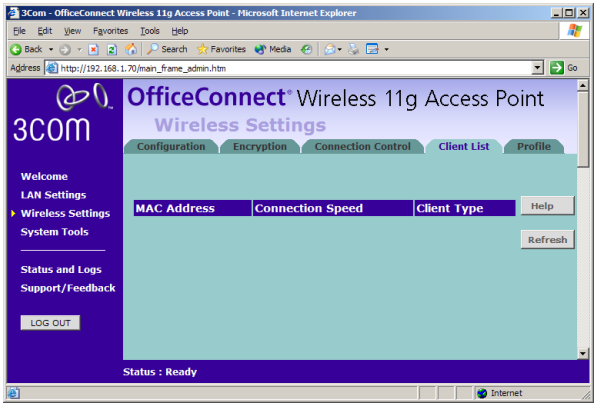
Deleting a MAC Address

The connection rights for a Wireless PC listed in the table can be removed by pressing *Delete* for that entry in the table.

Once an entry has been deleted it cannot be undone. Please wait 30 seconds for changes to take effect.

Client List

Figure 32 Client List Screen



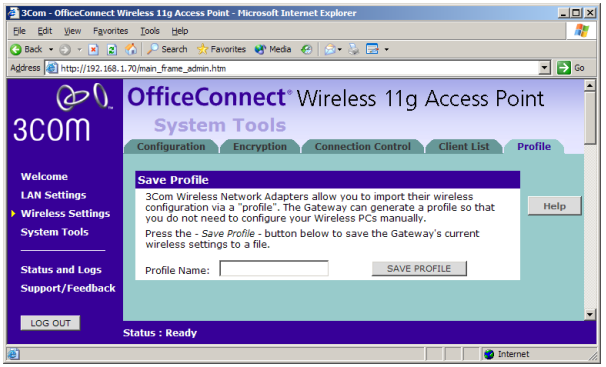
The Wireless Client List provides details on the devices that are connected to the Wireless LAN. The list is only created when Wireless Networking is enabled. For each device that is connected to the Wireless LAN the following information is displayed:

- MAC Address — The Media Access Control (MAC) address of the client's wireless network card.
- Connection Speed — The actual speed of the wireless connection. The speed depends on the specification of the wireless network card, the distance from the Access Point and any items obstructing and interfering with the signal.
- Client Type — The specification of the client's wireless network card.

As you connect more devices to the Wireless LAN, the client list will grow to a maximum of 128 (the maximum number of wireless devices that the Access Point can support).

Profile

Figure 33 Profile Screen



Some 3Com Wireless Network Adapters allow you to import Wireless configurations via a 'profile'. The Access Point can generate a profile so that you do not need to configure your Wireless PCs manually.

The profile contains three items as follows:

- **Service Area Name/SSID of the Access Point**

  This is configured on the *Configuration* tab under the *Wireless Settings* option.

- **Encryption settings from the Access Point**

  This is configured on the *Encryption* tab under the *Wireless Settings* option.

- **Profile Name**

  This is used to identify the profile once it has been imported into the Wireless Network Adapter configuration software.

Saving a Profile

To set up a profile (once the Service Area Name/SSID and Encryption settings have been configured in the Access Point):

1. Enter a Profile Name (up to 25 alphanumeric characters) and then click *Save Profile*.
2. Your browser will then prompt you to enter a file name and folder location in which to save the profile. Once the profile has been saved it can be copied on to another PC and imported into the 3Com Wireless Network Adapter.

For instructions on how to import a profile, refer to the User Guide that accompanies your 3Com Wireless Network Adapter(s).

If, once the profile is imported, the Wireless Network Adapter cannot connect to the Access Point, check that:

- the adapter is within range of the Access Point

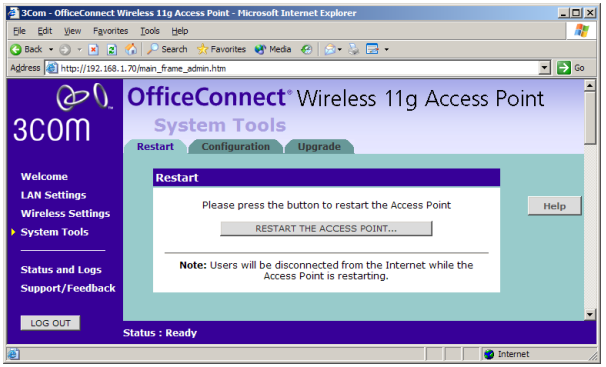
if *Connection Control* has been enabled in the Access Point, the MAC address of the Wireless Network Adapter must be included in the list of authorised Wireless PCs.

System Tools

The main frame of the System Tools screen includes three administration items: *Restart, Configuration,* and *Upgrade* (Figure 34).

Restart

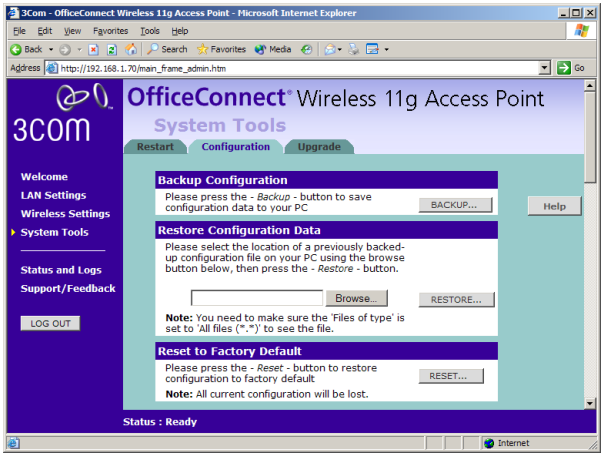
Figure 34 Restart Screen



If your Access Point is not operating correctly, you can choose to restart the Access Point by selecting *Restart the Access Point*, simulating the effect of power cycling the unit. No configuration information will be lost but the log files will be erased. Any network users who are currently connected to the Access Point will have their access interrupted whilst the restart takes place, and they may need to reboot their computers when the restart has completed and the Access Point is operational again.

Configuration

Figure 35 Configuration Screen



Select the *Configuration* tab to display the *Configuration* screen (Figure 35).

Backup Configuration

Click *BACKUP* to save the current Access Point configuration. You will be prompted to download and save a file to disk.

Restore Configuration Data

If you want to reinstate the configuration settings previously saved to a file, press *Browse* to locate the backup file on your computer, and then click *RESTORE* to copy the data into the Access Point's memory.

The password will remain unchanged.

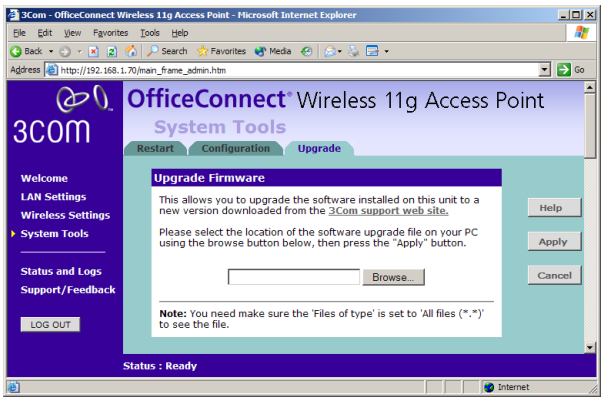
Reset to Factory Default

If you want to reset the settings on your Access Point to those that were loaded at the factory, click *RESET*. You will lose all your configuration changes. The Access Point reverts to a DHCP client and will therefore restart requiring a new IP address. To communicate with the Access Point you may need to rerun the DISCOVERY software to find out the IP address of the Access Point. See Appendix A for more information. You may need to reconfigure and restart your computer to re-establish communication with the Access Point.

Resetting the Access Point to its Factory default settings is the only way to switch between Access Point and Client Bridge modes.

Upgrade

Figure 36 Upgrade Screen

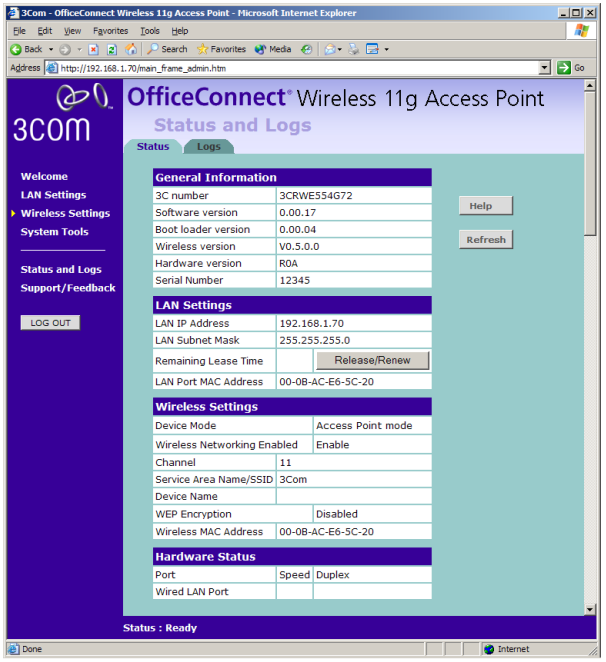


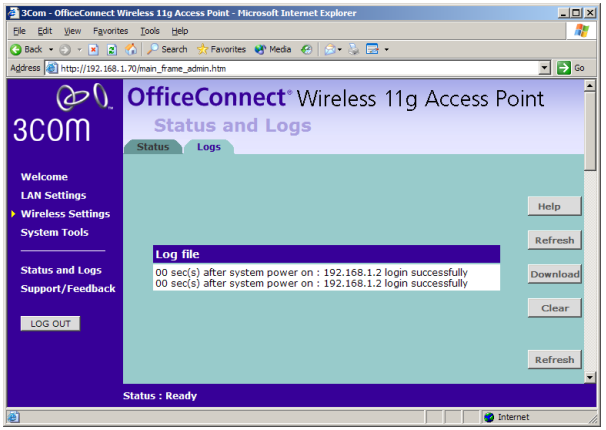
The Upgrade facility allows you to install on the Access Point any new releases of system software that 3Com may make available. To install new software, you first need to download the software from the 3Com support web site to a folder on your computer. Once you have done this, select *Browse* to tell your web browser where this file is on your computer, and then click *Apply*. The file will be copied to the Access Point, and once this has completed, the Access Point will restart. Although the upgrade process has been designed to preserve your configuration settings, it is recommended that you make a backup of the configuration beforehand, in case the upgrade process fails for any reason (for example, the connection between the computer and the Access Point is lost while the new software is being copied to the Access Point).

The upgrade procedure can take up to two minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Access Point during the upgrade procedure; if you do, the software may be corrupted and the Access Point may not start up properly afterwards. If the Alert LED comes on continuously after a failed upgrade, refer to Chapter 6, "Troubleshooting".

Status and Logs

Figure 37 Status and Logs Screen





Selecting *Status and Logs* from the main menu displays the *Status* and *Logs* screens (Figure 37) in your Web browser window. The *Status* screen displays a tabular representation of your network and Internet connection.

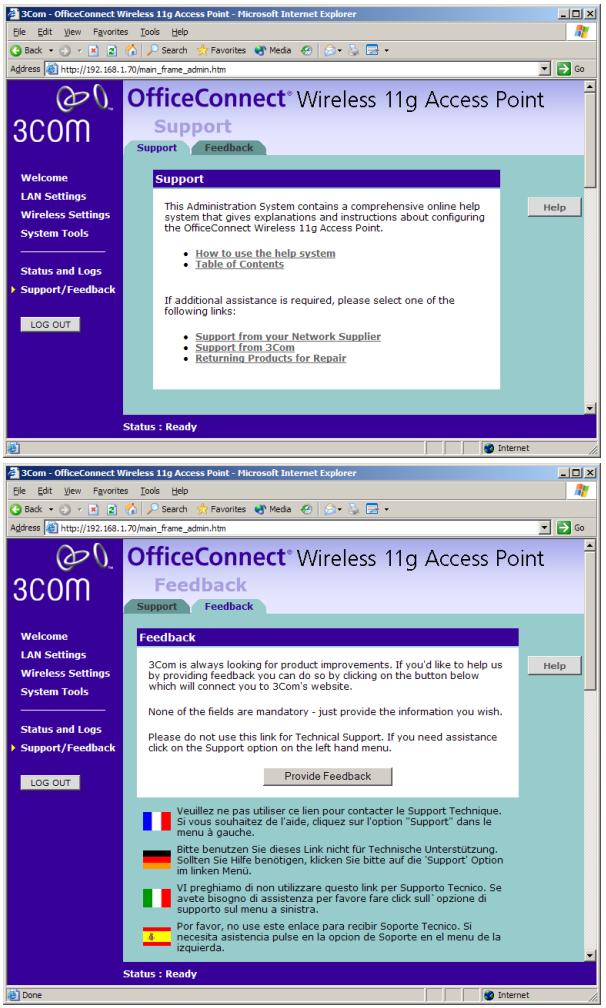
Status Status displays the current unit status, including a summary of the configuration

Logs Logs will allow you to view the events logged by the Access Point

You may be asked to refer to the information on the *Status* and *Logs* screens if you contact your supplier for technical support.

Support and Feedback

Figure 38 Support Screen



Selecting the *Support* tab from the *Support/Feedback* screen displays the support links screen, which contains a list of Internet links that provide information and support concerning the Access Point (Figure 38).

Selecting the Feedback tab from the *Support/Feedback* screen displays the feedback screen, allows you to provide feedback to 3Com on the operation of your Access Point (Figure 38). This screen should not be used to obtain technical support.

5 CLIENT BRIDGE MODE CONFIGURATION

What is Client Bridge Mode?

Client Bridge Mode is a secondary mode of the Access Point. When in Client Bridge Mode the Access point will act as a Wireless client, allowing one computer to access a wireless network. In this mode it will not longer act as an access point and will not provide wireless networking for other clients.

Switching to Client Bridge Mode

To switch your Access Point to Client Bridge mode you must reset the Access Point to its factory default settings.

When you reset the Access Point to its factory default settings you will lose all configuration information. 3Com recommends that backup your configuration before changing the mode of the Access Point.

To switch the Access Point to Client Bridge mode:

1. Click on the *System Tools* menu followed by the *Configuration* tab.
2. Click the *RESET...* button in the *Reset to Factory Default* section.

   The Access Point will restart.

   You may need to use the Discovery Application to reconnect to your Access Point after it has been reset to factory default settings. See Appendix A.
3. When the Country & Mode Selection screen appears, select:
   - **a** The country in which the Access Point is to operate.
   - **b** *Client Bridge Mode* as the operating mode of the Access Point.
4. Click *Apply*.

Configuring Client Bridge Mode

Once the Access Point has been switched into Client Bridge mode, you can configure it using the configuration Wizard or by setting options manually.

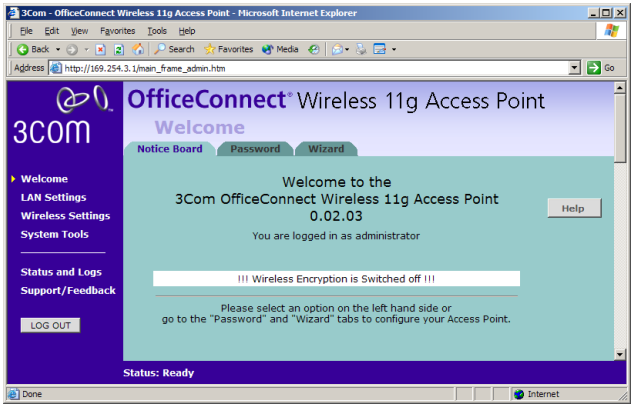
To configure the Access Point using the configuration wizard:

1. Click the *Welcome* menu, followed by the *Wizard* tab.
2. Click the *WIZARD...* button and follow the instructions provide on-screen.

To configure the Access Point manually see the sections in the rest of this chapter.

Welcome Menu

Figure 39 Access Point Welcome Screen



The *Welcome* section allows you to view the Notice board and to change your Password. You can also gain access to the Configuration Wizard. The *Welcome* screens are the same under Access Point mode and Client Bridge mode:

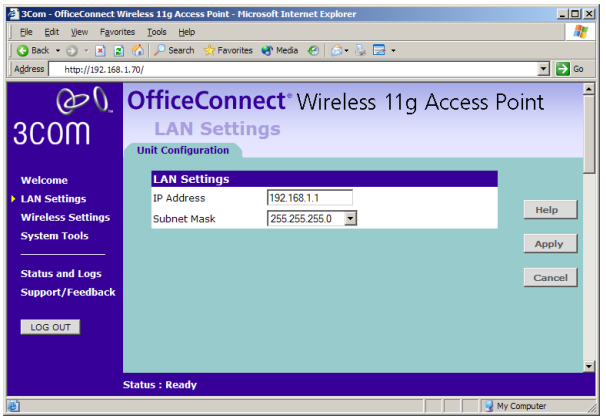
- See "Notice Board" on page 33 for details of the *Notice Board* screen.
- See "Password" on page 33 for details of the *Password* screen.
- See "Wizard" on page 34 for details of the *Wizard* screen.

The configuration wizard will display options relevant to configuring Client Bridge mode and will therefore differ from those shown in Chapter 3.

LAN Settings

The LAN Settings screen allows you to set the IP Address and Subnet Mask of your Access Point.

Figure 40 Unit Configuration Screen



To change the LAN settings for your Access Point:

1. Select *Unit Configuration*. The screen shown in Figure 40 is displayed.
2. Enter an *IP Address* and *Subnet Mask* in the LAN Settings field. The default static IP address of the Access Point is 192.168.1.1.

   You must set a static IP address for your Access Point when in Client Bridge mode. Client Bridge mode does not support DHCP. The Access Point must be allocated a free address within your wireless network's subnet to function correctly.

3. Check all of your settings, and then click *Apply*.

Wireless Settings

The Wireless Settings menu allows to enter the details of the wireless network to which you are connecting. These can be obtained from your network administrator.

Configuration

Figure 41 Configuration Screen

Enable Wireless Networking

Allows you to enable/disable wireless access to your LAN. When disabled, you will not be able to gain access to your Wireless LAN through this Access Point.

Service Area Name/SSID

Enter the name of your wireless network. If you do not enter the name correctly, you will not be able to connect to your wireless network.

Device Name

This option allows you to name the Access Point. The field accepts any alphanumeric string upto a maximum of 32 characters. This option allows your network administrator to identify wireless clients. In Client Bridge mode, Access Points are commonly named after their user or location (if fixed).

Encryption

When setting up wireless networks, it is important to remember that with encryption disabled, anyone with a Wireless PC can eavesdrop on your network. The Access Point supports two types of encryption:

- WPA — Wi-FI Protected Access (WPA) is a 256 bit encryption method with keys that change over time.
- WEP — Wireless Equivalent Privacy (WEP) is a 64 bit or 128 bit encryption method with user configurable fixed keys.

WPA provides a higher level of security, provided by its longer key and dynamic changes made to the key over time. 3Com recommends that you use WPA if supported by your wireless network.

The Access Point can only use one type of encryption to access the wireless network. If you enable WPA, the options for WEP will not be available. If you enable WEP, the options for WPA will not be available.

Figure 42 Encryption Keys Screen

To set up WPA encryption on your Access Point:

1 In the WPA Encryption Type drop-down box select one of the Enabled options:

- Select *Enabled - Manual Pre-shared key* if you have been supplied a set of hexadecimal digits
- Select *Enabled - Pre-shared Passphrase* if you have been suppled with a passphrase

2 Enter the pre-shared key or passphrase in the fields provided.

- For a pre-shared key, enter a pair of hexadecimal digits in each of the 32 *Key* fields, as supplied by your network administrator. Each field can contain a hexadecimal number from 00 to ff, for example 1a.
- For a pre-shared passphrase enter the passphrase in the *Passphrase* field.

3 Click Apply to enter the key.

To set up WEP encryption on your Access Point:

1. In the WEP Encryption Type drop-down box select the strength of the encryption supported by your wireless network.
2. Select the method used to generate the WEP encryption key. There are four methods available:
   - Manual Key Entry - This method allows you to manually enter hex keys. Virtually all manufacturers support this scheme. Enter a two digit hexadecimal number in every box. Hexadecimal numbers are formed from 0-9 and A-F.
   - 3Com Encryption String - This method is supported by 3Com Wireless products. The string can contain any alphanumeric characters and must be between 6 and 30 characters long. A single string will automatically generate 4 unique keys for 64 or 128 bit WEP.
   - ASCII - This method is supported by some adapter cards running under Windows XP. The string must be exactly 5 characters for 64 bit WEP and 13 characters for 128 bit WEP. You must enter a separate string for each of the 4 Keys. You can leave a string blank provided this Key is not selected as the Active Transmit Key.
   - Passphrase - This is another common method and similar to the 3Com Encryption string. In 64 bit WEP, the passphrase will generate 4 different keys. However, in 128 bit WEP, this method only generates 1 key which is replicated for all 4 keys. The passphrase can be up to 31 characters long and may contain any alphanumeric characters.
3. Click *Apply* to enter the key.

System Tools

The main frame of the System Tools screen includes three administration items: *Restart, Configuration,* and *Upgrade* (Figure 43).

Restart

Figure 43 Restart Screen

The *System Tools* screens are the same under Access Point mode and Client Bridge mode:

- See "Restart" on page 50 for details of the *Restart* screen.
- See "Configuration" on page 50 for details of the *Configuration* screen.
- See "Upgrade" on page 51 for details of the *Upgrade* screen.

Status and Logs

Selecting *Status and Logs* from the main menu displays the *Status* and *Logs* screens in your Web browser window. The *Status* and *Logs* screens are the same under Access Point mode and Client Bridge mode:

- See "Status" on page 54 for details of the *Status* screen.
- See "Logs" on page 54 for details of the *Logs* screen.

Support and Feedback

Selecting the *Support* tab from the *Support/Feedback* screen displays the support links screen, which contains a list of Internet links that provide information and support concerning the Access Point. The *Status* and

Logs screens are the same under Access Point mode and Client Bridge mode:

- See "Support and Feedback" on page 54 for details of the *Support* and *Feedback* screens.

6 TROUBLESHOOTING

Basic Connection Checks

- Check that the Access Point is connected to your switch or hub and that all the equipment is powered on. Check that the LAN port link status LED on the Access Point are illuminated, and that any corresponding LEDs 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 initialised until the start-up procedure has completed.
- If the link status LED does not illuminate for the LAN port, check that you do not have a faulty cable. Try a different cable. Check also that the Uplink/Normal switch is in the correct position.

Browsing to the Access Point Configuration Screens

If you have connected your Access Point, admin computer and switch together but cannot browse to the Access Point configuration screens, check the following:

- Confirm that the physical connection between your computer and the Access Point is OK, and that the link status LEDs on the Access Point and NIC 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 your computer is configured correctly. Make sure that the computer can communicate with other devices on the network. Ensure that the NIC is configured for autonegotiation.
- 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 *Use Proxy Server* option is unchecked.

- When entering the address of the Access Point into your web browser, ensure that you use the full URL including the http:// prefix (e.g. **`http://192.168.1.1`**).
- If you cannot browse to the Access Point, re-run the DISCOVERY software described in Appendix A to discover the Access Point and the IP address it has been allocated from the DHCP server. If there is no DHCP server on your network, the DISCOVERY software changes the IP address of the Access Point so that it is in the same subnet as your admin computer.

Forgotten Password and Reset to Factory Defaults

If you can browse to the Access Point configuration screen but cannot log on because you do not know or have forgotten the password, follow the steps below to reset the Access Point to it's 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 wireless network. All other computer users will lose their network connections whilst this process is taking place, so choose a time when this would be convenient.*

1. Remove power from the Access Point.
2. Hold down the *Reset* button on the rear of the unit and re-apply power to the Access Point. The Alert LED will flash as the Access Point starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly. Keep *Reset* button held down and remove power from the Access Point.
3. Release the *Reset* button.
4. Re-apply power to the Access Point, and when the start-up sequence has completed, browse to the IP address of the Access Point and run the configuration wizard. You may need to restart your computer before you attempt this.
5. When the configuration wizard has completed, you may reconnect your network as it was before.

Wireless Networking

- Ensure that you have a Wi-Fi certified 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 95 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 Access Point is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Access Point.
- If you have a wired and wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the Access Point Wireless LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to "Wireless Settings" on page 39 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 Access Point. The SSID is case-sensitive
- Ensure that you are using the same level of security on all of your wireless computers (None, 40/64 or 128 bit) and that all devices are using the same keys, and the same order of keys where appropriate.
- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using Wireless Connection control on the Access Point.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Access Point. For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage. Additionally consider moving the wireless computer closer to the Access Point 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 select *Clear Channel Select* on the Access Point.
- Sources of interference: The 2.4Ghz ISM band is used for 802.11b. 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 Access Point 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 Access Point to establish whether this problem exists.
- Most wireless computer Adapters will scan the channels for the wireless Access Point. If a wireless computer has not located the

Access Point 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 Access Point channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.

- Speed of connection: The 802.11b standard 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 are 11Mbps, 5.5Mbps, 2Mbps and 1Mbps. In general the closer you are to the Access Point the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Access Point or moving the Wireless computer closer to the Access Point. In an ideal network the Access Point 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 Wireless Card documentation and vendor for more details.

Alert LED

The Alert LED will flash when the Access Point unit is first powered up while the system software checks the hardware for proper operation. Once the Access Point has started normal operation, the Alert LED will go out.

- If the Alert LED does not go out following start up, but illuminates continuously, this indicates that the software has detected a possible fault with the hardware. Remove power from the Access Point, wait 10 seconds and then re-apply power. If the Alert LED comes on continuously again, then a fault has been detected. Locate the copy of the Access Point software on the accompanying CD-ROM or 3Com web site (**`http://www.3com.com`**) and upload it to the Access Point to see if this clears the fault (refer to "Recovering from Corrupted Software" below). If this does not fix the problem, contact your supplier for further advice.

Recovering from Corrupted Software

If the Alert LED remains permanently on following power-up, it is possible that the system software has become corrupted. In this condition, the Access Point will enter a "recovery" state; DHCP is disabled, 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 Access Point unit in this state.

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

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

`www.3com.com`.

1. Remove power from the Access Point and connect the admin computer to the LAN port.
2. You will need to reconfigure this computer with the following static IP address information:
   - IP address: 192.168.1.2
   - Subnet mask: 255.255.255.0
   - Default Gateway address: 192.168.1.1
3. Restart the computer, and re-apply power to the Access Point.
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 Microcode Recovery utility in the Access Point.
5. Follow the on-screen instructions. Enter the path and filename of the software image file.
6. When the upload has completed, the Access Point will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.
7. Reconnect your Access Point to your network. Do not forget to reconfigure the computer you used for the software upload.

   If the Access Point 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 Access Point to Factory Defaults?

See "Forgotten Password and Reset to Factory Defaults" on page 66.

How many wireless clients does the Access Point support?

A maximum of 128 wireless clients are supported.

There is a single LAN ports on the Access Point. 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 Access Point. 3Com wireless access points and OfficeConnect hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

`http://www.3com.com/`

Where can I download software upgrades for the Access Point?

Upgrades to the Access Point software are posted on the 3Com support web site, accessible by visiting:

`http://www.3com.com`.

What other online resources are there?

The 3Com Knowledgebase at:

`http://knowledgebase.3com.com`

is a database of technical information covering all 3Com products. It is updated daily with information from 3Com technical support services, and it is available 24 hours a day, 7 days a week.

A USING DISCOVERY

Running the Discovery Application

3Com provides a user friendly Discovery application for detecting the Access Point on the network.

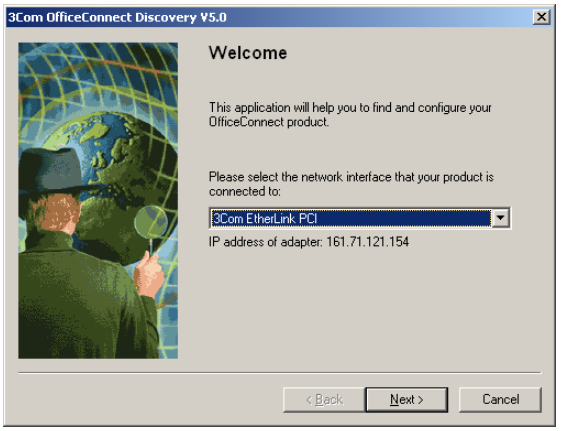
If you are unable to use the Discovery application, the Access Point on initial power-up will attempt to obtain an IP address from your local DHCP server. Consult your DHCP Server log to obtain the IP address that was allocated to your Access Point.

Windows Installation (95/98/2000/Me/NT)

1 Insert the Access Point CD-ROM in the CD-ROM drive on your computer. A menu will appear; select *Discovery*.

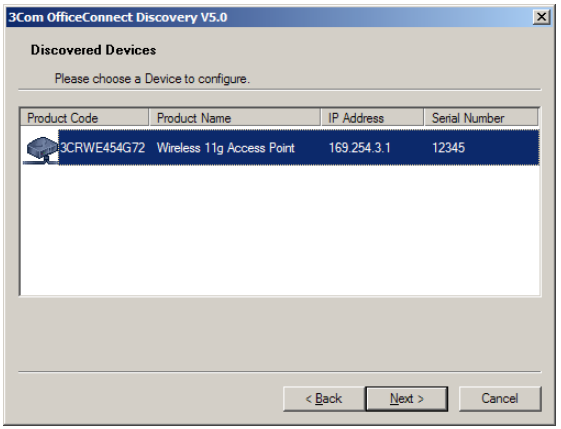
Discovery will find the Access Point even if it is unconfigured or misconfigured.

Figure 44 Discovery Welcome Screen



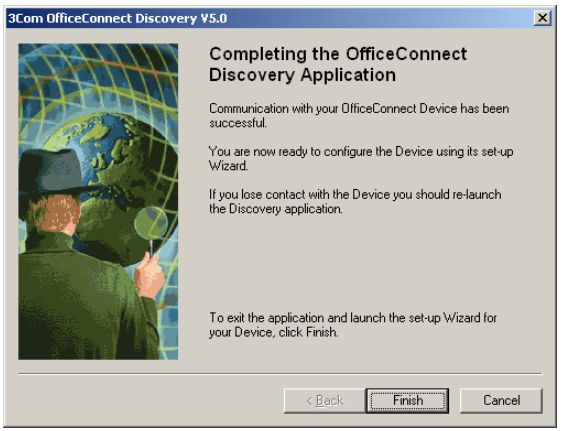
2 When the *Welcome* screen is displayed, select the NIC from which the Access Point will be discovered. Then click on *Next* and wait until the application discovers the Access Points connected to your LAN.

Figure 45 Discovered Access Point Screen



3 Figure 45 shows an example Discovered Devices screen. Highlight the *Wireless 11g Access Point* by clicking on it, and press *Next*.

Figure 46 Discovery Finish Screen



4 Click on *Finish* to launch a web browser and display the login page for the Access Point.

B 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 Access Point over the Network

To manage a device over the network, the Access Point 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 Access Point, you will probably only encounter two types of IP Address and subnet mask structures.

Type One

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

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

This type of IP Address operates on a subnet mask of '255.255.255.0'.

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

Table 3 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
Access Point	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 4 for an example about how a network (only four computers represented) and a Access Point might be configured.

Table 4 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
Access Point	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 Access Point 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 or Windows NT 4.0. 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.

C TECHNICAL SPECIFICATIONS

This section lists the technical specifications for the OfficeConnect Wireless 11g Access Point.

Wireless 11g Access Point

Interfaces

LAN connection - 10Mbps/100Mbps dual speed Ethernet port (10BASE-T/100BASE-TX)

WLAN Interfaces

Standard IEEE 802.11g, Direct Sequence Spread Spectrum (DSSS)
Transmission rate: 54Mbps, automatic fallback to 48, 36, 24, 18, 12, or 6 Mbps
Maximum channels: 14
Range up to 304.8m (1000ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz
Sensitivity: 6, 12, 18, 24, 36, 48 Mbps: -85 dBm;
54 Mbps -66 dBm typical
Modulation: CCK, BPSK, QPSK, OFDM
Encryption: 40/64 bit WEP, 128 bit WEP, WPA
Maximum clients: 128
O/P Power: 18dBm

Standard IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)
Transmission rate: 11bps, automatic fallback to 5.5, 2, or 1 Mbps
Maximum channels: 14
Range up to 304.8m (1000ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz
Sensitivity: 1, 2, 5.5 Mbps: -85 dBm; 11 Mbps -82 dBm typical
Modulation: CCK, BPSK, QPSK, OFDM
Encryption: 40/64 bit WEP, 128 bit WEP, WPA
Maximum clients: 128
O/P Power 18dBm

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

7VA, 23.9 BThU/hr

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

- Width = 220 mm (8.7 in.)
- Depth = 135 mm (5.3 in.)
- Height = 24 mm (1 in.)

Weight

Approximately 500 g (1.1 lbs)

Standards

Functional:	ISO 8802/3 IEEE 802.3 IEEE 802.11b, 802.11g, Wi-Fi
Safety:	UL60950 CSA 22.2 #60950 IEC 60950 EN 60950
EMC:	EN 55022 Class B EN 55024 CISPR 22 FCC Part 15 Class B* ICES-003 Class B CNS 13438 Class A ETSI EN 301 489–17
Radio	CFR 47 FCC Part 15.207, 15.209, 15.247 and 15.249. ETS 300 328 (2.4 GHz ISM band wide band transmission systems. RSS-210
Environmental:	EN 60068 (IEC 68)

*See "FCC Statement" on page 97 for conditions of operation.

System Requirements

Operating Systems

The Access Point will support the following Operating Systems:

- Windows 95/98
- Windows NT 4.0
- Windows ME
- Windows 2000
- Windows XP
- Mac OS 8.5 or higher
- Unix

Ethernet Performance

The Access Point complies to the IEEE 802.3i, u and x specifications.

Wireless Performance

The Access Point has been designed to conform to the Wi-Fi interoperability test standard.

Wi Fi™
The Standard for Wireless Fidelity.

Cable Specifications

The Access Point 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).

D SAFETY INFORMATION

Important Safety Information

***WARNING**: Warnings contain directions that you must follow for your personal safety. Follow all directions carefully.*
You must read the following safety information carefully before you install or remove the unit:

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

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

***WARNING**: Only stack the Access Point with other OfficeConnect units.*

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

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

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

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

***WARNING**: Disconnect the power adapter before moving the unit.*

***WARNING: RJ-45 ports.** These are shielded RJ-45 data sockets. They cannot be used as telephone sockets. Only connect RJ-45 data connectors to these sockets.*

Wichtige Sicherheitshinweise

***VORSICHT:** Warnhinweise enthalten Anweisungen, die Sie zu Ihrer eigenen Sicherheit befolgen müssen. Alle Anweisungen sind sorgfältig zu befolgen.*
Sie müssen die folgenden Sicherheitsinformationen sorgfältig durchlesen, bevor Sie das Geräts installieren oder ausbauen:

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

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

***VORTSICHT:** Stapeln Sie das Geräts nur mit anderen OfficeConnect Gerätes zusammen.*

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

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

***VORSICHT:** Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.*

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Access Point haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.*

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

VORSICHT: RJ-45-Anschlüsse. *Dies sind abgeschirmte RJ-45-Datenbuchsen. Sie können nicht als Telefonanschlußbuchsen verwendet werden. An diesen Buchsen dürfen nur RJ-45-Datenstecker angeschlossen werden.*

Consignes importantes de sécurité

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

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

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

AVERTISSEMENT: *Seulement entasser le moyer avec les autres moyeux OfficeConnects.*

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

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

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

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

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

AVERTISSEMENT: Ports RJ-45. *Il s'agit de prises femelles blindées de données RJ-45. Vous ne pouvez pas les utiliser comme prise de téléphone. Branchez uniquement des connecteurs de données RJ-45 sur ces prises femelles.*

E END USER SOFTWARE LICENSE AGREEMENT

3Com Corporation
END USER SOFTWARE LICENSE AGREEMENT

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

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

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

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

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

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

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

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

UNITED STATES GOVERNMENT LEGENDS: The Software, Documentation and any other technical data provided hereunder is commercial in nature

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

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

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

GOVERNING LAW: This Agreement shall be governed by the laws of the State of California, 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 desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

3Com Corporation, 5500 Great America Parkway, P.O. Box 58145, Santa Clara, CA 95052-8145 (408) 326-5000

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 infra-structure mode, used by the Access Point. (see also Infra-structure mode.)

Auto-negotiation Some devices in the OfficeConnect 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. The bandwidth for 802.11g is 54 Mbps.

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 OfficeConnect Wireless 11g Access Point 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 Gateway operates.

Client The term used to described 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.

Encryption A method for providing a level of security to wireless data transmissions. The OfficeConnect Wireless 11g Access Point uses two types of encryption; WPA and WEP. WPA is a more powerful level of encryption than WEP.

ESSID Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the Access Point 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 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.

Infra-structure mode Infra-Structure mode is the 802.11g configuration supported by the Access Point. You will need to ensure all of your clients are set up to use infra-structure mode in order for them to communicate with the Access Point. (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.

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.

Network A Network is a collection of computers and other computer equipment that are 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.

RJ-45 A standard connector used to connect Ethernet networks. The "RJ" stands for "registered jack".

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

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

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

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

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

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

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

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

Traffic The movement of data packets on a network.

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

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

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

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

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

Wizard A Windows application that automates a procedure such as installation or configuration.

WLAN Wireless Local Area Network. A WLAN is a group of computers and devices connected together by wireless in a relatively small area (such as a house or office).

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

INDEX

A
Access 13
Addresses
    IP 73
Administration Password 26, 33
Automatic Addressing 75

C
Cable Specifications 79
Channels 97
Configuration
    backup 51
    restore 51
Conventions
    notice icons, About This Guide 8
    text, About This Guide 8
Country Selection 24

D
DHCP 27, 38, 75
Discovery Application 71

F
Forgotten Password 66

I
Internet
    addresses 73
IP Address 27, 28, 34, 73

L
LAN 26, 34, 59
LED 14
Login 23, 72
Logs 54

M
MAC Address
    deleting 46
    modifying 46

N
Network
    addresses 73
Networking
    wireless 66
NIC
    wireless 14

P
Password 23, 33
Profile 48

R
Reset to Factory Defaults 51, 66
Restart 50, 63

S
Setup Wizard 21, 34
Specifications
    technical 77
Static Addressing 75
Status 54
Subnet Mask 27, 28, 73
Summary 30
Support Information 54, 63
Support Links 55, 63

T
TCP/IP 27, 73
Technical
    specifications 77
    standards 77
Time Zone 50

U

Unit Configuration 34
Upgrade 51

W

Wireless
- authorised PCs 45
- channel selection 39
- client list 47
- configuration 39, 60
- connection control 44
- encryption 41, 60
- LED 15
- networking 66
- NIC 14
- service area name 40, 60
- settings 28, 39, 59

Regulatory Notices for the Wireless 11g Access Point

Channels

Use of the Wireless 11g Access Point is only authorized for the channels approved by each country. For proper installation, login to the management interface and select your country from the drop down list. Table 5 below details the channels permitted by the local regulatory agencies:

Table 5 Channels

Channels	Country
1–13	Australia, Austria, Bahrain, Belarus, Belgium, Chile, China, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Finland, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malaysia, Netherlands, New Zealand, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Russia, Saudi Arabia, Singapore, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, Uruguay, Venezuela.
1–11	Argentina, Brazil, Canada, Columbia, Mexico, Taiwan, United States
10–13	France, Jordan
5–7	Israel
1–14	Japan

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules, and the Canadian Department of Communications Equipment Standards entitled, “Digital Apparatus,” ICES-003. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

Information to the User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.
- Consult the dealer or an experienced radio/television technician for help.

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

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4. In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model:	**Description:**
3CRWE454G72	Wireless 11g Access Point

to which this declaration relates, is in conformity with the following standards or other normative documents:

- ANSI C63.4-1992 Methods of Measurement
- Federal Communications Commission 47 CFR Part 15, subpart B
  15.107 (a)Class B Conducted Limits
  15.109 (a)Class B Radiated Emissions Limits
- 15.107 (e)Class B Conducted Limits
  15.109 (g)Class B Radiated Emissions Limits

Exposure to Radio Frequency Radiation: The radiated output power of the 3Com OfficeConnect Wireless 11g Access Point is far below the FCC radio frequency exposure limits. Nevertheless, the 3Com OfficeConnect Wireless 11g Access Point shall be used in such manner that the potential for human contact during normal operation is minimized. The distance between the antennas and the user should not be less than 20 cm.

CE Statement (Europe)

This product complies with the European Low Voltage Directive 73/23/EEC, EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC and the Radio and Telecommunications Terminal Equipment Directive 99/5/EC.

CSA Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

BSMI Statement

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

FCC

CAUTION: *To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

RF Exposure Compliance Statement (U.S.)

CAUTION*: The 3Com OfficeConnect Wireless 11g Access Point has been certified as a mobile computing device as per FCC Section 2.1091. In order to comply with the FCC RF exposure requirements, the 3Com OfficeConnect Wireless Cable/DSL Gateway must only be installed with approved antennas and a minimum separation distance of 20 cm (8 in) must be maintained from the antenna to any nearby persons.*

Potential RF Interference (Canada)

CAUTION*: To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or it's transmit antenna) that is installed outdoors is subject to licensing.*

3Com Corporation, Corporate Headquarters,
5500 Great America Parkway, Santa Clara,
CA 95052-8145, USA.

To learn more about 3Com products and services, visit our World Wide Web site at **www.3com.com**

All specifications are subject to change without notice.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and OfficeConnect are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies.

DUA0045-4AAA01
Rev. 01