WiFlyer™

User Manual

ALWAYS ON WIRELESS

Always On Wireless, Inc.
3701 Kirby • Suite 1090
Houston, Texas 77098
Phone 713.523.9334 • Fax 713.521.2120

Version 1.0; last updated September 29, 2004

Table of Contents

Introduction to the WiFlyer™ Base Station

T he WiFlyer™ base station is the world's first portable WiFi access point to provide wireless Internet access using either dialup or broadband connections. By simply connecting the WiFlyer to the nearest phone line or Ethernet cable, you can instantly create a WiFi hotspot with shareable Internet access at your home, hotel, or office – even internationally. Great for road warriors and homes and offices without DSL or cable, the pocket-sized WiFlyer is easily set up through an Internet browser, eliminating the hassles of software installation. Compatible with AOL®, MSN®, EarthLink®, and most dialup ISPs and broadband connections, WiFlyer is a great at providing wireless convenience anywhere you go.

WiFlyer features:

- Wireless WiFi / 802.11b Internet access using existing dial-up or broadband services.

- Sleek, portable design easily fits in any briefcase or laptop bag - or even in your pocket.

- Easy to install and use by connecting to a standard phone line or Ethernet broadband connection.

- Browser automatically defaults to intuitive WiFlyer web pages for easy dial setup.

- No software installation required – works with any WiFi-enabled Windows®, Linux®, UNIX®, Mac® OS and OSX® system.

- Fully compatible with acceleration software and services to achieve up to a 5x speed increase over standard dialup connections.

- Connect to a DSL or cable modem and share both wired and wireless connections.

- Quick-connect button eliminates time waiting for dial-up connection.

- Secure wireless communications using up to 128-bit WEP encryption and WiFi Protected Access (WPA).

- Unlike other travel WiFi base stations, includes full powered antennas for extended range.

- International design and approval for worldwide use.

WiFlyer is a wireless local area network (LAN) technology that provides high performance wireless communication between multiple computers and the Internet. When connected to the Internet, WiFlyer allows you to share a single Internet connection with more than one computer at the same time and share files between computers. To use WiFlyer to access the Internet, you need an account with an Internet service provider (ISP). Fees may apply. In addition, you need a traditional way to access the Internet, through a phone line, cable or DSL modem, or Ethernet network.

About the WiFlyer Base Station
The WiFlyer Base Station establishes a wired connection to the Internet and wireless connections to WiFi equipped computers. A 56K modem is built into the base station for dialup Internet access or you can use the Ethernet connection for cable or DSL broadband connections to the Internet.   There is a LAN Ethernet connection as well to connect wired computers or printers. The base station manages communications between the Internet and WiFi enabled computers. The WiFlyer Base Station can connect to the Internet in the following ways:

- Using a standard telephone line to connect to the modem (☎) port

- Using 10Base-T Ethernet to connect a cable or DSL modem or an existing Ethernet network with Internet access to the WAN (Internet) port

Once the base station is connected to the Internet, WiFi-equipped computers can connect to the Internet by joining the WiFlyer network. Computers connected to the WiFlyer network by Ethernet can also share the base station's Internet connection. See Chapter 3, "Setting Up Your WiFlyer Base Station," for instructions on how to set up the base station for Internet access and how to connect computers by Ethernet.

Package Contents
The WiFlyer package contains the following contents:

- WiFlyer Base Station

- Phone cord (RJ-11 connector)

- Power Adapter

- Quick Start Guide

- WiFlyer CD – contains User Manual, Easy Switch Broadband Installation software and additional enhancement software.

- Warranty/registration card

WiFlyer at a Glance
The rear side WiFlyer Base Station has four ports.
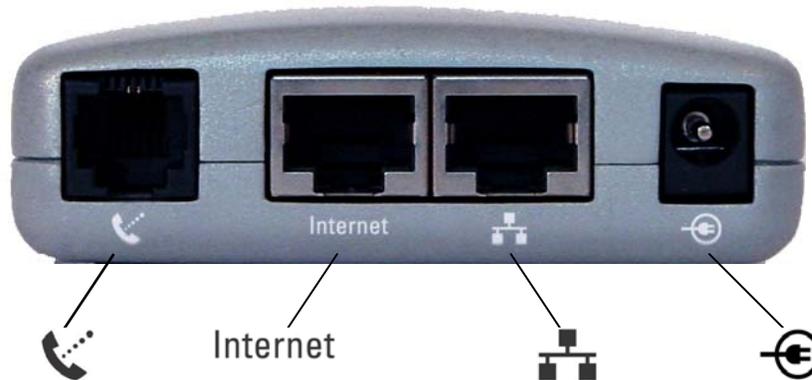
Port	Description
📞	**Internal modem port – for wireless access with a dialup connection** Connect one end of the phone cord to the internal modem port and the other end to a standard telephone jack.
Internet	**Ethernet WAN port – for wireless access with a broadband connection** Connect a DSL or cable modem or an existing Ethernet network with Internet access to the Ethernet WAN port on the WiFlyer Base Station.
🖧	**Ethernet LAN port – for Ethernet computers and printers without WIFi** Connect computers or printers with a network port but no WiFi to the Ethernet LAN port on the WiFlyer Base Station.
⊖	**Power adapter port** Plug the WiFlyer Base Station power adapter into the power adapter port and connect it to an electrical outlet.

Setting Up Your WiFlyer

What You Need to Set Up the WiFlyer Base Station for Internet Access
Before you set up the WiFlyer Base Station for Internet access, make sure of the following:

▪ You have a computer that is WiFi enabled, either with a wireless card or built in WiFi capability.

▪ Your computer has a current version of a web browser installed. Supported browsers include Internet Explorer, Safari, Netscape and Mozilla / Firefox.

▪ You have an account with an Internet service provider (fees may apply) or you have Internet access through a network.

▪ For more information on using WiFlyer with your Internet account, contact your Internet service provider (ISP) or go to the WiFlyer Support Knowledge Base at http://www.wiflyer.com

Powering up the WiFlyer
▪ Plug the WiFlyer Base Station power adapter into the power adapter port and connect it to an electrical outlet. The WiFlyer Base Station automatically turns on when the power adapter is plugged in and connected to an electrical outlet. There is no power switch.

When you plug in the base station the Power light indicator glows. This light indicates that the base station is starting up. The startup process takes about 20 seconds. See "WiFlyer Base Station Indicator Lights" for an explanation of the lights on the WiFlyer Base Station.

 Important
Use only the power adapter that came with your WiFlyer Base Station. Adapters for other electronic devices may look similar, but they may damage the base station.

Connecting to a Dial-up Internet Connection

Connect the WiFlyer Base Station to your standard phone line

- If you use a standard modem and analog telephone line (the type of telephone line found in most residences) to access the Internet, connect one end of the phone cord to the WiFlyer internal modem (📞) port and the other end to your telephone jack.

<div style="background:#eee">

Important

Do not plug the base station into a digital telephone line.

</div>

Connecting to a Broadband Internet Connection

Connect the WiFlyer Base Station to your DSL modem, cable modem, or network.

- If you have an Internet account that uses a device such as a DSL or cable modem, connect one end of the Ethernet cable to DSL or cable modem and the other end of the Ethernet cable to the Ethernet WAN (Internet) port on the WiFlyer Base Station.

WiFlyer Base Station Indicator Lights

The following explains what the lights on the WiFlyer Base Station mean.

Light	Indicator	Status
⏻	On / Off	**Power indicator** When the WiFlyer is connected to a power source, the indicator light is On.
📞	On / Off	**Modem indicator** When a connection is established with your ISP, the indicator light is On.
	Flashing	The indicator flashes as the WiFlyer is establishing a connection during dial up.
((•))	On / Off	**Wireless Network indicator** When a wireless network connection is established, the indicator is On.
	Flashing	The indicator flashes when data is crossing the port
🖧	On / Off	**LAN Port indicator** When a connection is made through the LAN port, the indicator is On.
	Flashing	The indicator flashes when data is crossing the port
○	On / Off	**WAN Port indicator** When a connection is made through the WAN port, the indicator is On.
	Flashing	The indicator flashes when data is crossing the port

Configuring Your WiFlyer Base Station

T his chapter describes how to perform the basic configuration of your WiFlyer Base Station. In order to use the browser-based Web Configuration Manager, your computer must have a modern web browser program installed.

Configuring the WiFi Network

The next step is connecting your PC or Mac to the WiFlyer WiFi network. For Windows XP use the following instructions. If your computer uses an operating system other than Windows XP consult the manual that came with your WiFi card or WiFi enabled system.

1. Right click the Wireless Network Connection icon on the bottom right hand corner of your screen. Ensure that the icon is the one for your wireless network connection and not for your Local Area Connection by passing the mouse cursor over each connection icon.

Wireless Network Connection Icon
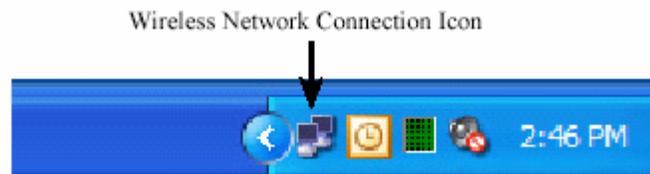
The following box should appear after you right click the Wireless Network Connection Icon.

Wireless Network Connection

The following wireless network(s) are available. To access a wireless network, select it from the list, and then click Connect.

Available wireless networks:

- wiflyer
- SMC
- drillinginfo

⚠ This wireless network is not secure. Because a network key (WEP) is not used for authentication or for data encryption, data sent over this network might be subject to unauthorized access.

☐ Allow me to connect to the selected wireless network, even though it is not secure

If you are having difficulty connecting to a network, click Advanced

[Advanced...] [Connect] [Cancel]

2. Highlight WiFlyer, by left clicking it, and check "Allow me to connect to the selected wireless network, even though it is not secure". To enable security features

3. Next click the connect button.

4. If WiFlyer is not listed under available wireless networks, click Advanced, otherwise go to step 5

    a. In the Wireless Network Connect Properties screen, click the refresh button next to the Available networks box. If nothing appears, make sure your wireless connection is turned on. There may be a manual switch on your computer to turn on your wireless connection, see the manual included with your machine to learn more.
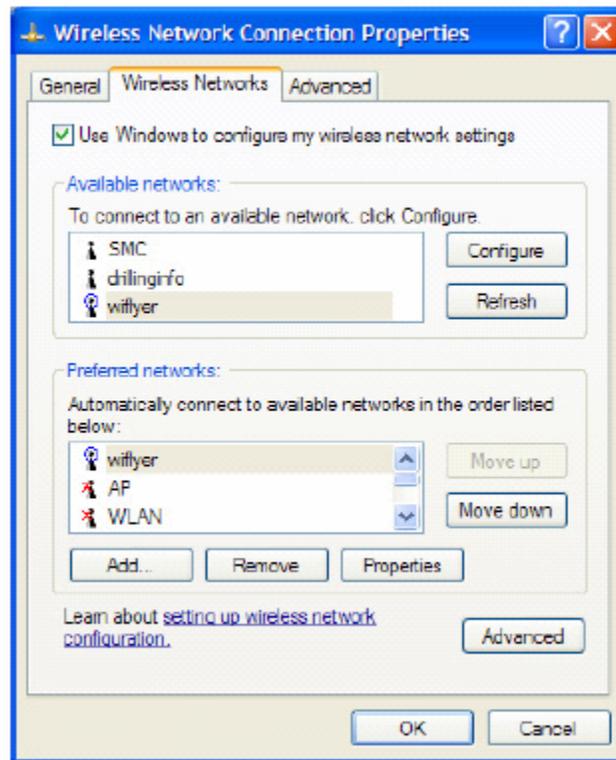
After you have clicked refresh the WiFlyer network will be listed.

    b.   Click OK.

    c.   In the "Available networks" box, highlight WiFlyer, and check "Allow me to connect to the selected wireless network, even though it is not secure".

    d.   Click connect.

5. Wait for "Connected to WiFlyer" to appear above the Wireless Network Connection icon on your taskbar.
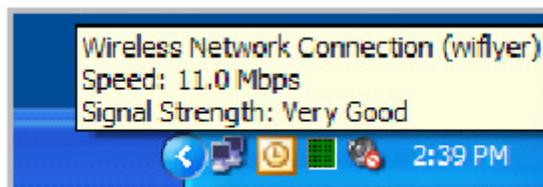
You are now on the WiFlyer WiFi network. Continue to the dialup section to connect for dialup, or skip to the broadband section to configure broadband connectivity.

Configuring the WiFlyer Using a Dial-up Connection

Use the following instructions if you connect to the internet using a dial-up connection.

1. Close your email client (Outlook®, Outlook Express®, Eudora®, etc)

2. Open a web browser.

   Your web browser should automatically connect to the WiFlyer dialup configuration page. If your browser does not connect to the dial page enter http://192.168.0.77 in the address bar of your browser.

3. Enter your ISPs access number, user name and password.

4. Select the country you are dialing from, and the connection type. Standard connection is used for all ISPs except AOL and MSN. If your ISP is AOL or MSN chose the AOL or MSN type.

5. Click Dial Now!

Your browser will switch to the Connection Status screen. The icons on the connection status screen will change color as your modem connection progresses. You are now connected to your ISP. Enjoy your dialup WiFlyer.

Configuring the WiFlyer Using a Broadband Connection

Use the following instructions if you connect to the internet using a broadband connection.

1. Open your web browser

   Your web browser should automatically connect to the WiFlyer dialup configuration page. If your browser does not connect to the dial page, enter http://192.168.0.77 in the address bar of your browser.

2. Click the Switch to Broadband button to change the WiFlyer into broadband mode.

3. In the broadband administration screen choose Static, DHCP, or PPPoE mode for your broadband connection. Most Ethernet connections are DHCP.

   a. If your provider requires a static IP address, enter the IP address settings in the Address Settings area.

   b. If your connection is PPPoE enter in your username and password in the PPPoE settings area.

4. Click save and you are connected to the internet.

WiFlyer Basic Menu Features

T he WiFlyer operates in two modes, dial-up and broadband. To make the base station as easy to use as possible each mode has been tailored to minimize the amount of information the user has to enter.

Dialup Configuration

Dial Configuration
The dial configuration page is the main page the user will use to configure and make dialup connections. This is the page you will enter the basic information needed to connect to your ISP. The only required entries on this page are Access Number, User name, Password and ISP.

Feature	Description
Access Number	The number you dial to access your Internet Service Provider (ISP) and connect to the internet.
Location	Optional entry to help you label the city or place you are dialing from
Save to phonebook	Select the checkbox to save the ISP access number to the phonebook
User name	The user name used to log into your ISP
Enter ISP password	The password used to log into your ISP
Remember Password	Select the checkbox to enable the WiFlyer to remember your password
Country	The country where you are dialing from. This entry sets certain country specific phone line properties to ensure proper international operation.
ISP	This feature implements specific dial settings required for some ISPs. This feature also determines what phone numbers are listed in the ISP lookup feature.

Feature	Description
	Select Default in every case your ISP is not explicitly listed.
	Select AOL®, MSN® or EarthLink® if any of those are your ISP.
Connection Status	Located in the top right hand corner of the dial page, connection status indicates if the WiFlyer is currently connected by modem and if so the speed of that connection.

Dial Options

Configure the advanced dialing options needed to connect to your ISP

Feature	Description
Dial this number before you reach an outside line	If you must dial a number to reach an outside line, enter the number in the field and select the checkbox to enable the feature.
Dial this number to turn off call waiting	Call waiting can disconnect your dialup connection. To turn off call waiting, select the checkbox and enter the required code (usually *70)
Ignore dial tone	Used in some international situations where the dial tone is not the standard dial tone
Rotary phone, not touch tone service	If you are using a rotary phone, select this option.
Voicemail on this phone (wait for carrier detect)	Select this option to allow the WiFlyer to wait for dial tone after the stuttering tone indicating a voicemail message
Enable redial	In the event of a busy signal at you ISP, you can enable the WiFlyer to redial the number by selecting this option.
Redial if line is dropped	If the modem connection is dropped, attempt to reconnect. The user may set the number and frequency of redial attempts.
Disconnect on no activity (minutes)	Disconnect modem after user defined amount of inactivity

WiFi Network Options

On this page you can configure the basic wireless access point settings. The external antenna option should only be chosen if you have an external antenna. The WiFlyer will not transmit if you have selected this option and have not connected an external antenna. Any new settings will not take effect until the access point is rebooted.

Feature	Description
SSID	This is the name of the WiFi network, which must be the same on the base station and the client machines. The default network name is WiFlyer, but no problems will be caused by changing it.
Channel	The frequency range or channel the base station transmits upon. Default channel is 6 but some users may want to change the channel to reduce interference with other WiFi devices.
Antenna	Change this setting if you are using an external antenna.

Local Network Options

On this page you can configure the local network settings for the WiFlyer

Feature	Description
LAN IP address	The IP addresses that the network uses to identify the WiFlyer. Unless absolutely necessary do not change the IP address of the WiFlyer.
Default gateway announcement using RIP	RIP - an interior gateway protocol defined by RFC 1058 that specifies how routers exchange routing table information.
Metric (cost) of using this gateway	Used only if RIP is enabled. The cost of the hop from one RIP enabled router to another.
DHCP server	The server that assigns IP addresses to machines using the WiFlyer. In almost all cases the DHCP server must be enabled.
DHCP address range start	First IP address of the DHCP range
DHCP address range end	Last IP address of the DHCP range
DHCP timeout in minutes	Amount of time before the DHCP client must request a new IP address

Phonebook

The phonebook feature of the WiFlyer allows you to store up to ten phone numbers used to connect with your ISP. The first nine numbers are user configurable, the tenth number is the last number entered into the dial configuration page.

Feature	Description

Feature	Description
Select	Allows the user to select the number to be entered into the dial configuration page
Location	Optional entry to allow the user to specify a city or place associated with the phone number
Access Number	Phone number for the ISP

Access Numbers

You may find ISP Numbers in your area using either the state or area code where you are located. Both state and area code are not required.

Feature	Description
Area Code	Area code of the dial up number you are looking for
State	State of the dialup number you are looking for.

Broadband Configuration Features

Broadband is the catch all term used to refer to cable, DSL and local Ethernet networks connected to the internet.

Broadband Configuration page
On this page you can configure the IP address settings used by the WAN port of the WiFlyer. For DHCP mode, you do not need to fill in the address settings. For static mode, the IP address settings must be entered below. Most ISPs use DHCP mode, check your ISP documentation to be sure.

Mode

Feature	Description
WAN Mode	Select the mode your ISP uses to assign IP addresses.
	Static – Least common ISP connection type
	DHCP – used by most cable modems and local networks
	PPPoE – used by most DSL providers

Address Settings

If you are using static mode, enter the static address information provided by your Internet Service Provider (ISP).

Feature	Description
Default IP address	The default IP address that the network uses to identify the WiFlyer.
Default subnet mask	A mask used to determine what subnet an IP address belongs to.
Default gateway	The gateway in a network that a computer will use to access another network if a gateway is not specified for use.
Primary DNS server	The primary server that translates domain names into IP addresses.
Secondary DNS server	The secondary server that translates domain names into IP addresses.

PPPoE Settings

PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. PPPoE is most commonly used by DSL providers.

Feature	Description
User name	Username provided by your ISP
Enter password	Password provided by your ISP
Confirm password	Repeat password
Authentication type	PAP or CHAP, choose the method used by your ISP, most ISPs currently use CHAP since it is more secure
Service Name	
MTU	Short for *Maximum Transmission Unit,* the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Only advanced users should change this setting.

Advanced Configuration Features

T his chapter covers the features in the Advanced Configuration section of the user interface. Features covered in this section include firmware upgrades, firewall and advanced network settings.

Administration

This page covers general administration of the WiFlyer, including firmware upgrades, reversion of all settings to factory defaults, and rebooting.

WiFlyer Firmware Upgrade

Firmware is the program that controls how the WiFlyer operates. Periodic firmware updates may be recommended to introduce new features to the WiFlyer or to fix problems that may be discovered with the device.

Feature	Description
File to upload	To upgrade the WiFlyer firmware, enter the name of the WiFlyer firmware upgrade file, and click on the Upgrade button. See chapter 7 for more details on the firmware upgrade process.

WiFlyer Control

Feature	Description
Reboot	Clicking the Reboot button will immediately reboot the WiFlyer. A reboot is necessary in order to change most configuration options.
Reset Configuration	Clicking the Reset Configuration button will reset all configuration options to factory default values, and the WiFlyer will reboot. Note the IP address of the WiFlyer will also be reset and it may be necessary to change the address in your browser

Feature	Description
	to access this website again.
WiFlyer Name	Name of the base station on the network
Allow configuration from the WAN interface	Enabling this setting allows the WiFlyer to be administered remotely over the internet
Port number for WAN web server	Outgoing port on the web server
Respond to ping requests on the WAN interface	Enables or disables ping responses from the internet

Advanced Wireless Features

To improve performance of wireless network some parameters can be configured to match your specific network.

Advanced Settings

Feature	Description
Maximum associated stations	Maximum number of WiFi stations the unit may communicate with
Fragmentation threshold	The size at which packets will be fragmented and transmitted a piece at a time instead of all at once. Setting the Fragmentation Threshold too low may result in poor performance.
RTS threshold	The packet size at which the AP will issue a Request to Send before sending the packet.
Beacon period	The amount of time in Kusecs (one Kusec equals 1,024 microseconds) between radio beacons from the base station to its client stations (laptops, PCs, etc). Beacons are packets sent by an Access Point to synchronize a wireless network.
DTIM interval	A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. This setting, always a multiple of the beacon period, determines how often the beacon contains a traffic indicator map (TIM). The TIM alerts stations in sleep state to stay awake long enough to receive their data frames.
Transmission rate (Mbits/s)	The maximum rate of transmission of the base station, or the method the base station negotiates downward with its clients in case it cannot transmit at maximum throughput.
Preamble type	Most modern base stations and clients support both the long and short preamble.

MAC Address Cloning

Some Internet Service Providers (ISPs) require that you tell them the address of the computer that is attached to your cable or DSL modem. The WiFlyer can modify its own address so that it appears to have the same address as a computer on your local network.

Feature	Description
Clone	Copies the MAC address of the Ethernet card installed by your ISP, and replaces the WAN MAC address with this Ethernet card MAC address. It is not recommended that you change the default MAC address unless required by your ISP.
MAC address cloning enabled	Enable MAC address cloning
MAC address	The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.

Demilitarized Zone (DMZ) Host

A DMZ host is a single computer on the local network that is exposed to the external network. The WiFlyer implements virtual DMZ by sending all packets that cannot be translated to the DMZ host.

The WiFlyer will forward all unsolicited connections to the DMZ address. If the DMZ is enabled then the port filters specified on this page will limit the packets which are forwarded to the DMZ host. The general port filters page can be used to limit packets which the DMZ host can send to the Internet.

If you have a client PC that cannot run Internet applications properly from behind the base station, then you can set the client up to unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP Address of the internal computer that will be the DMZ host. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

Feature	Description
DMZ enabled	Enable the DMZ
DMZ address	Enter the IP Address of the internal computer that will be the DMZ host.

DMZ Port Filtering Configuration

Feature	Description
Enabled Name	Name of the network service being forwarded, optional field
Source IP Start	The beginning IP address that is allowed to send packets to the DMZ
Source IP End	The ending IP address that is allowed to send packets to the DMZ
Protocol	Select the protocol type, UDP or TCP
DMZ Port Start	The beginning port range that will be allowed to send packets to the DMZ
DMZ Port End	The ending port range that will be allowed to send packets to the DMZ

Virtual Server Configuration

Virtual server is also called *port forwarding*, and is where the WiFlyer forwards all traffic received on an external port to a computer on the internal network. A virtual server is required when internal computers need to run network servers, such as a web-server.

The WiFlyer can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP Address can be automatically redirected to local servers in the LAN (Local Area Network). The WiFlyer firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the WiFlyer are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the WiFlyer redirects the external service request to the appropriate server within the LAN network.

Note: Using the same port number for a virtual server that is being used by the WiFlyer for the web-server or upgrade service will prevent the WiFlyer services from working. The default ports for the webserver and upgrade service are TCP port 80 and UDP port 69.

Feature	Description
Enabled Name	Enter the name referencing the virtual service.
IP Address	The server computer in the LAN (Local Area Network) that will be providing the virtual services.
Private Port	The port number of the service used by the Private IP computer.
Protocol	The protocol used for the virtual service.
Public Port	The port number on the WAN (Wide Area Network) side that will be used to access the virtual service.

Port Trigger Configuration

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the WiFlyer. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Feature		Description
Enabled Name		Name of the network service being forwarded, optional field
Trigger Ports	Protocol	TCP or UDP for incoming port
	Ports From	This is the first port used to trigger the application. It can be either a single port or a range of ports.
	Ports To	This is the ending port used to trigger the application.
Port Range to Open	Protocol	TCP or UDP for incoming port
	Ports From	This is the first outgoing port for the application.
	Ports To	This is the last outgoing port in the range for the application.

Security Features

T he WiFlyer has several security features that allow users to safely connect to the internet and protect themselves from network intrusions.

Base Station Password

Feature	Description
Enable password	If the password feature is enabled, users must enter a password to log into the WiFlyer.
Enter configuration password	Enter a password to log onto the WiFlyer
Confirm password	Enter the password a second time to confirm

Wireless Security

Security settings including WEP, WPA, and access point visibility. Wired Equivalent Privacy (WEP) can be used to protect wireless network traffic from eavesdroppers and to restrict unauthorized wireless users from accessing the network via the WiFlyer. WiFi Protected Access (WPA) is a security method like WEP but more secure. WPA is not supported by all WiFi cards.[*]

---

[*] WPA firmware upgrade for the WiFlyer will be supplied in the 4th quarter of 2004.

AP Visibility

When Invisibility is selected, the base station is protected against discovery by wireless sniffers, and all wireless clients must explicitly use and know the SSID.

Feature	Description
Visibility Status	You can disable the SSID broadcast. This requires network users to configure their wireless network card by manually entering the network name.

WEP Configuration

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the access point and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. If you leave a key box blank then this means a key of all zeros

Feature	Description
Enable WEP	Select Enabled or Disabled. Disabled is the default setting.
	Short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
WEP key lengths	Select the level of encryption desired: 64, or 128-bit.
	In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.
WEP key 1 - 4	Input up to 4 WEP keys; and select the one you wish to use.
Default WEP key to use	Select the default WEP key
Deny unencrypted data	Only allow encrypted data over the network
Authentication	Open or Shared. Open means any system may send packets on the network, although the packets may be

Feature	Description
	rejected if they use the wrong WEP key. Shared requires the correct WEP key or clients may not send packets on the network.

WPA Configuration

If personal WiFi Protected Access (WPA-PSK) is enabled, a pass phrase is needed to associate with the key. Enter a phrase between 8 and 63 characters.

Feature	Description
Enable WPA	Select Enabled or Disabled. Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology includes two improvements over WEP: Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.
Pass phrase	Add a user authentication pass phrase.

Wireless Address Filtering

Each wireless station has a unique address, also known as a MAC address. By restricting the MAC addresses that can connect to the wireless interface, unauthorized users can be excluded from using the WiFlyer.

Feature	Description
Enable access control	Choose to disable MAC filters, or choose to allow or deny MAC addresses listed below.
MAC address 1 – 16	Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Internet.

Port Filtering Firewall

Port filtering is used to limit the applications that can send traffic through the WiFlyer. It can be used to limit network access by local users, for example, to prevent the use of instant messaging software. Port filtering is handled separately for the DMZ Host.

A firewall is a program that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet will want a firewall to prevent outsiders from accessing its own private data resources.

> **Note:**
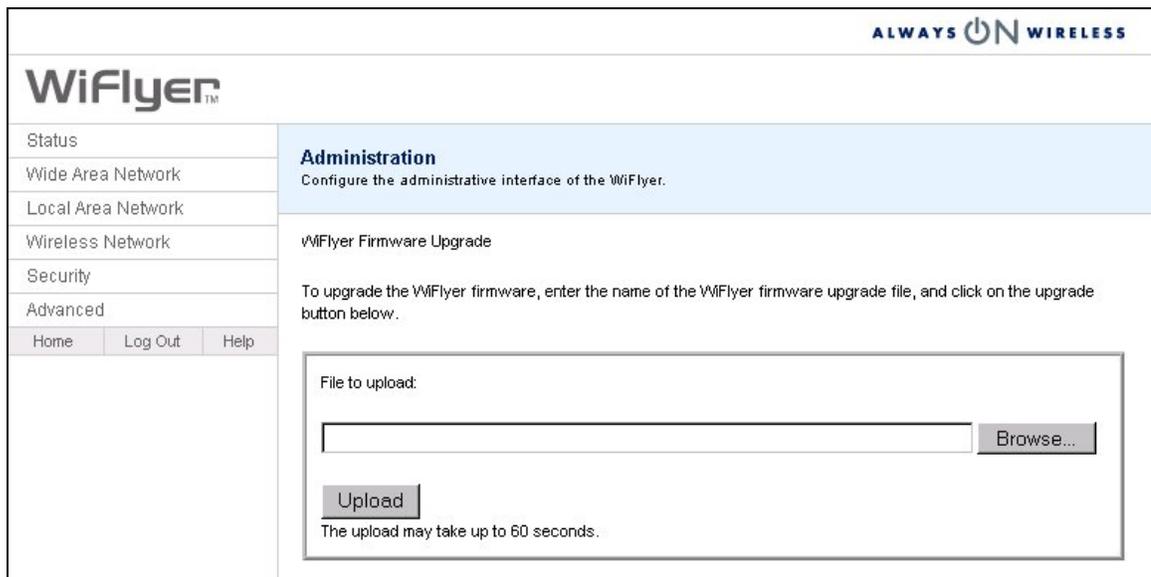> The WiFlyer MAC Address filtering rules have precedence over the Firewall Rules.

Feature	Description
Enabled Name	Optional field to indicate the name of the network application
Source IP Start	Enter the incoming IP address range for the rule, not required.
Source IP End	
Destination IP Start	Enter the local IP Address range for the rule, not required.
Destination IP End	
Protocol	TCP or UDP
Destination Port Start	First port in prohibited inbound range
Destination Port End	Last port in prohibited inbound range

Troubleshooting and FAQs

Upgrading the WiFlyer Firmware

If you experience problems with your WiFlyer or to access additional features that may be provided after your purchase, it may be necessary to upgrade the firmware. To upgrade the firmware, complete the following procedures:

1. Save the new firmware file from the wiflyer.com support site. The file will have a .BIN extension.

2. From the Advanced menu, select Administration. The Advanced page appears.

3. Click the Browse button to navigate to the folder where you saved the new firmware file.

4. Select the file.

5. Click the Upload button.

The WiFlyer will reboot automatically.

Checking the WiFlyer Status

To check the WiFlyer status, complete the following procedure:

▪ From the Advanced menu, select Status. The Information page appears.

ALWAYS ⏻N WIRELESS

WiFlyer™

| Status |
| Wide Area Network |
| Local Area Network |
| Wireless Network |
| Security |
| Advanced |
| Home | Log Out | Help |

Information
Basic information about the WiFlyer.

NOTE: You may need to reload this page to see the current settings.

General
Firmware Revision: 090204B
SDK Revision: 5.4.B2.1249
WAN
Mode: Static IP Address
MAC address: 08000E200000
IP address: 192.168.2.50
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1
Primary DNS server: 10.10.10.5
Secondary DNS server: 10.10.10.10
LAN
MAC address: 08000E200000
IP address: 192.168.0.77
Wireless LAN
SSID: wiflyer
Channel: 6
WEP in use: No
Active DHCP Server Leases
000BDB9F37B1: 192.168.0.109

Connect speed:

The Information page contains the following:

Feature	Description
Firmware Revision	The version of firmware installed on the WiFlyer.
WAN Mode	The WAN mode will display the mode your ISP uses to assign IP addresses. The WAN mode can either be Static, DHCP, or PPPoE. If you are using the Static mode, you must manually enter the IP address, subnet mask, and default gateway settings. Under DHCP and PPPoE, the settings are assigned automatically. You can set the WAN Mode on the Broadband Configuration page.
MAC address	The MAC address of the WAN port. If you enable MAC address cloning from the Advanced Configuration page, this is the MAC address that is cloned.
IP address	The IP address of the WiFlyer.
Subnet mask	If you are using the Static mode, you must manually enter the Subnet mask. If you are using DHCP or PPPoE mode, the setting is assigned automatically.
Default gateway	If you are using the Static mode, you must manually enter the Default gateway. If you are using DHCP or PPPoE mode, the setting is assigned automatically.
Primary DNS server	The primary Internet service that translates domain names into IP addresses. If you are using the Static mode, you must manually enter the Primary DNS server. If you are using DHCP or PPPoE mode, the setting is assigned automatically.
Secondary DNS server	The secondary Internet service that translates domain names into IP addresses. If you are using the Static mode, you must manually enter the Secondary DNS server. If you are using DHCP or PPPoE mode, the setting is assigned automatically.
LAN MAC address	The MAC address of the LAN.
IP address	The LAN IP address. If this default LAN IP address is already used on your network, you may experience IP address conflicts. WiFlyer strongly advises against changing this setting from the default.
Wireless LAN SSID	Short for service set identifier. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.
Channel	The wireless channel used by your wireless network.

Feature	Description
WEP in use	Shows whether WEP security is enabled.
Active DHCP Server Leases	Lists the MAC address and IP address for each client that is connected to the WiFlyer DHCP server.

WiFlyer Specifications

Power Supply

Use only the supplied power adapter with your WiFlyer. Use of any other power supply may damage your unit and invalidate approvals.

Federal Communications Commission (FCC) Statement

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

The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment must be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This Equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

You can determine if your system is causing harmful interference by turning it on and off. Once your system is off, if the interference stops it is probably being caused by your system.

There is no guarantee that interference will not occur in any particular installation. If this equipment does cause harmful interference to radio or television reception the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Important: Changes or modifications to this product not authorized by Always On Wireless, Inc. could void the EMC compliance and negate your authority to operate the product.

This product was tested for FCC compliance under conditions that included the use of Always On Wireless shielded cables and connectors between components. It is important that you use Always On Wireless shielded cables and connectors to reduce the possibility of causing interference to radios, television sets, and other electronic devices. You can obtain proper cables and connectors through Always On Wireless authorized dealers.

Industry Canada Statement
This class B device meets all requirements of the Canadian interference-causing equipment regulations.

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

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

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

This equipment must be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device has been designed to operate with an antenna having a maximum gain of 6 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.