WIRELESS REMOTE ACCESS PLATFORM

USER MANUAL

WRAP™ PRODUCT SERIES

Version 1.1.3

2002-10-28

TABLE OF CONTENTS

1 INTRODUCTION

WRAP™

The Wireless Remote Access Platform (WRAP™) from BlueGiga Technologies is a series of integrated hardware and software products, which cost-effectively add wireless connectivity to machines and devices. WRAP products enable substantial cost and timesavings by providing you with a complete solution for remotely accessing devices in the short, local and global range. BlueGiga's WRAP products are certified, integrated solutions including all necessary hardware, operating system, protocols, stacks, servers, APIs, and application software processing capabilities. The solution is a robust and configurable platform, which enables you to easily place a wide variety of new or existing applications on top of it.

WRAP™ 1260

The WRAP 1260 MicroServer is a compact Bluetooth MicroServer with RS-232 interface for professional cable replacement, machine network connectivity (M2M) and wireless Man-Machine Interface (MMI). WRAP MicroServers combine Bluetooth™ and Internet technologies and include all the necessary components for machines and devices to communicate wirelessly over Bluetooth. It also has powerful processing and memory design to host applications inside. The WRAP 1260 is also available as an OEM version (WRAP 1160).

WRAP™ 3000

The WRAP 3000 Industrial Access Server is a compact Bluetooth Gateway with an Ethernet interface to leverage existing networks in wireless Machine-to-Machine (M2M) communications. The WRAP 3000 enables you to link a large variety of equipment directly to your company's computer network for remote reading, data logging, machine diagnostics, monitoring, system updates or other wireless transactions. The WRAP 3000 is suitable for many applications in various environments, from industrial manufacturing sites to commercial payment systems. The WRAP 3000 is also available as an OEM version.

WRAP™ 2151

The BlueGiga Technologies WRAP 2151 Starter Kit is built on the WRAP architecture, which simply means that you get a complete development environment for wirelessly connecting machines to users and networks. Whether you want to read, control, diagnose devices, or log data, the WRAP 2151 makes it easy to get started and provides you with a rich set of helpful tools to make your wireless system design successful. The WRAP 2151 Starter Kit is a versatile and flexible application creation environment including many development tools and features: configuration tools, system utilities, GNU compiler and tools, several ANSI C/Waba/Java sample applications, application programming interfaces, and thin servers.

To get started with the WRAP 2151 Starter Kit, you don't need to be an embedded development specialist. Just install it and explore its possibilities using this manual as a reference.

1.1 LICENSES AND WARRANTY

Warning: BlueGiga Technologies is hereby willing to license the enclosed WRAP product and its documentation under the condition that the terms and conditions described in the License Agreement is understood and accepted. This is supplied within every WRAP product both in hardcopy and softcopy (file \doc\WRAP_warranty_and_license.pdf on the WRAP CD-ROM). The use of the WRAP product will indicate your assent to the terms. If you do not agree to these terms, BlueGiga Technologies will not license the software and documentation to you, in which event you should return this complete package with all original materials, equipment, and media.

The following software components: GCC compiler tool chain, uClinux kernel, and uClinux-userland applications are licensed under the terms and conditions of the GPL General Public License (file \doc\GPL.txt on the WRAP CD-ROM). Upon request, BlueGiga will distribute a complete machine-readable copy of the source of the aforementioned software components during a period of three (3) years from the order date of the product. Delivery costs of the source code will be charged from the party requesting the source code.

The BlueGiga WRAP Product Limited Warranty Statement is located in the file \doc\WRAP_warranty_and_license.pdf on the WRAP CD-ROM.

1.2 CERTIFICATION INFORMATION

WRAP™ 1260

This product is CE approved (10.9.2002) and Bluetooth qualified v.1.1. (6.9.2002). It has been measured against specification standards Radio spectrum (R&TTE, Article 3.2) ETSI EN 300 328-2 v1.3.1. / EN 301 489-1/17 and FCC part 15.247. Supported Bluetooth profiles are: LAN-AP, LAN-DT, GAP, SDAP, Serial-DevA and Serial-DevB.

Warning: Changes or modifications made to this equipment not expressly approved by BlueGiga Technologies Inc. may void the FCC authorization to operate this equipment.

The radiated output power of WRAP™ 1260 is far below the FCC radio frequency exposure limits. Nevertheless, the WRAP™ 1260 shall be used in such a manner that the potential for human contact during normal operation is minimized.

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 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.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

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.

WRAP™ 3000

This product is CE approved (10.9.2002) and Bluetooth qualified v.1.1. (6.9.2002). It has been measured against specification standards Radio spectrum (R&TTE, Article 3.2) ETSI EN 300 328-2 v1.3.1. / EN 301 489-1/17 and FCC part 15.247. Supported Bluetooth profiles are: LAN-AP, LAN-DT, GAP, SDAP, Serial-DevA and Serial-DevB.

Warning: Changes or modifications made to this equipment not expressly approved by BlueGiga Technologies Inc. may void the FCC authorization to operate this equipment.

The radiated output power of WRAP™ 3000 is far below the FCC radio frequency exposure limits. Nevertheless, the WRAP™ 3000 shall be used in such a manner that the potential for human contact during normal operation is minimized.

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 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.

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

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.

WRAP™ 2151

BlueGiga WRAP 2151 Starter Kit is a development and demo tool and shall be used for development or demo purposes only. The product may only be used by you if and to the extend you are a professional business manufacturer or developer.

BlueGiga WRAP 2151 Starter Kit has not been tested for compliance with the Bluetooth system specifications and it has not passed CE, FCC or any other certification tests.

1.3 BLUEGIGA TECHNOLOGIES CONTACT INFORMATION

Please check http://www.bluegiga.com for news and latest product offerings. For more information, contact sales@bluegiga.com.

Please contact support@bluegiga.com if you need technical support. To speed up the processing of your support request, please include as detailed information of your product and your problem situation as possible. Please begin your email with the following details:

- WRAP product type
- WRAP product serial number
- WRAP Software version
- End customer name
- Date of purchase

2 QUICK START

The WRAP boards are delivered with the latest release of the WRAP platform installed. No additional installation is required for getting started with the WRAP. Just connect the Ethernet cable (WRAP 2151 and 3000 only) and the power cable and the WRAP boots up. After this, you can connect to the WRAP using a device that has Bluetooth LAN Access Client profile support. The WRAP board can be seen in Bluetooth inquiries called as "BlueGiga_xxx", where xxx will be the last three digits of the product serial number. If you cannot use Bluetooth to connect to WRAP, read further.

2.1 MANAGEMENT CONSOLE

The simplest way to configure, monitor, and control the WRAP board is to do it from a management console. By "management console" we mean any PC running terminal emulation software (such as HyperTerminal in Windows or minicom in Linux) connected with the serial cable shipped with the product to the management port of the WRAP board. The location of the management port in WRAP 1260 and WRAP 3000 is shown in Figure 1 and in WRAP 2151 Starter Kit in Figure 2.

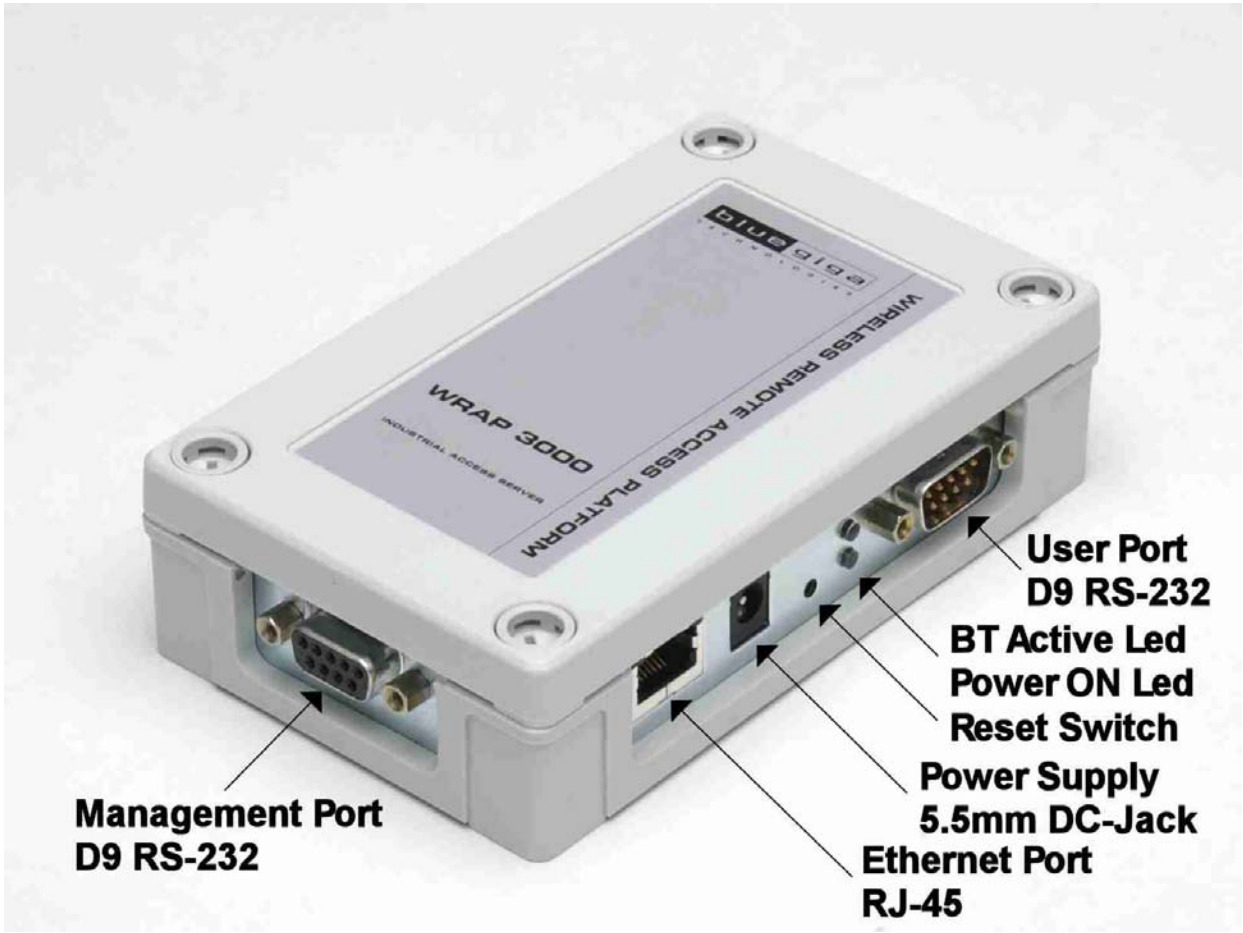

Figure 1. WRAP 1260 and WRAP 3000 Management Port Connector Location.

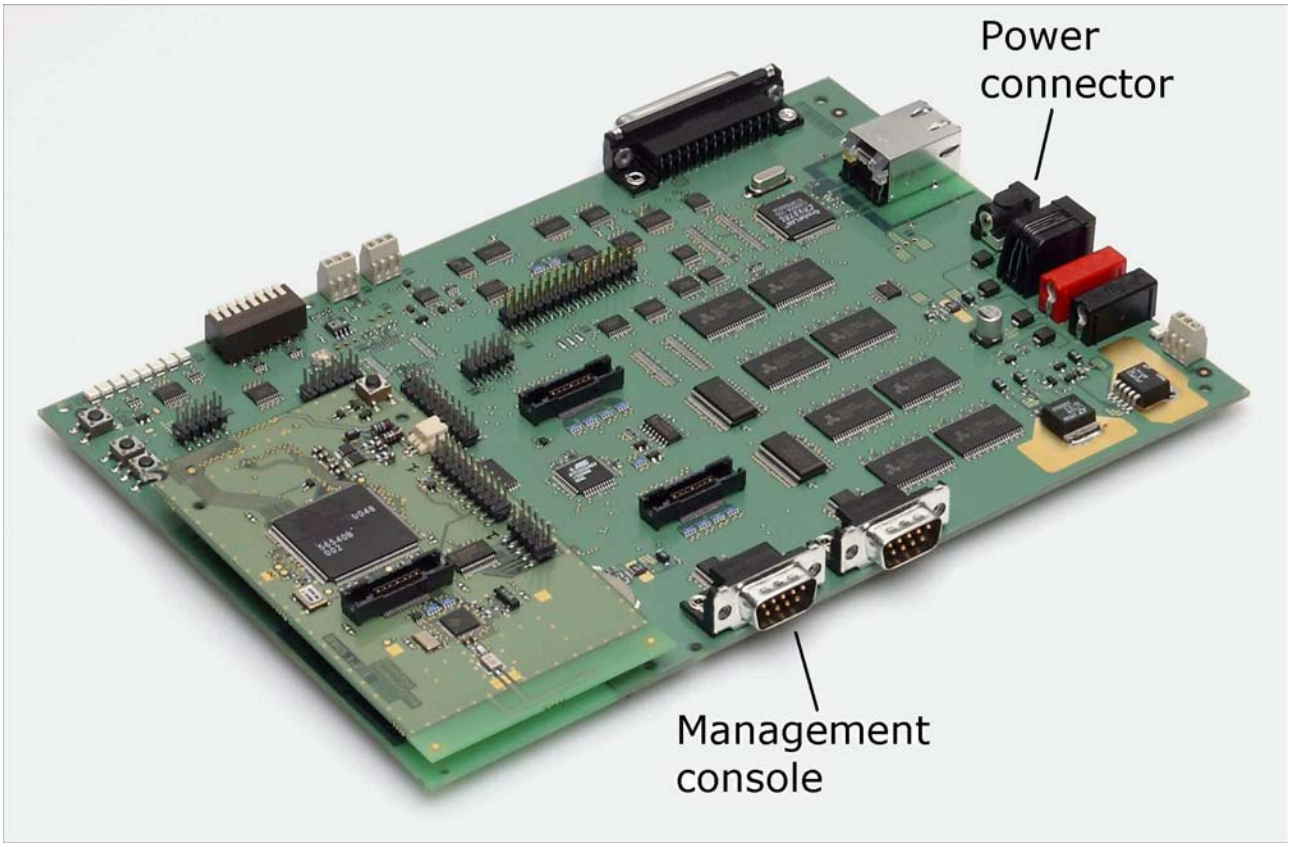

Figure 2. WRAP 2151 Starter Kit Management Port Connector Location.

The serial port settings for the management console are shown in Table 1. When you use the management console, you are automatically logged in as the superuser (root). The serial cable is in fact a standard direct cable for WRAP 1260 and WRAP 3000 products and a standard cross-over cable for WRAP 2151 Starter Kit.

Setting	Value
Speed	115 200 bps
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Table 1. The Management Console Port Settings.

2.2 ACCESSING WITH TELNET

When the WRAP is connected to a LAN, you can also use a telnet client to connect to the board (to the standard telnet port, 23) and perform the same functions remotely as you would locally from the management console. To see the IP address of the WRAP board, connect to the WRAP with a management console, power on the board and after the system is up and running, give the command "ifconfig". The field "inet addr" for the interface "eth0" contains the IP address of the WRAP board. For example, in the following capture from the management console, the IP address is "10.1.1.32":

```
/> ifconfig
eth0      Link encap:Ethernet  HWaddr 00:07:80:80:00:81
          inet addr:10.1.1.32  Bcast:10.1.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:17 Base address:0x300

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
/>
```

If you don’t see the interface "eth0" in the output of "ifconfig" command or the IP address is "0.0.0.0", but you have connected the Ethernet cable to the WRAP board before power up, you might be connected to a LAN without a DHCP server. Check this from your network administrator and if required, configure the network settings of the WRAP manually with the "setup" application described in section 3.2.

When you are connected to WRAP using the Bluetooth LAN Access profile, you can use a telnet client in the same way as you would use over wired LAN.

When you are logging in to WRAP with telnet, you need to log in as "root", whose default password is "buffy". It can be changed with "passwd" program at WRAP prompt.

3 CONFIGURATION

When the WRAP is installed and powered up for the first time, the default configuration settings are being used. With these settings, the WRAP automatically configures its network settings assuming that the board is connected to a LAN network with a DHCP server running. After booting, you can use the WRAP as a Bluetooth LAN access point to the network without any changes in configuration. Also the Serial Port Profile is enabled by default in listening mode.

3.1 USING THE SETUP APPLICATION

The basic configuration settings are changed using the "setup" application. It displays the settings in a hierarchical menu. Navigating the menu is accomplished by entering the number or the letter of the setting to view and/or change and pressing <enter>. Pressing only <enter> either accepts the previous value of the setting or returns to the previous level in the menu hierarchy. The settings and their meanings, and the default values are described in the following sections.

3.2 NETWORK CONFIGURATION

Note: this setting is not applicable for WRAP 1x60.

`1. Enable Interface Eth0 [Y]`

This option determines whether or not an Ethernet interface is brought up at all at boot. If set to no, the other options in the Network Configuration menu are not visible.

`2. Use Dynamic network configuration [Y]`

This option determines whether or not automatic configuration of the Ethernet interface using DHCP should be attempted at boot. If set to yes, the following options in the Network Configuration menu are not visible.

`3. IP address of the host [10.0.0.101]`

If the dynamic network configuration is disabled (step 2), the IP address of the WRAP must be entered here.

`4. Subnet mask [255.255.255.0]`

If the dynamic network configuration is disabled (step 2), the network mask of the WRAP must be entered here.

`5. IP address of the default gateway [10.0.0.254]`

If the dynamic network configuration is disabled (step 2), the IP address of the default gateway in the LAN to which the WRAP is connected must be entered here.

`6. Hostname of the device [wrap]`

The hostname of the WRAP device. Local applications will see this name.

`7. Domain of the device [local.net]`

The domain name of the WRAP device. Local applications will see this name.

`8. IP address of the primary name server [10.0.0.1]`

The IP address of the primary name server.

`9. IP address of the secondary name server [10.0.0.2]`

The IP address of the secondary name server.

3.3 BLUETOOTH SETTINGS

Bluetooth settings are divided into general and profile specific settings, which are described in the following sections.

3.3.1 GENERAL BLUETOOTH SETTINGS

1. `Friendly Name [BlueGiga_*]`

   The name shown when this device is found when inquired by other Bluetooth devices. The name may end with asterisk (*), which will be replaced with the last 3 digits of the serial number of this WRAP board.

2. `Bluetooth Server Socket Interface Password [buffy]`

   The password required to enter before any commands when discussing with the WRAP Bluetooth Server Socket Interface.

3. `Connectable and Discoverable Mode [3]`

   The setting specifying whether this device is connectable and/or discoverable or not by other Bluetooth devices.

   When a device is connectable, other Bluetooth devices can make a Bluetooth connection to it. Before making a connection, the calling device must know the Bluetooth address of the device to connect. The Bluetooth addresses are found by making an inquiry. When a device is discoverable, it shows up in inquiries. Possible values for all combinations of these settings are:

   0: Not connectable, not discoverable

   1: Not connectable, discoverable

   2: Connectable, not discoverable

   3: Connectable and discoverable (default)

4. `Master/Slave Role Switch Policy [1]`

   The setting specifying how the connecting Bluetooth devices should decide their roles. When a device is calling another Bluetooth device, it originally is the master and the answering device is the slave. When the connection is being built, a role switch can be made. Normally, access point devices want to be the master for all their slaves, and therefore they require a master-slave switch when a new device is connecting. This is also how WRAP is configured by default. Other possible combinations are:

   0: Allow switch when calling, don't request when answering

   1: Allow switch when calling, request when answering (default)

   2: Don't allow switch when calling, request when answering

   If you have problems in connecting to WRAP, this might be due the fact that your client device does not support a master/slave switch. In this case, set this setting to "0".

3.3.2 LAN ACCESS PROFILE SETTINGS

1. `Enable Lan Access Profile [Y]`

   Whether the Lan Access Profile is enabled or not.

2. `Lan Access Login Name and Password []`

   The login name and password required from the Lan Access Clients. Must be entered as a single string, separated with a space. An example: "guest buffy". If empty (default), no login is required.

3. `Service Name (shown in SDP) [Lan Access Using PPP]`

   The name of this service shown in the Service Discovery.

3.3.3 SERIAL PORT PROFILE SETTINGS

Note: visibility of some of these settings is controlled by the "Act as the Calling Device" -setting.

Note2: Serial Port Profile is disabled if SMS Gateway is enabled as they share the same physical serial port.

1. `Enable Serial Port Profile [Y]`

Whether the Serial Port Profile is enabled or not.

2. `Act as the Calling Device [N]`

   Whether this device should act as the calling device (DevA) or the answering device (DevB).

3. `BPS Rate [9600]`

   The bits-per-second rate of the connection. Possible values are 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400 and 460800.

4. `Data Bits [8]`

   The number of data bits in the connection. Possible values are 5, 6, 7 and 8.

5. `Parity [0]`

   The parity bit setting of the connection. Possible values are: 0: no parity, 1: odd parity and 2: even parity.

6. `Stop Bits [1]`

   The number of stop bits in the connection. Possible values are 1 and 2.

7. `Hardware Flow Control (RTS/CTS) [Y]`

   Whether the hardware flow control is used in the connection or not.

8. `Software Flow Control (XON/XOFF) [N]`

   Whether the software flow control is used in the connection or not.

9. `Service Name (shown in SDP) [Serial Port]`

   The name of this service shown in the Service Discovery. (This setting is visible only when setting 2. "Act as the Calling device" is disabled.)

10. `Bluetooth Address of the Remote Device [00:07:80:80:01:1f]`

    The Bluetooth address of the device to be contacted. (This setting is visible only when setting 2. "Act as the Calling device" is enabled.)

11. `Server Channel of the Remote Device [10]`

    The Bluetooth server channel of the device to be contacted. (This setting is visible only when setting 2. "Act as the Calling device" is enabled.)

3.3.4 OBEX SETTINGS

1. `Enable Object Push Profile [Y]`

   Whether the Object Push Profile is enabled or not.

2. `Service Name (shown in SDP) [OBEX Object Push]`

   The name of this service shown in the Service Discovery.

3. `Enable File Transfer Profile [Y]`

   Whether the File Transfer Profile is enabled or not.

4. `Service Name (shown in SDP) [OBEX File Transfer]`

   The name of this service shown in the Service Discovery.

3.3.5 OPTIONAL COMMAND LINE PARAMETERS FOR BLUETOOTH SERVER []

This setting can be used to override the defaults. For example, "—port 4242" would set the Bluetooth server control port to 4242 instead of the default 10101. However, you should not give any optional parameters for the Bluetooth server if you don’t know what you are doing.

3.4 RAMDISK SETTINGS

```
1. Size of the ramdisk (in kilobytes) [512]
```

The size of the ramdisk (/mnt/ram/). Sizes below minimum (currently 50) and above maximum (currently 1024) are not allowed.

3.5 SYSTEM LOGGER SETTINGS

```
1. Log locally [Y]
```

This option determines whether or not the System Logger (syslogd) should log locally (to /var/log/messages).

```
2. Address of the Remote Syslog Server []
```

The address of the device in the network to which the System Logger should log to. **Note:** This remote device must be configured to accept syslogd connections from this WRAP board. See the system logger documentation on the remote device for more information on how to do that.

3.6 WEB SERVER SETTINGS

```
1. Web Server logging device [/dev/null]
```

The file to which the Web Server (httpd) logs all requests and connections. Use /dev/console for console output and, for example, /tmp/httpd.log if you want to save this information. Be careful, however, not to fill the RAM filesystem (use a cron job to free disk space from time to time).

Note: If the file is invalid, httpd does not start at boot.

3.7 SMS GATEWAY SETTINGS

Note: SMS Gateway is disabled by default as Serial Port Profile is enabled by default, because they share the same physical serial port. Disable Serial Port Profile first to be able to enable SMS Gateway.

1. Enable SMS Gateway at startup [N]

   Whether the SMS Gateway (smsgw) should be started automatically when the system boots up or not.

2. SMS Gateway logging device [/dev/null]

   The file to which the SMS Gateway (smsgw) logs all traffic. Use /dev/console for console output and, for example, /tmp/smsgw.log if you want to save this information. Be careful, however, not to fill the RAM filesystem (use a cron job to free disk space from time to time).

3.8 /ETC/RC.USER

While not configurable with the "setup" application, the file /etc/rc.user is important for system boot configuration. It is the file executed as the last task by the system boot script.

By default, the file /etc/rc.user does not exist, but you should create one if you want to do some special automatic initialization at every boot, like starting up your own servers.

Small textual configuration files (like the /etc/rc.user file) are often most quickly done by using the "cat" command. In the following example, we create a new /etc/rc.user file:

```
/> cat > /etc/rc.user
#!/bin/sh
echo Starting up my server
/usr/local/bin/myserverd &
echo Everything booted up
<ctrl-D>
/>
```

Note: Instead of typing the contents of the file, you can of course also copy-and-paste it from your favourite text editor.

You can also create and edit the file using the "vi" editor at WRAP telnet prompt. **Note:** Currently it is not possible to use "vi" at management console due some WRAP operating system problems. However, it is also possible to use your own text editor. Just download the file, edit it locally in your computer and upload the file back again. Downloading and uploading files is described in section 4.4.

3.9 RESETTING CONFIGURATION

You can restore the default configuration by deleting the main configuration file and rebooting the board. When the system starts up, the default configuration settings are restored. If you have changed the configuration only by using the "setup" application, the following commands at WRAP command prompt are enough:

```
/> rm /etc/sysconfig
/> reboot
```

If you have made changes to other configuration files by editing them manually and want to restore the original file(s), just delete the file(s) in question and reboot the board.

3.10 ADVANCED CONFIGURATION

More advanced configuration can be done by editing the appropriate files in /etc directory. Do not change these files unless you are an expert user. The most "safe" files and their purposes are listed in Table 2.

File	Purpose
/etc/bluetooth.conf	WRAP Bluetooth Server Socket Interface commands that are run every time the Bluetooth Server starts. See the WRAP SDK manual for details.
/etc/crontab	Cron daemon settings. Standard crontab format.
/etc/ftpd.conf	FTP daemon configuration file. Self documented.
/etc/profile	Basic user profile.

Table 2. The Supported Advanced Configuration Files.

4 USING THE SYSTEM

This chapter describes the basic features of a BlueGiga WRAP board and their usage. This includes using the WRAP board as a Bluetooth LAN Access Point, Bluetooth Serial Port Cable Replacer, using the Web and FTP servers for uploading content for browsing and downloading, as well as getting familiar with the utility applications and the pre-compiled examples on the WRAP CD.

Using the features described in this chapter does not require the WRAP Software Development Environment to be installed.

4.1 BLUETOOTH

The Bluetooth server is started automatically at power-up. By default, it acts as a LAN Access point following the Lan Access Profile specification. Also the Serial Port Profile is activated. The Bluetooth server can be accessed and controlled (by applications or even interactively with a telnet client) using the socket interface, described in the WRAP SDK manual. Currently, the maximum amount of simultaneous Bluetooth connections is four due the amount of runtime memory a single LAN Access connection requires.

4.1.1 BLUETOOTH SERVER SOCKET INTERFACE PASSWORD PROTECTION

The access to the Bluetooth Server Socket Interface is password protected by default. The password is "buffy" and it can be set with the "setup" application (see section 3.3.1). Password is case sensitive. The password must be typed as the first command after the server has replied with "READY." See the WRAP SDK Manual for further details.

4.1.2 LAN ACCESS PROFILE

This profile is automatically started. By default, no authentication is needed. The default settings can be changed with the "setup" application (see section 3.3.2), or runtime with the socket interface (see the WRAP SDK Manual).

The WRAP board can also act as a LAN Access Client, but in this case it must be controlled manually using the socket interface, described in the WRAP SDK Manual.

4.1.3 SERIAL PORT PROFILE

The Serial Port Profile is used to replace an RS-232 serial cable between two devices with a Bluetooth connection. The physical setup is shown in Figure 3.

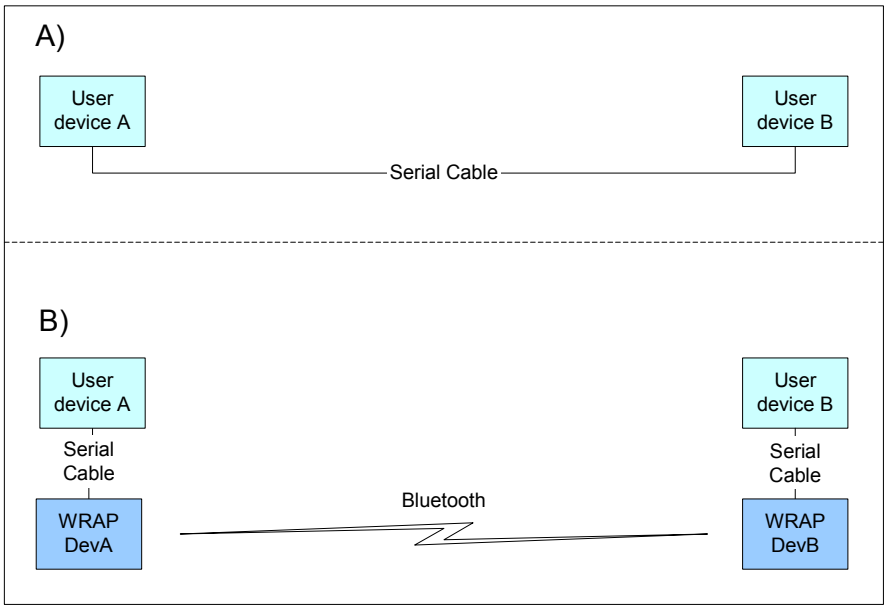

Figure 3. Serial Cable Replacement Physical Setup.

The state A) in the figure is the start situation with a serial cable connecting the devices. This cable is to be replaced with a Bluetooth connection.

In the state B) the long serial connection is replaced with a Bluetooth Serial Port Profile connection between the two WRAP devices. Those WRAP devices are then connected locally to the user devices with (short) serial cables. The cable between the user device A and the WRAP device A must be a cross-over cable. The cable between the user device B and the WRAP device B must be the same cable (direct or cross-over) that was used in state A).

If RTS/CTS handshaking is used to ensure correct data transfer, the serial cables must have these pins connected. **Note:** This handshaking is "local": it takes place between the user device and the WRAP board. No handshaking between the user device A and the user device B on the other end of the Bluetooth connection is provided.

DCD, DTR and DSR signals are not supported. This also means that the user device A and B will not be able to tell whether or not the Bluetooth connection is up. If the connection is up, the data flow is guaranteed to be error free.

When the physical setup is ready, you can create the Bluetooth connection. By default, the Serial Port Profile is started up at boot with the default settings, that is, listening in DevB mode, at 9600 bps, 8 data bits, no parity, 1 stop bit and RTS/CTS enabled. To change these settings, use the "setup" application, as described in section 3.3.3.

You can also start the Serial Port Profile manually by using the "serialport" application. To see the usage of this application, give the command "serialport --help" at WRAP command prompt.

Note: When Serial Port Profile is enabled, the WRAP SMS Gateway Server cannot be used as they share the same physical user serial port

4.1.4 OBJECT PUSH AND FILE TRANSFER PROFILE

WRAP has also two OBEX profiles: the Object Push Profile (ObjP) and File Transfer Profile (FTP). You can use these profiles to transfer files easily between different WRAP devices and other devices supporting them.

These profiles are handled by forwarding incoming calls to "obexserver" program, which handles both profiles. The default work directory is /tmp/obex and users have full read and write access there. By default that directory also contains the default vCard.

Outgoing calls can be made by "obexbrowser" program which is documented in the WRAP SDK Manual.

Two simple command line utilities, "obexput" and "obexget" are also provided. They can be used to send and retrieve a single file to and from another Bluetooth device supporting OBEX. Give either of the commands without parameters to get a short help of using the command.

4.2 SERVERS

The WRAP server applications are started automatically at system power-up or when needed by the Bluetooth server or the Internet services daemon. The servers and their purposes are described in Table 3.

Server	Purpose
bluetooth	WRAP Bluetooth Server, described in detail in section 4.1 and in WRAP SDK Manual.
httpd	WRAP Web Server, described in detail in section 4.2.1.
crond	Daemon to execute scheduled commands. Configurable with /etc/crontab in the same way as any UNIX crond.
ftpd	Internet File Transfer Protocol Server. Configurable with /etc/ftpd.conf.
dhcpcd	DHCP client daemon for automatic network configuration.
In.telnetd	Telnet protocol server.
inetd	Internet services daemon
pppd	Point to Point Protocol daemon. Used by Bluetooth server. Can be used manually over the user serial port (/dev/ttyS3).
syslogd	System logging daemon. Configurable with the setup application.
smsgw	WRAP SMS gateway server, described in detail in section 4.2.2. **Note:** By default this server is not started at power-up.

Table 3. WRAP Servers.

4.2.1 WEB SERVER

The integrated web server in the BlueGiga WRAP supports HTTP/1.0 methods GET and POST, and has light user authentication capabilities. The content can be either static or dynamic – the WWW server is CGI/1.1 compatible.

The web server is always running and the content (http://wrap-ip-address/) is located in the /var/www/htdocs/ directory in the WRAP file system. By default, there is only a simple example file, index.html, there, but it can be replaced, and more directories and pages can be added with FTP or Xmodem.

The directory is accessed with FTP as /flash/var/www/htdocs.

For further information, see web examples in section 4.4.

4.2.2 SMS GATEWAY SERVER

The WRAP SMS Gateway server supports Nokia 20 or Nokia 30 compatible GSM terminals for sending and receiving SMS messages. The device must be connected to the user serial port when the server starts up. The terminals must be configured to operate in RS232/AT-command mode and the PIN-code query of the SIM-card at power-up must be disabled. The configuration of the terminal is done with N20 or N30 Configurator application.

To enable WRAP SMS Gateway Server, use "setup" application, as described in section 3.7.

For further information of using "smsgw", see "makesms" example in section 4.4.

Note: When WRAP SMS Gateway Server is enabled, the Serial Port Profile cannot be used as they share the same physical user serial port.

4.2.3 TELNET

Users must authenticate before access to WRAP via telnet is permitted. Default password for user "root" is "buffy". The password can be changed on WRAP using command "passwd". The telnet port is the default, 23.

4.3 UTILITIES

The WRAP is basically a small Linux system. Whether logged in from the management console or with telnet, your shell session starts as the root user in the root directory. After that, you have the option to use most of the standard *NIX utilities, briefly listed and described in Table 4. Most of the commands have a small built-in usage help that can be seen by starting the command with "-h" parameter.

Application	Purpose
basename	Strip directory and suffix from filenames.
cat	Concatenate files and print on the standard output.
chgrp	Change group ownership.
chmod	Change file access permissions.
chown	Change file owner and group.
clear	Clear the terminal screen.
cmp	Compare two files.
cp	Copy files and directories.
cut	Remove sections from each line of files.
date	Print or set the system date and time. **Note:** date command does not store the date into the real time clock. Use WRAP RTC application instead.
dd	Convert and copy a file.
df	Report filesystem disk space usage.
dirname	Strip non-directory suffix from file name.
du	Estimate file space usage.
echo	Display a line of text to standard output.
env	Run a command in a modified environment.
expr	Evaluate expressions.
false	Do nothing, unsuccessfully.
find	Search for files in a directory hierarchy.
free	Display amount of free and used memory in the system.
ftp	Internet file transfer program.
grep	Print lines matching a pattern.
gunzip	Expand gzip compressed files.
gzip	Compress files into gzip format.
head	Output the first part of files.
hostname	Show or set the system's host name.
ifconfig	Configure a network interface.
ipfwadm	Set up, maintain, and inspect the IP firewall and accounting rules in the Linux kernel.
kill	Terminate a program.
killall	Kill processes by name.
ln	Make links between files.
logger	Make entries into the system log.
ls	List directory contents.
md5sum	Compute and check MD5 message digest.
mkdir	Make directories.
mkfs.minix	Make a Linux MINIX filesystem.
mktemp	Make temporary file name (unique)
more	File perusal filter for crt viewing.
mount	Mount a file system.
mv	Move (rename) files.
obexbrowser	WRAP obexbrowser. A command line OBEX client interface.
obexget	WRAP OBEX tool for retrieving a file from a remote device with OBEX support.
obexput	WRAP OBEX tool for sending a file to a remote device with OBEX support.
passwd	Update a user's authentication token(s).
pidof	Find a process ID of a running program.
ping	Send ICMP ECHO_REQUEST packets to network hosts.
ps	Report process status.
pwd	Print name of the current/working directory.
reboot	Reboot the system.
renice	Alter priority of running processes.
rm	Remove files or directories.
rmdir	Remove empty directories.
route	Show / manipulate the IP routing table.

rtc	WRAP Real Time Clock (RTC) programming application. Run "rtc –h" for usage. Remember that parameters containing spaces must be enclosed in quotes.
sh	Shell: sh, ., break, case, cd, continue, eval, exec, exit, export, for, if, read, readonly, set, shift, trap, umask, wait, while
sed	A Stream EDitor.
setup	WRAP Setup Application. See chapter 3.
sleep	Delay for a specified amount of time.
sort	Sort lines of text files.
tail	Output the last part of files.
tar	Tar archiving utility.
telnet	User interface to the TELNET protocol.
test	Check file types and compare values.
touch	Change file timestamps.
tr	Translate or delete characters.
true	Do nothing, successfully.
umount	Unmount file systems.
uname	Print system information.
uniq	Remove duplicate lines from sorted lines.
unzip	List, test and extract compressed files in a ZIP archive.
uptime	Tell how long the system has been running.
uudecode	Decode a file create by uuencode.
uuencode	Encode a binary file.
wc	Print the number of bytes, words and lines in files.
vi	A text editor.
wget	A utility to retrieve files from the World Wide Web.
wrapid	WRAP identification program. Shows build and hardware configuration information.
which	Shows the full path of (shell) commands.
zcat	Expand gzip compressed files to standard output.
xargs	Build and execute command lines from standard input.
xmodem	WRAP Xmodem Transfer application. Run without parameters for usage.

Table 4. Utilities.

4.4 TRANSFERRING FILES TO/FROM WRAP

Using and configuring WRAP often requires that some files are downloaded from the WRAP and/or uploaded to WRAP.

There are two ways of doing this:

1. By FTP (using Ethernet or Bluetooth)
2. By Xmodem (using terminal software connected to the management port of the WRAP)

4.4.1 TRANSFERRING FILES TO/FROM WRAP USING FTP

FTP is a fast and easy way to upload files to the WRAP. If you wish to use FTP for transferring data to (and from) the WRAP, there has to be a FTP daemon running on the WRAP, which normally is the case, and your computer must be connected to the same network with the WRAP. This network can be either your LAN or a Bluetooth LAN access connection up and running between the WRAP and your computer.

To be able to upload files to WRAP, you must log in as "root", whose default password is "buffy" (the password can be changes at WRAP prompt with the command "passwd"). If you login anonymously, you can only download files from the OBEX directory (see section 4.1 for details).

The latest web browsers can also act as FTP clients. For example with Internet Explorer 6, you can access WRAP over FTP simply by browsing to address ftp://root:buffy@wrap-ip-address/. After this, you can navigate in the directories and move and copy files just like you would in the explorer.

After connecting to the WRAP FTP daemon, you need to decide where you want to put your files – either on the ramdisk for testing purposes or on the flash filesystem for preserving your files between power-offs. The ramdisk is accessed through the ram-directory and the flash filesystem through the flash-directory after logging in with FTP.

In the following example we will upload our application to the /tmp directory (on the ramdisk in WRAP) using a simple FTP client (normally called "ftp" and available both in Linux and Windows command prompt). User input is shown **like this**.

```
$ ftp <wrap-ip-address>
Connected to <wrap-ip-address>.
220 Welcome to Stupid-FTPd server.
User (<wrap-ip-address>:(none)): root
331 Guest login ok, send your e-mail address as password.
Password: buffy (not echoed)
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd ram/tmp
250 CWD command successful.
ftp> put testapp
200 PORT command successful.
150 FILE: testapp
226 Transfer complete.
ftp: 133120 bytes sent in 0.91Seconds 145.96Kbytes/sec.
ftp> bye
221 Bye.
```

If you want to save the application to /usr/local/bin (on the flash filesystem), you will have to replace 'cd ram/tmp' with 'cd flash/usr/local/bin'. To examine the directory structure on the WRAP, please see the appendix in the WRAP SDK manual.

4.4.2 TRANSFERRING FILES TO/FROM WRAP USING TERMINAL SOFTWARE

If your WRAP is not connected to a LAN (either using Ethernet or Bluetooth), you may use your favourite terminal software (like HyperTerminal in Windows) to transfer data to the WRAP. The WRAP contains an Xmodem protocol application called "xmodem", which allows it to transfer data over the console using almost any terminal software available.

1. Connect your computer to the WRAP management UART using the serial cable shipped with the product, and start your terminal software (115 200bps, 8 data bits, no parity, 1 stop bit, no flow control).
2. At WRAP's command prompt, change your working directory to where you want to upload your application, and run the "xmodem" application in WRAP with your application name as parameter. To download a file, use "xmodem –s " instead.
3. Start Xmodem send from your terminal software.

Example upload:

```
/> cd /tmp
/mnt/ram/tmp> xmodem testapp
start xmodem transfer now.
Now start xmodem (checksum, not CRC) send from your terminal.
xmodem receive completed.
```

Example download:

```
/> cd /tmp
/mnt/ram/tmp> xmodem -s test.log
start xmodem transfer now.
Now start xmodem (checksum, not CRC) receive from your terminal.
xmodem send completed.
```

If you want to save the application to /usr/local/bin (on the flash filesystem), you will have to replace 'cd /tmp' with 'cd /usr/local/bin'. To examine the directory structure on the WRAP, please see the appendix in the WRAP SDK manual.

4.5 APPLICATION EXAMPLES

To demonstrate the software development features of the WRAP, the WRAP Software Development Environment comes with several application examples. On the WRAP CD, these examples are provided in a package that can be installed on the WRAP for testing without installing the WRAP Software Development Environment.

4.5.1 INSTALLING EXAMPLES

The compiled examples are located on the WRAP CD in the file \tar\bin-examples- bg.tar and are not installed on the WRAP board during the initial installation procedure described in chapter 2. The examples must be uploaded and installed on the WRAP board manually.

Uploading can be done with FTP or Xmodem, as described in section 4.5.1. After uploading, the examples archive needs to be unpacked with the tar command before they can be used.

Here is an example session from a Windows 2000 laptop, in which all examples are transferred and unpacked, and the led example is started in the end:

```
C:\>d:
D:\>cd tar
D:\tar>ftp <wrap-ip-address>
Connected to <wrap-ip-address>.
220 Welcome to Stupid-FTPd server.
User (<wrap-ip>:(none)): root
331 Guest login ok, send your e-mail address as password.
Password: buffy (not echoed)
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd ram/tmp
250 CWD command successful.
ftp> put bin-examples-bg.tar
200 PORT command successful.
150 FILE: bin-examples-bg.tar
226 Transfer complete.
ftp: 133120 bytes sent in 0.91Seconds 145.96Kbytes/sec.
ftp> bye
221 Bye.
D:\tar>telnet <wrap-ip-address>
wrap login: root
password: buffy (not echoed)
/> cd /tmp
/mnt/ram/tmp> tar xvf bin-examples-bg.tar
./btsend
. . .
./www/index.html
/mnt/ram/tmp> ./led
Clear all LEDs, 0: OFF 1: OFF 2: OFF 3: OFF 4: OFF 5: OFF 6: OFF 7: OFF
Press ENTER to continue...
```

4.5.2 RUNNING EXAMPLES

After the examples have been transferred to the WRAP, they can be run from the directory to which they were unpacked. The examples with their usage and purpose are described in Table 5. **Note:** The example WWW pages must be transferred to flash filesystem where the Web server can find them. In this user manual it is assumed that this has been done by giving command "mv www/* /var/www/htdocs" in the directory where the bg-examples-bin.tar –file was unpacked.

Example, source in wrap/src/examples/	Usage, when installed to mnt/ram/tmp and it is the current directory	Purpose
helloworld	./helloworld	The "Hello, world!" application.
serial	./serial /dev/ttyS3	"Hello, world!" to the serial port.
btsend	./btsend – 12 on the first device, ./btsend <bdaddr of first> 12 on second	Machine 2 Machine example. "Hello, world!" over Bluetooth. **Note:** currently uses the default Bluetooth password "buffy"
io/led io/dip io/gpio io/ad	./led ./dip ./gpio ./ad	I/O: LED example. I/O: DIP example. I/O: GPIO example. I/O: A/D example. Only for WRAP 2151.
m2n	echo testmessage | ./m2n	Machine 2 Networks example. System Logger configuration needed for actual remote connection. Without it, simulates it locally.
man2m	./ledserver & browse with Java-enabled browser to http://wrap-ip-adress/man2m/ **Note:** assumes WWW pages moved as guided.	Man 2 Machine example. Also demonstrates Java applets.
www	Browse to http://wrap-ip-address/ **Note:** assumes WWW pages moved as guided.	Demonstration of the web server capabilities.
waba	CLASSPATH=$CLASSPATH:. export CLASSPATH waba –a ConnectionTest cat tmp	A WABA application which retrieves a web page from http://www.hut.fi into file "tmp"
makesms	Browse to http://wrap-ip-address/sms/ **Note:** assumes WWW pages moved as quided, "makesms" example application is in /usr/local/bin and WRAP SMS Gateway is up and running (see section 4.2.2).	Demonstrates WRAP SMS Gateway by sending SMS messages with required Nokia N30 or N20 GSM Terminal.
obexbrowser	Documented in the WRAP SDK Manual.	Demonstrates the usage of the WRAP OBEX libraries implementing Object Push Profile and File Transfer Profile clients.

Table 5. Examples, Their Usage and Purpose.

If you do not want to re-install the examples after every system power-off, they can be stored to the flash filesystem. Simply use mv command to move the executables of the examples you want to save into /usr/local/bin. After this, you can execute the examples from anywhere (without the ./) and access the web examples directly under http://wrap-ip-address/www/).

4.6 SYSTEM RE-INSTALL

The WRAP platform can be re-installed with the WRAP CD. It contains applications for both Windows and Linux that erase the flash file system and re-install the platform with the default configuration settings. The same program can be used to upgrade the WRAP or to reset the WRAP to initial (delivered) state.

4.6.1 SYSTEM REQUIREMENTS

The following hardware and software is required to re-install WRAP:

- PC with
- Serial port (D9 connector)
- CD-ROM drive
- Operating System
    - Windows 2000 or
    - Linux (tested with RedHat 6.2, 7.0, 7.1, 7.2 and 7.3)

4.6.2 RE-INSTALLING WRAP USING MICROSOFT WINDOWS

To re-install WRAP under Windows:

1. Insert the WRAP CD into the CD-ROM drive.
2. Enter the root of the CD and double click reinstall.exe.
3. Make sure that the WRAP board is connected to the PC via the management serial cable (see section 2.1 for details of connectors), and that the power cable is disconnected.
4. (Optional) If you use a serial port other than the default COM1, you can change it from the Settings menu.
5. Click the Install WRAP button.
6. When asked to do so, turn on the WRAP board by connecting the power cable.
7. Wait for a couple of minutes until the software has completed the installation process. (A message will be displayed.)
8. Close the installation software by clicking Exit button.
9. (Optional) Start a terminal emulator (the serial port settings for the console are 115200bps, 8 data bits, no parity, one stop bit) if you want to see the system boot-up procedures.
10. Restart the WRAP board: either press the reset button on the board (see the corresponding hardware manual), or disconnect the power cable, wait for 10 seconds, and reconnect the power cable. **Note:** at least some laptops require that also the management console cable is disconnected before restarting.

4.6.3 RE-INSTALLING WRAP USING LINUX

To re-install WRAP under linux, mount the WRAP CD, change the current working directory to where it is mounted, run reinstall-script as root, and follow the instructions. The management serial cable must be connected and, when asked, the power cable needs to be connected too. See section 2.1 for details of connectors.

Example (things you need to type are in written **`like this`**):

```
$ su -
$ mount /dev/cdrom /mnt/cdrom
$ cd /mnt/cdrom
$ ./reinstall (or 'sh reinstall' if you get access denied error)
```

After installing the boot loader and the operating system to the WRAP board, you may boot your WRAP hardware (press the reset button or disconnect and reconnect the power cable) and begin using it.

5 BLUETOOTH TECHNOLOGY OVERVIEW

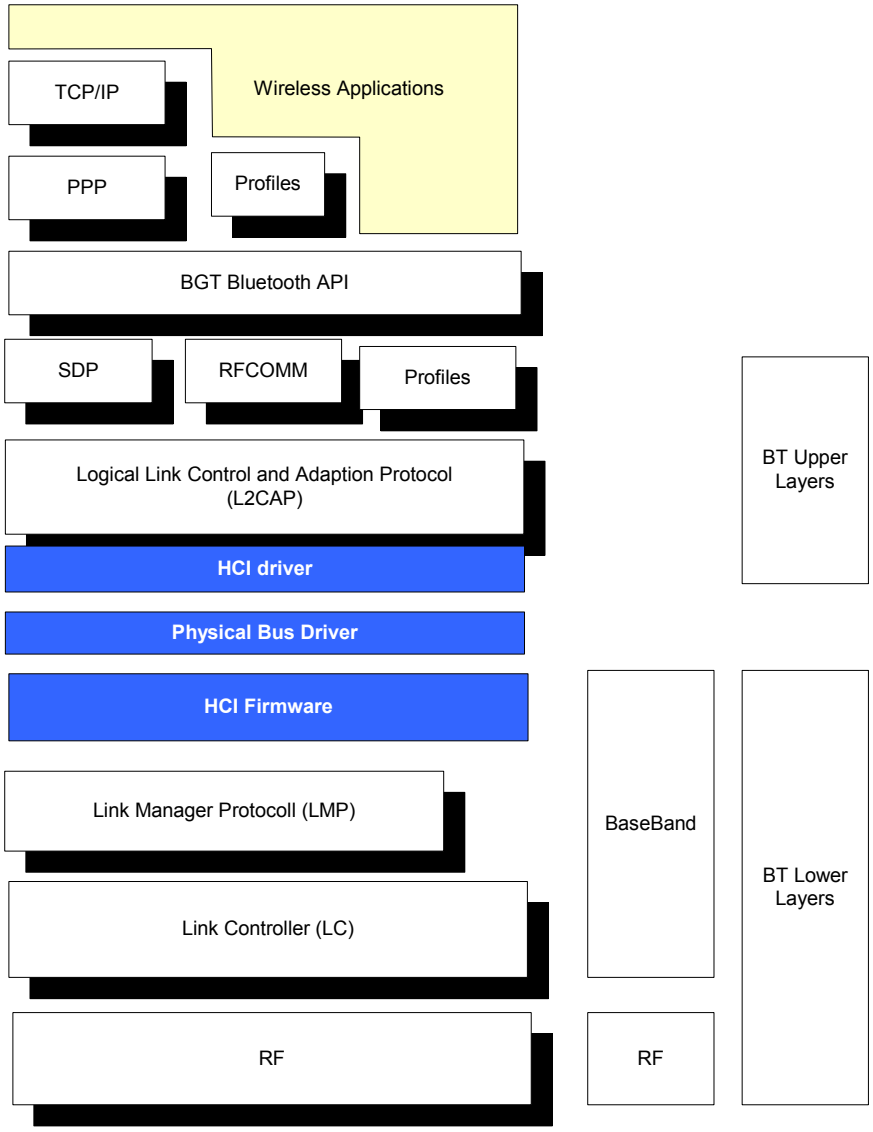

Figure 4. Bluetooth Software and Hardware Components.

5.1 FREQUENCY BANDS AND CHANNEL ARRANGEMENT

The Bluetooth system operates in the license-free 2.4 GHz ISM (Industrial Science Medial) band using frequency hopping spread spectrum (FHSS). In the vast majority of countries around the world this frequency band is 2400 – 2483.5 MHz. Some countries have, however, national limitations on the frequency range. In order to comply with these national limitations, special frequency hopping algorithms have been specified for these countries. It should be noted that products implementing the reduced frequency band will not work with products implementing the full band. Products implementing the reduced frequency band must therefore be considered local versions.

The Bluetooth frequency band is divided into distinct channels with 1 MHz channel spacing. In order to comply with out-of-band regulations in each country, a guard band is used at the lower and upper band edge. For the USA, Europe, and most other countries the frequency range is 2.400 – 2483.5 MHz and the corresponding channels are f = 2402 + k MHz; k = 0 ¼ 78. In France, the frequency range is 2.4465 – 2.4835 GHz and the corresponding channels are f = 2454 + k MHz; k = 0 ¼ 22. Transmission utilises channel hopping over the specified range at 1600 kHz hop frequency. When operating in countries that permit only a subset of the overall spectrum, transmission utilises only the approved portions of the spectrum. The Bluetooth system utilises Gaussian frequency shift keying (GFSK). The signalling rate is 1 Mbit/s.

5.2 POWER CONSIDERATIONS

The Bluetooth system transceivers are classified into three power classes to support different link ranges.

- Power Class 1. Output power is 1 – 100 mW (0 – 20 dBm) with mandatory power control ranging from 4 to 20 dBm.
- Power Class 2. Output power is 0.25 – 2.5 mW (-6 – +4 dBm) with optional power control.
- Power Class 3. Output power is less than 1 mW (0 dBm) with optional power control.

BlueGiga's WRAP products support 10 m link range with Option 1 (Power Class 1).

5.3 RADIO FREQUENCY PROPAGATION

The radio frequency signal propagates in free space as a spherical wave, from a point source to all directions equally. In reality, the signal source always differs from a theoretic isotropic signal source. The power distribution of wireless telecommunication equipment in space is determined by the antenna radiation pattern. In free space the signal propagates with the speed of light and attenuates with 1/r2 relation. In reality, the environment always differs from free space. The propagation environment of wireless telecommunication equipment is restricted by all obstacles.

The basic mechanism of radio propagation is attributed to reflection, diffraction, and scattering depending on existing obstacles. Since the radio frequency signal propagates in all directions the transmitted signal arrives at the receiver following multiple paths deformed by the aforementioned propagation mechanisms. The received signal is the superposition of attenuated and delayed replicas of the transmitted signal leading to fading of the transmitted signal and broadening of the duration of the transmitted pulse. The transmitted pulse delay spread leads to inter-symbol interference (ISI) because the subsequent symbols interfere with each other. The ISI leads to a bit error probability (BIT) floor that is independent of the signal to noise ratio (SNR). Depending on the time delay spread of the transmitted pulse or the amount of widening that the transmitted pulse experiences across the radio channel, the multipath interference differs. When the time delay spread of the transmitted signal is very small with respect to the signalling time the multipath interference essentially leads to the signal fading phenomena of the received signal. When the time delay spread of the transmitted signal is high with respect to the signalling time the multipath interference leads to the symbol interference phenomena of the received signal as well.

A major difference between indoor and outdoor environments is that the former is considerably more sensitive to changes in the geometry of the environment than the latter. This is because of the differences in distance between obstacles. For example, a door being shut rather than open may have a major impact on an indoor environment whereas a comparable event in an outdoor environment may have a minor impact.

The Bluetooth standard has been designed to operate in noisy radio frequency environments. Transmission utilises fast frequency hopping and short packages to make the link efficient and robust. Fast hopping and short packages limit the impact of interfering devices on the same frequency band.