SF-3000

IEEE 802.11b Wireless Access Bridge

User Manual

September 1, 2003
Version 1.00

Before operating the unit, please read this manual thoroughly, and retain it for future reference.

Contents

Chapter 1. Introduction

1.1 Introducing the SF-3000

The SF-3000 is a fully interoperable with IEEE 802.11b compliant Outdoor Wireless Last-mile product. The SF-3000 operates in bridge-to-bridge mode, and supports point-to–point as well as point-to-multipoint topologies, for maximum flexibility in configuring building-to-building networks.

1.2 Product Features

Protocol Supported :

- TCP/IP
- NAT/NAPT
- DHCP client
- Virtual Server (NAT inbound server)

Security Features :

- User authentication in Web-based manager
- MAC address based access control
- Wireless 64-/128-bit WEP encryption

Management supported :

- Web-based Manager
- Telnet configuration
- Console (RS-232) configuration
- SNMP v1, SNMP MIB-II and private MIB

Firmware Upgrade :

- TFTP (Transparent FTP)
- Xmodem and 1K Xmodem

1.3 Package Contents

The product package contains the following items.

1. One (1) SF-3000 Outdoor Wireless Access Bridge unit
2. One (1) 24V, 0.83A AC/DC adapter with wall-plug power cord
3. One (1) Inline Power Injector (PoE)

4. One (1) 30m RJ-45 CAT-5 Ethernet cable
5. One (1) 1.8m RS-232 Console Cable
6. One (1) 1.8m Grounding Cable
7. One (1) User manual CD-disc
8. One (1) wall mounting kit
9. One (1) mast mounting kit

1.4 System Requirements

Installation of the Outdoor Wireless Access Bridge requires:

1. A Windows-based PC/AT compatible computer or Ethernet data device with an available RJ-45 Ethernet port to run the configuration program or with TCP/IP connection to the Ethernet network.
2. A 10/100Base-T Ethernet RJ-45 Ethernet cable is connected to Ethernet network.
3. A RS-232 Consol Port cable is connected to PC/AT compatible computer.
4. An AC power outlet (100~240V, 50~60Hz) supplies the power.

1.5 Inline Power Injector (PoE)

The SF-3000 is equipped with an Inline Power Injector module. The Inline Power Injector (PoE) deliver both data and power to the Access Point via a signal Ethernet cable.

1. This works great in areas where you may not have power and/or Ethernet easily accessible, like a roof.
2. This also allows you to more easily place the AP closer to the antenna, thus reducing signal loss over antenna cabling.
3. Ethernet signal travels well over CAT 5 cable but 2.4GHz signal doesn't do as well over antenna cabling.
4. Ethernet cabling is much cheaper than Antenna cabling.

Chapter 2. Installation and Basic Configuration

This chapter describes the procedures for installing the SF-3000.

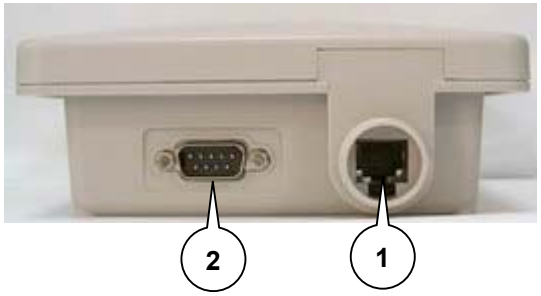
2.1 Before You Start

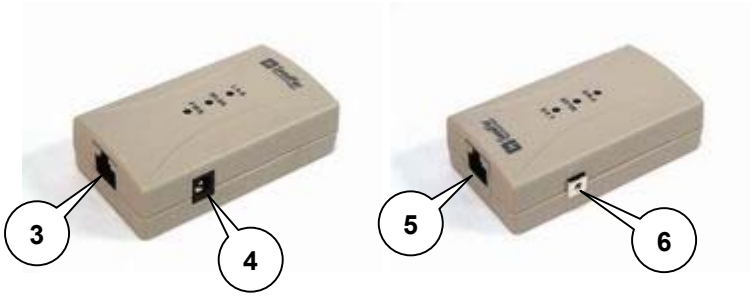
After unpacking the system, make sure the following items are present and in good condition.

1. SF-3000
2. 24V, 0.83A AC/DC adapter with wall-plug power cord
3. Inline Power Injector (PoE)
4. 30m RJ-45 CAT-5 Ethernet cable
5. Cross over Ethernet Cable
6. 1.8m RS232 Console Port Cable
7. 1.8m Grounding Wire
8. User's Manual Disk
9. Wall/Mast Mounting Kit

2.2 Locate the SF-3000 and Inline Power Injector Ports

- Ethernet port 1 for connecting the 30m RJ-45 CAT-5 Ethernet cable.
- RS232 port 2 for connecting the 1.8m RS-232 console port cable.
- Data input port 3 for connecting the Ethernet Cable to a Hub Switch Router or a PC.
- 24V power adapter input port 4
- Power & Data output port 5 for connecting the other end of the 30m RJ-45 CAT-5 Ethernet Cable.
- Grounding port 6.





The SF-3000 can be mounted on the wall, you can use the Wall Mount kit to mount the SF-3000 as shown in **Figure 2.2.1**.

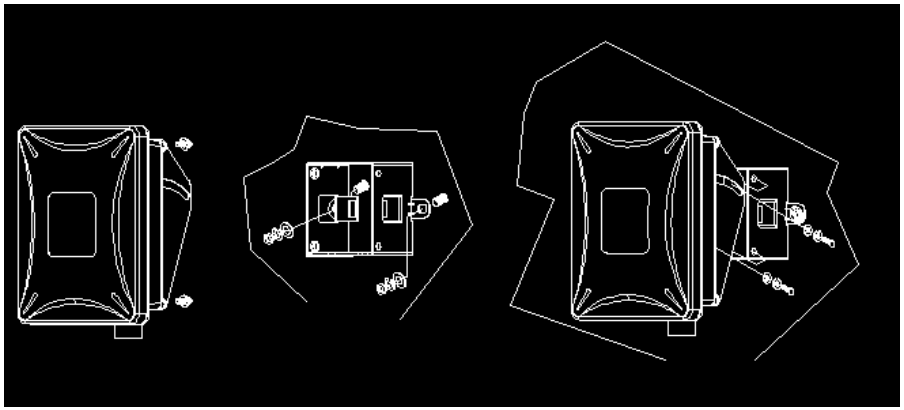


Figure 2.2.1

You can also mount the SF-3000 to the mast as shown in **Figure 2.2.2**.

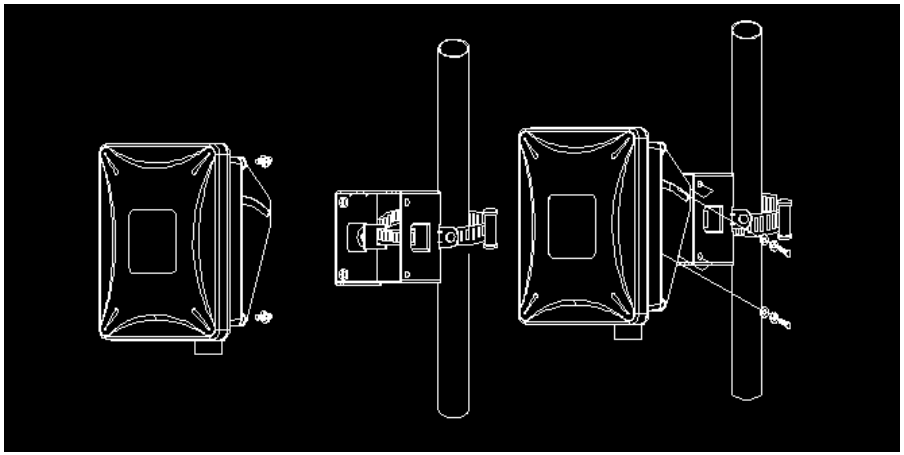
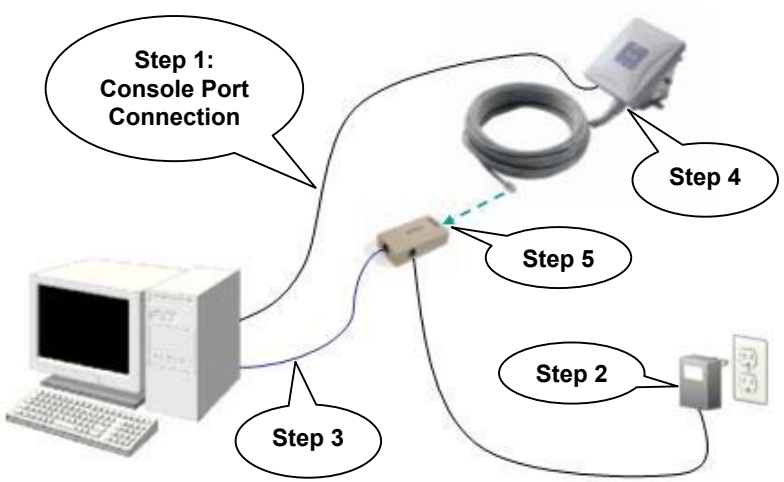


Figure 2.2.2

2.3 Preparing Installation

Before installing your Outdoor Wireless LAN system for your outdoor application in a hard-to-reach location, we recommend that you configure and test all the devices first.

For configuring the SF-3000, you need follow the quick steps below to power up the SF-3000:



Step 1 Attach the 1.8m (RS-232) null modem cable to the Serial Port Adapter. Connect the other cable end (DB9 female) to a terminal or a PC running a terminal emulation program.

Step 2 Plug the 24V power adapter into a power outlet or power strip. The Power LED on the top of the Inline Power Injector will light up.

Step 3 Run the cross over Ethernet cable (included in your package) from Data Input Port (at the bottom of the Inline Power Injector) to the Ethernet Port on a PC.

NOTE: This connection is required for setting up initial configuration information. After configuration is completed, this cable will be removed, and then you should run an Ethernet cable from Data Input Port (at the bottom of the Inline Power Injector) to the LAN connection (such as to a hub, bridge or directly into a patch panel).

Step 4 Use one direct Ethernet cable to plug one RJ-45 Ethernet connector into the Ethernet port at the bottom of the SF-3000.

Step 5 Plug another RJ-45 Ethernet connector (the other end of the Ethernet cable) into the Power & Data Output Port on the top of the Inline Power Injector.

When the SF-3000 receives power over the Ethernet cable, the SF-3000 will start its boot sequence and the Active LED on the top of the Inline Power Injector will light up.

You can configure the SF-3000 using the HTML browser, such as Internet Explorer or Netscape Navigator from a remote host or PC.

2.4 Basic Configuration

2.4.1 What you need to know

The SF-3000 can be configured into two operation roles:

Wireless Access Bridge and ***Wireless Client Router***

The SF-3000 is shipped with default configuration is as a bridge between an Ethernet and Wireless network. Users simply need to attach the SF-3000 to your wired LAN. If users would like to configure the SF-3000, please refer to the following procedures.

2.4.2 Basic Configuration Steps

This section will describe a 5-step configuration to setup your SF-3000 workable.

1. Select an operation mode for your SF-3000 on the web page "/**General Config/System/**", and click **FINISH** to refresh this page.
2. Modify the factory-set default parameters on the web page "/**General Config/System/**", and click **FINISH** to save your changes.
3. Modify the factory-set default parameters on the web page "/**General Config/Wireless/**", and click **FINISH** to save your changes.

4. (Optional) Modify others parameters on the web page "/**General Config/**", and click **FINISH** to save your changes.
5. Move on page "/***Utility/Administration/"***, select the ***Save then Restart*** and then click **FINISH** to take effect the previous configuration changes.

2.4.3 Logging into the Web Interface

The SF-3000 supports access to the configuration system through the use of an HTTP Interface (web browser).

- Web Configuration

Before configuring the SF-3000, you need to know the IP Address assigned to the unit. When shipped from the factory, the IP Address (192.168.5.99) was assigned to the SF-3000 by default. **To start a web connection use:**
http://192.168.2.1

- Identify the IP Address assigned to the unit

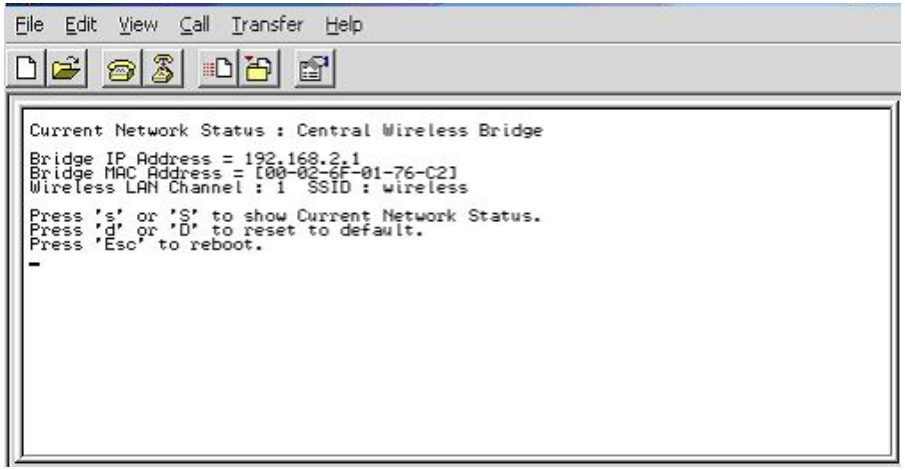
However, the IP Address may be changed and you cannot connect the unit using the default IP Address. In this case, you must identify the SF-3000 IP Address before configuration. To identify the IP Address, you can use the Serial Port to gain access the current network status.
To start a Serial Port connection:

1. Attach a serial data (RS-232) cable to the Serial Port Adapter. Connect the other cable end to a terminal or a PC running a terminal emulation program. Use a 9-pin female to 9-pin female NULL Modem cable.
2. Set the terminal to 115200 baud rate, None Parity, 8 data bits, 1 Stop bit, and ANSI compatible.
3. Running a terminal emulation program on your PC, such as ***Hyper Terminal***, and then set the following connection properties:

- Click the **Start icon > Program > Accessories > Communication > Terminal**.
- Create a new connection file, and then select a Com Port <*COM1, COM2, etc., depending on your PC*> with ***115200*bps / 8-bits / 1-stop**.
- Click the properties icon in the **Tool Bar > setting > select Emulation terminal *VT100* > ok**.

4. Reboot or turn on your SF-3000.

5. When the SF-3000 is powered up, the "Current Network Status" will be displayed as shown in following:



- Web Access Procedures

Once you identify the IP Address assigned to your SF-3000, use your web browser to configure the SF-3000 through the HTTP Interface.

The following procedure explains how to configure each item.
1. Open your browser and enter the IP Address
2. Press **ENTER** and the SF-3000 ***Login*** screen appear as shown in following:

3. Enter **root** in the **User Name** and the **Password** fields. And then the web configuration user interface screen appears as shown in following:

- Web Configuration Structure

The web configuration user interface be grouped in a tree structure, and contains the following settings or information:

▽ General Configuration
- System
- TCP/IP
  - — Virtual Server
  - — SNMP
- Wireless
- Security
  - — MAC Filter

▽ Running Status
- System Info
- Statistic Info
- Wireless Link Info

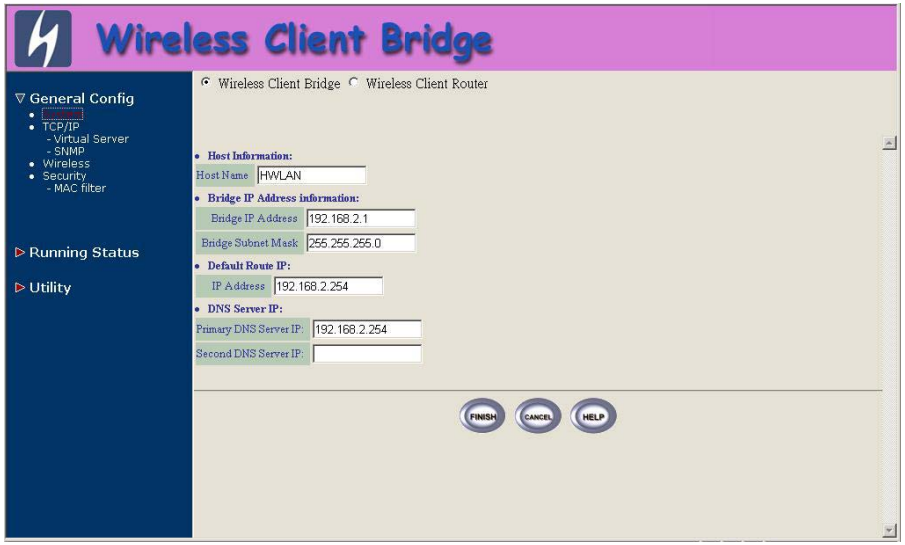
▽ Utility
- Software Upgrade
- Administration

Move through the tree by clicking on an icon to expand or collapse the tree. The nodes on the tree represent web pages that allow you to view and modify the parameters.

2.4.4 Set SF-3000's Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP

- Operation Mode

When setting up SF-3000, you have to decide which Operation Mode that your SF-3000 works. This feature is available in the "/**General Config/System/**" page as shown in following:



- Host Information

The Host Name is not an essential setting, but it helps identify the device in network. Use this setting to assign a name to the device.

- Bridge IP Address Information

Use this setting to assign or change the bridge's IP address.

- Bridge Subnet Mask

Enter an IP subnet mask to identify the sub network so the IP address can be recognized on the LAN.

- Default Route IP

Enter the default Gateway IP Address.

- DNS Server IP

Enter the Primary/Secondary DNS Server IP Address.

After that, click **FINISH** at the bottom of this page to complete the modification of this page.

2.4.5 Set Wireless Encryption for Wireless Interface

The SF-3000 supports 64-bit and 128-bit encryption:

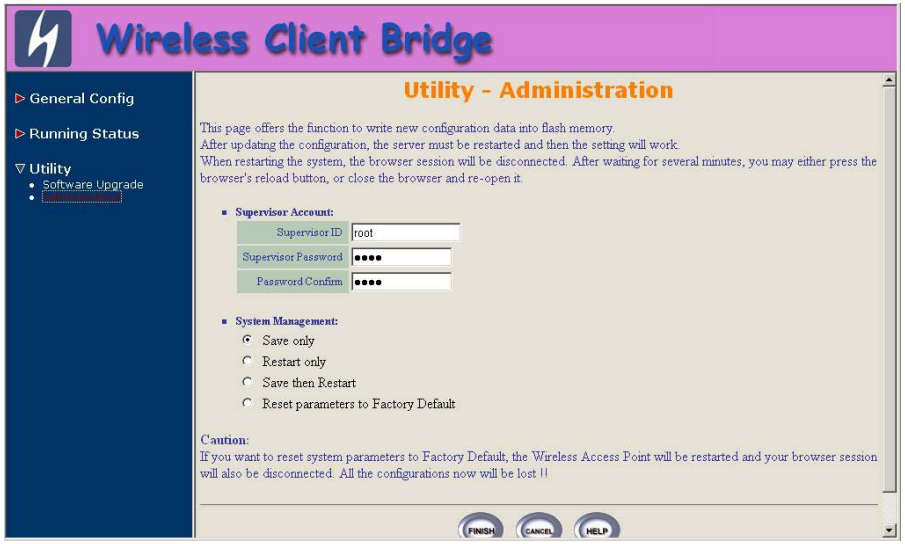
For **64-bit** encryption, an encryption key is 10 hexadecimal characters (0-9 and A-F) or 5 ASCII characters.

For **128-bit** encryption, an encryption key is 26 hexadecimal characters or 13 ASCII characters.

Modify the WEP encryption parameters on the web page "/**General Config/Woreless/**", Enter 1~15 characters into the **WEP Key** field, and then click **KeyGen** to generate the WEP64 or WEP128 key patterns.

2.4.6 Change Supervisor Account & Password

Click ***Utility*** > ***Administration.*** The following figure shows the **Utility/ Administration** page.



- Supervisor Account

Change the supervisor's user name & password in the Supervisor Account field, and click **FINISH**. To take effect the previous configuration changes.

- Apply the New Settings

1. Click ***Utility*** > ***Administration,*** select the ***Save then Restart*** to apply the new configuration settings.

2. Click **FINISH**. To take effect the previous configuration changes.

Hint: It takes about 10 seconds, to complete the restart process.

2.4.7 Upgrade the Firmware

- Setup your TFTP Server

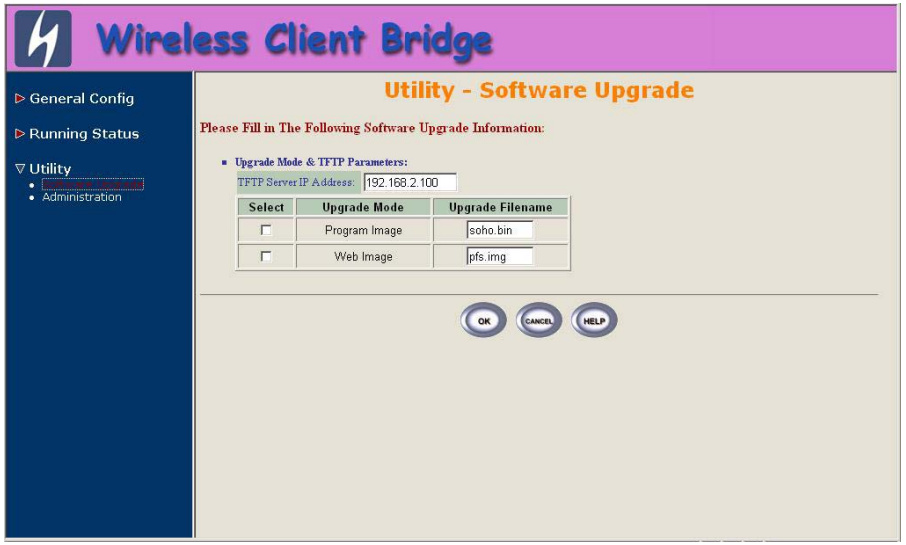
The Trivial File Transfer Protocal (TFTP) Server allows you to transfer files across a network. You can download the firmware files for SF-3000 upgrades.
After the TFTP Server is installed, make sure you have the proper TFTP Server IP address, the proper SF-3000's firmware files, and that the TFTP Server is operational.

- Update the Firmware using the TFTP method

1. Click ***Utility,*** select ***Software Upgrade*** page as shown in following figure, and then you can use TFTP to upgrade your SF-3000. In here, you must specify the ***TFTP server IP*** and select which file you want to upgrade it (***Program image, Web image***), then click **OK** button to start the TFTP upgrade process.

2. If the upgrade process is success, the SF-3000 will apply the new settings and start rebooting right away.

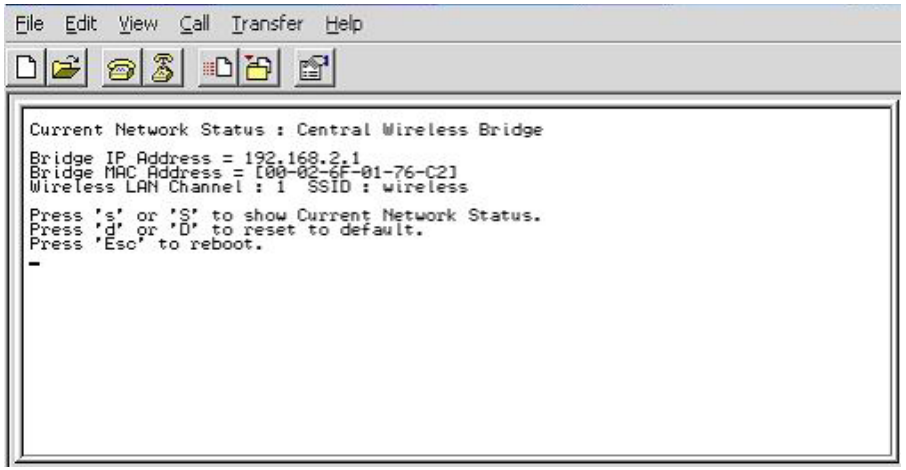
Hint: You must set up a TFTP Server and this server must contain the latest new image files.



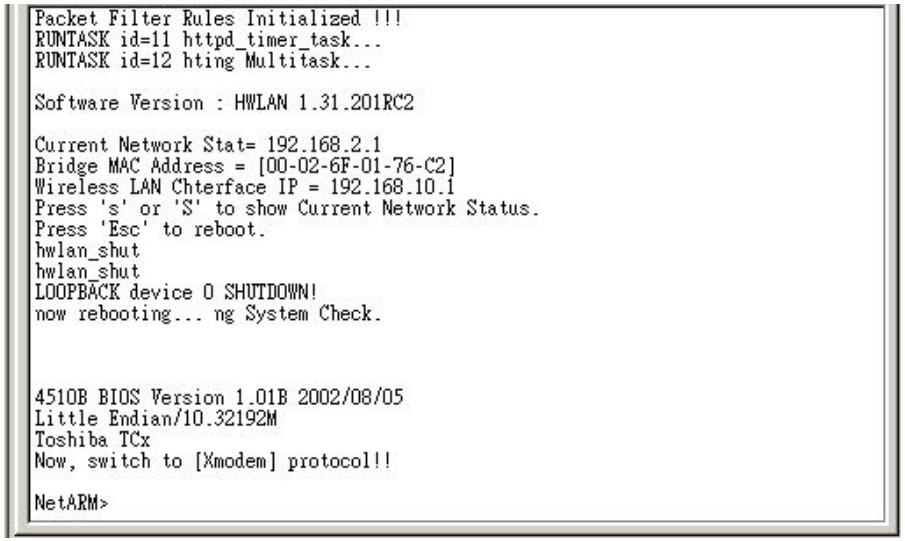
- Upgrade the Firmware using RS-232 console

Please refer to 2.5.3, it will introduce how to use RS-232 console in ***- Identify the IP Address assigned to the unit***.

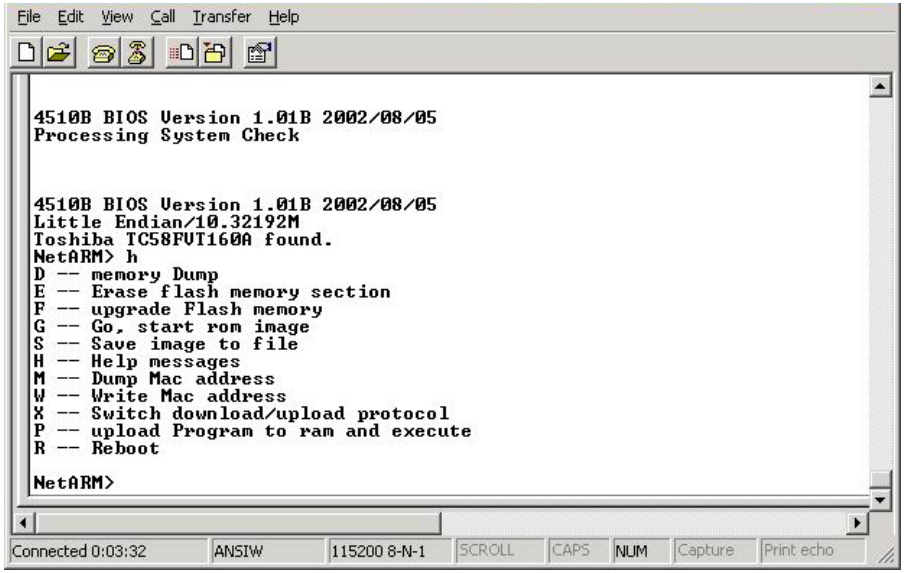
If the connection is ok, when the SF-3000 is powered up, the “Current Network Status” will be displayed as shown in following:



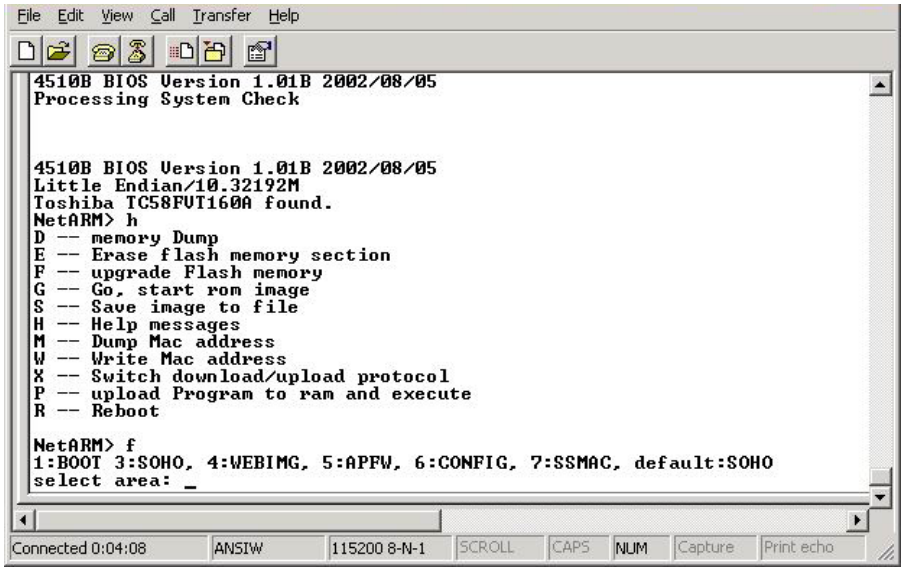
Press “**Esc**” keystroke to reboot the SF-3000 and during the boot process, press “**x**”, then it will display prompt character **NetARM>** as shown in following figure:



Press “h” keystroke, it will display related commands as shown in following figure:



Select “**F -- upgrade Flash memory**” and it will display upgrade items for selection as shown in following figure.



Firstly, select “**3:SOHO**” and then select “**4:WEBIMG**” to update the firmware files one by one.

After you press “**3**” keystroke and make sure the window start to display “C” character continued, meanwhile click **Transfer** and select the new firmware files (soho.bin), then press OK to start to transfer file to SF-3000. After the upgrade finished, remember to press “**R**” keystroke to reboot the sytem.

The following is to select “**4**” to upgrade WEBIMG file. The procedures are all the same with upgrading SOHO file, but you should select (pfs.img) correctly for WEBIMG file upgrade.

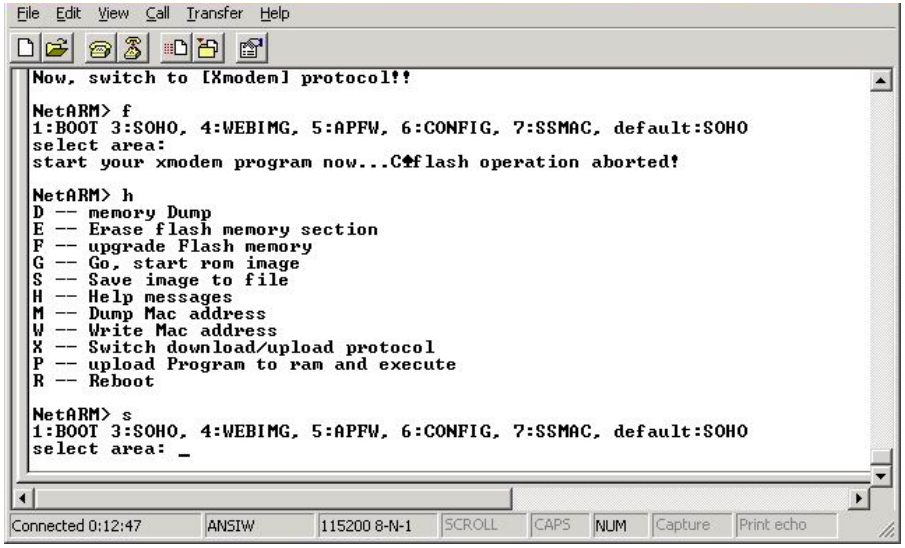
Note : The default transfer protocol is using “Xmodem”, so please make sure you select correct protocol to download/upload files when you try to upgrade the SF-3000’s firmware files.

2.4.8 Back-up the SF-3000’s Configuration Files

After you have configured the SF-3000, you can back-up its configuration files. Then you can download the back-up files at a later date and return the SF-3000’s configuration to the settings specified in back-up files.

- Downloading Configuration Files

Just same with upgrade firmware procedures, after the prompt character **NetARM>** is displayed, select “**S – Save image to file**” and then select “**6:CONFIG**” to back-up the SF-3000’s configuration as shown in following figure. The back-up file will be saved as “CONFIG.IMG”.



- Uploading Configuration Files

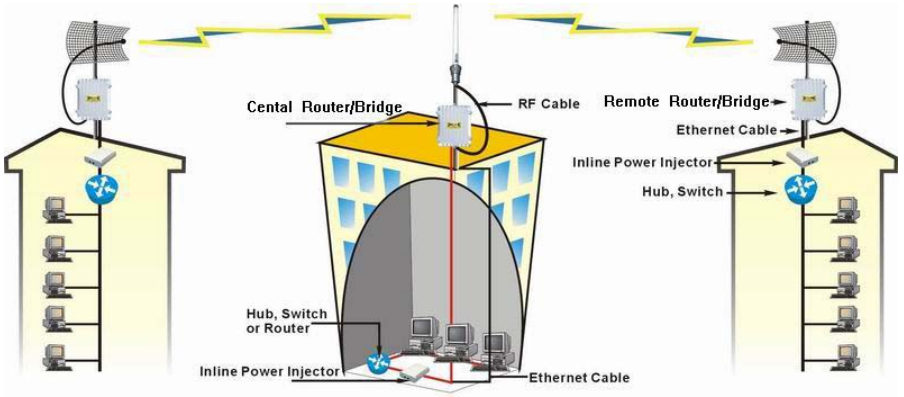
If you want to upload an configuration file to SF-3000, you should select “**F -- upgrade Flash memory**” and then select “**6:CONFIG**”. Make sure the window start to display “C” character continued, meanwhile click **Transfer** and select the CONFIG.IMG, then press OK to start to transfer file to SF-3000.

```
4510B BIOS Version 1.01B 2002/08/05
Little Endian/10.32192M
Toshiba TC58FVT160A found.
NetARM> f
1:BOOT 3:SOHO, 4:WEBIMG, 5:APFW, 6:CONFIG, 7:SSMAC, default:SOHO
select area: 6
start your zmodem program now...CCCCCCCCCCCCC
erasing 0x30000.... done!
programming.......... done!

NetARM> f
1:BOOT 3:SOHO, 4:WEBIMG, 5:APFW, 6:CONFIG, 7:SSMAC, default:SOHO
select area: 6
start your zmodem program now...CCCCCCCCCCCCCCCCCC65536

ata recieved ok.
start flash operation? (y/[N]) y
erasing 0x30000.... done!
programming.......... done!

NetARM>
```

Note : Remember to press "R" to reboot the system after you upload the configuration file to the SF-3000.

Chapter 3. Network Topologies

This section describes several main types of installations commonly implemented using the Outdoor Wireless System. This is by no means intended to be an exhaustive list of all possible configurations, but rather shows examples of some of the more common implementations. The SF-3000 can only be configured into Wireless Client Router/Bridge to accomplish the broadband wireless point-to-point, point-to-multipoint systems (as shown in following figuration).

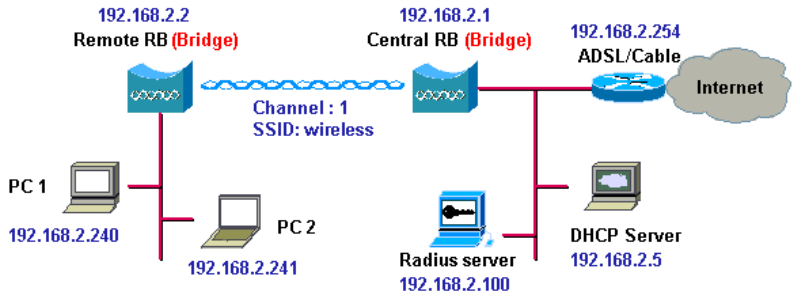


The SF-3000 can performed in router or bridge modes. In a Point-to-Multipoint topology, all communication between network systems is done through a centralized agent. In the Outdoor Wireless Router/Bridge product, the centralized agent is Central Router or Central Bridge and the individual network notes may be Wireless Client Router or Bridge.

To show some possibilities of Point-to-Multipoint topologies, the following examples are provided:

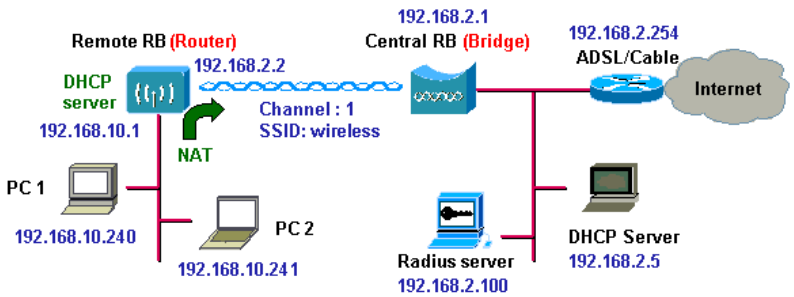
1. Wireless Access Bridge-to-Central Wireless Bridge
2. Wireless Client Router-to-Central Wireless Bridge
3. Wireless Access Bridge-to-Central Wireless Router
4. Wireless Client Router-to-Central Wireless Router

3.1 Wireless Access Bridge-to-Central Wireless Bridge



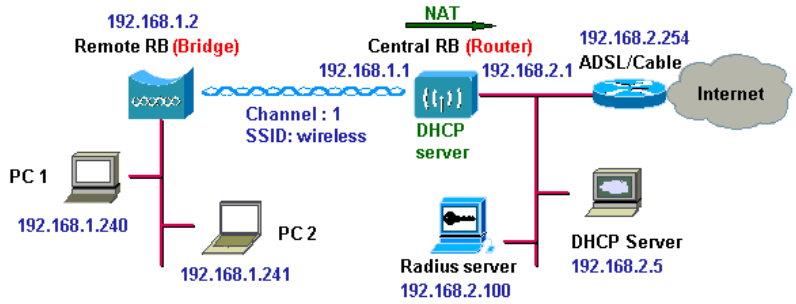
1. **Set the Central RB as a bridge (***bridge IP address is 192.168.2.1***).**
2. **Set Wireless parameters on Central RB: Channel (***1***) and SSID (***wireless***)**
3. **Set the Remote RB as a bridge (***bridge IP address is 192.168.2.2***).**
4. **Set Wireless parameters on Remote RB: Channel (***1***) and SSID (***wireless***), these parameters must same with Central RB.**
5. **Left side subnet is transparent to the right side.**
6. **DHCP server assign IP address to PC1 and PC2**

3.2 Wireless Client Router-to-Central Wireless Bridge



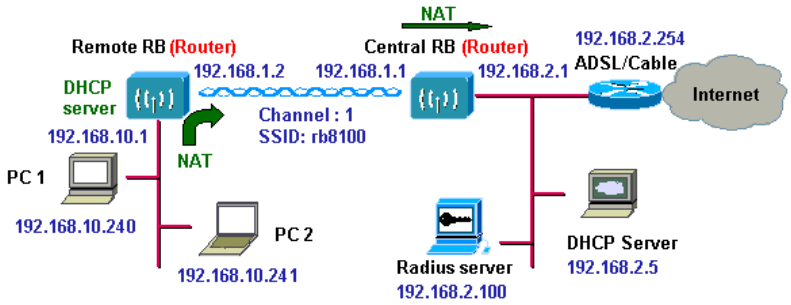
1. **Set the Central RB as a bridge (***bridge IP address is 192.168.2.1***).**
2. **Set Wireless parameters on Central RB: Channel (***1***) and SSID (***wireless***).**
3. **Set the Remote RB as a Router (***Wireless Interface IP is 192.168.2.2, Ethernet Interface IP is 192.168.10.1, must turn on* ***NAT*** *on* ***Wireless*** *Interface, default route is 192.168.2.254***).**
4. **Set Wireless parameters on Remote RB: Channel (***1***) and SSID (***wireless***), these parameters must same with Central RB.**
5. **Set the DHCP server service on the Remote RB and apply it on Ethernet Interface.**
6. **The Remote RB assign IP address to PC1 and PC2**

3.3 Wireless Access Bridge-to-Central Wireless Router



1. **Set the Central RB run as a Wireless Router (***Wireless Interface IP is 192.168.1.1, Ethernet Interface IP is 192.168.2.1, must turn on* ***NAT*** *on* ***Ethernet*** *interface, default route is 192.168.2.254***).**
2. **Set Wireless parameters on Central RB: Channel (***1***) and SSID (***wireless***)**
3. **Set the DHCP server service on the Central RB and apply it on Wireless Interface.**
4. **Set the Remote RB as a Bridge (***Bridge Interface IP is 192.168.1.2***).**
5. **Set Wireless parameters on Remote RB: Channel (***1***) and SSID (***wireless***), these parameters must same with Central RB.**
6. **The Central RB assign IP address to PC1 and PC2**
7. **The operator can also turn off NAT behavior on Central RB and two subnets are transparent.**

3.4 Wireless Client Router-to-Central Wireless Router



1. **Set the Central RB run as a Wireless Router (***Wireless Interface IP is 192.168.1.1, Ethernet Interface IP is 192.168.2.1, default route is 192.168.2.254***).**
2. **Set Wireless parameters on Central RB: Channel (***1***) and SSID (***wireless***).**
3. **Set the Remote RB as a Wireless Router (***Wireless Interface IP is 192.168.1.2, Ethernet Interface IP is 192.168.10.1, default route is 192.168.1.1***).**
4. **Set Wireless parameters on Remote RB: Channel (***1***) and SSID (***wireless***), these parameters must same with Central RB.**
5. **Set the DHCP server service on the Remote RB and apply it on Ethernet Interface.**
6. **The Remote RB assigns IP address to PC1 and PC2.**

The operator can also turn off NAT behavior on Central RB and turn on NAT behavior on Remote RB. In this case, any outgoing packets will transfer to 192.168.1.2.

- **Remote RB:** turn on NAT on Wireless Interface.

The operator can also turn on NAT behavior on Central RB and turn on NAT behavior on Remote RB.

- **Central RB:** turn on NAT on Ethernet interface.
- **Remote RB:** turn on NAT on Wireless Interface.

Chapter 4. Network Parameters

4.1 IP Configuration

The IP Configuration method is different in each Operating Mode. And you can refer to following descriptions to know the details:

Wireless Client Bridge

Select the Wireless Access Bridge mode, and then enter the IP Address manually into the **Bridge IP Address** field.

- Bridge IP Address
Use this setting to assign or change the bridge's IP address.

After that, click **FINISH** at the bottom of this page to complete the modification of IP address.

Wireless Client Router

In this mode, you can assign an Wireless and Ethernet IP address to the SF-3000 manually.

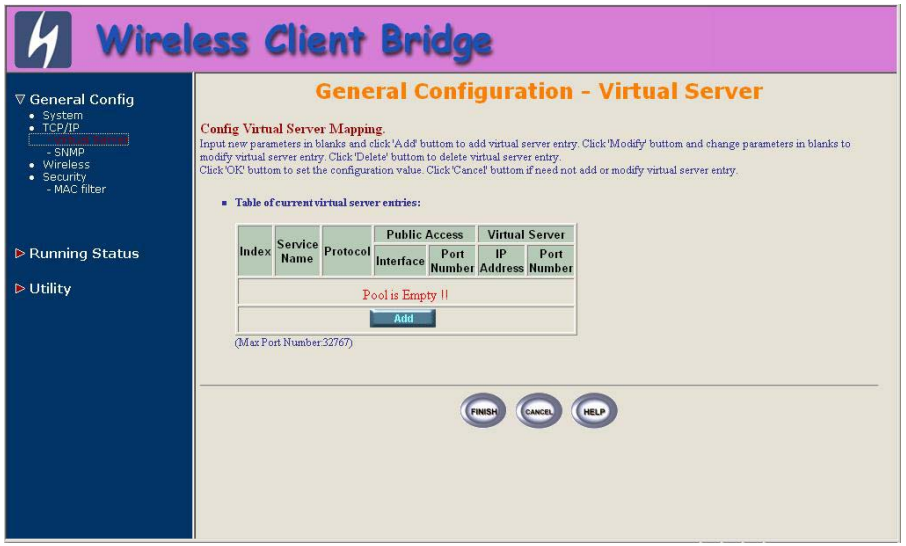
- NAPT
This function allows home users and small businesses to connect their network to the Internet cheaply and efficiently. You have to **Enable** it to allow the subscribers to connect to the Internet in this mode.

After that, click **FINISH** at the bottom of this page to complete the IP address modifications.

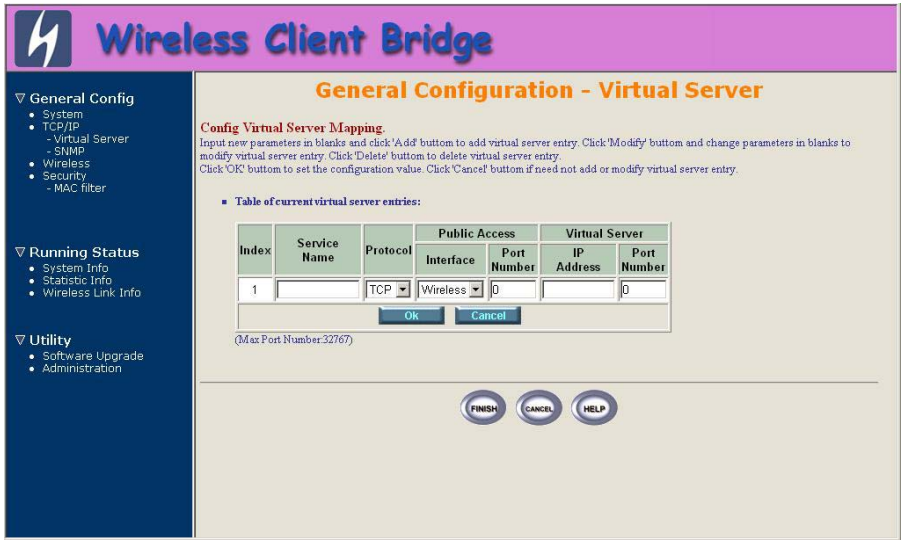
4.2 Virtual Server

Sometimes, the operator can expose the internal servers on the local intranet to the public Internet. For this, you must create the Virtual Server Mapping for these invisible internal servers.

Select the ***"/General Config/ TCP/IP/Virtual Server"***, and then the ***Virtual Server*** screen appears. The following figure shows the current virtual server entry table. (***Default Virtual Server Mapping pool is empty***)



1. Click **Add**, the Virtual Server Entry Edit page appears as following figure.



2. To edit the Virtual Server Entry, specify all the entry fields to allow Internet user to access the Internal servers.

Alias name of this internal server, such as FTP.

- Access Interface

Indicate the translation occurs on which interface (Wireless interface / Ethernet interface), such as Ethernet.

- Protocol

Indicate which protocol (TCP/UDP) you want to translate from outside to internal server, such as TCP.

Public Access Port number: Indicate which socket port (1 ~ 65535) you want to translate from outside to internal server, such as 21.

Virtual Server IP address: Specify the private IP address of the internal server, such as 192.168.1.100.

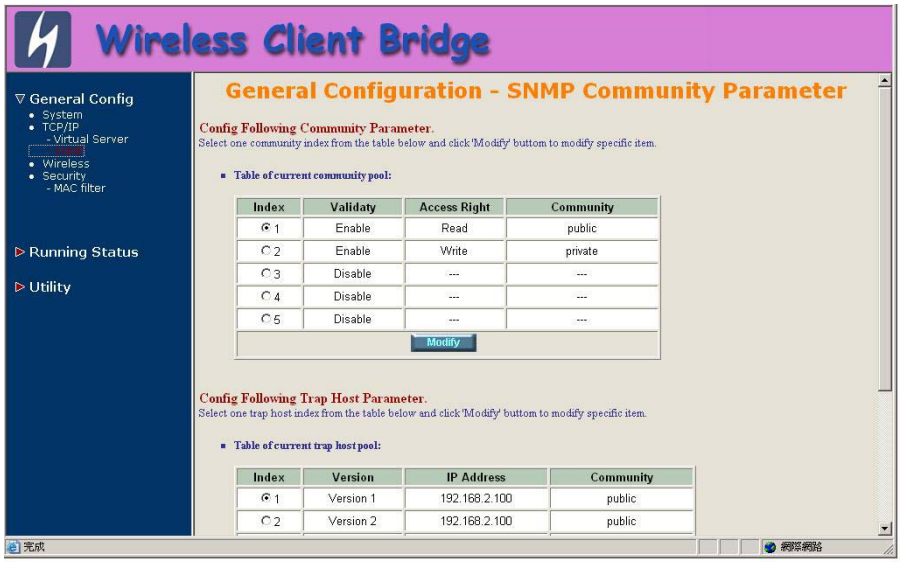
Virtual Server Port number: Specify the socket port (1 ~ 65535) of the internal server, such as 21.

3. Click **OK**. The Virtual Server Entry Table appears with the entries list.
4. To modify or delete a virtual server entry, click the select button beside the entry index number and click [ ] or [ ].
5. To add another entry to the Virtual Server Mapping Pool, repeat step 1 through step 3.

1. When you have included all the entries you need, click **FINISH**.

4.3 Configure SNMP

Select the "**/General Config/ TCP/IP/SNMP**", and then the SNMP screen appears. The following figure shows the current SNMP community pool and trap host pool.



4.3.1 Configure Community Pool

The SNMP Community Pool has five entries.

1. To modify a entry, click the select button beside the entry index number and then click **Modify**, the configuration page appears as following figure.

2. Specify the Validity, Access Right and Community field.

- Validity
Select **Enable** or **Disable** to control this community.

- Access Right
Select a command from the pull down menu for this field.

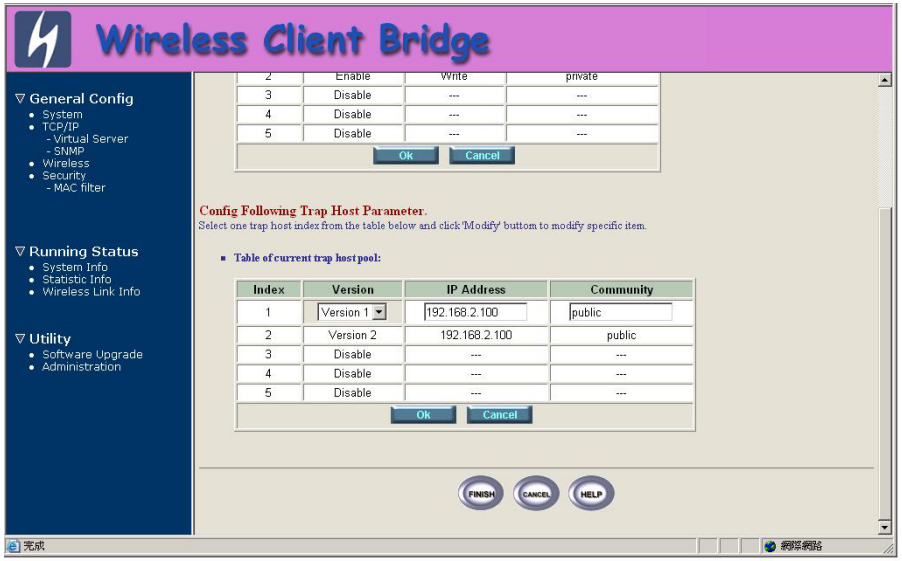
- Community
Enter the password related the Access Right in this field.

3. Click **OK**. To refresh the current community pool.
4. To modify another community entry to the current community pool, repeat step 1 through step 3.
5. When you have modified all the entries you need, click **FINISH**.

4.3.2 Configure Trap Host Pool

The Trap Host Pool has five entries.

1. To modify a entry, click the select button beside the entry index number and click **Modify**. The configuration page appears as following figure.



2. Specify the Version, IP Address and Community field.

- Version
Select **Disable, Version 1** or **Version 2** to control this trap host.

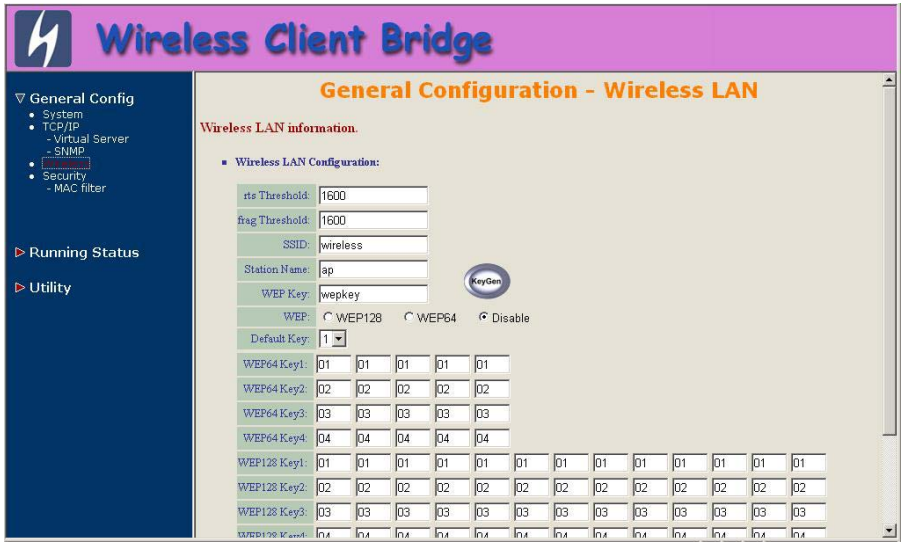
- IP Address
Enter the Trap Host IP Address.

- Community
Enter the password in this field.

3. Click **OK**. To refresh the current trap host pool.
4. To modify another trap host entry to the current trap host pool, repeat step 1 through step 3.
5. When you have modified all the entries you need, click **FINISH**.

4.4 Configure Wireless related parameters

Select "***/General Config/Wireless"***. The Wireless LAN information page appears as following figure.
In here, enter the ***Channel*** (default is ***1***), ***rts Threshold*** (default is ***1600***), ***frag Threshold*** (default is ***1600***), ***SSID*** (default is ***wireless***) and ***Station Name*** (default is ***ap***) that are suitable for your radio network and then you can clicked radio button to disable WEP or enable 64/128 bit ***WEP services*** (default is ***disable***), if WEP is enabled, you must input corresponded ***Default Key index*** and ***WEP Key*** and then click **KeyGen** to generate the WEP64 & WEP128 key patterns. After that, click **FINISH** at the bottom of this page to complete the modification.



- rts Threshold

This setting determines the packet size at which the bridge issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the bridge and not each other. Enter a setting ranging from **0 to 2339** bytes.

- frag Threshold

This setting determines the size at which packets are fragmented (sent as several pieces instead of as one block). Enter a setting ranging from **256 to 2338** bytes. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

- SSID

The **Service Set ID (SSID)** can be any alphanumeric, case-sensitive entry from **2 to 32** characters long. This string functions as a password to joint the radio network.

- Hide SSID

You use this setting to choose whether devices that do not specify an SSID are allowed to associate with the access point. With Yes selected, the SSID used by other devices must match exactly the AP's SSID.

- Deny Any

You use this setting to choose whether devices that specify **the well define SSID keyword 'ANY' or 'any'** are allowed to associate with the access point. With **Yes** selected, the SSID **'ANY' or 'any'** used by other devices are not allowed to associate with the access point

- Station Name

Enter any alphanumeric, case-sensitive entry.

- WEP Key

Enter 1~15 characters for 64 and 128 bits WEP KEY encryption, and then click **KeyGen** to generate the WEP64 & WEP128 key patterns.

- WEP

You can **Disable** or **enable** 64/128 bit WEP services here.

- Default Key

Select an encryption key from the pull down menu.

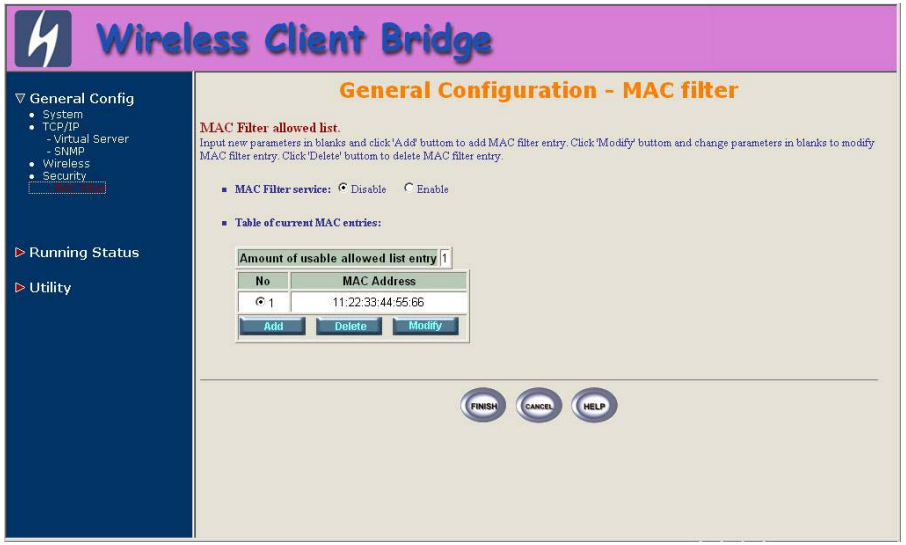
- WEP64 Key1~4 & WEP128 Key1~4

The keys in these fields can be generated automatically by **KeyGen** function. For 40-bit encryption, enter 10 hexadecimal digits; for 128-bit encryption, enter 26 hexadecimal digits. Hexadecimal digits include the numbers 0 through 9 and the letters A through F. Your 40-bit WEP keys can contain any combination of 10
of these characters; your 128-bit WEP keys can contain any combination of 26 of these characters. The letters are not case-sensitive.

4.5 Security

4.5.1 MAC based Access Control

1. Click ***General Config***, select ***MAC Filter*** page, and choice the MAC Filter services is ***Enable*** or ***Disable*** as shown in following figure.



You can specify the MAC address of a wireless client station. All MAC entries in the MAC address table are permitted to connect into the RB. You can also click ***ADD***, ***DELETE***, ***MODIFY*** button to maintain this MAC address table. After that, click **FINISH** at the bottom of this page to complete the modification of this page.

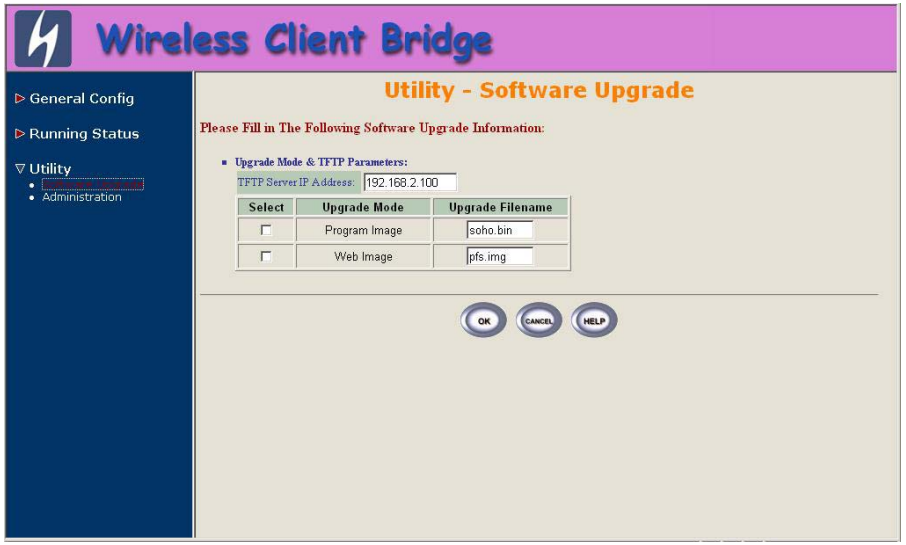
4.6 Utility

4.6.1 Software Upgrade

1. Click ***Utility***, select ***Software Upgrade*** page as shown in following figure, and then you can use TFTP to upgrade your AP. In here, you must specify the ***TFTP server IP*** and select which file you want to upgrade it (***Program image, Web image***), then click ***OK*** button to start the TFTP upgrade process.

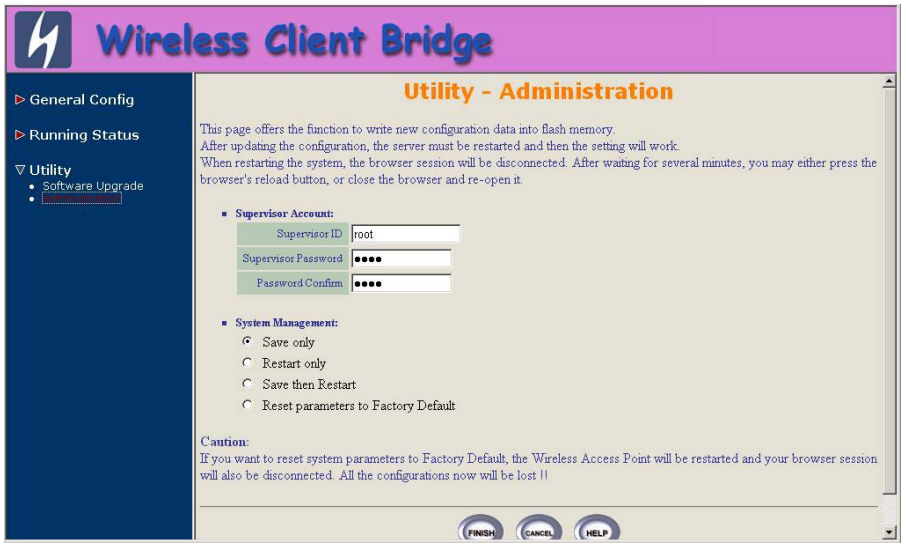
2. If the upgrade process is success, the AP will apply the new settings and start rebooting right away.

Hint: You must set up a TFTP server and this server must contain one latest new image.



4.6.2 Administration

1. Click ***Utility***, ***Administration.*** The following figure shows the **Utility – Administration** page.



- Supervisor Account

Change the supervisor's user name & password in the Supervisor Account field, and Click **FINISH**. To take effect the previous configuration changes.

- Apply the New Settings

Click ***Utility***, ***Administration,*** select the ***Save then Restart*** to apply the new configuration settings.

2. Click **FINISH**. To take effect the previous configuration changes.

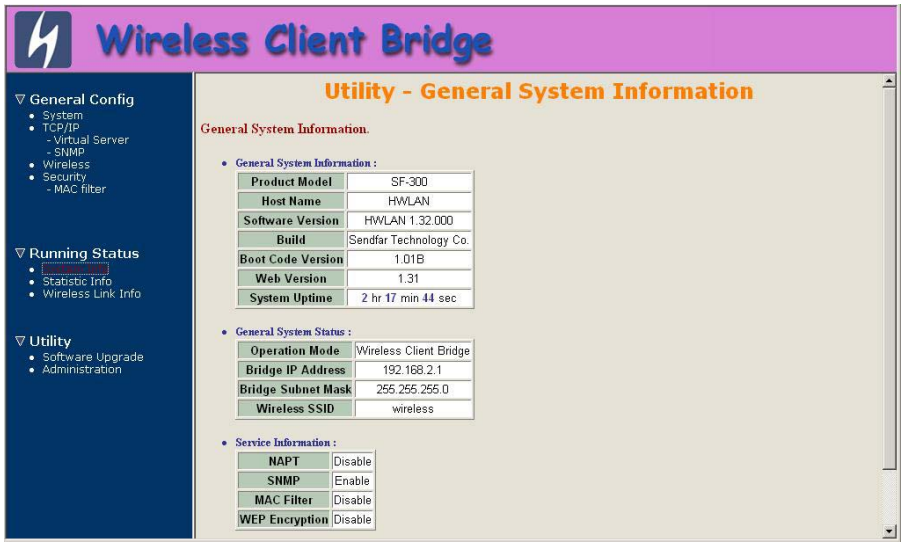
Hint: It takes about 10 seconds, to complete the restart process.

Chapter 5. Monitor Information

You can see the system running status and the some information on this window. Click the **Running Status** link on the left window, you can choose which function that you want to monitor.

5.1 System Information

Click **Running Status**, **System Info**. The following figure shows the **System Information** page.



In this page, you can see the system information and most running parameters.

- General System Information

This block displayed the Product Model, Host Name, Software Version, Build, Boot Code Version, Web Version, AP Firmware version and System Uptime.

- General System Status

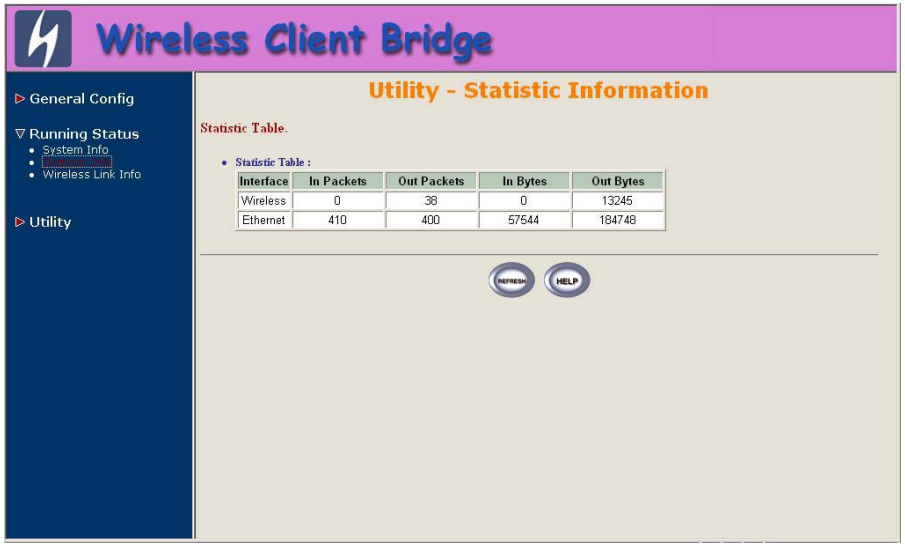
This block displayed the Operation Mode, Interface IP/Net mask and brief wireless parameters, if the operator turn on the DHCP or PPPoE services, you can also see the related information on here.

- Services Information

This block displayed which service is turn on or not. It is includes the NAPT, DHCP server, SNMP, 802.1x access control, MAC Filter and WEP encryption.

5.2 Statistic Information

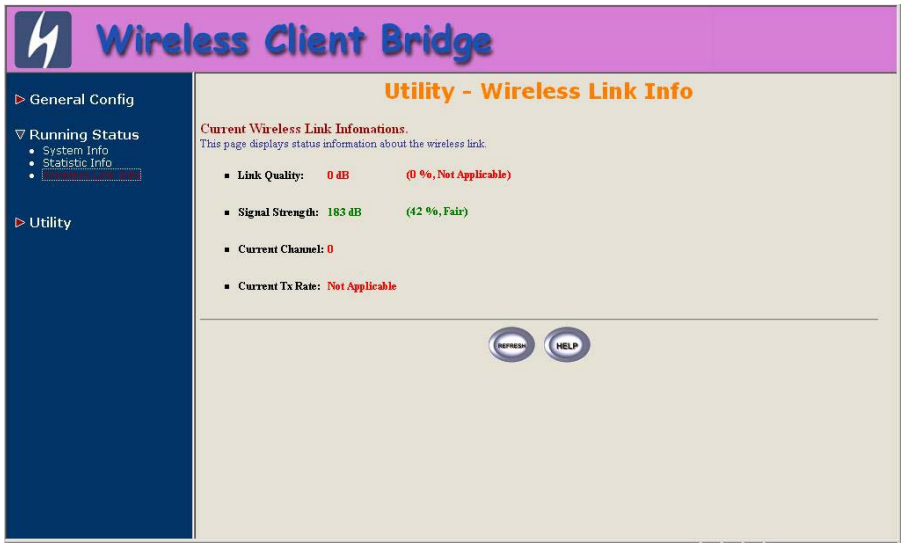
Click **Running Status**, **Statistic Info.** The following figure shows the **Statistic of Interface** page.



In this page, you can see the packet statistic of each interface, Wireless and Ethernet. This statistic table includes the **In Packets**, **Out Packets**, **In Bytes** and **Out Bytes**.

5.3 Wireless Link Information

This item only displayed on Remote RB mode.
Click **Running Status**, **Wireless Link Info**. The following figure shows the **Radio Link Information** page.



In this page, you can see four information about this radio link: **Link Quality**, **Signal Strength**, **Current used channel** and **Current Tx Rate**.

Chapter 6. Specifications

Hardware Specifications

- General

Radio Data Rate	11, 5.5, 2 and 1 Mbps, Auto Fall-Back
Client Interface	10Base-T Ethernet
Range (open environment)	300m @ 11 Mbps 400m @ 5.5Mbps 500m @ 2 Mbps 800m @ 1 Mbps
EMC Certifications	FCC Part 15 ETSI 300/328
Compatibility	Fully interoperable with IEEE802.11b compliant products
Power Supply	AC/DC Adapter：24V / 0.83A **(via AC power outlet 100~240V, 50~60Hz)** PoE：24V

- Network Information

Network Architecture	Infrastructure
Drivers	Windows 95/98/ME/2000/NT 4.0/XP
Access Protocol	CSMA/CA
Roaming	IEEE802.11b compliant
Security	64-/128-bit data encryption

Radio Specifications

Frequency Band	2.4 – 2.484 GHz
Radio Type	Direct Sequence Spread Spectrum (DSSS)
Modulation	CCK (11, 5.5Mbps) DQPSK (2Mbps) DBPSK (1Mbps)
Operation Channels	North America：11 Japan：14 Europe：13 Spain：2 France：4
Available Transmit Power Settings	23dBm (200 mW) 20dBm (100 mW)
Antenna	5dBi Omni rubber antenna 9dBi Flat Patch antenna 12dBi Flat Patch antenna (option)
Sensitivity @FER=0.08	11 Mbps < -85dBm 5.5 Mbps < -88dBm 2 Mbps < -91dBm 1 Mbps < -93dBm

Environmental

Temperature Range	0 to 55℃ (operating) -20 to 75℃ (storage)
Humidity (non-condensing)	5% to 95% typical

Physical Specifications

Dimensions	138.7mm x 104.0mm x 38.0mm
Weight	500g

Software Specifications

Protocol	✧ TCP/IP ✧ NAT/NAPT ✧ DHCP Client ✧ Virtual Server Mapping (NAT inbound server) ✧ 802.1d Transparent Bridging
Security	✧ 64-/128-bit WEP encryption ✧ MAC address based access control ✧ User authentication in Web-based Manager
Management	✧ Web-based Manager ✧ TelnetI configuration ✧ Console (RS-232) configuration ✧ SNMP v1

	✧ SNMP MIB-II ✧ Private MIB
Firmware upgrade	✧ TFTP (Trivial FTP) ✧ Xmodem, 1K Xmodem ✧ Zmodem

Chapter 7. Default Settings

7.1 General Configuration

7.1.1 System

Parameter	Description	Default Value
Host Name	Host name for the RB	HWLAN
Operation Mode	1. Wireless Access Bridge 2. Wireless Client Router	Wireless Access Bridge
Bridge IP Address	For Wireless Access Bridge with Operation Mode	192.168.2.1
Bridge Subnet Mask		255.255.255.0
Wireless Interface Address	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
NAPT Interface	1. Enable 2. Disable	Disable
Default Route IP	IP address of the gateway for default route when TCP/IP filtering	192.168.2.254
Primary DNS Server IP	IP addresses of the DNS Servers of your Local ISP	192.168.2.254
Second DNS Server IP		

7.1.2 Virtual Server

Parameter	Description	Default Value
Service Name	Specify the service for public access	NULL
Protocol	Select a protocol for public access	NULL
Public Access	Interface	NULL
	Port Number	NULL
Virtual Server	IP address	NULL
	Port Number	NULL

Note: (Maximum Entry: 10, Maximum Port Number: 32767)

7.1.3 SNMP

7.1.3.1 Table of SNMP Community Pool

Parameter		Description	
Index 1	Validity	Enable or disable the function of the corresponding community index	
Index 2			
Index 3			
Index 4			
Index 5			
Index 1	Access Right	Select the access right (Deny/Read/Write/Create) for SNMP Manager	
Index 2			
Index 3			
Index 4			
Index 5			
Index 1	Community	Specify the type of community (public or private) for SNMP Manager	
			private
Index 3			---
Index 4			---
Index 5			

7.1.3.2 Table of SNMP Trap Community Host Pool

Parameter		Description	Default Value
Index 1	Version	Select or disable the SNMP Version Version 1: MIB1 Version 2: MIB2	Version1
Index 2			Version2
Index 3			---
Index 4			---
Index 5			---
Index 1	IP Address	Specify the IP address of the SNMP Manager for SNMP Trap Report	192.168.2.100
Index 2			192.168.2.100
Index 3			---
Index 4			---
Index 5			---
Index 1	Community	Specify the type of community	public
		Manager	public
Index 3			---
Index 4			---
Index 5			---

7.1.4 Wireless LAN

Parameter	Description	Default Value
RTS Threshold	Set RTS (Request To Send) threshold value	1600
Fragmentation Threshold	Set fragmentation threshold value	1600
SSID	Wireless LAN service area identifier of the RB (case sensitive)	wireless
Hide SSID	Yes or No	No
Deny ANY	Yes or No	No
Station Name	Show the name of the AP	ap
WEP Key	Push the “KeyGen” button to generate the WEP key patterns automatically	wepkey
WEP	1. WEP128 2. WEP64 3. Disable	Disable
Default Key	Select a WEP key to encrypt each frame transmitted from the radio using one the of the 4 Keys from the Key Panel	1
Key Panel	When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. ***Note: each key must consist of hex digits, it means that***	

	only digit 0 -9 and letters A-F are valid entries. If entered incorrectly, program will not write keys to a driver.	

7.2 Utility

7.2.1 Software Upgrade

Parameter	Description	
TFTP Server IP Address	Specify the IP address of the TFTP server to upgrade the firmware of the RB	
Upgrade Filename	Program Image	
	Web Image	

7.2.2 Administration

Parameter	Description	Default Value
Supervisor ID	Supervisor's identity code	root
Supervisor Password	Supervisor's password	root
Password Confirm	Confirm the password again	root

Chapter 8. Regulatory Compliance Information

Radio Frequency Interference Requirements

This device complies with Part 15 of FCC Rules and Canada RSS-210.
Operation is subject to the following conditions:
This device may not cause harmful interference.
This device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement

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

This transmitter must not be co-located or operating in conjunction with any other antenna of transmitter.

Interference Statement

Federal Communication Commission Interference Statement□
This equipment has been tested and found to comply with the limits for a Class B digital device, □ pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection □ against harmful interference in a residential installation. This equipment generates, uses and can □ radiate radio frequency energy and, if not installed and used in accordance with the instructions, □ may cause harmful interference to radio communications. However, there is no guarantee that □ interference will not occur in a particular installation. If this equipment does cause harmful □ interference to radio or television reception, which can be determined by turning the equipment off □ and on, the user is encouraged to try to correct the interference by one of the following measures:□
□
-•Reorient or relocate the receiving antenna.□
-•Increase the separation between the equipment and receiver.□
-•Connect the equipment into an outlet on a circuit different from that□ to which the receiver is connected.□
-•Consult the dealer or an experienced radio/TV technician for help.□
□
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.□
FCC Caution: Any changes or modifications not expressly approved by the party responsible for □ compliance could void the user's authority to operate this equipment.□

Professional Installation

Per the recommendation of the FCC, the installation of high gain directional antenna to the system, which are intended to operated solely as a point-to-point system and whose total power exceeds +30dBm EIRP, require professional installation. It is the responsibility of the installer and the end user that the high power systems are operated strictly as a point-to-point system.

Systems operating as a point-to-multipoint system or use non directional antennas cannot exceed +30dBm EIRP power requirement under any circumstances and do not require professional installation.