



11 Mbps Wireless LAN Access Point 8000 User Guide

Version 1.0

<http://www.3com.com/>
<http://support.3com.com/registration/frontpg.pl/>

Published January, 2002
Version 1.0

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 2002 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

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

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

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

UNITED STATES GOVERNMENT LEGEND

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

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR2. 1 01(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

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

3Com and AirConnect are registered trademarks and the 3Com logo is a trademark of 3Com Corporation.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

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

EXPORT RESTRICTIONS: This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license.

CONTENTS

1 INTRODUCTION

- Setting up a Wireless Network 1
 - Wireless and Wired Networks 1
 - Network Security and RADIUS Support 1
- AP8000 Feature Summary 2
- Installation Overview 3
- Software Utilities 4

2 INSTALLING THE ACCESS POINT

- Before You Begin 5
- Deciding Where to Place Equipment 6
- Connecting the Standard Antenna 6
- Placing the Access Point 7
 - Mounting on a Wall 7
 - Mounting on a Ceiling 8
- Connecting Power 9
- Connecting to an Ethernet Network 10
- Checking the LEDs 10
- Antenna Options 11
 - Omnidirectional Antenna 11
 - Ceiling Mount Omnidirectional Antenna 11
 - Ceiling Mount Hallway Antenna 12
 - Directional Panel Antenna 12
- Connecting an Optional Antenna 13

3 ACCESS POINT SECURITY

- Security Configuration Options 15
- Using the Wireless 802.1X Agent 16
 - Authentication and Login 16
 - 802.1x Client Properties 17

4 MANAGING THE WIRELESS LAN

- Overview 19
- Starting the Device Manager 19
 - Selecting a Device 19
 - The Pre-IP Configuration Wizard 20
 - Installing the Management Device on a Computer 21

Using the Configuration Management System	21
System Configuration	21
Access Point Properties	22
Network Properties	22
Data Transmission Properties	23
Security	24
AP Encryption	24
User Access List	25
RADIUS Authentication and Accounting	26
Management	26
SNMP Management	26
TFTP Setup	26
System Log Setup	26
Tools	27
Upgrade System	27
Downloading Upgrade Files	27
Installing an Upgrade	27
Change Administration Password	27
Configuration Backups	28
Statistics	28
System Status	29
Restoring an Access Point to Factory Defaults	29
Interoperating with Third-Party Equipment	29

5 CONDUCTING A SITE SURVEY

Choosing Trial Locations	31
Environmental Requirements	31
Electrical Requirements	32
Summary of the Survey Procedure	32
Using the Site Survey Tool	32
Setting up Equipment	33
Launching the Tool	33
Configuring the Site Survey	33
Running the Tests	33
Interpreting Test Results	35
Site Survey Menus	36

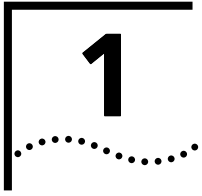
6 TROUBLESHOOTING

A TECHNICAL SUPPORT

Online Technical Services	39
World Wide Web Site	39
3Com Knowledgebase Web Services	39
3Com FTP Site	39
Support from Your Network Supplier	40
Support from 3Com	40

INDEX

REGULATORY COMPLIANCE INFORMATION



INTRODUCTION

The 3Com wireless product family lets you set up a local area network (LAN) without the restraints of network cabling. If your office already has an Ethernet LAN, the 3Com 11 Mbps Wireless LAN Access Point 8000 can extend the network without additional cabling. The access point security features will also extend the security of installed wired networks to include all wireless components.

Setting up a Wireless Network

The type of network you configure depends on the size of your office and whether you require a connection to a wired LAN. A simple configuration consists of an access point and several clients. The clients can associate with the wireless network anywhere within the coverage area of the access point.

For more complex requirements, you can configure several access points as separate networks at the same site. The access points use different network identifiers called wireless LAN service areas (WLAN service areas) or Extended Service Set Identities (ESSID). Client computers can roam within the coverage areas of access points that have the same WLAN service areas.

Wireless and Wired Networks

An access point can be connected to a wired LAN by an Ethernet cable acting as a bridge between the wired and wireless networks. In this configuration, the access point provides the link between the wired network and wireless clients. Clients can move freely throughout the service area of the access point and remain associated with the larger network, allowing client access to the full range of network services.

For complete wireless coverage, several access points can be connected to an existing LAN. Wireless clients can roam freely between different access points with the same WLAN service areas and remain associated with the larger network.

Network Security and RADIUS Support

The Access Point 8000 provides a multiple-layer security solution, supporting the IEEE 802.1x, Remote Access Dial-In User Service (RADIUS) Authentication, and the Extensible Authentication Protocol (EAP). If you do not have a centralized RADIUS server, the access point's Dynamic Security Link manages network login. The access point's internal data base supports up to 1000 users.

The security configuration options include:

Authentication	Encryption	Description
802.11 standard Open	No encryption	Basic area network name with no encryption.
802.11 standard 40-bit shared key	40-bit shared key	Standard WiFi Requirement to insure interoperability.
802.11 standard 128-bit shared key	128-bit shared key	Strong encryption. Compatible with other vendors' 128-bit shared key scheme including AirConnect, Agere, and Cisco.
Dynamic Security Link 128-bit dynamic key	128-bit dynamic key	3Com proprietary scheme to enable user-level authentication with 128-bit dynamic per user, per session key.
802.1x/RADIUS Authentication (EAP-MD5)	No encryption 40-bit shared key 128-bit shared key	RADIUS authentication using the MD5 authentication method (username- and password-based) and access point encryption.
802.1x/RADIUS Authentication (EAP-TLS)	40-bit dynamic key 128-bit dynamic key	Certificate-based mutual RADIUS authentication with 40 and 128-bit Dynamic encryption key.
802.1x/RADIUS Serial Authentication (EAP-TLS, EAP-MD5)	40-bit dynamic key 128-bit dynamic key	Mutual RADIUS authentication implementation based on proposed IEEE draft. Uses 3Com Universal Client Certificate to allow client and RADIUS to mutually authenticate (EAP-TLS) and perform User authentication (EAP-MD5).

AP8000 Feature Summary

Clear channel select	When initializing, automatically scans the frequency spectrum and selects the channel with the least interference.
Power over Ethernet	Powered over the Ethernet cable to reduce the number of cables.
Access point discovery	Clients and network administrators can discover access points and ESSIDs within the same network segment. The network administrator can also discover, manage, and upgrade access points across routers by means of the 3Com Network Supervisor (3NS).
Rate control	Rate Control options available in the access point to select Optional, Required, or Not Used.
Transmit power control	Adjustable power level from minimum to maximum to extend transmission range.
Roaming within segments	Allows client to roam between access points within the same segment.
User support	Supports up to 256 simultaneous users, regardless of mode of operation.
DHCP support	Uses DHCP to obtain a leased IP address and network configuration information from a server. If the network has no DHCP server, the access point's internal DHCP server assigns IP addresses to clients in a stand-alone wireless network.
SNMP and MIB interfaces	SNMP, HP OpenView, and 3Com Network Supervisor (3NS).
Support for multiple access points	Simultaneous setup and configuration of multiple access points, as well as simultaneous upgrades. Bulk configuration and profile download capability.
Authentication features	Supports RADIUS authentication between the wireless client and the RADIUS servers, in conjunction with the IEEE 802.1x.

802.1x Support	Port-based network access control utilizes the physical characteristics of the switched LAN infrastructures to authenticate devices attached to a LAN port, and prevent access to that port in cases where the authentication process fails.
Encryption	Supports 40-bit and 128-bit shared encryption, and 128-bit dynamic encryption key. Compatible with Cisco and Agere/Lucent Access Points and Clients, Microsoft
Management tools	Web server in the access point supports device configuration and management through your web browser. Access point software tools run under Windows 95, 98, 98se, Me, WinNT 4.0 SP4 or above, Windows 2000, and Windows XP. The 3Com Network Supervisor discovers and displays a map of all Wireless Clients within a segment. Built-in Web server simplifies firmware upgrades. Web-based interface requires Java script support and so is compatible with Internet Explorer 5.0 or greater and Netscape Communicator 6.0 or greater.

Installation Overview

- 1 Choose the best place for the installation (flat surface, wall, or acoustical ceiling). Look for a location away from equipment that might cause radio interference. The site should be elevated and centrally located relative to the users on your wireless network.
- 2 Make sure that you are familiar with the following items and have them available where required for your installation:
 - Access point
 - 3Com Integrated Power-over-Ethernet power supply and power cord
 - Standard category 5 straight (8-wire) Ethernet cable
 - Mounting hardware (for wall- or ceiling-mount installations)

It may be useful for you to conduct a site survey before permanently installing the access point. See "Conducting a Site Survey" on page 31.

- 3 Install the access point following the steps outlined in "Installing the Access Point" on page 5.
- 4 Connect the access point to the power supply and connect the power supply to a power source. (If you use your own power-over-Ethernet hub or switch, ensure that your equipment also complies with the IEEE 802.3af standard.)
- 5 If you are linking your wireless network to your wired Ethernet network, run an Ethernet segment from the To Hub/Switch port on the power brick to a LAN port. (Be sure you do not connect the Ethernet segment to the port labeled To Access Point. Doing so may damage network components.)
- 6 After hardware installation is complete, install the access point tools, utilities, and user guide from the installation CD.
- 7 To set access point security or configure the wireless network, refer to "Managing the Wireless LAN" on page 19.
- 8 To set up a wireless client to authenticate through the access point to your RADIUS server, refer to "Using the Wireless 802.1X Agent" on page 16.
- 9 For information on improving the signal between the access point and a wireless client, see "Antenna Options" on page 11.

Software Utilities

The 3Com Administrator Utilities CD includes tools and utilities to help you set up and administer the wireless components of your network. Software tools and utilities are presented as Tools and Utilities options on the main menu of the CD and include:

- **Install the Utility Software and Documentation.** This option installs the Wireless Infrastructure Device Manager Tool which you can use to monitor access points and select devices for administrative changes. It also installs the Site Survey Tool and product documentation in other languages as translations become available.
- **Install TFTP Server Tool.** A TFTP server is required for firmware upgrades and for backing up and restoring access point configuration files. This option launches 3CDaemon, which installs a TFTP server for you. You do not have to select this option if you already have a TFTP server set up.
- **Install 802.1x Client Tool.** This option installs the Wireless Authentication Agent for 802.1x support. If you will be using the access point in conjunction with a RADIUS authentication server, you must install this agent on each wireless client PC in the network. On systems running Windows XP this agent is not required because 802.1x support is built into the operating system.
- **Install the 3Com Network Supervisor.** The 3Com Network Supervisor is a centralized network management software program. It is not required for managing access points. It is included for sites that require centralized network management and are not already using an SNMP-based tool.
- **Install the 3Com Network Supervisor Service Pack 2.** This is an upgrade package for the 3Com Network Supervisor. You should install the service pack only after installing the 3Com Network Supervisor.
- **Install Adobe Acrobat Reader.** For users who do not already have Acrobat Reader for viewing the PDF documentation, a current version is included on the CD.
- **Install Internet Explorer 5.5.** For users who do not already have a browser that supports the HTML version 4 (required for the Configuration Management System user interface), a current version of Internet Explorer is included on the CD. If you need to change or upgrade to a browser that supports the HTML version 4 interface of the Configuration Management System, you can install this software.

2

INSTALLING THE ACCESS POINT

Before You Begin

The following items are required for installation:

- 3Com Integrated Power-over-Ethernet power supply and power cord.
- Standard category 5 straight (8-wire) Ethernet cable for connecting the access point to the power supply. This length of cable must reach from the access point to the power supply.

If you plan to connect the access point to a wired network, you will need an additional length of Ethernet cable.

- If you plan to mount the access point on a wall:
 - Mounting template
 - Wall mount hardware kit
- If you plan to mount the access point to the T-rail grid of an acoustical ceiling:
 - Mounting bracket
 - Two #6 panhead screws



For advanced installations, we recommend that you conduct a site survey before permanently installing the access point. A site survey tool is provided on the 3Com Administrator Utilities CD. To conduct the survey, you must also use the administrator utilities to set up a wireless client. See "Conducting a Site Survey" on page 31.



CAUTION: *Only professional network personnel should install the access point, cables, and antennas.*

After hardware installation is complete:

- Install the access point tools, utilities, and user guide from the installation CD.
- Review the default system settings and ensure they are suitable for your site.
- If required, use the administrative utilities to change configuration parameters. See "Using the Configuration Management System" on page 21.

For the latest networking information, see the 3Com Corporation World Wide Web at:

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

Deciding Where to Place Equipment

Select a clean, dry location that provides good reception. The site should not be close to transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators and other equipment.

If you are connecting the access point to a wired network, the location must provide an Ethernet connection. The power supply also requires an Ethernet connection, and in addition must be located near a power source. An Ethernet cable will have to run from the power supply to the access point.

An access point provides coverage at distances of up to 1000 feet. Signal loss can occur if metal, concrete, brick, walls, or floors block transmission. If your office has these kinds of obstructions, you may need to add additional access points to improve coverage.

If you plan to use one of the available optional antennas instead of the standard detachable antennas, review “Antenna Options” on page 11 before selecting the final location and be sure to allow for routing the antenna cable.

Do not install the access point in wet or dusty areas without protection. Make sure the temperature ranges between -20°C to 55°C (-4°F to 131°F).

Connecting the Standard Antenna

The access point is supplied with standard detachable antennas. These should be attached before the access point is installed.

- 1 Carefully unpack the standard detachable antennas.
- 2 Screw an antenna into each of the sockets in the access point housing.
- 3 Hand-tighten the antennas.
- 4 Position the antennas so they turn out and away from the access point at a 45-degree angle.

As a rule, the initial orientation of the antennas should be perpendicular to the floor. After network startup, you may need to adjust the antennas to fine-tune coverage in your area.

Depending on the coverage required for your site, you may want to replace the standard detachable antennas with one of the external antennas available for use with the access point. See “Antenna Options” on page 11 .

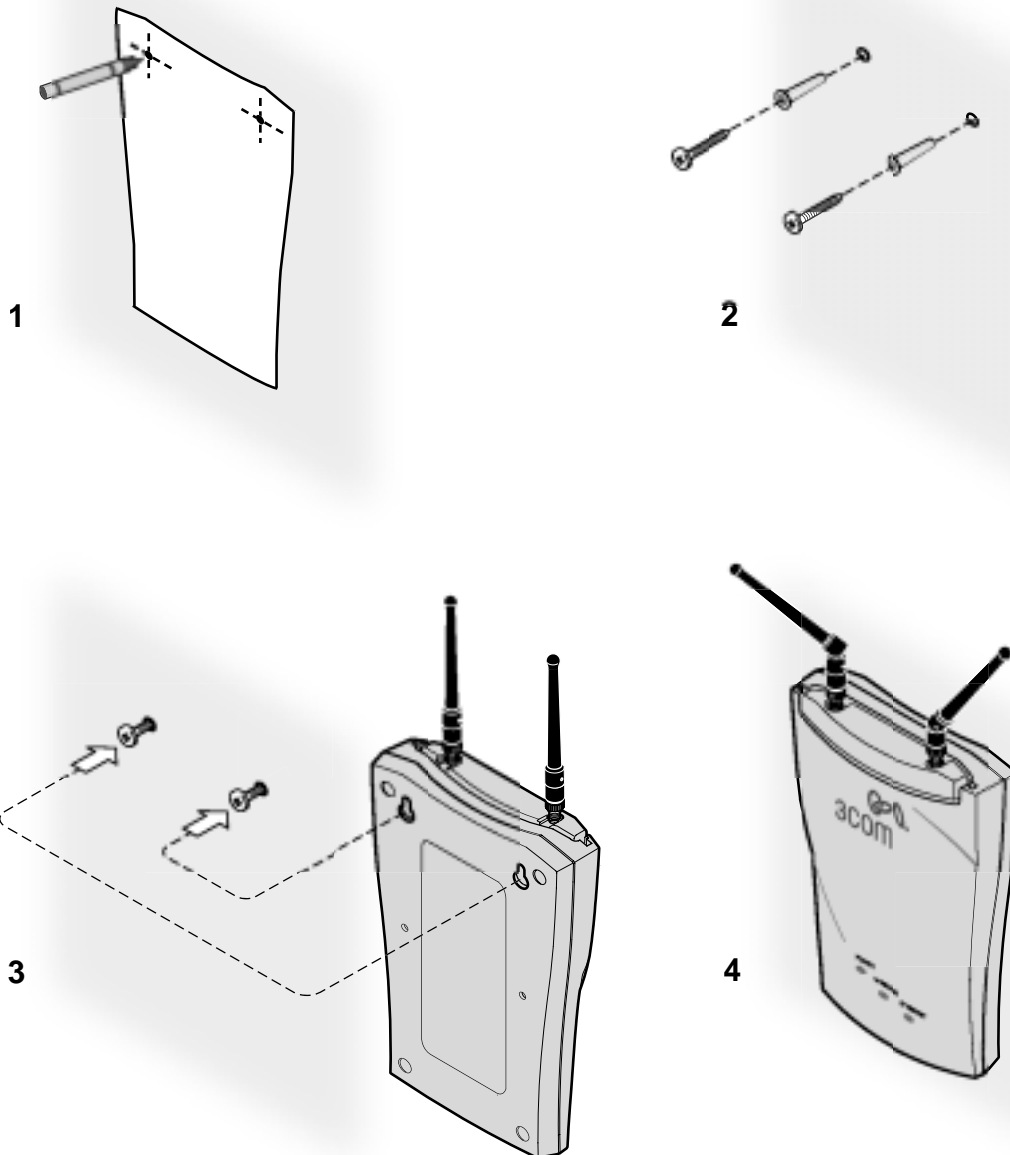
The standard detachable antennas do not have an electrical connection between the mask mount and the coaxial cable shield. However, adding a lightning arrester will correct this situation by grounding the outer shield as recommended. Some arrester designs provide over-voltage protection for the signal sent down the cable. If you use such a design, be sure that it can pass signals used in the 2.5GHz signal range. Many inexpensive units are available with F connectors, but these are typically designed for cable TV-UHF applications and may degrade the signals in the band used by the wireless bridge.

Placing the Access Point

The access point can be placed on a flat surface such as a table or desktop or it can be mounted on a wall or to the T-rail grid of an acoustical ceiling. If you choose a flat surface, select one clear of obstructions and provides good reception. Place the access point and adjust the antenna so that the arms point up and away from the access point at a 45-degree angle.

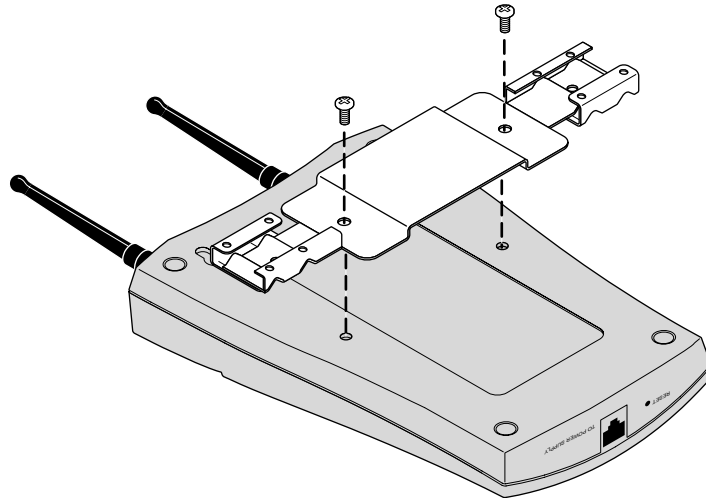
Mounting on a Wall

To mount an access point on a wall, follow the instructions on the mounting template supplied in the box and refer to the following illustration. Preferably, mount the access point near the ceiling above any obstructions that could block transmission. Position the antenna so that the arms point out and away from the access point at a 45-degree angle

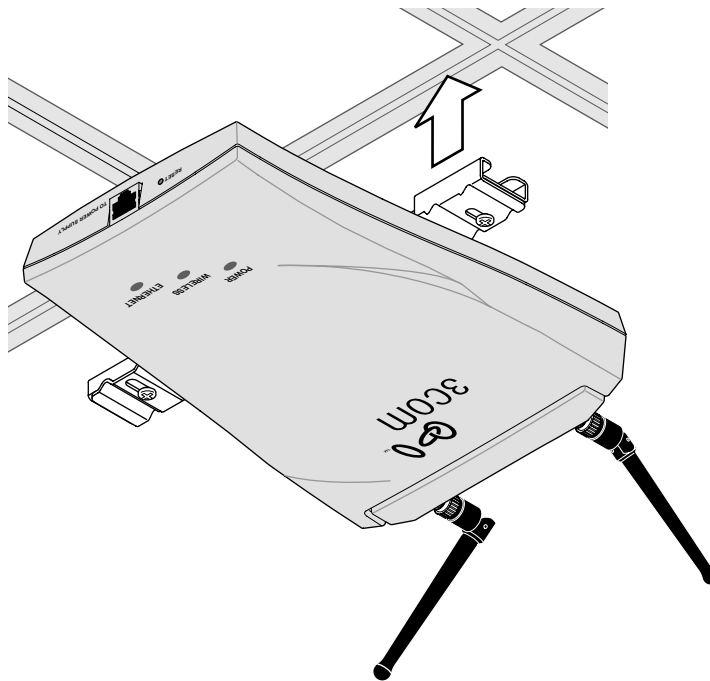


Mounting on a Ceiling

To mount an access point to the T-rail grid of an acoustical ceiling, you must first attach the mounting bracket to the access point as shown.



Align the T-rail grips with the ceiling T-rail, adjusting them so they grip the T-rail snugly. Tighten the screws on the T-rail grip. Position the antenna so that the arms point down and away from the access point at a 45-degree angle.



NOTE: After installation, there may be some play in the fit of the T-rail grips on the T-rail. This is likely due to the size of the T-rails but should not prevent a secure grip.

Connecting Power

The access point is powered by the 3Com Integrated Power-over-Ethernet power supply, which provides power over a standard category 5 straight (8-wire) Ethernet cable. This eliminates the need to run standard power directly to the access point.

The power supply can be located at any point between the access point and the LAN access port (if you plan to connect to a wired LAN), where a convenient power outlet exists.

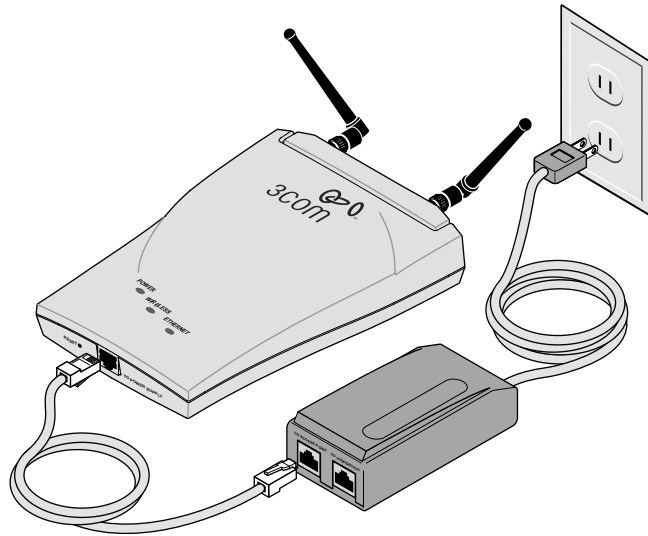


NOTE: The access point is IEEE 802.3af compliant. Before connecting the access point to your own power-over-Ethernet hub or switch, ensure that your equipment also complies with the IEEE 802.3af standard.

When you connect the power make sure you connect the cable to the port labeled *To Access Point* on the power supply. When the access point receives power, the LEDs light.



CAUTION: If you supply your own Ethernet cable for connecting power, be sure that it is standard cable that has not been altered in any way. Use of nonstandard cable could damage the access point.

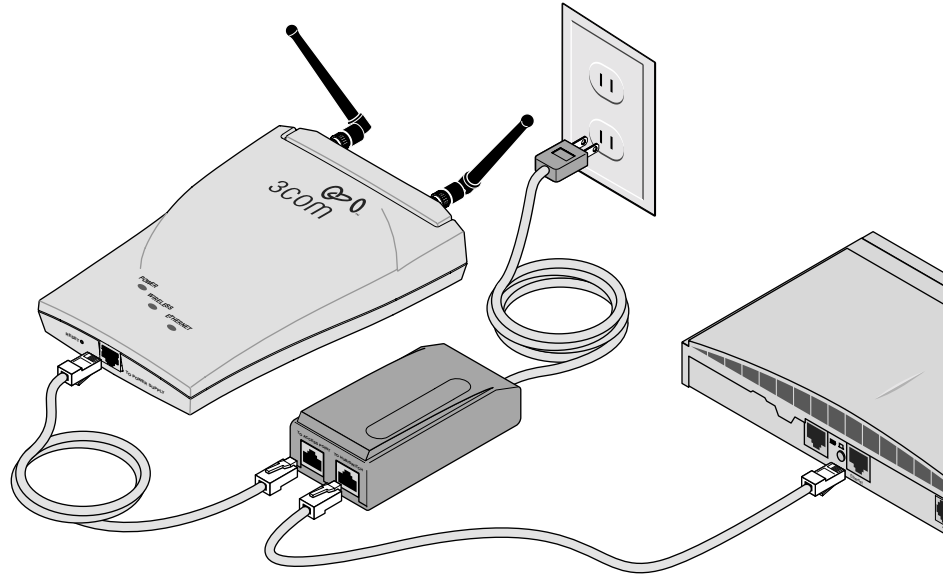


Connecting to an Ethernet Network

Use a standard Ethernet cable to connect the access point to an Ethernet network, as shown below.



CAUTION: To avoid damaging other components connected to the network, make sure that the Ethernet cable connected to the LAN port is plugged into the To Hub/Switch port on the power supply (not the To Access Point port).



Checking the LEDs

Table 1

LED	Description
Power	<ul style="list-style-type: none">■ On—Access point has power.■ Off—Access point is not receiving power.
Wireless	<ul style="list-style-type: none">■ Blinking—The access point is operating. The blink speed ranges from approximately once every 2.5 seconds to approximately 10 times per second, depending on the signal strength and transmission speed.■ Off—The access point is not receiving power.
Ethernet	<ul style="list-style-type: none">■ Blinking—Wired LAN traffic is detected. Faster blinking indicates heavier traffic.■ Off—There is no wired LAN connection or the access point is not receiving power.

Antenna Options

The standard detachable portable antenna supplied with the access point is a multi-purpose antenna suitable for a variety of environments, including office LANs, physical plants, and factory floors. If your site has special requirements that might be served by different types of antenna, four optional antenna models are available, as shown below:

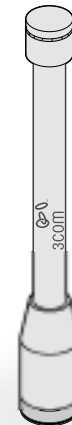
Model number	3CWE490	3CWE492	3CWE497	3CWE498
Design and type	Omnidirectional (fiberglass)	Ceiling-mount omnidirectional	Ceiling-mount hallway	Directional Panel (indoor/outdoor)
Frequency Range	2.400-2.4835 GHz	2300-2500 Mhz	2300-2500 Mhz	2300-2500 Mhz
Gain	4 dBi	2.5 dBi	4 dBi	8 dBi
VSWR across band	< 1.5:1	< 1.35:1	< 1.5:1	< 1.5:1
Max. power input		50 Watts	10 Watts	20 Watts
Temperature range	-40°C to +80°C	-40°C to +80°C	-40°C to +71°C	-40°C to +80°C
Dimensions (inches)	10" (height)	4.25 (diameter)	2.6 x 1.8 x 0.2	5.1 x 4.7 x 1.5
Weight	5.34 oz.	8 oz.	2 oz.	8 oz.
Cable		12" RG58/U	12" LMR100	12" RG58/U

Omnidirectional Antenna

The fiberglass omnidirectional antenna (model number 3CWE490) is designed for use in harsh indoor environments. It can be centrally located on the ceiling to provide uniform coverage over a wide area.

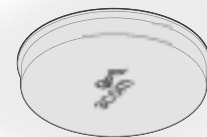
This antenna features a built-in matching network that eliminates the need for a ground plane.

This antenna can be mounted on the ceiling by means of a standard ceiling-mount bracket. Before installing, ensure that access is available for cable routing.



Ceiling Mount Omnidirectional Antenna

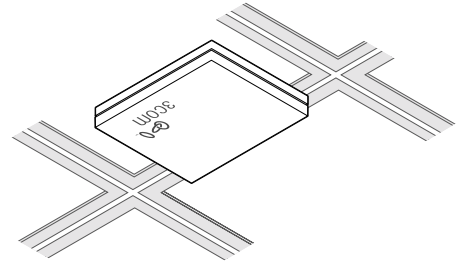
The ceiling-mount omnidirectional antenna (model number 3CWE492) is designed to cover large, open areas. It should be located at or near the center of the ceiling of a large, open area (such as an open office space divided into cubicles) to provide uniform coverage in all directions.



It is mounted by means of a single-hole stud mount, and so can be fixed easily to drop ceiling tiles or to a solid ceiling surface where cable routing access is available.

Ceiling Mount Hallway Antenna

The ceiling-mount hallway antenna (model number 3CWE497) has a bidirectional design that makes it ideal for use in long corridors. Its small size means it can provide extended WLAN coverage with minimum visibility.



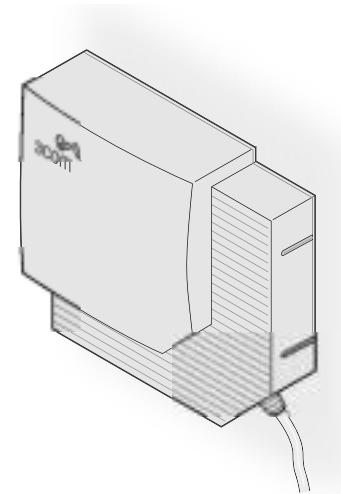
This model includes a bracket for quick installation on standard one-inch ceiling rails. In addition, mounting holes allow for installation to any flat surface with screws.

Directional Panel Antenna

The ceiling, wall, and corner-mount flat-panel directional antenna (model 3CWE498) provides stable coverage both indoors and outdoors.

The panel can be mounted virtually anywhere and in any orientation.

The flat-panel antenna directional operates with a gain of 8 dBi. Depending on the country where the access point is being installed, there may be transmit power restrictions:



- When using this antenna in the United States, Canada, Mexico, Argentina, Brazil, Taiwan, Malaysia, New Zealand, Colombia, India, and Peru, no transmission power restrictions apply.
- *In all other countries*, transmit power is limited to 100 MW. You must manually select Low or Medium power from the Data Transmission Properties page of the configuration management system. See “Data Transmission Properties” on page 23 for information on manually selecting transmission levels.

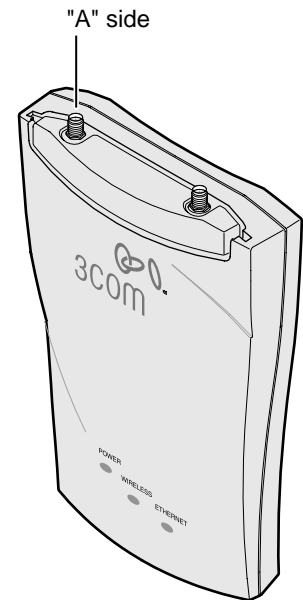
By default, the access point automatically selects the optimal channel for network broadcasts. If you are using this antenna in France or Singapore, you must manually select from channels 10–13. See “Data Transmission Properties” on page 23 for information on manually selecting radio channel settings.

Connecting an Optional Antenna

To ensure the physical safety of anyone near the antenna and to prevent damage to the access point, follow the building codes for antenna installations in your area. Also, keep the following considerations in mind:

- When connecting the optional antenna to the access point, remember to use only the A-side connector on the access point.
- While aligning the antenna, you may want to use the Site Survey tool (preferably installed on a mobile PC that can be used at the antenna site) to adjust the antenna to achieve the maximum possible received signal strength. See "Using the Site Survey Tool" on page 32 for more information.

- 1 Position the antenna so that there are minimal obstacles between it and any client with which it will communicate. While maintaining a direct line of sight between the antenna and a client is not strictly necessary, such an arrangement helps to ensure a strong signal. Ensure that access is available for routing the antenna cable from the antenna to the access point.
- 2 If they are installed, remove both arms of the standard detachable antenna.
- 3 Connect one end of the optional antenna cable to the antenna.
- 4 Secure the antenna in place and rout the antenna cable to the access point.
- 5 Connect the free end of the antenna cable to the A side connection on the access point.
- 6 Make certain that antennas and antenna masts are appropriately grounded to prevent injury or damage from lightning strikes.



3

ACCESS POINT SECURITY

The access point multiple-layer security solution supports IEEE 802.1x, Remote Access Dial-In User Service (RADIUS) Authentication, and Extensible Authentication Protocol (EAP). If you do not have a centralized RADIUS server, the access point's Dynamic Security Link manages network login.

The access point supports any RADIUS implementation compliant with RFC 2865 and following standard EAP, RFC 2284, 2716, 2548 protocols. However, while supporting 802.1x / RADIUS authentication, 3Com does not supply RADIUS software or configuration instructions other than what is applicable for access point configuration. Refer to your system administrator for RADIUS software or configuration parameters for your site.



Before you can authenticate a PC-based wireless client through your RADIUS server, you must install and run the Wireless Authentication Agent. See "Using the Wireless 802.1X Agent" on page 16.

Security Configuration Options

Open Network. The open-network option assumes that neither authentication nor encryption are required. Network security is achieved by means of the wireless network area name or SubSystemID (SSID).

40-bit Shared Encryption Key (Wi-Fi) Settings. For this option, the network administrator sets up encryption keys for the wireless network and supplies users with an encryption string or hexadecimal keys. You must set up encryption keys on both the client and access point. This option can be used with local access point authentication or with EAP-MD5 RADIUS authentication.

128-bit Shared Encryption Key Settings. This option is compatible with 128-bit shared key from other vendors, including 3Com AirConnect, Agere, and Cisco. The network administrator sets up encryption keys for the wireless network and supplies users with an encryption string or hexadecimal keys. You must set up encryption keys on both the client and access point. This option can be used with local access point authentication or with EAP-MD5 RADIUS authentication.

3Com 128-bit Dynamic Security Link Encryption Settings. 3Com's proprietary 128-bit Dynamic Security Link is built into the access point and permits user-level authentication. Users must log in with username and password. Once authenticated, the access point dynamically creates a unique 128-encryption key for the user for that session. Since the access point has a built-in username and password database that support up to 1000 names, encryption keys do not have to be supplied. This option can be used only with local access point authentication.

802.1x RADIUS. The IEEE 802.1X standard specifies a general method for the provision of port-based network access control. It provides an architecture framework for User-RADIUS authentication through an authenticator such as a wireless access point or a switch.

Based on the IEEE 802.1x standard for port-based network access control, standard security protocols such as EAP and RADIUS provide centralized user identification, authentication, dynamic key management and accounting.

The access point supports several authentication methods, including EAP-MD5, EAP-TLS, and serial authentication, each of which enables different levels of authentication and encryption based on the requirements of your site. In addition, it supports RADIUS Accounting per RFC2866: Username, Start time, Stop time, and Packet input/output. When a client is successfully authenticated to a RADIUS authentication server and RADIUS accounting service is enabled, the RADIUS client sends information to the RADIUS accounting server that can generate accounting information and reports.



3Com does not supply RADIUS software or configuration instructions other than what is applicable for access point configuration. Refer to your system administrator for additional third-party software and configuration information. The access point supports any RADIUS server that complies with RFC 2865 and follow the standard EAP, RFC 2284, 2716, 2548.

Using the Wireless 802.1X Agent

The Wireless Authentication Agent lets wireless clients associate with the access point and authenticate with the RADIUS server that resides on the wired network.

Before you can authenticate a PC-based wireless client through your RADIUS server, you must install and run the Wireless Authentication Agent, you will need a copy of the agent on each client computer with a RADIUS server account. Clients that run Windows 95, 98, ME, NT, or 2000 require the 802.1x client tool in order to authenticate to the server.

The Wireless Authentication Agent can be installed from the 3Com Administrator Utilities CD. Clients running under Windows XP have 802.1x support enabled through the operating system and do not require the agent. Although it is not required on Windows XP systems, you may still install and use it. This might be preferred if you want all PC wireless clients at your site to use the same procedures and interface for authentication to your RADIUS server.

Authentication and Login

Once installed, authentication becomes part of the client computer's startup process. At login, it prompts for user name and password. The user name and password must match the user name and password kept by the RADIUS server for that user. The status icon in the system tray monitors the authentication process.

The user can access the authentication agent software from the agent icon in the system tray to log off or log on manually. When a computer is logged off manually, the agent suspends the authentication process until the next login and connection to an access point.

802.1x Client Properties

The Properties window (right-click the agent icon in the system tray) opens the Properties window where you can configure the agent for the type of authentication the client should use.

The checkbox at the top enables access control using 802.1x. This function must be enabled for the authentication to work. If this box is unchecked, the remainder of the window is grayed out.

Use the Network Adapter field to select the network adapter to use for connections requiring authentication. The list box lists all the network adapters found in the computer.

Use the Authentication Method field to specify the authentication method used for this connection. The Wireless Authentication Agent supports two types of authentication:

- EAP MD5
- EAP Serial Authentication

This option is used for connections using 3Com wireless LAN PC cards. If the user selects EAP Serial Authentication, the agent checks whether a suitable card is used for the network connection. If not, it reports an error.

4

MANAGING THE WIRELESS LAN

Overview

If your 3Com wireless lan has only one access point, a few clients, and no special security requirements, you can use the 3Com 11 Mbps Wireless LAN Access Point 8000 just as it was shipped from the factory. If your network is more complex, you will want to organize access points so that you can maintain a secure network and manage the wireless LAN easily.

These tools help you manage the wireless LAN:

- **3Com Wireless Infrastructure Device Manager**—The Device Manager starts up with a display of the 3Com infrastructure devices on the same network segment as your workstation. You can use this map to locate 3Com wireless LAN devices on the network, select a device, view its properties, and launch the configuration management system.

The Wireless Infrastructure Device Manager can also be installed on a third party wireless client or on a desktop computer connected to the network. See “Installing the Management Device on a Computer” on page 22.

- **3Com 11 Mbps Wireless LAN Access Point 8000 Configuration Management System**—The Configuration Management System resides on the access point and lets you configure that access point through your Web browser. For instructions on accessing this tool, see “Selecting a Device” below.

Starting the Device Manager

Make sure that the 3Com Wireless Infrastructure Device Manager is installed. The device to be configured must be either connected directly to the computer or associating with the wireless network, and it must be connected to power. If you have more than one device connected, make a note of the MAC address of the device you want to select so that you can identify it in the device manager.

To launch the device manager, select *Start / Programs / 3Com Wireless Infrastructure Device Manager / 3Com Wireless Infrastructure Device Manager*.

If you have more than one network adapter installed on your computer, you may be prompted to choose a network adapter. Choose the appropriate adapter and click *OK*.

Selecting a Device

The Wireless Network Tree appears in the 3Com Wireless Infrastructure Device Manager window. The tree lists all WLAN service areas on the network and expands to show the 3Com wireless LAN devices that are associated to each service area. Devices in a different subnet than your computer are identified with

exclamation points (!). You can refresh this display by clicking *Refresh*. You should refresh the display, for example, after you change a device IP address.

- 1 In the Wireless NetworkTree, select the device you want to configure.

If more than one wireless LAN device appears in the tree and you are not sure that you have selected the right one, click *Properties* and check the MAC address to verify that it is the one you want.

- 2 Click *Configure*.

If the selected device is on the same subnet as your computer, the Configuration Management System main page appears in your Web browser. If your workstation and the device are on different subnets, it launches the Pre-IP Configuration Wizard described below.

The following table describes the functions of the buttons in the 3Com Wireless Infrastructure Device Manager window.

Button	Description
Properties	Displays the following properties of the selected device: Device Name, Device Type, wireless LAN service area ID (ESSID), IP Address, Subnet Mask, and MAC Address.
Configure	Launches the Configuration Management System for the selected device. If the selected device is on a different subnet, you are prompted to assign an address on the same subnet as your computer.
Refresh	Scans the network and displays the connected 3Com 11 Mbps Wireless LAN devices.
Choose NIC	If your computer has more than one network interface card installed, allows you to choose which card you want to use.
Close	Closes the device manager window and ends the session.
Help	Launches the device manager help page in your browser.

The Pre-IP Configuration Wizard

The Pre-IP Configuration Wizard lets you specify the IP settings that will be configured on the selected wireless device. It will propose IP address and subnet mask settings derived from the computer to match its subnet. You can accept the suggested settings or change them as required.

If the selected device is on a different subnet, the device manager helps you to assign an IP address on the same subnet as your computer. You may accept the address offered or enter an address and click *Next*. The next window prompts for an administrative password to allow the new IP address to be set. If this is the first time the device is being configured, leave the password field blank and click *Next*. The Configuration Management System main page appears in your Web browser.

The password screen prompts for the administration password for the selected device. When the units are shipped from the factory, there is no administration password and you should leave the password field blank. If an administration password has been set for the device, enter the password and click *Finish*.

Installing the Management Device on a Computer

The device manager can be installed on a third party wireless client or on a desktop computer wired to the LAN.

- 1 Turn on the computer.
- 2 Put the *3Com Administrator Utilities CD* in the CD-ROM drive.
- 3 In the main screen, click *Tools and Utilities*.
- 4 In the next screen, click *Install the Administration Tool*.
- 5 Follow the instructions on the screens to complete the installation.
- 6 After you install it, you can launch the tool by double-clicking the *3Com access point Management* icon on your computer desktop, or, from the Windows Start menu select *Start/Programs/3Com 11 Mbps Wireless LAN Administrator Utilities/3Com access point Management*.

The Wireless Network Tree appears in the Wireless Infrastructure Device Manager window.

Using the Configuration Management System

The Configuration Management System lets you view and modify the configuration settings on individual access points one device at a time.

The software is viewed on your browser (Internet Explorer 5 or higher or Netscape Communicator 6 or higher) as a hierarchical structure of web pages. The left-hand frame contains a navigation tree. You may select which page to view by clicking on the page names in the navigation tree. The corresponding pages are displayed in the right frame of the window.

The Configuration Management System is password protected. If you are starting it for the first time, it asks you to enter and confirm an administrative password. Otherwise, it prompts for the current administration password. You can change the administrative password from the Change Administrative Password page under Tools (see "Change Administration Password" on page 27).



NOTE: Any changes you make on any of the configuration pages must be saved before you leave the page. Otherwise, the settings will revert back to the current settings. New settings are applied to the device as each save operation is completed.

Each page has a question mark icon in the upper right corner that you can use to find help on the contents of that page.

System Configuration

The system configuration parameters are concerned with high-level network management, including:

- Access point properties
- Network properties
- Data transmission properties

Access Point Properties

The Access Point Properties screen displays the properties of the selected access point. You can change properties by entering values in the fields and clicking the radio buttons (see the following table). When you are finished, click *Submit*.

The following table describes the properties.

Property	Description	Default Value
Device Name	This name appears in the Known Access Points List window. You can change the default name to one of your choice.	3ComAccessPoint_xxxx (where xxxx is the last four hex digits of the MAC address)
Device Location	Optionally, you can enter the location of the access point.	None
WLAN Service Area	To enable clients to roam among multiple access points, the access points must have identical WLAN service areas. To maintain wireless association, the WLAN service area on the client and the access point with which it is associated must match exactly. Therefore, if you are associated with the access point that you are configuring and you change the access point WLAN service area, make sure to change the client WLAN service area also.	3Com Wireless Network
Help File Location	<ul style="list-style-type: none"> ■ Web Server: Help files are located on the network at the specified Help File Path. ■ Local Drive: Help files are located on your computer at the specified Help File Path. 	Local Drive
Help File Path	The location of the Configuration Management System help files on the web server or on the local drive.	D:\WLAN?APHELP

Network Properties

The *Network Properties* screen appears, where you can change the settings shown in the table below.

Setting	Description
Access Point Network	<p>This setting lets you change the IP address of the access point.</p> <p>To let the access point get an IP address automatically from a DHCP server, click <i>Obtain an IP address automatically</i> and click <i>Save</i>.</p> <p>To specify an IP address, click <i>Specify an IP address</i>, enter the IP address parameters in the spaces provided, and click <i>Save</i>.</p> <p>If you change the IP address, you cannot continue to configure the access point using the old IP address. Therefore, if you want to continue configuring this access point after you save this change, you must do the following:</p> <ol style="list-style-type: none"> 1 Close your browser. 2 Return to the device manager Wireless Network Tree and click <i>Refresh</i>. 3 Select the access point and click <i>Configure</i> to start a new configuration session. <p>When you specify an IP address, the access point cannot act as a DHCP server. Make sure that clients are using IP addresses on the same network.</p>

Setting	Description
Wireless DHCP Server	<p>If your wired network has a DHCP server, it is recommended that you use it. However, the access point provides a DHCP server so that operating systems that do not support automatic IP addressing can communicate with it.</p> <p>The access point's default IP address is 169.254.xxx.1, where xxx is the last two bytes of the access point's MAC address. When it is acting as a DHCP server, the access point can assign up to 253 IP addresses to currently associated wireless clients. The IP addresses range from 169.254.xxx.2 to 169.254.xxx.254.</p> <p>If the access point detects that another DHCP server is available, all wireless clients get IP addresses from that DHCP server.</p> <p>If your wired LAN DHCP server goes down, the access point assigns IP addresses after the lease periods on the previous IP addresses expire.</p> <p>To let the access point act as a DHCP server when there is no other DHCP server available, click <i>Enable</i> and click <i>Save</i>.</p> <p>To turn off the access point DHCP server capability regardless of whether or not another DHCP server is available, click <i>Disable</i> and click <i>Save</i>.</p>
Gateways	<p>You can specify up to three additional gateway IP addresses. These settings are optional. (Only the default gateway is required).</p>

Data Transmission Properties

The Data Transmission Properties screen lets you select radio channel settings and performance settings.

- **Auto Channel Select**—To allow the access point to find a channel automatically, click the *Automatically select the best channel* radio button.

When this option is enabled, the access point scans the primary channels to determine the traffic on those channels and chooses the channel with the least number of packets.

 - If you are using a high-gain antenna such as the optional flat-panel directional antenna (model 3CWE498) in France or Singapore, you must manually select from channels 10–13. See “Data Transmission Properties” on page 24 for information on manually selecting radio channel settings.
 - The access point will select between channels 1–13. If your network supports clients that do not acknowledge 13 channels, you will have to manually select a channel within the reach of those clients. For example, if you have clients that only support channels 1–11

To select a specific channel, click the *Specify the channel* check box and choose a channel from the *Channel* list.
- **Network Traffic Accelerator**—To increase performance, click *On (Enhanced performance)*. If you experience problems when equipment other than 3Com 11 Mbps Wireless LAN equipment is being used, click *Off*.
- **Data Preamble**—To increase performance, click *Short (Enhanced performance)*. When equipment that does not support short preamble is also being used, click *Long*.
- **Data Rate**—These settings configure the data rates used for wireless transmissions. By default, the access point selects the best data rate for the current connection.

 - If “Automatically set the best data rate” is selected, the Data Rate cannot be selected manually.

- If “Manually set the data rate” is selected, the 5.5Mbps and 11Mbps options become active. You may not alter the settings for the 1Mbps and 2Mbps rates since these rates must always be available to transmit certain types of wireless traffic.

The data rates may either be Required or Optional. When the data rate is set to Optional, the AP determines if it is appropriate to use that data rate or if the signal strength requires a lower data rate to be used. If the data rate is set to Required, the AP does not have the option to modulate to a lower data rate, and may lose connection with signals that cannot support the higher data rate.

- **Beacon Period**—The beacon period sets the amount of time between beacons sent out from the AP.
- **Radio Antenna**—These settings determine whether the radio will use one or two antennas. If the user attaches an external antenna, this parameter should be set to Diversity Off. Generally, if the radio is using the built-in antennas, this parameter should be set to Diversity On to maximize the transmission and reception qualities of using both antennas.

Transmit Power—You can adjust the transmit power between High, Medium, and Low. These settings may need to be adjusted for compatibility with different types of external antennas that have different gains. These adjustments may be required to be legally compliant with the communications regulations in certain countries. For example, if you are using a high-gain antenna such as the optional flat-panel directional antenna (model 3CWE498) in the United States, Canada, Mexico, Argentina, Brazil, Taiwan, Malaysia, New Zealand, Colombia, India, and Peru, no transmit power restrictions apply. If you are using it in any other country, however, you must manually select Low or Medium power.

Security

In addition to providing wireless encryption, access point security can be integrated with upper layer authentication provided by a RADIUS server on the wired LAN using IEEE 802.1X support. (For a description of security settings, see the chapter on Access Point Security.) The Security screens let you manage these features for each access point.

AP Encryption

The Security Setup page lets you select the type of security to be used on the access point. The access point can be configured to support one type of security at a time. You can change the settings by entering values in the fields and clicking the radio buttons. If you use shared keys, you must enter all the keys, then click a radio button to specify which key to use.

The following table describes the settings. To maintain wireless association, the settings on clients and all the access points they associate with must match exactly.

Setting	Description
No Security (Open System)	No encryption is used. The network communications could be intercepted by unintended recipients.
40-bit Shared Key (Wi-Fi)	<p>This option encrypts the wireless transmissions to protect data, but still permits communication among compatible wireless LAN clients and access points from third-party manufacturers.</p> <p>This type of security requires you to set up encryption in one of the following ways:</p> <ul style="list-style-type: none"> ■ An encryption string is a string of characters between 6 and 30 characters long. The string can be any combination of letters and numbers and is case sensitive. The encryption string can be used only with other 3Com 11 Mbps wireless PC Cards and AccessPoints. ■ Hexadecimal keys are sequences of hexadecimal digits arranged into four keys. A hexadecimal digit may be a letter from A to F or a number from 0 to 9. This type of encryption is compatible with equipment from other manufacturers that use Wi-Fi certified 40-bit encryption.
128-bit Shared Encryption Key Settings.	This option is compatible with 128-bit shared key including from other vendors, including AirConnect, Agere, and Cisco. The network administrator sets up encryption keys for the wireless network and supplies users with an encryption string or hexadecimal keys. You must set up encryption keys on both the client and access point.
128-bit Dynamic Security Link	<p>This is the highest level of security, requiring a user name and password to access the wireless LAN. The user name and password set up on the access point must match those set up on the client. Each network session creates a unique, one-time encryption code. If you choose this type of security, you must also set up access control as described in "User Access List" on page 25.</p> <p>If you check the <i>Require Windows user authentication</i> check box, clients will be required to enter a user name and password every time they associate with the network. If you leave this box unchecked, the system will authenticate clients based on the access control list and the saved passwords on the clients.</p>

User Access List If you configure an access point for 128-bit Dynamic Security Link, there must be at least one entry in the User Access List. The User access List determines which users are allowed access to the access point. You can define up to 1000 users.

To modify a password, click *Change User Password*. Select the user name and click *Change user password*. In the next page, change the password in the spaces provided and click *OK*. If you click *Reset*, the radio button is cleared and you can choose another user name.

RADIUS Authentication and Accounting

The RADIUS Authentication/Accounting screen lets you define the servers to be used for RADIUS authentication and accounting functions. You must set up authentication and accounting parameters if you plan to enable any type of RADIUS authentication as configured on the Encryption page. These include primary authentication and dynamic key exchange servers, along with primary and secondary accounting servers as required. If you enter an invalid IP address for any of the servers, an error message is displayed.

Once an accounting server is set up, you can turn accounting on or off from this screen. If the servers are set up and accounting is turned off, the settings remain saved.

Management

The Management pages let you configure the access point for use with third-party SNMP management programs and specify the TFTP server you will use for various administrative functions, including backing up and restoring access point settings and setting up the access point system log.

SNMP Management

The SNMP Management screen lets you set up the configuration for using the access point in conjunction with third-party SNMP management programs. From this page, you can:

- Modify the Read Only or Read Write community names. Activation of either Modify button displays the corresponding page where the community names can be set.
- Identify one or two host machines to receive SNMP traps.
- Identify which traps to send to the trap host or hosts.

TFTP Setup

A TFTP server must be set up in order to perform firmware updates, backups, and restores. The TFTP Setup screen identifies the TFTP server that will be used. If you do not have a TFTP server, you can install the one shipped with the access point. Use the 3Com Administrator Utilities CD (Tools and Utilities options) to start the 3CDAEMON and install the TFTP Server Tool.

You must supply the IP address of the TFTP server computer. The default TFTP client port number is 69, the TCP/UDP port number that is most commonly used for TFTP, although you can change this to a different port number if required.

System Log Setup

The System Log screen lets you set up one or two computers for saving log files and to enable or disable logging. Log files are not viewable through the Configuration Management System or the access point, and so must be accessed from the host computer.

By default, logging is off. If you turn on logging, you must specify at least one host. You must also enter the TCP/UDP port number that will be used for sending the log information from the access point to the host systems using syslog. By default, the port is set to 514, the TCP/UDP port number that is most commonly used for syslog, although you can change this to a different port number if required.

When logging is enabled, log information is saved until the function is turned off.

Tools

Use the Tools options to upgrade access point firmware and change the administration password.

Upgrade System

You can download firmware updates or updates of the Web server file system (the files that make up the Configuration Management System) from the 3Com Web site at <http://www.3com.com> and install those updates on the access point. To perform a firmware upgrade, you must have user "Anonymous" defined with no password.

To avoid problems that could occur if a wireless association were interrupted during the upgrade, it is recommended that you perform the upgrade from a computer that is wired to the LAN.



If you upgrade both the firmware and the Web server file system, be sure to upgrade the Web server file system first.

Downloading Upgrade Files

To locate upgrade files and download them to your computer:

- 1 Log on to the 3Com Web site at <http://www.3com.com>.
- 2 Navigate to the product support page.
- 3 Navigate to the software download page and locate the files you want to download.
- 4 Follow the instructions to download the files into a directory on your computer.
- 5 Copy or move the files to the TFTP server upload/download directory.

Installing an Upgrade

- 1 In the Configuration Management System navigation tree under Tools, click *Upgrade System*.
- 2 Select the items to upgrade:
To upgrade the Web server file system, click the *Web Server File System* check box.
To upgrade firmware, click the *Access Point Firmware* check box.
- 3 Enter the upgrade file names that you downloaded earlier and click *OK*.
If you choose the wrong file, click *Clear Entry*. The selected file is cleared and you can browse again for a different file.
- 4 Click *Upgrade*.

The upgrade file is copied from the TFTP server to the access point and the access point restarts using the new upgrade.

Change Administration Password

In the Configuration Management System navigation tree under Tools, click *Change Administration Password*. The Change Administration Password screen appears, where you can change the password for the access point. Enter the current password and new password in the spaces provided and click *OK*.

Configuration Backups

Access Point configurations can be saved as data files and later used to restore the access point configuration. The Backup Configuration screen lets you save access point settings in an external file. (You must have a TFTP server set up on which to store the backup file. This is the server specified on the TFTP setup page.

When you back up a configuration, you must supply the name of the file that the configuration is saved to. This file will be written to the upload/download directory of the TFTP server. If you need to change the TFTP configuration, click the Change button to open the TFTP Setup screen.

Use the Restore Configuration screen to restore settings from a previously saved backup file to the current access point. If you select All Configuration Settings, the saved configuration is restored completely.

If you select Only Template Settings, only general configuration parameters such as WLAN service area, data transmission settings, security settings, RADIUS server settings, and management setup information are restored. Template settings would be used in common by several access points in a network and provide an easy way to reconfigure all access points in a network, if required. Template parameters do not affect nor overwrite settings unique to individual access points, such as device name, location, IP addresses, and administration passwords.

Statistics

The statistics screens display various categories of operational and performance statistics associated with the access point. The values do not update dynamically, but you can update them at any time by refreshing the display.

If you click on the Start Refresh button, the refresh cycle begins and the values on the screen are updated according to a predefined polling rate.

- **RF Statistics.** Displays performance data for the radio transmissions to and from the access point. The statistics related to transmissions from the access point are listed in the Transmitted table on the left. Statistics related to radio signals received by the access point are listed in the Received table on the right.
- **Ethernet Statistics.** Displays performance data for the wired Ethernet traffic to and from the access point. The statistics related to wired transmissions from the access point are listed in the Transmitted table on the left. Statistics related to Ethernet traffic received by the access point are listed in the Received table on the right.
- **Interface Statistics.** Displays the interface statistics for the access point. The top table displays the interface counts, showing the cumulative packets or frames sent and received and the bytes sent and received over the Ethernet and wireless interfaces. The bottom table displays the rates per second for each of these parameters.
- **Channel Retry Statistics.** Provides statistics for each of the radio channels supported by the access point. For each channel, the table indicates the number of frames sent and received, and the number of retries that have occurred for that channel.
- **Forwarding Counts.** Displays the cumulative number of packets forwarded between the two types of interfaces. The rows represent the source, and the columns represent the destination of the forward.

System Status

In the Configuration Management System navigation tree under System Status, you can view the following information:

- Click *Currently Associated Clients* to see a list of MAC addresses of the wireless clients currently associating with the access point.
- Click *System Summary* to see information about the access point.

From the System Summary page, you can also click *Go to Wireless Details* to see a one-page display of the current wireless configuration settings for the access point.

Restoring an Access Point to Factory Defaults

You can restore access point settings to the defaults that were set at the factory by inserting a pointed object (such as the point of a ball point pen) into the reset hole on the front near the RJ-45 connector and holding for five seconds.

Interoperating with Third-Party Equipment

Because 3Com 11 Mbps Wireless LAN equipment complies with IEEE 802.11 standards, it can interoperate with third-party equipment that also complies with the standards. However, some third party equipment may not support 3Com access point enhanced performance features. You may need to turn off the Network Traffic Accelerator and Data Preamble transmission properties (set to "Long") to support this equipment on the network.

5

CONDUCTING A SITE SURVEY

[This information is currently being revised for another manual. When that document is reviewed and completed, the new Site Survey section will replace this chapter.]

To ensure that you have selected the best location for an access point, conduct a *site survey* before permanently installing the hardware. The 3Com Site Survey utility helps you evaluate locations for access points.

You need the following items to conduct a site survey:

- An access point, power brick, and mounting hardware
- Wireless client with 3Com Administrator Utilities installed

To set up the tests, temporarily install the access point in several trial locations. To set up a wireless client computer with 3Com Administrator Utilities, use the *3Com Administrator Utilities CD* when you install the wireless client.



The Site Survey utility is designed to test one access point at a time. The tool cannot be used with access points from other manufacturers.

Choosing Trial Locations

Look at your site floor plan and make a list of work areas where clients are likely to be positioned. For example, list the office cubicles where users will be logging on to the 3Com Wireless LAN. Then select several trial locations for the access point and make a list of these locations. For example, you may wish to test the access point mounted on the ceiling, on a desk, and on a wall.

Look for locations in the center of the room and away from potential transmission barriers. Consider the following environmental and electrical factors when you choose locations.

Environmental Requirements

Look for installation locations away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment. Avoid areas with excessive moisture, heat, and dust. Signal loss can occur when metal, concrete, interfering metal fire breaks, walls, or floors block transmission. Doorways and passages can also affect the radio signal.

You should also consider the following items:

- If there any radio frequency (RF) systems already in use at the site, their signals could interfere with the access point signals.
- If the access point will be connecting to a wired LAN, the access point must be installed close enough to connect to the hub with an Ethernet cable.
- Available AC power. See “Electrical Requirements” below.

Electrical Requirements

The access point draws power over Category 5 Ethernet cabling using a power brick. Because erratic electrical power can lead to serious transmission problems and loss of data, 3Com recommends using one of the following power alternatives.

- Preferred: Isolated ground circuit with online, uninterruptible power supply (UPS) that also acts as filter and surge suppressor
- Good: Isolated ground circuit with surge suppressor
- Fair: Dedicated circuit with UPS
- Acceptable: Dedicated circuit with surge suppressor

If you must use a nondedicated circuit, avoid using the following types of devices on that circuit, because they can affect the reliability of the circuit:

- Devices with components intended or known to produce heat (such as space heaters, laser printers, heat guns, or soldering irons)
- Single devices drawing more than 20% of the rated value of the circuit
- Multiple devices drawing a total of more than 60% of the rated circuit value



The access point must be powered 24 hours a day. 3Com recommends that you avoid providing power to the access point from an energy management system.

Summary of the Survey Procedure

Following is a summary of the basic procedure for setting up and running the site survey tests. For details, see the topics indicated in the steps.

- Set up the access point in the first trial location and set up a client in the first work area.

See "Setting up Equipment" on page 33.

- Launch the Site Survey tool, configure the site survey, and run the tests from the first work area.

See "Launching the Tool" on page 33, "Configuring the Site Survey" on page 33, and "Running the Tests" on page 33.

- Move the client to the next work area and run the Site Survey tool again.

Repeat this step for each work area.

- Set up the access point in the next trial location and run the Site Survey tool again from each of the work areas.

Repeat this step for each trial location.

- At the end of the testing, use the results from the Site Survey tool to help you decide on the best location for the access point.

Based on the tests, the Site Survey tool lists the locations in descending order from best to worst. For more information, see "Interpreting Test Results" on page 35.

Using the Site Survey Tool

If you have set up more than one access point, make sure that only the access point you are testing is powered on, or make sure that each access point has a unique WLAN Service Area.

Setting up Equipment Place the access point in the first test location and connect it to power.

When the access point receives power, the LEDs light.

Place the wireless client computer in the first test location and turn on the computer. Make sure the client has 3Com Administrator Utilities installed and that it is associating with the access point that you want to test.

Launching the Tool Launch the Site Survey tool as follows:

- 1 In the Windows system tray, click the 3Com icon to display the 3Com WLAN Launcher.

If the 3Com WLAN Launcher is not already running, you can start it from the Windows Start menu. Select *Start/Programs/3Com WLAN Launcher*.

- 2 In the 3Com WLAN Launcher, click the *Hammer* icon to display the 3Com WLAN Configuration Utility window.

- 3 In the Tools window, double-click the *Site Survey* icon.

The 3Com 11 Mbps Wireless LAN Site Survey window and the Site Survey dialog box appear.

Configuring the Site Survey In the Site Survey Configuration dialog box:

- 1 Verify that the test access point is listed in the Current AP field.

The Current AP field lists the access point MAC address and its WLAN service area. If you need to change the access point, click the ellipsis (...) to bring up the Network/Security window, where you can select a different WLAN service area.

- 2 Select the tests to perform:

Ping Currently Associated AP—Finds the average round trip value (in milliseconds) of a ping to the access point.

Throughput (UDP Test)—Finds the value (in kilobytes per second) of a transmission between the client and the access point. This value is only meaningful for the test; it does not reflect throughput with a network.

For the most accurate results, select both tests.

- 3 Click *OK*.

Running the Tests In the 3Com 11 Mbps Wireless LAN Site Survey window:

- 1 In the AP Test Location field, type the location of the access point. For example, if you are testing the access point located on a desk, type **Desk**.

- 2 In the PC Test Location field, type the location of the wireless client. For example, if you are in office number 1, type **Office1**.

- 3 From the Run menu, select *Start Test*.

The tests take a few moments to run. When they are finished, the results appear in the window. For details on the information that is presented, see "Interpreting Test Results" on page 35.

- 4 Optionally, save the test: From the File menu, select *Save*. Name the test and save it in the location of your choice. The Site Survey tool appends the characters *.ssf* to the file name.
- 5 Move the client to the next test location and perform the next test:
 - a If you previously saved the test, open it: From the File menu, select *Open*. Select the saved test, and click *OK*.
 - b In the PCTest Location field, type the new location of the wireless client. For example, if you are in office number 2, type **Office2**.
 - c From the Run menu, select *Start Test*.

The tests take a few moments to run. When they are finished, the results appear in the window.
- 6 Repeat the tests in all of the client test locations. Specify a unique name for each client test location.
- 7 When you are finished testing the first access point location in all of the client test locations, place the access point in the next location, power it up, and repeat the tests from the same client test locations. Repeat this process for all access point locations. Make sure that you specify a new name for each access point location, and that you use the same set of client test locations for each access point location.

At any time during the testing, you can save the current set of tests, start a new set of tests, and print test results. For a description of the commands available in the utility, see “Site Survey Menus” on page 36.

Interpreting Test Results

As you run the tests, the Site Survey utility keeps track of results and builds a list of access point locations rated from best to least desirable. In the 3Com 11 Mbps Wireless LAN Site Survey window you see the following information:

- **Rated AP Test Locations**—This list of access point locations appears in the left-hand pane of the window, and is sorted from best to least desirable, based on the test results in the right-hand pane.
- **AP Test Location**—This column lists access point locations associated with client test locations listed in the PC Test Location column. You can sort this list in ascending or descending order by clicking the AP Test Location column head.
- **PC Test Location**—This column lists client test locations associated with access point locations listed in the AP Test Location column. You can sort this list in ascending or descending order by clicking the PC Test Location column head.
- **Throughput**—This column lists the throughput in kilobytes per second for each pair of access point and client test locations. Larger numbers indicate better throughput. You can sort this list in ascending or descending order by clicking the Throughput column head.
- **Avg Ping RTT**—This column lists the average time it takes for a ping to travel round trip from the client to the access point, in milliseconds. Smaller numbers indicate faster ping rates. You can sort this list in ascending or descending order by clicking the Avg Ping RTT column head.

The Site Survey utility recommends access point locations based purely on the test numbers. You can use the recommendations to guide your decision about access point locations. For example, you may decide, based on factors such as where users will most often be located or your own special knowledge about the test results, that a location other than the most recommended is the best for your site.

Site Survey Menus

The following tables describe the command menus in the 3Com 11 Mbps Wireless LAN Site Survey window.

Table 2

File	
New Survey	Start a new set of tests.
Open	Open a set of tests that you saved previously.
Save	Save the current set of tests.
Save As	Save the current set of tests with a new name.
Print	Print the current set of test results.
Print Preview	Show a preview of how the printout will look.
Print Setup	Set up the print page.
Exit	Exit the Site Survey utility.

Table 3

Edit	
Delete Selected Items	Deletes the currently selected row from the right hand pane.
Delete All From List	Deletes all test results in the current survey.

Table 4

View	
Tool Bar	Make the tool bar visible or invisible.
Status Bar	Make the status bar visible or invisible.

Table 5

Run	
Start Tests	Start the tests for the current AP Test Location and PC Test Location.

Table 6

Help	
Help	Displays help for the site survey tool.
About Site Survey	Displays information about this version of the site survey tool.

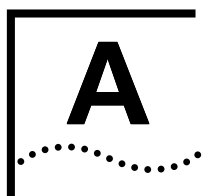
6

TROUBLESHOOTING

If you have difficulty with the access point, try the solutions in the following table.

Symptom	Solutions
Access point does not power up.	Make sure the Ethernet cable is plugged into the port labeled <i>To Access Point</i> on the power brick. Check for a faulty access point power supply. Check for a failed AC power supply
No operation.	Verify the access point configuration. Review access point firmware revisions and update firmware if necessary. Make sure that there are no duplicate IP addresses on the network. Unplug the access point and ping the assigned address to make sure that no other device responds to that address.
Access point powers up, but has no connection to the wired network.	Make sure that the Ethernet cable is plugged into the port labeled <i>To Hub/Switch</i> on the power brick. Verify the network wiring and topology for proper configuration. Check that the cables used are the proper type.
Access point powers up, but does not associate with wireless clients.	Confirm that the WLAN service area on the access point matches that on the clients. Verify that the clients are operating correctly. Make sure that security settings on the access point match those on the clients. Make sure that the access point antennas are positioned properly. Check the range and move clients closer if necessary.
Slow or erratic performance.	Try changing the wireless channel on the access point. Check the access point antennas, connectors, and cabling for loose connections. Check the wired network topology and configuration for malfunctions.
Running on a computer connected to the wired LAN, the access point device manager cannot find an access point.	The access point cannot discover devices across routers. Make sure that the computer is connected to the same network as the access point.

Symptom	Solutions
While you are configuring the access point, the Configuration Management System stops responding.	<p>To maintain wireless association, the WLAN service area on the client and the access point with which it is associated must match exactly. Therefore, if you are associated with the access point that you are configuring and you change the access point WLAN service area, make sure to change the client WLAN service area to match.</p> <p>If you change the IP address and save the change, you cannot continue to configure the access point using the old IP address. Therefore, if you want to continue configuring this access point after you save this change, you must do the following:</p> <ol style="list-style-type: none"> 1 Close your browser. 2 Return to the device manager Wireless Network Tree and click <i>Refresh</i>. 3 Select the access point and click <i>Configure</i> to start a new configuration session.
After you specify an IP address for an access point, the device manager continues to point to the old IP address when you select the access point in the Wireless Network Tree.	In the Access Point Management window click the <i>Refresh</i> button to refresh the Wireless Network Tree. Then click the access point in the Wireless Network Tree and click <i>Properties</i> . The IP address you specified is now listed. If you want to continue configuring the access point, click <i>Configure</i> .
Your wired LAN DHCP server malfunctions, but the access point DHCP server fails to assign IP addresses.	If the Wireless DHCP Server property on the access point is enabled, the access point assigns IP addresses after the lease periods on the previous IP addresses expire. If you want to force the access point to start assigning IP addresses before the lease periods expire, unplug the access point from the power source and plug it back in to reboot it.
The access point stops assigning IP addresses after you assign it an IP address.	Set the access point to obtain an IP address automatically. It cannot act as a DHCP server when it has an assigned IP address.
PC Cards other than 3Com 11 Mbps Wireless LAN PC Cards cannot communicate with the access point.	The cards may not support the access point's enhanced performance features. Try turning the Network Traffic Accelerator and Data Preamble transmission properties (set to "Long") off.



TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site enter this URL into your Internet browser:

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

This service provides access to online support information such as technical documentation and software library, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **<http://knowledgebase.3com.com>**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**



You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, call the 3Com technical telephone support phone number at the location nearest you.

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

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers. These numbers are correct at the time of publication. Refer to the 3Com Web site for updated information.

Country	Telephone Number
Asia, Pacific Rim	
Australia	1 800 678 515
Hong Kong	800 933 486
India	+61 2 9242 5179 or 000800 6501111
Indonesia	00 531 616 439
Japan	03 5783 1270
Malaysia	1800 801 777
New Zealand	0800 446 398
Pakistan	+61 2 9937 5083
Philippines	1235 61 266 2602
P.R. of China	10800 61 00137 or 021 6350 1590 or 00800 0638 3266
Singapore	800 6161 463
S. Korea	02 3455 6455 or 00798 611 2230
Taiwan, R.O.C.	0080 611 261
Thailand	001 800 611 2000

Or, send a description of the problem by email to: apr_technical_support@3com.com

Country	Telephone Number
Europe, Middle East and Africa	
From anywhere in these regions, call:	+44 (0)1442 435529 phone +44 (0)1442 436722 fax
Europe and South Africa	
From the following countries, you may use the toll-free numbers:	
Austria	0800 297468
Belgium	0800 71429
Denmark	800 17309
Finland	0800 113153
France	0800 917959
Germany	0800 1821502
Hungary	06800 12813
Ireland	1800 553117
Israel	1800 9453794
Italy	800 8 79489
Luxembourg	0800 23625
Netherlands	0800 0227788
Norway	800 11376
Poland	00800 3111206
Portugal	0800 831416
South Africa	0800 995014
Spain	900 983125
Sweden	020 795482
Switzerland	0800 55 3072
U.K.	0800 966197
Latin America	
Brazil	0800 13 3266
Mexico	01 800 849CARE
Puerto Rico	800 666 5065
Central and South America	AT&T +800 998 2112
North America	
	1 800 NET 3Com (1 800 638 3266)
	Enterprise Customers: 1 800 876-3266

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense. To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+65 543 6500	+65 543 6348
Europe, South Africa, and Middle East	+31 30 6029900	+31 30 6029999
Central and South America	525 201 0075	
Argentina	0810 222 3266	
Bolivia	511 241 1691	
Brazil	0800 133266 or 55 11 5643 2700	
Caribbean	525 201 0004	
Chile	562 240 6200	
Colombia	525 201 0004	
Ecuador	525 201 0004	
Mexico	525 201 0004	
Paraguay	525 201 0004	
Peru	511 241 1691	
Uruguay	525 201 0004	
Venezuela	525 201 0004	

From the following countries, you may call the toll-free numbers; select option 2 and then option 2:

Austria	0800 297468
Belgium	0800 71429
Denmark	800 17309
Finland	0800 113153
France	0800 917959
Germany	0800 1821502
Hungary	06800 12813
Ireland	1800553117
Israel	1800 9453794
Italy	800 879 489
Netherlands	0800 0227788
Norway	800 11376
Poland	00800 3111206
Portugal	0800 831416
South Africa	0800 995014
Spain	900 983125
Sweden	020 795482
Switzerland	0800 55 3072
U.K.	0800 966197
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266)

Enterprise Customers:
1 800 876 3266

INDEX

Numbers

- 128-bit Dynamic Security Link 25
- 3Com Knowledgebase Web Services 39
- 3Com Wireless Infrastructure Device Manager 19
- 40-bit Shared Key (Wi-Fi) security 25

A

- access point
 - IP address 22
 - changing 22
 - DHCP server 23
 - troubleshooting 38
 - LEDs 10
 - restoring factory defaults 29
- adapter, choosing 20
- administration password, changing 27
- administration tool 19

B

- bridge
 - configuring 20

C

- changing passwords
 - administration 27
 - user 25
- choosing a NIC 20
- circuit, nondedicated 32
- Configuration Management System 20
- Configure button 20

D

- device manager 19
 - launching 19
- DHCP server 23, 38
- Dynamic Security Link 25

E

- electrical considerations 32
- encryption
 - string 25

F

- firmware upgrade 27
 - access point 27

G

- guidelines, security 25

H

- hexadecimal keys 25

I

- installation
 - access point 5
 - firmware
 - access point 27
- interoperating with third-party equipment 29
- IP address
 - DHCP server 23
 - refreshing after changing 20
 - specifying 22
 - troubleshooting 38

L

- launching the device manager 19
- LED
 - access point 10
- locating devices 19, 20

M

- MAC address, use in locating devices 19, 20

N

- network supplier support 40
- NIC, choosing 20
- No Security 25
- nondedicated circuit, recommendations 32

O

- online technical services 39
- open system 25

P

- password
 - changing administrator 27
 - changing user 25
- PC Card
 - third party 29
- power, 24-hour requirement 32

- Properties button 20

R

- Refresh button 20
- restoring access point settings to factory defaults 29
- returning products for repair 42

S

- security
 - 128-bit Dynamic Security Link 25
 - 40-bit Shared Key (Wi-Fi) 25
 - guidelines 25
 - no security 25
- server, DHCP 23
- site electrical considerations 32
- site survey 31

T

- technical support
 - 3Com Knowledgebase Web Services 39
 - network suppliers 40
 - product repair 42
 - third-party interoperability 29
- troubleshooting 37
 - access point firmware 27

U

- upgrading
 - access point firmware 27

W

- wireless network tree 19
- World Wide Web (WWW) 39

REGULATORY COMPLIANCE INFORMATION

FCC RADIO-FREQUENCY EXPOSURE NOTICE

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

This product does not contain any user serviceable components. Any unauthorized product changes or modifications will invalidate 3Com's warranty and all applicable regulatory certifications and approvals. This product must be installed by a professional technician/installer.

FCC PART 15 NOTICE (APPLICABLE TO USE WITHIN THE USA)

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

WARNING: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from the one which the receiver is connected to.
- Consult the dealer or an experienced radio/TV technician for help.

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

The Interference Handbook

This booklet is available from the U.S. Government Printing Office, Washington, D.C. 20402. Stock No. 004-000-00345-4.

MANUFACTURER'S DECLARATION OF CONFORMITY

3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA 95054-8145
(408) 326-5000

Declares that the product:

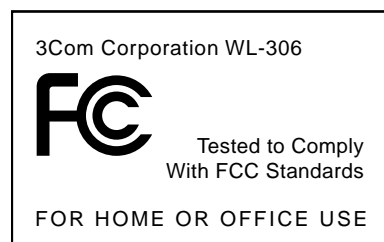
Date: 13 November 2001

Brand Name: 3Com Corporation

Model Number: WL-306

Equipment Type: Wireless LAN Access Point

Complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



INDUSTRY CANADA NOTICE (APPLICABLE TO USE WITHIN CANADA)

This Class B digital apparatus complies with Canadian ICES-003.

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

AVIS DE CONFORMITÉ À LA RÉGLEMENTATION D'INDUSTRIE CANADA

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, cet appareil doit être utilisé à l'intérieur seulement et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal.

**EUROPEAN COMMUNITY - CE
NOTICE**

Marking by the symbol:



indicates compliance with the essential requirements of Directive 73/23/EC and the essential requirements of articles 3.1(b), 3.2 and 3.3 of Directive 1999/5/EC. Such marking is indicative that this equipment meets or exceeds the following technical standards:

- EN 300 328-2 - Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques
- ETS 300 826 - Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for 2,4 GHz wideband transmission systems and High Performance Radio Local Area Network (HIPERLAN) equipment
- EN 60950 - Safety of information technology equipment, including electrical business equipment.

SAFETY COMPLIANCE NOTICE

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

- UL Standard 1950 / CSA C22.2 No. 950
- IEC 60950
- EN 60950

Published February, 2002

User Guide Version 1.0.1