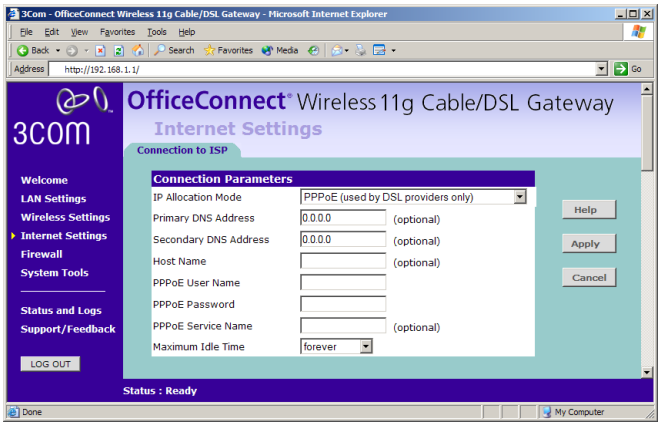
- *Use this PC's MAC address* - This field is automatically filled in with the MAC address of the PC you are using to configure the Gateway. You should use this address only if you were previously using this computer to connect directly to your modem.
- *Enter a new MAC address manually* - Use this option if you want to specify a new MAC address. Enter the new MAC address.

5 Check all settings and click *Apply.*

PPP over Ethernet

Figure 43 PPPoE Setup Screen



To setup the Gateway for use with a PPP over Ethernet connection, use the following procedure:

1 Select *PPP over Ethernet* in the *IP Allocation Mode* field. (Figure 43)

2 Enter your *Primary DNS Address* and *Secondary DNS address*.

Your ISP may provide you with primary and secondary DNS addresses. If they have been provided, enter the addresses in the appropriate text boxes. If not, leave *0.0.0.0* in the boxes.

3 Enter the *Host Name* (optional).

Some ISPs require a host name. If your ISP has this requirement, enter the host name in the *Host Name* text box.

4 Enter your PPP over Ethernet user name in the *PPPoE User Name* text box.

5 Enter a password in the *PPPoE Password* text box.

6 Enter your PPP over Ethernet service name in the *PPPoE Service Name* text box. Not all ISPs require a PPPoE service name. Only enter a service name if your ISP requires this.

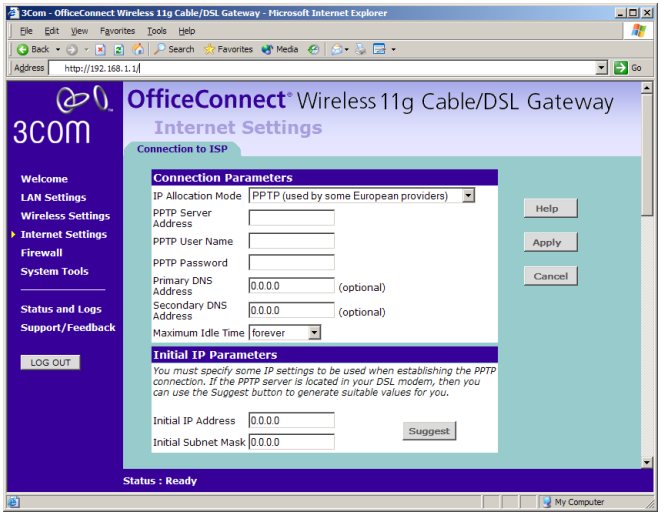
7 Select an idle time from the *Maximum Idle Time* drop-down list.

This value will correspond to the amount of idle time (no Internet activity) that will pass before the Gateway automatically ends your PPP over Ethernet session.

Since the Gateway contains its own PPPoE client, you no longer need to run PPPoE client software on your computer to access the Internet.

PPTP

Figure 44 PPTP Setup Screen



To setup the Gateway for use with a PPTP connection, use the following procedure:

1 Select *PPTP (used by some European providers)* in the *IP Allocation Mode* field. (Figure 44)

2 Enter your PPTP server address in the *PPTP Server Address* text box (this is typically the address of your modem).

3 Enter your PPTP user name in the *PPTP User Name* text box.

4 Enter your password in the *PPTP Password* text box.

5 Enter your *Primary DNS Address* and *Secondary DNS address*.

Your ISP may provide you with primary and secondary DNS addresses. If they have been provided, enter the addresses in the appropriate text boxes. If not, leave *0.0.0.0* in the boxes.

6 Select an idle time from the *Maximum Idle Time* drop-down list.

This value will correspond to the amount of idle time (no Internet activity) that will pass before the Gateway automatically ends your PPTP session.

7 IP settings must be used when establishing a PPTP connection. Fill in the *Initial IP Address* and the *Initial Subnet Mask* fields if your ISP has provided you with these settings. Alternatively, if the PPTP server is located in your DSL modem, click *Suggest* to select an IP address on the same subnet as the PPTP server.

Firewall

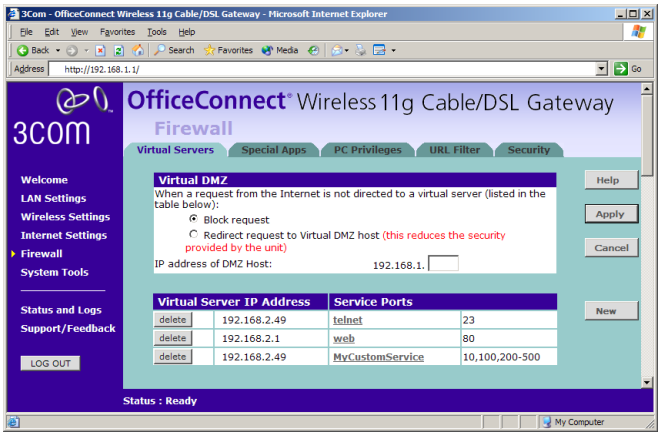
On the main frame of the *Firewall* setup screen is a menu with five tabs: Virtual Servers, Special Applications, PCs Privileges, URL Filter, and Security.

Virtual Servers

Selecting the *Firewall* option on the main menu displays the Virtual Servers setup screen. (Figure 45)

Virtual DMZ

Figure 45 Virtual Servers Screen



DMZ (De-Militarized Zone) Host is a computer without the protection of the firewall. This feature allows a single computer to be exposed to unrestricted 2-way communication from outside of your network. This feature should be used only if the Virtual Server or Special Applications options do not provide the level of access needed for certain applications.

To configure one of your computers as a DMZ host, enter the last digit(s) of the IP address of the computer in the *IP Address of DMZ Host* text box, and then click *Apply*.

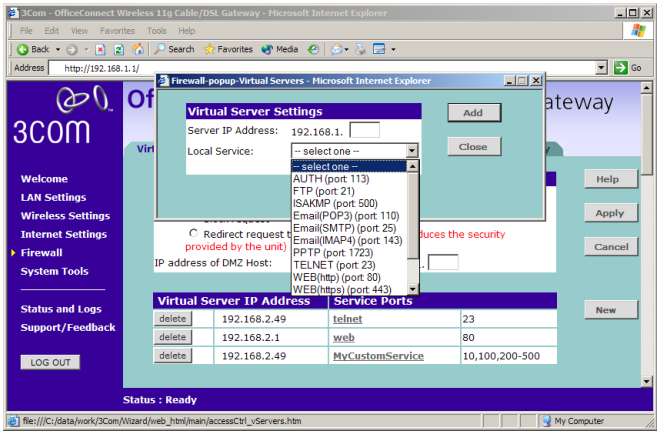
Virtual Server

Activating and configuring a virtual server allows one or more of the computers on your network to function as a public server. For example, one of your computers could be configured as an FTP server, allowing others outside of your office network to download files of your choosing. Or, if you have created a Web site, you can configure one of your computers as a Web server, so that others can view your Web site.

To configure a virtual server:

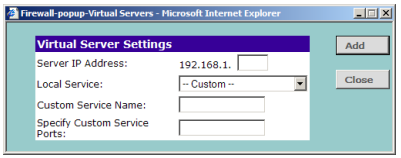
1. Click *New* on the right side of the screen to open the *Virtual Server Settings* dialogue box. (Figure 46)
2. Enter the last digit(s) of the IP address of the computer in the *Server IP Address* text box.
3. Select the Service from the pull-down list. (Figure 46)

Figure 46 Virtual Servers Settings Screen



Or select *Custom* to specify a suitable name for the service and then enter the port numbers required for that service. (Figure 47)

Figure 47 Custom Setup Screen

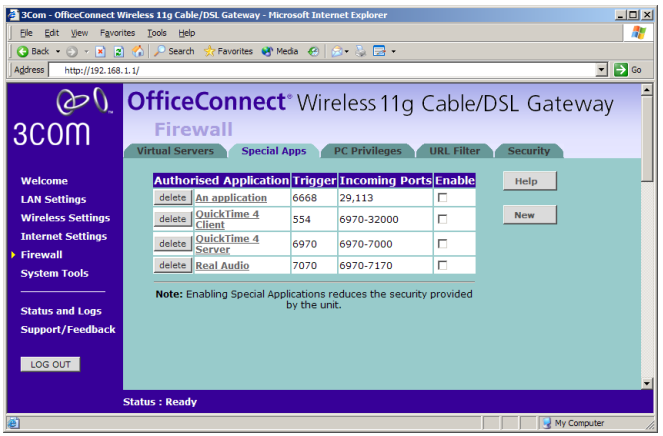


4 Click *Add* to save the settings.

The port numbers are specified using a comma-separated list, with hyphens to denote port number ranges. So for example, entering *2, 3, 5-7* would cause ports 2, 3, 5, 6, and 7 to be activated.

Special Applications

Figure 48 Special Applications Screen



Select *Special Applications* tab to display *Authorized Application* setup screen. (Figure 48)

Some software applications require special or multiple connections to the Internet and these would normally be blocked by the firewall. For example Internet Telephony or Video conferences require multiple connections.

So that these special applications can work properly and are not blocked, the firewall needs to be told about them. In each instance there will be a

trigger port and incoming port(s), where traffic on the trigger port tells the firewall to open the incoming ports.

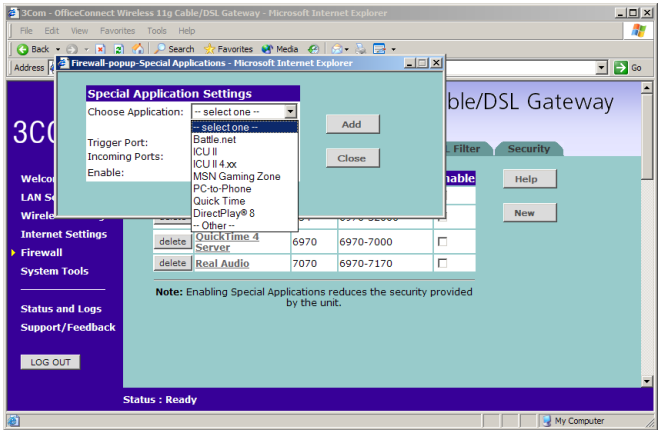
Each defined Special Application only supports a single computer user, and up to 10 Special Applications can be defined. Any incoming ports opened by a Special Application trigger will be closed after five minutes of inactivity.

To configure special applications:

1 Click *New*.

2 Select the applications from the pull-down list. (Figure 49)

Figure 49 Special Application Settings Screen

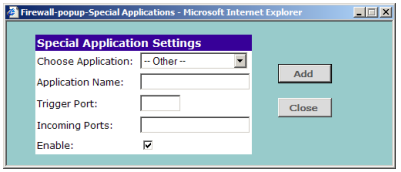


Or select *Other* to specify a suitable name for the special application and then enter a value in the *Trigger Port* and *Incoming Ports* text boxes (Figure 49). These values correspond to the outbound port numbers issued by the application.

The port numbers are specified using a comma-separated list, with hyphens to denote port number ranges. So for example, entering *2, 3, 5-7* would cause ports 2, 3, 5, 6, and 7 to be activated.

The Gateway will automatically allow FTP and NetMeeting sessions. You do not need to configure these as Special Applications.

Figure 50 Other Applications Setup Screen

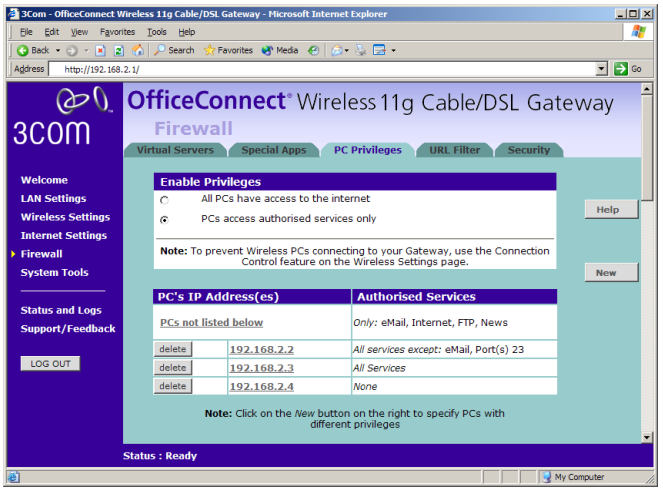


3 Click *Add* to save your settings.

Only one computer on your network can use the special application at any one time.

PC Privileges

Figure 51 PC Privileges Screen



Select *PC Privileges* to display the PC Privilege setup screen (Figure 51).

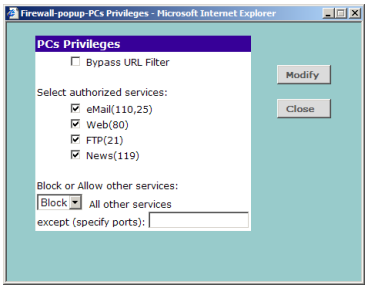
Access from the local network to the Internet can be controlled on a computer-by-computer basis. In the default configuration the Gateway will allow all connected computers unlimited access to the Internet.

PC Privileges allows you to assign different access rights for different computers on your network.

To use access control for all computers:

1. Click *PCs access authorized services only.*
2. Select *All PCs* to setup the access rights for all computers connected to the Gateway.
3. Select authorized services by clicking in the appropriate check box(es) (Figure 52).

Figure 52 All PCs Setup Screen



In addition to the four authorized services listed, you can choose to allow or block access to other services. You can either:

- Allow all other services with exceptions, or
- Block all other services with exceptions

4. To do this, select *Allow* or *Block* from the drop down menu and enter the exceptions into the text box.

The port numbers are specified using a comma-separated list, with hyphens to denote port number ranges. So for example, entering *2, 3, 5-7* would cause ports 2, 3, 5, 6, and 7 to be activated.

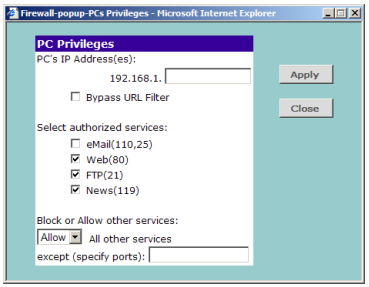
For example, to block access to all services except Web (80) and a service that uses ports 2,3,5,6 and 7:

1. Tick the Web(80) *check box.*

2. Select 'Block' *all other services.*

3. Enter '2, 3, 5-7' *in the* 'except (specify ports) *box. See* Figure 53.

Figure 53 PC Privileges Setup Screen Example



5 Click *Modify* to save the settings or *Close* to discard them.

To assign different access rights for different computers:

1 If not already selected, click *PCs access authorized services only.*

2 Click *New* to display the *PC Privileges* setting screen.

3 Enter the last digit(s) of the IP address of the computer in the PC's IP Address text box.

4 Select authorized services by clicking in the appropriate check box(es).

In addition to the four authorized services listed, you can choose to allow or block access to other services. You can either:

- Allow all other services with exceptions, or
- Block all other services with exceptions

See step 4 of the previous section for more details.

5 Click *Add* to save the settings.

URL Filter

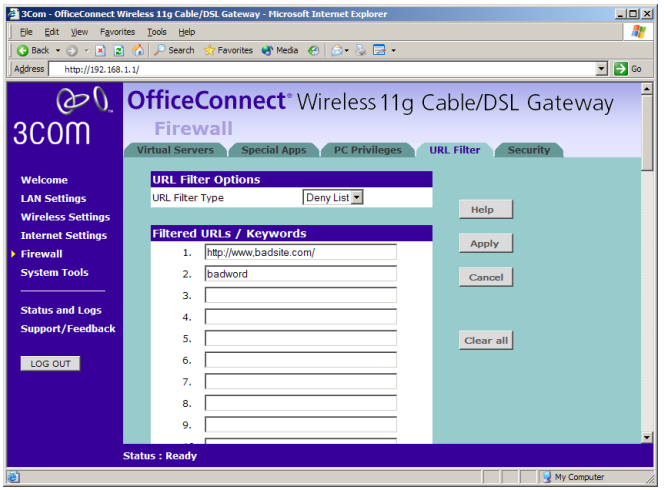
Select *URL Filter* to control your clients' access to Web sites. The Gateway's URL Filter has three settings:

- Disabled — Users can browse all Web sites. None will be filtered.
- Deny List — Users can browse all Web sites apart from those sites listed in the deny list and those whose URLs contain keywords listed in the deny list. See "Deny List" on page 70.
- Allow List — Users are unable to browse any Web sites except of those listed in the allow list and those whose URLs contain keywords listed in the allow list. See "Allow List" on page 71.

Deny List

To allow users access to all Web sites except for those you choose to block, choose *Deny List* in the URL Filter Type drop-down box (Figure 54).

Figure 54 URL Filter Screen showing Deny List



To filter a specific site, enter the URL for that site. For example, to stop your users from browsing a site called **`www.badsite.com`**, enter **`www.badsite.com`** or **`badsite.com`** in one of the fields.

If badsite.com has multiple sub-domains, such as this.badsite.com and that.badsite.com then you can either:

- Block them individually by entering **`this.badsite.com`** in one field and **`that.badsite.com`** in another.

  or

- Block them by entering the keyword **`badsite.com`** into one of the fields. This will block all URLs containing the string *badsite.com*. As well as blocking **`this.badsite.com`** and **`that.badsite.com`**, the keyword badsite.com would block searches that mentioned badsite.com in their domain name, for example **`www.notabadsite.com`**.

To filter a generic keyword enter it into one of the fields. You should exercise caution when choosing a keyword as many keywords are

contained within other words. For example, filtering the word sex would filter the following example URLs:

- **`www.sussex.com`**
- **`www.thisexample.com`**

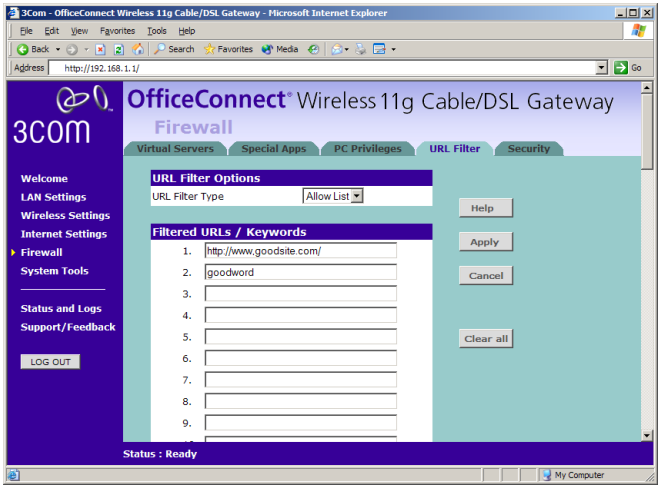
You can filter up to 30 keywords and URLs.

Computers that should not be subject to URL filtering can be excluded by ticking the Bypass URL Filter checkbox in the PC Privileges setup screen. See *"PC Privileges" on page 67*.

Allow List

To stop users from accessing any Web sites that you have not specifically allowed, choose *Allow List* in the *URL Filter Type* drop-down box (Figure 55).

Figure 55 URL Filter Screen showing Allow List



To allow a specific site, enter the URL for that site. For example, to let your users browse a site called **`www.goodsite.com`**, enter **`www.goodsite.com`** or **`goodsite.com`** in one of the fields.

If goodsite.com has multiple sub-domains, such as **`this.goodsite.com`** and **`that.goodsite.com`** then you can either:

- Allow them individually by entering **`this.goodsite.com`** in one field and **`that.goodsite.com`** in another.

  or

- Allow them by entering the keyword **`goodsite.com`** into one of the fields. This will allow all URLs containing the string **`goodsite.com`**. As well as allowing **`this.goodsite.com`** and **`that.goodsite.com`**, the keyword **`goodsite.com`** would allow sites that had the string goodsite.com in their URL, for example **`xxxgoodsite.com`**.

To filter a generic keyword enter it into one of the fields. You should exercise caution when choosing a keyword as sites that you may wish to block may be allowed if you choose too general a keyword.

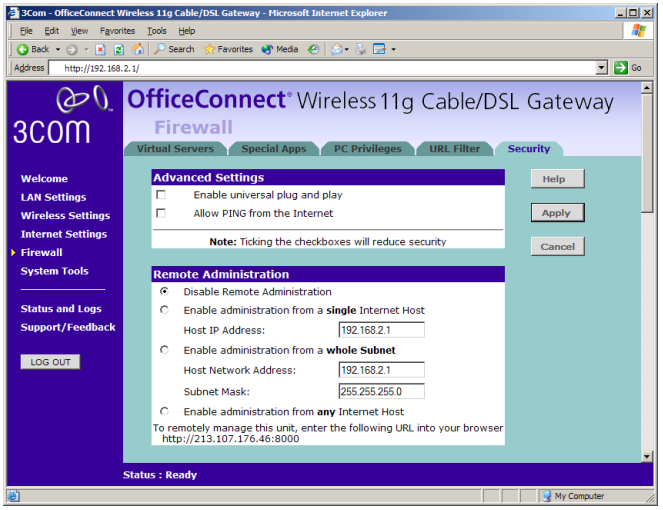
The Gateway filters all traffic from domains that have been blocked using the URL filter. If need to access an external mail server, FTP server or other named device outside your network, you must list it in one of the allow fields.

You can filter up to 30 keywords and URLs.

Computers that should not be subject to URL filtering can be excluded by ticking the Bypass URL Filter checkbox in the PC Privileges setup screen. See "PC Privileges" on page 67.

Security Select *Security* to display the Security screen (Figure 56).

Figure 56 Security Screen



The Internet connects millions of computer users throughout the world. The vast majority of the computer users on the Internet are friendly and have no intention of breaking into, stealing from, or damaging your network. However, there are hackers who may try to break into your network.

Enable universal plug and play Universal plug and play allows compatible software to read and change some the Gateway's firewall settings. This reduces the configuration required but lessens your control of the Gateway's firewall.

3Com recommends that you leave this feature disabled for maximum security.

Allow PING from the Internet PING is a utility, which is used to determine whether a device is active at the specified IP address. PING is normally used to test the physical connection between two devices, to ensure that everything is working correctly.

By default the Gateway has PING disabled in order to make the device more difficult to find on the Internet and less prone to attack.

This feature is enabled by clicking on the check box so that a tick can be seen and then select *Apply*.

3Com recommends that you leave this disabled.

Enabling Remote Administration

It is possible to administer the Gateway remotely. This can be set to one of four different levels using the following options:

1. *Disable Remote Administration* - This option is set as default.
2. *Enable administration from a **single** Internet Host* - Only the specified IP address can manage the Gateway. Any other users will be rejected.
3. *Enable administration from a **whole subnet*** - This option allows a number of users within a subnet to administer the Gateway.
4. *Enable administration from **any** Internet Host* - This options allows any host to access the administration pages.

To remotely administer your Gateway, enter **`http://xxx.xxx.xxx.xxx:8000`** in the location bar of the browser running on the remote computer, where *xxx.xxx.xxx.xxx* is the Internet IP address of the Gateway. You may then login using the administration password.

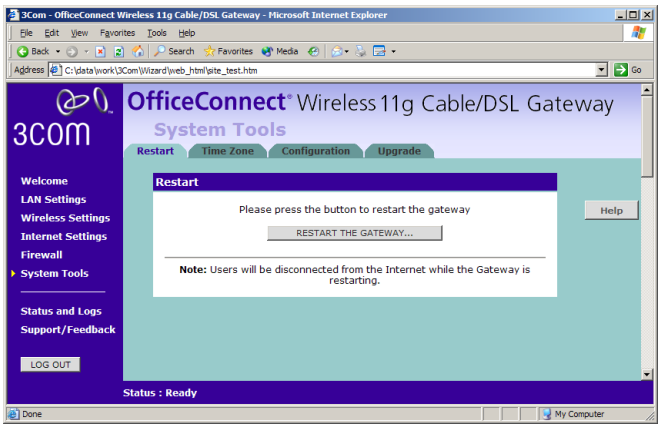
Your Internet IP address can be found at the bottom of the screen. See Figure 56.

System Tools

The main frame of the System Tools screen includes four administration items: *Restart, Time Zone, Configuration,* and *Upgrade* (Figure 57).

Restart

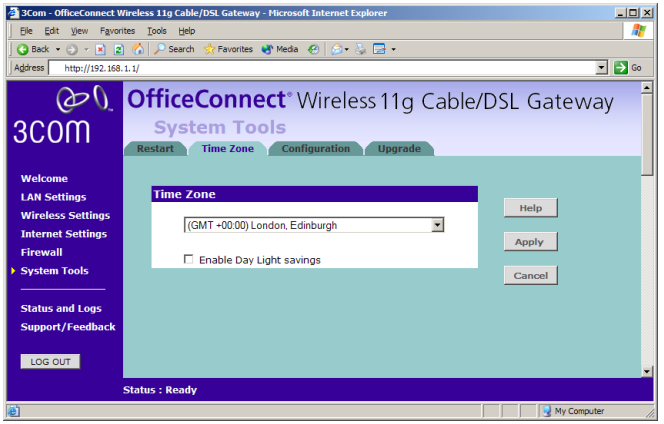
Figure 57 Restart Screen



If your Gateway is not operating correctly, you can choose to restart the Gateway by selecting *Restart the Gateway*, simulating the effect of power cycling the unit. No configuration information will be lost but the log files will be erased. This function may be of use if you are experiencing problems and you wish to re-establish your Internet connection. Any network users who are currently accessing the Internet 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 Gateway is operational again.

Time Zone

Figure 58 Time Zone Screen



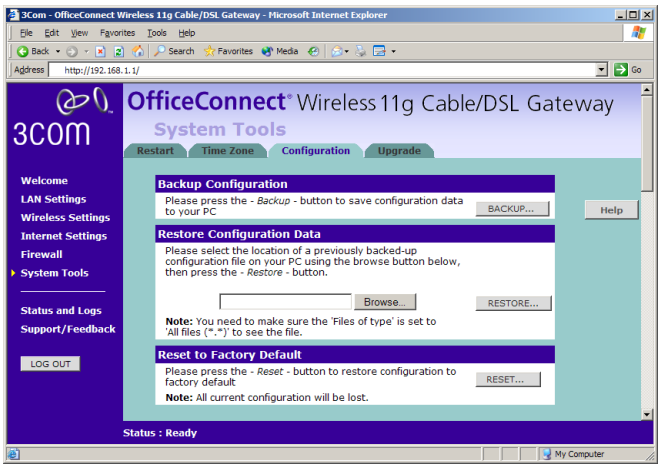
Choose the time zone that is closest to your actual location. The time zone setting is used by the system clock when displaying the correct time in the log files.

If you use Daylight saving tick the Enable Daylight savings box, and then click *Apply* (Figure 58).

The Gateway reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. It does not cause the system clock to be updated for daylight savings time automatically.

Configuration

Figure 59 Configuration Screen



Select the *Configuration* tab to display the *Configuration* screen (Figure 59).

Backup Configuration

Click *BACKUP* to save the current Gateway 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 Gateway's memory.

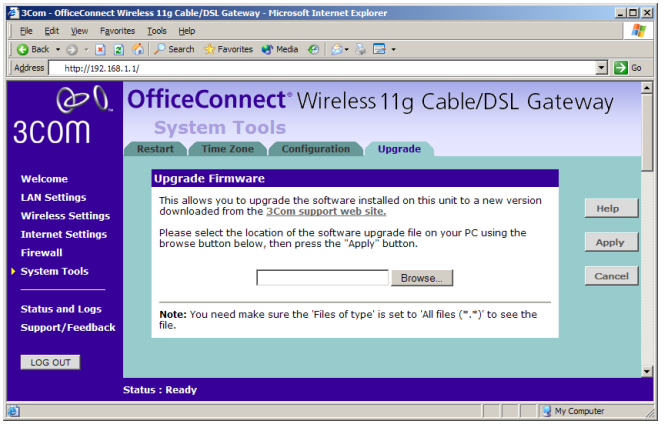
The password will remain unchanged.

Reset to Factory Default

If you want to reset the settings on your Gateway to those that were loaded at the factory, click *RESET*. You will lose all your configuration changes. The Gateway LAN IP address will revert to 192.168.1.1, and the DHCP server on the LAN will be enabled. You may need to reconfigure and restart your computer to re-establish communication with the Gateway.

Upgrade

Figure 60 Upgrade Screen



The Upgrade facility allows you to install on the Gateway 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 Gateway, and once this has completed, the Gateway 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 Gateway is lost while the new software is being copied to the Gateway).

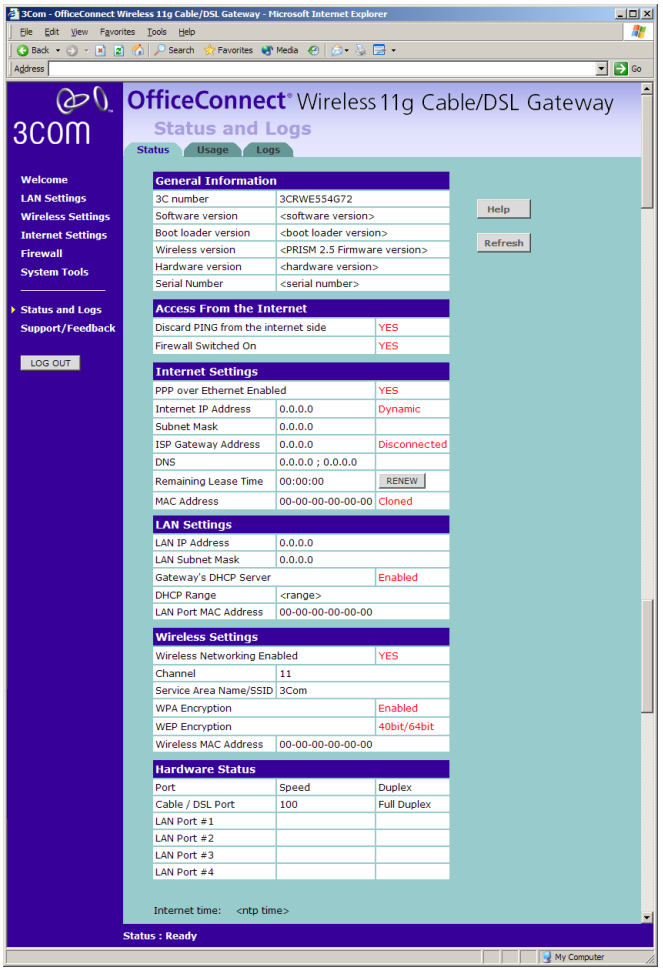
The upgrade procedure can take up to two minutes, and is complete when the Alert LED has stopped flashing and is permanently off. Make sure that you do not interrupt power to the Gateway during the upgrade procedure; if you do, the software may be corrupted and the Gateway may not start up properly afterwards.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

Status and Logs

Selecting *Status and Logs* from the main menu displays the *Status, Usage,* and *Logs* screens in your Web browser window.

Status The *Status* screen displays a tabular representation of your network and Internet connection. (Figure 61)

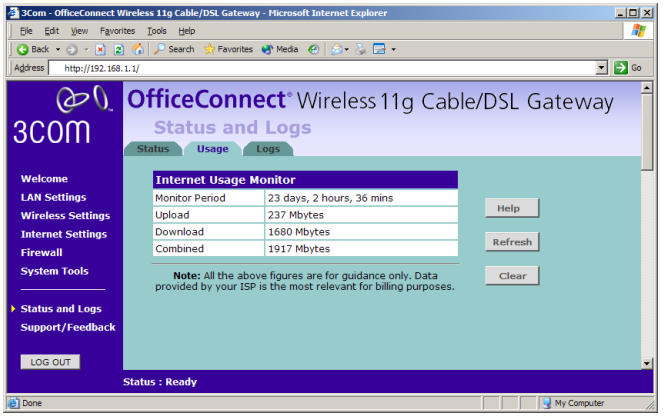
Figure 61 Status Screen



Usage Usage displays an approximate count of the traffic since the Gateway was last reset. (Figure 62)

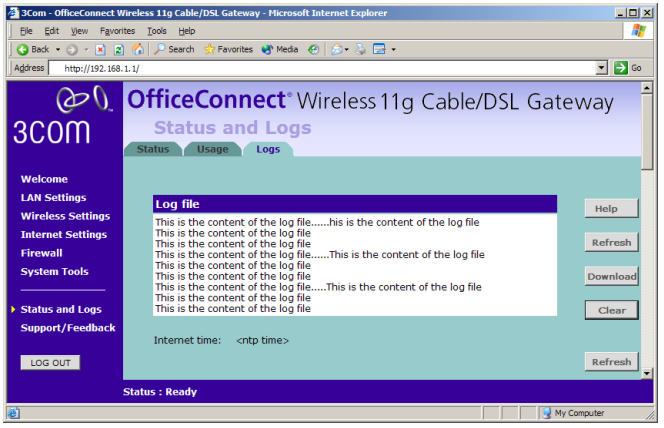
The counts are approximate and should be used as a guide only. Contact your ISP for accurate logging information.

Figure 62 Usage Screen



Logs Logs will allow you to view both the normal events, and security threats logged by the Gateway.

Figure 63 Logs Screen



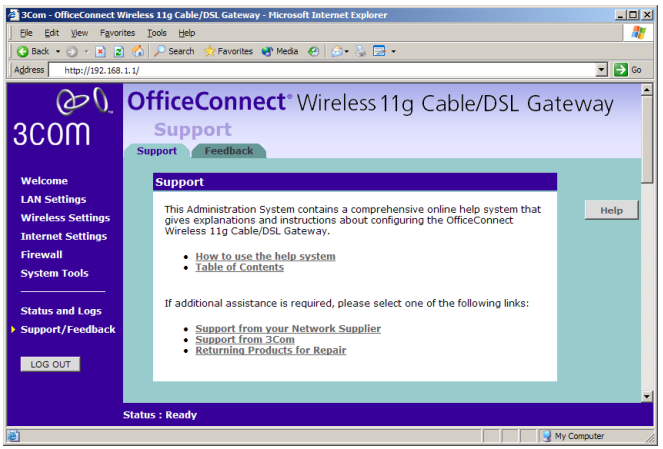
You may be asked to refer to the information on the Status and Logs screens if you contact your supplier for technical support.

Support/Feedback

Selecting *Support/Feedback* from the main menu displays the *Support* and *Feedback* screens.

Support

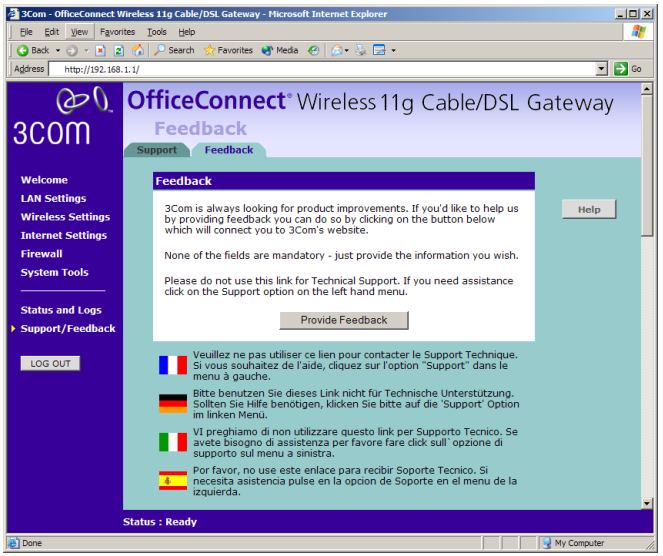
Figure 64 Support Screen



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 Gateway (Figure 64).

Feedback

Figure 65 Feedback Screen



Selecting the *Feedback* option displays the Feedback screen and allows you to provide feedback to 3Com on the operation of your Gateway (Figure 65). This screen should not be used to obtain technical support.

6 TROUBLESHOOTING

Basic Connection Checks

- Check that the Gateway is connected to your computers and to the cable/DSL modem, and that all the equipment is powered on. Check that the LAN Status and Cable/DSL Status LEDs on the Gateway are illuminated, and that any corresponding LEDs on the cable/DSL modem and the NIC are also illuminated.
- Ensure that the computers have completed their start-up procedure and are ready for use. Some network interfaces may not be correctly initialized until the start-up procedure has completed.
- If the link status LED does not illuminate for a port that is connected, check that you do not have a faulty cable. Try a different cable.

Browsing to the Gateway Configuration Screens

If you have connected your Gateway and computers together but cannot browse to the Gateway configuration screens, check the following:

- Confirm that the physical connection between your computer and the Gateway is OK, and that the LAN Status LEDs on the Gateway and NIC are illuminated and indicating the same speed (10Mbps or 100Mbps). Some NICs do not have status LEDs, in which case a diagnostic program may be available that can give you this information.
- Ensure that you have configured your computer as described in Chapter 3, *Setting Up Your Computers*. Restart your computer while it is connected to the Gateway to ensure that your computer receives an IP address.
- When entering the address of the Gateway into your web browser, ensure that you use the full URL including the http:// prefix (e.g. **`http://192.168.1.1`**).
- Ensure that you do not have a Web proxy enabled on your computer. Go to the *Control Panel* and click on *Internet Options*. Select the

Connections tab and click on the *LAN Settings* button at the bottom. Make sure that the *Proxy Server* option is unchecked.

- If you cannot browse to the Gateway, use the *winipcfg* utility in Windows 95/98/ME to verify that your computer has received the correct address information from the Gateway. From the *Start* menu, choose *Run* and then enter **`winipcfg`**. Check that the computer has an IP address of the form 192.168.1.xxx (where xxx is in the range 2-254), the subnet mask is 255.255.255.0, and the default Gateway is 192.168.1.1 (the address of the Gateway). If these are not correct, use the *Release* and *Renew* functions to obtain a new IP address from the Gateway. Under Windows 2000, use the *ipconfig* command-line utility to perform the same functions.
- If you still cannot browse to the Gateway, then use the Discovery program on the accompanying CD-ROM as described in Appendix A.

Connecting to the Internet

If you can browse to the Gateway configuration screens but cannot access sites on the Internet, check the following:

- Confirm that the physical connection between the Gateway and the cable/DSL modem is OK, and that the link status LEDs on both Gateway and modem are illuminated.
- Confirm that the connection between the modem and the cable/DSL interface is OK.
- Ensure that you have entered the correct information into the Gateway configuration screens as required by your Internet Service Provider. Use the "Internet Settings" screen to verify this.
- For DSL users, check that the PPPoE or PPTP user name, password and service name are correct, if these are required. Only enter a PPPoE service name if your ISP requires one.
- For cable users, check whether your ISP requires a fixed MAC (Ethernet) address. If so, use the *Clone MAC Address* feature in the Gateway to ensure that the correct MAC address is presented, as described on page 60.
- For cable users, check whether your ISP requires a fixed *Host Name*. If so, enter the required *Host Name* in the *Internet Settings* screen.
- Ensure that your computers are not configured to use a Web proxy. On Windows computers, this can be found under *Control Panel* > *Internet Options* > *Connections*.

Forgotten Password and Reset to Factory Defaults

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

1. Remove power from the Gateway.
2. Disconnect all your computers and the cable/DSL modem from the Gateway.
3. Using a straight through Ethernet cable, connect the Ethernet Cable/DSL port on the rear of the Gateway to any one of the LAN ports.
4. Re-apply power to the Gateway. The Alert LED will flash as the Gateway 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, remove power from the Gateway.
5. Remove the cable connecting the Cable/DSL port to the LAN port, and reconnect one of your computers to one of the Gateway LAN ports.
6. Re-apply power to the Gateway, and when the start-up sequence has completed, browse to:

   `http://192.168.1.1`

   and run the configuration wizard. You may need to restart your computer before you attempt this.
7. When the configuration wizard has completed, you may reconnect your network as it was before.

Wireless Networking

- Ensure that you have an 802.11b or 802.11g wireless adapter for each wireless computer, and that it is correctly installed and configured. Verify that each Wireless computer has either Windows 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 Gateway contains an Access Point that is designed to operate in Infrastructure mode. Ad Hoc mode is not supported by the Gateway.

- If you have a wired and a wireless NIC in the same computer, ensure that the wired NIC is disabled.
- Check the status of the Gateway 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 47 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 Gateway. The SSID is case-sensitive
- Ensure that the encryption method and level that you use on your clients are the same as those configured on the Gateway. The Gateway can simultaneously support WPA and WEP encryption, but can only support one configuration of each.
- Ensure that you have the Wireless computer enabled in the list of allowed MAC addresses if you are using Wireless Connection control on the Gateway.
- If you are having difficulty connecting or are operating at a low speed try changing the antenna positions on the rear of the Gateway. 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 Gateway to confirm that the building structure or fittings are not adversely affecting the connectivity. If this resolves the problem consider relocating the Wireless computer or the Gateway, or trying a different channel on the Gateway.
- Sources of interference: The 2.4Ghz ISM band is used for 802.11b and 802.11g. This is generally a licence free band for low power applications, and you may have other devices at your location that operate in this frequency band. You should take care to ensure that there are no devices like microwave ovens for example close to the Gateway 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 Gateway to establish whether this problem exists.
- Most wireless computer Adapters will scan the channels for the wireless Gateway. If a wireless computer has not located the Gateway 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 Gateway channel number. Please refer to your Wireless computer adapter documentation and vendor to do this.

- Speed of connection: The 802.11b and 802.11g standards will automatically choose the best speed depending on the quality of your connection. As the signal quality weakens then the speed falls back to a lower speed. The speeds supported by 802.11g are 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps. The speeds supported by 802.11b are 11 Mbps, 5.5 Mbps, 2 Mbps and 1 Mbps. In general the closer you are to the Gateway the better the speed. If you are not achieving the speed you had anticipated then try moving the antenna on the Gateway or moving the Wireless computer closer to the Gateway. In an ideal network the Gateway should be located in the centre of the network with Wireless computers distributed around it. Applications are generally available with the computer wireless card to carry out a site survey. Use this application to find the optimal siting for your wireless computer. Consult your Computer Card documentation and vendor for more details.

Power LED or Power Adapter OK LED Not Lit

- Check that your Gateway is receiving power by looking at the status of the Power LED on the front panel and the Power Adapter OK LED on the rear panel:
  - If both LEDs are lit green then the unit is receiving power.
  - If both LEDs are unlit then no power is being supplied to the unit. Check that the power adapter is plugged into a working mains outlet and that the mains outlet is supplying power. If the mains socket is supplying power then the power adapter or power adapter connection may be faulty. See "Replacement Power Adapters" below.
  - If the Power Adapter OK LED is lit but the Power LED is unlit then there may be a fault with your unit. Contact 3Com Technical Support.
- Check that you are using the correct power adapter for your Gateway. You should only use the power adapter supplied with your Gateway.

Replacement Power Adapters

If both the Power Adapter OK LED and Power LED are off, check your power adapter connection. If the mains outlet is working and is capable of supplying power to other devices, contact 3Com Technical Support and ask for a replacement power adapter. Please quote the power

adapter part number shown on the OfficeConnect power adapter you are using.

Alternatively, quote the part number for your region:

Table 3 Power Adapter Part Numbers

Part Number	Region
3C16740A	US and Canada
3C16741A	UK
3C16742A	Europe and Middle East
3C16743A	Japan
3C16744A	Australasia (except Japan and Korea)
3C16745A	South Africa
3C16747A	Korea
3C16748A	Argentina

Alert LED

The Alert LED will flash when the Gateway unit is first powered up while the system software checks the hardware for proper operation. Once the Gateway 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 Gateway, 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 Gateway software on the accompanying CD-ROM or 3Com web site (**`http://www.3com.com`**) and upload it to the Gateway 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.
- During normal operation, you may notice the Alert LED lighting briefly from time to time. This indicates that the Gateway has detected a hacker attack from the Internet and has prevented it from harming your network. You need take no specific action on this, unless you decide that these attacks are happening frequently in which case you may wish to discuss this with your ISP. The Gateway logs such attacks, and this information is available through the Status and Logs screens.

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 Gateway 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 Gateway unit in this state.

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

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

`www.3com.com`.

1. Remove power from the Gateway and disconnect the Cable/DSL modem and all your computers, except for the one computer with the software image.
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 Gateway.
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 Gateway.
5. Follow the on-screen instructions. Enter the path and filename of the software image file.
6. When the upload has completed, the Gateway will restart, run the self-test and, if successful, resume normal operation. The Alert LED will go out.
7. Refer to the Installation Guide to reconnect your Gateway to the Cable/DSL modem and the computers in your network. Do not forget to reconfigure the computer you used for the software upload.

   If the Gateway 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 Gateway to Factory Defaults?

See "Forgotten Password and Reset to Factory Defaults" on page 85.

How many computers on the LAN does the Gateway support?

A maximum of 253 computers on the LAN are supported.

How many wireless clients does the Wireless Cable/DSL Gateway support?

A maximum of 128 wireless clients are supported.

There are only 4 LAN ports on the Gateway. 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 Gateway. 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/`

Does the Gateway support virtual private networks (VPNs)?

The Gateway supports VPN passthrough, which allows VPN clients on the LAN to communicate with VPN hosts on the Internet. It is also possible to set up VPN hosts on your LAN that clients elsewhere on the Internet can connect to, but this is not a recommended configuration.

Where can I download software updates for the Gateway?

Updates to the Gateway 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

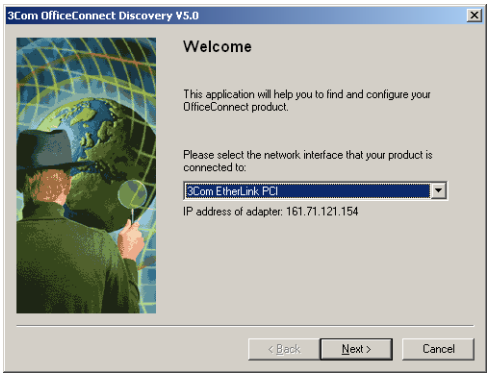
3Com provides a user friendly Discovery application for detecting the Gateway on the network.

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

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

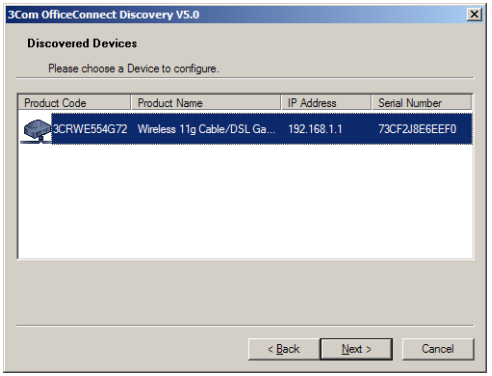
Discovery will find the Gateway even if it is unconfigured or misconfigured.

Figure 66 Discovery Welcome Screen



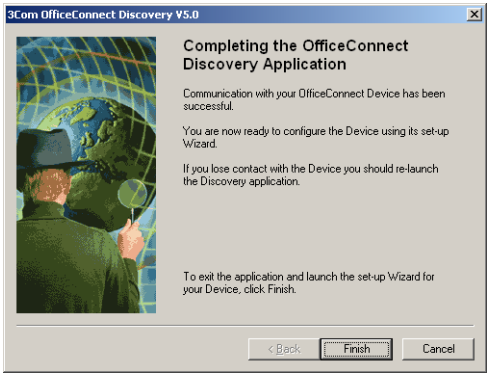
2 When the *Welcome* screen is displayed click on *Next* and wait until the application discovers the Gateways connected to your LAN.

Figure 67 Discovered Gateway Screen



3 Figure 68 shows an example Discovered Devices screen. Highlight the *Wireless Cable/DSL Gateway* by clicking on it, and press *Next*.

Figure 68 Discovery Finish Screen



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

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 Gateway over the Network

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

- An IP address
- A Subnet Mask

IP Addresses and Subnet Masks

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

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

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

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

The only value that will be different is the specific host device number. This value must always be unique.

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

Type One

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

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

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

See Table 4 for an example about how a network with three computers and a Gateway might be configured.

Table 4 IP Addressing and Subnet Masking

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

Type Two

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

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

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

See Table 5 for an example about how a network (only four computers represented) and a Gateway might be configured.

Table 5 IP Addressing and Subnet Masking

Device	IP Address	Subnet Mask
PC 1	192.168.100.8	255.255.0.0
PC 2	192.168.201.30	255.255.0.0
PC 3	192.168.113.155	255.255.0.0
PC 4	192.168.002.230	255.255.0.0
Gateway	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 Gateway contains a DHCP server, which allows computers on your network to obtain an IP address and subnet mask automatically. DHCP assigns a temporary IP address and subnet mask which gets reallocated once you disconnect from the network.

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

Static Addressing

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

Auto-IP Addressing

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

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

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

C TECHNICAL SPECIFICATIONS

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

Wireless 11g Cable/DSL Gateway

Interfaces

Cable/DSL modem connection — 10Mbps/100Mbps dual speed Ethernet port (10BASE-T/100BASE-TX)

LAN connection — four 10Mbps/100Mbps dual speed Ethernet ports (10BASE-T/100BASE-TX)

WLAN Interfaces

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

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

Encryption: 40/64 bit WEP, 128 bit WEP, WPA
Maximum clients: 128
O/P Power 18dBm

Operating Temperature

0 °C to 40 °C (32 °F to 105 °F)

Power

7VA, 23.9 BThU/hr

Humidity

0 % to 90 % (non-condensing) humidity

Dimensions

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

Weight

Approximately 500 g (1.1 lbs)

Standards

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

systems.
RSS-210

Environmental: EN 60068 (IEC 68)

*See "FCC Statement" on page 121 for conditions of operation.

System Requirements

Operating Systems

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

Wireless Performance

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

Wi Fi™
The Standard for Wireless Fidelity.

Cable Specifications

The Gateway 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 Gateway 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 Gateway with other OfficeConnect units.*

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

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

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

***WARNING**: There are no user-replaceable fuses or user-serviceable parts inside the Gateway. 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 Gateway erzeugt und verwendet Funkfrequenz (RF). In manchen Umgebungen ist die Verwendung von Funkfrequenz nicht gestattet. Erkundigen Sie sich bei den zuständigen Stellen, ob die Verwendung von Funkfrequenz in dem Bereich, in dem der Bluetooth Access Point eingesetzt werden soll, erlaubt ist.*

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

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

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

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

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

VORSICHT: *Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem Gateway 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: *La Gateway fournit et utilise de l'énergie radioélectrique (radio fréquence -rf). L'utilisation de l'énergie radioélectrique est interdite dans certains environnements. L'utilisateur devra se renseigner sur l'autorisation de cette énergie dans la zone prévue.*

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

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

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

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

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

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

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

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

E END USER SOFTWARE LICENSE AGREEMENT

3Com Corporation
END USER SOFTWARE LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

F ISP INFORMATION

Information Regarding Popular ISPs

WAN Types	Characteristics	Popular ISPs
Dynamic IP (Clone MAC)	Cable modem ISP, non-hostname based. Need to clone the MAC address in the Advanced tab of the Internet Settings page.	MediaOne, RoadRunner, Optimum Online, Time Warner, Charter, Adelphia, Metrocast.
Dynamic IP (Hostname)	Cable ISP, Requires Hostname to authenticate ie. cx213818-B. Need to enter the hostname in the Internet Settings page.	@Home Network, Cogoco, ComCast, Cox, Excite, Rogers, Shaw, Insight, Videotron
PPPoE (DSL)	Usually special software installed on PC, MacPOET/WinPOET, EnterNet 300. The Gateway has this software built in and you can remove it from your PC. You will need to enter the user name and password that your ISP provided to you in the PPPoE page of the Gateway. Leave the service name blank unless your ISP requires it.	Bell*, Century Tel, Citizens, Primus, Prodigy, Snet, Sprint FC, Verizon, First World, Brightnet, Earthlink, Ameritech, Covad, Mindspring, Sympatico DSL, USwest, Owest, SNet
PPTP	Cable or DSL, always on. Some European ISPs require a PPTP tunnel to authenticate their network.	KPN (Netherlands), Austria Telecom

Static (DSL)	DSL Modem, always on. Need to enter ALL IP information from ISP in the Static IP address section of the Internet Settings page.	CableSpeed, Cnet, Direct Link, Drizzle, DSL Extreme, Earthlink Wireless, Fast Point, Flashcom, GTE-WhirlWind, Heavenet, HSA Corp, I-55, InterAccess, LinkLine, Mission, Nauticom, NAS, Omitel, Onterra, Phatpipe, Rhythms, Speakeasy, Sterling, XO, Zyan
Static (Cable)	Cable Modem, Always on, ISP assigns specific IP information which needs to be entered on the "Fixed IP" page of the Gateway.	Cox Cable, Sprint, US Cable, Cable-Cable

*Bell includes Bell Advantage, Bell Canada, Bell South, PacBell and Southwestern Bell.

GLOSSARY

802.11b The IEEE specification for wireless Ethernet which allows speeds of up to 11 Mbps. The standard provides for 1, 2, 5.5 and 11 Mbps data rates. The rates will switch automatically depending on range and environment.

802.11g The IEEE specification for wireless Ethernet which allows speeds of up to 54 Mbps. The standard provides for 6, 12, 24, 36, 48 and 54 Mbps data rates. The rates will switch automatically depending on range and environment.

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

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

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

Ad Hoc mode Ad Hoc mode is a configuration supported by most wireless clients. It is used to connect a peer to peer network together without the use of an access point. It offers lower performance than infrastructure mode, which is the mode the gateway uses. (see also Infrastructure 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 Wireless Cable/DSL gateway 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.

DSL modem DSL stands for digital subscriber line. A DSL modem uses your existing phone lines to send and receive data at high speeds.

Encryption A method for providing a level of security to wireless data transmissions. The OfficeConnect Cable/DSL Gateway and Wireless Cable/DSL Gateway 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 gateway 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.

Gateway A device that acts as a central hub by connecting to each computer's network interface card and managing the data traffic between the local network and the Internet.

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.

Infrastructure mode Infrastructure mode is the wireless configuration supported by the Gateway. You will need to ensure all of your clients are set up to use infrastructure mode in order for them to communicate with the Access Point built into your Gateway. (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.

NAT Network Address Translation. NAT enables all the computers on your network to share one IP address. The NAT capability of the Gateway allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

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

PPPoE Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of data transmission originally created for dial-up connections; PPPoE is for Ethernet connections.

PPTP Point-to-Point Tunneling Protocol is a method of secure data transmission between two remote sites over the internet.

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

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.

universal plug and play Universal plug and play is a system which allows compatible applications to read some of their settings from the Gateway. This allows them to automatically configure some, or all, of their settings and need less user configuration.

URL Filter A URL Filter is a feature of a firewall that allows it to stop its clients form browsing inappropriate Web sites.

WAN Wide Area Network. A network that connects computers located in geographically separate areas (for example, different buildings, cities, or countries). The Internet is an example of a wide area network.

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

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

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

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

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

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

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

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

INDEX

A

Access Rights 69
Addresses
  IP 95
Administration Password 32, 43
Automatic Addressing 97

C

Cable Specifications 101
Channels 121
Clone MAC address 60
Configuration
  backup 77
  restore 77
Conventions
  notice icons, About This Guide 8
  text, About This Guide 8
Country Selection 30

D

DHCP 35, 38, 45, 97
DHCP Server 27
Discovery Application 93
DMZ 63
DNS 26, 36, 37, 60, 61, 63
  primary 36, 37, 59
  secondary 36, 37, 59
Dynamic 57
Dynamic IP Address 35, 57, 63

F

Firewall 63
Forgotten Password 85

G

Gateway 13

I

Internet
  addresses 95
Internet Addressing Mode 33
Internet Settings 57
  dynamic IP address 57
  PPPoE 57
  PPTP 57
  static IP address 57
IP Address 21, 36, 38, 45, 95
IP Allocation 58
ISP Connection 58
ISP Gateway Address 36

L

LAN 38, 44
LED 14
Login 94
Logs 80

M

MAC Address 35, 46
  deleting 54
  modifying 54

N

Network
  addresses 95
Networking
  wireless 85
NIC
  wireless 14

P

Password 29, 43
PC Privileges 67
PING 73
PPPoE 21, 28, 34, 57, 61
PPTP 21, 57, 62
Profile 55

R
Remote Administration 74
Reset to Factory Defaults 77, 85
Restart 75

S
Safety Information 19
Security 73
Setup Wizard 29, 44
Special Applications 65
Specifications
    technical 99
Static Addressing 97
Static IP Address 57, 59
Status 79
Subnet Mask 36, 38, 95
Summary 40
Support Information 80
Support Links 81

T
TCP/IP 25, 27, 38, 95
Technical
    specifications 99
    standards 99
Time Zone 32, 76

U
Unit Configuration 44
Upgrade 78
URL Filter 69

V
Virtual Servers 63, 64

W
WAN 33
Web Proxy 28
Wireless
    authorized PCs 53
    channel selection 47
    client list 55
    configuration 47
    connection control 53
    encryption 49
    LED 15
    networking 85
    NIC 14
    service area name 48
    settings 39, 47

Regulatory Notices for the Wireless 11g Cable/DSL Gateway

Channels

Use of the Wireless Cable/DSL Gateway 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, France*, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Liechtenstein, Lithuania, Luxembourg, Malaysia, Netherlands, New Zealand, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Russia, Saudi Arabia, Singapore, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, Uruguay, Venezuela.
1 - 11	Argentina, Brazil, Canada, Columbia, Mexico, Taiwan, United States
10 - 13	France*, Jordan
5 - 7	Israel
1-14	Japan

* The channels available for use in France depend on the region in which you are located.

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:**
3CRWE554G72	Wireless 11g Cable/DSL Gateway

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

- ANSI C63.4-1992 Methods of Measurement

- Federal Communications Commission 47 CFR Part 15, subpart B
  15.107 (a)Class B Conducted Limits
  15.109 (a)Class B Radiated Emissions Limits
- 15.107 (e)Class B Conducted Limits
  15.109 (g)Class B Radiated Emissions Limits

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

CE Statement (Europe)

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

CSA Statement

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

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

BSMI Statement

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

FCC

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

RF Exposure Compliance Statement (U.S.)

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

Potential RF Interference (Canada)

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

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

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

All specifications are subject to change without notice.

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

DUA0055-4AAA01
Rev. 01