Installation Guide
BS11
BS52 / BS51
BS52/23 / BS51/23
BS5432 / BS5431
BS5432i / BS5431i
BS5411i / BS2411i
SU51 / SU51/23

Revision 2.4

RepeatIT AB
Hamngatan 33
172 66 Sundbyberg
Sweden

Tel: +46 8 570 106 66
Fax: +46 8 570 106 67
E-mail: info@repeatit.se
www.repeatit.se

1. Installation

The Repeatit Base Station (BS) should always be mounted on the highest possible place with its antenna having clear line of sight to all clients.

Together with the BS, the following equipment is provided in your box:

- Base Station
- Power over Ethernet adaptor
- IP65 rated RJ45 connector
- Mounting kit
- Installation Guide

1.1 Hardware setup

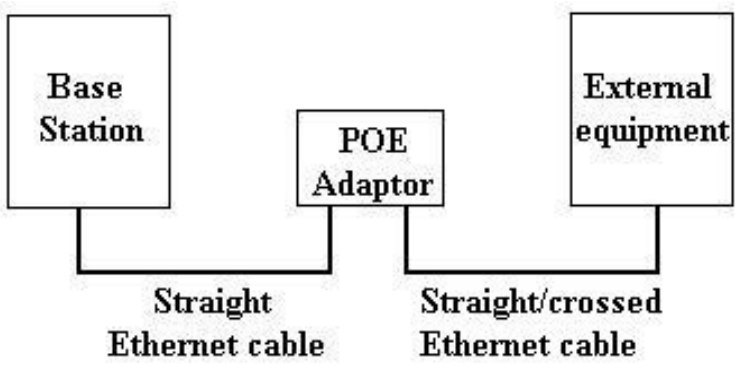

Figure 1 - Hardware setup

The BS should be connected to the Power over Ethernet (POE) adaptor's *P+DATA OUT* socket. Since both data and power is fed over the cable, all eight conductors should be used, and the Ethernet cable shall be straight. To the POE's *DATA IN* socket, external equipment can be connected. When configuring the BS, a computer usually is used, and then the cable between the POE and the computer should be crossed. If the BS is connected to for example a network switch, the cable between the switch and the POE adaptor usually is straight.

The BS unit is configured in a browser window. Start your browser and type the following line in the address field:

http://10.0.0.1

Press *Enter*. A login window is shown. The default login settings are:

User name: *admin*
Password: *public*

Type the user name and the password in the fields provided and press OK. In the browser window, all relevant BS settings can be monitored.

1.2 Base station configuration

The BS is intended to be used together with the Radio Control Software (RCS) developed by Repeatit. The configurations that can be made directly on the BS are overridden by the RCS as soon as a connection between the BS and the RCS is established and the BS is synchronized. Though, the network settings (IP address, netmask, RCS address etc.) always have to be set directly on the BS. In section 1.3, the configuration process when using the RCS is described. If the BS is to be used without the RCS, check section 1.4. The rest of this section describes the different tabs in the configuration window.

1.2.1 Main window

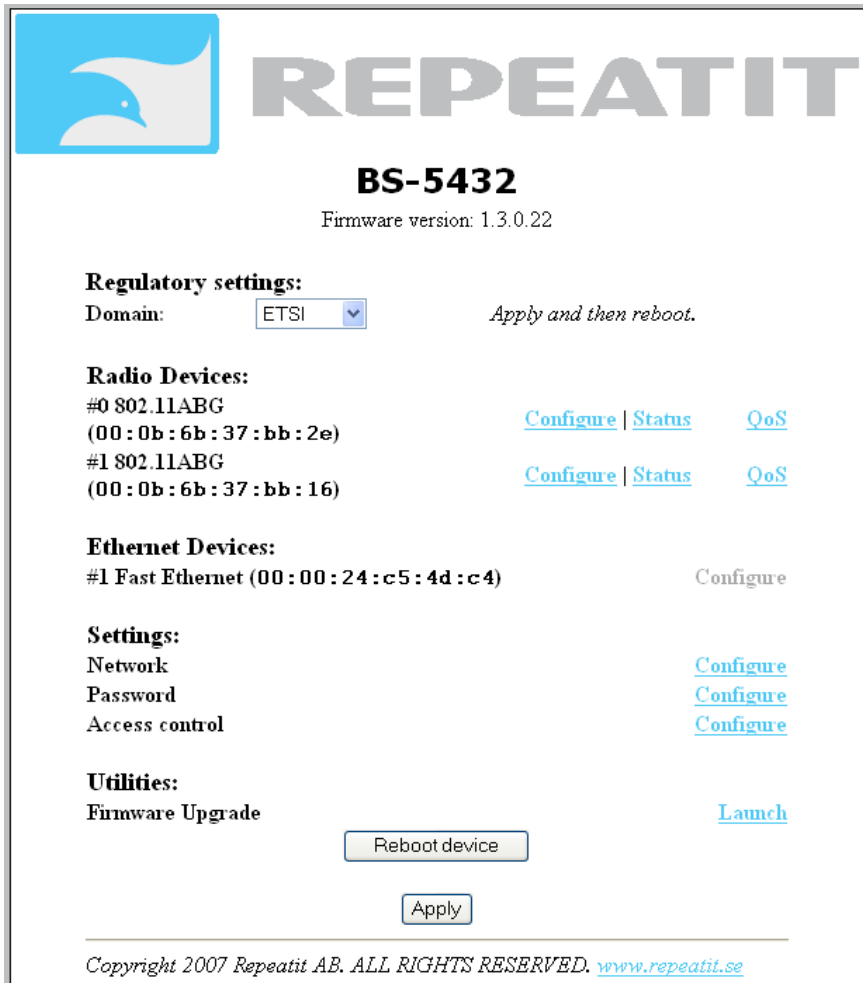

Figure 2 - The main window.

Regulatory settings
ETSI or ETSI-UK can be set depending on which regulatory domain the equipment is intended to be used.

Radio Devices
Configuration of the radio device is described in section 1.2.2 and section 1.2.3. The *Status tab* is described in section 1.2.4.

Ethernet devices
This is the Ethernet interface of the base station. It can not be configured.

Settings
Network settings are described in section 1.2.5. *Password settings* are described in section 1.2.6. *Access control settings* are described in section 1.2.7.

Utilities
Here, the firmware can be upgraded. Usually, this is done from the RCS.

Restore to Default
Pressing this button restores the unit to factory defaults.

Reboot device
Reboots the device.

1.2.2 Configure tab – Master mode

A radio interface can be configured in two different ways; either as a master or as a client. The Master mode is shown in Figure 3. To store changes, press *Apply*.

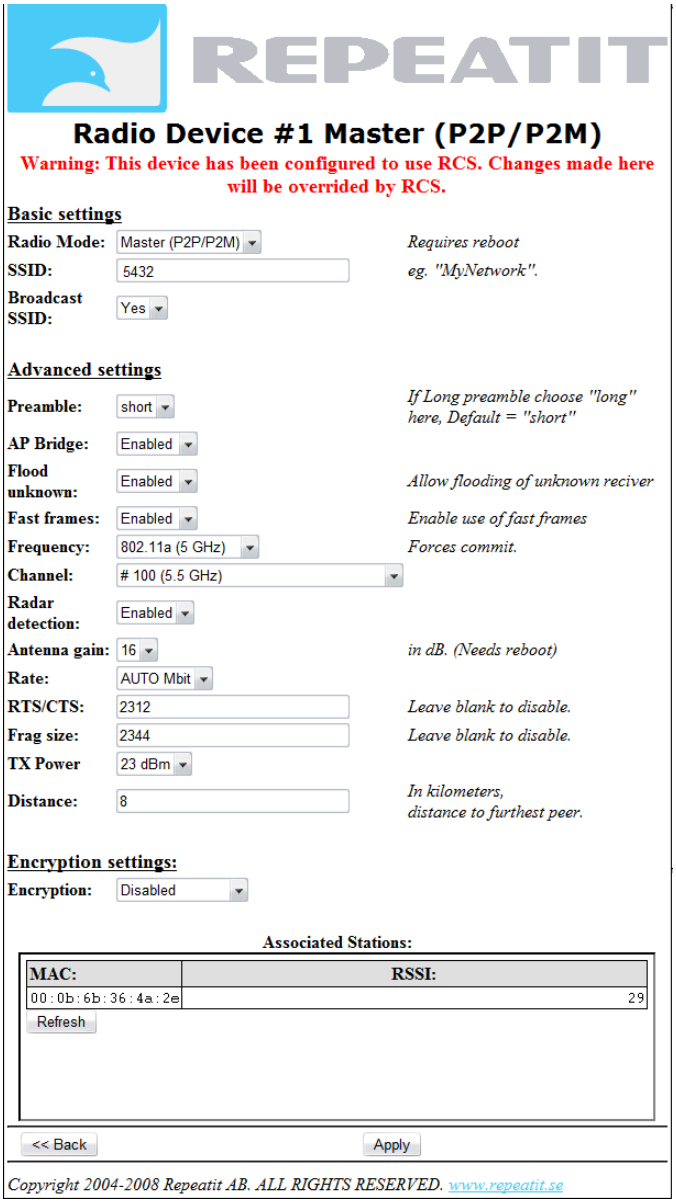

Figure 3 - Radio device in Master mode.

Basic settings

Radio mode:	Master/Slave.
SSID:	Wireless network name. This is the name that the customers will see when they perform a scan from their CPEs (Client Premise Equipment).
Broadcast SSID:	Tells whether the SSID should be visible when a scan is performed or not.

Advanced settings

Preamble:	How clients should negotiate a connection, “long” is available for legacy support.
Antenna:	Primary is the internal antenna, secondary the N-connector. (This is only available on BS-xxxx***i*** models)
AP Bridge:	Should the BS bridge between clients or not.
Flood unknown:	Enabling this will make the BS send packets addressed to unknown recivers to all associated clients instead of dropping them. May be usefull on P2P links.
Fast frames:	Enable use of “Fast frames”, an almost standard way to improve throughput.
Frequency:	The frequency band to use. To enable turbo in client-mode this must be set to “Autoselect
Channel:	Within each frequency band, a number of different channels are available.
Radar detection:	Mandatory for the 5 GHz bands in most European countries. Check your national regulations.
Antenna gain:	The gain of the antenna in use.
Rate:	The available rates are different in various standards. The default value is *Auto*.
RTS/CTS:	Request to Send/Clear to Send. Leave out for default.
Frag size:	Fragmentation of packets. Leave out for default.
Tx power:	The transmit power from the radio device (this is not the eirp value, i.e. the antenna gain is *not* included).
Distance:	Approximate distance to CPE located at furthest place.

Encryption settings

WPA1&2 are available together with ciphers TKIP and CCMP/AES.
The BS and clients need to use the same setting, or the ”both” setting that allows either type.
The TKIP cipher has a hardware limit of 23 concurrent clients.

There is also support for legacy WEP encryption.
Be advised that the way to crack WEP encryption is well-known and fast.
If the wireless network makes use of WEP keys, the WEP keys settings must be configured in the BS. To adjust the WEP settings, change the selection from *Disabled* to either *WEP 128-bit* or *WEP 64-bit*.
The WEP key consists of hexadecimal numbers (0-9 and A-F), and the length of the key depends on the chosen key size (64 or 128 bits). If a 64-bit key is used, ten hex numbers shall be typed in the WEP key field. If a 128-bit key is used, 26 hex numbers shall be typed in. Observe that the same key set has to be used on the CPE side of the connection.

The *Authentication* method used is *Shared key*. It is also important that the right *WEP key number to use* is chosen. For example, if the BS uses WEP key #1, the CPEs also have to use this key number

Associated stations

Here, all associated stations should be presented when the CPEs are connected. If the RCS not is used, the clients (CPEs and other BS in client mode) have to be enabled under the *Access tab* (see section 1.2.7).

1.2.3 Configure tab – Client mode

For client mode settings, check Figure 4.

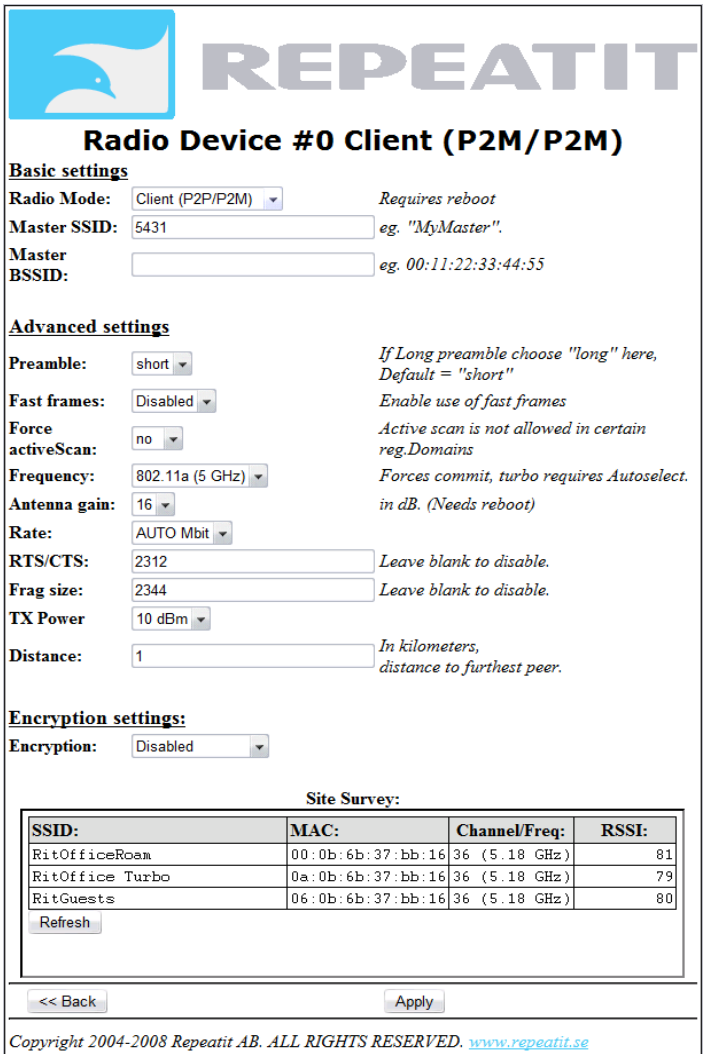

Figure 4 - Radio device slave mode.

Basic settings

Master SSID: The SSID set on the Master radio card (the radio device that the client shall connect to).

Master BSSID: The MAC address of the Master radio card. This address can be found in the Main window (see section 1.2.1) on the Master BS. Optional, mainly usefull if there are two or more APs with the same SSID

For advanced and encryption settings, check section 1.2.2.

Site survey

When the BS is in client mode, it is possible to scan the area for other wireless networks. This can be done in order to avoid interference or to find the Master BS.

To store changes, press *Apply*.

1.2.4 The Status tab

Each radio card has its own *Status tab*. This tab is used when two BSs are set up in a point-to-point link. When more than one client are connected to a BS, the Status tab cannot be used.

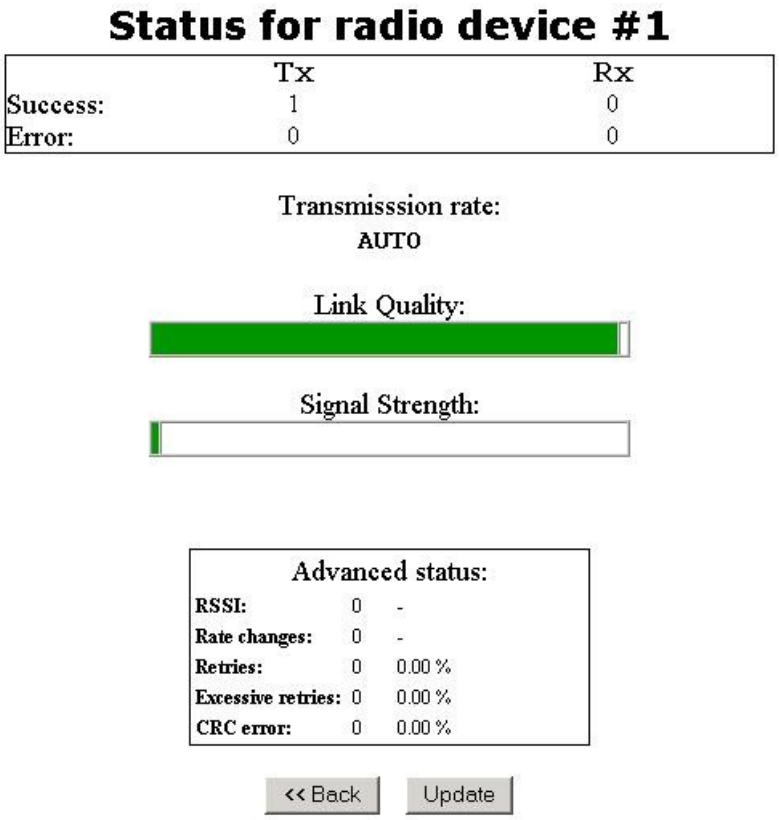

Figure 5 - The status tab.

1.2.5 The Network tab

This is usually the tab that is accessed first when configuring the BS. A screen-shot is shown in Figure 6.

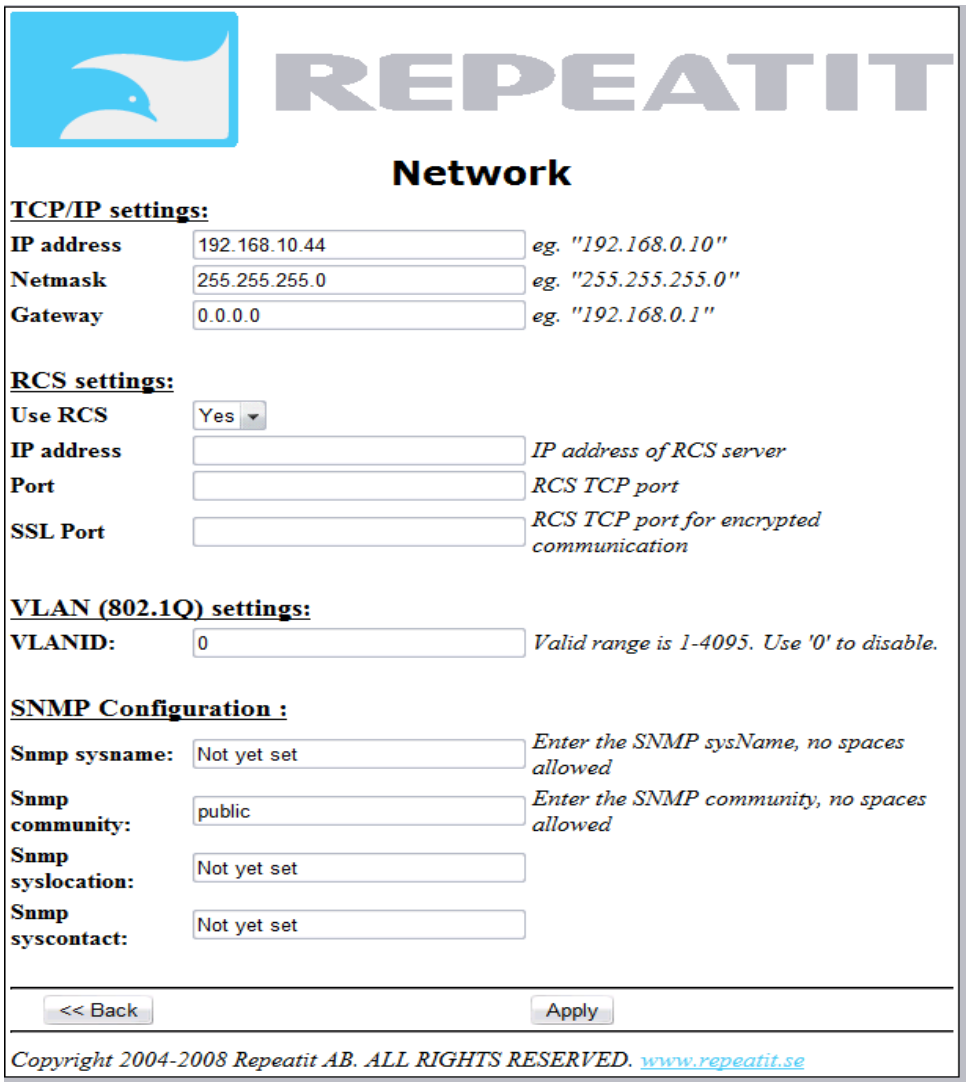

Figure 6 - The Network tab.

TCP/IP Settings

This is the IP settings for the BS.

RCS settings

If enabled, the IP address of the RCS can be typed in. It is also possible to choose which port the traffic between the BS and the RCS shall use. The default port number is 9999, encrypted communication defaults to 9998 if enabled. To disable either select port 0. Observe that the RCS and the base station need to have the same port selected.

VLAN settings

To use the base station in a VLAN, set the vlan ID here. **NB.** setting a VLAN is a good way to loose contact with your BS! Don't touch this setting unless you know what you are doing.

1.2.6 Password tab

Under this tab, the password can be changed. To do this, type the new password in the two boxes provided. Press *Apply*.

1.2.7 Access tab

When no RCS is used, the BS uses an internal accept list that can be set up to list alloved clients "Accept" or not allowed clients "Deny". To add a client to the list, type the client side MAC address in the Master BS *Add MAC* field on the form 00:11:22:33:44:55 and press *Add* (see Figure 7). When all clients are added, press *Apply*.

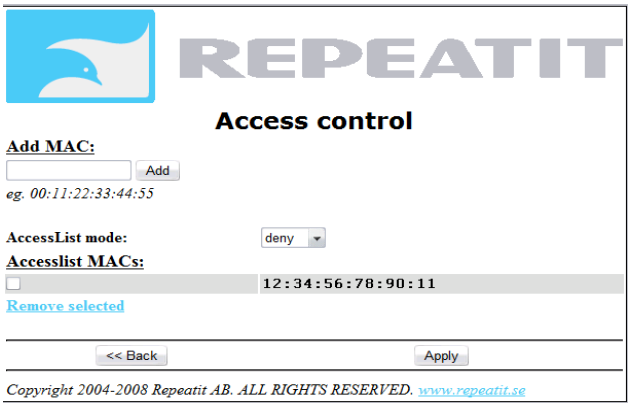

Figure 7 - Access control tab. In this example, one client is added.

1.3 Configuration of BS when RCS is used

If a connection between the BS and the RCS is established, the only settings that have to be made on the BS are network settings (see section 1.2.5). When the BS has been synchronized from the RCS, no more configurations have to be done on the BS.

1.4 Configuration of BS when RCS is not used

If no RCS address is provided, more configurations have to be done directly on the BS. Here is a checklist (refer to Figure 2):

1. Access the *Network Settings tab* (section 1.2.5) and change the IP settings for the BS.
2. Access the *Configure tab* (section 1.2.2) for each radio card and make all relevant settings.
3. Access the *Access Control tab* (section 1.2.7) and add all clients.
4. Reboot the BS.

2. Support

On our web site, http://www.repeatit.se, you can find the latest upgrades of all firmware, product news, FAQ and other information related to the products.

3. Our Warranty

Repeatit AB, Hamngatan 33, S-172 66 Sundbyberg, Sweden, guarantee that our products do not have any defects regarding material or function upon delivery. All of Repeatit's products are covered by a 12 moth international warranty.

If during the time of warranty the product displays any defects regarding material or function, the products should be returned to your reseller, who will, according to their own judgment, either repair or replace the product according to the following conditions:

3.1 Conditions

1. The warranty is only valid in combination with an original receipt issued by the reseller at the date of delivery or sales. The receipt needs to contain the product's serial number or similar identification.

2. If Repeatit repairs or replaces the product, the repaired or replaced product will be covered by the original warranty during the remainder of the guarantee period. During repair, some parts might be replaced. These parts are then the property of Repeatit AB.

3. The warranty does not cover normal wear and tear, faulty usage or handling, or other usage other than the one described by Repeatit AB. The warranty does not cover defects caused by accidents.

4. The warranty is not valid if service is performed on the product by a by Repeatit non-unauthorised person or company.

5. The warranty is not valid if any products that are not Repeatit original accessories are used with the product.

6. There are no warranty, written or oral, other than this printed warranty.