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

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

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

3 Click *Add*.

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

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

i> *Click* Close *to discard all changes.*

Modifying a MAC Address

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

2 Modify the MAC address. The MAC address can only be edited manually.

3 Press *Apply* to accept the changes.

Figure 31 MAC Address Table

Authorised Wireless PCs	
delete	C0-FF-EE-01-23-45
delete	00-0C-12-65-BF-98
delete	12-34-56-78-90-AB

i> *Click* Close *to discard all changes.*

Deleting a MAC Address

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

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

Client List   **Figure 32**   Client List Screen

The Wireless Client List provides details on the devices that are connected to the Wireless LAN. The list is only created when Wireless Networking is enabled. For each device that is connected to the Wireless LAN, the MAC address and Connection Speed of that device is displayed. As you connect more devices to the Wireless LAN, the client list will grow to a maximum of 128 (the maximum number of wireless devices that the Access Point can support).

Profile **Figure 33** Profile Screen
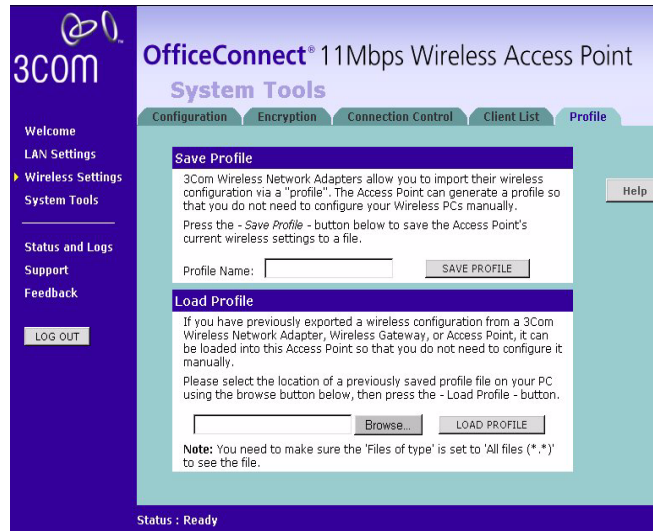
Some 3Com Wireless Network Adapters allow you to import Wireless configurations via a 'profile'. The Access Point can generate a profile so that you do not need to configure your Wireless PCs manually.

The profile contains three items as follows:

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

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

■ **Encryption settings from the Access Point**

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

■ **Profile Name**

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

Saving a Profile

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

1 Enter a Profile Name (up to 25 alphanumeric characters) and then click *Save Profile*.

2 Your browser will then prompt you to enter a file name and folder location in which to save the profile. Once the profile has been saved it can be copied on to another PC and imported into the 3Com Wireless Network Adapter.

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

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

■ the adapter is within range of the Access Point

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

Importing a Profile

You can import a profile that has already been saved.

1 Click *Browse* and navigate to the folder where you have saved the profile on your admin computer.

2 Select the Profile you want to import and click *Load Profile*.

i *Only the Service Area Name and WEP settings will be imported from the profile.*

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

Restart   **Figure 34**   Restart Screen

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

Configuration   **Figure 35**   Configuration Screen
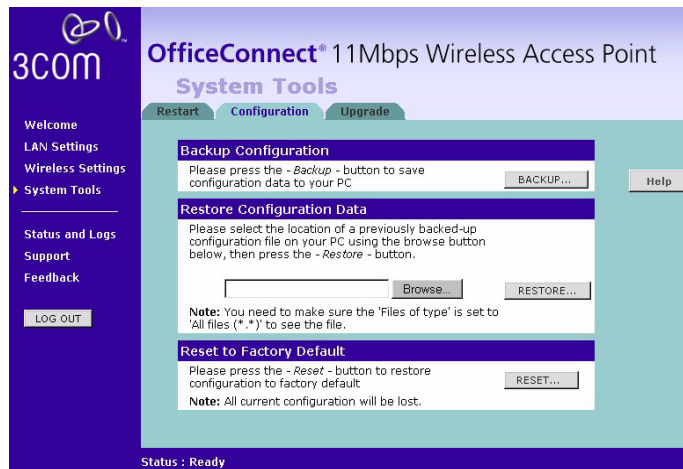
Select the *Configuration* tab to display the *Configuration* screen
([Figure 35](#)).

Backup Configuration

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

Restore Configuration Data

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

> **i** > *The password will remain unchanged.*

Reset to Factory Default

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

**Upgrade**   **Figure 36** Upgrade Screen

The Upgrade facility allows you to install on the Access Point any new
releases of system software that 3Com may make available. To install new
software, you first need to download the software from the 3Com

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

The upgrade procedure can take up to two minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Access Point during the upgrade procedure; if you do, the software may be corrupted and the Access Point may not start up properly afterwards. If the Alert LED comes on continuously after a failed upgrade, refer to Chapter 5, "Troubleshooting".

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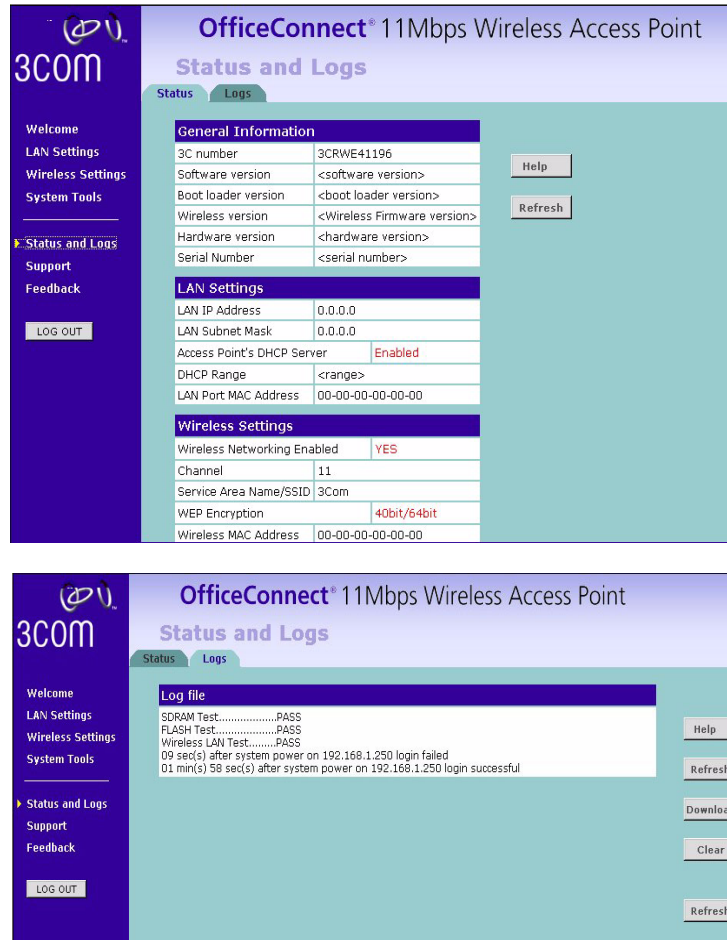
Selecting *Status and Logs* from the main menu displays the *Status* and *Logs* screens (Figure 37) in your Web browser window. The *Status* screen displays a tabular representation of your network and Internet connection.

 The screen shot in Figure 37 *does not show a full status screen and the screen can be scrolled to view more information.*

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

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

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

Support **Figure 38** Support Screen
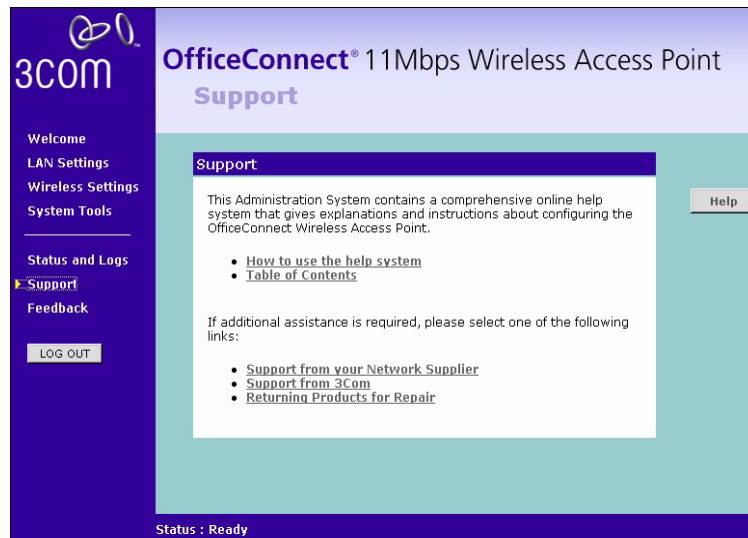
Selecting the *Support* option on the main menu displays the support links screen, which contains a list of Internet links that provide information and support concerning the Access Point (Figure 38).

5 T**ROUBLESHOOTING**

Basic Connection Checks

- Check that the Access Point is connected to your switch or hub and that all the equipment is powered on. Check that the LAN port link status LED on the Access Point are illuminated, and that any corresponding LEDs are also illuminated.

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

- If the link status LED does not illuminate for the LAN port, check that you do not have a faulty cable. Try a different cable. Check also that the Uplink/Normal switch is in the correct position.

Browsing to the Access Point Configuration Screens

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

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

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

- If you cannot browse to the Access Point, re-run the DISCOVERY software described in Appendix A to discover the Access Point and the IP address it has been allocated from the DHCP server. If there is no DHCP server on your network, the DISCOVERY software changes the IP address of the Access Point so that it is in the same subnet as your admin computer.

Forgotten Password and Reset to Factory Defaults

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

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

1 Remove power from the Access Point.

2 Hold down the *Reset* button on the rear of the unit and re-apply power to the Access Point. The Alert LED will flash as the Access Point starts up, and after approximately 30 seconds will start to flash more slowly (typically 2 seconds on, 2 seconds off). Once the Alert LED has started to flash slowly. Keep *Reset* button held down and remove power from the Access Point.

3 Release the *Reset* button.

4 Re-apply power to the Access Point, and when the start-up sequence has completed, browse to the IP address of the Access Point and run the configuration wizard. You may need to restart your computer before you attempt this.

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

Wireless Networking

- Ensure that you have a Wi-fi certified 802.11b wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 95 or higher or MAC OS 8.5 or higher.

- Verify that your wireless computers are configured to work in Infrastructure mode and not Ad Hoc mode. The Access Point is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Access Point.

- Check the status of the Access Point Wireless LED, it should be lit if wireless is enabled and will flash when there is wireless activity. If not lit go to "Wireless Settings" on page 37 and enable wireless networking.

- Ensure that the TCP/IP settings for all devices are correct.

- Ensure that the Wireless Clients are using the same SSID or Service Area Name as the Access Point. The SSID is case-sensitive

- Ensure that you are using the same level of security on all of your wireless computers (None, 40/64 or 128 bit) and that all devices are using the same keys, and the same order of keys where appropriate.

- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using Wireless Connection control on the Access Point.

- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Access Point. For more effective coverage you can try reorientating your antennae. Place one antenna vertically and one horizontally to improve coverage. Additionally consider moving the wireless computer closer to the Access Point to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or select *Clear Channel Select* on the Access Point.

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

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

- Speed of connection: The 802.11b standard will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds are 11Mbps, 5.5Mbps, 2Mbps and 1Mbps. In general the closer you are to the Access Point the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Access Point or moving the Wireless computer closer to the

Access Point. In an ideal network the Access Point should be located in the centre of the network with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Wireless Card documentation and vendor for more details.

Alert LED

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

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

Recovering from Corrupted Software

If the Alert LED remains permanently on following power-up, it is possible that the system software has become corrupted. In this condition, the Access Point will enter a "recovery" state; DHCP is disabled, and the LAN IP address is set to 192.168.1.1. Follow the instructions below to upload a new copy of the system software to a Access Point unit in this state.

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

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

www.3com.com.

1 Remove power from the Access Point and connect the admin computer to the LAN port.

2 You will need to reconfigure this computer with the following static IP address information:

- IP address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default Gateway address: 192.168.1.1

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

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

http://192.168.1.1.

This will connect you to the Microcode Recovery utility in the Access Point.

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

6 When the upload has completed, the Access Point will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.

7 Reconnect your Access Point to your network. Do not forget to reconfigure the computer you used for the software upload.

If the Access Point does not resume normal operation following the upload, it may be faulty. Contact your supplier for advice.

Frequently Asked Questions	**How do I reset the Access Point to Factory Defaults?**

See "Forgotten Password and Reset to Factory Defaults" on page 54.

How many wireless clients does the Access Point support?

A maximum of 128 wireless clients are supported.

There is a single LAN ports on the Access Point. How are additional computers connected?

You can expand the number of connections available on your LAN by using hubs, switches and wireless access points connected to the Access Point. 3Com wireless access points and OfficeConnect hubs and switches provide a simple, reliable means of expanding your network; contact your supplier for more information, or visit:

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

Where can I download software upgrades for the Access Point?

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

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

What other online resources are there?

The 3Com Knowledgebase at:

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

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

A USING DISCOVERY

Running the Discovery Application

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

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

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

1 Insert the Access Point CD-ROM in the CD-ROM drive on your computer. A menu will appear; select *Gateway Discovery*.
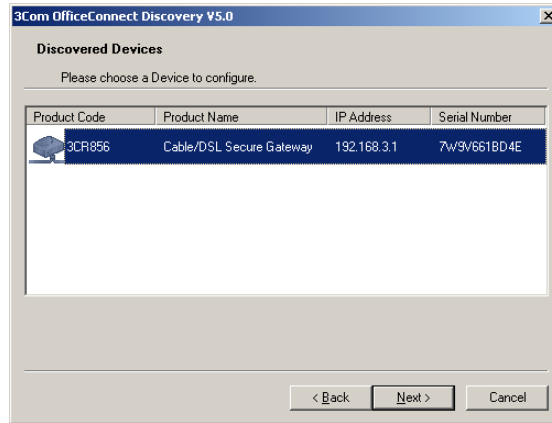
> *Discovery will find the Access Point even if it is unconfigured or misconfigured.*

Figure 39 Discovery Welcome Screen

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

Figure 40   Discovered Access Point Screen

3 Figure 40 shows an example Discovered Devices screen. Highlight the *11Mbps Wireless Access Point* by clicking on it, and press *Next*.

Figure 41   Discovery Finish Screen

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

B   IP ADDRESSING

**The Internet
Protocol Suite**

The Internet protocol suite consists of a well-defined set of communications protocols and several standard application protocols. Transmission Control Protocol/Internet Protocol (TCP/IP) is probably the most widely known and is a combination of two of the protocols (IP and TCP) working together. TCP/IP is an internationally adopted and supported networking standard that provides connectivity between equipment from many vendors over a wide variety of networking technologies.

**Managing the
Access Point over
the Network**

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

- An IP address
- A Subnet Mask

**IP Addresses and
Subnet Masks**

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

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

For your network to work correctly, all devices on the network must have:

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

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

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

Type One

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

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

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

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

Table 3 IP Addressing and Subnet Masking

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

Type Two

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

- Part one ('192.168') identifies the network on which the device resides.
- Part two ('.100.8') identifies the device within the network.

This type of IP Address operates on a subnet mask of '255.255.0.0'.

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

Table 4   IP Addressing and Subnet Masking

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

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

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

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

DHCP Addressing

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

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

Static Addressing

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

Auto-IP Addressing

Network devices use automatic IP addressing if they are configured to acquire an address using DHCP but are unable to contact a DHCP server. Automatic IP addressing is a scheme where devices allocate themselves

an IP address at random from the industry standard subnet of 169.254.x.x (with a subnet mask of 255.255.0.0). If two devices allocate themselves the same address, the conflict is detected and one of the devices allocates itself a new address.

Automatic IP addressing support was introduced by Microsoft in the Windows 98 operating system and is also supported in Windows 2000.

C TECHNICAL SPECIFICATIONS

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

11Mbps Wireless Access Point

Interfaces

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

WLAN Interface

Standard IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)
Transmission rate: 11Mbps, automatic fallback to 5.5, 2 or 1Mbps
Maximum channels: 13
Range up to 304.8m (1000ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz
Sensitivity: 1,2,5.5Mbps: -80dBm; 11Mbps -76dBm typical
Modulation: CCK, BPSK, QPSK
Encryption: 40/64bit, 128 bit WEP
Maximum clients: 128
O/P Power 18dBm

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

7VA, 23.9 BThU/hr

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

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

Weight

Approximately 592 g (1.3 lbs)

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

Safety: UL 1950, EN 60950
CSA 22.2 #950
IEC 60950

EMC: EN 55022 Class B
EN 55024
AS/NZS 3548 B
FCC Part 15 Class B*
ICES-003 Class B
CNS 13438 Class A
ETS 300-826

Radio CFR 47 FCC Part 15.207, 15.209, 15.247 and 15.249.
ETS 300 328 (2.4 GHz ISM band wide band transmission systems.

Environmental: EN 60068 (IEC 68)

*See <u>"Safety Information"</u> on <u>page 69</u> for conditions of operation.

System Requirements   **Operating Systems**

The Access Point will support the following Operating Systems:

- Windows 95/98
- Windows NT 4.0
- Windows ME
- Windows 2000

- Windows XP
- Mac OS 8.5 or higher
- Unix

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

Wireless Performance   The Access Point complies with the IEEE 802.11b specification and conforms to the WiFi interoperability test standard.

Wi Fi™

**The Standard for
Wireless Fidelity.**

Cable Specifications   The Access Point supports the following cable types and maximum lengths:

- Category 3 (Ethernet) or Category 5 (Fast Ethernet or Dual Speed Ethernet) Twisted Pair — shielded and unshielded cable types.
- Maximum cable length of 100m (327.86 ft).

D SAFETY INFORMATION

Important Safety Information

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

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

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

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

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

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

WARNING: *This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.*

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

WARNING: Disconnect the power adapter before moving the unit.

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

Wichtige Sicherheitshinweise

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

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

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

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

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

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

VORSICHT: Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden.

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

VORSICHT: Vor dem Ausbau des Geräts das Netzadapterkabel herausziehen.

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

Consignes importantes de sécurité

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

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

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

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

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

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

AVERTISSEMENT: *L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme CEI 950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.*

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

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

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

E END USER SOFTWARE LICENCE AGREEMENT

3Com Corporation
END USER SOFTWARE LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ENTIRE AGREEMENT: This Agreement sets forth the entire understanding and agreement between you and 3Com and supersedes all prior agreements, whether written or oral, with respect to the Software and Documentation, and may be amended only in a writing signed by both parties.

Should you have any questions concerning this Agreement or if you desire to contact 3Com for any reason, please contact the 3Com subsidiary serving your country, or write:

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

GLOSSARY

802.11b The IEEE standard to which the 3Com OfficeConnect 11Mpbs Wireless Access Point conforms. This standard provides for 1,2,5.5 and 11 Mbps data rates and a set of fundamental signaling methods and other services (see WECA).

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

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

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

Ad Hoc mode Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infra-structure mode, which is the mode the gateway uses. (see also Infra-structure mode.)

Auto-negotiation Some devices in the OfficeConnect range support auto-negotiation. Auto-negotiation is where two devices sharing a link, automatically configure to use the best common speed. The order of preference (best first) is: 100BASE-TX full duplex, 100BASE-TX half duplex, 10BASE-T full duplex, and 10BASE-T half duplex. Auto-negotiation is defined in the IEEE

802.3 standard for Ethernet and is an operation that takes place in a few milliseconds.

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

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

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

Channel Similar to any radio device, the OfficeConnect 11Mbps Wireless Access Point allows you to choose different radio channels in the wireless spectrum. A channel is a particular frequency within the 2.4GHz spectrum within which the Gateway operates.

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

DHCP Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer on your network. Windows 95, Windows 98 and Windows NT 4.0 contain software that assigns IP addresses to workstations on a network. These assignments are made by the DHCP server software that runs on Windows NT Server, and Windows 95 and Windows 98 will call the server to obtain the address. Windows 98 will allocate itself an address if no DHCP server can be found.

DNS Server Address DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as 3com.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "3com.com" into

your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

Encryption A method for providing a level of security to wireless data transmissions. The OfficeConnect 11Mbps Wireless Access Point uses two levels of encryption; 40/64 bit and 128 bit. 128 bit is a more powerful level of encryption than 40/64 bit.

ESSID Extended Service Set Identifier. The ESSID is a unique identifier for your wireless network. You must have the same ESSID entered into the Access Point and each of it's wireless clients.

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

Ethernet Address See MAC address.

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

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

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

Half Duplex A system that allows packets to transmitted and received, but not at the same time. Contrast with full duplex.

Hub A device that regenerates LAN traffic so that the transmission distance of that signal can be extended. Hubs are similar to repeaters, in that they connect LANs of the same type; however they connect more LANs than a repeater and are generally more sophisticated.

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

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

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

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

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

ISP   Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN   Local Area Network. A network of end stations (such as PCs, printers, servers) and network devices (hubs and switches) that cover a relatively small geographic area (usually not larger than a floor or building). LANs are characterized by high transmission speeds over short distances (up to 1000 metres).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Traffic The movement of data packets on a network.

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

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

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

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

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

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

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

INDEX

REGULATORY NOTICES FOR THE 11MBPS WIRELESS ACCESS POINT

Channels

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

Table 5   Channels

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

FCC Statement

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

Information to the User

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

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

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

How to Identify and Resolve Radio-TV Interference Problems

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

FCC Declaration of Conformity

We declare under our sole responsibility that the

Model: **Description:**
3CRWE41196   11Mbps Wireless Access Point

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

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

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

CE Statement (Europe)

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

CSA Statement

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

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

BSMI Statement

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

FCC

⚠ *CAUTION: To assure continued compliance, (for example, use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

RF Exposure Compliance Statement (U.S.)

⚠️

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

Potential RF Interference (Canada)

⚠️

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

3com