Parani-MSP1000

For Wireless Multi-Serial Communications,
based on Bluetooth Technology

User Guide

Version 1.2.8

User Guide for the Parani-MSP1000

Firmware version 1.2.X

Last revised on September 11, 2015

Printed in Korea

Copyright

Copyright 2007~2015, Sena Technologies, Inc. All rights reserved.

Sena Technologies reserves the right to make changes and improvements to its product without providing notice.

Trademark

Parani™ is a trademark of Sena Technologies, Inc.

Bluetooth is a trademark by the Bluetooth SIG Inc.

Windows® is a registered trademark of Microsoft Corporation.

Ethernet® is a registered trademark of XEROX Corporation.

Notice to Users

Proper back-up systems and necessary safety devices should be utilized to protect against injury, death or property damage due to system failure. Such protection is the responsibility of the user.

This device is not approved for use as a life-support or medical system.

Any changes or modifications made to this device without the explicit approval or consent of Sena Technologies will void Sena Technologies of any liability or responsibility of injury or loss caused by any malfunction.

Technical Support

Tel: (+49) 761-592100

Fax: (+49) 761-59210-39

E-Mail: support@ParaniSerial.com

Website: http://www.ParaniSerial.com

Revision History

Revision	Date	Name	Description
V1.0.0	2007-09-11	Hanjun Yeom	Final v1.0.0 release
V1.1.1	2008-01-11	Hanjun Yeom	Revised for v1.1.0 release.
V1.2.0	2008-04-15	K. Lee	Revised for v1.2.0 release.
V1.2.2	2008-11-06	K. Lee	Revised for v1.2.2 release.
V1.2.4	2010-03-04	HR Zo	Revised for v1.2.4 release
V1.2.7	2011-12-26	HR Zo	Package does not contain CD-ROM
V1.2.8	2015-09-11	K. Lee	Change the contact information

Contents

1. Introduction

1.1. Overview

The Parani-MSP1000 is a Bluetooth Access Point used to enable Bluetooth devices to be connected to a 10/100Mbps Ethernet network. Parani-MSP1000 supports 7, 14, and 28 Bluetooth connections, according to the model, and supports up to 3Mbps throughput through the Bluetooth 2.0+EDR specification. The Parani-MSP1000 is a class 1 Bluetooth device that supports 150m using the basic dipole antenna and up to 1 km using the patch antenna. The Parani-MSP1000 supports such various Bluetooth profiles such as, Serial Port (SPP), LAN Access over PPP (LAP), Dial-up Networking (DUN), Personal Area Networking (PAN) and FTP for use with various applications.

For those user's applications requiring secure data communication, the Parani-MSP1000 supports SSLv2 SSLv3, TLSv1, SSHv1 and SSHv2 for data encryption. In addition, an IP address filtering function is provided for protecting unintentional data streams to be transmitted to the Parani-MSP1000. The dual Ethernet, fail-over feature may also be also helpful to users who want to have a failsafe Ethernet connection in times when the main Ethernet connection should fail.

A COM/TTY port redirector software is provided for free for Windows/Linux, for user's applications that still require the use of COM ports.

The Parani-MSP1000 is based on embedded Linux system and supports versatile Python script engine. Users may customize the Parani-MSP1000 for various functionalities, by using Python script. Users may run a custom Python script in the 2MB user space provided by the Parani-MSP1000.

The Parani-MSP1000 provides users with a full-featured system management functionality which includes the use of the system status display, firmware upgrade, remote reset and system log display by connecting through any one of the multiple interfaces such as, telnet, SSH, serial console port or web interface.

Typical application areas of the Parani-MSP1000 are:
- Industrial automation
- Wireless building automation
- Wireless POS system
- Wireless printing
- Wireless factory monitoring
- Wireless machine monitoring

- Security/Access control system

- General data acquisition application

- Truck/Bus monitoring system

- Car diagnostics

Please note that this manual assumes that the user has some knowledge of Bluetooth and TCP/IP Internetworking protocols and terminologies.

1.2. Package Check List

- DC Power Adapter

- Quick Start Guide

- RS232 Serial Console Cable

- Ethernet Cross Cable

- Dipole antenna

1.3. Product Specification

	Parani-MSP1000
Ethernet interface	Dual 10/100 Base-T Ethernet with RJ45 connector
	Supports Static IP and Dynamic IP address
Bluetooth interface	Bluetooth v2.0 + EDR Class 1 Level: 17dBm Frequency: 2.4GHz Profiles - Serial Port, LAN access over PPP, PAN, Dial up Networking

	Working distance:
	  DAT-G01R Antenna - Stub(Dafault) Antenna up to 150m
	  DAT-G01R Antenna - DAT-G01R Antenna up to 200m
	  DAT-G01R Antenna - DAT5-G01R Antenna up to 300m
	  DAT-G01R Antenna - PAT-G01R Antenna up to 500m
	  DAT5-G01R Antenna- DAT5-G01R Antenna up to 400m
	  DAT5-G01R Antenna- PAT-G01R Antenna up to 600m
	  PAT-G01R Antenna - PAT-G01R Antenna up to 1000m

Point to multi point connectivity	MSP1000A : Up to 7 Bluetooth connections MSP1000B : Up to 14 Bluetooth connections MSP1000C : Up to 28 Bluetooth connections
Network protocols	IPv4, ICMP, ARP, TCP, HTTP, Telnet, TFTP, SSH, https, SSL, TLS, DNS, SCP, Syslog, NTP
Configuration	Web, Telnet, SSH, Serial Console
Diagnostic LED	Power, Status, Ethernet0, Ethernet1 Signal Strength, No of Connections
Power	Supply voltage: 5V DC Nominal Current Consumption: 1.2A@ 5VDC approximately

	Common power supply options: Power via a standard AC-plug DC-adapter
Hardware interface	LAN 10/100 x 2 Inclusive hub function Ethernet/RS232C COM supported
Environmental	Operating temperature: 0 ~ 50 °C Storage temperature: -30 ~ 85 °C Humidity: 90% Non-condensing

Physical properties	Dimension (LxWxH)
	  203 x 170 x 44 (mm)
	  7.99 x 6.69 x 1.73 (in.)

	Weight
	  MSP1000A : 1414g
	  MSP1000B : 1432g
	  MSP1000C : 1468g

Approvals	FCC, CE, MIC, Telec
COM port redirector Software	Serial/IP
Warranty	3-year limited warranty

Note *:

Bluetooth v2.0 supports the AFH function. The AFH function is used to decrease the amount of interference between WiFi and Bluetooth radios by automatically avoiding any active WiFi channels. However, AFH does not provide a complete solution, allowing WiFi and Bluetooth to work together in harmony; AFH will only decrease the likelihood of interference. It is highly recommended for users to test their wireless system throughly before deployment, since the overall system performance can be influenced by various environmental factors such as distance and other environmental radio interference.

2. Getting Started

2.1. External View
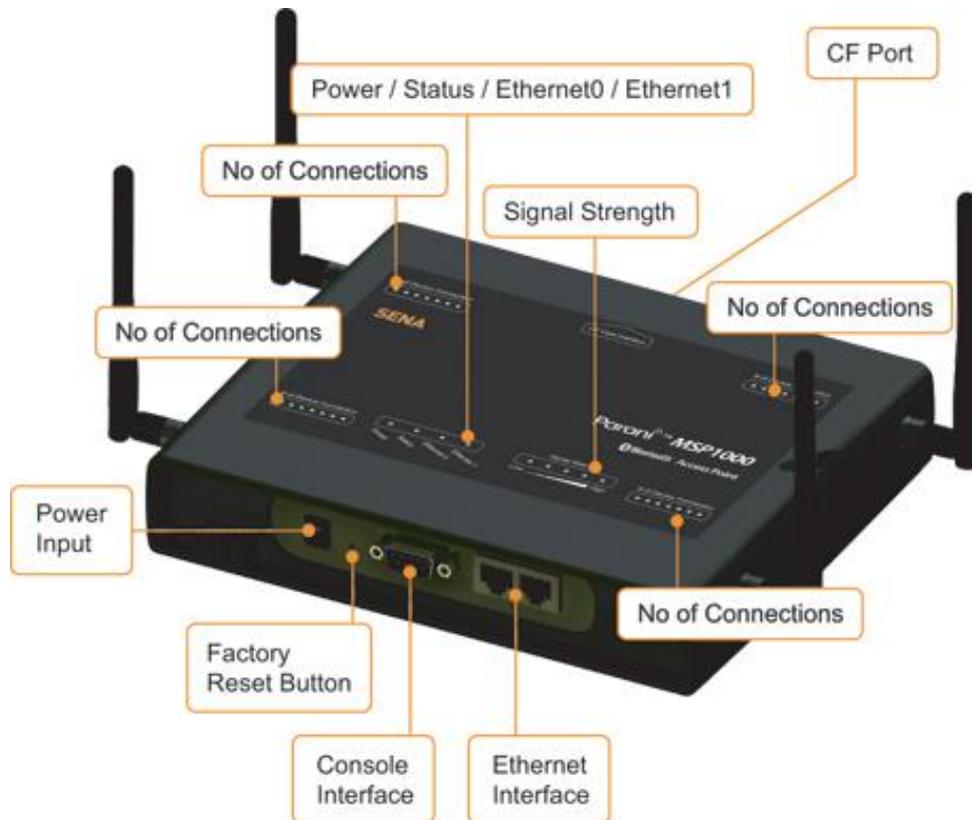
Figure 2-1 External view of the Parani-MSP1000

2.2. LED Indicators

The Parani-MSP1000 has a number of LED indicator lamps for status display. Table 2-1 describes the function of each LED indicator lamp.

Table 2-1 LED indicator lamps

Lamps		Function
Ethernet	**Ethernet 0**	Blinks whenever there is any activity on the Ethernet 0 port
	Ethernet 1	Blinks whenever there is any activity on the Ethernet 1 port
Bluetooth	**Signal Strength**	Shows the signal strength of Bluetooth sessions currently connected to the Parani-MSP1000.
	No of Connections	Shows the number of Bluetooth sessions currently connected to the Parani-MSP1000
System	**Status**	Solid GREEN, if system is running and ready to be used.
	Power	Solid GREEN, if power is supplied

2.3. Connecting the Hardware

This section describes how to connect the Parani-MSP1000 to your equipment for initial testing/installation.

- Connect the power source to the Parani-MSP1000
- Connect the Parani-MSP1000 to a Ethernet network.

2.3.1. Connecting the power

Connect the power cable to the Parani-MSP1000. If the power is properly supplied, the [Power] lamp will light up solid green.

Figure 2-2 Connecting the power to the Parani-MSP1000

2.3.2. Connecting to the network

Plug one end of the Ethernet cable to the Parani-MSP1000 [Eth0] port. The other end of the Ethernet cable should be connected to an Ethernet network. If the cable is properly connected, the Parani-MSP1000 will have a valid connection to the Ethernet network. This will be indicated by:
The [Eth0] LED flashing to indicate incoming/outgoing Ethernet packets.

Figure 2-3 Connecting a network cable to the Parani-MSP1000

2.4. Configurations

The Parani-MSP1000 provides several techniques to configure your unit for the environment.

- **RS232 Serial console**

  If users want to configure the MSP1000 before connecting the unit to a network or if a network connection is not available, they can accomplish this by using RS232 serial console cable provided in the package.

- **Remote console**

  Users who require a menu-driven interface from a remote location can utilize Telnet (port 23) or SSH (port 22) connections to the Parani-MSP1000 using Telnet or SSH client. The menu-driven user interface provides limited functions for initial configuration.

NOTE : Please note that Parani-MSP1000 supports only the SSH v2, so user must use the SSH client which is able to support SSH v2.

- **Web Interface**

  Remote users who want to use a web browser to configure the Parani-MSP1000 can connect to the Parani-MSP1000 using a conventional web browser, such as Internet Explorer or Firefox Navigator. The Web Interface comprises of an Easy-to-use menu-driven user interface that provides full-featured configuration of the MSP1000 .

2.4.1. Configuration using the RS232 serial connection

1) Connect one end of the console cable to the console port on the Parani-MSP1000.

Figure 2-4 Connecting a system console cable to the Parani-MSP1000

2) Connect the other end of the cable to the serial port of the user's computer.

3) Run a terminal program (i.e. HyperTerminal). Set the serial configuration parameters of the terminal program as follows:

- **9600 Baud rate**
- **Data bits 8**
- **Parity None**
- **Stop bits 1**
- **No flow control**

4) Press the [ENTER] key.

5) Enter your username and password into the Parani-MSP1000. The factory default user settings are as follows.

    Login: root   Password: root

6) After logging in , users can use various shell commands in the CLI(Command Line interface). For details on usage of the CLI, refer to the chapter 10. "CLI Guide".

7) "editconf" command will allow you to enter the text-menu driven interface .

```
[root@MSP1000 /]# editconf
--------------------------------------------------------------------------------
Welcome to MSP1000 configuration page
Current Time  : 7/14/2007 12:22:56   Serial No.      : msp1000-test1234
F/W Rev.      : v1.0.0               MAC Addr.(eth0) : 00:01:95:AF:BF:DD
IP Mode (eth0) : Static              IP Addr.(eth0)  : 192.168.161.5
--------------------------------------------------------------------------------
1. Network configuration
2. System administration
3. System status & log
4. CF card configuration
5. Monitoring
6. Save changes
7. Exit without saving
8. Exit and apply changes
9. Exit and reboot
 <ESC> Back, <ENTER> Refresh
--> 1
```

8) Select menu 1. [Network Configuration] and then proceed to [Ethernet 0] configuration to set up the IP address of the box. Users may set up the network configuration according to their environment. Once network set-up is done, users may access the box through telnet/ssh connection or via a web browser.

```
--------------------------------------------------------------------------------
 Network Configuration
--------------------------------------------------------------------------------
1. ETHERNET 0 (eth0) configuration
2. ETHERNET 1 (eth1) configuration
3. Firewall configuration
4. TCP configuration
 <ESC> Back, <ENTER> Refresh
--> 1

--------------------------------------------------------------------------------
 ETHERNET 0 (eth0) configuration
--------------------------------------------------------------------------------
1. IP mode: Static IP
2. IP address: 192.168.14.123
3. Subnetmask: 255.255.0.0
4. Gateway: 192.168.1.1
5. Primary DNS: 168.126.63.1
6. Secondary DNS: 168.126.63.2
 <ESC> Back, <ENTER> Refresh
-->
```

From the main menu screen, the users may select a menu item for configuration of the Parani-MSP1000 parameters by selecting the menu number and pressing the [ENTER] key. In the submenu screen, users can configure the required parameters guided by online comments.

*NOTE: Be sure to perform "**save**" and "**apply**" command before you exit from editconf menu program. All the parameters can be stored into the non-volatile memory space of the box, but the settings will not be stored until users perform "**save**" command on the menu. All the configuration change will be effective after entering "**apply**" command.*

2.4.2. Configurations using Ethernet connection

The IP address of the Parani-MSP1000 must be known before users can access the box using the Remote console. The default IP address of the Parani-MSP1000 is **192.168.161.5**. Once users know the IP address of the box, they can access to it either by using telnet/ssh program or a web browser. The default user name and password is as same as the serial console interface as follows.

```
root : root
```

1) Telnet/SSH Access

The steps for accessing telnet/ssh interface is exactly same as in the serial console access. Please take steps from 5) to 8) in chapter 2.4.1 to get into the menu-driven user interface.

2) Web Access

The Parani-MSP1000 supports both HTTP and HTTPS (HTTP over SSL) protocols.

*Figure 2-5 Login screen of the Parani-MSP1000 web management*
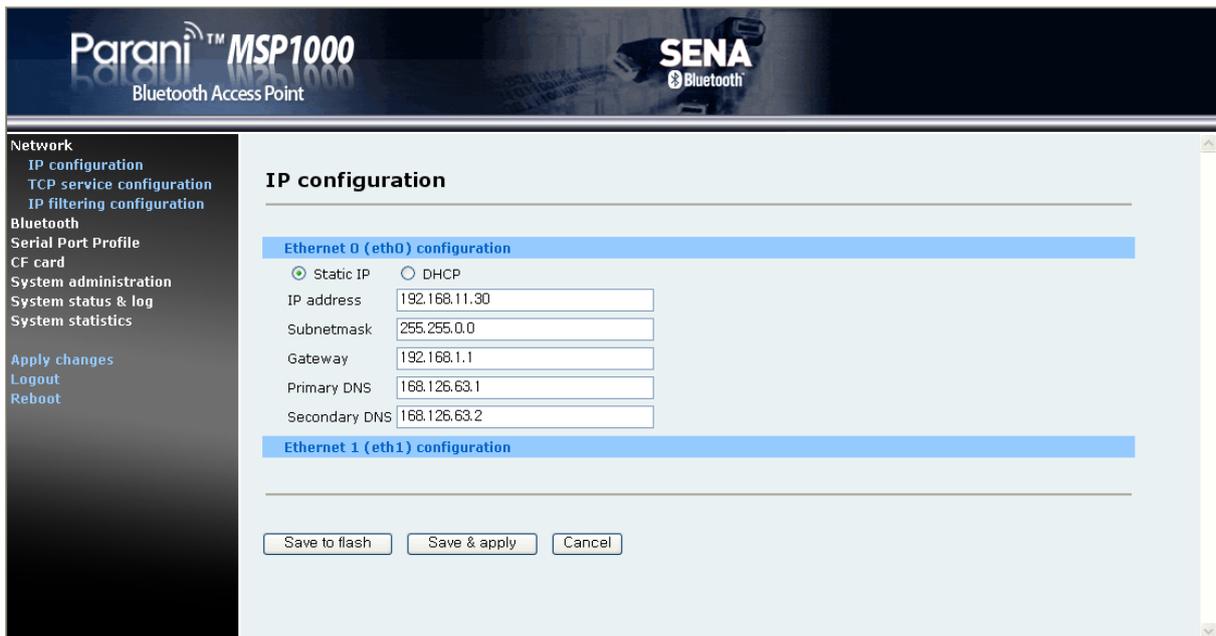
Figure 2-6 The Parani-MSP1000 web management screen

Figure 2-6 shows the configuration homepage of the Parani-MSP1000 Web management interface. A menu bar is provided on the left hand side of the screen. The menu bar includes the uppermost configuration menu groups. Selecting an item on the menu bar opens a tree view of all the submenus available under each grouping.   Selecting a submenu item will allow the user to modify parameter settings for that item. Every page will allow the user to [Save to Flash], [Save & apply] or [Cancel] their actions. After changing the configuration parameter values, the users must select [Save] to save the changed parameter values to the non-volatile memory.

To apply all changes made, the user must select [Apply Changes].   This option is available on the bottom of the menu bar. Only when the user selects [Apply changes] will the new parameter values be applied to the Parani-MSP1000 configuration. Users also can select [Save & apply] to save parameters and apply changes in one step.
If the user does not want to save the new parameter values, the user must opt to [Cancel]. All changes made will be lost and the previous values restored. Any changes that are already saved or applied cannot be canceled.

2.4.3. Configurations using Bluetooth wireless connection

The Parani-MSP1000 provides PAN (Personal Area Network) profile service as a way to access the configuration interface of the box through using a Bluetooth connection. Users may initially configure the box using Bluetooth connection when their PC or lap-top has Bluetooth communication capability.

Please refer to the following:

1) Attach the power adapter to the Parani-MSP1000. Do not attach the Ethernet cable on the MSP1000 or the PC.

2) Search for the Parani-MSP1000 using Bluetooth Scan software and then connect to the device using [Network Access Point] protocol.

3) Make sure the connection is made, and then check the IP address of the PC or laptop.
   The Parani-MSP1000 has a built-in DHCP server, and it leases the 10.0.0.x IP address to the client computer. The default IP address of the Parani-MSP1000 in this PAN is 10.0.0.1.

4) Try to connect to the Parani-MSP1000 by IP address, 10.0.0.1 using web or telnet program.

5) Users can configure the box using wireless connection.

3. Network Configuration

3.1. IP Configuration

3.1.1. Ethernet 0 (eth0) configuration

The Parani-MSP1000 requires a valid IP address to operate within the user's network environment. If the IP address is not readily available, contact the system administrator to obtain a valid IP address for the Parani-MSP1000. Please note that the Parani-MSP1000 requires a unique IP address to connect to the user's network.

The users may choose one of two Internet protocols in setting up IP address: i.e.

- **Static IP**
- **DHCP** (Dynamic Host Configuration Protocol)

The Parani-MSP1000 is initially defaulted to **STATIC** mode, with a static IP address of **192.168.161.5**. *Table 3-1* shows the configuration parameters for all two IP configurations. *Figure 3-1* is an example of what the actual web-based GUI display looks like.

Table 3-1 IP configuration Parameters

| Static IP	IP address
	Subnet mask
	Default gateway
	Primary DNS/ Secondary DNS
DHCP	Primary DNS/ Secondary DNS (Optional)
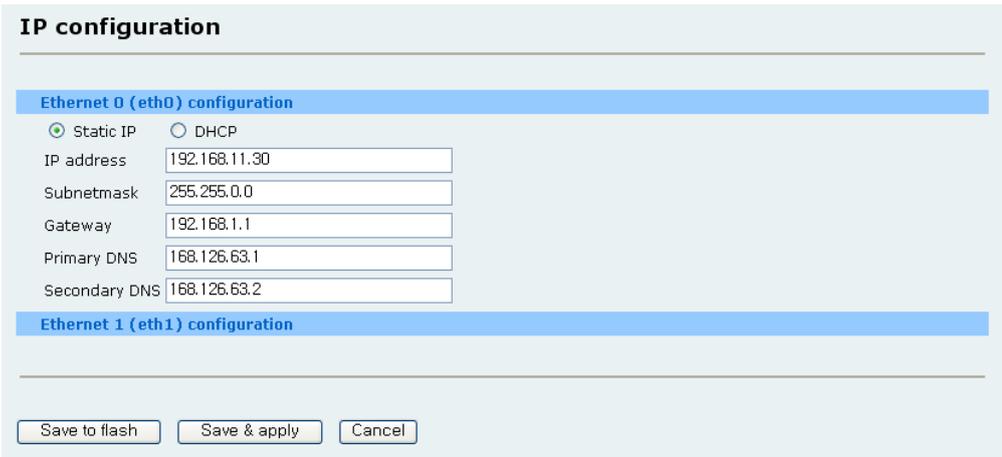
Figure 3-1 IP Configuration

3.1.1.1. When using a Static IP Address

When using a **Static IP** address, the user must manually specify all the configuration parameters associated with the IP address of the Parani-MSP1000. These include the IP address, the network subnet mask, the gateway computer and the domain name server computers. This section will look at each of these in more detail.

Note: The Parani-MSP1000 will attempt to locate all this information every time it is turned on.

● **IP address**

A Static IP address acts as a "static" or permanent identification number.   This number is assigned to a computer to act as its location address on the network. Computers use these IP addresses to identify and talk to each other on a network. Therefore, it is imperative that the selected IP address be both unique and valid in a network environment.

Note: *192.168.1.x, 172.16.x.x and 10.x.x.x will never be assigned by and ISP (Internet Service Provider).   IP addresses using this form are considered private. Actual applications of the Parani-MSP1000 may require access to public network, such as the Internet. If so, a valid public IP address must be assigned to the user's computer. A public IP address is usually purchased or leased from a local ISP.*

● **Subnet mask**

A subnet represents all the network hosts in one geographic location, such as a building or local area network (LAN). The Parani-MSP1000 will use the subnet mask setting to verify the origin of all packets. If the desired TCP/IP host specified in the packet is in the same geographic location (on the local network segment) as defined by the subnet mask, the Parani-MSP1000 will establish a direct connection. If the desired TCP/IP host specified in the packet is not identified as belonging on the local network segment, a connection is established through the given default gateway.

● **Default gateway**

A gateway is a network point that acts as a portal to another network. This point is usually the computer or computers that control traffic within a network or a local ISP (Internet service provider). The Parani-MSP1000 uses the IP address of the default gateway computer to communicate with hosts outside the local network environment. Refer to the network administrator for a valid gateway IP address.

● **Primary and Secondary DNS**

The DNS (Domain Name System) server is used to locate and translate the correct IP address for a requested web site address.   A domain name is the web address (i.e. **www.yahoo.com**) and is

usually easier to remember. The DNS server is the host that can translate such text-based domain names into the numeric IP addresses for a TCP/IP connection.

The IP address of the DNS server must be able to access the host site with the provided domain name. The Parani-MSP1000 provides the ability to configure the required IP addresses of both the Primary and Secondary DNS servers addresses. (The secondary DNS server is specified for use when the primary DNS server is unavailable.)

3.1.1.2. When using Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage and automate the assignment of IP addresses centrally in an organization's network. DHCP allows the network administrator the ability to supervise and distribute IP addresses from a central point and automatically send a new IP address when a computer is plugged into a different network location.

When in static IP mode, the IP address must be entered manually at each computer. If a computer is moved to another network location, a new IP address must be assigned. DHCP allows all the parameters, including the IP address, subnet mask, gateway and DNS servers to be automatically configured when the IP address is assigned. DHCP uses a "lease" concept in assigning IP addresses to a computer. It limits the amount of time a given IP address will be valid for a computer. All the parameters required to assign an IP address are automatically configured on the DHCP server side, and each DHCP client computer receives this information when the IP address is provided at its boot-up.

Each time the device is reset, the Parani-MSP1000 broadcasts a DHCP request over the network. The reply generated by the DHCP server contains the IP address, as well as the subnet mask, gateway address, DNS servers and the "lease" time. The Parani-MSP1000 immediately places this information in its memory. Once the "lease" expires, the Parani-MSP1000 will request a renewal of the "lease" time from the DHCP server. If the DHCP server approves the request for renewal, the Parani-MSP1000 can continue to work with the current IP address. If the DHCP server denies the request for renewal, the Parani-MSP1000 will start the procedure to request a new IP address from the DHCP server.

Note: While in DHCP mode, all network-related parameters for the Parani-MSP1000 *should be configured automatically, including the DNS servers*

A DHCP sever assigns IP addresses dynamically from an IP address pool, which is managed by the network administrator. This means that the DHCP client, i.e. the Parani-MSP1000, receives a different IP address each time it boots up. The IP address should be reserved on the DHCP server side to assure that the user always knows the newly assigned Parani-MSP1000 address. In order to reserve the IP address in the DHCP network, the administrator needs the MAC address of the Parani-MSP1000 found on the label sticker at the bottom of the Parani-MSP1000.

3.1.2. Ethernet 1 (eth1) configuration

The Parani-MSP1000 has two Ethernet ports. The users may configure the secondary Ethernet (eth1) to "Bridged with eth0", "Bridged with pan0" or "Disable".

- **Bridged with eth0**

  The eth1 will be bridged to eth0. It will work as a fail-over link to eth0. When the eth0 is unplugged, the Parani-MSP1000 sends packets through eth1 instead of eth0. While in this operating mode, the IP address of eth1 is the IP address configured for the eth0. When the switching from eth0 to eth1 or from eth1 to eth0 occurs, it should not affect the TCP sessions.

- **Bridged with pan0**

  The eth1 will be bridged to network interface for Personal Area Network (pan0). The Parani-MSP1000 treats the hosts connected via eth1 as the hosts connected via Bluetooth profiles (PAN, LAP and DUN). This means that the hosts connected to Parani-MSP1000 via eth1 are able to communicate the hosts connected to Parani-MSP1000 via Bluetooth.

- **Disable**

  The eth1 will be disabled.

## 3.2. Dynamic DNS Configuration

When users connect the Parani-MSP1000 to a DSL line or use a DHCP configuration, the IP address might be changed whenever it reconnects to the network. It can therefore be very difficult to post all related contacts for each new IP address. In addition, if the administrator only has access through the remote console, there is no way to know if an IP address has changed, or what the new IP address is.

A Dynamic DNS service is provided by various ISPs or organizations to deal with the above issue. By using the Dynamic DNS service, users can access the Parani-MSP1000 through the hostname registered in the Dynamic DNS Server regardless of any IP address change.

By default, the Parani-MSP1000 only supports Dynamic DNS service offered at Dynamic DNS Network Services, LLC (www.dyndns.org). Contact Sena technical support for issues regarding other Dynamic DNS service providers.

To use the Dynamic DNS service provided by Dynamic DNS Network Services, the user must set up an account in their Members'' NIC (Network Information Center - http://members.dyndns.org). The user may then add a new Dynamic DNS Host link after logging in to their Dynamic DNS Network Services Members NIC.

After enabling the Dynamic DNS service in the Dynamic DNS Configuration menu, the user must enter the registered Domain Name, User Name, and Password. After applying the configuration change, users can access the Pro Series using only the Domain Name.

Figure 3-2 Dynamic DNS Configuration

3.3. SMTP Configuration

The Parani-MSP1000 can send an email notification when the number of system log messages reaches to certain value The user must configure a valid SMTP server send these automatically generated emails. The Parani-MSP1000 supports three SMTP server types:

- SMTP without authentication
- SMTP with authentication
- POP-before-SMTP

These examples can be seen in Figure 3-3. Required parameters for each SMTP configuration include:

- SMTP server IP address
- SMTP user name
- SMTP user password
- Device mail address

The device mail address specifies the sender's email address for all log and alarm delivery emails. SMTP servers often check only the sender's host domain name of the email address for validity. Consequently, the email address set for the device can use an arbitrary username with a registered hostname (i.e. *arbitrary_user@yahoo.com* or *anybody@sena.com*).

The SMTP user name and SMTP user password are required when either SMTP with authentication or POP-before-SMTP mode is selected.

Figure 3-3 SMTP Configuration

3.4. IP filtering Configuration

The Parani-MSP1000 prevents unauthorized access using an IP address based filtering method. The users can allow one of the following scenarios by changing the parameter settings:

- Any host cannot access a specific service of the Parani-MSP1000

- Only one host of a specific IP address can access a specific service of the Parani-MSP1000

- Hosts on a specific subnet can access a specific service of the Parani-MSP1000

- Any host can access a specific service of the Parani-MSP1000

The IP filtering feature is intended to control access to Telnet console, SSH console, Web server or each Serial Port Profile session, which may be enabled or disabled. The factory default of the IP filtering feature is "All services and ports are accessible from any host".

The meanings of each parameter in IP filtering configuration are as follows,

- Interface

  Apply IP filtering rule to the incoming packet through this interface. This is configurable one of eth0 or pan0.

- Option and IP address/mask

  Input field to describe a specific range of host on the network. The user may allow a host or a group of hosts to access the Parani-MSP1000. The user must then enter the IP address and subnet of access. Any user on a remote host must stay in the specified subnet boundary to access the Parani-MSP1000. To allow only a specific host to access the Parani-MSP1000, enter the IP address of the specific host and just give 255.255.255.255 for the subnet with Normal option. To allow any hosts to have access to the Parani-MSP1000, give 0.0.0.0 for both of the IP address and subnet with Normal option also. Refer to *Table 3-2* for more details.

- Port

  The TCP port number to which the IP filtering rule will be applied. User can select one of

23(Telnet), 22(SSH), 80(HTTP), 443(HTTPS) or each Serial Port Profile session.

● Chain rule

Set the basic rule for the host to access the Parani-MSP1000 as one of Accept or Drop.

Figure 3-4 IP filtering Configuration

Table 3-2 Input examples of Option and IP address/mask combination

Allowable Hosts	Input format	Option
	IP address/mask	
Any host	0.0.0.0/0.0.0.0	Normal
192.168.1.120	192.168.1.120/255.255.255.255	Normal
Any host except 192.168.1.120	192.168.1.120/255.255.255.255	Invert
192.168.1.1 ~ 192.168.1.254	192.168.1.0/255.255.255.0	Normal
192.168.0.1 ~ 192.168.255.254	192.168.0.0/255.255.0.0	Normal
192.168.1.1 ~ 192.168.1.126	192.168.1.0/255.255.255.128	Normal
192.168.1.129 ~ 192.168.1.254	192.168.1.128/255.255.255.128	Normal
None	0.0.0.0/0.0.0.0	Invert

3.5. TCP service Configuration

If a TCP session is established between two hosts, the connection should be closed (normally or abnormally) by either of the hosts to prevent the lock-up of the corresponding TCP port. To prevent this type of lock-up situation, the Parani-MSP1000 provides a TCP "keep-alive" feature. The Parani-MSP1000 will send packets back and forth through the network periodically to confirm that the network exists. The corresponding TCP session is closed automatically if there's no response from the remote host.

To use the TCP "keep-alive" feature with the Parani-MSP1000, the users should configure three parameters as follows:

- **TCP keep-alive time:**

  This represents the time interval between the last data transmission and keep-alive packet submissions by the Parani-MSP1000. These "keep-alive" messages are sent to the remote host to confirm that the session is still open. The default time value is 15 sec.

- **TCP "keep-alive" probes:**

  This represents how many "keep-alive" probes will be sent to the remote host, until it decides that the connection is dead. Multiplied with the "TCP 'keep-alive' intervals", this gives the time that a link is forced to close after a "keep-alive" packet has been sent for the first time. The default is 3 times

- **TCP keep-alive intervals:**

  This represents the waiting period until a "keep-alive" packet is retransmitted. The default value is 5 seconds.

By default, the Parani-MSP1000 will send the keep-alive packets 3 times with 5 seconds interval after 15 seconds have elapsed since the time when there's no data transmitted back and forth.

Figure 3-5 TCP keep-alive configuration

4. Bluetooth Configuration

4.1. General properties

This menu describes configuration for the Bluetooth parameters of the Parani-MSP1000.

- **Bluetooth friendly name**

  "%h" inserts the host name configured in the Host name configuration. "%d" inserts the device id.

- **Discoverable (Inquiry scan)**

  When this is enabled, the Parani-MSP1000 is "discoverable."

- **Connectable (Page scan)**

  When this is enabled, the Parani-MSP1000 is "connectable to."

- **Authentication**

  When this is enabled, the Parani-MSP1000 requires pass key (PIN code) for incoming connections. If the pass key is incorrect, the connection will be rejected.

- **PIN code**

  This PIN code is applied for incoming and outgoing connections both.

- **Encryption**

  When this is enabled, the Parani-MSP1000 applies encryption to all Bluetooth connections.

- **Class of device**

  Specify the kind of device and type of available service on this device. The Class of device is composed three bytes (0xSSDDdd): Major Service Class (SS), Major Device Class (DD), Minor Device Class (dd).

  Major Service Class:

  Bit 1: Positioning (Location identification)

  Bit 2: Networking (LAN, Ad hoc, …)

  Bit 3: Rendering (Printing, Speaker, …)

  Bit 4: Capturing (Scanner, Microphone, …)

  Bit 5: Object Transfer (v-Inbox, v-Folder, …)

  Bit 6: Audio (Speaker, Microphone, Headset service, …)

  Bit 7: Telephony (Cordless telephony, Modem, Headset service, …)

  Bit 8: Information (WEB-server, WAP-server, …)

  Major Device Class:

  0x00: Miscellaneous

  0x01: Computer (desktop, notebook, PDA, organizer, …)

  0x02: Phone (cellular, cordless, payphone, modem, …)

  0x03: LAN / Network Access point

  0x04: Audio / Video (headset, speaker, stereo, video display, vcr, …)

0x05: Peripheral (mouse, joystick, keyboards, …)

0x06: Imaging (printing, scanner, camera, display, …)

Minor Device Class:

The meaning of this byte depends on the major class allocation, please refer to the Bluetooth specifications for more details.

● **Supervision timeout**

This is the timeout to presume disconnection. The smaller value becomes, the more quickly Parani-MSP1000 can detect an abnormal disconnection. But when the communication is suspended, it may be regarded as disconnection.(0 ~ 40 sec, infinite if value is 0)

● **Save link-key**

When this is enabled, the Parani-MSP1000 stores generated link-key at the flash memory.

● **Delete link-key**

The Parani-MSP1000 deletes stored link-key at the flash memory.

● **Specific pin code**

The Parani-MSP1000 can configure PIN code of a specific device.

● **Available Bluetooth devices**

The information of all the built-in Bluetooth devices is displayed.

Figure 4-1 Bluetooth General Properties

4.2. Operation mode

There are 3 types of mode, so users may have to select one for its own application.

4.2.1 AP mode

Bluetooth devices that supports PAN, DUN and LAP have the ability to access the LAN through the Parani-MSP1000.

4.2.2 Repeater mode

Parani-MSP1000 in Repeater mode can be used to function as a Repeater to expend the range of Bluetooth network or avoid obstacles between Parani-MSP1000 and Bluetooth devices.
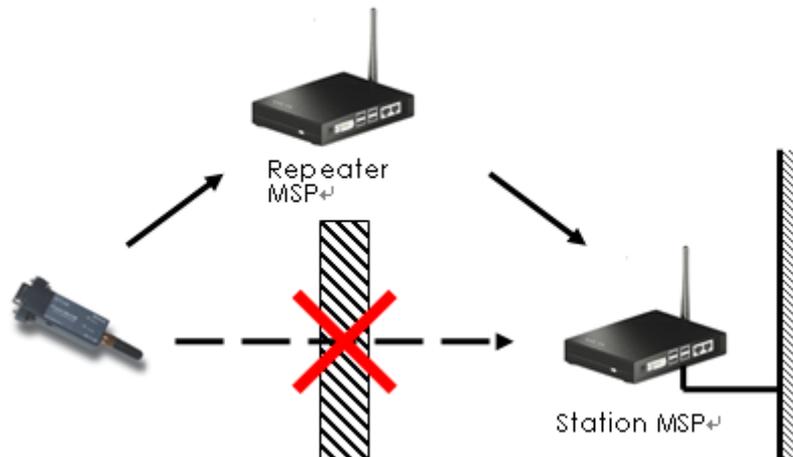

Figure 4- 2 Bluetooth communication using Repeater

To use the Repeater feature with the Parani-MSP1000, the users should configure four parameters as follows:

● **Station BD Address**
● **Local IP**
● **Netmask**
● **Gateway**

Figure 4- 3 Repeater mode configuration

4.2.3. Station mode

The Station transfers data from Repeater to outside. A Bluetooth module of Station can be connected from seven Repeaters. But Repeater-to-Repeater connection is not allowed.

4.3. AP service

The Parani-MSP1000 supports the Personal Area Network profile, Dial-up Network profile and LAN access over PPP profile. Bluetooth devices that supports PAN, DUN and LAP have the ability to access the LAN through the Parani-MSP1000.

Figure 4-4 Bluetooth AP Service

4.3.1. Private address

The Parani-MSP1000 uses private addresses for PAN, DUN and LAP connections. When using PAN, the Parani-MSP1000 assigns IP address via DHCP, and when using DUN and LAP, the Parani-MSP1000 assigns IP address via Internet Protocol Control Protocol (IPCP). Available private addresses are as follows:

- **10.0.0.0 ~ 10.255.255.255**

Table 4-1 Reserved Addresses in 10.x.x.x

10.0.0.1	Reserved for Parani-MSP1000
10.0.0.50 ~ 10.0.0.99	Reserved for PAN connections
10.0.0.100 ~ 10.0.0.200	Reserved for LAP & DUN connections

- **172.16.0.0 ~ 172.16.255.255**

Table 4-2 Reserved Addresses in 172.16.x.x

172.16.0.1	Reserved for Parani-MSP1000

172.16.0.50 ~ 172.16.0.99	Reserved for PAN connections
172.16.0.100 ~ 172.16.0.200	Reserved for LAP & DUN connections

● **192.168.0.1 ~ 192.168.0.255**

Table 4-3 Reserved Addresses in 192.168.0.x

192.168.0.1	Reserved for Parani-MSP1000
192.168.0.50 ~ 192.168.0.99	Reserved for PAN connections
192.168.0.100 ~ 192.168.0.200	Reserved for LAP & DUN connections

When Static IP addresses are required, the IP address should not be reserved.

4.3.2. Personal Area Networking (PAN)

● **Disable**

The Parani-MSP1000 stops the GN or NAP service.

● **Group ad-hoc Network (GN) Controller**

The Parani-MSP1000 forwards node in a peer-to-peer style network (Bluetooth Piconet).

● **Network Access Point (NAP)**

The Parani-MSP1000 acts as proxy, router or bridge between an existing network infrastructure (LAN) and Bluetooth clients.

4.3.3. Dial-Up Networking (DUN)

When this option is "Enable", the Parani-MSP1000 provides DUN profile for incoming Bluetooth connections.

4.3.4. LAN Access over PPP (LAP)

When this option is "Enable", the Parani-MSP1000 provides LAP profile for incoming Bluetooth connections.

4.3.5. Port forwarding

Port Forwarding is the technique of taking packets destined for a specific TCP of UDP port and machine. When the device that is connected to the Parani-MSP1000 via Bluetooth runs as a server such as Web server, FTP server, and Telnet server, the Parani-MSP1000 should redirect the packet to the device..

The Port forwarding configuration has four parameters as follows:

- **Local port**

  The source TCP or UDP port number

- **Remote IP**

  The destination IP address

- **Remote port**

  The destination TCP or UDP port number

- **Protocol**

  TCP or UDP

For example, when a device whose IP address is 172.16.0.10 runs as a Web server, the configuration should be as follows:

- **Local port:** 8080

  Any TCP port number except Telnet(23), SSH(22), HTTP(80) and HTTPS(443) port

  These ports are already used by the Parani-MSP1000 for configuration.

- **Remote IP:** 172.16.0.10

- **Remote port:** 80

- **Protocol:** TCP

4.4. FTP configuration

The Parani-MSP1000 provides FTP(File transfer profile) service. Mobile phones, PDA s and PCs are able to upload and download any file to/from the Parani-MSP1000.

- **FTP service**

  When this value is "Enable", the Parani-MSP1000 provides the FTP service.

- **Base directory**

  The directory for the FTP service. User space(2MB), ram(8MB) and cf-card are available. Please note that if the directory is "RAM", the files will be stored in the ram. The files will be removed when the Parani-MSP1000 restarts.

Figure 4- 5 Bluetooth FTP Configuration

4.5. Connections

The Bluetooth connections currently connected to the Parani-MSP1000 are displayed. Definitions and descriptions of each parameter are described as follows:

- **Inf**

  The Bluetooth interface

- **BD address**

  The remote BD address

- **Device name**

  The name of remote Bluetooth device

- **LM**

  The Link mode of the Parani-MSP1000. The "M" means Master and the "S" means "Slave"

- **RSSI & LQ**

  The RSSI and Link Quality (LQ) show the signal strength. The closer LQ is to 255 and RSSI is to 0, this means the Parani-MSP1000 has a good connection to the connected Bluetooth device. In general, the wireless connectivity is at its best within 10 meters

Connections

PAN connections

	No.	Inf	BD address	Device name	LM	RSSI	LQ
☐	1	hci-0	00:09:DD:50:4B:94	LEECOM2	M	3	253

LAP & DUN connections

	No.	Inf	BD address	Device name	LM	RSSI	LQ
☐	1	hci-1	00:09:DD:50:49:D2	JOKER	M	9	254

SPP connections

	No.	Inf	BD address	Device name	LM	RSSI	LQ
☐	1	hci-0	00:01:95:06:1E:EE	PSD100v1.1.0-061EEE	M	8	229

[Refresh] [Disconnect]

Figure 4- 6 Bluetooth Connections

5. Serial Port Profile (SPP) Configuration

The Bluetooth devices that support Serial Port Profile are able to create connections with the Parani-MSP1000, and are then able to send/receive data to/from remote host via TCP/IP.

5.1. Pairing mode

The operation mode option is as follows:

● **Disable**

The SPP service will be disabled.

● **Connector**

The Parani-MSP1000 scans nearby Bluetooth devices, and initiates connection to them. The Parani-MSP1000 doesn't accept any incoming connection.

● **Acceptor**

The Parani-MSP1000 accepts all incoming connections. The Parani-MSP1000 will not create any outgoing connections.

● **Custom**

The Parani-MSP1000 will only communicate with the registered Bluetooth devices. The user should set up the BD addresses of the Bluetooth devices and each paring mode.

Figure 5-1 Pairing mode

5.2. Pairing mode - Connector

The Parani-MSP1000 scans nearby Bluetooth devices with an interval, and tries to create connection to them. The configurable parameters are as follows:

- **Scan interval**

  The Parani-MSP1000 scans neighborhood Bluetooth devices with this interval (in seconds). This value means the time required for the Parani-MSP1000 to recognize a new device.

  Note: *Too short interval may make the data rate slow.*

- **Scan mode**

  Parani-MSP1000 scans with IAC or Bluetooth friendly name.

- **Inquiry access code (IAC)**

  The Parani-MSP1000 scans nearby Bluetooth devices with this IAC. The IAC should be in range from 9e8b00 to 9e8b3f (in hexadecimal). Most of Bluetooth devices are set up as generic IAC (9e8b33). To connect to the devices, the IAC should be generic IAC. However, when the IAC is generic, it is possible the Parani-MSP1000 finds too many Bluetooth devices to connect. If then, it is efficient to use limited IAC or user-defined IAC. To use non-generic IAC, the IAC of Bluetooth device to which the Parani-MSP1000 connect should also be changed.

- **Remote device name**

  The Parani-MSP1000 attempts to connect to the devices whose name start with the configured name.

5.3. Pairing mode - Acceptor

The Parani-MSP1000 accepts all incoming connections.

5.4. Pairing mode - Custom

The Parani-MSP1000 communicates with only the registered Bluetooth devices. When using this mode, the detail configuration is prepared in the Port configuration. Please, refer to *5.5 Port configuration.*

5.5. Port configuration

The Port configuration has different submenus according to the Pairing mode. The Port pairing mode menu and Logging menu are prepared only when the Pairing mode is "Custom".

Figure 5-2 Port configuration

5.5.1. Port pairing mode (Custom mode only)

If the mode is "Acceptor", the Parani-MSP1000 waits for incoming connection from the Bluetooth device. If the mode is "Connector", the Parani-MSP1000 attempts to connect the Bluetooth device.

5.5.2. Service category - CLI

When a new connection is created, the Parani-MSP1000 provides a CLI for the connection. With this option, system administrators are able to access to CLI without the use of a serial cable.

Figure 5-3 Service category - CLI

5.5.3. Service category - Network

When a new Bluetooth connection is created, the Parani-MSP1000 starts the registered network service. If the network service is client, the Parani-MSP1000 creates an outgoing connection and if the network service is server, the Parani-MSP1000 listen on a TCP port. And then, if TCP connection is established, the data received from SPP is transmitted to TCP/IP and the data received from TCP/IP is transmitted to SPP. If there are more than one registered network service, each network service operates independently.

Figure 5-4 Service category - Network

5.5.4. Service category – Serial hub

In Serial hub mode, Parani-MSP1000 relays data communications between Bluetooth devices. With Parani-SD only 1:1 cable replacement is possible, however, incorporating Parani-MSP1000 multiple Parani-SDs can communicate each other, 1:N multi-serial with Parani_SD.

Note: The serial hub mode is supported only when the Pairing mode is "Custom"
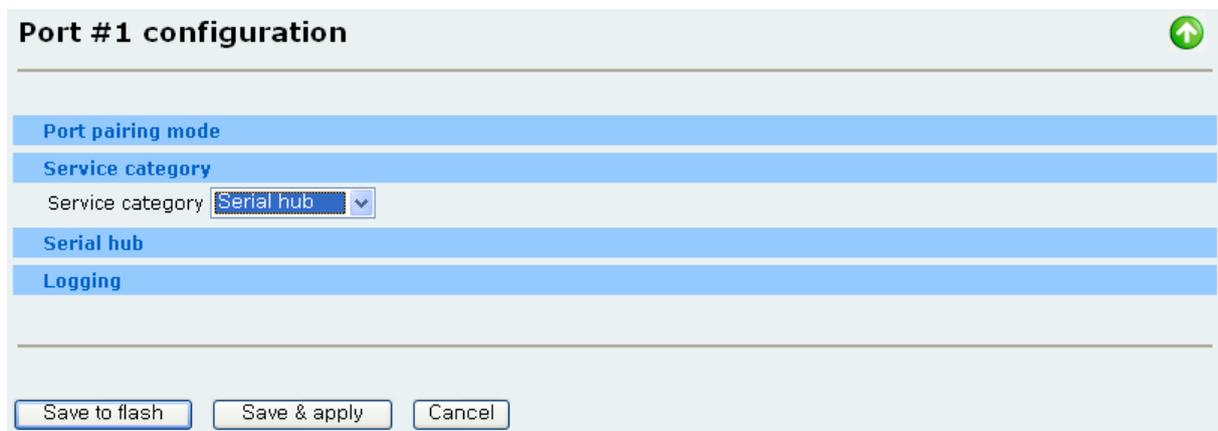

Figure 5- 5 Service category – Serial hub

5.5.5. Frame buffer

The available options are as follows:

● **Disable**

The frame buffer functionality is disabled. The Parani-MSP1000 sends the data received from SPP to remote hosts as soon as possible.

● **Fixed size**

The Parani-MSP1000 waits until the received data size is the configured fixed size.

- **Timeout**

  The Parani-MSP1000 waits until the received data size is the configured fixed size or the timer is expired. If the timeout is zero, it means unlimited.

- **Delimiter**

  The Parani-MSP1000 waits until the configured delimiter is arrived, the received data size is the configured fixed size or the timer is expired. If the timeout is zero, it means unlimited.

- **STX + data + ETX**

  The Parani-MSP1000 waits until a frame composed of STX + data and ending in an ETX, the received data size is the configured fixed size or the timer has expired. If the timeout is zero, it means unlimited.

- **STX + data + ETX + wildcard-characters**

  The Parani-MSP1000 waits until a frame composed of STX, data, ETX and some wildcard-characters is arrived, the received data size is the configured fixed size or the timer is expired. If the timeout is zero, it means unlimited.

Figure 5-6 Frame buffer configuration

5.5.6. Network service

The available options are as follows:

- **Network service mode**

  The available modes are server, client, tunneling and vertex. If the server is selected, the Parani-MSP1000 waits for an incoming connection. If the client is selected, the Parani-MSP1000 tries to connect to the pre-defined remote host. The tunneling mode is a mixed mode of server and client. The Parani-MSP1000 waits for incoming connection, but when there is data received from SPP and the incoming connection is not established yet, the Parani-MSP1000 tries to connect to

remote host like the client mode. In vertex mode, data from a host are sent to all of connected Bluetooth devices.

Figure 5-7 Server mode

Figure 5-8 Client mode

Figure 5-9 Tunneling mode

Figure 5-10 Vertex mode

- **Service protocol**

  When the network service mode is server or client, the available protocols are RawTCP, SSL, Telnet and SSH. When the network service mode is tunneling, the available protocols are RawTCP, SSL.

- **Inactivity timeout**

  If there is no data for the configured inactivity timeout, the network session will be terminated.

- **Local port number / Base port number**

  When the network service mode is server or tunneling, a TCP port number is required for incoming connection. When the Pairing mode is "Custom", the user should set up the local port number for each SPP connection. When the Pairing mode is "Acceptor" or "Connector", it is impossible to configure the local port number for each SPP connection because the SPP connections are dynamic. In this case, the Parani-MSP1000 allocates a TCP port number based on the Base port number. The allocated port number will be within the range from the Base port number to Base port number + 27.

  Note: Please, avoid the duplication of the TCP port number. If possible, do not use the well known ports. When setting up the Base port number, range from the Base port number to the Base port number + 27 must not be overlapped with other network services.

- **Authentication**

  When the network service mode is server, the Parani-MSP1000 requires the incoming connection to login. The user account for login should be registered in User management.

- **Users allowed to access**

  The only users registered in this option are able to login the network service.

- **Primary/Secondary remote host & port**

  When the network service mode is client or tunneling, the Parani-MSP1000 attempts to connect to these hosts.

- **Username & Password**

  When the network service mode is client and the remote hosts require the Parani-MSP1000 to login, the Parani-MSP1000 logins with this account. If the username or password is not configured, the Parani-MSP1000 doesn't try to login.

● **Periodic connection**

When the network service mode is client, the Parani-MSP1000 attempts to create an outgoing connection with this interval. If the periodic connection is zero, it means that the Parani-MSP1000 never initiates connection when there is no data received from SPP.

● **When Bluetooth connection is established: Initiate connection or Do nothing**

If the "Initiate connection" is selected, the Parani-MSP1000 attempts to connect to remote host immediately when Bluetooth connection is established. However, If the "Do nothing" is selected, the Parani-MSP1000 waits until data is arrived from SPP.

● **Vertex port**

It is a TCP port to communicate with Bluetooth devices. The user can select one of some vertex ports.

5.5.7. Logging (Custom mode only)

If the Pairing mode (not port pairing mode) is "Custom", the logging functionality is available. The configurable parameters are as follows:

● **Activation**

When this is "enable," the Parani-MSP1000 starts logging the data sent/received to/from the SPP connection.

● **Log location**

The data is able to be logged to memory or CF memory (when a CF memory is plugged). The logged data is saved to a file whose name is "*portlogs/the_BD_address.log*"

● **Data stream to be logged**

● **Logging mode**

If the data is composed of only readable text (not including binary codes), select "Text." If the data includes binary codes, select "Pure binary" or "Readable binary." When the logging mode is "Readable binary," the Parani-MSP1000 converts the binary data to text data and save it.

● **Reduce the port log file [Time to reduce the log data] to [Log buffer size]**

The system log should be reduced because the internal memory for system log is limited. The Parani-MSP1000 has a 16 Megabytes memory for system log and port log. If the internal memory is full, the system log will not be recorded anymore.

Table 5-1 The time to Reduce logged data

Every month	First day of every month 00:00:00 AM
Every week	Every Sunday 00:00:00 AM
Every day	Every day 00:00:00 AM
Every hour	Every hour 0 minute 0 second exactly
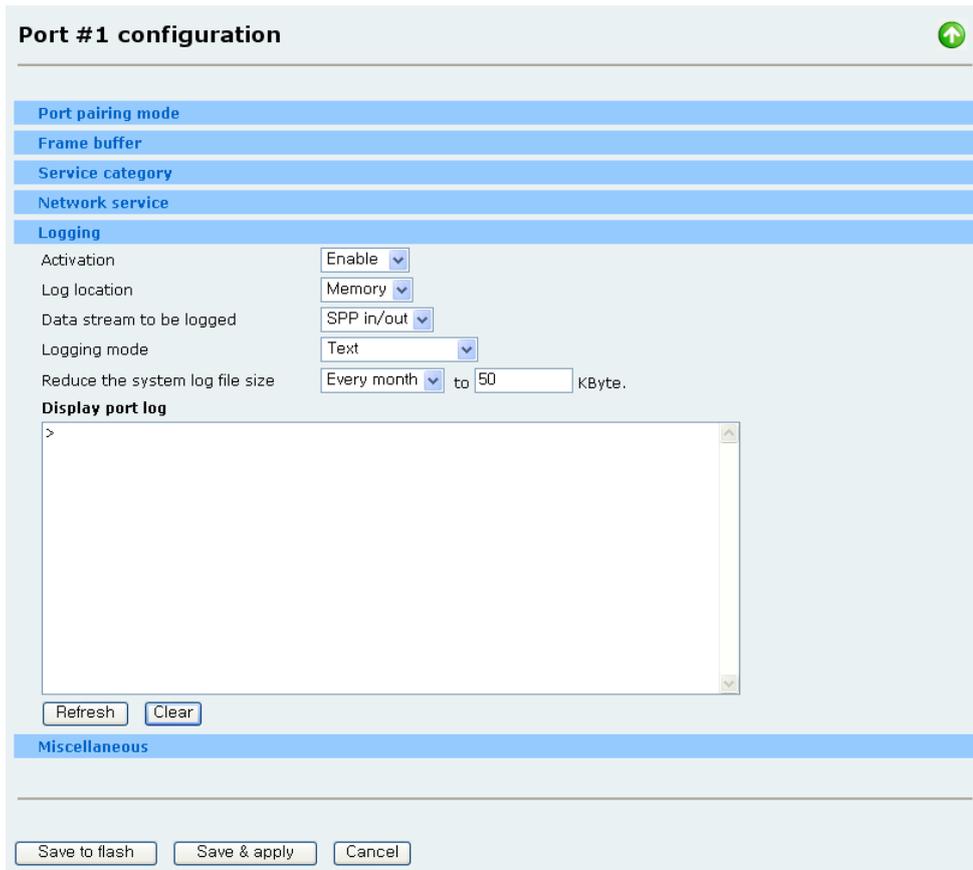
Figure 5-11 Port Logging mode

5.5.8. Serial hub

The serial hub mode is supported only when the Pairing mode is "Custom". This field shows BD address of connectable Bluetooth devices, so the user can select some devices.
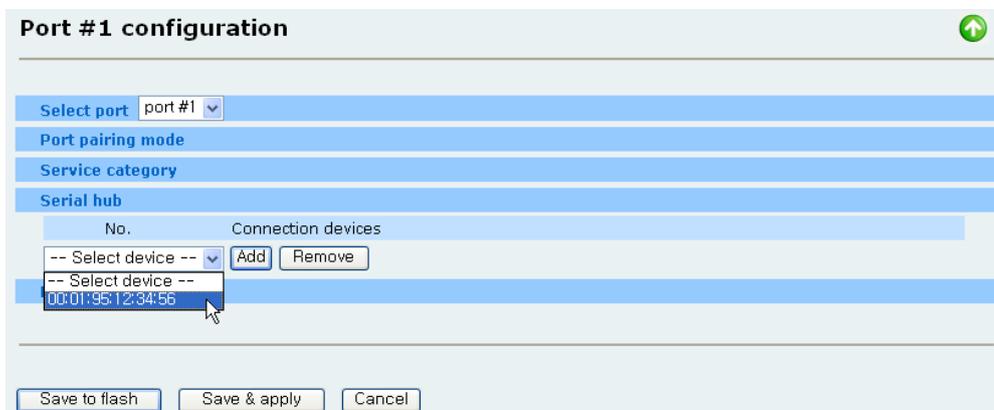
Figure 5-12 Serial hub configuration

5.5.9. Miscellaneous

● **7-bit data emulation**

This option is useful in using with the Parani-SD Series or the Parani-ESD Series. The Parani-SD/ESD Series do not support 7-data-bits. The Parani-MSP1000 emulates 7-data-bits instead of the Parani-SD/ESD Series.

Note: In order to use 7-bit data emulation, the serial device connected to the Parani-SD/ESD should support Odd, Even or Space parity (while the Parani-SD/ESD is set to No Parity). The 7-bit data emulation option cannot be used with non-parity.
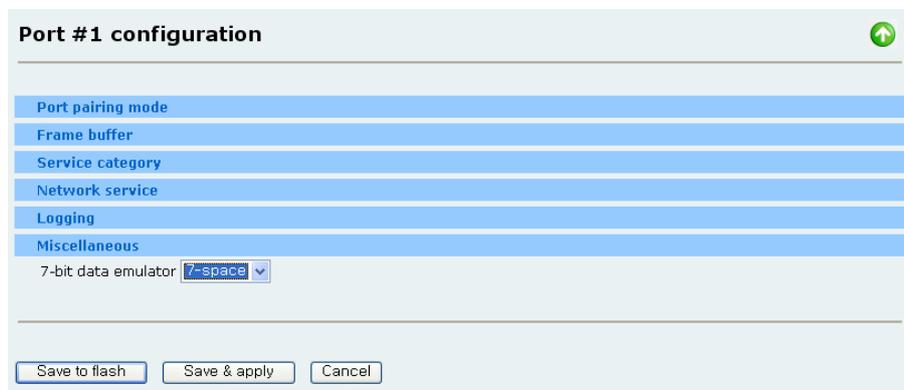
Figure 5-13 Miscellaneous setting

5.6. Vertex configuration

It is a configuration to send the date delivered from a host to all of connected Bluetooth devices. The configurable parameters are as follows:

● **Vertex port**

This is a TCP port to communicate with Bluetooth devices.

● **Inactivity timeout**

If there is no data for the configured inactivity timeout, the network session will be terminated.
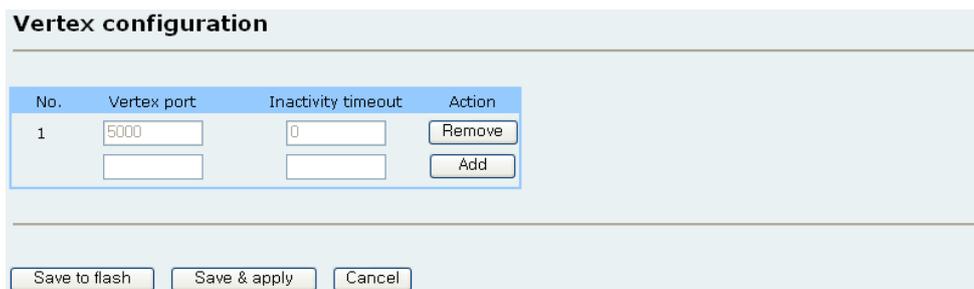
Figure 5- 14 Vertex configuration

5.7. Connections

The SPP connections currently connected to the Parani-MSP1000 are displayed. Definitions and descriptions of each parameter are described as follows:

- **Inf**

  The Bluetooth interface

- **BD address**

  The remote BD address

- **Service description**

  The network service linked with the SPP connection is displayed.

Figure 5-15 SPP connections

5.8. Monitoring (Sniffing)

The Parani-MSP1000 supports port monitoring (sniffing) functionality for debugging and installation. The port monitoring enables the user to sniff the data received/sent from/to SPP.

To access the port monitoring:

1) Access the console management via Telnet or SSH
2) Select the Monitoring menu, SPP connections and the connection to sniff

```
--------------------------------------------------------------------------------
Welcome to MSP1000 configuration page
Current Time   : 8/26/2007 06:55:14   Serial No.     : MSP1000-00001
F/W Rev.       : v1.0.0               MAC Addr.(eth0) : 00:01:95:AF:BE:11
IP Mode (eth0) : Static               IP Addr.(eth0)  : 192.168.11.30
--------------------------------------------------------------------------------
1. Network configuration
2. System administration
3. System status & log
4. CF card configuration
5. Monitoring
6. Save changes
7. Exit without saving
8. Exit and apply changes
9. Exit and reboot
 <ESC> Back, <ENTER> Refresh
--> 5
--------------------------------------------------------------------------------
Welcome to MSP1000 monitoring menu
```

```
 Current time    : 07/28/0107 16:03:36   Serial No.      : msp1000-test-2
 F/W Rev.        : v0.0.1_0827_1         MAC Addr.(eth0) : 00:01:95:AF:BE:11
 IP Mode (eth0) : Static IP              IP Addr. (eth0) : 192.168.11.30
 ----------------------------------------------------------------------------
 1. System status
 2. Bluetooth neighborhoods
 3. PAN connections
 4. LAP & DUN connections
 5. SPP connections
 6. TCP connections
  <Enter> Refresh
 ---> 5
 ----------------------------------------------------------------------------
 SPP connections
 ----------------------------------------------------------------------------
 No.  BD address          Device name          LM    RSSI   LQ
  1.  00:01:95:06:7C:4A   PSD200v2.0.0-067C4A   M     0      214
  2.  00:01:95:05:CB:DF   PSD100v1.1.0-05CBDF   M     0      214
  Enter a command, available commands are as follows:
    dc [index] - disconnect the connection
 ---> 2
    Select data stream to monitor:
       1. SPP ---> TCP
       2. SPP <--- TCP
       3. SPP <--> TCP
    ---> 3
    Select monitoring mode:
       1. Text
       2. Binary
    ---> 2
    Press 'Q', to exit
    Press SPACE, to stop
    Press ESC, to menu
 <16:04:30, SPP -> TCP>
 0000h: 61 73 64 73 61 64 73 61 64 73 64 61 73 61 64   ; asdsadsadsdasad

 <16:04:30, SPP <- TCP>
 0000h: 61 73 64 73 61 64 73 61 64 73 64 61 73 61 64   ; asdsadsadsdasad
```

Note: *The configuration menu via serial port doesn't support port monitoring because the data rate of serial port is too slow to sniff the Bluetooth data.*

6. CF card Configuration

The Parani-MSP1000 has a CF card slot for increased expandability. It supports two types of PC cards:

-   ATA/IDE fixed disk card
-   Modem card

The ATA/IDE fixed disk card allows the user the ability to store and carry system and SPP data logs. Using the card slot for a modem cards allows the users can make an out-of-band access to the Parani-MSP1000 without occupying one a serial port with an to connect to an external modem.

6.1. When using an ATA/IDE fixed disk card

After inserting an ATA/IDE fixed disk card, select the "Probe" button. If the card is not formatted, select the "Format" button and select the "Probe" button again. The Parani-MSP1000 supports EXT2, ETX3 and VFAT file system for the disk card.
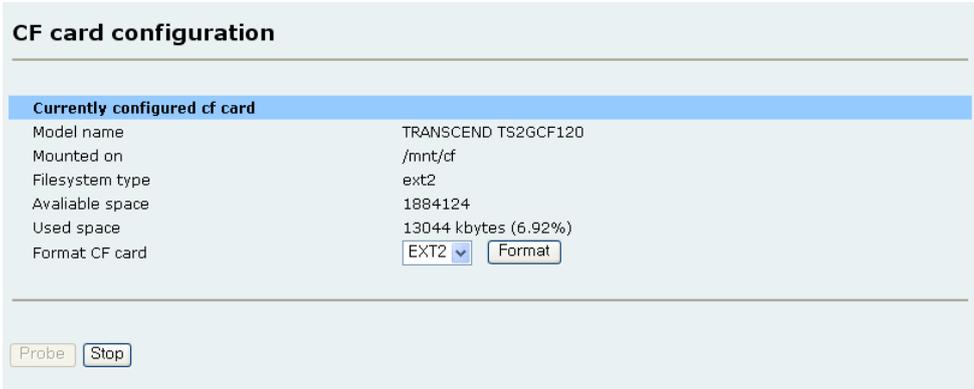
Figure 6-1 ATA/IDE fixed disk card configuration

6.2 Serial modem card configuration

The user can access to the Parani-MSP1000 via serial modem. The user can configure User name, Password, Authentication method, Remote / Local IP as shown in Figure 6-2.

Figure 6- 2 Modem card configuration

7. System administration

7.1. Host name

The Parani-MSP1000 has its own name for administrative purposes.

Figure 7-1 Host name configuration

7.2. User management

The Parani-MSP1000 utilizes user profile types to manage accessibility to different functions. There three levels of user types include: root, admin and user.

The root and admin group has full read/write access of the Parani-MSP1000 configuration. The difference between root and admin is that the root is able to access the shell but the admin group isn't. The user group has no right to modify any of the Parani-MSP1000 configurations and only change their respective passwords.

The factory default user names and the passwords are:

System Super User

Login: **root**   Password: **root**

System Administrator

Login: **admin**   Password: **admin**.
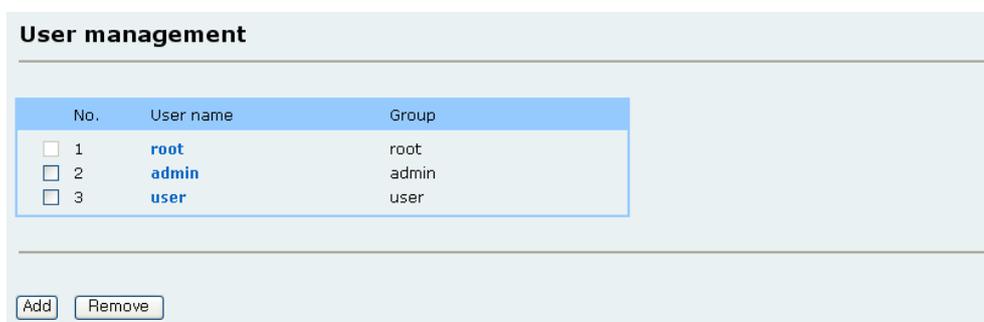
Figure 7-2 User management

7.2.1. Adding a new user

In order to add a new user:

1. Select "Add" button.
2. Enter the username (user id)
3. Choose the user group between admin and user.
4. Select "Submit" button.

Note: Adding a new root user is not allowed.

7.2.2. Removing a user

In order to remove an existing user:

1. Check the checkbox at the front of the user to be removed.
2. Select "Remove" button.

Note: Removing the root user is not allowed.

7.2.3. Editing a user

In order to modify an existing user:

1. Select the username (user ID).
2. Modify the username, the group or the password.
3. Select "Submit" button.

7.3. Security

The Parani-MSP1000 uses SSL and TLS protocol for Web configuration (HTTPS) and network service of the SPP. The SSL and TLS are based on the certificate, private key and the certificates of trusted CAs. The Parani-MSP1000 provides a way to replace the certificates.
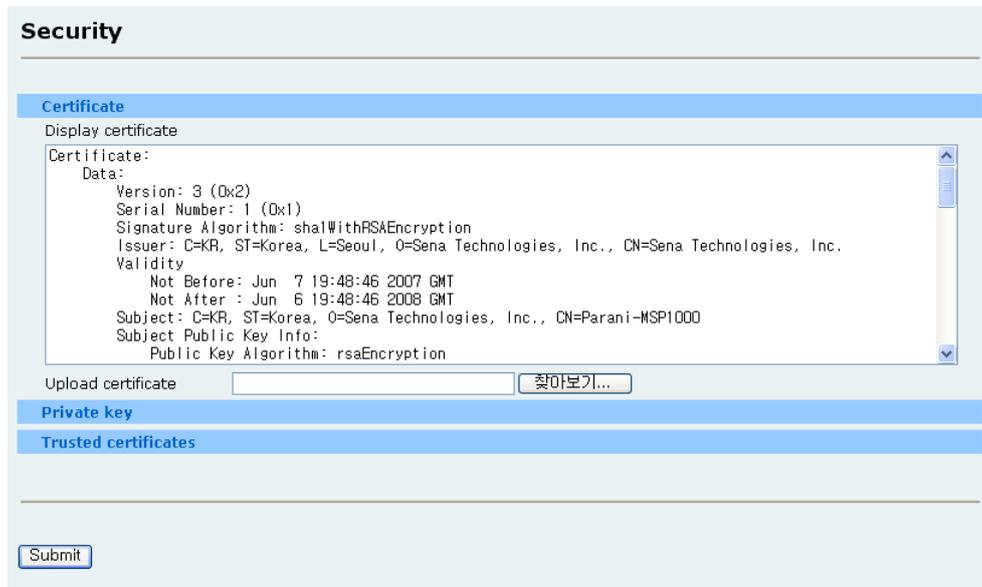
Figure 7-3 Security configuration

7.3.1. Changing certificate

The Parani-MSP1000 supports .PEM format for certificate.

In order to change the certificate (for this Parani-MSP1000)

1. Select Certificate menu
2. Select the certificate file
3. Select "Submit" button.

7.3.2. Changing private key

The Parani-MSP1000 supports .PEM format for private key. The private key must be a pair of the certificate that is uploaded in the Certificate menu. If the private key is encrypted, the passphrase that is required in decrypting the private key must be configured.

In order to change the private key (for this Parani-MSP1000)

1. Select Private key menu
2. Select the Private key file
3. Enter the passphrase (optional)
4. Select "Submit" button.

7.3.3. Uploading a new Trusted CA certificate

The Parani-MSP1000 supports .PEM format for certificate. When the Parani-MSP1000 connects to a SSL or TLS server, the Parani-MSP1000 requires the certificate of the CA that issues the certificate of the SSL or TLS server. If the Parani-MSP1000 fails in finding the certificate, the SSL connection will

not be established.

In order to upload a new certificate of trusted CA:

    1.   Select Certificates of Trusted CA menu

    2.   Select the certificate file of CA

    3.   Select "Submit" button.

Note: If there is already the same name of file, rename the certificate. The name of file doesn't affect the certificate.

7.3.4. Removing a Trusted CA certificate

In order to remove an existing certificate of trusted CA:

    1.   Check the checkbox at front of the CA.

    2.   Select "Remove" button.

7.4. Date and Time

The Parani-MSP1000 maintains current date and time information. The Parani-MSP1000 clock and calendar settings are backed up by internal battery power. The user can change the current date and time.

Figure 7-4 Date and time configuration

There are two date and time settings. The first is to use the NTP server to maintain the date and time settings. If the NTP feature is enabled, the Parani-MSP1000 will obtain the date and time information from the NTP server at each reboot. If the NTP server is set to 0.0.0.0, the Parani-MSP1000 will use the default NTP servers. In this case, the Parani-MSP1000 should be connected from the network to the Internet. The second method is to set date and time manually without using the NTP server. This

will allow the date and time information to be kept maintained by the internal battery backup.

The user may also need to set the timezone and the time offset from UTC depending on the users' location. If the user uses daylight saving time, the user may also need to set the daylight saving time properties such as; the daylight saving timezone, the time offset from UTC, start data and time, end date and time.

7.5. Configuration management

The user may export the current configurations to a file at such locations as CF card, user space or local machine and import the exported configurations as current configurations from CF card, user space or local machine.

The users may restore the factory default settings at any time by selecting "Factory default" at the location property or by pushing the hardware factory default reset switch on the back panel of the Parani-MSP1000.

The following parameters should be properly set up in order to export / import configurations as follows:

Configuration export
> **Location :** Location to export to.
> **Encrypt :** One of **Yes or No**.
> **File name**

Configuration import
> **Location :** Location to import from. By selecting **Factory default**, the user may restore the factory settings.
> **Configuration selection :** Determines what kinds of configurations are imported.
> **Encrypt : Yes or No**.
> **File selection :** List all the exported files satisfying the encrypting option at the selected location which is one of CF card and user space.
> **Local :** Helps to browse the exported file at local machine if location is local machine.

> To export the current configurations:
> 1. Select the location to export to.
> 2. Select the encrypting option
> 3. Type the file name.

4. Click the [Export] button.
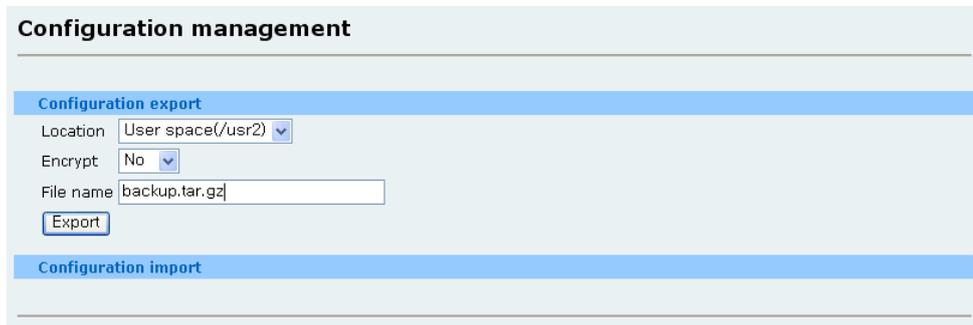
Figure 7-5 Configuration export

To import the exported configurations:
1. Select the location to import from.
2. Select the configurations to import.
3. Select the encrypting option.
4. Select the file to import from the file selection list box if location is neither local machine nor factory default.
5. Select the file to import by clicking browse button if location is local machine.
6. Click the [Import] button.

Figure 7-6 Configuration import

7.6. Firmware upgrade

Firmware upgrades are available via serial, remote console or web interface. The latest upgrades are available on the Sena web site at http://www.sena.com/support/downloads/.

7.6.1 Manual firmware upgrade

To upgrade firmware via the web:

1. Select the latest firmware binary by clicking browse button.
2. Select and upload the selected version.
3. Once the upgrade has been completed, the system will reboot to apply the changes.

Figure 7-7 Firmware upgrade

To use either a remote or serial console to upgrade your firmware, the TELENT/SSH or terminal emulation program must support Zmodem transfer protocol. The previous settings will be retained after the firmware upgrade.

To upgrade firmware via a remote console:

1. Obtain the latest firmware.
2. Connect the terminal emulation program using either TELENT/SSH or a serial console port.
   (TELNET or SSH is recommended since the process of firmware upgrade by serial console requires extremely long time.)
3. Select from the firmware upgrade menu as shown in

```
--------------------------------------------------------------------------------
Welcome to MSP1000 configuration page
Current Time  : 8/26/2007 06:55:14   Serial No.     : MSP1000-00001
F/W Rev.      : v1.0.0               MAC Addr.(eth0) : 00:01:95:AF:BE:11
IP Mode (eth0) : Static              IP Addr.(eth0)  : 192.168.11.30
--------------------------------------------------------------------------------
1. Network configuration
2. System administration
3. System status & log
4. CF card configuration
5. Monitoring
6. Save changes
7. Exit without saving
8. Exit and apply changes
9. Exit and reboot
 <ESC> Back, <ENTER> Refresh
--> 2
```

```
--------------------------------------------------------------------------------
  System administrator
--------------------------------------------------------------------------------
1. Device name: MSP1000
2. User management
3. Security
4. Date and Time
5. Configuration management
6. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
--> 6
waiting to receive.**B0100000023be50
```

4. Follow the online directions and transfer the firmware binary file using the Zmodem protocol.

5. Once the upgrade has been completed, the system will reboot to apply the changes

6. *If the firmware upgrade fails, the Parani-MSP1000 will display an error messages. It will also maintain the current firmware version.*

```
--------------------------------------------------------------------------------
Welcome to MSP1000 configuration page
Current Time  : 8/26/2007 06:55:14   Serial No.     : MSP1000-00001
F/W Rev.       : v1.0.0              MAC Addr.(eth0) : 00:01:95:AF:BE:11
IP Mode (eth0) : Static              IP Addr.(eth0)  : 192.168.11.30
--------------------------------------------------------------------------------
1. Network configuration
2. System administration
3. System status & log
4. CF card configuration
5. Monitoring
6. Save changes
7. Exit without saving
8. Exit and apply changes
9. Exit and reboot
 <ESC> Back, <ENTER> Refresh
--> 2
--------------------------------------------------------------------------------
  System administrator
--------------------------------------------------------------------------------
1. Device name: MSP1000
2. User management
3. Security
4. Date and Time
5. Configuration management
6. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
--> 6
waiting to receive.**B0100000023be50
```

7.6.2. Automatic firmware upgrade

To use the function to upgrade the firmware and configuration or to upload a user file or to run a user command at boot time, users have to set the following properties:

- **Automatic firmware and configuration upgrade at boot time**

  It determines whether the Parani-MSP1000 upgrade at boot time or not.

- **Protocol**

  It determines which protocol the Parani-MSP1000 uses to communicate with the remote host on upgrading.

- **IP address of remote server**

  It determines to which host the Parani-MSP1000 connects to get the hash file, firmware image and configuration file.

- **Hash file name**

  It determines the name of hash file that is used to specify the firmware image file and configuration file to upgrade. The Parani-MSP1000 checks if the Parani-MSP1000 needs to upgrade or not by comparing the version at hash file with the Parani-MSP1000 firmware version. Hash file format is below:

  ① Firmware upgrade : <TYPE>,<NAME>,<VERSION>

      <TYPE> - 1

      <NAME> - the name of firmware image.

      <VERSION> - the version of firmware

  ② Configuration upgrade : <TYPE>,<NAME>,<OPTION>,<VERSION>

      <TYPE> - 2

      <NAME> - the name of configuration file

      <OPTION> - [E][N]

          E : Encrypted configuration file

          N : Non-encrypted configuration file

      <VERSION> : the version of configuration file

  ③ User file upload : <TYPE>,<NAME>,<OPTION>,<PATH>

      <TYPE> - 3

      <NAME> - the name of target file

      <OPTION> - [F][X][Z]

          F : forced copy (remove if there is same file already)

          X : uncompress the file to the specified location

          Z : unzip the file to the specified location

      <PATH> - Directory path where the specified file will be uploaded

  ④ User command run : <TYPE>,<COMMAND>

      <TYPE> - 4

      <COMMAND> - command to run

Hash file example is below:

```
1,msp1000.img,v1.0.0
2,conf.enc,E,v1.0.0
3,userfile.tar.gz,FXZ,/mnt/ram
4,mkdir /mnt/ram/testdir
```


Figure 7- 8 Automatic firmware upgrade

7.7. Change password

To change the current user's password, type the current password, a new password and confirm the new password and then click the "Submit" button.

Figure 7-9 Change password

8. System status & log

8.1. System status

The Parani-MSP1000 displays the system status. This screen is used for management purposes. System status data includes the model name, serial number, firmware version and the network configuration of the Parani-MSP1000.
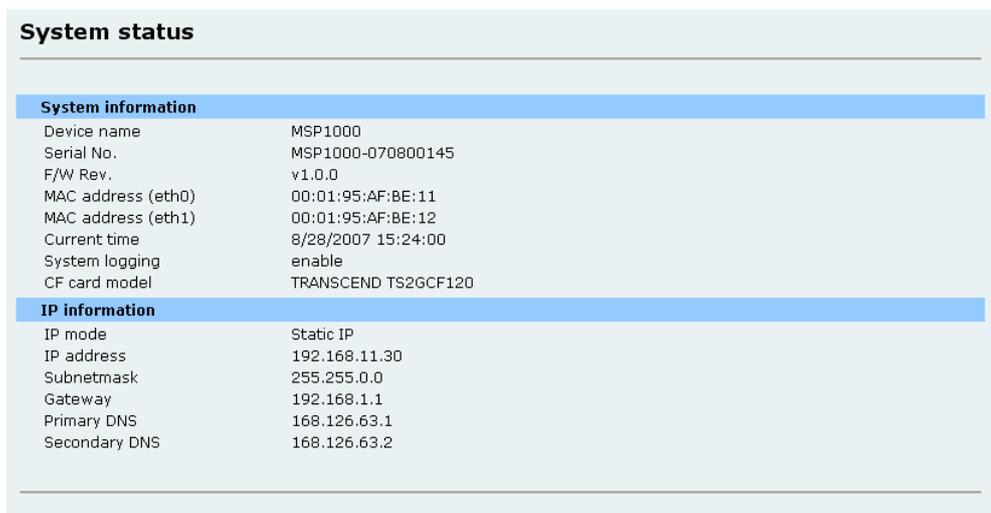
System status

System information
Device name	MSP1000
Serial No.	MSP1000-070800145
F/W Rev.	v1.0.0
MAC address (eth0)	00:01:95:AF:BE:11
MAC address (eth1)	00:01:95:AF:BE:12
Current time	8/28/2007 15:24:00
System logging	enable
CF card model	TRANSCEND TS2GCF120

IP information
IP mode	Static IP
IP address	192.168.11.30
Subnetmask	255.255.0.0
Gateway	192.168.1.1
Primary DNS	168.126.63.1
Secondary DNS	168.126.63.2

Figure 8-1 System status

8.2. System logging

The Parani-MSP1000 provides the system logging feature as well as the system status display. The users can configure the Parani-MSP1000 to enable or disable the system logging process and select the system log buffer size and the log storage location.

- **Enable/Disable**

    This parameter defines whether to use system logging.

- **Log location**

    The system log can be stored to in the **Parani-MSP1000 internal memory,** the **ATA/IDE fixed disk card** inserted in CF slot or remote SYSLOG server. If the internal memory is used to store system log data, the log data will be cleared when the Parani-MSP1000 is turned off. To preserve the system log data, set the storage location to be the ATA/IDE fixed disk card or SYSLOG server.

- **SYSLOG server name & log facility**

    The Parani-MSP1000 supports the use of a remote message logging service, SYSLOG service for the system. To use the remote SYSLOG service, the user must specify the SYSLOG server's

IP address and the facility to be used.

To receive log messages from the Parani-MSP1000, the SYSLOG server must be configured as "remote reception allowed". If there is a firewall between the Parani-MSP1000 and the SYSLOG server, there must be a rule that allows all outgoing and incoming UDP packets to travel across the firewall.

The Parani-MSP1000 supports SYSLOG facilities from `local0` to `local7`. The user can employ these facilities to save messages from the Parani-MSP1000 separately in the SYSLOG server.

● **Reduce system log (Time to reduce the log data) to (system log size)**
The system log should be reduced because the internal memory for system log is limited. The Parani-MSP1000 has a 16 Megabytes memory for system log and port log. If the internal memory is full, the system log will not be recorded anymore.

Table 8-1 The time to Reduce logged data

Every month	First day of every month 00:00:00 AM
Every week	Every Sunday 00:00:00 AM
Every day	Every day 00:00:00 AM
Every hour	Every hour 0 minute 0 second exactly
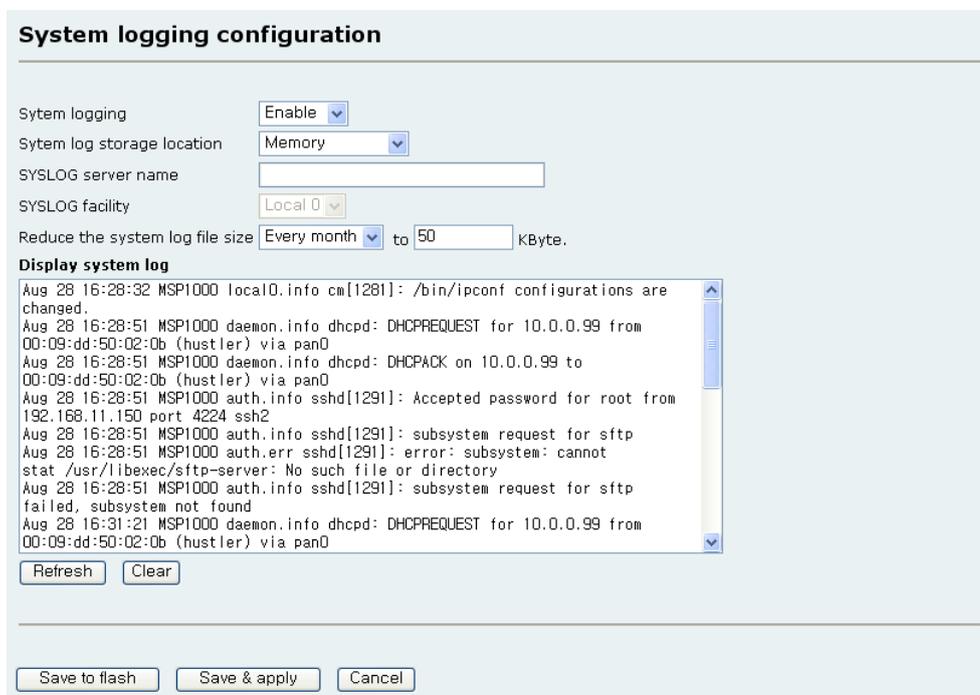
Figure 8-2 System logging configuration

9. System statistics

9.1. Network interfaces

Network interfaces statistics displays basic network interfaces usage of the Parani-MSP1000, **lo, eth0** and **eth1. lo** is a local loop back interface and **eth0** and **eth1** are network interfaces of Parani-MSP1000.

Network interfaces statistics

Interface		lo	eth0	eth1
Receive	Bytes	98774	3680903	0
	Packets	3406	37254	0
	Errors	0	0	0
	Drop	0	0	0
	FIFO	0	0	0
	Frame	0	0	0
	Compressed	0	0	0
	Multicast	0	0	0
Transmit	Bytes	98774	881231	2944358
	Packets	3406	7422	33348
	Errors	0	0	0
	Drop	0	0	0
	FIFO	0	0	0
	Frame	0	0	0
	Compressed	0	0	0
	Multicast	0	0	0

Figure 9-1 Network interfaces statistics

9.2. IP

The IP Statistics screen provides statistical information about packets/connections using an IP protocol. Definitions and descriptions of each parameter are described below:

Forwarding :

Specifies whether IP forwarding is enabled or disabled.

DefaultTTL :

Specifies the default initial time to live (TTL) for datagrams originating on a particular computer.

InReceives :

Shows the number of datagrams received.

InHdrErrors :

Shows the number of datagrams received that have header errors. Datagrams Received Header Errors is the number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

InAddrErrors :

Specifies the number of datagrams received that have address errors. These datagrams are

discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E).

ForwDatagrams :

Specifies the number of datagrams forwarded.

InUnknownProtos :

Specifies the number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

InDiscard :

Specifies the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This count does not include any datagrams discarded while awaiting reassembly.

InDelivers :

Specifies the number of received datagrams delivered.

OutRequests :

Specifies the number of outgoing datagrams that an IP is requested to transmit. This number does not include forwarded datagrams.

OutDiscards :

Specifies the number of transmitted datagrams discarded. These are datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space.) This count would include datagrams counted in Datagrams Forwarded if any such packets met this (discretionary) discard criterion.

OutNoRoutes :

Specifies the number of datagrams for which no route could be found to transmit them to the destination IP address. These datagrams were discarded. This count includes any packets counted in Datagrams Forwarded that meet this "no route" criterion.

ReasmTimeout :

Specifies the amount of time allowed for all pieces of a fragmented datagram to arrive. If all pieces do not arrive within this time, the datagram is discarded.

ReasmReqds :

Specifies the number of datagrams that require reassembly.

ReasmOKs :

Specifies the number of datagrams that were successfully reassembled.

ReasmFails :

Specifies the number of datagrams that cannot be reassembled.

FragOKs :

Specifies the number of datagrams that were fragmented successfully.

FragFails :

Specifies the number of datagrams that need to be fragmented but couldn't be because the IP header specifies no fragmentation. For example, if the datagrams "Don't Fragment" flag was set, the datagram would not be fragmented. These datagrams are discarded.

FragCreates :

Specifies the number of fragments created.
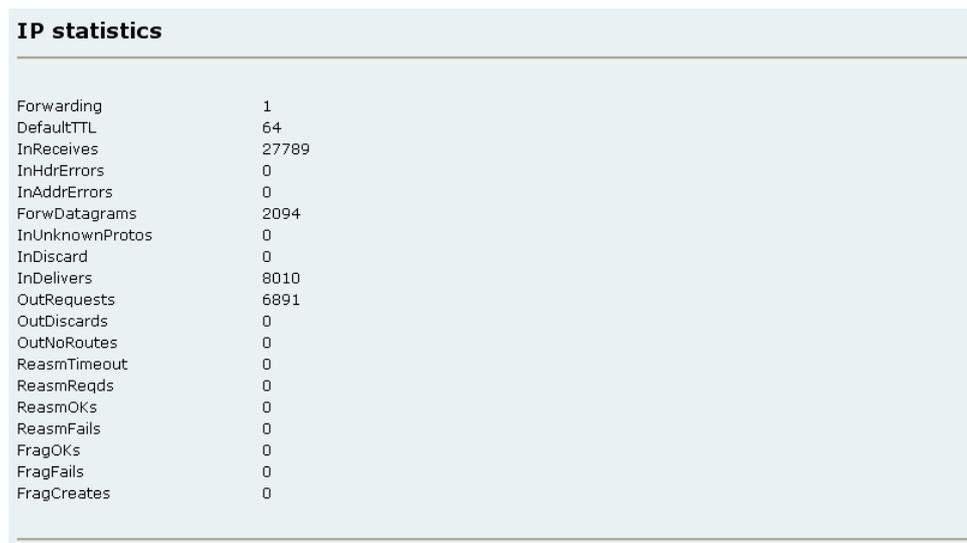
```
IP statistics

Forwarding            1
DefaultTTL            64
InReceives            27789
InHdrErrors           0
InAddrErrors          0
ForwDatagrams         2094
InUnknownProtos       0
InDiscard             0
InDelivers            8010
OutRequests           6891
OutDiscards           0
OutNoRoutes           0
ReasmTimeout          0
ReasmReqds            0
ReasmOKs              0
ReasmFails            0
FragOKs               0
FragFails             0
FragCreates           0
```

Figure 9-2 IP statistics

9.3. ICMP

The ICMP Statistics screen provides statistical information about packets/connections using an ICMP protocol. Definitions and descriptions of each parameter are described below:

InMsgs, OutMsgs :

Specifies the number of messages received or sent.

InErrors, OutErrors :

Specifies the number of errors received or sent.

InDestUnreachs, OutDestUnreachs :

Specifies the number of destination-unreachable messages received or sent. A destination-unreachable message is sent to the originating computer when a datagram fails to reach its intended destination.

InTimeExcds, OutTimeExcds :

Specifies the number of time-to-live (TTL) exceeded messages received or sent. A time-to-live exceeded message is sent to the originating computer when a datagram is discarded because the

number of routers it has passed through exceeds its time-to-live value.

InParmProbs, OutParmProbs :

Specifies the number of parameter-problem messages received or sent. A parameter-problem message is sent to the originating computer when a router or host detects an error in a datagram's IP header.

InSrcQuenchs, OutSrcQuenchs :

Specifies the number of source quench messages received or sent. A source quench request is sent to a computer to request that it reduces its rate of packet transmission.

InRedirects, OutRedirects :

Specifies the number of redirect messages received or sent. A redirect message is sent to the originating computer when a better route is discovered for a datagram sent by that computer.

InEchos, OutEchos :

Specifies the number of echo requests received or sent. An echo request causes the receiving computer to send an echo reply message back to the originating computer.

InEchoReps, OutEchoReps :

Specifies the number of echo replies received or sent. A computer sends an echo reply in response to receiving an echo request message.

InTimestamps, OutTimestamps :

Specifies the number of time-stamp requests received or sent. A time-stamp request causes the receiving computer to send a time-stamp reply back to the originating computer.

InTimestampReps, OutTimestampReps :

Specifies the number of time-stamp replies received or sent. A computer sends a time-stamp reply in response to receiving a time-stamp request. Routers can use time-stamp requests and replies to measure the transmission speed of datagrams on a network.

InAddrMasks, OutAddrMasks :

Specifies the number of address mask requests received or sent. A computer sends an address mask request to determine the number of bits in the subnet mask for its local subnet.

InAddrMaskReps, OutAddrMaskReps :

Specifies the number of address mask responses received or sent. A computer sends an address mask response in response to an address mask request.

```
ICMP statistics                                    64

InMsgs                    1
InErrors                  0
InDestUnreachs            0
InTimeExcds               0
InParmProbs               0
InSrcQuenchs              0
InRedirects               0
InEchos                   0
InEchoReps                1
InTimestamps              0
InTimestampReps           0
InAddrMasks               0
InAddrMaskReps            0
OutMsgs                   4
OutErrors                 0
OutDestUnreachs           4
OutTimeExcds              0
OutParmProbs              0
OutSrcQuenchs             0
OutRedirects              0
OutEchos                  0
OutEchoReps               0
OutTimestamps             0
OutTimestampReps          0
OutAddrMasks              0
OutAddrMaskReps           0
```

Figure 9-3 ICMP statistics

9.4. TCP

The TCP Statistics screen provides statistical information about packets/connections using a TCP protocol. Definitions and descriptions of each parameter are described below:

RtoAlgorithm :

Specifies the retransmission time-out (RTO) algorithm in use. The Retransmission Algorithm can have one of the following values.

> 0 : CONSTANT - Constant Time-out
>
> 1: RSRE - MIL-STD-1778 Appendix B
>
> 2: VANJ - Van Jacobson's Algorithm
>
> 3: OTHER – Other

RtoMin :

Specifies the minimum retransmission time-out value in milliseconds.

RtoMax :

Specifies the maximum retransmission time-out value in milliseconds.

MaxConn :

Specifies the maximum number of connections. If the maximum number is set to -1, the maximum number of connections are dynamic.

ActiveOpens :

Specifies the number of active opens. In an active open, the client is initiating a connection with the server.

PassiveOpens :

Specifies the number of passive opens. In a passive open, the server is listening for a connection request from a client.

AttemptFails :

Specifies the number of failed connection attempts.

EstabResets :

Specifies the number of established connections that have been reset.

CurrEstab :

Specifies the number of currently established connections.

InSegs :

Specifies the number of segments received.

OutSegs :

Specifies the number of segments transmitted. This number does not include retransmitted segments.

RetransSegs :

Specifies the number of segments retransmitted.

InErrs :

Specifies the number of errors received.

OutRsts :

Specifies the number of segments transmitted with the reset flag set.

TCP statistics

RtoAlgorithm	1
RtoMin	200
RtoMax	120000
MaxConn	4294967295
ActiveOpens	0
PassiveOpens	35
AttemptFails	0
EstabResets	26
CurrEstab	3
InSegs	1031
OutSegs	1299
RetransSegs	7
InErrs	0
OutRsts	0

Figure 9-4 TCP statistics

9.5. UDP

The UDP Statistics screen provides statistical information about packets/connections using a UDP protocol. Definitions and descriptions of each parameter are described below:

InDatagrams :

Specifies the number of datagrams received.

NoPorts :

Specifies the number of received datagrams that were discarded because the specified port was invalid.

InErrors :

Specifies the number of erroneous datagrams that were received. Datagrams Received Errors is the number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

OutDatagrams :

Specifies the number of datagrams transmitted.

UDP statistics

InDatagrams	3685
NoPorts	4
InErrors	0
OutDatagrams	3554

Figure 9-5 UDP statistics

10. CLI guide

10.1. Introduction

The Parani-MSP1000 **Root** user can access the Linux console command line interface (CLI) of the Parani-MSP1000 by via the serial console or Telnet/SSH. In the CLI, the authorized user can perform standard Linux commands to view the status of the Parani-MSP1000, edit the configuration, apply configuration changes, define user scripts and transmit files between the Parani-MSP1000 and remote hosts.

The Parani-MSP1000 provides 2048 KB user space mounted in `/usr2` for read/write capabilities in its internal flash memory. Using the user space, the users user can make create their own scripts or executable binaries to customize the Parani-MSP1000 for their own purpose.

A **Root** users can will always have access to the CLI always by through the serial console or by using a Telnet/SSH client from their workstation.

10.2. Flash memory partitions

The Parani-MSP1000 internal flash is partitioned as shown in the table below. The users can freely access the Mtdblock4 which is mounted on /usr2 for their own needs. The users can also access files at /etc, /var, and /temp. However, accessing these files at the RAM disk will not affect the Parani-MSP1000 after rebooting.

Block	Type	Mount point	Size (KB)
Mtdblock0	Bootloader	None	384
Mtdblock1	Linux Kernel	None	2048
Mtdblock2	Ram disk image (16MB)	/etc, /var, /tmp	256
Mtdblock3	Cramfs (Read only)	/	11648
Mtdblock4	JFFS2 (R/W)	/usr2	2048
Total			16348

Note: Do not access each mtdblock using mount or dd command in the CLI.
This may make the Parani-MSP1000 inoperable.

10.3. Accessing CLI

Serial console:

1) Connect the console port of the Parani-MSP1000 with the PC serial port

2) Run the PC terminal emulation program

3) Configure the PC serial port to: 9600-8-N-1 No flow control

4) Press <enter>

5) Login with the Parani-MSP1000 root account

Telnet/SSH console:

1) `telnet` *Parani-MSP1000_ip_address* or

2) `ssh root@` *Parani-MSP1000_ip_address*

10.4. Running user-defined scripts

Shell script /usr2/rc.user is automatically called when the Parani-MSP1000 is booting. Users can modify the rc.user file to run user-defined script or binaries

```
#!/bin/bash
#
# rc.user : Sample script file for running user programs at boot time
#
#PATH=/bin:/usr/bin:/sbin:/usr/sbin
# Add shell command to execute from here

echo 'This is the welcome message defined by users'exit 0
```

10.5. File transmission

The users can use an ftp client for file transmission and use `/usr2` directory for data read/write

```
root@192.168.0.117:~# cd /usr2
root@192.168.0.117:/usr2# ftp 192.168.2.3
Connected to 192.168.2.3.
220 lxtoo.senalab.co.kr FTP server (Version wu-2.6.1-16) ready.
Name (192.168.2.3:root): sena
331 Password required for sena.
Password:
230 User sena logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get test.tgz
local: test.tgz remote: test.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for test.tgz (350 bytes).
226 Transfer complete.
350 bytes received in 0.04 secs (9.6 kB/s)
ftp> bye
```

In addition to a regular FTP client, the user can copy files securely as encrypted using scp client program. If the user wants to copy a file from the Parani-MSP1000(192.168.0.120) to user's PC, type a command on the user's PC as shown below:

```
[root@localhost work]# scp root@192.168.0.120:/usr2/rc.user /work
The authenticity of host '192.168.0.120 (192.168.0.120)' can't be established.
RSA key fingerprint is c1:70:ab:52:48:ab:e5:dc:47:9c:94:ed:99:6f:94:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.120' (RSA) to the list of known hosts.
root@192.168.0.120's password:
rc.user             100% |*****************************|   173       00:00
[root@localhost work]#
```

11. Approval Information

11.1. FCC

11.1.1. FCC Compliance 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

11.1.2. RF Exposure Statement

The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operation in conjunction with any other antenna or transmitter.

11.1.3. Do not

Any changes or modifications to the equipment not expressly approved by the party responsible for compliance could void user's authority to operate the equipment.

11.2. CE

11.2.1. EC-R&TTE Directive

Directive 1999/5/EC.

11.3. MIC

11.4. Telec
Construction Design Certification No. 006NYC0070

12. RF Information

12.1. Radio Frequency Range

2.402~2.480GHz

12.2. Number of Frequency Channel

79 channels

12.3. Transmission Method

FHSS(Frequency Hopping Spread Spectrum)

12.4. Modulation Method

GFSK(Gaussian-filtered Frequency Shift Keying)

12.5. Radio Output Power

+18dBm

12.6. Receiving Sensitivity

-88dBm

12.7. Power Supply

DC5V

Appendix A. Connections

A.1. Console pin-outs

The pin assignment of the Parani-MSP1000 DB9 connector is summarized in Table A-1. Each pin has a function according to the serial communication type configuration.
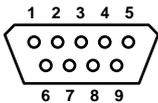
Figure A-1 Pin layout of the DB-9 connector

Table A-1 Pin assignment of DB-9 connector for console and serial port

Pin	RS232 (console and serial ports)
1	DCD
2	Rx
3	Tx
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

A.2. Ethernet Wiring Diagram
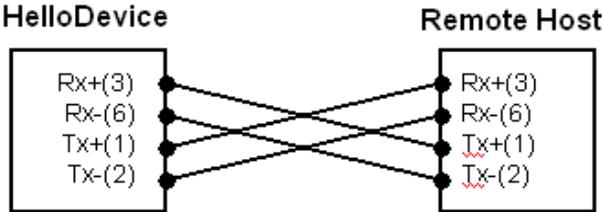
Figure A-2 Ethernet direct connection using crossover Ethernet cable
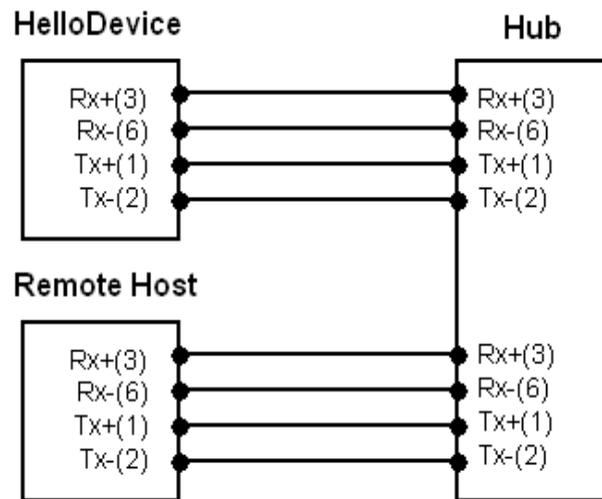
Figure A-3 Ethernet connection using straight through Ethernet cable

Appendix B. Well-known port numbers

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. *Table B-1* shows some of the well-known port numbers. For more details, please visit the IANA website:

http://www.iana.org/assignments/port-numbers

Table B-1 Well-known port numbers

| Port number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

Appendix C. Using Python

The Parani-MSP1000 supports python language for user customization.

C.1. Running Python

There are two different ways to start Python.

C.1.1 Interactive Interpreter from Command Line Interface

You can enter Python and start coding right way in the interactive interpreter by starting it from the command line.

```
[root@MSP1000 usr2]# python
Python 2.5 (r25:51908, Mar 14 2007, 11:33:06)
[GCC 4.0.0 (DENX ELDK 4.0 4.0.0)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> a = 1
>>> b = 2
>>> c = a + b
>>> c
3
>>>
```

C.1.2 As a script from the Command Line Interface

A Python script can be executed by invoking the interpreter from the command line. Be sure that the file permission mode allows execution.

```
[root@MSP1000 usr2]# cat cal.py
#!/bin/python

a = 1
b = 2
c = a + b
print "a + b = %d" % c

[root@MSP1000 usr2]# ./cal.py
a + b = 3
[root@MSP1000 usr2]#
```

C.2. Adding libraries and modules

Users can upload additional Python libraries and modules. The additional libraries and modules should be located in the /usr2. When uploading files, the Bluetooth FTP and Secure Copy (scp) are available.

```
[root@MSP1000 usr2]# scp 192.168.7.8:/home/array.so ./
```

```
Warning: Permanently added '192.168.7.8' (RSA) to the list of known hosts.
root@192.168.7.8's password:
array.so                                  100%  101KB 101.4KB/s   00:01
[root@MSP1000 usr2]#
```

C.3. Executing Python script at boot time

The Parani-MSP1000 executes the /usr2/rc.user at boot time. Users should make the rc.user execute the Python script.

C.3.1 Example: Inquiring near devices and transferring file.

Step 1. Make a Python code. (btsender.py)

```
#!/bin/python

import bluetooth
import lightblue
import select
from time import *
import threading

scan_interval = 90
send_interval = 300
file_path = "/usr2/advertising.jpg"
# Available class
# Miscellaneous, Computer, Phone, LAN/Network Access point, Audio/Video,
Peripheral, Imaging
# Usage  : available_class = ["class_name", ...]
# example : available_class = ["Computer"]
#           available_class = ["Computer", "Phone"]
available_class = ["Phone"]

class MyDiscoverer(bluetooth.DeviceDiscoverer):

    def pre_inquiry(self):
        self.done = False

    def device_discovered(self, address, device_class, name):
        major_classes = ( "Miscellaneous",
                    "Computer",
                    "Phone",
                    "LAN/Network Access point",
                    "Audio/Video",
                    "Peripheral",
                    "Imaging" )

        major_class = (device_class >> 8) & 0xf

    if major_class >= 7:
        return

    for item in available_class:
        if item == major_classes[major_class]:
            service_classes = ( (16, "positioning"),
                    (17, "networking"),
                    (18, "rendering"),
                    (19, "capturing"),
                    (20, "object transfer"),
                    (21, "audio"),
                    (22, "telephony"),
```

75

```
                       (23, "information"))

           for bitpos, classname in service_classes:
               if device_class & (1 << (bitpos-1)) and classname == "object
transfer":
               scan_info.append(address)

    def inquiry_complete(self):
        self.done = True

def sendfile(bdaddr, i):
    if len(send_info) > 0:
        for item in send_info:
            if item['addr'] == bdaddr:
                return

    services = lightblue.findservices(addr=bdaddr, servicetype=lightblue.OBEX)
    address, serviceport, servicename = services[0]
    lightblue.obex.sendfile(address, serviceport, file_path)
    temp = {'addr': bdaddr, 'time': time()}
    send_info.append(temp)

def update_send_info():
    cur_time = time()

    for item in send_info:
        if cur_time - item['time'] > send_interval:
            send_info.remove(item)

send_info = []

while True:
    scan_info = []
    threads = []
    nloops = 0

    d = MyDiscoverer()
    d.find_devices(lookup_names = True)

    readfiles = [ d, ]

    while True:
        rfds = select.select( readfiles, [], [] )[0]

        if d in rfds:
         d.process_event()

        if d.done: break

    if len(send_info) > 0:
        update_send_info()

    for item in scan_info:
        t = threading.Thread(target=sendfile, args=(item, 0))
        threads.append(t)
        nloops += 1

    for i in range(0, nloops):
        threads[i].start()
        sleep(5)

    for i in range(0, nloops):
        threads[i].join()

    del scan_info
    del threads
    del nloops
```

```
    sleep(scan_interval)
```

Step 2. Upload the Python code

```
[root@MSP1000 usr2]# scp 192.168.7.8:/home/btsender.py ./
root@192.168.7.8's password:
btsender.py                              100% 2644    2.6KB/s   00:00
[root@MSP1000 usr2]#
```

Step 3. Modify the /usr2/rc.user

```
[root@MSP1000 usr2]# vi rc.user
#

#PATH=/bin:/usr/bin:/sbin:/usr/sbin

# Add shell command to execute from here

/usr2/btsender.py &
```

Step 4. Restart the Parani-MSP1000

```
[root@MSP1000  usr2]#  reboot
```

Appendix D. Control Commands

The Parani-MSP1000 is controllable by Control commands through 2525 TCP port. Every command responds with +OK if successful, otherwise –ERR.
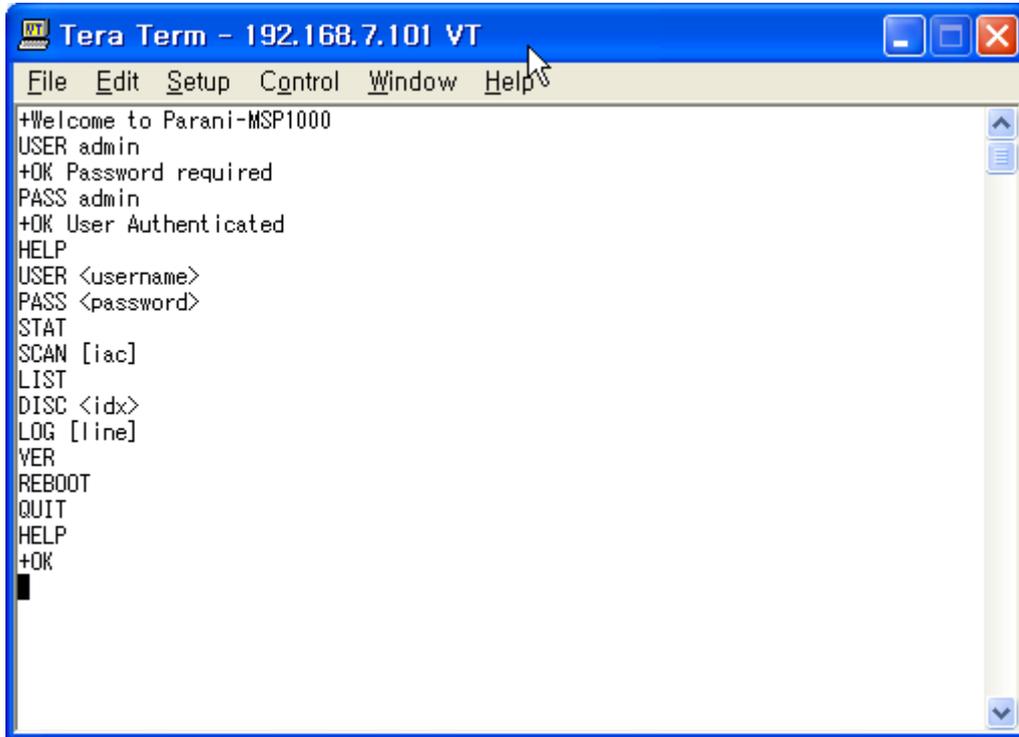
Figure D-1 Control command

D.1. Commands for Control port

<OPT> : Necessary, [OPT] : Optional

Synopsis	USER <username>
Description	To enter login name.
Example	USER admin +OK Password required

Synopsis	PASS <password>
Description	To enter the password for logging in.
Example	PASS 1234 +OK User Authenticated

Synopsis	STAT
Description	Displays current Bluetooth device status. Idx|bdaddr|tx-byte|rx-byte|tx-error|rx-error
Example	STAT 0|00:01:95:00:00:D2|131570|235803|0|0 +OK

Synopsis	SCAN [IAC]
Description	To see the inquired device list. IAC – Inquiry Access Code. User may inquire the device with same IAC code. Bdaddr|name
Example	SCAN 00:01:95:07:08:51|PSD200v1.1.0-070851 00:02:72:CE:A4:2A|ubunto-0 00:01:95:08:24:CF|MSP1000-0 +OK

Synopsis	LIST
Description	To see the connected Bluetooth device list. Higher link quality, better link status. Zero rssi means the most efficient RF condition. With link quality lower than 200, throughput may be affected or link may be lost. Idx|dev_id|bdaddr|name|link_quality|rssi
Example	LIST 0|0|00:01:95:07:3C:E7|PSD100v1.1.1-073CE7|255|22 +OK

Synopsis	DISC <idx>
Description	Parani-MSP1000 may disconnect forcibly by DISC command, giving index value in LIST command.
Example	LIST 0|0|00:01:95:07:3C:E7|PSD100v1.1.1-073CE7|255|22 +OK DISC 0 +OK LIST +OK

Synopsis	LOG [line]
Description	To see system log. If line number specified, only latest [line] rows will be displayed.
Example	LOG 1 Apr 11 01:42:13 MSP1000 local0.info web[507]: Authentication for 'root' passed. +OK

Synopsis	VER
Description	To see software version of Parani-MSP1000.
Example	VER +OK v1.2.0

Synopsis	HELP
Description	Displays all control commands available.
Example	HELP USER <username> PASS <password> STAT SCAN [iac] LIST DISC <idx> LOG [line] VER REBOOT QUIT HELP +OK

Synopsis	REBOOT
Description	To reboot Parani-MSP1000. (only root)
Example	REBOOT +OK Reboot

Synopsis	QUIT
Description	To quit the communication with Parani-MSP1000.
Example	QUIT +OK Disconnected

Appendix E. Warranty

E.1. GENERAL WARRANTY POLICY

Sena Technologies, Inc. (hereinafter referred to as SENA) warrants that the Product shall conform to and perform in accordance with published technical specifications and the accompanying written materials, and shall be free of defects in materials and workmanship, for the period of time herein indicated, such warranty period commencing upon receipt of the Product.

This warranty is limited to the repair and/or replacement, at SENA's discretion, of defective or non-conforming Product, and SENA shall not be responsible for the failure of the Product to perform specified functions, or any other non- conformance caused by or attributable to: (a) any misapplication or misuse of the Product; (b) failure of Customer to adhere to any of SENA's specifications or instructions; (c) neglect of, abuse of, or accident to, the Product; or (d) any associated or complementary equipment or software not furnished by SENA.

Limited warranty service may be obtained by delivering the Product to SENA or to the international distributor it was purchased through and providing proof of purchase or receipt date. Customer agrees to insure the Product or assume the risk of loss or damage in transit, to prepay shipping charges to SENA, and to use the original shipping container or equivalent.

E.2. LIMITATION OF LIABILITY

EXCEPT AS EXPRESSLY PROVIDED HEREIN, SENA MAKES NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, WITH RESPECT TO ANY EQUIPMENT, PARTS OR SERVICES PROVIDED PURSUANT TO THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER SENA NOR ITS DEALER SHALL BE LIABLE FOR ANY OTHER DAMAGES, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION IN CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), SUCH AS, BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS OR BENEFITS RESULTING FROM, OR ARISING OUT OF, OR IN CONNECTION WITH THE USE OF FURNISHING OF EQUIPMENT, PARTS OR SERVICES HEREUNDER OR THE PERFORMANCE, USE OR INABILITY TO USE THE SAME, EVEN IF SENA OR ITS DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL SENA OR ITS DEALERS TOTAL LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT.

E.3. HARDWARE PRODUCT WARRANTY DETAILS

WARRANTY PERIOD: SENA warranties embedded hardware Product for a period of one (1) year, and external hardware Product for a period of three (3) or five (5) years according to the Product type.

WARRANTY PROCEDURE: Upon return of the hardware Product SENA will, at its option, repair or replace Product at no additional charge, freight prepaid, except as set forth below. Repair parts and replacement Product will be furnished on an exchange basis and will be either reconditioned or new. All replaced Product and parts become the property of SENA. If SENA determines that the Product is not under warranty, it will, at the Customers option, repair the Product using current SENA standard rates for parts and labor, and return the Product at no charge in or out of warranty.

WARRANTY EXCLUSIONS: Damages caused by
- Accidents, falls, objects striking the SENA product,
- Operating the Product in environments that exceed SENA's temperature and humidity specifications,
- Power fluctuations, high voltage discharges,
- Improper grounding, incorrect cabling,
- Misuse, negligence by the customer or any other third party,
- Failure to install or operate the product (s) in accordance to their SENA User Manual,
- Failure caused by improper or inadequate maintenance by the customer or any other third party,
- Floods, lightning, earthquakes,

- Water spills,
- Replacement of parts due to normal wear and tear,
- Hardware has been altered in any way,
- Product that has been exposed to repair attempts by a third party without SENA's written consent,
- Hardware hosting modified SENA Software, or non-SENA Software, unless modifications have been approved by
  SENA.
- Battery component capacity degradation due to usage, aging, and with some chemistry, lack of maintenance.

E.4. SOFTWARE PRODUCT WARRANTY DETAILS

WARRANTY PERIOD: SENA warranties software Product for a period of one (1) year.
WARRANTY COVERAGE: SENA warranty will be limited to providing a software bug fix or a software patch, at a reasonable time after the user notifies SENA of software non-conformance.

E.5. THIRD-PARTY SOFTWARE PRODUCT WARRANTY DETAILS

The warranty policy of the third-party software is conformed to the policy of the corresponding vendor