3Com Wireless 7760
11 a/b/g PoE Access Point

3CRWE776075 / WL-561

www.3Com.com
10015003 Rev. AA
March 2006

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

Copyright © 2006, 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, 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, contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

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

All technical data and computer software are commercial in nature and developed solely at private expense.

Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

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

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

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

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

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

ENVIRONMENTAL STATEMENT

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

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

Conserving energy, materials and natural resources in all operations.

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

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

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

Improving our environmental record on a continual basis.

End of Life Statement

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

Regulated Materials Statement

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

Environmental Statement about the Documentation

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

Contents

1 **Introduction**
Key Product Features 2

2 **Installing your 3Com Wireless 7760 Access Point**
Unpacking the device 6
Deciding where to place your AP 7
Wall Mounting the Wireless 7760 9

3 **Configuring the Wireless 7760**
Networks with a DHCP Server 12
Networks without a DHCP Server 13
Using the 3Com Installation CD 13
System Status 16
System Configuration 19
Service 33
Syslog function 38
Management 39
Connecting through the Com Port 46
Restoring factory settings 46

A **Troubleshooting**
Diagnosing Problems 47

B **Obtaining Support for your 3Com Product**
Register Your Product to Gain Service Benefits 50
Solve Problems Online 50
Purchase Extended Warranty and Professional Services 51
Access Software Downloads 51
Contact Us 51
Telephone Technical Support and Repair 52

C **End User License Agreement**

Index

1 INTRODUCTION

The 3Com Wireless 7760 11a/b/g PoE Access Point is a high performance access point that allows you to join isolated wired Ethernet networks into a unified wireless local area network (WLAN). The Access Point (AP) supports Wi-Fi Protected Access security standards to provide a higher level of security for network data and communications. The Wireless 7760AP is also fully compatible with IEEE 802.11a, 802.11g, and also 802.11b, so it connects with all existing 802.11b-compliant devices.

Key Product Features

Access Point 7760 —The product operates using 11a or 11g modes. This access point creates an enterprise-class wireless LAN supporting up to 64 simultaneous users.

Security

3Com offers one of the most robust suites of standards-based security on the market today. To protect sensitive data broadcast over the wireless LAN, 3Com supports Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA and WPA2). 3Com strengthens this basic security mechanism with additional security features, including MAC address access control lists, IEEE 802.1x per-port user authentication with RADIUS server authentication support, Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), Wireless Protected Access (WPA) and Extensible Authentication Protocol (EAP) support: EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP.

Performance And Reliability

3Com wireless access point performance features ensure reliable and seamless connections for users wherever they roam. Automatic channel selection automatically finds the least loaded channel for interference-free communication. Auto network connect and dynamic rate shifting keep users connected through a wide variety of conditions by changing to the optimum connection speed as they move through the network.

Manageability

3Com offers a wide range of standards-based management support, from SNMP to 3Com Network Supervisor and HP OpenView for seamless integration with your wired network.

Wireless Infrastructure Device Manager and Wireless LAN Device Discovery tools let you configure parameters, run diagnostics, backup and restore configurations, and monitor performance from anywhere on the network using an embedded web server browser.

With Power over Ethernet (PoE) support, the same Category 5 cable that connects your access point to the data network also provides its power. A single cable installation dramatically improves your choice of mounting configurations because you no longer need to consider AC power outlet locations. PoE support makes it easier than ever to overcome installation problems with difficult-to-wire or hard-to-reach locations.

Wireless Network Standards

Understanding the characteristics of the 802.11a and 802.11g standards can help you make the best choice for your wireless implementation plans.

802.11a

Ratified in 2002, 802.11a operates at the 5GHz band and supports data rates at up to 54Mbps. Because there are fewer devices in the 5GHz band, there's less potential for RF interference. However, because it is at an entirely different radio spectrum, it is not compatible with 802.11b and 802.11g.

The higher spectrum provides about 50m (164ft) of coverage. Consider 802.11a when you need high throughput in a confined space and you are:

- Running high-bandwidth applications like voice, video, or multimedia over a wireless network that can benefit from a five-fold increase in data throughput.
- Transferring large files like computer-aided design files, preprint publishing documents or graphics files, such as MRI scans for medical applications that demand additional bandwidth.
- Supporting a dense user base confined to a small coverage area. Because 802.11a has a greater number of non-overlapping channels, you can pack more wireless devices in a tighter space.

802.11b/g

802.11b and 802.11g both operate in the 2.4GHz band. 802.11b can support data rate up to 11Mbps. 802.11g can support data rate up to 54Mbps. They both support the widest coverage – up to 100m (328ft). It is however, subject to a greater risk of radio interference because it operates in the more popular 2.4GHz band.

Consider 802.11g when you need wider coverage and vendor compatibility and you are:

- Maintaining support for existing 802.11b users and the existing wireless investment while providing for expansion into 802.11g.
- Implementing a complete wireless LAN solution, including Ethernet Adapters, gateways, access points and clients; Wi-Fi certification guarantees compatibility among vendors.
- Providing access to hot spots in public spaces such as coffee shops or university cafeterias.

IEEE 802.3af

The IEEE 802.3af-2003 Power over Ethernet standard defines terminology to describe a port that acts as a power source (PSE) to a powered device (PD). The IEEE 802.3af standard states that power may be delivered by an end-point PSE, using either the active data wires of an Ethernet port or the spare wires, to a powered device. An end-point PSE, such as a Power over Ethernet capable Ethernet switch, may implement either scheme. If a mid-span PSE is used, then the mid-span PSE can only implement power delivery over the spare pairs of the copper cabling and cannot be used to deliver Power over Ethernet over 1000BASE-T connections. It should be noted that even if a device supports both methods of providing power, only one mechanism may be used to deliver power to a powered device.

The first mechanism is to use the data pairs (pins 1, 2 & 3, 6) to transmit power, which is sometimes referred to as "phantom" power. The second power delivery mechanism is to use the unused, from a 10/100BASE-T perspective, pairs (pins 4, 5 & 7, 8) to deliver power that is supported within mid-span power delivery.

2 INSTALLING YOUR 3COM WIRELESS 7760 ACCESS POINT

This chapter contains the information you need to install and set up the Wireless 7760AP. It covers the following topics:

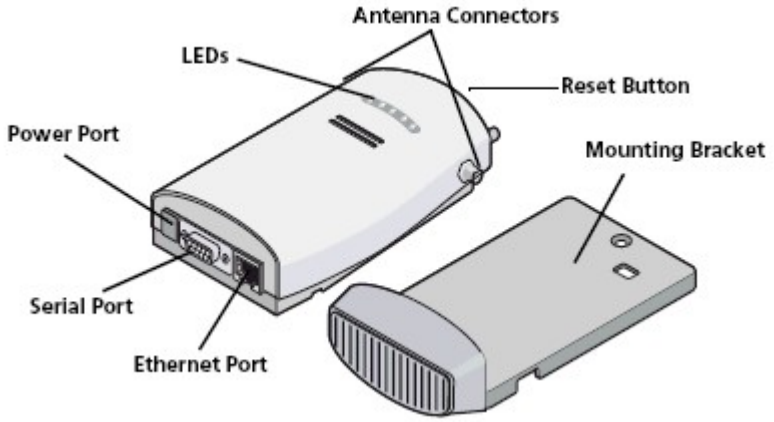
- Unpacking the device
- Decide where to place the AP
- Connecting the Access Point
- Checking the LED indicators
- Attaching an External Antenna
- For first time use -Installing Device Manager

Unpacking the device

Make sure that you have the following items in the box:

- CD
- PoE Injector
- Power cord
- Two external 2.4 GHz and 5.3 GHz dual-band antennas
- Mounting bracket (attached to the access point)
- Wall-mounting hardware:
- Locking bar (used for securing a wall- or ceiling-mounted installation)
- Two sheet metal screws
- Two thread screws
- Two wall anchors
- Four adhesive rubber feet (used for a flat-surface installation).

The Figure below shows the front view of the AP, including the LEDs and connecting ports.



Deciding where to place your AP

Place the AP in a dry, clean location near the hub, switch, computer or printer that will be connected to the AP. The location must have a power source and be within the following distance of a Wi-Fi compliant wireless LAN access point or wireless access point.

The key to maximizing the wireless range is to follow these basic guidelines:

- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise. The location should be away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators.
- Keep the number of walls and ceilings between the AP and other network devices to a minimum - each wall or ceiling can reduce your AP's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal

will travel straight through a wall or ceiling (instead of at an angle) for better reception.

- Building materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

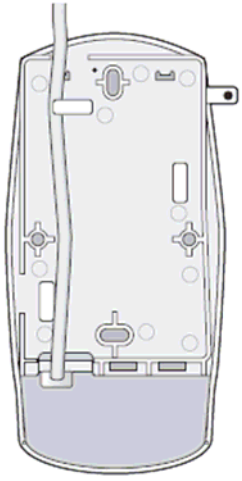
Wall Mounting the Wireless 7760

For convenient positioning the device comes with a cradle that can be wall mounted. For additional security, the Access point also comes with a locking bar, which can be used with a security lock (not provided) to lock the Access point to the cradle after the Access point is mounted to a wall.

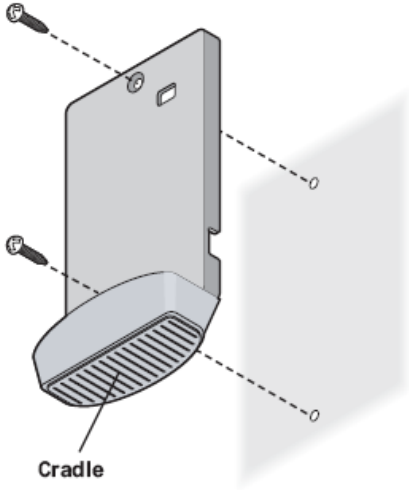
To wall-mount the Access Point:

1. Route Ethernet cable through the large opening in the cradle.
2. Screw the cradle to a wall.

   The figures below show a cable being routed through the large opening in the cradle and then the cradle being mounted to a wall.



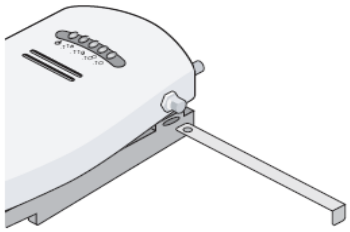
Routing a cable



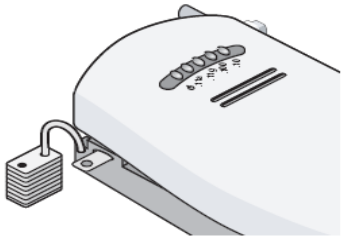
Wall-mounting the cradle

3. Connect Ethernet cable to the port on the front of the access point.
4. Snap the access point onto the mounting bracket.

To install the locking bar, push the locking bar through the opening in the side of the mounting bracket until the hole on the locking bar is exposed. Insert a lock (not provided) through the hole on the locking bar, and then close the lock to secure it in place.



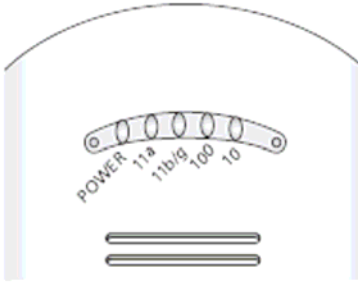
Inserting the locking bar



Securing the bar with a lock

Checking the LED Indicators

When the AP is connected to power, LEDs indicate activity as follows:



LED	Color	Activity	
Power	Green	On:	Power On
		Off:	Power Off
11a	Green	On:	WLAN On
		Blinking:	sending/receiving data from wireless LAN
		Off:	Transmitter is off
11b/g	Green	On:	WLAN On
		Blinking:	sending/receiving data from wireless LAN
		Off:	Transmitter is off
100	Green	On:	Good Link
		Blinking:	sending/receiving data from LAN Port
		Off:	No link
10	Green	On:	Good Link
		Blinking:	sending/receiving data from LAN Port
		Off:	No link

Power up

Self test (POST)

At power up, the product will carry out a self-test (POST). POST will run a test on the wireless circuit to check it is functioning correctly.

When running the POST test, 11a and 11b/g's LEDs will flash alternatively.

When firmware is corrupted, 11a and 11b/g's LEDs will flash alternatively also.

Attaching an External Antenna

This AP comes with two antennas. They are external removable monopole dual-band 2.4 GHz/5 GHz antennas. They can be rotated over 360 degrees and are omni-directional with a gain of less than 2 dBi. The RF connector is an R-SMA type.

If you require a different type of antenna for the Access Point 7760, several options are available from the 3Com (www.3Com.com).

3 CONFIGURING THE WIRELESS 7760

If the default AP configuration does not meet your network requirements, or if you want to customize the settings for your own network, you can use these tools to change the configuration:

1. Launch the 3Com Wireless Infrastructure Device Manager (Widman) utility
2. Directly connect to the device through it's Ethernet port or console port

Networks with a DHCP Server

If your network has a DHCP server, an IP address is automatically assigned to the AP. It takes between one and two minutes for the Access Point to determine if there is a DHCP server on the network. Use the 3Com Wireless Infrastructure Device Manager (Widman) included on the 3Com Installation CD to locate the Access Point on the network and view its IP address.

After you determine the AP's IP address, you can enter that IP address into a web browser on a computer on the same subnet to view the Access Point's system status or change its configuration.

Networks without a DHCP Server

If your network does not have a DHCP server, the Access Point uses a factory assigned IP address (169.254.2.2). You can use that IP address to configure the Access Point, or you can assign a new IP address to the Access Point.

To verify that the Access Point is using the default IP address assigned at the factory:

1. Connect a computer directly to the Access Point using the supplied standard Category 5 UTP Ethernet cable.
2. Enter the Access Point's default IP address (169.254.2.2) into the computer's web browser. If the Configuration Management System starts, the Access Point is using the factory assigned IP address. You can configure the Access Point with the following login information:
   - Login name: admin
   - Password: password

   If the Configuration Management System does not start, the Access Point is on a different subnet than the computer. Install and start the 3Com Wireless Infrastructure Device Manager to discover the Access Point's IP address.

Using the 3Com Installation CD

The 3Com Installation CD contains the following tools and utilities:

3Com Wireless Infrastructure Device Manager—an administration tool that helps you select 3Com wireless LAN devices and launch their configurations in your Web browser.

Launch the 3Com Wireless Infrastructure Device Manager (Widman) utility

1 Turn on the computer.

2 Insert the 3Com Installation CD into the CD-ROM drive.

The CD will Autorun. If it does not Autorun, you can start the setup menu from the Windows Start menu. For example: **Start > Run > d: setup.exe.**

3 In the menu click Tools and Utilities.

4 In the next screen, click the software you want to install.

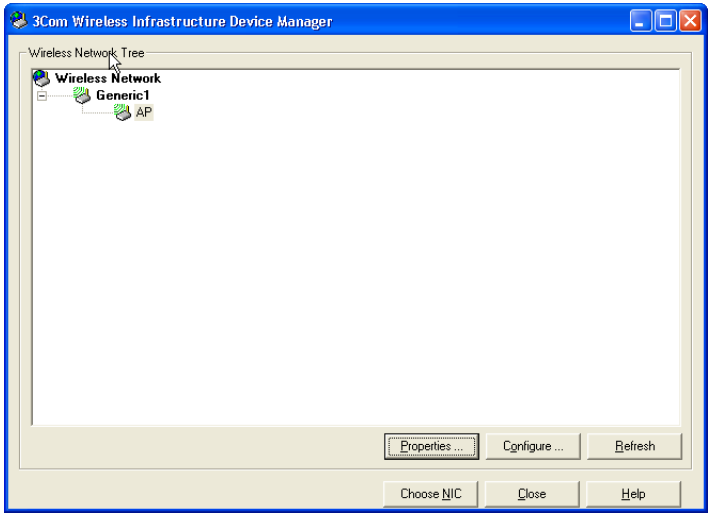
5 Follow the on screen instructions to complete the installation.

Reboot the computer if prompted to do so.

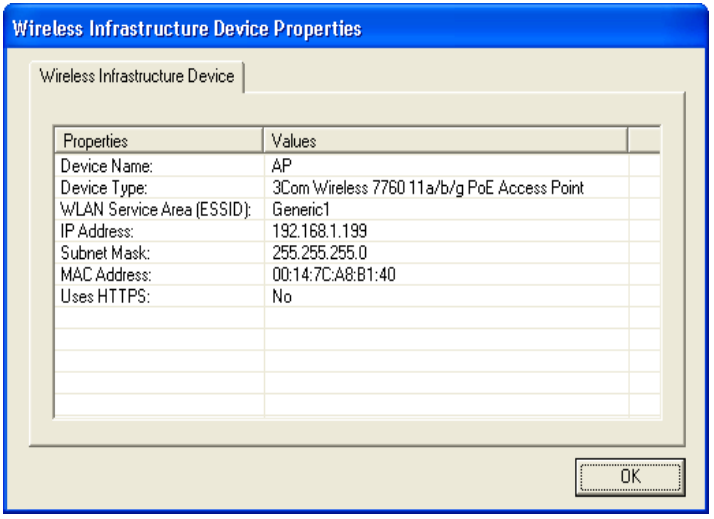
Launching the 3Com Wireless Infrastructure Device Manager

To be able to configure the Access Point you need to run the Wireless Infrastructure Device Manager. Go to **Start** > **Programs** > **3Com Wireless** > **Wireless Infrastructure Device Manager**

If the device is working correctly the following screen should be seen.



Click on the Properties button to see the following screen



Directly connect to the device through its Ethernet port or console port

Follow the instructions below to login into the AP Configuration screen:

1 Load a web browser and enter http://169.254.2.2

2 The Logon screen appears

To log on to the Web interface:

1 Username, type **admin (case sensitive)**

3 Password, type **password**

4 Click **Log On**.

First Time Only

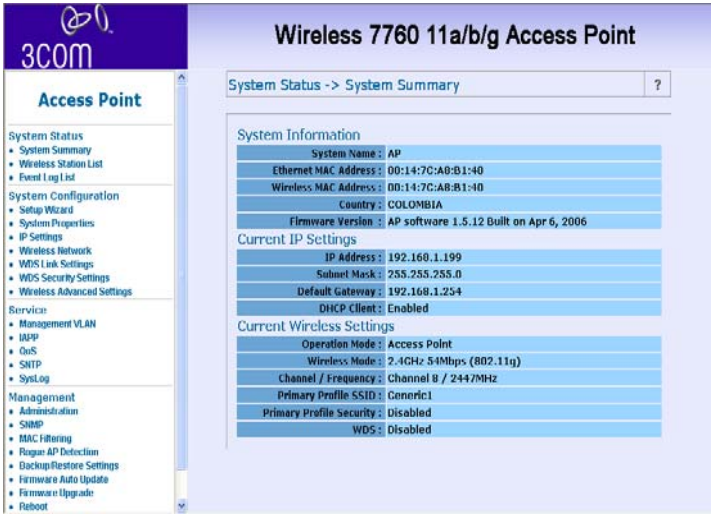
After you have logged in for the first time you will be asked to select your country from the drop down menu.

System Status

The Web interface has been designed to enable you to easily perform advanced configuration tasks and view information about the AP.

System Summary

After you click Logon from the Log On Screen, you'll see the system status page on the screen. The System summary page is the default page that will pop up once you successfully log in. The system summary page shows all the configuration information about your AP.



Wireless Station List Through this page, you can easily identify the adjacent wireless stations. It will automatically observe the adjacent wireless station's ID (if specified), MAC address, SSID and current status.

Event Log List The event log list stores a record of all the events happen within this designated WLAN.

System Configuration

In this section, you will learn how to configure the basic functions of your wireless AP.

Setup Wizard

The setup Wizard will walk you through the setting up of the Office Connect Access Point

Screen 1 allows you to setup the following information:

- **SSID** (Service Set Identifier) – This is the name of wireless network. Input 1-32 characters
- **Wireless Mode** – Choose the required network mode from the drop down menu.
- **Channel/Frequency** – Choose a frequency from the drop down menu or select SmartSelect (recommended) to let the device select a channel.
- Click **Next** to continue the configuration or **click** clear to start again.

Screen 2 allows you to setup the following information:

- **IP Network Setting**- Check the radio button for either obtaining an IP address via DHCP or specifying an IP Address manually.
- **IP Address** – Enter the IP address that you want to assign.
- **IP Subnet Mask** - Enter your networks subnet address.
- **Default Gateway** – If used enter the gateway address that the device should go through.

Screen 3 allows you choose the security settings. Choose the following settings from the drop down menu:

- No security
- WEP
- WPA - Only
- WPA2 - Only
- WPA2 - Mixed

Click **Close** to close without saving, click **Finish** to save the settings, Click **Back** to return to screen 2.

System Properties

The System properties page allows you to define Device name, location, operation modes and Load Type.

There are 5 operation modes to choose from:

Access Point mode

A Wireless LAN data transceiver that uses radio waves to connect a wired network with wireless station.

Wireless Workgroup Bridge mode (Client Bridge mode)

It acts as a wireless client in the network. Through this mode, you can connect to an access point through this device.

Ad-hoc mode (peer to peer)

An Ad-hoc mode allows 2 wireless clients to communicate to each other. An Ad-hoc network is a wireless network composed of stations without Access Points.

Repeater mode

A repeater is placed between two access points to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication.

Wireless Bridge mode

A wireless bridge connects two separate networks operating on the 802.11 standard.

Load Types are either:

FAT

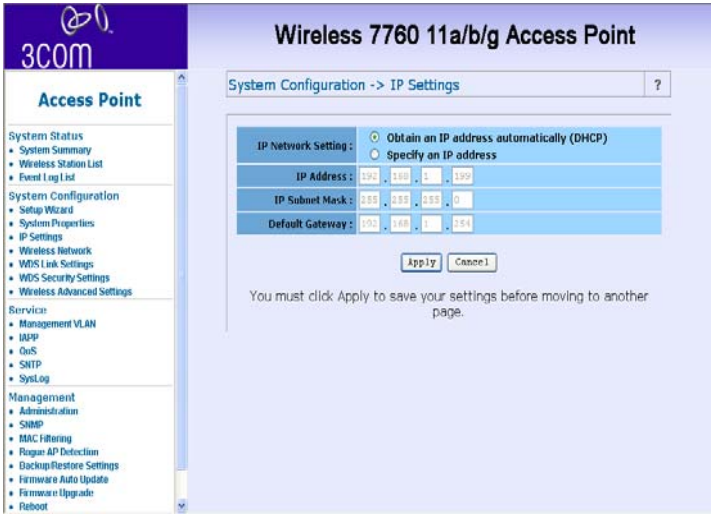
Default is set to be FAT mode AP. FAP AP has complete set of AP features which can work alone as an individual AP.

FIT

FIT mode AP needs to be connected to a 3Com Wireless Switch to provide complete feature sets.

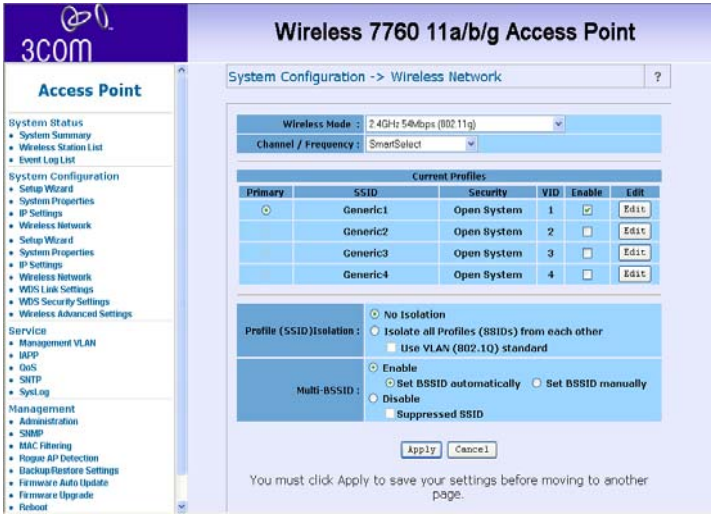
IP Settings This setting must match the network's method of IP address assignment. Choose DHCP or Static IP. With Dynamic Host Configuration Protocol (DHCP), IP addresses are assigned

predetermined for periods of time. Choose Static IP if your network does not have an automatic system for IP address assignment.



Wireless Network

The Wireless 7760 supports Multiple SSIDs which allows it to act as multiple APs appearing in a Wireless LAN network. You can configure up to 4 SSIDs on the device.



Wireless Mode

You can select your desired wireless operating mode from the drop-down manual.

The AP supports *Super Dynamic* and *Static* modes and boosts throughput up to 108 Mbps.

The *Super Dynamic* mode allows automatic switching between normal and turbo modes without modification by the user. The feature increases throughput when bandwidth demands are high. When bandwidth demands are low and at regular intervals, normal mode allows legacy connectivity and new associations. The *Super Dynamic* mode connection between the Ethernet Adapter and the access point may turn to normal mode connection if another station associates with the access point in normal mode. The *Super Static* mode operates by using two radio channels and does not switch to normal mode. *Super Static* mode must be configured by the user on both the access point and the station.

Note that in order to enable Super mode, the opposite client service needs to provide the same specification.

Channel / Frequency

Select the channel for your wireless LAN in Channel/Frequency block. The default setting is SmartSelect it selects the channel which provides the best transmission quality. The frequencies available vary depending which wireless mode you select.

Current Profiles

A maximum of 4 profiles can be configured. Check the **Enable** button to activate a profile. Click the **Edit** button to change its configuration.

SSID

Service Set Identifier. This is the assigned name for a wireless Wi-Fi network. Stations must use this unique identifier to communicate with an Access Point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

BSSID

Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format and can only be edited when Multi BSSID is enabled in the previous screen.

Suppressed SSID

If you want to disable the broadcast of your SSID, you should check the Suppressed SSID box. It also calls SSID Broadcast disable or Hide SSID.

VLAN ID

If your network uses VLANs, you can assign an SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

Station Separation

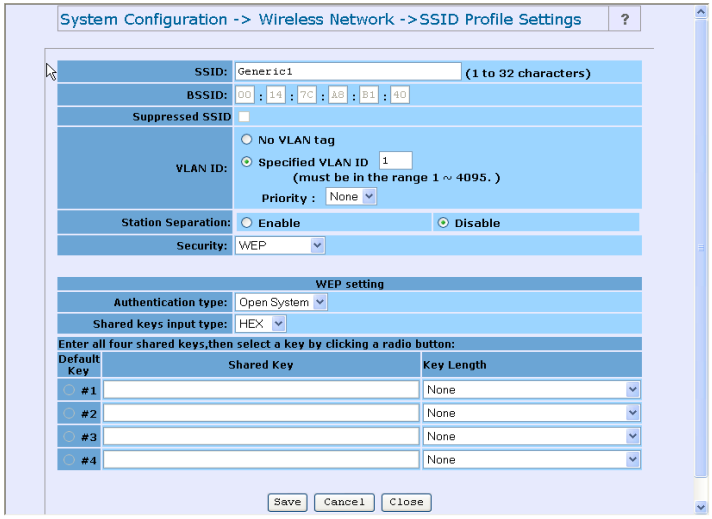
Choose either enable or disable to control the selected VAP (Virtual Access Point).

Security

There are 4 levels of security available and all have differing properties:

WEP

Wired Equivalent Privacy data encryption provides data security. WEP Share Key authentication and WEP data encryption will block all but the most determined hacker.



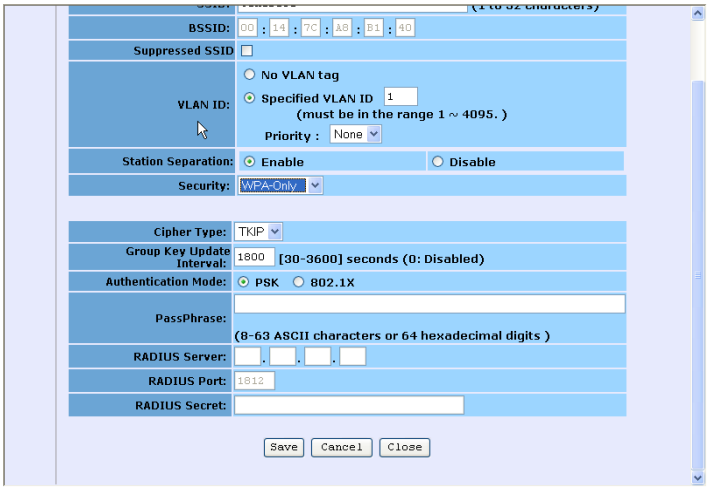
From the drop down list choose open-system or shared key authentication.

Select the desired input method (HEX or ASCII)

From the drop down list choose from 40/64, 104/128, 128/152 key lengths.

WPA Only

Wi-Fi Protected Access was constructed to provide improved data encryption, (which was weak in WEP), and to provide user authentication.



Only allows WPA clients to connect to the VAP.

You can choose TKIP or AES for encryption method

The Group key update interval is configurable, default value is 1800 seconds

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication (default: PSK).

If you choose PSK you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X you will need access to a RADIUS server, port and secret

WPA2-Only

Only allows WPA 2 clients to connect to the VAP.

You can choose TKIP or AES for the encryption method

The Group key update interval is configurable, default value is 1800 seconds

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication (default: PSK).

If you choose PSK you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X you will need access to a RADIUS server, port and secret.

WPA2-Mixed

Only allows both WPA and WPA2 clients to connect to the VAP.

You can choose TKIP or AES for encryption method

The Group key update interval is configurable, default value is 1800 seconds

You can choose personal mode (PSK) or enterprise mode (802.1X) authentication. The default setting is PSK.

If you choose PSK you will need to enter a pass phrase of 8-63 ASCII characters or 64 hexadecimal digits.

If you choose 802.1X you will need access to a RADIUS server, port and secret.

Profile (SSID) Isolation

Stations connected to different profiles cannot access each other. Choose from **No Isolation** (Full access), **Isolate all Profiles (SSIDs) from each other**, check **use VLAN (802.1Q) standard**.

Multi-BSSID

Check **enable** Multiple BSSIDS to allow each profile to send an individual beacon and station separation configuration. This can be done is manually or automatically.

WDS Link Settings

WDS (Wireless Distribution System) allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time.

WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.

Dynamically assigned and rotated encryption key are not supported in a WDS connection. This means that WPA and other dynamic key assignment technologies may not be used. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.

Enter the MAC address of the other APs you want to link to and click enable.

Supports up to 8 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

Example of a WDS topology:

AP1 <-- WDS --> Master AP (our AP) <-- WDS --> AP3<-- WDS --> AP4

WDS Security Settings

This item is only available in Access Point Mode and Wireless Bridge Mode.

Choose the required security level from: **None**, **WEP**, **WPA-PSK (TKIP)**, **WPA-PSK (AES)**, **WPA2-PSK (TKIP)** or **WPA2-PSK (AES).**

If using **WEP** security enter the WEP key, if using **WPA** enter the pass phrase.

Wireless Advanced Settings

To configure the advanced wireless setting, click Wireless Advanced Settings and the tool bar and Wireless Advanced Settings menu will appear.

Data Rate

Choose between the following data rates 12, 18, 24, 36, 48, 72, 96, 108, and best. Default is Best.

Transmit Power

Choose between the following power levels Full, Half (-3dB), Quarter (-6dB), Eighth (-9dB) or Minimum. Default is Full.

Beacon Interval

The interval time between 20ms and 1000ms for each beacon transmission. The default is 100ms.

Data Beacon Rate (DTIM)

The Delivery Traffic Indication Message. Specify the data beacon rate between 1 and 255. Default is 1.

Fragment Length

The maximum packet size is used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value. The default is 2346.

RTS Threshold

Request to send threshold. The packet size that is used to determine if it should use the CSMA/CA mechanism or the CSMA/CD mechanism

802.11d support

802.1d allows the device to communicate in areas where the 802.11 standard is not allowed. It adds features and restrictions to ensure compliance.

Antenna Type

If you have added additional external antennas check the "External High-Gain Radio Antenna" radio button. The original packing includes 2 external antennas. If the user purchases other type of antennas, then they need to check the high-gain antenna box.

Service

Management VLAN If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

IAPP Inter-Access Point Protocol (IAPP)

802.11F (IAPP) Support - Choose either Enable or Disable

IAPP allows multiple access points to communicate and pass location information about their associated stations. If you enable 802.11F support you should manually add BSSID/IP mapping:

Enter the BSSID and IP addresses of the AP. Click **Add**

Only stations roaming from one of the listed APs to this AP are allowed to re-associate with this AP. Others will be requested to go through the full association process.

QoS

This section provides the administrator with the Quality of Service (QoS) data.

The QoS setting is only available in AP Mode and Wireless Client Mode.

The QoS Setting should be modified with caution because radio behavior is affected. These parameters can be modified when the radio for QoS service is Enabled.

Ack-Policy - when the Ack-Policy is checked. The device will not send ACK frames. The default value is disabled.

Setting	Description
Min Contention Window	For each access category, enter the minimum contention window value. Channel access is prioritized by assigning smaller contention window values to a higher priority traffic class. If a channel is busy or a transmission collides, a node chooses a random number between 0 and the current contention window minimum.
Max Contention Window	For each access category, enter the maximum contention window value. The minimum contention window value is doubled each time a collision occurs until the maximum is reached. A small contention window value decreases the access delay but increases the probability of a collision.
Fixed Slot Time	For each access category, enter the fixed slot time. Channel access can be strictly prioritized by assigning smaller contention window values to a higher priority traffic class. Traffic in the access category must wait for this fixed number of slots after each packet is received before resuming its random back-off.
Transmit Opportunity Limit	Enter the number of microseconds that qualified transmitters can transmit through the normal back-off procedure with a set of pending packets. Larger values allow a client to control the channel for longer periods of time, allowing it to achieve higher throughput in this access category at the expense of longer access times for all access categories.
Admission Control	Note: In this release, clients are blocked from using an access category when they select Enable for Admission Control. The Admission Control check boxes control client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category. However, access points do not support the admission control procedure in this release, so clients cannot use the access category when you enable Admission Control. default : disable

The default value table:

AC TYPE	Min Contention Window (2x-1; x can be 0-10)	Max Contention Window (2x-1; x can be 0-10)	Fixed Slot Time (0-15)	Transmit Opportunity (0-65535 µS)
AC_BK	4	10	7	0
AC_BE	4	6	3	0
AC_VI	3	4	1	3008 (6016 when 11b)
AC_VO (3)	2	3	1	1554 (3264 when 11b)

SNTP

Simple Network Time Protocol (SNTP) allows the administrator to configure the network time settings.

The following settings can be configured.

SNTP client enable/disable	Click the radio button to enable. If it is disabled, the user has to input time manually. If it is enabled, the device will try to fetch time from configured SNTP servers.
Set Time	Includes Year, Month, Day, Hour and Minute. These fields are grayed out and un-configurable if SNTP is enabled.
Timezone selection	This selection will adjust the time obtained from the SNTP server. Note: This selection does not affect manual time input for they are considered to be input at the same time.
Daylight Saving	The start/end date of daylight saving will change automatically based on the time zone selection. Note: Start and End dates can be input manually, to avoid and regional policy changes.
Primary and Secondary SNTP server/port setting	If SNTP is enabled, this device will try to fetch time from the primary server first. The timeout for primary NTP server is 5 seconds. If the Primary NTP server fails after 5 seconds the Secondary NTP server will be tried for 5 seconds. In the event that the secondary server fails the device will wait for 60 seconds before trying the Primary server again. This continues until a time is available.

To avoid using an invalid NTP server address, this device will store the fetched/configured time. After it boots up, it will use the stored time first and adjust time if time is fetched.

Syslog function

In the event of an error the device can send a message to a specified server.

System Log Click either **Enable** or **Disable** to activate or deactivate the system log function.

Syslog Server Enter the IP address of the server that will receive the error information. The default IP address is 0.0.0.0

Syslog Port Enter the port number that your server can be accessed by. The default port number is 514.

Syslog Level Choose from the following levels - in order of severity - of detail to be recorded. The default setting is Error.

- Emergency - System is unusable
- Alert - Action must be taken immediately
- Critical - Critical condition
- Error - Error condition
- Warning - Warning condition
- Notice - Normal, but significant condition
- Informational - Informational messages

Management

This section describes how to use the management and information features of your Wireless 7760 Access Point.

Administration

In this section, you can change the user administrator name and password. The default Administrator name is *admin* (case sensitive), and password is *password*. Click "Apply" to save changes.

SNMP

The SNMP administrative functions are changed through this section. The following functions can be changed:

- Enable/Disable SNMP
- Contact info
- Community names for read-only and read/write
- Trap destination IP address
- Community name

This function is not available in Wireless Bridge mode.

MAC Filtering

MAC filtering allows the administrator to filter MAC addresses of network cards that can access the access point.

- Enable/Disable filter
- Change filter rule to allow or deny
- Add/delete MAC addresses in the filter table

This function is only available in AP mode.

Rogue AP Detection

Unspecified Access Points may try to access the network through this device. Rogue AP detection can prevent this.

- Change Rogue AP definition
- Legal AP list - The list of allowed access points.
- Detect rogue AP – All channels are scanned and Access Points without security or not in legal AP are considered rogue.

This function is only available in AP mode.

Backup/ Restore Settings

This section allows the user back up the Access Point's current settings and restore back to the factory default. Once you have the Access Point working properly you should back up the information to have it available if something goes wrong.

Firmware Auto Update

The Wireless 7760 can auto upgrade the firmware if there is a newer version available. If you enable the Auto Upgrade function, the Wireless 7760 will automatically check for an updated version of firmware in the assigned FTP server for each time interval assigned. Remember to insert the correct FTP server IP address, username, password and corrected route to the FTP server.

Firmware Upgrade

In this section, you can see the current firmware version of your AP. You can also manually upgrade your firmware by assigning the correct route to your new firmware file.

Once you have chosen the upgrade file click upgrade.

Rebooting

You can reboot the Wireless access point from the browser interface.

After you click reboot the following window will be displayed.

After rebooting the login page will automatically be displayed.

Connecting through the Com Port

Instead of using an IP address to configure the Access Point a Null modem cable, connected to the AP's serial port, can be used.

In your terminal settings ensure that the following configuration is met:

Bits per Second – 9600
Data Bits – 8
Parity – None
Stop bits – 1
Flow Control - none

Once connected enter the user name and password. The default values are as follows:

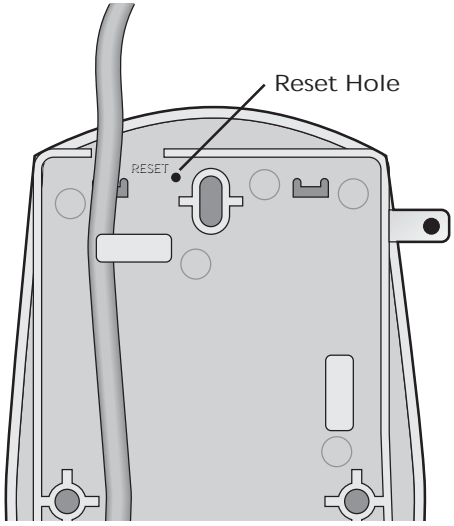
Username: admin
Password: password

Once logged in, type"**?**" for a list of commands.

Restoring factory settings

The Access Point can be reset to the default factory settings either through the web browser (**see Backup/ Restore Settings**) or manually.

To restore the settings manually, insert a pointed object (such as the end of a straightened paper clip) into the reset hole on the back of the Access Point, and hold for five seconds.



A TROUBLESHOOTING

Diagnosing Problems

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

Symptom After you change the IP address, after you restore a backup configuration, or after you reset the Access point to factory defaults, the Configuration Management System stops responding and you cannot continue configuring the Access point. If you change the IP address and click Apply, you cannot continue to configure the device using the old IP address. Similarly, after you restore a backup configuration or reset the Access point to factory defaults, the IP address setting may be changed.

Solution (s) To recover from this situation and continue configuring the Access point:

1. Close your browser.
2. Return to the 3Com Wireless Infrastructure Device Manager and click Refresh.
3. Select the device and click Configure to start a new configuration session and set its IP address.

Symptom The Wireless Network Tree does not appear in the 3Com Wireless Infrastructure Device Manager window.

Solution (s) Verify that you are using the correct network adapter. In the device manager window, click **Choose NIC**. Select the network adapter for the network you want to scan, and click OK

Symptom The Access point has a yellow exclamation point (!) next to it in the Wireless Infrastructure Device Manager.

Solution (s)

- The Access point is on a different subnet than the computer attempting to configure it.
- To recover from this situation and continue configuring the Access point:

1. Close your browser.
2. Return to the 3Com Wireless Infrastructure Device Manager and click Refresh.
3. Select the device and click Configure to start a new configuration session.
4. Make sure the subnet address matches that of the computer.

Symptom Two Access points cannot communicate in ad-hoc mode.

Solution (s) Adjust the positions of the Access points to improve reception.

To ensure correct operation in ad-hoc mode, the settings on the two Access points must match exactly.

Launch the Access point Configuration Management System and make sure that the Wireless LAN Service Area, channel selections, Data Preamble setting, and security setting are the same on both Access points.

Symptom You are running Windows NT. After you connect the Access point, your computer cannot obtain a valid IP address.

Solution (s) The Access point configuration settings may not be compatible with the network. If they are not, and your Windows NT computer is set up to obtain its IP address from a DHCP server, the Access point is unable to associate with the network to obtain the IP address.

To work around this, set a static IP address on your computer. Then set the Access point configuration to match the network. When the Access point is able to associate, reset your computer to obtain its IP address from the DHCP server. If the Access point should also obtain its IP settings from the DHCP server, make sure this is

configured properly on the IP Network page and applied just before ending the session.

Symptom Disconnecting the Access point

Solution (s) To disconnect the Access point:

CAUTION: Disconnecting the Access point ends the network association. To avoid possible data loss, exit all networking applications on connected devices before you disconnect the Access point.

1. Unplug the Access point Ethernet cable from the hub or other device.
2. Unplug the Access point power cord.

Symptom Uninstalling Software and Documentation

Solution (s) If you want to uninstall the 3Com 11a/b/g Wireless Workgroup Access point software and documentation, you can either use the standard operating system procedure for removing programs or use the following shortcut:

From the Windows Start menu, select **Start** > **Programs** > **3Com Wireless** > **Uninstall 3Com Wireless Infrastructure Device Manager**.

When prompted to confirm, click **OK**.

Symptom Upgrading Access point Firmware.

Solution (s) Firmware is the software that is installed on the Access point at the factory. Some problems can be solved by installing a new version of the firmware.

For details on how to download a firmware update from the 3Com customer support Web site and install it on your Access point, see "Upgrading the System" on page 43

B OBTAINING SUPPORT FOR YOUR 3COM PRODUCT

3Com offers product registration, case management, and repair services through eSupport.3Com.com. You must have a user name and password to access the services, described in this appendix.

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at:

http://eSupport.3Com.com/

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

The 3Com Knowledge base helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

http://knowledgebase.3Com.com

It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

http://www.3Com.com/

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

You are entitled to bug fix / maintenance releases for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

http://eSupport.3Com.com/

To obtain software releases that follow the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

Contact Us

3Com offers telephone, Internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

http://eSupport.3Com.com/

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 level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at http://eSupport.3Com.com/. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

http://csoweb4.3Com.com/contactus/

C END USER LICENSE AGREEMENT

Customer shall take all steps necessary to protect Wind River's and its licensors' proprietary rights in the Run-Time Module and to ensure that each Run-Time Module distributed by Customer will be accompanied by a localized copy of an End User License Agreement.

Such End User License Agreement shall prohibit the End User from: (i) copying the Run-Time Module, except for archive purposes consistent with the End User's archive procedures; (ii) transferring the Run-Time Module to a third party apart from the Target Application; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the Source Code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the Target Application.

In addition, the End User License Agreement shall: (i) state that the Run-Time Module is licensed, not sold and that Customer and its licensors retain ownership of all copies of the Run-Time Module; (ii) expressly disclaim all implied warranties, including without limitation the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement; (iii) exclude liability for any special, indirect, punitive, incidental and consequential damages; and (iv) require that any further distribution of the Run-Time Module be subject to the same restrictions set forth herein.

The End User License Agreement shall also state that, with respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the End User License Agreement and that the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

INDEX

8

802.11a 3
802.11b/g 4
802.11d 33

A

Access Point Detection *44*
Access Point mode *21*
Ad-hoc mode *22*
Administration *41*
Advanced WLAN *32*

B

Backup *45*
Beacon Interval 32
BSSID *25*, *28*

C

Com Port *48*
Configuring 11
Contention *37*

D

Data Beacon Rate ..... *See* DTIM
Data Rate 32
default IP address 12
Default IP address 14
Delivery Traffic Indication Message 32
Device Manager Software *13*
DHCP Server 11
DTIM ..... 32. *See* Delivery Traffic Indication Message

E

External Antenna 10

F

factory settings *48*
FAT *22*
Firmware *46*
Firmware Upgrade *46*
FIT *22*
Fragment Length 33

I

IAPP ..... *See* Inter Access Point Protocol
IEEE802.3af 5
Installation 6
Installing Software *12*
Inter Access Point Protocol 34
IP Settings *23*

L

LED Indicators....9
Logging On....*14*
Login name....12

M

MAC Filtering....*43*

P

Package Contents....6
Password....12, *15*, *48*
Placement....7
Power over Ethernet....3

Q

QoS....*See* Quality of Service
Quality of Service....35

R

Rebooting....*47*
Repeater....*22*
Restore....*45*
RTS Threshold....33

S

Security....2, *26*
Setting Up....*19*
Simple Network Management Protocol 42
Simple Network Time Protocol....38
SNMP... *See* Simple Network Management Protocol
SNTP....*See* Simple Network Time Protocol
SSID....*25*, *28*
Suppressed SSID....*26*
System Properties....*21*
System Summary....*16*

T

terminal settings....*48*
Time Slot....*37*
Transmit Power....32

U

Username....*15*, *48*

V

VLAN ID....*26*
VLAN Management....*34*

W

Wall Mounting....8
WDS Security....*31*
WEP....*See* Wired Equivalent Privacy
Wi-Fi Protected Access....27, 28
Wi-Fi Protected Access 2....28
Wired Equivalent Privacy....26
Wireless Client....*22*
Wireless Distribution System....29. *See* Wireless Distribution System
Wireless Network Standards....3
Wireless Range....4, 7
WPA....*See* Wi-Fi Protected Access
WPA2....*See* Wi-Fi Protected Access 2
WPA-Mixed....*See* Wi-Fi Protected Access