

SF-3000

IEEE 802.11b Outdoor Wireless Client Bridge

User Manual

February 23, 2004

Version 1.01



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

Contents

CHAPTER 1.	INTRODUCTION	1
1.1	INTRODUCING THE SF-3000	1
1.2	PRODUCT FEATURES	1
1.3	PACKAGE CONTENTS	1
1.4	SYSTEM REQUIREMENTS	1
1.5	INLINE POWER INJECTOR (PoE)	2
CHAPTER 2.	INSTALLATION AND BASIC CONFIGURATION	3
2.1	BEFORE YOU START	3
2.2	LOCATE THE SF-3000 AND INLINE POWER INJECTOR PORTS	4
2.3	PREPARING INSTALLATION	6
2.4	BASIC CONFIGURATION	7
2.4.1	What you need to know	7
2.4.2	Basic Configuration Steps	7
2.4.3	Logging into the Web Interface	8
2.4.4	Set Operating Mode, IP Address, Subnet Mask, Default Route IP, DNS Server IP of SF-3000	11
2.4.5	Set Wireless Encryption for Wireless Interface	13
2.4.6	Change Supervisor Account & Password	13
2.4.7	Upgrade the Firmware	14
2.4.8	Back-up the SF-3000's Configuration Files	18
CHAPTER 3.	NETWORK TOPOLOGIES	20
3.1	WIRELESS CLIENT BRIDGE-TO-CENTRAL WIRELESS BRIDGE	21
3.2	WIRELESS CLIENT ROUTER-TO-CENTRAL WIRELESS BRIDGE	22
3.3	WIRELESS CLIENT BRIDGE-TO-CENTRAL WIRELESS ROUTER	23
3.4	WIRELESS CLIENT ROUTER-TO-CENTRAL WIRELESS ROUTER	24
CHAPTER 4.	NETWORK PARAMETERS	26
4.1	IP CONFIGURATION	26
4.2	VIRTUAL SERVER	27
4.3	CONFIGURE SNMP	30
4.3.1	Configure Community Pool	30
4.3.2	Configure Trap Host Pool	32
4.4	CONFIGURE WIRELESS RELATED PARAMETERS	34
4.5	SECURITY	37
4.5.1	MAC based Access Control	37
4.6	UTILITY	38

4.6.1	Software Upgrade	38
4.6.2	Administration	39
CHAPTER 5.	MONITOR INFORMATION	40
5.1	SYSTEM INFORMATION	40
5.2	STATISTIC INFORMATION	42
5.3	WIRELESS LINK INFORMATION	43
CHAPTER 6.	SPECIFICATIONS	44
6.1	HARDWARE SPECIFICATIONS	44
6.2	SOFTWARE SPECIFICATIONS	45
CHAPTER 7.	DEFAULT SETTINGS	47
7.1	GENERAL CONFIGURATION	47
7.1.1	System	47
7.1.2	Virtual Server	47
7.1.3	SNMP	48
7.1.3.1	Table of SNMP Community Pool	48
7.1.3.2	Table of SNMP Trap Community Host Pool	48
7.1.4	Wireless LAN	49
7.2	UTILITY	50
7.2.1	Software Upgrade	50
7.2.2	Administration	50
CHAPTER 8.	REGULATORY COMPLIANCE INFORMATION	51

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 remote bridge mode, and connects SendFar RB-8110 Outdoor Wireless Router Bridge to construct point-to-point as well as point-to-multipoint topologies, for maximum flexibility in configuring building-to-building networks to WISP.

1.2 Product Features

- ✓ Outdoor enclosure in compliance with IP67
- ✓ RF transmit power 100mW (20dBm) with -85dBm Rx sensitivity @ 11Mbps data rate
- ✓ Embedded 9dBi patch directional antenna
- ✓ Support 24VDC 0.8A Power-over-Ethernet
- ✓ NAT/NAPT and Virtual Server Mapping support
- ✓ MIB-II and Private MIB support
- ✓ MAC address based access control

1.3 Package Contents

The product package contains the following items.

1. One (1) SF-3000 Outdoor Wireless Client Bridge unit
2. One (1) 100~240VAC, 50~60Hz AC/DC adapter with wall-mount plug and DC plug power cord
3. One (1) 24VDC, 830mA Inline Power Injector (PoE)
4. One (1) 30m RJ-45 CAT-5 Ethernet cable
5. One (1) 1.8m RS-232 null modem console cable
6. One (1) 1.8m grounding wire
7. One (1) User manual CD-disc
8. One (1) wall/mast mounting kit, including one (1) band clamp

1.4 System Requirements

Installation of the Outdoor Wireless Client Bridge requires the following:

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) delivers both data and power to SF-3000 unit via a signal Ethernet cable, and gives the following benefits to improve the performance vs. installation cost ratio.

1. This works great in areas where you may not have power and/or Ethernet easily accessible, like house roof.
2. This also allows you to place the SF-3000 unit closer to the antenna, more easily 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 of 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 Outdoor Wireless Client Bridge unit
2. AC/DC adapter 100~240VAC, 50~60Hz with wall-mount plug and DC plug power cord
3. Inline Power Injector (PoE) 24VDC, 830mA
4. RJ-45 CAT-5 Ethernet cable 30m
5. RS-232 null modem console cable 1.8m
6. Grounding wire 1.8m
7. User manual CD-disc
8. Wall/mast mounting kit, including one (1) band clamp



2.2 Locate the SF-3000 and Inline Power Injector Ports

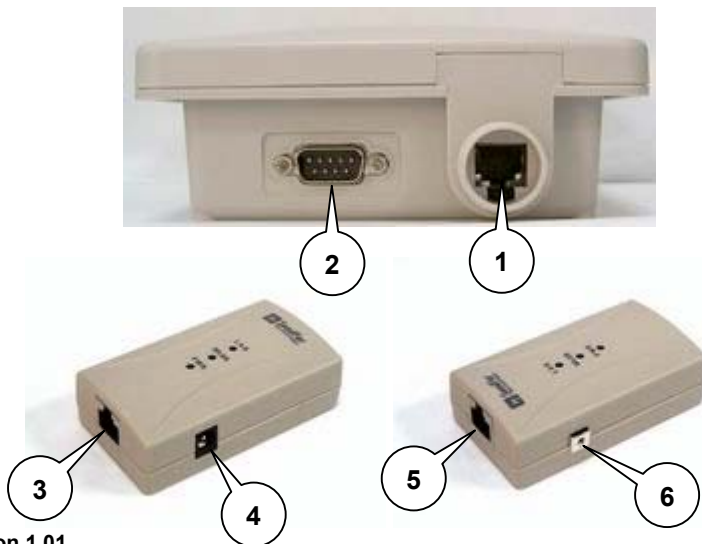
■ Interface on the SF-3000 Unit

- ✓ **Ethernet Port 1** for connecting the 30m RJ-45 CAT-5 Ethernet cable.
- ✓ **RS-232 Console Port 2** for connecting the 1.8m RS-232 null modem console cable.

■ Interface on the Inline Power Injector

- ✓ **Data Input Port 3** for connecting cross-over Ethernet Cable to PC or straight Ethernet cable to Hub Switch Router.
- ✓ 110~240VAC, 50~60Hz AC/DC power adapter **DC Input Port 4**
- ✓ **Power & Data Output Port 5** for connecting the 30m RJ-45 CAT-5 Ethernet Cable.
- ✓ **Grounding Port 6**.

NOTE: The cross-over or straight type Ethernet cable is not provided in SF-3000 shipping package as an accessory. User can find one from computer store in accordance with the length required for indoor deployment.



■ Mount SF-3000 on A Wall/Pole

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**.

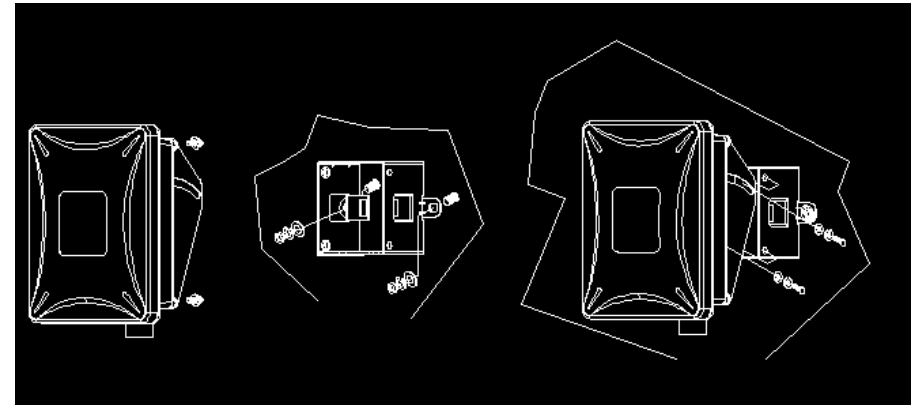


Figure 2.2.1

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

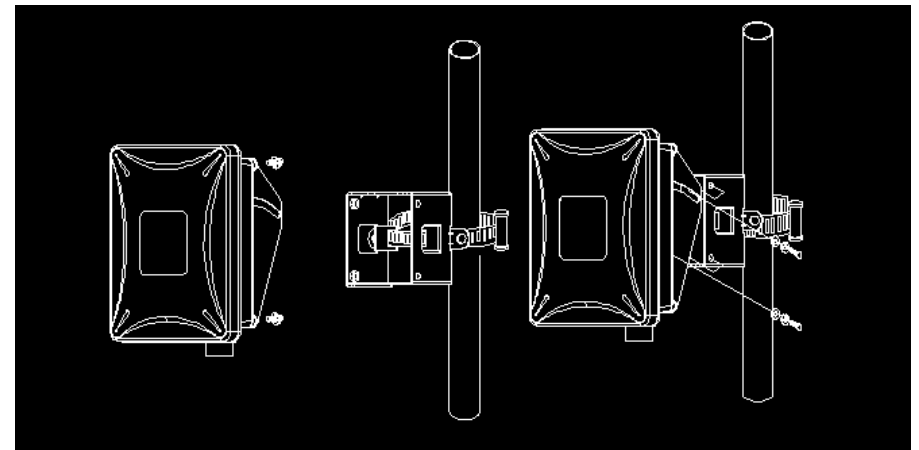
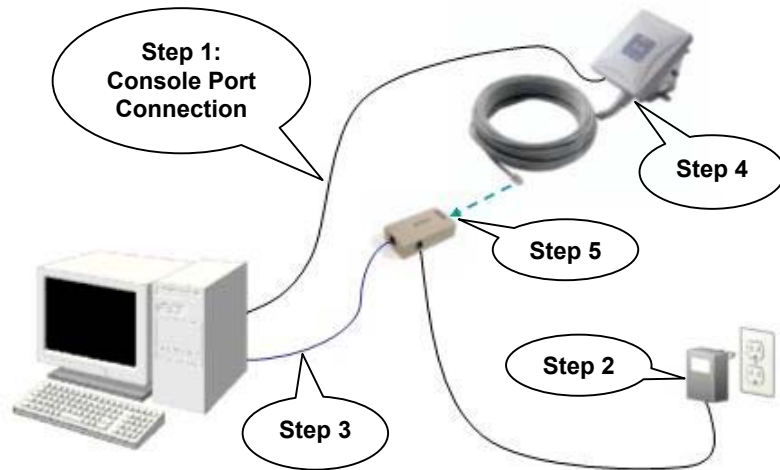


Figure 2.2.2

2.3 Preparing Installation

Before installing SF-3000 for the outdoor application in a hard-to-reach location, we recommend to configure and test all the devices first.

For configuring the SF-3000, please follow the quick steps below to power up the SF-3000.



Step 1 Attach the 1.8m RS-232 null modem console cable to the **Console Port** on the SF-3000 unit (refer to [page 4](#)), and the other end (DB9 female type) to a terminal or a PC running a terminal emulation program.

Step 2 Plug the DC plug of the AC/DC power adapter into the **DC Input Port** of Inline Power Injector and the wall-mount plug into a power outlet or power strip (refer to [page 4](#)). The Power LED on the Inline Power Injector will light up.

Step 3 Run the cross-over type uplink Ethernet cable from **Data Input Port** (refer to [page 4](#)) to the Ethernet port on a PC.

NOTE: This connection is required for setting up initial configuration information. After configuration is completed, the RS-232 null modem console cable shall be removed, and run a cross-over Ethernet cable from **Data Input Port** to PC, or a straight Ethernet cable to LAN connection, e.g. Hub.

Step 5 Attach one straight Ethernet cable to the **Power & Data Output Port** on the Inline Power Injector (refer to [page 5](#)).

Step 6 Plug the other end of the straight Ethernet cable to the **Ethernet Port** (refer to [page 5](#)) on the SF-300.

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

You can configure the SF-3000 via HTML browser, such as Microsoft 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, including **Wireless Client Bridge** and **Wireless Client Router**.

The SF-3000 is shipped with default configuration to function as a client bridge between an Ethernet and Wireless network by attaching SF-3000 to the wired LAN simply. If user would configure SF-3000, please refer to the following procedures.

2.4.2 Basic Configuration Steps

This section describes a five-step configuration procedure to setup SF-3000 workable upon your topology requirement.

Step 1 Select an operation mode for SF-3000 on the web page “/General Config/System/”, and click **FINISH** to refresh this page.

Step 2 Modify the factory-default parameters on the web page “/General Config/System”, and click **FINISH** to save the changes.

Step 3 Modify the factory-default parameters on the web page “/General Config/Wireless”, and click **FINISH** to save the changes.

Step 4 (Optional) Modify other parameters on the web page “/General Config”, and click **FINISH** to save the changes.

Step 5 Move to page “/Utility/Administration”, select the **Save** then **Restart** and then click **FINISH** to take effect on 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 Configuration

Before configuring SF-3000, user needs 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, user may change the IP Address later and cannot connect the unit by using the default IP Address. In this case, it is a must to identify the SF-3000 current IP Address before configuring. To identify the IP Address, user can use the serial port (refer to [page 4](#)) to gain access of the current network status.

To start a Serial Port connection by following the steps below.

Step 1 Attach the RS-232 null modem console cable (refer to [page 4](#) and [page 6](#)) to the **RS-232 Console Port** on SF-3000. Connect the other end to a terminal or a PC running a terminal emulation program.

Step 2 Set the terminal to **115200 baud rate, None Parity, 8 data bits, 1 Stop bit**, and **ANSI compatible**.

Step 3 Run a terminal emulation program on PC, such as **Hyper Terminal**, and set the following connection properties.

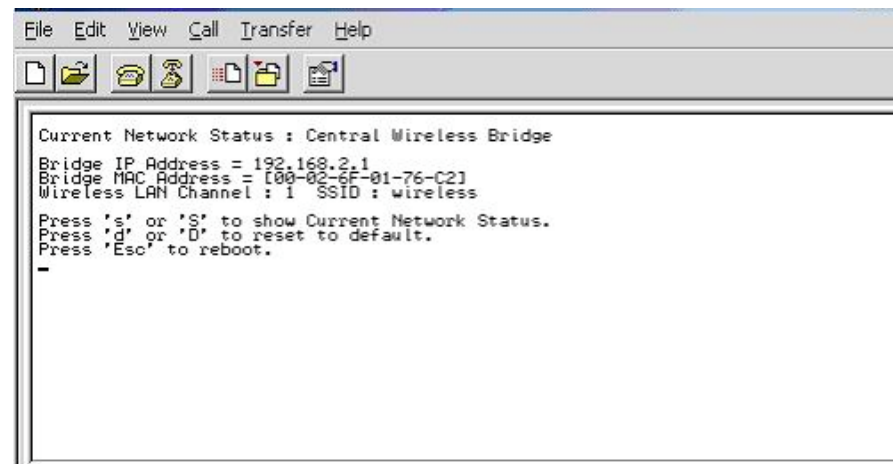
Step 3.1 Click the **Start icon > Program > Accessories > Communication > Terminal**.

Step 3.2 Create a new connection file, and select a Com Port <COM1, COM2, etc., depending on PC> with **115200bps / 8-bits / 1-stop**.

Step 3.3 Click the properties icon in the **Tool Bar > setting > select Emulation terminal VT100 > ok**.

Step 4 Reboot SF-3000.

Step 5 When the SF-3000 is powered up, the “**Current Network Status**” will be displayed as shown below.



```
File Edit View Call Transfer Help
[Icons]
Current Network Status : Central Wireless Bridge
Bridge IP Address = 192.168.2.1
Bridge MAC Address = [00-02-6F-01-76-C2]
Wireless LAN Channel : 1 SSID : wireless
Press 's' or 'S' to show Current Network Status.
Press 'd' or 'D' to reset to default.
Press 'Esc' to reboot.
-
```

■ Web Access Procedures

Once you identify the IP Address assigned to SF-3000, use web browser to configure SF-3000 through the HTTP Interface. The following procedure explains how to configure each item.

Step 1 Open your browser and enter the IP Address

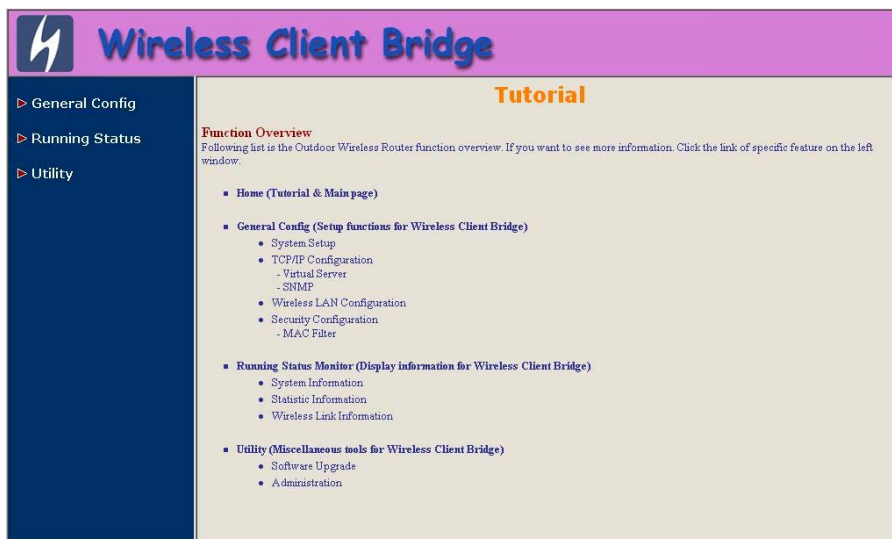
Step 2 Press <ENTER> key and the SF-3000 **Login** screen appears as shown below.



The dialog box titled "Enter Network Password" contains the following fields and options:

- Site: 192.168.2.1
- Realm: System Setup
- User Name: root
- Password: [masked]
- ☒ Save this password in your password list
- Buttons: OK, Cancel

Step 3 Enter "root" in the **User Name** and the **Password** fields, and click **OK** to enter the web configuration user interface screen as shown below.



■ Web Configuration Structure

The web configuration user interface is grouped into 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 viewing and modifying the parameters.

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

■ Operation Mode

When setting up SF-3000, you have to decide which Operation Mode in which SF-3000 will function. This option is available in the "/General Config/System/" page as shown below.

■ Host Information

The Host Name is not an essential setting, but it helps to 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 SF-3000 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, and 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 WEP encryption.

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

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

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

2.4.6 Change Supervisor Account & Password

Enter the **Utility > Administration** page. The figure below shows the **Utility/ Administration** page.

■ Supervisor Account

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

■ Apply the New Settings

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

Step 2 Click **FINISH** to take effect on 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 Protocol (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 firmware files, and the TFTP Server is operational.

■ Update the Firmware using the TFTP method

Step 1 Enter the **Utility > Software Upgrade** page as shown in the figure below, and can use TFTP to upgrade SF-3000. Here, user 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.

Step 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.

The screenshot shows the 'Utility - Software Upgrade' page of a Wireless Client Bridge. The page has a purple header with a lightning bolt icon and the title 'Wireless Client Bridge'. Below the header is a sidebar with navigation links: 'General Config', 'Running Status', and 'Utility' (which is expanded to show 'Administration'). The main content area is titled 'Utility - Software Upgrade' and contains the text 'Please Fill in The Following Software Upgrade Information:'. Below this text is a section for 'Upgrade Mode & TFTP Parameters'. It includes a text field for 'TFTP Server IP Address' with the value '192.168.2.100'. There is a table with two columns: 'Select' and 'Upgrade Mode'. The table has two rows: 'Program Image' and 'Web Image'. The 'Program Image' row has a checked checkbox and the filename 'soho.bin'. The 'Web Image' row has an unchecked checkbox and the filename 'pfs.img'. At the bottom of the form are three buttons: 'OK', 'CANCEL', and 'HELP'.

Select	Upgrade Mode	Upgrade Filename
☒	Program Image	soho.bin
☐	Web Image	pfs.img

■ Upgrade the Firmware using RS-232 console

Please refer to [Provision 2.4.3](#) that introduces how to use RS-232 console port.

■ Identify the IP Address assigned to the unit.

Step 1 If the connection is normal, when the SF-3000 is powered up, the "Current Network Status" will be displayed as shown below.

The screenshot shows a terminal window with a menu bar (File, Edit, View, Call, Transfer, Help) and a toolbar with icons for file operations. The main text area displays the 'Current Network Status' for a 'Central Wireless Bridge'. The status information includes: 'Bridge IP Address = 192.168.2.1', 'Bridge MAC Address = [00-02-6F-01-76-C2]', and 'Wireless LAN Channel : 1 SSID : wireless'. Below this information are instructions: 'Press 's' or 'S' to show Current Network Status.', 'Press 'd' or 'D' to reset to default.', and 'Press 'Esc' to reboot.'.

```
Current Network Status : Central Wireless Bridge
Bridge IP Address = 192.168.2.1
Bridge MAC Address = [00-02-6F-01-76-C2]
Wireless LAN Channel : 1 SSID : wireless

Press 's' or 'S' to show Current Network Status.
Press 'd' or 'D' to reset to default.
Press 'Esc' to reboot.
```

Step 2 Press <Esc> keystroke to reboot the SF-3000. Press <x> key during the boot process, and it will display prompt character **NetARM>** as the figure shown in the next page.

```
Packet Filter Rules Initialized !!!
RUNTASK id=11 httpd_timer_task...
RUNTASK id=12 hting Multitask...

Software Version : HWLAN 1.31.201RC2

Current Network Stat= 192.168.2.1
Bridge MAC Address = [00-02-6F-01-76-C2]
Wireless LAN Chterface IP = 192.168.10.1
Press 's' or 'S' to show Current Network Status.
Press 'Esc' to reboot.
hwlan_shut
hwlan_shut
LOOPBACK device 0 SHUTDOWN!
now rebooting... ng System Check.

4510B BIOS Version 1.01B 2002/08/05
Little Endian/10.32192M
Toshiba TCx
Now, switch to [Xmodem] protocol!!

NetARM>
```

Step 3 Press “h” keystroke, it will display related commands as the figure shown below.

```
File Edit View Call Transfer Help

4510B BIOS Version 1.01B 2002/08/05
Processing System Check

4510B BIOS Version 1.01B 2002/08/05
Little Endian/10.32192M
Toshiba TC58FUT160A found.
NetARM> h
D -- memory Dump
E -- Erase flash memory section
F -- upgrade Flash memory
G -- Go, start rom image
S -- Save image to file
H -- Help messages
M -- Dump Mac address
W -- Write Mac address
X -- Switch download/upload protocol
P -- upload Program to ram and execute
R -- Reboot

NetARM>
```

Step 4 Select “F -- upgrade Flash memory” and it will display upgrade items for selection as the figure shown below.

```
File Edit View Call Transfer Help

4510B BIOS Version 1.01B 2002/08/05
Processing System Check

4510B BIOS Version 1.01B 2002/08/05
Little Endian/10.32192M
Toshiba TC58FUT160A found.
NetARM> f
D -- memory Dump
E -- Erase flash memory section
F -- upgrade Flash memory
G -- Go, start rom image
S -- Save image to file
H -- Help messages
M -- Dump Mac address
W -- Write Mac address
X -- Switch download/upload protocol
P -- upload Program to ram and execute
R -- Reboot

NetARM> f
1:BOOT 3:SOHO, 4:WEBIMG, 5:APFW, 6:CONFIG, 7:SSMAC, default:SOHO
select area: _
```

Step 5 Select “3: SOHO” and select “4: WEBIMG” to update the firmware files one by one.

Step 6 While the window starts to display “C” character continuously, click **Transfer** and select the new firmware files <soho.bin> file, press “OK” to start to transfer file to SF-3000.

Step 7 Select “4” to upgrade WEBIMG file. The procedures are the same with upgrading SOHO file (go back to step 5), but should select <pfs.img> file correctly for WEBIMG file upgrade.

Step 8 After the upgrade completes, remember to press “R” keystroke to reboot the system.

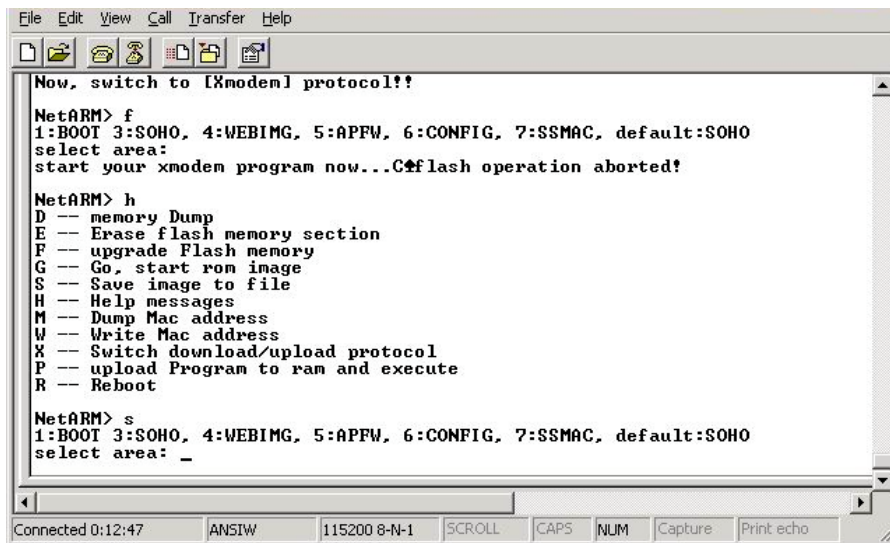
Note: The default transfer protocol is using “Xmodem”, so please make sure you select correct protocol to download/upload files when you try to upgrade the SF-3000’s firmware files.

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

After configuring SF-3000, user can back-up the configuration files. User can upload the latest back-up files and recover the SF-3000 configuration to the settings specified in the back-up files.

■ Downloading Configuration Files

Just being the same with firmware upgrade 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 configuration as the figure shown below. The back-up file will be saved as <CONFIG.IMG> file.



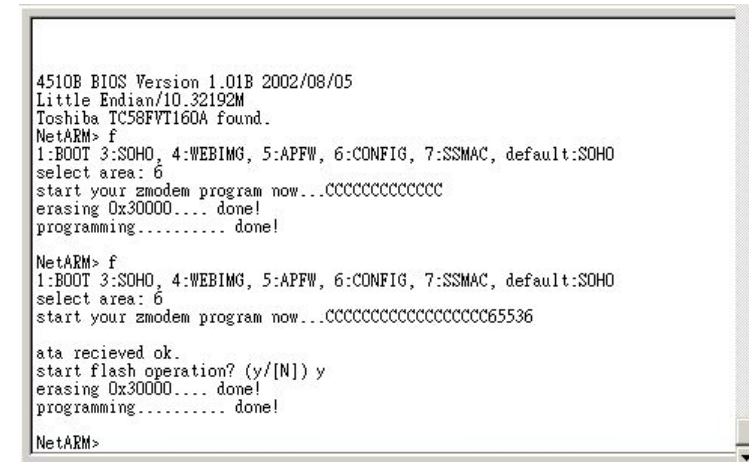
```
File Edit View Call Transfer Help
Now, switch to [Xmodem] protocol!!
NetARM> f
1:BOOT 3:SOHO, 4:WEBIMG, 5:APFW, 6:CONFIG, 7:SSMAC, default:SOHO
select area:
start your xmodem program now...C*flash operation aborted!

NetARM> h
D -- memory Dump
E -- Erase flash memory section
F -- upgrade Flash memory
G -- Go, start rom image
S -- Save image to file
H -- Help messages
M -- Dump Mac address
W -- Write Mac address
X -- Switch download/upload protocol
P -- upload Program to ram and execute
R -- Reboot

NetARM> s
1:BOOT 3:SOHO, 4:WEBIMG, 5:APFW, 6:CONFIG, 7:SSMAC, default:SOHO
select area: _
```

■ Uploading Configuration Files

To upload an configuration file to SF-3000, user should select "**F -- upgrade Flash memory**" and then select "**6: CONFIG**". While the window starts to display "C" character continuously, click **Transfer** and select the preferred <CONFIG.IMG>, then press **OK** to start transferring 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...CCCCCCCCCCCC
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...CCCCCCCCCCCCCCCCCCCC65536

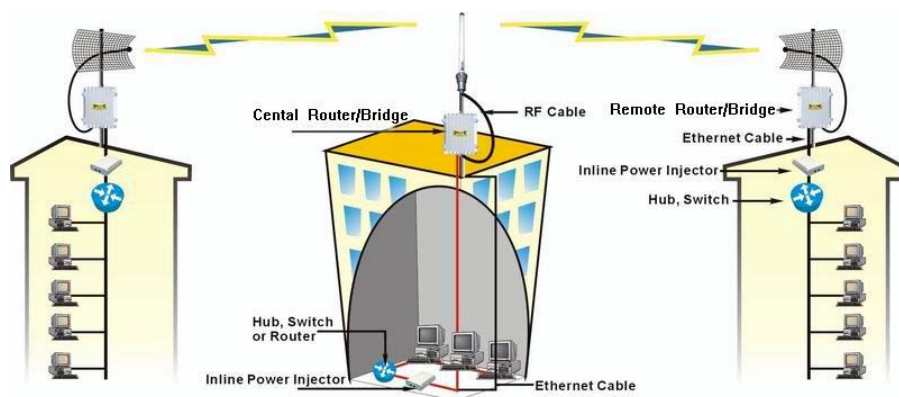
ata recieved ok.
start flash operation? (y/[N]) y
erasing 0x30000.... done!
programming..... done!

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 chapter describes several main types of installations implemented by using the Outdoor Wireless System commonly. 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 with SendFar RB-8110 (as the figure shown below).

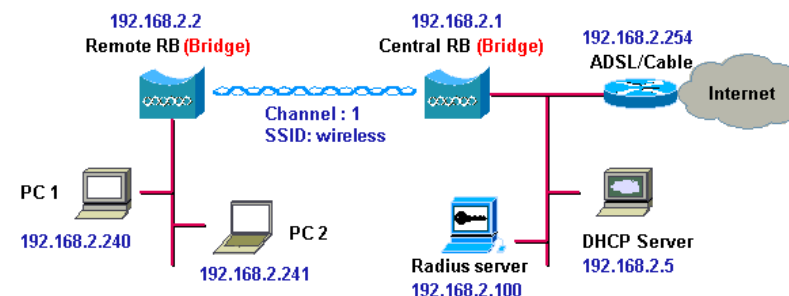


The SF-3000 performs in either router or bridge mode. In a Point-to-Multipoint topology, all communication between network systems is done through a centralized agent. Among the Outdoor Wireless Router/Bridge products, the centralized agent is Central Router or Central Bridge (SendFar RB-8110) and the individual network nodes may be Wireless Client Router or Bridge (SendFar SF-3000).

To show the available Point-to-Multipoint topologies, the following examples are provided.

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

3.1 Wireless Client Bridge-to-Central Wireless Bridge



Step 1 Set the Central Outdoor Unit ^{*1} (hereinafter, "COU") to perform a bridge (bridge IP address: 192.168.2.1).

Step 2 Set Wireless parameters on COU: **Channel (1)** and **SSID (wireless)**

Step 3 Set the Remote Outdoor Unit ^{*2} (hereinafter, "ROU") to perform a bridge (bridge IP address: 192.168.2.2).

Step 4 Set Wireless parameters on ROU: **Channel (1)** and **SSID (wireless)**, and these parameters must be the same with COU.

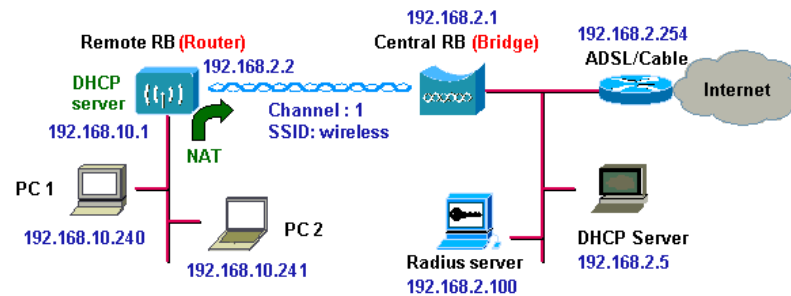
Step 5 Left side subnet is transparent to the right side.

Step 6 DHCP server assign IP address to PC1 and PC2

Remarks:

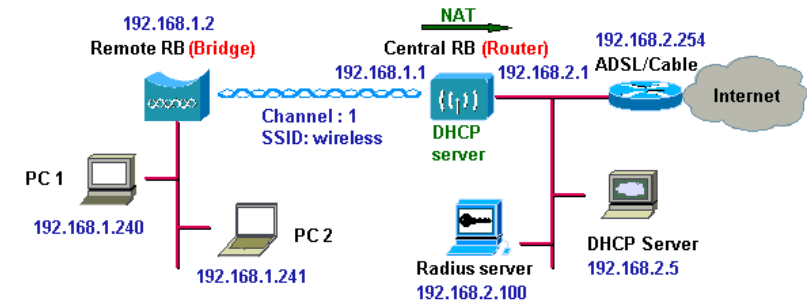
- *1 COU refers to SendFar RB-8110 Outdoor Wireless Router Bridge
- *2 Both SendFar RB-8110 and SF-3000 could function the role of ROU

3.2 Wireless Client Router-to-Central Wireless Bridge



- Step 1** Set the COU to perform a bridge (**bridge IP address: 192.168.2.1**).
- Step 2** Set Wireless parameters on COU: **Channel (1)** and **SSID (wireless)**.
- Step 3** Set the ROU to perform a Router (**Wireless Interface IP: 192.168.2.2, Ethernet Interface IP: 192.168.10.1**). It is a must to enable NAT on Wireless Interface (**default route is 192.168.2.254**).
- Step 4** Set Wireless parameters on ROU: **Channel (1)** and **SSID (wireless)**, these parameters must same with COU.
- Step 5** Set the DHCP server service on the ROU and apply it on Ethernet Interface.
- Step 6** The ROU assigns IP addresses to PC1 and PC2

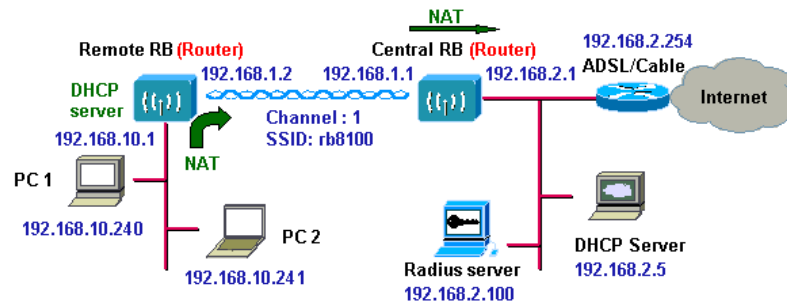
3.3 Wireless Client Bridge-to-Central Wireless Router



- Step 1** Set the COU to perform a Wireless Router (**Wireless Interface IP: 192.168.1.1, Ethernet Interface IP: 192.168.2.1**). It is a must to enable NAT on Ethernet interface (**default route: 192.168.2.254**).
- Step 2** Set Wireless parameters on COU: **Channel (1)** and **SSID (wireless)**
- Step 3** Set the DHCP server service on the COU and apply it on Wireless Interface.
- Step 4** Set the ROU to perform a Bridge (**Bridge Interface IP: 192.168.1.2**).
- Step 5** Set Wireless parameters on ROU: **Channel (1)** and **SSID (wireless)**, and these parameters must be the same with the COU.
- Step 6** The COU assigns IP addresses to PC1 and PC2.
- Step 7** The operator can also disable NAT behavior on COU to make the two subnets transparent.

3.4 Wireless Client Router-to-Central Wireless Router

The operator can also enable NAT behavior on COU (**enable NAT on Ethernet interface**) and enable NAT behavior on ROU (**enable NAT on Wireless Interface**).



Step 1 Set the COU to perform a Wireless Router (**Wireless Interface IP: 192.168.1.1, Ethernet Interface IP: 192.168.2.1, default route: 192.168.2.254**).

Step 2 Set Wireless parameters on COU: **Channel (1)** and **SSID (wireless)**.

Step 3 Set the ROU to perform a Wireless Router (**Wireless Interface IP: 192.168.1.2, Ethernet Interface IP: 192.168.10.1, default route: 192.168.1.1**).

Step 4 Set Wireless parameters on ROU: **Channel (1)** and **SSID (wireless)**, and these parameters must be the same with COU.

Step 5 Set the DHCP server service on the ROU and apply it on Ethernet Interface.

Step 6 The ROU assigns IP addresses to PC1 and PC2.

The operator can also disable NAT behavior on COU and enable NAT behavior on ROU (**enable NAT on Wireless Interface**). In this case, any outgoing packets will transfer to **192.168.1.2**.

Chapter 4. Network Parameters

4.1 IP Configuration

The IP Configuration method is different in each Operating Mode. User could refer to the following descriptions for details.

■ Wireless Client Bridge

Step 1 Select the Wireless Client Bridge mode, and enter the IP Address manually into the **Bridge IP Address** field.

Step 2 Use **Bridge IP Address** setting to assign or change the bridge's IP address.

Step 3 Click **FINISH** at the bottom of this page to complete the modification of IP address.

■ Wireless Client Router

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

The **NAPT** function allows home users and small businesses to connect their network to the Internet cost-effectively and efficiently. User has to enable it to allow the subscribers to connect to the Internet in this mode.

Click **FINISH** at the bottom of this page to complete the IP address modifications after enabling NAPT function.

4.2 Virtual Server

Sometimes, the operator might 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.

Step 1 Select the “/General Config/ TCP/IP/Virtual Server”, and then the **Virtual Server** screen appears. The figure below shows the current virtual server entry table. (The **Virtual Server Mapping** pool is empty as default)

Wireless Client Bridge

General Configuration - Virtual Server

Config Virtual Server Mapping
Input new parameters in blanks and click 'Add' button to add virtual server entry. Click 'Modify' button and change parameters in blanks to modify virtual server entry. Click 'Delete' button to delete virtual server entry. Click 'OK' button to set the configuration value. Click 'Cancel' button if need not add or modify virtual server entry.

■ Table of current virtual server entries:

Index	Service Name	Protocol	Public Access		Virtual Server	
			Interface	Port Number	IP Address	Port Number
Pool is Empty !!						

(Max Port Number:32767)

Add

FINISH **CANCEL** **HELP**

Step 2 Click **Add**, and the Virtual Server Entry Edit page appears as the figure shown below.

Wireless Client Bridge

General Configuration - Virtual Server

Config Virtual Server Mapping
 Input new parameters in blanks and click 'Add' button to add virtual server entry. Click 'Modify' button and change parameters in blanks to modify virtual server entry. Click 'Delete' button to delete virtual server entry.
 Click 'OK' button to set the configuration value. Click 'Cancel' button if need not add or modify virtual server entry.

■ Table of current virtual server entries:

Index	Service Name	Protocol	Public Access		Virtual Server	
			Interface	Port Number	IP Address	Port Number
1		TCP	Wireless	0		0

Ok Cancel

(Max Port Number:32767)

FINISH CANCEL HELP

Step 4 Click **OK**. The Virtual Server Entry Table appears with the entries list.

Step 5 To modify or delete a virtual server entry, click the select button beside the entry index number and click **Modify** or **Delete**.

Step 6 To add another entry to the Virtual Server Mapping Pool, repeat step 1 through step 3.

Step 7 When user has included all the entries preferred, click **FINISH**.

Step 3 To edit the Virtual Server Entry, specify all the entry fields to allow Internet user to access the internal servers.

- ✓ **Service Name.** Alias name of this internal server, such as FTP.
- ✓ **Protocol.** Indicate which protocol (TCP/UDP) user wants to translate from outside to internal server, such as TCP.
- ✓ **Access Interface.** Indicate the translation occurs on which interface (Wireless interface / Ethernet interface), such as Ethernet.
- ✓ **Public Access Port number.** Indicate which socket port (1 ~ 65535) user wants 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.

4.3 Configure SNMP

Select the “/General Config/ TCP/IP/SNMP”, and the SNMP screen appears. The figure below shows the current SNMP community pool and trap host pool.

General Configuration - SNMP Community Parameter

Config Following Community Parameter:
Select one community index from the table below and click 'Modify' button to modify specific item.

Table of current community pool:

Index	Validity	Access Right	Community
1	Enable	Read	public
2	Enable	Write	private
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

Modify

Config Following Trap Host Parameter:
Select one trap host index from the table below and click 'Modify' button to modify specific item.

Table of current trap host pool:

Index	Version	IP Address	Community
1	Version 1	192.168.2.100	public
2	Version 2	192.168.2.100	public

4.3.1 Configure Community Pool

The SNMP Community Pool has five entries.

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

General Configuration - SNMP Community Parameter

Config Following Community Parameter:
Select one community index from the table below and click 'Modify' button to modify specific item.

Table of current community pool:

Index	Validity	Access Right	Community
1	Enable	Read	public
2	Enable	Write	private
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

OK Cancel

Config Following Trap Host Parameter:
Select one trap host index from the table below and click 'Modify' button to modify specific item.

Table of current trap host pool:

Index	Version	IP Address	Community
1	Version 1	192.168.2.100	public
2	Version 2	192.168.2.100	public
3	Disable	---	---

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 preferred, 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.

The screenshot shows the 'Wireless Client Bridge' configuration interface. On the left is a navigation menu with sections: General Config (System, TCP/IP, Virtual Server, SNMP, Wireless, Security, MAC filter), Running Status (System Info, Statistic Info, Wireless Link Info), and Utility (Software Upgrade, Administration). The main area is titled 'Config Following Trap Host Parameter.' and includes a sub-instruction: 'Select one trap host index from the table below and click 'Modify' button to modify specific item.' Below this is a table labeled 'Table of current trap host pool:' with columns: Index, Version, IP Address, and Community. The table contains five rows. Row 1 is selected. Below the table are 'Ok' and 'Cancel' buttons. At the bottom of the main area are 'FINISH', 'CANCEL', and 'HELP' buttons.

Index	Version	IP Address	Community
1	Version 1	192.168.2.100	public
2	Version 2	192.168.2.100	public
3	Disable	---	---
4	Disable	---	---
5	Disable	---	---

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 preferred, click **FINISH**.

4.4 Configure Wireless related parameters

Step 1 Select “/General Config/Wireless” and the Wireless LAN information page appears as the figure shown below.

The screenshot shows the 'General Configuration - Wireless LAN' page. On the left is a navigation menu with 'General Config' expanded, showing 'System', 'TCP/IP', 'Virtual Server', 'SNMP', 'Security' (highlighted), and 'MAC filter'. Below this are 'Running Status' and 'Utility'. The main area is titled 'General Configuration - Wireless LAN' and contains 'Wireless LAN information.' and 'Wireless LAN Configuration:'. The configuration fields include: 'rts Threshold' (1600), 'frag Threshold' (1600), 'SSID' (wireless), 'Station Name' (ap), 'WEP Key' (wepkey), and 'WEP' settings (WEP128 selected, WEP64 and Disable unselected). Below these are 'Default Key' (1) and several key pattern grids for WEP64 and WEP128. A 'KeyGen' button is located next to the 'WEP Key' field.

Step 2 In the Wireless LAN information page, set the following parameters suitable for your radio network.

- ✓ **Channel** (default parameter: 1)
- ✓ **rts Threshold** (default parameter: 1600)
- ✓ **frag Threshold** (default parameter: 1600)
- ✓ **SSID** (default parameter: wireless)
- ✓ **Station Name** (default parameter: ap)

Step 3 Click radio button to disable WEP or enable 64/128 bit **WEP services** (default parameter: **disable**). If WEP is enabled, input corresponded **Default Key index** and **WEP Key** and then click **KeyGen** to generate the WEP64 & WEP128 key patterns.

Step 4 Click **FINISH** at the bottom of this page to complete the modification.

The following gives more info about the parameters set in the Wireless LAN information page to users.

■ rts Threshold

The setting determines the packet size, ranging from **0 to 2339** bytes, 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.

■ frag Threshold

The setting determines the size, ranging from **256 to 2338** bytes, at which packets are fragmented (sent as several pieces instead of as one block). 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 join the radio network.

■ Hide SSID

Use this setting to decide whether devices that do not specify an SSID are allowed to associate with the access point or not. With “**Yes**” selected, the SSID used by other devices must match exactly the AP’s SSID.

■ Deny Any

Use this setting to decide whether devices that specify **the well define SSID keyword ‘ANY’ or ‘any’** are allowed to associate with the access point or not. 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 automatically.

■ WEP

User 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. The 40-bit WEP keys can contain any combination of 10 of these characters; the 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

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

Wireless Client Bridge

General Configuration - MAC filter

MAC Filter allowed list.
Input new parameters in blanks and click 'Add' button to add MAC filter entry. Click 'Modify' button and change parameters in blanks to modify MAC filter entry. Click 'Delete' button to delete MAC filter entry.

■ MAC Filter service: ☒ Disable ☐ Enable

■ Table of current MAC entries:

Amount of usable allowed list entry: 1

No	MAC Address
1	11:22:33:44:55:66

User can specify the MAC address of a wireless client station. All MAC entries in the MAC address table are permitted to connect to the SF-3000. User 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

Step 1 Click **Utility**, select **Software Upgrade** page as the figure shown below, and then use TFTP to upgrade AP. In the **Utility – Software Upgrade** page, user must specify the **TFTP server IP** and select by which file to upgrade (**Program image, Web image**), then click **OK** button to start the TFTP upgrade process.

Step 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.

The screenshot shows the 'Utility - Software Upgrade' page of the Wireless Client Bridge. The left sidebar has a tree view with 'Utility' expanded and 'Software Upgrade' selected. The main content area has a title 'Utility - Software Upgrade' and a subtitle 'Please Fill in The Following Software Upgrade Information:'. Below this, there is a section 'Upgrade Mode & TFTP Parameters:' with a text field for 'TFTP Server IP Address' containing '192.168.2.100'. A table with three columns: 'Select', 'Upgrade Mode', and 'Upgrade Filename' is present. The table has two rows: 'Program Image' with a checked checkbox and filename 'soho.bin', and 'Web Image' with an unchecked checkbox and filename 'pfs.img'. At the bottom of the main area are three buttons: 'OK', 'CANCEL', and 'HELP'.

Select	Upgrade Mode	Upgrade Filename
☒	Program Image	soho.bin
☐	Web Image	pfs.img

4.6.2 Administration

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

The screenshot shows the 'Utility - Administration' page of the Wireless Client Bridge. The left sidebar has a tree view with 'Utility' expanded and 'Administration' selected. The main content area has a title 'Utility - Administration' and a subtitle 'This page offers the function to write new configuration data into flash memory. After updating the configuration, the server must be restarted and then the setting will work. When restarting the system, the browser session will be disconnected. After waiting for several minutes, you may either press the browser's reload button, or close the browser and re-open it.' Below this, there is a section 'Supervisor Account:' with three text fields: 'Supervisor ID' (containing 'root'), 'Supervisor Password' (containing four dots), and 'Password Confirm' (containing four dots). A section 'System Management:' has four radio buttons: 'Save only' (selected), 'Restart only', 'Save then Restart', and 'Reset parameters to Factory Default'. At the bottom of the main area are three buttons: 'FINISH', 'CANCEL', and 'HELP'.

- ✓ **Supervisor Account.** Change the supervisor's user name & password in the Supervisor Account field, and Click **FINISH** to take effect on the previous configuration changes.
- ✓ **Apply the New Settings.** Click **Utility, Administration**, select the **Save** then **Restart** to apply the new configuration settings.

Step 2 Click **FINISH** to take effect on the previous configuration changes.

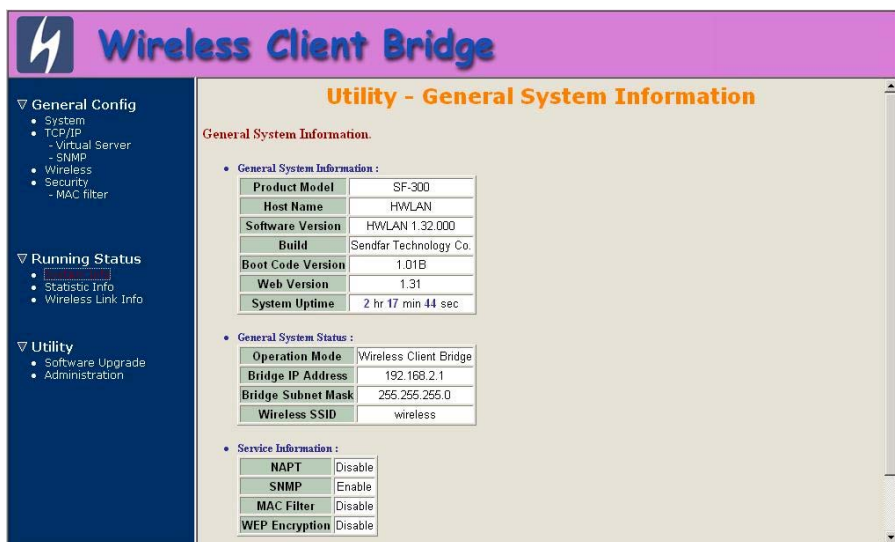
Hint: It takes about 10 seconds, to complete the restart process.

Chapter 5. Monitor Information

User can find the system running status and other information on this window. Click the **Running Status** link on the left window, use can choose which function that he wants to monitor.

5.1 System Information

By selecting “Running Status/System Info”, enter the **System Information** page as the figure shown below.



In this page, user can find the system information and most of the running parameters.

■ General System Information

The following information can be found in this block.

- ✓ Product Model
- ✓ Host Name
- ✓ Software Version
- ✓ Build (Built by)
- ✓ Boot Code Version

- ✓ Web Version
- ✓ AP Firmware version
- ✓ System Uptime

■ General System Status

The following information can be found in this block.

- ✓ Operation Mode
- ✓ Interface IP/Net mask
- ✓ Brief wireless parameters

If the DHCP or PPPoE services is enabled, user can also see the related information here.

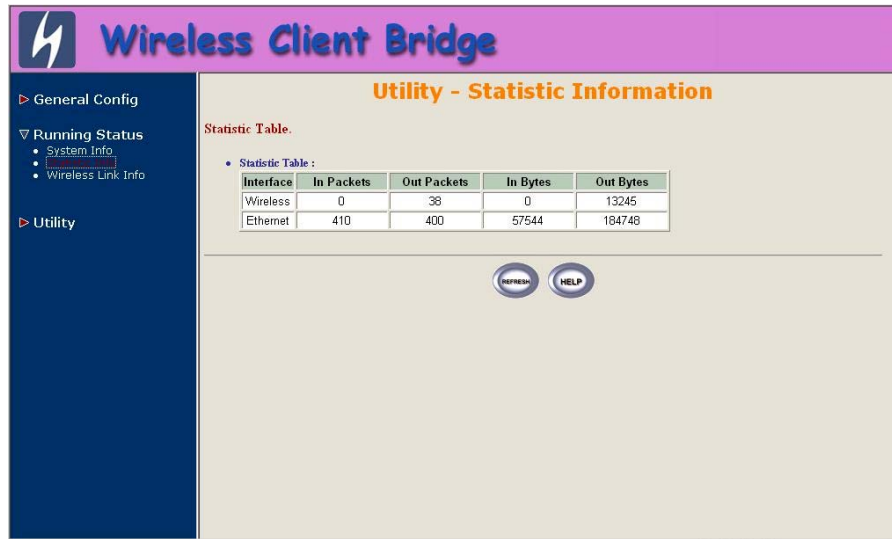
■ Services Information

This block shows whether the following services are enabled or disabled.

- ✓ NAPT
- ✓ SNMP
- ✓ MAC Filter
- ✓ WEP encryption.

5.2 Statistic Information

By selecting “Running Status/Statistic Info”, the figure below shows the **Statistic of Interface** page.



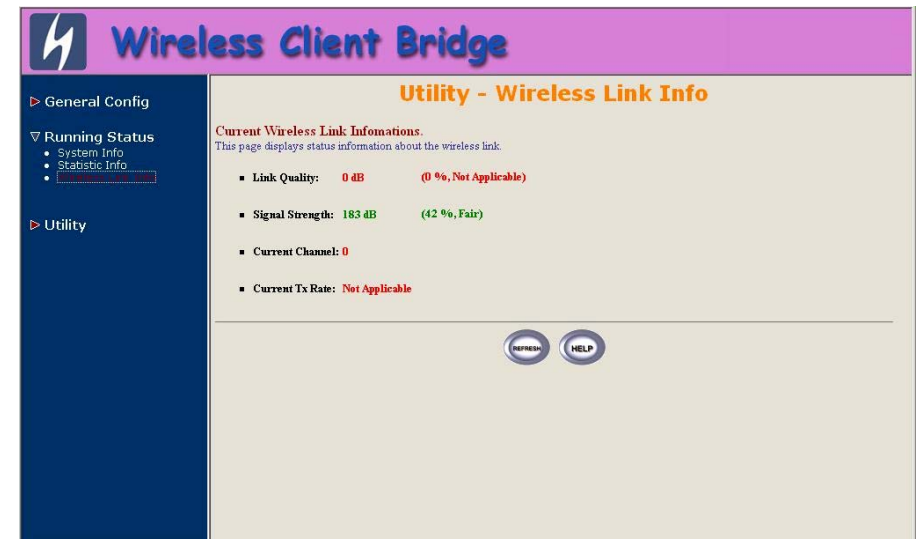
In this page, user can find the packet statistic of each interface, Wireless and Ethernet. This statistic table includes the following information.

- ✓ In Packets
- ✓ Out Packets
- ✓ In Bytes
- ✓ Out Bytes.

5.3 Wireless Link Information

This item only displayed on ROU mode.

By selecting “Running Status/Wireless Link Info”, the figure below shows the **Radio Link Information** page.



In this page, user can find the following information about the radio link.

- ✓ Link Quality
- ✓ Signal Strength
- ✓ Current used channel
- ✓ Current Tx Rate.

Chapter 6. Specifications

6.1 Hardware Specifications

■ General

Radio Data Rate	11, 5.5, 2 and 1 Mbps, Auto Fall-Back
Client Interface	10/100Base-T Ethernet
Range (Open environment)	300m @ 11 Mbps 400m @ 5.5Mbps 500m @ 2 Mbps 800m @ 1 Mbps
Regulatory & Safety Certifications	FCC Part 15 EN 300 328-1 EN 300 328-2 EN 301 489-1 EN 301 489-17 EN 60950 IP67 DGT
Compatibility	Fully interoperable with IEEE802.11b compliant products
Power Supply (AC/DC Power Adaptor)	Input: 100~240V, 50~60Hz Output: 24V, 830mA

■ Network Information

Network Architecture	Infrastructure (via SendFar AP/RB-8110 AP or Bridge)
Drivers	Windows 95/98/ME/2000/NT 4.0
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
Transmit Power	10dBm (ETSI) 19dBm (FCC)
Antenna	Embedded 9dBi patch antenna
Sensitivity @ FER=0.08	11 Mbps < -85dBm 5.5 Mbps < -88dBm 2 Mbps < -91dBm 1 Mbps < -93dBm

■ Environmental

Temperature Range	Operating: 0 to 55°C Storage: -20 to 75°C
Humidity (non-condensing)	5% to 95% typical

■ Physical Specifications

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

6.2 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 Telnet 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 Client Bridge 2. Wireless Client Router	Wireless Client Bridge
Bridge IP Address	For Wireless Client Bridge with	192.168.2.1
Bridge Subnet Mask	Operation Mode	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	Default Value
Index 1	Validity	Enable
Index 2		Enable
Index 3		Disable
Index 4		Disable
Index 5		Disable
Index 1	Access Right	Read
Index 2		Write
Index 3		---
Index 4		---
Index 5		---
Index 1	Community	public
Index 2		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	Version1
Index 2		Version2
Index 3		---
Index 4		---
Index 5		---
Index 1	IP Address	192.168.2.100
Index 2		192.168.2.100
Index 3		---
Index 4		---
Index 5		---
Index 1	Community	public
Index 2		public
Index 3		---
Index 4		---

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

7.3 Utility

7.3.1 Software Upgrade

Parameter	Description	Default Value
TFTP Server IP Address	Specify the IP address of the TFTP server to upgrade the firmware of the RB	192.168.2.100
Upgrade Filename	Program Image	soho.bin
	Web Image	pfs.img

7.3.2 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

This equipment has been tested and found to comply with the limits for a Class C digital device pursuant to Part 15 of the FCC Rules and Regulation. 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 instruction manual, may cause harmful interference to nearby TV's, VCR's, radio, computers, or other electronic devices. To minimize or prevent such interference, this equipment should not be placed or operated near these devices. If interference is experienced, moving the equipment away from them will often reduce or eliminate the interference.

However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Re-orient 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 which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

■ 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.

■ Information to User

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

■ Manufacturer's Declaration of Conformity

SendFar Technology Co., Ltd.
15Fl., No. 866-2, Chungjeng Road
Junghe, Taipei
Taiwan, R.O.C.
+886 2 2228 7748

Declares that the product:

Date : November 18, 2003
Brand Name : SendFar Technology Co., Ltd.
Model Number : SF-3000
Equipment Type : Wireless Access Bridge

Complies with Part 15 Class C 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.



■ European Community – CE Notice

Marking by the symbol :



Indicates compliance with the essential requirements of **Directive 1999/5/EC**. Such marking is indicative that this equipment meets or exceeds the following technical standards:

- ✓ EN 300 328-2
- ✓ EN 301 489-1
- ✓ EN 301 489-17
- ✓ EN 60950

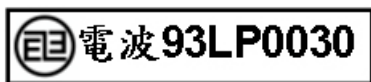
Marking by the symbol :



Indicates compliance with the essential requirements of **R&TTE Directive 99/5/EC**, and the product is permitted to be used in the following EC countries, including **Germany, UK, The Netherlands, Belgium, Norway,**

Sweden, Denmark, Finland, France, Italy, Spain, Austria, Iceland, Ireland, Portugal, Switzerland, Greece and Luxembourg.

■ 中華民國交通部電信總局低功率射頻電機型式認證
型式認證標籤式樣：



依據交通部電信總局『低功率輻射性電機管理辦法』第十四條規定，經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

依據交通部電信總局『低功率輻射性電機管理辦法』第十七條規定，低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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.

IMPORTANT NOTE:

FCC 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 20cm between the radiator & your body.

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