OTHER PRODUCTS AVAILABLE FROM ROVING NETWORKS

RN-1000	Bluetooth Access Point & Print Server
RN-700	Bluetooth Terminal Server & Serial Gateway
RN-USB	Bluetooth Class I (long range) USB Adapter
RN-400U	Bluetooth USB Printer Adapter
RN-800S-AD	Bluetooth Sensor AtoD 16bit, 8 channel
RN-30S	Bluetooth embedded serial module, class I
RN-24S	Bluetooth embedded serial module class II
	(4-24Vdc input, 8 GPIO, high power switches)

ROVING networks
WIRELESS FOR LESS

For more information and support:

Contact Roving Networks: phone 408-395-6539 fax 603-843-7550

431 Monterey Avenue, Suite 5

Los Gatos, California, 95030 USA

Email : info@rovingnetworks.com

http://www.rovingnetworks.com

ROVING networks
WIRELESS FOR LESS

FireFly Install Guide

OPERATING MODES

0-Slave Mode - The default mode, whereby other devices can discover and connect to the FireFly.

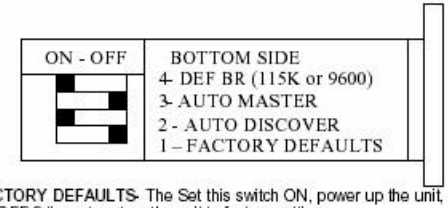
1 - Master Mode (SM,1<CR>) Enables outbound connections. To connect, use the "C" command.

2-Trigger Mode (SM,2<CR>) Automatically connects to stored address, when data is received on local serial port of master.

3-Auto Master Mode (SM,3<CR>) Automatically connects to stored address on power up.

NOTE: In all master modes the device will not be discoverable or remote configurable.

CONFIGURATION SWITCHES



1- FACTORY DEFAULTS- The Set this switch ON, power up the unit, and toggle the switch from ON to OFF 2 times to return the unit to factory settings.

2-AUTO DISCOVER MODE – In Slave mode, will set a special class of device which is used by a remote FireFly Master to auto connect. IF Switch 3 also SET, the device performs a search, stores, and connects to a remote slave which has this switch 2 set .

3- AUTO MASTER MODE- FireFly will act as master, and auto-connect to a stored remote address. You first set the BT address of the device to connect to using the SR command. Or, have FireFly auto discover and connect by setting this AND Switch 2.

4- DEFAULT BAUDRATE- OFF (factory setting) = 115K, ON = 9600, (overridden if configured via software.

LEDs

MODE	GREEN LED BLINK
Configuring	Fast, 10 x per second
Boot up, Remote Configurable	2 times per second
Discoverable/Idle	1 time per second
Connected	On Solid

The YELLOW Led shows physical state of the data pins, pulse stretched for eye visibility, and blinks when data is TRANSMITTED or RECEIVED on the TX and RX pins.

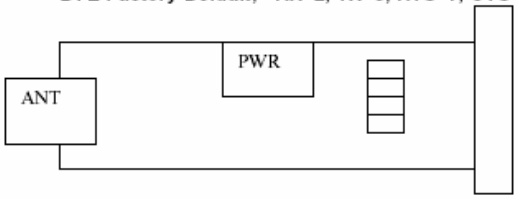
Power Jack

Center pin is +5V,outer cylinder is GND. Input can be 4VDC or greater, but not greater than 9 VDC. Power draw is 30-50ma when connected depending on data rate, can be as low as 2ma average when not connected depending on parameter settings.

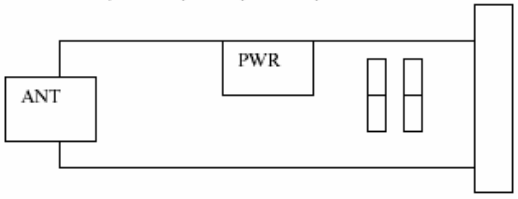
SERIAL PIN CONFIGURATIONS

NAME	DB-9 male	IO DIR	DCE(PC)*	DTE	3-WIRE-DCE
1-DCD	NC				
2-RX	2-RX	IN←	|	--	|
3-TX	3-TX	OUT→	|	--	|
4-DTR	NC				
5-GND	5-GND	<—>			
6-DSR	NC				
7-RTS	7 -RTS	OUT→	|	--	|
8 - CTS	8 -CTS	IN←	|	--	X
9 - RING	V+	IN←			

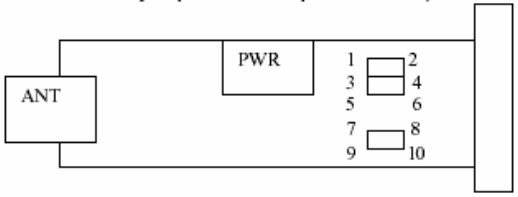
DTE Factory Default, RX=2, TX=3, RTS=7, CTS=8



DCE , RX=3, TX=2, RTS=8, CTS=7



DTE 3 Wire ((CTS shorted to RTS) , remove 3rd , 4th jumpers and install 1 jumper between pins 9 and 10)



COMMON PROBLEMS and QUESTIONS:

My Bluetooth client can see the FireFly and its serial service, but I can't connect: This is most likely caused by a security setting on your client. If a pincode is required, **the default is "1234"**. Some clients have these settings off by default, others have them on. To check and disable security: From your PC desktop, click My Bluetooth Places, go to the Bluetooth Device configuration (or Advanced Configuration) drop down menu, click on the client applications tab, Select the Bluetooth serial port application name, and click on the properties button, if "secure connection", or "authentication", or "encryption" is checked, un check it.

Changing the clients COM port: Widcomm stack, (and others) allows you to connect to FireFly using a "Virtual COM" port mapper. The software installs with a default COM port, usually COM3, COM4, or COM5. To change this setting: From your PC desktop, click My Bluetooth Places, go to the Bluetooth Device configuration (or Advanced Configuration) drop down menu, click on the client applications tab, Select the Bluetooth serial port application name, and click on the properties button, then you can change the com port.

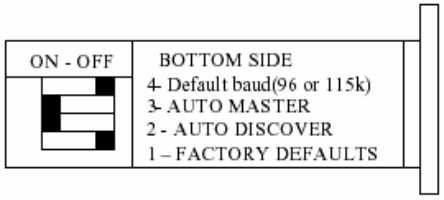
Connecting to more than one FireFly from the same client at the same time: Bluetooth allows 7 devices at a time in a piconet. Widcomm stack allows you to create multiple instances of serial port profile and connect to multiple FireFlys at the same time. To do this: From your PC desktop, click My Bluetooth Places, goto the Bluetooth Device configuration (or Advanced Configuration) drop down menu, click on the client applications tab, Select the Bluetooth serial port application name, and click on the ADD COM port button, then you can add another Bluetooth serial port and assign it to another virtual com port (such as COM9).

Connections can be made but during data transfer, no characters flow, or bytes are dropped. Check to see if your flow control signals are properly connected, and enabled in the serial software you are using. A common mistake is to connect during the boot config timer window, in this case, all characters will be ignored until a $$$ is seen, and no characters are forwarded to the remote device. If remote configuration is enabled, a good way to ensure that the device is not waiting for configuration is to issue "—"<cr> at the beginning of a connection and before any user data is sent.

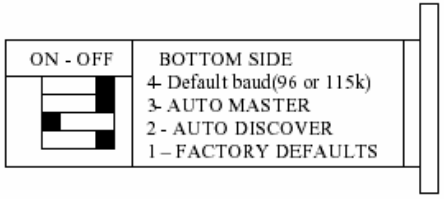
Another common problem is related to hardware flow control,it is not enough to simply disable flow control in your communications software, the FireFly expects to use hardware flow control, so do disable this on the FireFly you must either remove the CTS flow control jumper, or short pins 7 and 8 (RTS,CTS) of your cable to permanently enable the flow control.

INSTANT CABLE REPLACEMENT EXAMPLE:

MASTER



SLAVE



1. Set switches 2 and 3 as shown above.
2. Power up both devices
3. Master finds and store slave address, and auto connects.
4. Set Switch 2 on both Master and Slave back to OFF (so that they don't try to re-pair each time power is cycled).

Making a Connection

FireFly shows up under Service discovery as "FireFly-zpdq" where the zpdq is the last 2 bytes of the Bluetooth address. To connect to FireFly, browse for services, you should see: "SPP on FireFly-zpdq". **Default baudrate is 115200, no parity, 8 bits, 1 stop.** FireFly uses Serial Port Profile and can be connected to as a Virtual COM port on PCs, Palms, PocketPCs, or other clients.

NOTE: Only one client can connect to FireFly at a time, and there is a limit of 7 total devices in a Bluetooth Piconet network.

If authentication is not required, generally you can simply connect to the FireFly by clicking on the service shown by your client.

If authentication is required, the default passkey of "1234", or the passkey that has been configured should be entered.

Changing Configuration

FROM LOCAL SERIAL PORT- Connect a null-modem cable (pins 2,3 swapped) from a PC or a straight cable from an ASCII terminal to the FireFly. Communication settings of your program should match the stored settings, for example: the default is 115,200Kbps, 8 bits, No Parity, 1 stop bit. Once you change these parameters, they will be stored permanently.

Run your favorite terminal emulator, Hyperterminal*** or other program. (see note below to download our free emulator). Type $$$ on your screen (3 dollar signs). You should see **CMD** returned to you. This will verify that your cable and settings are correct. Valid commands will return an **AOK**. Errors in format will return **ERR**, and unrecognized commands will return a ?. Type "h"<cr> to see a list of commands, and "d"<cr> to see a summary of current settings.

REMOTE VIA BLUETOOTH- Make a connection via Bluetooth, then use your favorite terminal emulator, and follow the directions above for local configuration. To return to data mode, type a final "---" (3 minus signs) <cr>, or reset the device and connect again.
NOTE: remote configuration can only occur if the bootup configuration timer (default 60 seconds) has not expired. This timer is set to 0 (remote config disabled) for master mode, and auto-connect slave mode, so that data can immediately flow between the 2 devices in cable replacement fashion.

*****Roving Networks recommends downloading our free teraterm terminal emulator, as Hyperterminal has a number of "features" in WinXP (such as auto-baud detection which does not work) which render it effectively inoperable for a local serial port connection. Teraterm can be downloaded at:**

http://www.rovingnetworks.com/support/teraterm.zip

COMMAND SUMMARY
*****SET COMMANDS*****stored in flash, and only take effect AFTER reboot

Example: SU,9600 sets Uart Baudrate to 9600

SN,myname sets Bluetooth name to "myname"
SA,1 enables secure authentication
SP,secret sets security pincode to "secret"
SF,1 restores all values to factory defaults

CMD	VALUE	TYPE	DEFAULT	DESCRIPTION
SA	0,1	dec	0	Enable Authentication
SE	0,1	dec	0	Enable encryption
SF	1	dec		Reset to Factory Defaults
SL	E,O,N	char	N	Parity, Even, Odd, or None
SM	0,1,2,3	dec	0	Mode (0-slav, 1=mstr, 2=trigr,3=auto mstr)
SN	string	1-16 char	FireFly-x	Bluetooth Name
SO	string	1-8 char	NOT SET	Status string or break character(s)
SP	string	1-16 char	1234	Security Pin Code
SR	string	12 chars	NOT SET	Remote Address (123456789ABCDEF)
ST	word	seconds	60	Config Timer(0=no config, 255=always on)
SU	string	2-4 char	115K	Baudrate:1200,2400,4800,9600,384k,576k 115k,230k,460k)
SX	0,1	dec	0x1F00	Bonding (locks to a single remote address)

***** DISPLAY COMMANDS *****

CMD	DESCRIPTION
D	Basic Settings
E	Extended Settings
G<X>	A single setting matching the commands above
GB	Bluetooth Address of this device
&	I/O Ports (shows the value of the switches)
V	Firmware Revision

***** OTHER COMMANDS *****

CMD	VAL1	VAL2	DESCRIPTION
C	<addr>		Connect to Remote Address(in Master Mode only)
H			Help, Show list of commands
I	<time>	<COD>	Inquiry Scan, time= xx seconds ,optional COD filter
R	1		Reboot device immediate
U	<rate>	<E,O,N>	Temporary UART Change, immediate, not stored

A complete list of commands can be found at www.rovingnetworks.com/support

NOTES ON OPERATION:

Master Modes: There are 3 different master modes which can be enabled:

1. Manual Mode. In this mode, the Blueport makes connections when a Connect Command "C", is received. This command can also contain the Bluetooth address of the remote device. If no device is specified, then the store remote address is used. The connection can be broken if the special break character or string is sent (use the SO command to set the break character) **This is a low speed connect mode**.

2. Trigger Mode. In this mode, the Blueport makes connections automatically when a character is received on the serial port. The connection will continue as long as characters are received on either end. There is a configurable timeout (which is set using the ST command) which will cause a disconnect after XX (from 1 to 254) seconds of inactivity. **This is a low speed connect mode**.

3. Auto Mode. In this mode, the Blueport makes connections automatically on powerup, and re-connects when connection is lost. This mode can also be enabled by setting Dip Switch #2. This is the high speed connect mode, and cannot be broken by software break characters.

Low Speed Connect Mode NOTE in Manual and Trigger mode, the Blueport is making a LOW speed connection, that is, data is being processed by the Blueport before being sent over the air. Because the Blueport is looking for break or config character(s), the latency will increase and data rate will be decreased in these modes. Thus it is recommended that for data rates above 57.6K these modes not be used.

Configuration Timer Settings

VALUE (decimal)	DESCRIPTION
0	No remote config, No local config when connected
1-252	Time in seconds from powerup to allow config
253	Continous config LOCAL only
254	Contiuous config, REMOTE only
255	Continous config, both LOCAL and REMOTE

Security Issues, Pin Codes and Link Keys: If A> Blueport, or B> the remote device has authentication enabled, the following process occurs: The first time a connection is made, a "passkey" is used. This is a series of numbers or characters, "1234" is the default for the Blueport. Once this is entered, the remote Bluetooth device and the Blueport compare their passkeys and if they match, a link key is generated, which is stored by the Blueport. Upon subsequent connections, the devices will first compare link keys and if they match no pin code will have to be re-entered. If the remote device is a PC or PDA, a prompt is generally made to the user to enter this pincode. To remove the stored link key on the remote device, generally you "unpair" with the Blueport. To remove the link key on the Blueport, you can change the Pin Code. This will remove any previously stored link keys from the blueport, forcing a new Pin Code exchange process to occur upon subsequent connection attempts.

Roving Networks, Inc. **Bluetooth Device** **FCC ID: T9JRN41-1**

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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.

Caution: This user guide information is only provided to OEM or module installer. Do not supply to the end user.