WiFlyer+v

User Manual

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

Version 1.0; last updated May 5, 2006

Table of Contents

Chapter

1

Introduction to the WiFlyer®+v Base Station

The portable WiFlyer+v wireless bridge allows you to instantly set up all your office communications needs. Simply connect to any wireless WiFi network to enable a high-quality Internet phone line, two Ethernet data ports and a USB network printer connection.

Affordable Internet Phone Line
Over broadband WiFi, the WiFlyer+v provides a standard telephone connection with its own local telephone number, unlimited calling in the U.S. and Canada, and advanced premium features such as Call Waiting, Caller ID, 3-way Conferencing and Voice Mail.

Never Miss Calls
Select to ring your Internet phone and cell phone at the same time & you can pick up the call wherever more convenient. At home, use the Internet phone instead of your cell phone to reduce cell phone charges & improve call quality.

No Dedicated Phone Required
If you already have an existing phone and landline, you can share it for Internet calling too. Internet calls ring twice while Call Waiting allows switching between the two lines.

Convenient, Wireless Printing
Connect a printer directly to its USB or Ethernet port and print from any desktop or laptop computer on the local wireless network.

Long Range, High-Speed Ethernet
Connect your desktop or laptop computer directly to a 10/100 Ethernet port to get a faster, more reliable data connection at longer ranges than using an ordinary WiFi adapter. To further extend range, easily upgrade to a hi-gain antenna through a standard SMA connector.

WiFlyer+v features:

- Triple mode operation, WiFi bridge, WiFi broadband Access Point and WiFi dialup access point.

- Wireless WiFi / 802.11 b/g Internet access using existing WiFi, broadband or dial-up or services.
- Internet Phone capability
- Print server
- Sleek, portable design easily fits in any briefcase or laptop bag - or even in your pocket.
- Easy to install and use by connecting to any available WiFi network, Ethernet broadband connection or standard phone line.
- Browser automatically defaults to intuitive WiFlyer+v web pages for easy dial setup.
- No software installation required – works with any WiFi-enabled Windows®, Linux®, PocketPC®, PalmOS®, Mac® OS and OSX® system.
- Secure wireless communications using WPA or WEP encryption.
- Designed for international use and includes auto-switching 120-240v power supply

Package Contents

The WiFlyer+v package contains the following contents:

- WiFlyer+v Base Station
- Ethernet Cables (x2)
- Power Adapter
- Quick Start Guide.
- Warranty/registration card

WiFlyer+v at a Glance

The rear side WiFlyer+v Base Station has four ports. They are from left to right, the phone port, the Ethernet WAN port, the Ethernet LAN port and the power adapter port.

Port	Description
	**Internal modem port – for wireless access with a dialup connection** Connect one end of the phone cord to the WiFlyer modem port and the

other end to a standard telephone wall 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+v 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+v Base Station.

Power adapter port

Plug the WiFlyer+v Base Station power adapter into the power adapter port and connect it to an electrical outlet.

Left View of the WiFlyer+v

The left side of the WiFlyer+v has two ports and a volume control slider

The rear port is for a standard telephone. This port is for the phone you will use to make your Internet Phone calls. If you plug in your standard landline to the modem port of the unit you can make standard calls over the traditional phone system with this phone as well.

The port towards the front of the unit is the USB port. Plug your printer into the USB port and you will be able to use your printer with any PC on the wireless network.

The volume slider at the front of the unit allows you to control the volume of the speaker during dialup connections.

Right View of the WiFlyer+v

The button on the right side of the WiFlyer+v allows you to quickly connect and disconnect your WiFlyer+v to dialup once you have configured the unit. Once you have entered your dialup settings on the dial configuration page if you wish to connect or

disconnect from your ISP simply press the button. If you are currently disconnected from your ISP the WiFlyer+v will dialup and make a connection with the settings you have entered on the dialup configuration page. If you are connected the WiFlyer+v will cleanly disconnect your ISP connection and free your phone line for voice use.

The button also allows you to reset the unit to factory defaults. To reset the unit to factory defaults follow the procedure outlined in Appendix A, Troubleshooting

Top View of WiFlyer+v
The indicator lights of the WiFlyer+v are on the top of the unit. These lights flash as the WiFlyer+v is engaged in various activities.

Light	Indicator	Status
	On / Off	**Power indicator** When the WiFlyer+v 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+v is establishing a connection during dial up.
	On / Off	**Message Light** When there is a voicemail message on the VoIP line the indicator is On.
	On / Off	**Internet Phone** When internet phone service is available, the indicator is On.
	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.

Chapter

2

Setting Up Your WiFlyer+v

What You Need to Set Up the WiFlyer+v

Before you set up the WiFlyer+v for Internet access, make sure of the following:

- You have a computer that is network enabled, with an Ethernet port, wireless card or built in WiFi capability.
- Your computer has a current version of a web browser installed. Supported browsers include Internet Explorer, Safari, Opera, Netscape and Mozilla / Firefox.
- You have an account with an Internet service provider over WiFi, Broadband or dialup.

Powering up the WiFlyer+v

Plug the WiFlyer+v power adapter into the power adapter port and connect it to an electrical outlet. The WiFlyer+v 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 unit the Power light indicator glows. This light indicates that the base station is starting up. The startup process takes about 20 seconds. See “WiFlyer+v Indicator Lights” for an explanation of the lights on the WiFlyer+v.

Important

Use only the power adapter that came with your WiFlyer+v. Adapters for other electronic devices may look similar, but they may damage the unit.

WiFlyer+v Modes of Operation

The WiFlyer+v is a 3 mode device that can connect to the internet over WiFi, Broadband or Dialup connections. The following chapters describe how to connect your WiFlyer+v to the internet in each of the three modes of operation.

Chapter

3

Bridge Mode

Bridge Mode is the default mode of the WiFlyer+v. Bridge mode is used to connect the WiFlyer+v to a WiFi network. This WiFi network can be your existing home WiFi network, a Muni WiFi network or a network created by another WiFlyer+v in Access Point mode.

To connect your WiFlyer+v to an existing WiFi network

1. Plug in the power on the WiFlyer+v
2. Connect an Ethernet cord into your laptop on one end and the port next to the power supply on the WiFlyer on the other.
3. Open a web browser on your laptop and if you are not automatically redirected to the WiFlyer configuration page go to http://192.168.2.1.
4. You should now be on the WiFlyer's login page. Initially there is no password on the WiFlyer so leave the password blank and click login.
5. You will now see a list of wireless access points the WiFlyer sees in your area, click on the network name of the network you would like to connect to.
6. You should now be on the Wireless Networking page. If security is set up on the wireless network you will need to enter your WPA or WEP key in the fields at the bottom of the screen. Click connect and the WiFlyer+v will reboot.
7. Once the WiFlyer+v has rebooted wait 30 seconds for the unit to calibrate the network connection. Once that is complete you are connected to the internet.

Chapter

4

Broadband Access Point Mode

Connecting to a Broadband Internet Connection

Connect the WiFlyer+v Base Station to your DSL modem, cable modem, or local area 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 port on the WiFlyer+v Base Station.

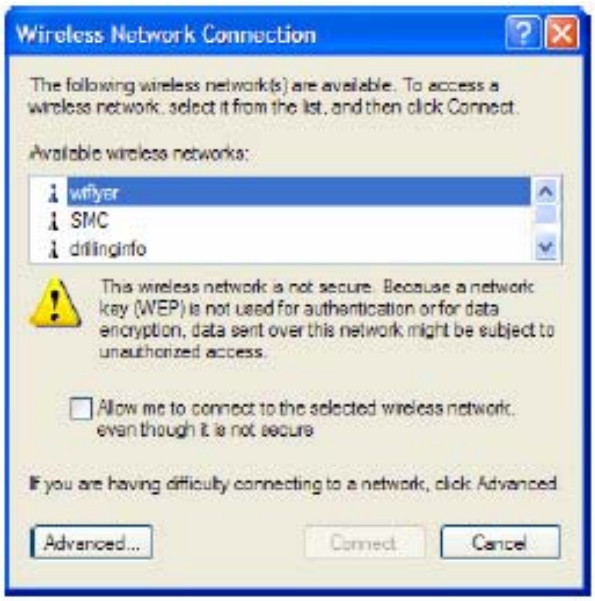
Configuring the WiFi Network

The next step is connecting your computer to the WiFlyer+v 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.

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

Next, scroll up/down to “View Available Wireless Network” and left click on it.

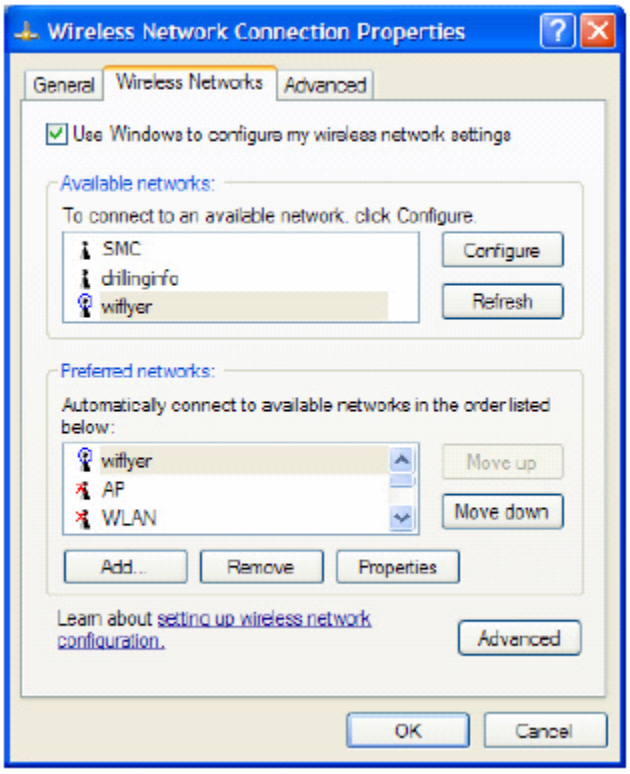


2. Highlight WiFlyer+v, by left clicking it, and check “Allow me to connect to the selected wireless network, even though it is not secure”. To enable security features see Chapter 6.

3. Next click the connect button.

4. If WiFlyer+v 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.



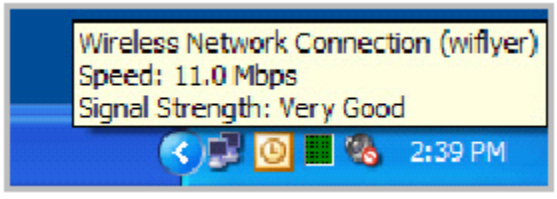
After you have clicked refresh the WiFlyer+v network will be listed.

b. Click OK.

c. In the "Available networks" box, highlight WiFlyer+v, 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+v" to appear above the Wireless Network Connection icon on your taskbar.



You are now on the WiFlyer+v WiFi network. Continue to the dialup section to connect for dialup, or skip to the broadband section to configure broadband connectivity.

Configuring the WiFlyer+v Using a Broadband Connection

After you have connect to the Wiflyer+v's wireless network you will need to configure your broadband connection to the internet. To configure your internet connection:

1. Open your web browser.

2. Your browser should automatically connect to the WiFlyer+v broadband configuration page. If your browser does not connect to the broadband configuration page enter http://192.168.2.1 in the address bar of your browser.

3. In the broadband administration screen choose Static, DHCP, or PPPoE mode for your broadband connection. Most cable modem connections are DHCP, while most DSL connections are PPPoE.
   a. If your provider requires a static IP address enter the IP address settings in the Address Settings area. Consult the documentation provided by your ISP for more information.
   b. If your connection is PPPoE enter your username, password, and authentication method in the PPPoE settings area.

   Most PPPoE connections use PAP for authentication, if you are having trouble connecting try switching your authentication method to CHAP.

4. Click save.

5. Click connect and you are free to surf the Internet wirelessly!

Chapter

5

Dialup Access Point Mode

The first step to use the WiFlyer+v with dialup is connecting the phone line to your unit. Connect one end of the phone cord to the WiFlyer+v internal modem port and the other end to your telephone jack.

Important

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

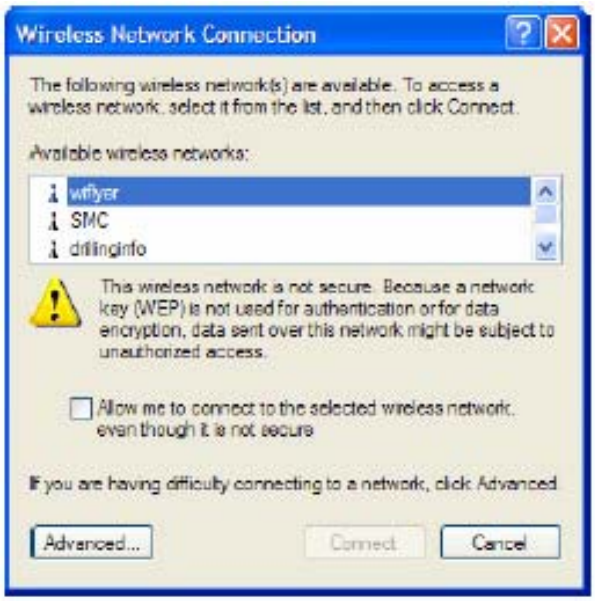
Configuring the WiFi Network

The next step is connecting your computer to the WiFlyer+v 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.

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

Next, scroll up/down to “View Available Wireless Network” and left click on it.

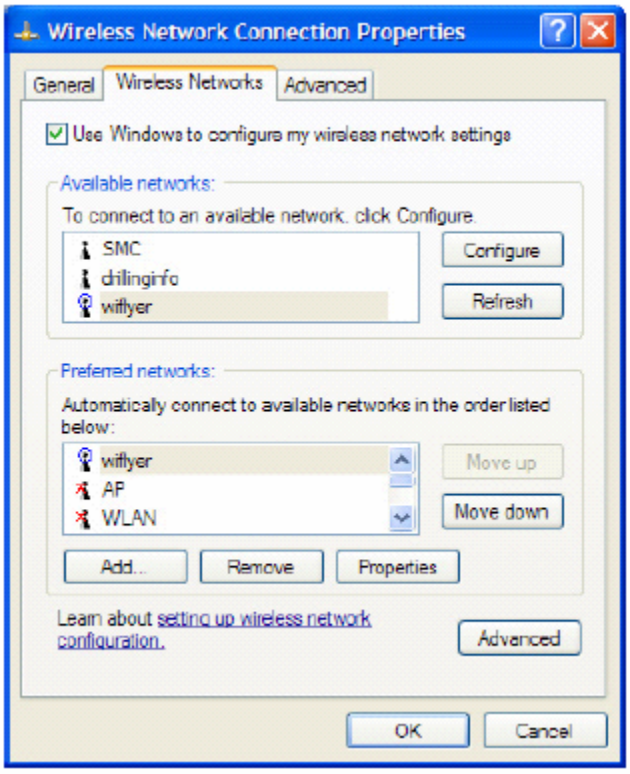


2. Highlight WiFlyer+v, by left clicking it, and check “Allow me to connect to the selected wireless network, even though it is not secure”. To enable security features see Chapter 6.

3. Next click the connect button.

4. If WiFlyer+v 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.



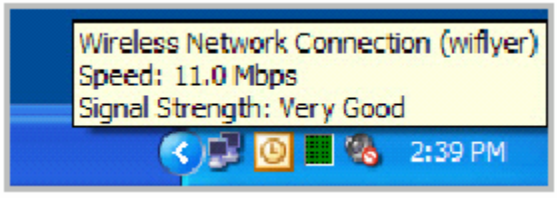
After you have clicked refresh the WiFlyer+v network will be listed.

b. Click OK.

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

d. Click connect.

6. Wait for "Connected to WiFlyer+v" to appear above the Wireless Network Connection icon on your taskbar.



You are now on the WiFlyer+v WiFi network. Continue to the dialup section to connect for dialup, or skip to the broadband section to configure broadband connectivity.

Configuring the WiFlyer+v 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, Mail, etc)

2. Open a web browser (Internet Explorer, Safari, etc.)

3. Your web browser should automatically connect to the WiFlyer+v dialup configuration page. If your browser does not connect to the dial page enter http://192.168.2.1 in the address bar of your browser.

.

4. Select your Internet Service Provider and click "Save". "Default" is used for all ISPs except AOL®, EarthLink®, iPass®, Netscape® and MSN®.
   NOTE: Selecting AOL, EarthLink or MSN also enables Access Number lookup. Click "Access Numbers" to locate an access number by area code or state for your selected ISP.

5. Once you have selected or entered an access number, enter your ISP username (screen name for AOL users) and password.

6. Click Dial Now!

7. Your browser will switch to the Connection Status screen. The icons on the connection status screen will change color as your modem connection progresses. Once you have made a successful connection to your ISP you will be redirected to the WiFlyer+v start page.

8. To return to the WiFlyer+v configuration pages, you must enter http://192.168.2.1. We recommend saving this page in your favorites on your browser. To disconnect you may either return to the dial page and click disconnect -- or press the quick connect button on the unit. As long as your settings have not changed you can press the quick connect button to reconnect as well. Enjoy your dialup WiFi!

Chapter

6

Advanced Configuration Features

This chapter covers the features in the Advanced Configuration section of the user interface. Features covered in this section include operating information of the WiFlyer+v, Internet phone settings, firmware upgrades, and firewall and advanced network settings.

Status

The Status section of the WiFlyer+v administration pages gives detail on the current configuration and operation of the WiFlyer+v. The status section is the area you will need to consult to perform troubleshooting and maintenance of your WiFlyer+v.

Device

Basic Internet (WAN) and local network (LAN) connection details can be found on this page.

Feature	Description
General	This section gives details on the current operating mode and firmware revision of the unit.
WAN	This section shows the status of the WAN connection including IP address, DNS and gateway information. This section also allows you to renew your DHCP lease. Clicking the DHCP Release button unassigns the router's IP address. The router will not respond to IP messages from the WAN side until you click the DHCP Renew button or power-up the router again. Clicking the DHCP Renew button causes the router to request a new IP address from the ISP's server.
LAN	This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your router. The detection "range" is limited

Feature	Description
	to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to "Automatically obtain an address") supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not.
Wireless LAN	Basic information on the WiFi connection. These settings can be changed in the Wireless Network section of the configuration pages. MAC Address The Ethernet ID (MAC address) of the wireless client. IP Address The LAN-side IP address of the client. Mode The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively. Rate The actual transmission rate of the client in megabits per second. Signal This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.
LAN Computers	This section shows the IP address given to client computers currently connected to the units DHCP. Also includes the name and MAC address of the client computers
IGMP Multicast memberships	If IGMP is enabled, this area of the screen show all multicast groups of which any LAN devices are members

Statistics

The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.

Feature	Description
Sent	The number of packets sent from the router.
Received	The number of packets received by the router.
TX Packets Dropped	The number of packets that were dropped while being sent, due to errors, collisions, or router resource limitations.
RX Packets Dropped	The number of packets that were dropped while being received, due to errors, collisions, or router resource limitations.
Collisions	The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).
Errors	The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN.

Logs

The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Feature	Description
What to View	Select the kinds of events that you want to view in your logs. • Firewall and Security • System • Router Status
View Levels	Select the level of events that you want to view. • Critical • Warning • Informational
Apply Log Settings Now	Click this button after changing Log Options to make them effective and permanent.
Refresh	Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.
Clear	Clicking this button erases all log entries.
Email Now	If you provided email information with the Administration -> Email screen, clicking the Email Now button sends the router log to the configured email address.
Save Log	Select this option to save the router log to a file on you

Feature	Description
	computer.

Wireless

The wireless section allows you to view the wireless clients that are connected to your wireless router.

Feature	Description
MAC Address	The Ethernet ID (MAC address) of the wireless client.
IP Address	The LAN-side IP address of the client.
Mode	The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.
Rate	The actual transmission rate of the client in megabits per second.
Signal	This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

Print Server

This section shows the status and network properties of the printer attached to the router through the USB port.

Feature	Description
Printer Status	Shows the status of the printer attached to the router. Note that certain printers (for example, the HP Business Inkjet 2300 printer) do not report status to the router; therefore, such a printer always shows a status of "Offline".
Raw TCP Port Printing	Shows the "IP Address" and "TCP Port" values that you need to enter when you configure your computer to use the printer in TCP Raw mode.
LPD/LPR Printing	Shows the "IP Address" and "Queue Name" values that you need to enter when you configure your computer to use the printer in LPR/LPD mode.

Wide Area Network

The WAN (Wide Area Network) section is where you configure your Internet Connection type when your WiFlyer+v is in broadband Access Point mode.

Broadband Wide Area Network Settings

There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider. Most cable connections are DHCP and most DSL connections are PPPoE although there are of course exceptions. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.

Static WAN Mode

Used when your ISP provides you a fixed IP address. You must manually enter the IP information in your IP configuration settings. Enter the IP address, Subnet Mask, Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all of this information.

DHCP WAN Mode

A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet.

Feature	Description
Host Name	Some ISP's may check your computer's Host Name. The Host Name identifies your system to the ISP's server. This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service.
Use Unicasting	This option is normally turned off, and should remain off as long as the WAN-side DHCP server correctly provides an IP address to the router. However, if the router cannot obtain an IP address from the DHCP server, the DHCP server may be one that works better with unicast responses. In this case, turn the unicasting option on, and observe whether the router can obtain an IP address. In this mode, the router accepts unicast responses from the DHCP server instead of broadcast responses.

PPPoE

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet.

Feature	Description
Dynamic IP	If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.
Static IP	If your ISP has assigned a fixed IP address, select this option. The ISP provides the value for the IP Address.
Service Name	Some ISP's may require that you enter a Service Name. Only enter a Service Name if your ISP requires one.
Reconnect Mode	There are times when a PPPoE connection is not always on. The WiFlyer+v router allows you to set the reconnection mode. The settings are: Always on: A connection to the Internet is always maintained. On demand: A connection to the Internet is made as needed. Manual: You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
Maximum Idle Time	Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

PPTP

PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet.

Feature	Description
Dynamic IP	If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.
Static IP	If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields: PPTP IP Address, PPTP Subnet Mask , and PPTP Gateway IP Address.
PPTP Server IP Address	The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.
Reconnect Mode	There are times when a PPTP connection is not always on. The WiFlyer+v router allows you to set the reconnection mode. The settings are: Always on- A connection to the Internet is always maintained. On demand- A connection to the Internet is made as

Feature	Description
	needed. Manual- You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
Maximum Idle Time	Time interval the machine can be idle before the PPTP connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

L2TP
L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet.

Feature	Description
Dynamic IP	If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.
Static IP	If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields: L2TP IP Address, L2TP Subnet Mask , and L2TP Gateway IP Address.
L2TP Server IP Address	The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.
Reconnect Mode	There are times when a PPTP connection is not always on. The WiFlyer+v router allows you to set the reconnection mode. The settings are: Always on- A connection to the Internet is always maintained. On demand- A connection to the Internet is made as needed. Manual- You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.
Maximum Idle Time	Time interval the machine can be idle before the L2TP connection is disconnected. The Maximum Idle Time value is only used for the "On demand" and "Manual" reconnect modes.

Advanced
These options apply to all WAN modes. In almost all cases you will not need to change the Advanced options in the WAN page. Only change these options if you are a networking expert or have been given instructions by your ISP.

Feature	Description
Use These DNS Servers	This option should be enabled if your ISP requires you to enter the DNS Server information. You will then be able to enter a primary and secondary DNS server.
Use the default MTU	If this option is checked (the default case), the router selects the usual MTU settings for the type of WAN interface in use. If this option is unchecked, the router uses the value of the MTU option (which follows).
MTU	The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
Link Drop Delay	When the the router detects that the WAN cable has been disconnected, it waits for "Link Drop Delay" seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical "glitches" in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.
WAN Port Speed	The Default is set to 10. If you have trouble connecting to the WAN, try the other settings.
Respond to WAN Ping	If you leave this option unchecked, you are causing the public WAN IP address of the router not to respond to `ping` commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Feature	Description
WAN Ping Inbound Filter	Select a filter that controls access as needed for WAN pings. If you do not see the filter you need in the list of filters, go to the Security -> Inbound Filter screen and create a new filter.
MAC Cloning Enabled	Some ISP's may check your computer's MAC address. Each networking device has it's own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new WiFlyer+v router has a different MAC address than the computer or router that initially connected to the ISP. To resolve this problem, the WiFlyer+v router has a special feature that allows you to clone (that is, replace the router's MAC address with) another MAC address.
MAC Address	If you have enabled MAC Cloning, you can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the WiFlyer+v router using that computer and click the Clone Your PC's MAC Address button. The WAN port will then use the MAC address of the network adapter in your computer.

Routing

Feature	Description
Add/Edit Route	Adds a new route to the IP routing table or edits an existing route.
Enable	Specifies whether the entry will be enabled or disabled.
Destination IP	The IP address of packets that will take this route.
Netmask	One bits in the mask specify which bits of the IP address must match.
Gateway	Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN.
Interface	Specifies the interface -- LAN or WAN -- that the IP packet must use to transit out of the router, when this route is used.
Metric	The relative cost of using this route.
Save	Saves the new or edited route in the following list. When

Feature	Description
	finished updating the routing table, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

Routes List
The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Route" section is activated for editing.

Dial Configuration [Dialup Mode only]

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	This is the number you dial to access your Internet Service Provider (ISP) and connect to the Internet.
Location	The location feature is an 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 is used to log into your ISP.
Enter ISP password	The password is used to log into your ISP.
Remember Password	Select the checkbox to enable the WiFlyer+v to remember your password.
Country	This is 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. Select Default in every case your ISP is not explicitly listed. After you make the selection make sure to click save in order to update the WiFlyer+v and have the settings take effect.
Connection Status	Located in the top right hand corner of the dial page, connection status indicates if the WiFlyer+v is currently connected by modem and if so the speed of that connection.

Dial Options [Dialup Mode only]

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	This feature is 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+v 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+v 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

Phonebook [Dialup Mode only]

The phonebook feature of the WiFlyer+v 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
Select	These features allows the user to select the number to be entered into the dial configuration page.
Location	This is an optional entry to allow the user to specify a city or place associated with the phone number.
Access Number	Access number is the phone number for the ISP.

Access Numbers [Dialup Mode only]

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	Enter the area code of the dial up number you are looking for.
State	Enter the state of the dialup number you are looking for.

Local Area Network

The Local Area Network is made up of the WiFlyer+v and any clients plugged into the LAN port or on the WiFlyer's WiFi network if the unit is in access point mode.

LAN

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

LAN Settings

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

Feature	Description
IP Address	The IP address of your router on the local area network. Your local area network settings are based on the address assigned here. For example, 192.168.0.1.
Subnet Mask	The subnet mask of your router on the local area network.

RIP (Routing Information Protocol)

Used to broadcast routing information amoung routers.

Feature	Description
Enable RIP	Enable RIP if required by the ISP, if the LAN has multiple routers, or if the LAN has auto-IP devices.
RIP Operating mode	This router supports both version 2 and version 1 of the RIP specification. V1. Use if none of the routers supports Version 2. V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1. V2 Multicast. Use if this is the only router on the LAN or if all the routers support Version 2.
Router Metric	The additional cost of routing a packet through this router.

Feature	Description
	The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.
Act as default router	Make this router the preferred destination for packets that are not otherwise destined.
Allow RIP updates from WAN	For security, disable this option unless required by the ISP.
RIP Password	RIP Version 2 supports the use of a password to limit access to routers through the RIP protocol. If the ISP or other LAN router requires a RIP password, enter the password here.

IGMP (Internet Group Management Protocol)
The IGMP protocol supports efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling IGMP.

DNS Relay
When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.

DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Enable DHCP Server
Once your WiFlyer+v router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically".

Your WiFlyer+v router, by default, has a static IP address of 192.168.2.1. This means that addresses 192.168.2.2 to 192.168.2.254 can be made available for allocation by the DHCP Server.

Feature	Description
DHCP IP Address Range	These two IP values (*from* and *to*) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically. It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see Static DHCP Client below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device.
DHCP Lease Time	The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.
Always Broadcast	If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

Number of Dynamic DHCP Clients
In this section you can see what LAN devices are currently leasing IP addresses.
Revoke: The `Revoke` option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking `Revoke` cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

Add/Edit DHCP Reservation
This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request

an IP address from the WiFlyer+v router. The WiFlyer+v router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

Feature	Description
Enable	Enable or Disable the DHCP reservation feature
IP address	The reserved IP address for the system. Note: You only must reserve an IP address if that IP address is in the DHCP range configured above. If the IP address is not in the DHCP range it is not necessary to use this feature.
MAC Address	To input the MAC address of your system, enter it in manually or connect to the WiFlyer+v router's Web-Management interface from the system and click the Copy Your PC's MAC Address button. A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the WiFlyer+v router from the computer and click the Copy Your PC's MAC Address button to enter the MAC address.
Computer Name	You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way.

MAC Address:

If you can't find the MAC address using either of the methods above then you can locate a MAC address in a specific operating system by following the steps below:

Operating System	Procedure
Windows 98 Windows Me	Go to the Start menu, select Run, type in winipcfg, and hit Enter. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address. This is the MAC address of the device.
Windows 2000 Windows XP	Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type ipconfig /all and hit Enter. The physical address displayed for the adapter connecting to the router is the MAC address.
Mac OS X	Go to the Apple Menu, select System Preferences, select

Operating System	Procedure
	Network, Change the ‘Show:” Dropdown to the network adaptor that is connected to the Wiflyer +V then click the ‘Ethernet’ button. MAC address is listed as ‘Ethernet ID’. (Alt: open Terminal app and type ‘ifconfig’ MAC address is listed as ‘ether’. En0: is the cabled Ethernet en1: is the Airport)

DHCP Reservations List
This shows clients that you have specified to have reserved DHCP addresses. An entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing.

Dynamic DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your host name to connect to your server, no matter what your IP address is.

Feature	Description
Enable Dynamic DNS	Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following parameters are displayed when the option is enabled.
Server Address	Select a dynamic DNS service provider from the pull-down list.
Host Name	Enter your host name, fully qualified; for example: `myhost.mydomain.net`.
Username or Key	Enter the username or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.
Password or Key	Enter the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.
Verify Password or Key	Re-type the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.
Timeout	The time between periodic updates to the Dynamic DNS, if your dynamic IP address has not changed. The timeout period is entered in hours.

If a dynamic DNS update fails for any reason (for example, when incorrect parameters are entered), the router automatically disables the Dynamic DNS feature and records the failure in the log.

Note: After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example `http://www.mydomain.info`) and the router will attempt to forward the request to port 80 on your LAN. If, however, you do this from a LAN-side computer and there is no virtual server defined for port 80, the router will return the router's configuration home page. Refer to the Advanced -> Virtual Server configuration page to set up a virtual server.

Wireless Networking

The wireless section is used to configure the wireless settings for your WiFlyer+v. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Wireless Network

This section allows you to make basic configuration changes to your wireless radio as well as wireless security. For a detailed description of wireless security features please go to the Wireless Security portion of the Security section.

Feature	Description
Enable Wireless Radio	This option turns off and on the wireless connection feature of the router. When you set this option, the following parameters are displayed.
Wireless Network Name	When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.
Visibility Status	The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
Auto Channel Select	If you select this option, the router automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the router uses the channel that you specify with the following Channel option.
Channel	A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between

Feature	Description
	clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.
Transmission Rate	By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.
802.11 Mode	If all of the wireless devices you want to connect with this router can connect in 802.11g mode, you can improve performance slightly by changing the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.

Advanced Wireless

Advanced Wireless settings should only be changed if you are a networking expert or if you have specific instructions from your ISP.

Feature	Description
Fragmentation Threshold	This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.
RTS Threshold	This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.
Beacon Period	Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.
DTIM Interval	A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
802.11d Enable	Enables 802.11d operation. 802.11d is a wireless specification for operation in additional regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries). The

Feature	Description
	current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard. Enable this option if you are operating in one of these "additional regulatory domains".
Transmit Power	Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.
WDS Enable	When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP. Make sure the APs are configured with same channel number.
WDS AP MAC Address	Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.

Security

This section is where you will configure the security features of the WiFlyer+v.

Wireless Security

This section is the dedicated area where you can configure Wireless Security. To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

WEP

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange -

alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.
Example:
64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)
128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)
64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)
128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

WPA-Personal and WPA-Enterprise
Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

Feature	Description
WPA Mode	WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.
Cipher Type	The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.
Group Key Update Interval	The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal
This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).
Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Example:
Wireless Networking technology enables ubiquitous communication

WPA-Enterprise
This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Feature	Description
Authentication Timeout	Amount of time before a client will be required to re-authenticate.
RADIUS Server IP Address	The IP address of the authentication server.
RADIUS Server Port	The port number used to connect to the authentication server.
RADIUS Server Shared Secret	A pass-phrase that must match with the authentication server.
MAC Address Authentication	If this is selected, the user must connect from the same computer whenever logging into the wireless network.

Advanced RADIUS Options / Optional Backup RADIUS Server
This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields Second RADIUS Server IP Address, RADIUS Server Port, Second RADIUS server Shared Secret, Second MAC Address Authentication provide the corresponding parameters for the second RADIUS Server.

Virtual Server

The Virtual Server option gives Internet users access to services on your LAN by forwarding internet requests to the appropriate server. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port.

For example:

You are hosting a Web Server on a PC that has LAN IP Address of 192.168.2.50 and your ISP is blocking Port 80.

1. Name the Virtual Server (for example: Web Server)
2. Enter the IP Address of the machine on your LAN (for example: 192.168.2.50
3. Enter the Private Port as [80]
4. Enter the Public Port as [8888]
5. Select the Protocol - TCP

6. Ensure the schedule is set to Always
7. Click Save to add the settings to the Virtual Servers List
8. Repeat these steps for each Virtual Server Rule you wish to add. After the list is complete, click Save Settings at the top of the page.

With this Virtual Server entry, Internet traffic to your external IP address on port 8888 (e.g. http://66.254.185.2:8888) will be redirected to your internal web server on port 80 at IP Address 192.168.2.50.

Add/Edit Virtual Server

In this section you can add an entry to the Virtual Servers List below or edit an existing entry.

Feature	Description
Enable	Entries in the list can be either active (enabled) or inactive (disabled).
Name	Assign a meaningful name to the virtual server, for example `Web Server`. Several well-known types of virtual server are available from the "Select Virtual Server" list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
IP Address	The IP address of the system on your internal network that will provide the virtual service, for example `192.168.2.50`.
Protocol	Select the protocol used by the service.
Private Port	The port that will be used on your internal network.
Public Port	The port that will be accessed from the Internet.
Inbound Filter	Select a filter that controls access as needed for this virtual server. If you do not see the filter you need in the list of filters, go to the Security -> Inbound Filter screen and create a new filter.
Schedule	Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the Administration -> Schedules screen and create a new schedule.
Save	Saves the new or edited virtual server entry in the following list. When finished updating the virtual server entries, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

Virtual Servers List

The section shows the currently defined virtual servers. A Virtual Server can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Virtual Server" section is activated for editing.

You might have trouble accessing a virtual server using its public identity (WAN-side IP-address of the gateway or its dynamic DNS name) from a machine on the LAN. Your requests may not be looped back or you may be redirected to the "Forbidden" page.

This will happen if you have an Access Control Rule configured for this LAN machine.

The requests from the LAN machine will not be looped back if Internet access is blocked at the time of access. To work around this problem, access the LAN machine using its LAN-side identity.

Requests may be redirected to the "Forbidden" page if web access for the LAN machine is restricted by an Access Control Rule. Add the WAN-side identity (WAN-side IP-address of the router or its dynamic DNS name) on the Advanced -> Web Filter screen to work around this problem.

Gaming

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). The Gaming section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats:

Range (50-100)
Individual (80, 68, 888)
Mixed (1020-5000, 689)

Edit/Add Game Rule

Here you can add entries to the Game Rules List below, or edit existing entries.

Example:

You are hosting an online game server that is running on a PC with a Private IP Address of 192.168.2.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect.

Feature	Description
Enable	Each entry in Game Rules List can be active (enabled) or inactive (disabled)
Name	Give the Gaming Rule a name that is meaningful to you, for example `Game Server`. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.
IP Address	Enter the local network IP address of the system hosting the game server, for example `192.168.2.50`.

Feature	Description
TCP Ports To Open	Enter the TCP ports to open. [6159-6180, 99]
UDP Ports To Open	Enter the UDP ports to open. [6159-6180, 99]
Inbound Filter	Select a filter that controls access as needed for this game rule. If you do not see the filter you need in the list of filters, go to the Security -> Inbound Filter screen and create a new filter.
Schedule	Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Administration -> Schedules screen and create a new schedule.
Save	Saves the new or edited Game Rule in the following list. When finished updating the game rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent. With this Gaming Rule enabled, all TCP and UDP traffic on ports 6159 through 6180 and port 99 is passed through the router and redirected to the Internal Private IP Address of your Game Server at 192.168.2.50.

Game Rules List
The section shows the currently defined game rules. A game rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Game Rule" section is activated for editing.

Access Control

The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.

Feature	Description
Enable	By default, the Access Control feature is disabled. If you need Access Control, check this option, and you will see the following configuration sections. **Note:** When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.
Policy Wizard	The Policy Wizard guides you through the steps of defining each access control policy. A policy is the "Who, What, When, and How" of access control -- whose computer will be affected by the control, what internet

Feature	Description
	addresses are controlled, when will the control be in effect, and how is the control implemented. You can define multiple policies. The Policy Wizard starts when you click the button below and also when you edit an existing policy.
Add Policy	Click this button to start creating a new access control policy.
Policy Table	This section shows the currently defined access control policies. A policy can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the Policy Wizard starts and guides you through the process of changing a policy. You can enable or disable specific policies in the list by clicking the "Enable" checkbox.

Web Filter

The Web Filter section is where you add the Web sites to be used for Access Control.

Feature	Description
Add/Edit Web Site	This is where you can add Web sites to the Allowed Web Site List or change entries in the Allowed Web Site List. The Allowed Web Site List is used for systems that have the Web filter option enabled in Access Control.
Enable	Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default.
Web Site	Enter the URL (address) of the Web Site that you want to allow; for example: `google.com`. Do not enter the `http://` preceding the URL. Enter the most inclusive domain; for example, enter `wiflyer.com` and access will be permitted to both `www.wiflyer.com` and `support.wiflyer.com`. **Note:** Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access `my.yahoo.com`, you need to enable access to `yahoo.com`, `yimg.com`, and `doubleclick.net`.
Save	Saves the new or edited Allowed Web Site in the following list. When finished updating the Allowed Web Site List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

Allowed Web Site List
The section lists the currently allowed web sites. An allowed web site can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Web Site" section is activated for editing.

MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

Feature	Description
Enable MAC Address Filter	When this is enabled, computers are granted or denied network access depending on the mode of the filter. **Note:** Misconfiguration of this feature can prevent any machine from accessing the network. In such a situation, you can regain access by activating the factory defaults button on the router itself.
Filter Settings Mode	When "only allow listed machines" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "only deny listed machines" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.
Filter Wireless Clients	When this is selected, the MAC address filters will be applied to wireless network clients.
Filter Wired Clients	When this is selected, the MAC address filters will be applied to wired network clients.
Add/Edit MAC Address	In this section, you can add entries to the MAC Address List below, or edit existing entries.
Enable	MAC address entries can be activated or deactivated with this checkbox.
MAC Address	Enter the MAC address of the desired computer or connect to the router from the desired computer and click the Copy Your PC's MAC Address button.
Save	Saves the new or edited MAC Address entry in the following list. When finished updating the MAC Address List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

MAC Address List
The section lists the current MAC Address filters. A MAC Address entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit MAC Address" section is activated for editing.

Firewall

The Firewall on the WiFlyer+v prevents users on the internet from accessing your internal network unless you specifically allow them access to the network.

Feature	Description
Enable SPI	SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking detailed state information on a per session basis. It validates that the traffic passing through that session conforms to the protocol. When the protocol is TCP, SPI checks that packet sequence numbers are within the valid range for the session, discarding those packets that do not have valid sequence numbers. Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.
Enable DMZ	DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer. **Note:** Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.
DMZ IP Address	Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address Automatically using DHCP, then you may want to make a static reservation on the LAN -> DHCP page so that the IP address of the DMZ machine does not change.

Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on IP Address.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.

Feature	Description
Add/Edit Inbound Filter Rule	Here you can add entries to the Inbound Filter Rules List below, or edit existing entries.
Name	Enter a name for the rule that is meaningful to you.
Action	The rule can either Allow or Deny messages.
Source IP Range	Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the Start and End boxes. Up to eight ranges can be entered. The Enable checkbox allows you to turn on or off specific entries in the list of ranges.
Save	Saves the new or edited Inbound Filter Rule in the following list. When finished updating the Inbound Filter Rules List, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

Inbound Filter Rules List
The section lists the current Inbound Filter Rules. An Inbound Filter Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Inbound Filter Rule" section is activated for editing.

In addition to the filters listed here, two predefined filters are available wherever inbound filters can be applied:

Allow All
Permit any WAN user to access the related capability.
Deny All
Prevent all WAN users from accessing the related capability. (LAN users are not affected by Inbound Filter Rules.)

VoIP and Multimedia

This section is where you configure your internet phone settings. In this section you can also configure your gaming and video priority settings for the router.

StreamEngine

The StreamEngine™ feature helps improve your network gaming performance by prioritizing applications. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

StreamEngine Setup

Feature	Description
Enable StreamEngine	This option is enabled by default. Enable it for better performance and experience with online games and other interactive applications, such as VoIP. StreamEngine is disabled by default when the unit is in Dialup mode.
Automatic Classification	This option is enabled by default so that your router will automatically determine which programs should have network priority.
Dynamic Fragmentation	This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.
Automatic Uplink Speed	When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).
Measured Uplink Speed	This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.
Uplink Speed	If Automatic Uplink Speed is disabled, this option allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISPs often specify speed as a downlink/uplink pair; for example, 1.5Mbps/284kbps. For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as www.dslreports.com. Note however that sites such as DSL Reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the Measured Uplink Speed or the ISP rated speed.

Feature	Description
Connection Type	By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results. Detected xDSL or Frame Relay Network When Connection Type is set to Auto-detect, the automatically detected connection type is displayed here.

Add/Edit StreamEngine Rule
Automatic classification will be adequate for most applications, and specific StreamEngine Rules will not be required. A StreamEngine Rule identifies a specific message flow and assigns a priority to that flow.

Note that rules can be applied in any order, not necessarily in the order entered or listed. Therefore, conflicting rules (for example, rules with overlapping address ranges) are not permitted.

Feature	Description
Enable	Each entry in StreamEngine Rules List can be active (enabled) or inactive (disabled)
Name	Create a name for the rule that is meaningful to you.
Priority	The priority of the message flow is entered here. 0 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).
Protocol	The protocol used by the messages.
Source IP Range	The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.
Source Port Range	The rule applies to a flow of messages whose LAN-side port number is within the range set here.
Destination IP Range	The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.
Destination Port Range	The rule applies to a flow of messages whose WAN-side port number is within the range set here.
Save	Saves the new or edited StreamEngine Rule in the

Feature	Description
	following list. When finished updating the StreamEngine rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.

StreamEngine Rules List
The section shows the currently defined StreamEngine rules. A StreamEngine rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit StreamEngine Rule" section is activated for editing.

Special Applications

The WiFlyer+v has preconfigured firewall rules set up for common applications like Instant Messenger and Netmeeting allowing you easy use of these applications without having to specially configure the firewall on your unit. This section allows you to enable and disable these special rules as well as add additional configuration information for these rules.

Application Level Gateway (ALG) Configurations
Here you can enable or disable ALGs. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

Feature	Description
PPTP	Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.
IPSec VPN	Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.
RTSP	Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.
Windows Messenger	Supports use of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) on LAN computers. The SIP ALG must also be

Feature	Description
	enabled when the Windows Messenger ALG is enabled.
FTP	Allows FTP clients and servers to transfer data across NAT. Refer to the Security -> Virtual Server page if you want to host an FTP server.
NetMeeting	Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the Advanced -> Virtual Server page for information on how to set up a virtual server.
SIP	Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.
Wake-On-LAN	This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable. The WOL device must be defined as such on the Security -> Virtual Server page. The LAN IP address for the virtual server is typically set to the broadcast address 192.168.2.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened.
MMS	Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet.

Add/Edit Special Applications Rule
The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

For example:
You need to configure your router to allow a software application running on any computer on your network to connect to a web-based server or another user on the Internet.

Feature	Description
Name	Enter a name for the Special Application Rule, for example `Game App`, which will help you identify the rule in the future. You can also select from a list of common applications, and the remaining configuration values will be filled in accordingly.

Feature	Description
Trigger Port Range	Enter the outgoing port range used by your application. [6500-6700]
Trigger Protocol	Select the outbound protocol used by your application. [Both]
Input Port Range	Enter the port range that you want to open up to Internet traffic. [6000-6200]
Input Protocol	Select the protocol used by the Internet traffic coming back into the router through the opened port range. [Both]
Schedule	Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Administration -> Schedules screen and create a new schedule.
Save	Saves the new or edited Special Applications Rule in the following list. When finished updating the special applications rules, you must still click the Save Settings button at the bottom of the page to make the changes effective and permanent.

With this Special Application Rule enabled, the router will open up a range of ports from 6000-6200 for incoming traffic from the Internet, whenever any computer on the internal network opens up an application that sends data to the Internet using a port in the range of 6500-6700.

Special Applications Rules List
The section shows the currently defined special applications rules. A special applications rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Special Applications Rule" section is activated for editing.

VoIP

This section is where you set up your internet phone settings. In most cases your WiFlyer+v will come pre-configured with your internet phone settings. You will only need to change the settings in this section if you want to add a second internet phone service or if you have changed services.

Feature	Description
SIP provider	Choose your Internet Phone provider
SIP user name	This is the username given to you by your Internet Phone provider
SIP password	Password given to you by your internet phone provider
SIP server URL	The SIP server URL. This should already be entered for you
SIP URL	The SIP domain URL. This should already be entered for you

Feature	Description
SIP port	The port your Internet Phone provider uses. By default this port is 5060, only change this if you are given instructions do to so by your
Enable STUN	Some Internet Phone networks require STUN. Only enable this feature if told to do so by your Internet Phone provider.
STUN URL	Enter the STUN URL given to you by your Internet Phone provider
STUN port	Enter the STUN port given to you by your Internet Phone provider
Choose internet phone line as default	This setting makes your internet phone line the default line. If your landline is plugged into the WiFlyer+v press ** to switch over to make calls on it instead of the Internet Phone line.
Use unique dialtone for internet phone line	This feature gives a dialtone that is different for the Internet Phone line than the standard dialtone used by a landline. This feature allows you to audibly tell when you are using the Interent Phone line.

SIP Contacts
In the SIP contacts section you can list SIP usernames from Mindspring or Gizmo to call from your telephone. Enter the SIP username in the numbered contact line and then dial the number followed by # to dial that person.

For example:

You have configured your SIP settings for Mindspring and have entered user@mindspring.com as a SIP contact on line number 1. To dial user@mindspring.com pick up your phone and dial 1#. You will now dial user@mindspring.com and talk to them over the Mindspring VoIP network.

Connection Wizards

This router has a USB port; so, if you have a USB flash drive, a USB port on your PC, and your PC runs Windows XP Service Pack 2 (SP2) or later, you can transfer wireless configuration data between your PC and the router with the USB flash drive. Go to the Windows Control Panel and select Wireless Network Setup Wizard. The Wireless Network Setup Wizard gives you the choices: "Use a USB flash drive" and "Set up a network manually". Select "Use a USB flash drive". Note: Do not connect more than one USB flash drive to the router, not even with a USB hub.

Internet Connection Setup Wizard

This wizard guides you through the following basic router setup steps:

- Set your Password

- Select your Time Zone
- Configure your Internet Connection

Wireless Security Setup Wizard

This wizard guides you through the following steps for setting up security for your wireless network:

- Name your Wireless Network
- Secure your Wireless Network

Printer Wizard

Before you can use a printer that is plugged into the router's USB connector, you must configure your computer for that printer. If the operating system of your computer is Win32 compatible, all you need to do is click the Printer Wizard button, and the configuration is done by a Printer Wizard ActiveX control. The Printer Wizard provides the necessary printer setup link between your PC and the router via the browser. The browser downloads the Printer Wizard program to your PC. You should already have a WAN connection, so that the browser can access the latest version of the program; however, the browser can always download some version of the program from the router itself. If the browser displays a pop-up window requesting permission to download the Printer Wizard program, answer Yes or OK.

If your computer's operating system is not Win32 compatible (for example, Mac, Linux, or an earlier version of Windows), the Printer Wizard button will not be available. Instead, you must follow your operating system's procedure for printer configuration. You can set up either a "TCP Raw" or a "LPR/LPD" connection to the printer. Refer to the Administration -> Print Server page to enable the protocol you wish to use. Then refer to Status -> Print Server to obtain the printer address and name or port number -- these are values that you have to enter in the operating system's printer setup procedure.

Following are printer set-up guidelines for some operating systems. These guidelines may become obsolete with the release of new operating system versions; so, when in doubt, consult the documentation or help for your operating system.

Printer Set-Up for Windows XP (LPR/LPD)

1. From the Start Menu, select "Control Panel"
2. From the Control Panel window, select "Printers and Faxes"
3. From the Printers and Faxes window, in the Printer Tasks pane, select "Add Printer"
4. From the Add Printer Wizard...
5. Click "Next".
6. Select "Local printer attached to this computer"
7. Click "Next".
8. Select "Create new port" and choose "Standard TCP/IP Port" from the "Type of port" list.

9. Click "Next".
10. From the "Add Standard TCP/IP Printer Port Wizard" ...
11. Click "Next".
12. Enter the IP address of the printer and click "Next". (note that the IP address can be found on Print Server web page under Status tab)
13. Under "Device Type" select "Custom" and click "Settings"
14. Under "Protocol" select LPR
15. Under "LPR Settings" type the queue name of the printer. (note that the queue can be found on Print Server web page under Status tab)
16. Leave LPR Byte Counting disabled for better performance
17. Enable SNMP Status using default settings.
18. Click "OK" and then click "Next" to continue.
19. Click "Finish".
20. Select the driver. Note that you may need to select "Have Disk" and locate the INF file on printer manufacturer's driver CD.
21. Give printer a name, choose default printer or not, and choose print test page or not.
22. Click "Finish" to complete setup.

Printer Set-Up Mac OS X (LPR/LPD)

1. From the Apple menu select System Preferences.
2. From the System Preferences window select "Print and Fax"
3. On the Print and Fax window, select "Set Up Printers"
4. On the "Printer Setup Utility" window, select "Add"
5. On the "Printer List" window, select IP Printing at the top.
6. In the second pulldown menu, select LPD/LPR
7. Next to "Printer Address:" type the printer's IP address
8. Next to "Queue Name:" enter the queue name
9. Next to "Printer Model:", choose the appropriate driver for the printer

Administration

The administration section of the WiFlyer+v lets you upgrade the firmware, set basic password information and

Basic Administration

The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.

Feature	Description
Admin Password	Enter a password for the user "admin", who will have full access to the Web-based management interface.
User Password	Enter a password for the user "user", who will have read-only access to the Web-based management interface.
Gateway Name	The name of the gateway can be changed here.

Feature	Description
Device Type	Select the operating mode of the unit: Bridge, Access Point or Dialup Access Point.
Enable Remote Management	Enabling Remote Management allows you to manage the router from anywhere on the Internet. Disabling Remote Management allows you to manage the router only from computers on your LAN.
Remote Admin Port	The port that you will use to address the management interface from the Internet. For example, if you specify port 1080 here, then, to access the router from the Internet, you would use a URL of the form: `http://my.domain.com:1080/`.
Remote Admin Inbound Filter	Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the Security -> Inbound Filter screen and create a new filter.
Admin Idle Timeout	The amount of time before the administration session (either remote or local) is closed when there is no activity.
Save Configuration	This option allows you to save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.
Restore Configuration from File	Use this option to load previously saved router configuration settings.
Save Configuration To Wireless Network Setup Wizard	If your PC's operating system is Windows XP Service Pack 2 (SP2) or later and you are using Windows Internet Explorer (IE) as your browser, you can use this option to save key parts of the router's current wireless security settings to your PC with Windows Connect Now (WCN) technology. The settings will then be available to propagate to other wireless devices.
WCN ActiveX Control	The WCN ActiveX Control provides the necessary WCN link between the router and your PC via the browser. The browser will attempt to download the WCN ActiveX Control, if it is not already available on your PC. For this action to succeed, the WAN connection must be established, and the browser's internet security setting must be Medium or lower (select Tools -> Internet Options -> Security -> Custom Level -> Medium). Click the Save to Windows Connect Now button, and the WCN technology will capture the wireless network settings from your router and save them on your PC.

Note: The WCN only saves a few of the wireless security settings. When you use WCN to propagate settings to other wireless devices, you may have to make additional settings manually on those devices.

Note that, in Microsoft's current implementation of WCN, you cannot save the wireless settings if a profile of the same name already exists. To work around this limitation, either delete the existing profile or change the SSID when you change the wireless settings; then, when you save the new settings, a new profile will be created.

Print Server

The router can support both "TCP Raw" and "LPD/LPR" printing protocols. Enable one or both as required by the devices on the LAN.

Feature	Description
Enable Raw Port Printing	Causes the router to support TCP raw (also known as Port 9100). Printers are identified by port numbers (9100 being the customary starting port number). This option must be enabled for the Print Wizard to function.
Enable LPD/LPR Printing	Causes the router to support the LPD/LPR protocol. Printers are identified by a symbolic queue name. This option is disabled by default; enable it if required by the devices on the LAN. This method of printing is generally preferred for Unix or Macintosh (starting with Mac OS 8.1).

Firmware

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance. To check for the latest firmware, click the Check Online Now button. If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.

To upgrade the firmware, follow these steps:

1. Click the Browse button to locate the WiFlyer+v upgrade file on your computer.
2. Once you have found the file to be used, click the Upload button below to start the firmware upgrade process. This can take a minute or more.
3. Wait for the router to reboot. This can take another minute or more.
4. Confirm updated firmware revision on status page.

Firmware Information
Here are displayed the version numbers of the firmware currently installed in your router and the most recent upgrade that is available.

Check Online

This option will check WiFlyer+v's support site to see if you have the latest version of the firmware available. If a newer version is available, download instructions will be displayed.

Firmware Upgrade
Note: Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the router by wire.

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Administration -> Admin screen.

Feature	Description
Upload	Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the router.
Firmware Upgrade Notification Options	Automatically Check Online for Latest Firmware Version When this option is enabled, your router will check online periodically to see if a newer version of the firmware is available. Email Notification of Newer Firmware Version When this option is enabled, an email will be sent to the email address configured in the email section whenever new firmware is available. You must have Email Notification enabled from the Administration -> Email screen.

Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the router's internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight saving can also be configured to automatically adjust the time when needed.

Time Configuration

Feature	Description
Time Zone	Select your local time zone from pull down menu.
Daylight Saving Enable	Check this option if your location observes daylight saving time.
Daylight Saving Offset	Select the time offset, if your location observes daylight saving time.
DST Start and DST End	Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun"

Feature	Description
	and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."

Automatic Time Configuration

Feature	Description
Enable NTP Server	Select this option if you want the router's clock synchronized to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.
NTP Server	Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your router here, or you can click the Copy Your Computer's Time Settings button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

Note: If the router loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the router, or you must enable the NTP Server option.

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

Feature	Description
Add/Edit Schedule Rule	In this section you can add entries to the Schedule Rules List below or edit existing entries.
Name	Give the schedule a name that is meaningful to you, such as "Weekday rule".
Day(s)	Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.
All Day - 24 hrs	Select this option if you want this schedule in effect all day for the selected day(s).
Start Time	If you don't use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email

Feature	Description
	events are normally triggered only by the start time.
End Time	The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not normally used for email events.
Save	Saves the new or edited Schedule Rule in the following list. When finished updating the Schedule Rules, you must still click the Save Settings button at the top of the page to make the changes effective and permanent.
Schedule Rules List	The section shows the currently defined Schedule Rules. A Schedule Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Schedule Rule" section is activated for editing.

Syslog

This section allows you to archive your log files to a Syslog Server.

Feature	Description
Enable Logging to Syslog Server	Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it. Enabling this option causes the following parameter to be displayed.
Syslog Server IP Address	Enter the LAN IP address of the Syslog Server.

Email

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

Feature	Description
Enable Enable Email Notification	When this option is enabled, router activity logs or firmware upgrade notifications can be emailed to a designated email address, and the following parameters are displayed.
From Email Address	This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.
To Email Address	Enter the email address where you want the email sent.
SMTP Server Address	Enter the SMTP server address for sending email.
Enable Authentication	If your SMTP server requires authentication, select this

Feature	Description
	option.
Account Name	Enter your account for sending email.
Password	Enter the password associated with the account.
Verify Password	Re-type the password associated with the account.

Email Log When Full or on Schedule

Feature	Description
On Log Full	Select this option if you want logs to be sent by email when the log is full.
Schedule	Select this option if you want logs to be sent by email according to a schedule.
Select Schedule	If you selected the Schedule option, select one of the defined schedule rules. If you do not see the schedule you need in the list of schedules, go to the Administration -> Schedules screen and create a new schedule.

Note: Normally email is sent at the start time defined for a schedule, and the schedule end time is not used. However, rebooting the router during the schedule period will cause additional emails to be sent.

System

This section allows you to reboot the device, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

Feature	Description
Reboot the Device	This restarts the router. Useful for restarting when you are not near the device.
Restore all Settings to the Factory Defaults	This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your router configuration settings, you can do so from the Administration -> Admin page.

Appendix

A

Troubleshooting and FAQs

Resetting to Factory Defaults

On occasion you will find a need to reset the WiFlyer+v to factory defaults, typically this occurs after you have entered a password or wireless security setting and then forgotten it. To reset the WiFlyer+v back to its factory defaults and clear the unit of its user configured settings:

1. Disconnect the power cable from the back of the unit.

2. Press and hold down the "quick connect" button.

3. Re-apply power while continuing to hold down the button.

4. Release the reset button once all 5 lights have come on and the unit has beeped 3 times.

5. If unit does not beep (volume off), wait for the lights to start coming on a second time before releasing the quick connect button (about 12 seconds).

Note:
Resetting to factory defaults will remove any custom configuration, including access numbers, that you have entered and you will need to configure the base station again.

Using AOL accounts

When using the WiFlyer+v with AOL, the WiFlyer+v will allow multiple users to surf the Internet using Internet Explorer, Safari or any other browser; you can access most AOL content and email through the AOL website at www.aol.com. You may also instant message using AIM, Yahoo Messenger or other IM client software; and check emails using an email software client such as Outlook, Outlook Express or Mail.

To use AOL's client software (such as AOL 8.0 or 9.0) you must create a new screen name for the WiFlyer. This screen name will only be used by the WiFlyer and must be 10 characters or less.

1. Start your AOL client and log in normally

2. Create screen name to use on the WiFlyer+v. Since the WiFlyer+v logs into AOL, you will want to create a special screen name for it. The screen name you create for the WiFlyer+v should be 10 characters or less (e.g. coolwifi09). To create a new screen name:

a. Sign on to AOL.
b. Click My AOL in the top toolbar.
c. Click Screen Names from the pop-up menu.
d. Click Create a Screen Name.
e. Click Create a Screen Name again on the new screen that comes up.
f. Enter the screen name you want to use in the box.
g. Press Enter.
h. Type the password you want to use twice.
i. Press Enter on the screen.
j. Click Continue.
k. Customize the new screen name with the preferences you want.
l. Click Continue.
m. Click Accept Settings,

3. Log out of your AOL client and connect to the WiFlyer's configuration pages (see the quick start guide for detailed instructions on how to connect to he WiFlyer's configuration pages) Configure WiFlyer+v with the new screen name and password you just created.

4. Click dial now on WiFlyer+v. After the WiFlyer+v connects launch the AOL client software and login using your normal screen name (not the new one you just created). You may also need to change the location dropdown box on the AOL client logon screen. The location dropdown box on the logon screen should be set to LAN, sometimes this setting is called network or TCP. Changing this setting ensures your client is not trying to dial your internal modem.

Appendix

B

WiFlyer+v Specifications

Power Supply

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

Federal Communications Commission (FCC) Part 15 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.

Federal Communications Commission (FCC) Part 68 Statement

This equipment complies with 47CFR, Part 68. The unit bears a label which contains, among other information, the certification number and Ringer Equivalence Number (REN). If requested, this information must be provided to the telephone company.

This equipment uses a RJ11C jack type for telephone network connection.

This equipment contains an FCC compliant modular jack. It is designed to be connected to the telephone network or premises wiring using compatible modular plugs and cabling which comply with the requirements of FCC Part 68 rules.

The REN is used to determine the number of devices which may be connected to the telephone line. An excessive REN may cause the equipment to not ring in response to an incoming call. In most areas, the sum of the RENs of all equipment on a line should not exceed five (5.0).

In the unlikely event that this equipment causes harm to the telephone network, the telephone company can temporarily disconnect your service. The telephone company will try to warn you in advance of any such disconnection, but if advance notice isn't practical, it may disconnect the service first and notify you as soon as possible afterwards. In the event such a disconnection is deemed necessary, you will be advised of your right to file a complaint with the FCC.

From time to time, the telephone company may make changes in its facilities, equipment, or operations that could affect the operation of this equipment. If this occurs, the telephone company is required to provide you with advance notice so you can make the modifications necessary to obtain uninterrupted service.

There a no user serviceable components within this equipment.

It shall be unlawful for any person within the United States to use a computer or other electronic device to send any message via a telephone facsimile unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, or other entity, or individual sent the message and the telephone number of the sending machine or of such business, other entity or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges. Telephone facsimile machines manufactured on or after December 20, 1992, must clearly mark such identifying information on each transmitted message. Facsimile modem boards manufactured on or after December 13, 1995, must comply with the requirements of this section.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to Party Line Service is subject to state tariffs. Contact your state public utility commission, public service commission, or corporation commission for more information.

Industry Canada Emissions 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 2 dBi. 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.

Industry Canada CS03 Statement

Notice: The industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operations and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements documents(s). The department does not guarantee the equipment will operate to the user's satisfaction.

Before installing the equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of concern. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Notice: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5. The REN of the WiFlyer+v is 0.3.