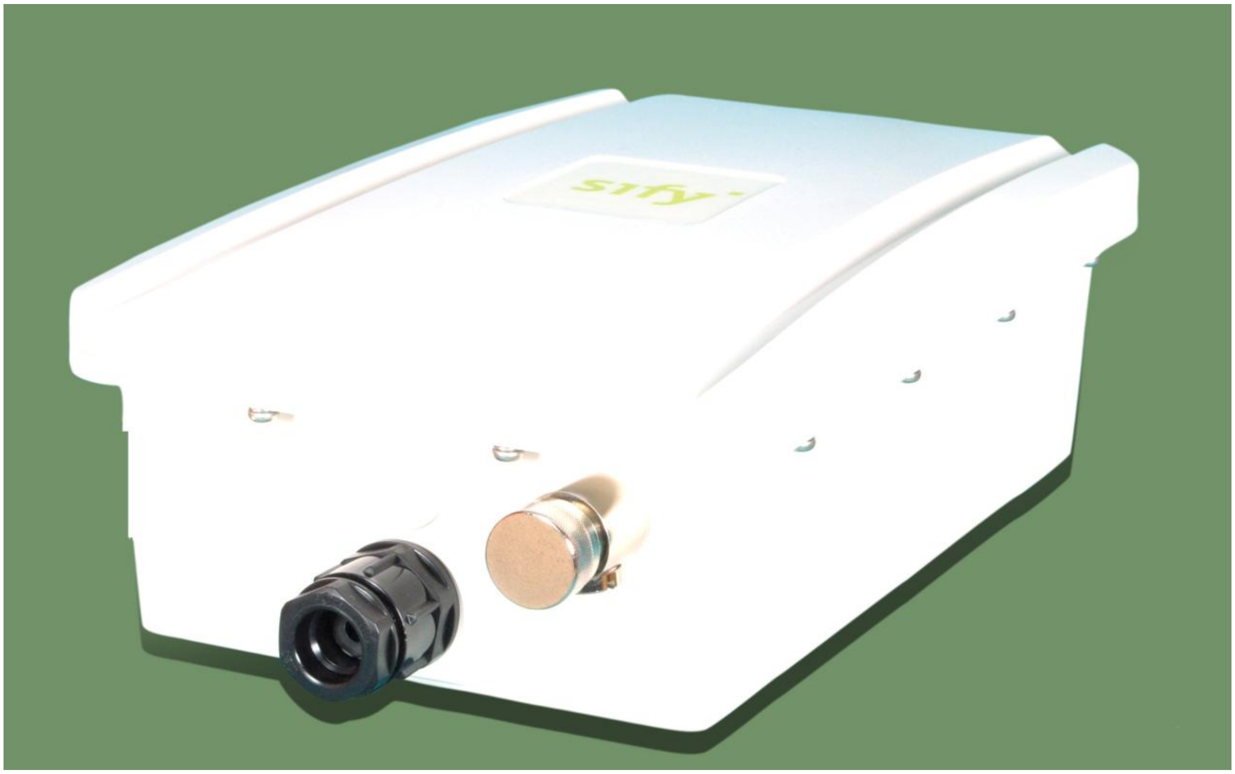
SIFY TECHNOLOGIES LTD.

SMAC User Manual



Author: ANE
Date: 03-Oct-2012
Revision: 4.0

Revision History

Revision	Date	Author	Change description
1.0	19-Jul-2011	ANE	Initial revision.
2.0	22-Dec-2011	ANE	1. Separated operation mode specific settings.
3.0	10-Jul-2012	ANE	1. Enterprise features added
4.0	03-Oct – 2012	ANE	2. Monitoring tab added.

Contents

About This Document

This document is written by SIFY. SIFY has rights to change any of this document without notice and all rights reserved. This document can only be used for guiding the configuration setup of SIFY products.

This document is to demonstrate the SIFY's SMAC5800 Wireless Access Point & Client Bridge. Please read the document carefully before setup the SMAC5800. If the damage is caused by the inappropriate behaviors, the repair will not be included in the warranty.

Formats

This document uses following symbols to indicate and highlight special message.

CAUTION	Caution: This symbol represents the Vital message and it could be harmful for the device or settings.
NOTE	Note: This symbol represents the important message for the settings.
TIP	Tip: This symbol represents the alternative choice that can save time or resources.

Before you start

The following equipments are essential to setup the SMAC5800:

1. One Computer/Notebook and internet accessible.
2. Two Ethernet Cables.
3. One SIFY device – SMAC5800.

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.

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.

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.

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

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

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.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

NOTE The equipments listed above are only for setup the SMAC5800, you will need more equipment to connect the internet and it is depend on your internet network structure. You may refer to the chapter 2 for more information.

1 Product Overview

Thank you for using SMAC5800. It is a powerful, enhanced, enterprise scale product with functions Outdoor Base and Outdoor Subscriber.

SMAC5800 uses the latest wireless technology 802.11n standard. It has faster transmit/receive wireless speed. SMAC5800 gives you a great advantage to save your time and cost to expend your network. It is also compatible with 802.11a.

SMAC5800 is easily to install almost anywhere with Power over Ethernet for quick indoor installation and regular Power by Adapter. SMAC5800 can manage power level control, Narrow bandwidth selection, Traffic shaping and Real-time RSSI indicator. SMAC5800 is fully support of security encryption including Wi-Fi Protected Access (WPA2-PSK), 128 bit - AES Encryption and IEEE 802.1x with RADIUS.

1.1 Feature

The following list describes the design of the SMAC5800 made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**

   There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**

   Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**

   Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**

   Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **Wireless extensions to Ethernet networks**

   Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

f) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

g) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

Benefits	
High Speed Data Rate Up to 300Mbps	Capable of handling heavy data payloads such as MPEG video streaming
High Output Power up to 23 dBm	Extended excellent Range and Coverage. Maximum Tx power will be limited based on country code selection and EIRP limit is applicable based on the frequency band.
IEEE 802.11a/n Compliant	Fully Interoperable with IEEE 802.11a/IEEE 802.11n compliant devices
Multi-Function	Users can use different mode in various environment
Point-to-point, Wireless Connectivity	Let users transfer data between two buildings
Support RSSI Indicator	Users can select the best signal to connect with AP easily
Power-over-Ethernet	Flexible Access Point locations and cost savings. SMAC5800 must uses the adapter provided in the package.
WPA2-PSK (AES) **802.1x support**	support advanced encryption system
MAC address filtering in AP mode	Ensures secure network connection
SNMP Remote Configuration Management	Help administrators to remotely configure or manage the Access Point easily.
VLAN	Specify a VLAN number for each SSID to separate the services

	among clients.
Wi-Fi Protect Access	Wi-Fi Protect Access is a standard-based interoperable security enhancement that increases the level of data protection and access control for existing and future wireless LAN system.

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- 1* Wireless Access Point / Client Bridge (SMAC5800)
- 1* Three Pin Indian type power cord
- 1* PoE Injector 24V/1A Power Adapter (PA1022-3T3)
- 1* Pole Mounting kit
- 1* Earthing cable with AP only

CAUTION

Using other Power Adapter than the one included with SMAC5800 may cause damage of the device.

1.3 System Requirement

The following conditions are the minimum system requirement.

- A computer with an Ethernet interface and operating under Windows XP, Vista, 7 or Linux.
- **Internet Browser** that supports HTTP and JavaScript.

1.4 Hardware Overview

Physical Interface	- 1 x LAN Port with PoE support - 1 x RF port

2 Computer Configuration Instruction

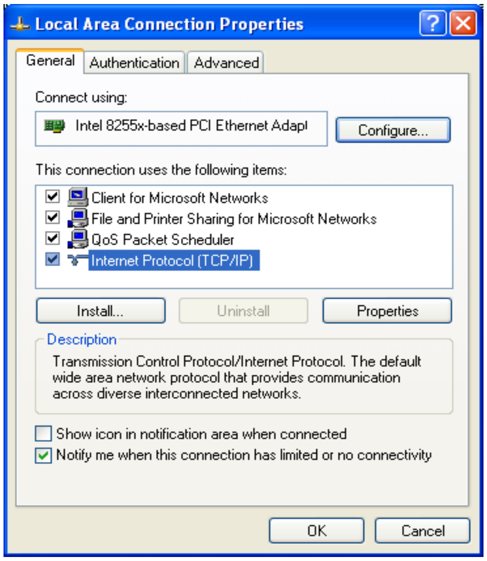
The default operating mode is Outdoor Base for AP hardware and Outdoor Subscriber for SU hardware. Device will not assign an IP address to the computer/notebook. Therefore, follow the steps to assign an IP address to your Ethernet card.

2.1 Assign a Static IP

In order to configure SMAC5800, please follow the instruction below:

1. In the **Control Panel**, double click **Network Connections** and then double click on the connection of your **Network Interface Card (NIC)**. You will then see the following screen.

2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Intel 8255x-based PCI Ethernet Adapt

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

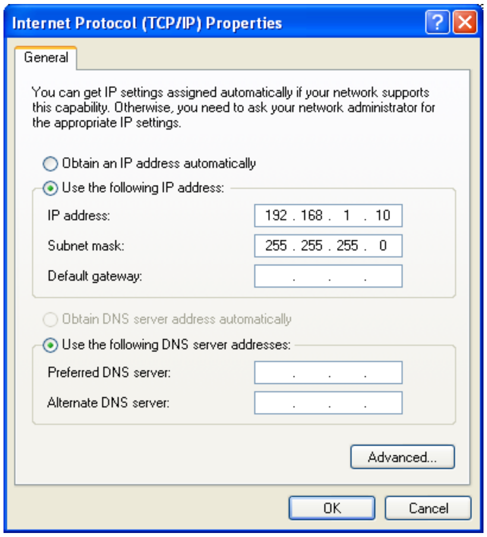
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

3. Select **Use the following IP address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.

4. Click on the **OK** button to close this window, and then close LAN properties window.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

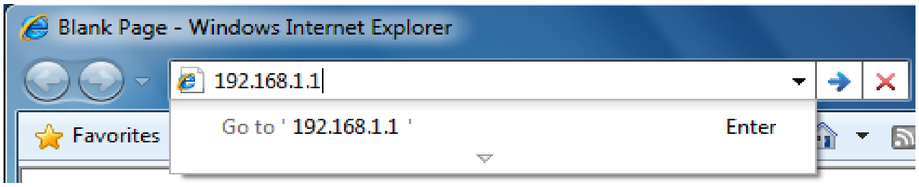
NOTE

IP Address entered in the TCP/IP Properties needs to be at the same subnet of the SMAC5800 IP Address. For example: SMAC5800's default IP Address is **192.168.1.1** so the IP Address in the TCP/IP settings could be **192.168.1.10**.

2.2 Logging Method

After complete the IP settings from last section, you can now access the web-based configuration menu.

1. Open web browser



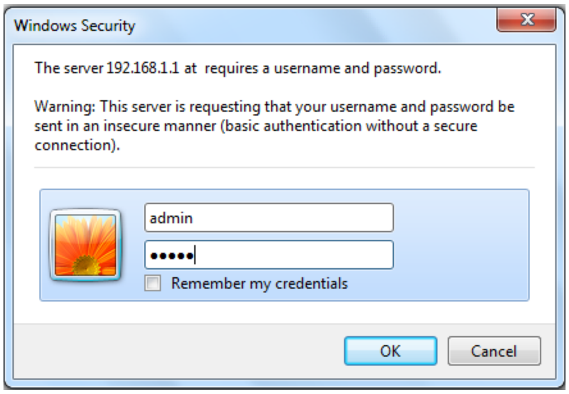
Blank Page - Windows Internet Explorer

192.168.1.1

Go to ' 192.168.1.1 '

2. Enter IP **192.168.1.1** into you address filter.

Caution: If you have changed the SMAC5800 LAN IP address, make sure you enter the correct IP Address.



Windows Security

The server 192.168.1.1 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

•••••

□ Remember my credentials

3. After connected to the SMAC5800 successfully, browser will pop out a Windows Security window. Please enter the correct **Username** and **Password**.

4. The default Username and Password are both **admin**.

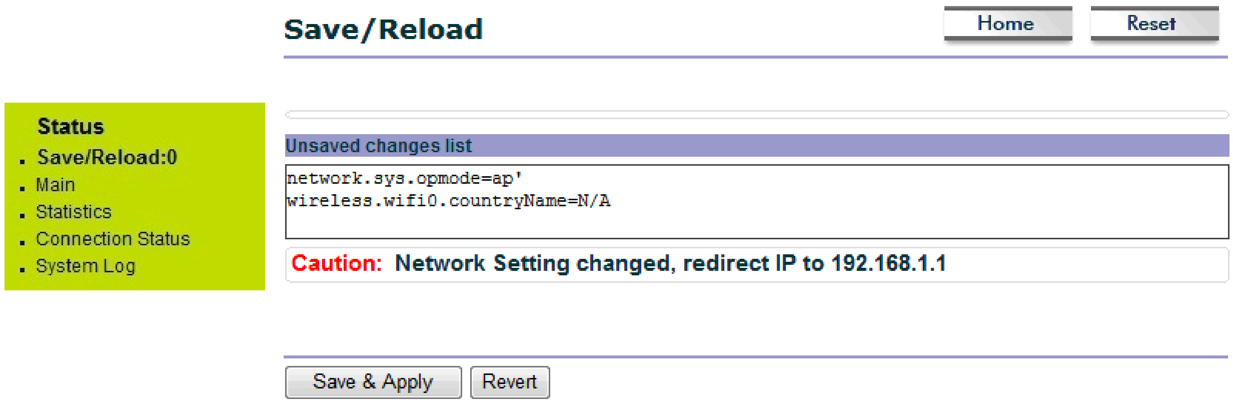
NOTE If you have changed the Username and Password, please enter your own Username and Password. **Password length** should be **minimum 8** and **maximum 16**.

3 Status

Status section is on the navigation drop-down menu. You will then see the options: Main, Statistics, Wireless Client List, System Log and Connection Status. Each option is described in detail below.

3.1 Save/Load

This page allows viewing the modified changes. The changes show in the Unsaved changes list table. You can decide to cancel all the changes or to compile to the new setting.



```
network.sys.opmode=ap'
wireless.wifi0.countryName=N/A
```

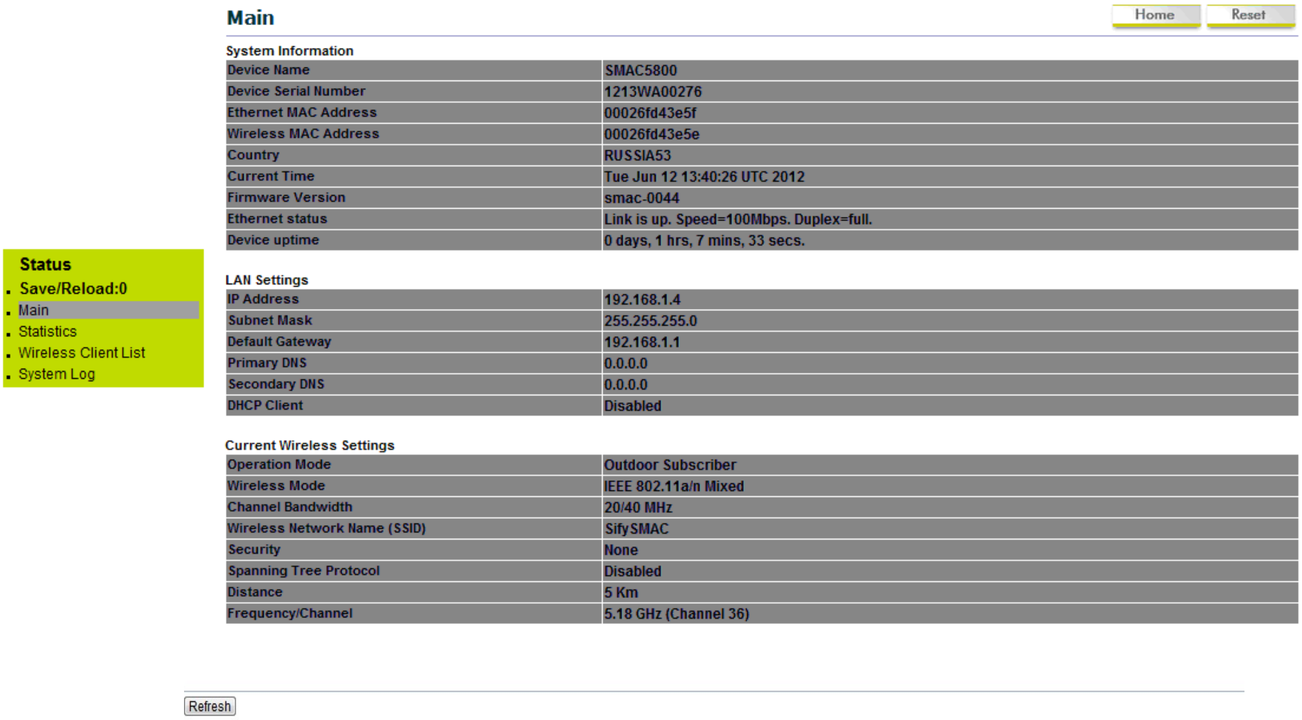
Caution: Network Setting changed, redirect IP to 192.168.1.1

NOTE

You cannot cancel the specific settings. You can only compile all the settings or revert to the previous settings.

3.2 Main

Click on the **Main** link under the **Status** drop-down menu or click **Home** from the top-right of the webpage. The status that is displayed corresponds with the operating mode that is selected. Information such as operating mode, system up time, firmware version, serial number, kernel version and application version are displayed in the 'System' section. LAN IP address, subnet mask, and MAC address are displayed in the 'LAN' section. In the 'Wireless section, the frequency, channel is displayed. The details of each SSID and its security settings are displayed.



Main

System Information

Device Name	SMAC5800
Device Serial Number	1213WA00276
Ethernet MAC Address	00026fd43e5f
Wireless MAC Address	00026fd43e5e
Country	RUSSIA53
Current Time	Tue Jun 12 13:40:26 UTC 2012
Firmware Version	smac-0044
Ethernet status	Link is up. Speed=100Mbps. Duplex=full.
Device uptime	0 days, 1 hrs, 7 mins, 33 secs.

LAN Settings

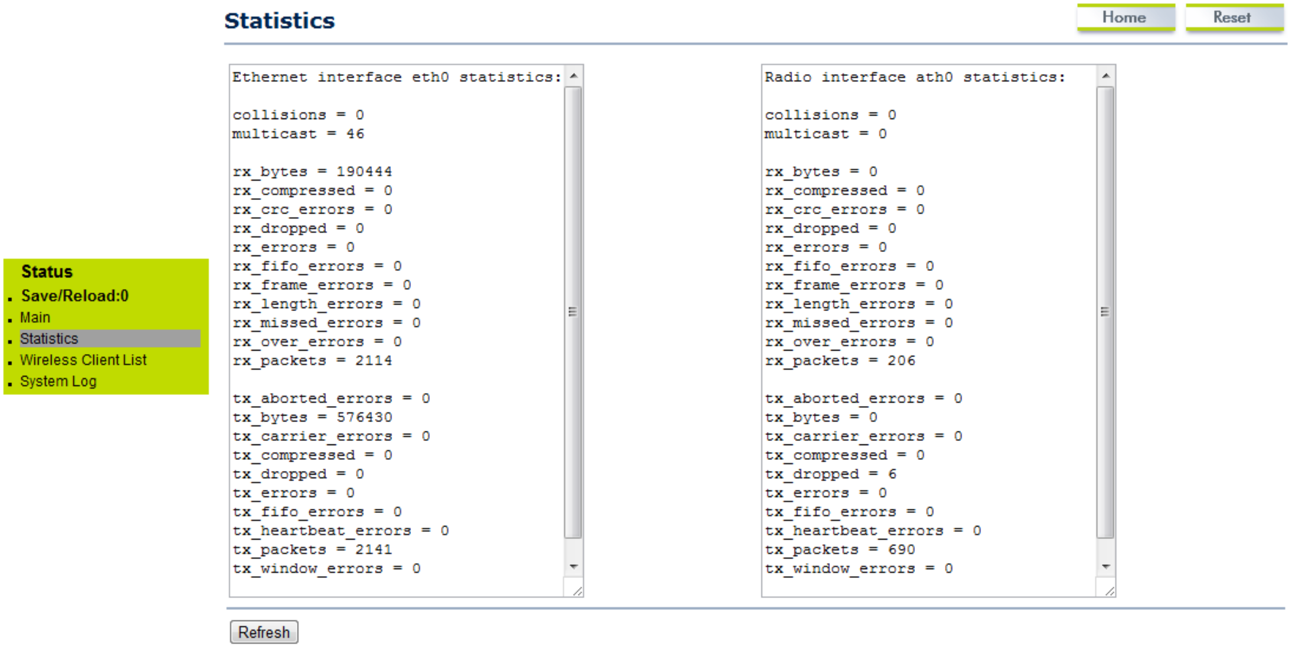
IP Address	192.168.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	Outdoor Subscriber
Wireless Mode	IEEE 802.11a/n Mixed
Channel Bandwidth	20/40 MHz
Wireless Network Name (SSID)	SifySMAC
Security	None
Spanning Tree Protocol	Disabled
Distance	5 Km
Frequency/Channel	5.18 GHz (Channel 36)

3.3 Statistics

Under the **Status** drop-down menu Click **Statistics** we can see the Ethernet and wireless interface statistics.



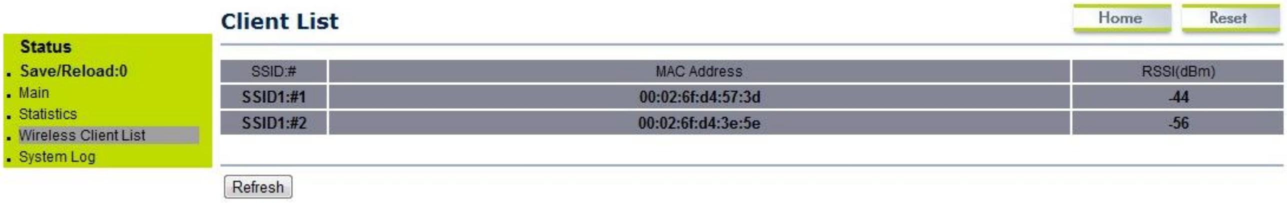
```
Ethernet interface eth0 statistics:

collisions = 0
multicast = 46

rx_bytes = 190444
rx_compressed = 0
rx_crc_errors = 0
rx_dropped = 0
rx_errors = 0
rx_fifo_errors = 0
rx_frame_errors = 0
rx_length_errors = 0
rx_missed_errors = 0
rx_over_errors = 0
rx_packets = 2114

tx_aborted_errors = 0
tx_bytes = 576430
tx_carrier_errors = 0
tx_compressed = 0
tx_dropped = 0
tx_errors = 0
tx_fifo_errors = 0
tx_heartbeat_errors = 0
tx_packets = 2141
tx_window_errors = 0
```

```
Radio interface ath0 statistics:

collisions = 0
multicast = 0

rx_bytes = 0
rx_compressed = 0
rx_crc_errors = 0
rx_dropped = 0
rx_errors = 0
rx_fifo_errors = 0
rx_frame_errors = 0
rx_length_errors = 0
rx_missed_errors = 0
rx_over_errors = 0
rx_packets = 206

tx_aborted_errors = 0
tx_bytes = 0
tx_carrier_errors = 0
tx_compressed = 0
tx_dropped = 6
tx_errors = 0
tx_fifo_errors = 0
tx_heartbeat_errors = 0
tx_packets = 690
tx_window_errors = 0
```

3.4 Wireless Client List

Click on the **Wireless Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the SMAC5800.

The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list. Default refresh time will be 10 seconds.



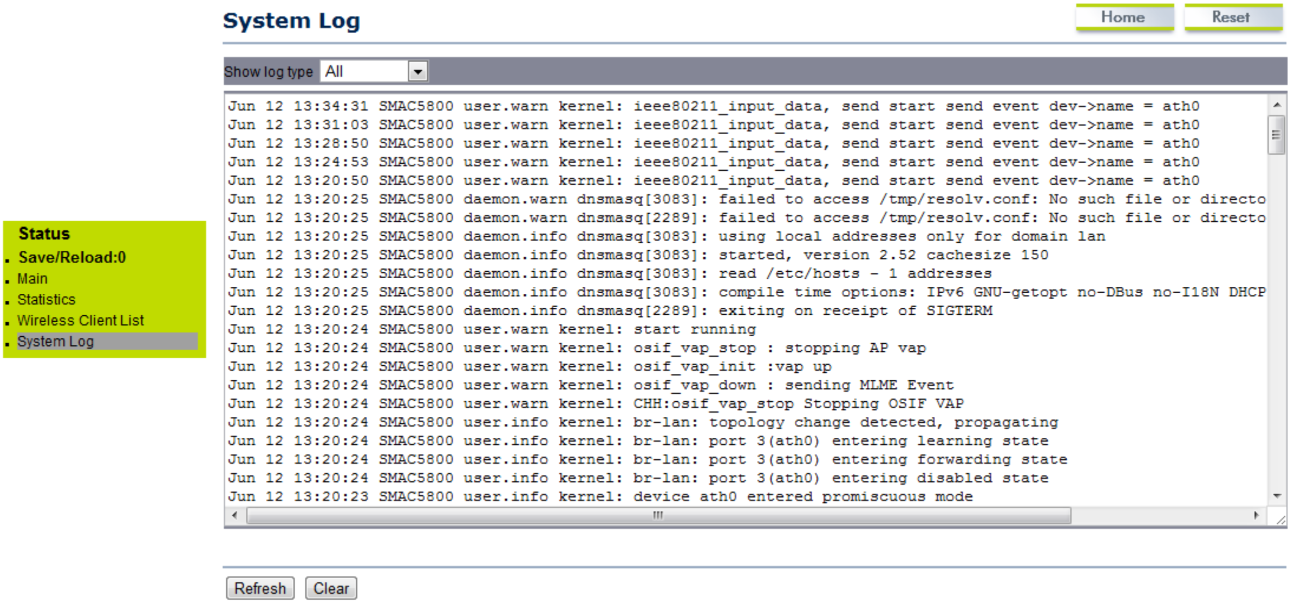
SSID:#	MAC Address	RSSI(dBm)
SSID1:#1	00:02:6f:d4:57:3d	-44
SSID1:#2	00:02:6f:d4:3e:5e	-56

NOTE

This will be shown in Outdoor Base mode only.

3.5 System Log

Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

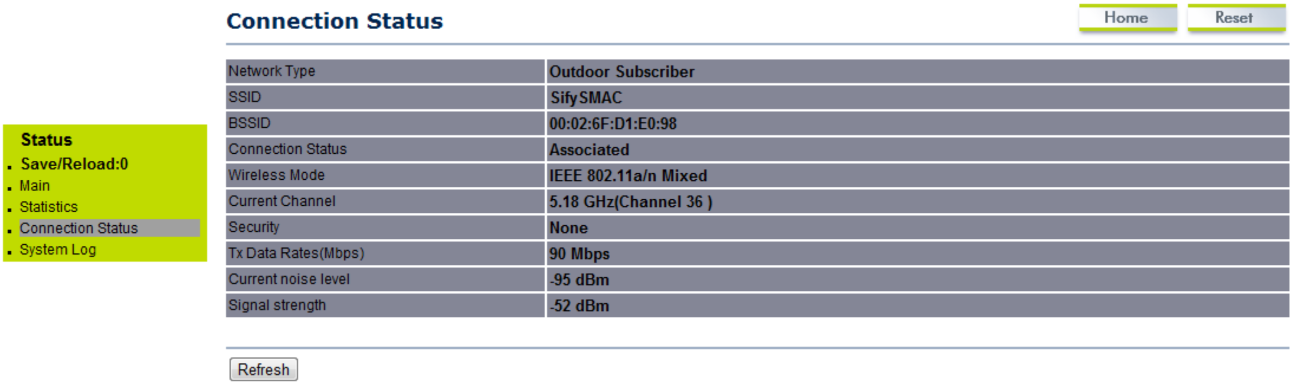


Show log type: All

```
Jun 12 13:34:31 SMAC5800 user.warn kernel: ieee80211_input_data, send start send event dev->name = ath0
Jun 12 13:31:03 SMAC5800 user.warn kernel: ieee80211_input_data, send start send event dev->name = ath0
Jun 12 13:28:50 SMAC5800 user.warn kernel: ieee80211_input_data, send start send event dev->name = ath0
Jun 12 13:24:53 SMAC5800 user.warn kernel: ieee80211_input_data, send start send event dev->name = ath0
Jun 12 13:20:50 SMAC5800 user.warn kernel: ieee80211_input_data, send start send event dev->name = ath0
Jun 12 13:20:25 SMAC5800 daemon.warn dnsmasq[3083]: failed to access /tmp/resolv.conf: No such file or directo
Jun 12 13:20:25 SMAC5800 daemon.warn dnsmasq[2289]: failed to access /tmp/resolv.conf: No such file or directo
Jun 12 13:20:25 SMAC5800 daemon.info dnsmasq[3083]: using local addresses only for domain lan
Jun 12 13:20:25 SMAC5800 daemon.info dnsmasq[3083]: started, version 2.52 cachesize 150
Jun 12 13:20:25 SMAC5800 daemon.info dnsmasq[3083]: read /etc/hosts - 1 addresses
Jun 12 13:20:25 SMAC5800 daemon.info dnsmasq[3083]: compile time options: IPv6 GNU-getopt no-DBus no-I18N DHCP
Jun 12 13:20:25 SMAC5800 daemon.info dnsmasq[2289]: exiting on receipt of SIGTERM
Jun 12 13:20:24 SMAC5800 user.warn kernel: start running
Jun 12 13:20:24 SMAC5800 user.warn kernel: osif_vap_stop : stopping AP vap
Jun 12 13:20:24 SMAC5800 user.warn kernel: osif_vap_init :vap up
Jun 12 13:20:24 SMAC5800 user.warn kernel: osif_vap_down : sending MLME Event
Jun 12 13:20:24 SMAC5800 user.warn kernel: CHH:osif_vap_stop Stopping OSIF VAP
Jun 12 13:20:24 SMAC5800 user.info kernel: br-lan: topology change detected, propagating
Jun 12 13:20:24 SMAC5800 user.info kernel: br-lan: port 3(ath0) entering learning state
Jun 12 13:20:24 SMAC5800 user.info kernel: br-lan: port 3(ath0) entering forwarding state
Jun 12 13:20:24 SMAC5800 user.info kernel: br-lan: port 3(ath0) entering disabled state
Jun 12 13:20:23 SMAC5800 user.info kernel: device ath0 entered promiscuous mode
```

3.5 Connection Status

Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.



Connection Status

Network Type	Outdoor Subscriber
SSID	Sify SMAC
BSSID	00:02:6F:D1:E0:98
Connection Status	Associated
Wireless Mode	IEEE 802.11a/n Mixed
Current Channel	5.18 GHz(Channel 36)
Security	None
Tx Data Rates(Mbps)	90 Mbps
Current noise level	-95 dBm
Signal strength	-52 dBm

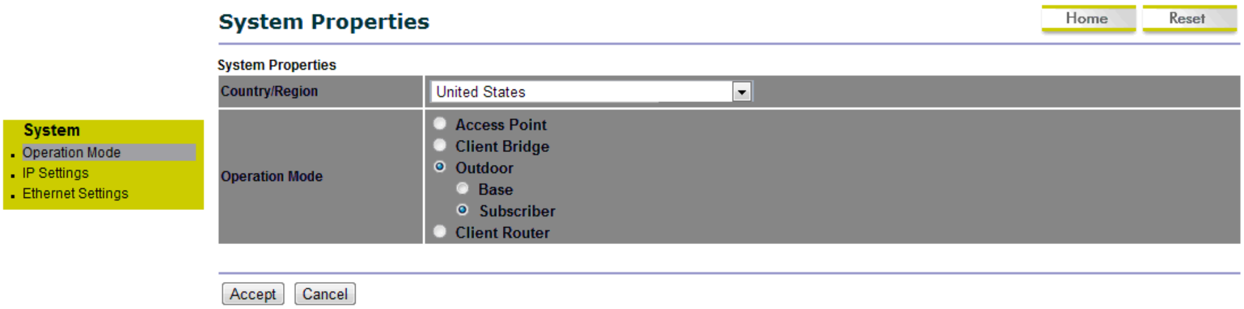
NOTE

This will be shown in **Outdoor Subscriber** mode only.

4 System

4.1 Switching Operation Mode

The SMAC5800 supports operation modes: Outdoor Base, Outdoor Subscriber. In order to switching between the operating modes, please go to **System ->** click **Operation mode**.



System Properties

System Properties

Country/Region	United States
Operation Mode	○ Access Point ○ Client Bridge ● Outdoor ○ Base ● Subscriber ○ Client Router

Country/Region: Select a Country/Region to conform local regulation.

Operation Mode: Select an operation mode via **Radio Button**.

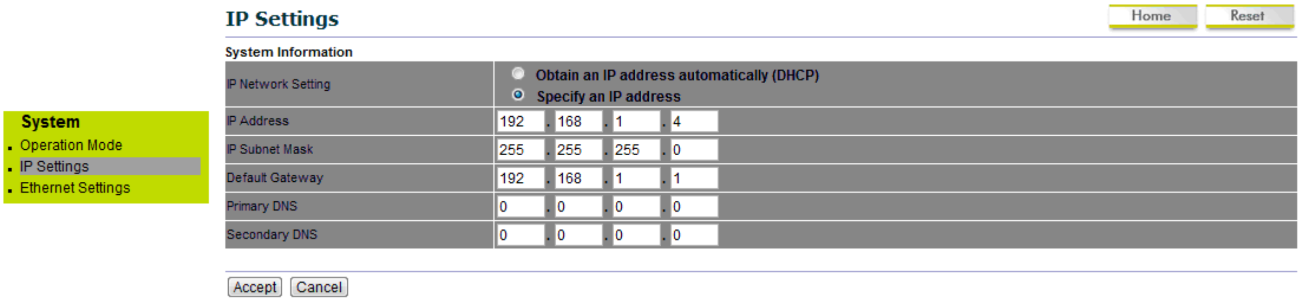
Click **Accept** to confirm the changes.

CAUTION

Accept does not compile the changes, you must go to Status -> Save/Load to apply the new settings.

4.2 IP Settings:

Go to **System ->** Click **IP settings**



System
- Operation Mode
- IP Settings
- Ethernet Settings

IP Settings

Home Reset

System Information

P Network Setting	○ Obtain an IP address automatically (DHCP) ● Specify an IP address
P Address	192 . 168 . 1 . 4
P Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 1 . 1
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

Accept Cancel

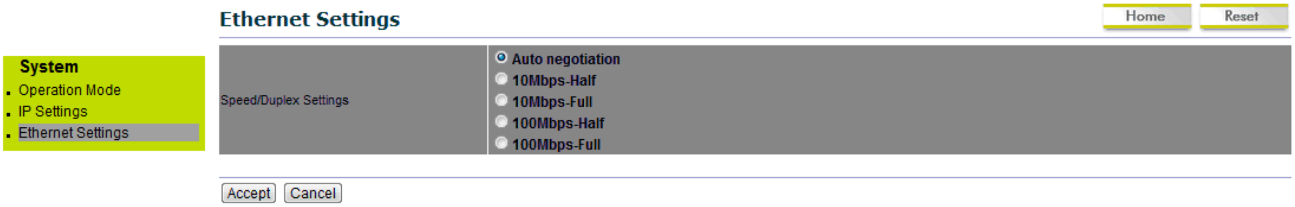
IP Network Setting	Select Radio button for **Obtain an IP address automatically** or **Specify an IP address**.
IP Address	Specify LAN port IP address.
IP Suet Mask	Specify Subnet Mask.
Default Gateway	Specify Default Gateway
Primary DNS	Specify Primary DNS
Secondary DNS	Specify Secondary DNS
Accept / Cancel	Press Accept to confirm the changes or Cancel to return previous settings.

CAUTION

Accept does not compile the changes, you must go to Status -> Save/Load to apply the new settings.

4.3 Ethernet Settings:

Go to **System -> Ethernet settings** to change the speed and duplex of the device SMAC5800.



Ethernet Settings

Speed/Duplex Settings
● Auto negotiation
○ 10Mbps-Half
○ 10Mbps-Full
○ 100Mbps-Half
○ 100Mbps-Full

5 Wireless Configuration

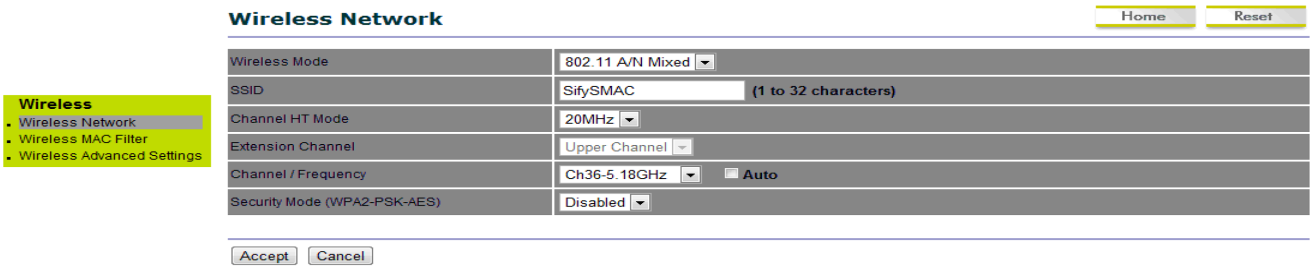
This section will guide you through all the wireless settings. Please read the instruction carefully. Inappropriate setting could lower the performance or affect the network structure. Before you continue, please make sure you have chosen the correct operating mode.

5.1.0 Wireless Settings

This section is the basic wireless settings. Please read the description carefully and check the steps on chapter 10 in case you need more detail information.

5.1.1 Outdoor Base Mode

Under **Wireless** → Click **wireless Network**



Wireless Network

Wireless Mode	802.11 A/N Mixed
SSID	SifySMAC (1 to 32 characters)
Channel HT Mode	20MHz
Extension Channel	Upper Channel
Channel / Frequency	Ch36-5.18GHz □ Auto
Security Mode (WPA2-PSK-AES)	Disabled

Wireless Mode	The wireless mode supports **802.11a/n** mixed modes. It is compatible with the most common known wireless band.

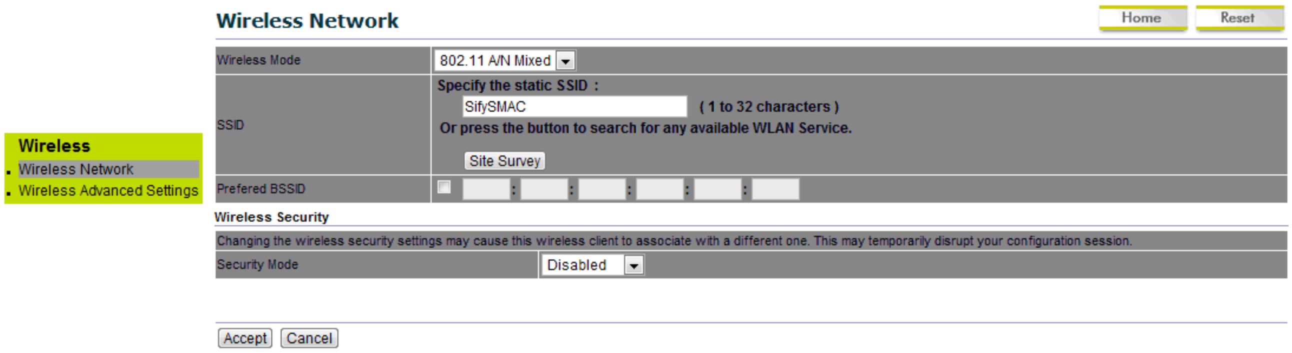
Channel HT Mode	The default channel bandwidth is **20 MHz**. The larger channel can provide better transmit quality and speed. 5/10/20 and 40 Mhz options are available
Extension Channel	Specify the upper channel or lower channel selection. It may influence the Auto channel function
Channel / Frequency	The channel availability is based on the country's regulation.
Auto	Place a **Check** mark to enable Auto channel selection.
Current Profile	Configure the SSID, it can help to divide group of clients to access the network. Just **Edit** to configure the profile.

CAUTION

Accept does not compile the changes, you must go to Status -> Save/Load to apply the new settings.

5.1.2 Outdoor Subscriber

Under **Wireless** → Click **wireless Network**



Wireless Network

Wireless Mode	802.11 A/N Mixed
SSID	Specify the static SSID : SifySMAC (1 to 32 characters) Or press the button to search for any available WLAN Service.
Prefered BSSID	□ : : : : :

Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	Disabled

Wireless Mode	The wireless mode supports **802.11a/n** mixed modes. It is compatible with the most common known wireless band.

Channel HT Mode	Automatically detect the change when changed on Outdoor base
Channel / Frequency	Automatically detect the change when changed on Outdoor base
Accept / Cancel	Press Accept to confirm the changes or Cancel to return previous settings.
Current Profile	Configure the SSID, it can help to divide group of clients to access the network .Just **Edit** to configure the profile.

CAUTION

Accept does not compile the changes, you must go to Status -> Save/Load to apply the new settings. Please refer to the chapter 4.1 for more detail.

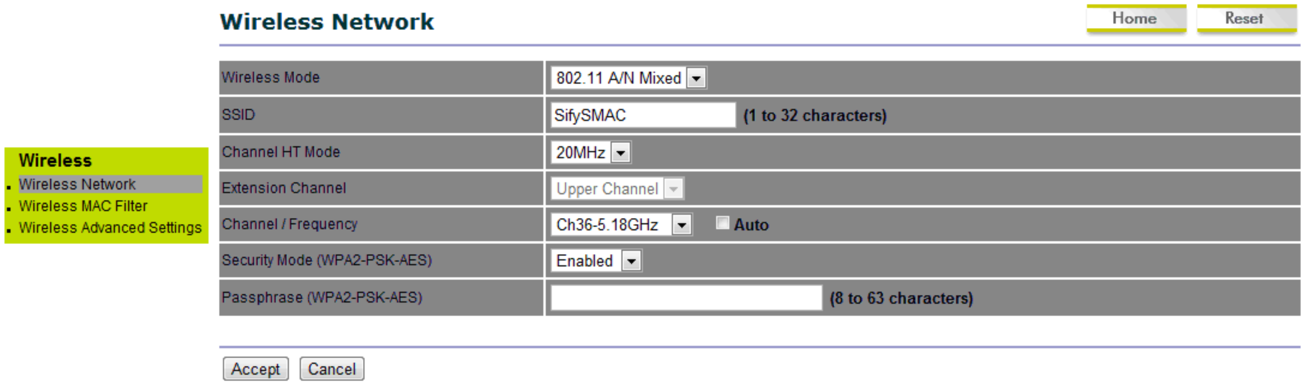
5.2 Wireless Security Settings

Wireless Security Settings section will guide you to the entire Security mode configuration:

We strongly recommend that WPA2-PSK as your security settings.

For Outdoor Base:

Under **Wireless** → Click **wireless Network**



Wireless Network

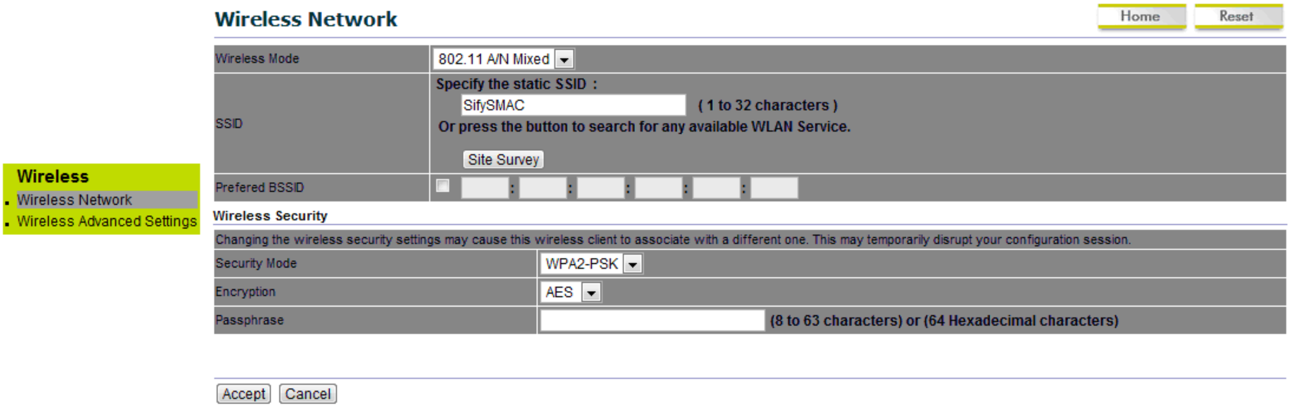
Wireless Mode	802.11 A/N Mixed
SSID	SifySMAC (1 to 32 characters)
Channel HT Mode	20MHz
Extension Channel	Upper Channel
Channel / Frequency	Ch36-5.18GHz □ Auto
Security Mode (WPA2-PSK-AES)	Enabled
Passphrase (WPA2-PSK-AES)	(8 to 63 characters)

Security Mode	Select **Enabled** from the drop down list to begin the configuration.

Encryption	Advanced Encryption System.
Passphrase	Specify the security password.
Passphrase Length	64 Hexadecimal characters password length.(**minimum 8 characters)**

For Outdoor Subscriber:

Under **Wireless** → Click **wireless Network**



Wireless Network

Wireless Mode	802.11 A/N Mixed
SSID	Specify the static SSID : SifySMAC (1 to 32 characters) Or press the button to search for any available WLAN Service.
Prefered BSSID	□ : : : : :

Wireless Security

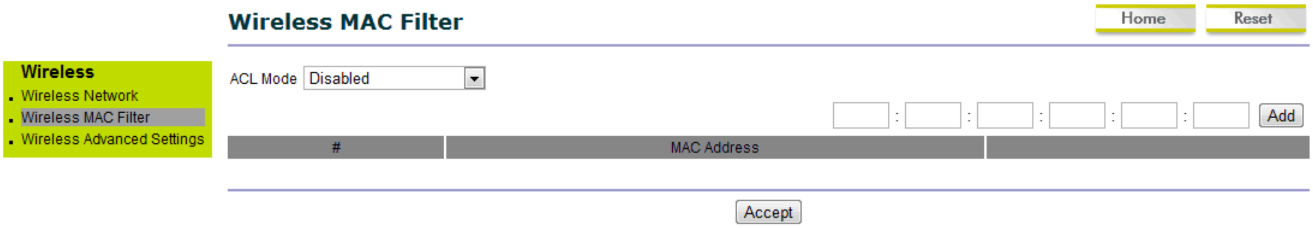
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	AES
Passphrase	(8 to 63 characters) or (64 Hexadecimal characters)

Security Mode	Select **WPA-PSK** from the drop down list to begin the configuration.
Encryption	Select **AES** for Encryption type.
Passphrase	Specify the security password.
Passphrase Length	64 Hexadecimal characters password length.(**minimum 8 characters**)

5.3 Wireless MAC Filter

Wireless MAC Filters is used to Allow or Deny wireless clients, by their MAC addresses, accessing the Network. You can manually add a MAC address to restrict the permission to access SMAC5800. The default setting is Disable Wireless MAC Filters.

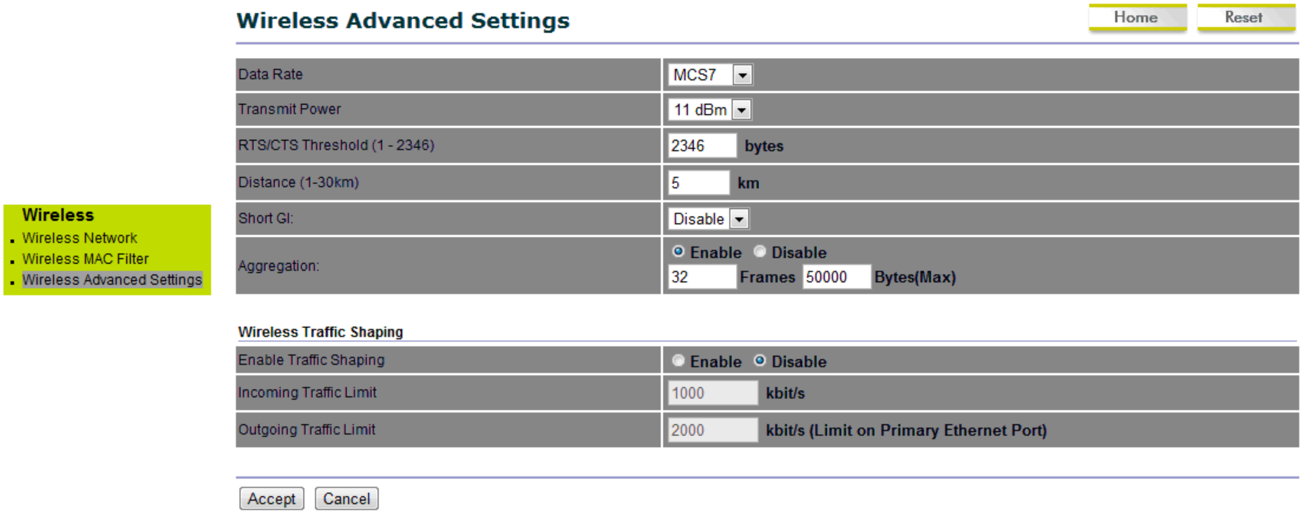


ACL Mode Disabled

ACL Mode	ACL Mode can help to deny or allow certain Client to access the network. Select Disable Deny MAC in the list or Allow MAC in the list from the drop down list.
MAC Address Filter	Specify the Wireless MAC address manually.
Add	Press **Add** to add the Wireless MAC address in the table.
Apply	Press **Apply** to apply the changes.

5.4 Wireless Advanced Settings

Under **Wireless** → Click **Wireless Advanced Settings**



Data Rate	MCS7
Transmit Power	11 dBm
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	5 km
Short GI:	Disable
Aggregation:	● Enable ○ Disable 32 Frames 50000 Bytes(Max)

Wireless Traffic Shaping

Enable Traffic Shaping	○ Enable ● Disable
Incoming Traffic Limit	1000 kbit/s
Outgoing Traffic Limit	2000 kbit/s (Limit on Primary Ethernet Port)

Data Rate	Select Data Rate from the drop down list. Data rate will affect the efficiency of the throughput. If the data rate is set to a small number, the lower through will get but it can transmit to longer distance.

Transmit Power	Select Transmit Power to increase or decrease Transmit Power. Higher transmit power will sometimes cause unable to connect to the network. On the other hand, the lower transmit power will cause client unable to connect to the device.
RTS/CTS Threshold	Specify Threshold package size for RTC/CTS. Using small number of the threshold will cause RTS/CTS packets to be sent more often to consuming more of the available bandwidth. In addition, if the heavy load traffic occurs, the wireless network can be recovered easily from interferences or collisions.
Distance	Specify distance rage between AP and Clients. Longer distance may lose high connection speed.
Short GI	Short GI is improved of 802.11n and 802.11a/g. It can increase 10% of the internet speed during the data transmission. For example, the 802.11a/g's GI is 800us; the short GI will be 400us.
Aggregation	Aggregation is to merge the typical size of data's header to one data. It is useful for the small size but larger amount packets.
Wireless Traffic Shaping	Place a **Check** to enable Wireless Traffic Shaping function.
Incoming Traffic Limit	Specify the wireless transmission speed for downloading in Kbits/seconds
Outgoing Traffic Limit	Specify the wireless transmission speed for uploading in kbits/seconds
Accept / Cancel	Press Accept to confirm the changes or Cancel to return previous settings.

CAUTION

1. Changing Wireless Advanced Settings may cause insufficient wireless connection quality.

2. Accept does not compile the changes; you must go to Status -> Save/Load to apply the new settings.

6.0.0 Enterprise Features

10.1.0 VLAN Configuration

Three VLAN modes are supported in Bridge mode SU

1.) Access VLAN mode

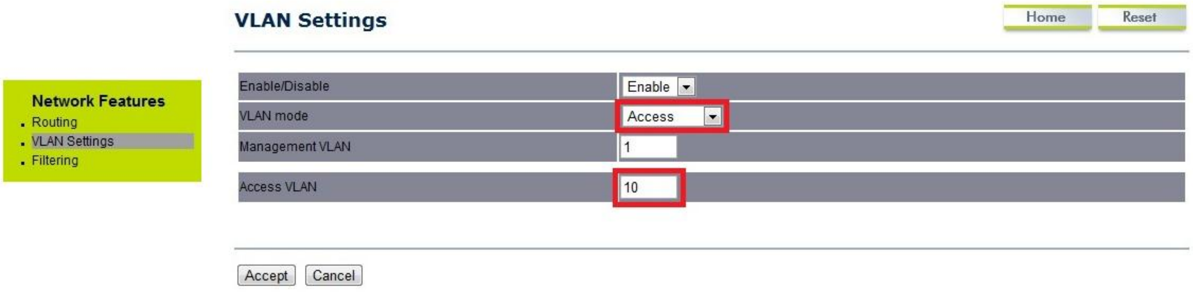
2.) Trunk mode

3.) Q-in-Q mode

Click on the **VLAN settings** under the **Network Features** menu. This function allows you to configure the different VLAN modes. VLAN mode will be available in Outdoor Subscriber mode only.

6.0.1 Access VLAN mode

Under the VLAN settings, select the VLAN mode as Access.



VLAN Settings

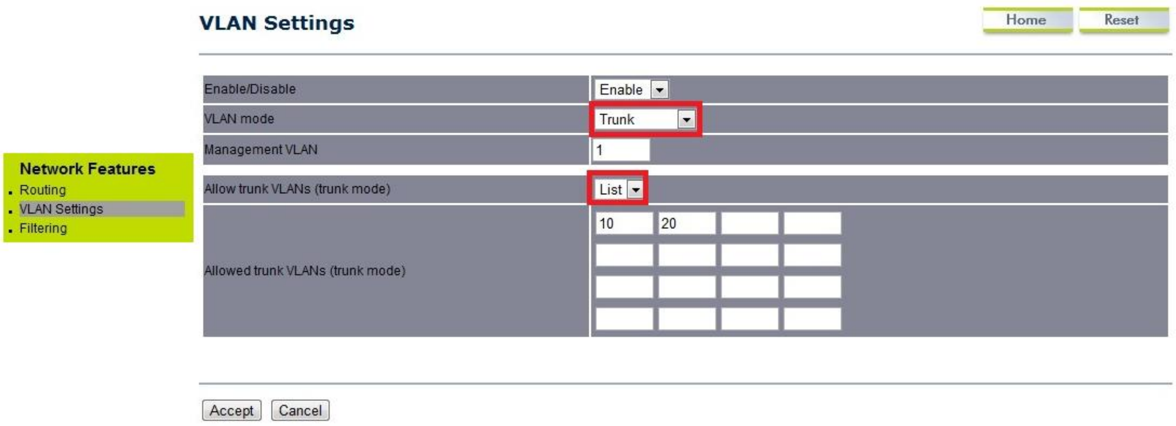
Enable/Disable	Enable
VLAN mode	Access
Management VLAN	1
Access VLAN	10

Enable/Disable	Select Enable or Disable function from the drop down list.
VLAN Mode	Select as Access for configuring in Access VLAN mode.

Management VLAN	Select the ID as one.
Access VLAN	Specify the access VLAN ID
Note	All the VLAN related changes will take effect immediately after clicking on 'accept' tab.

6.0.2 Trunk mode

Under the VLAN settings, select the mode as Trunk.



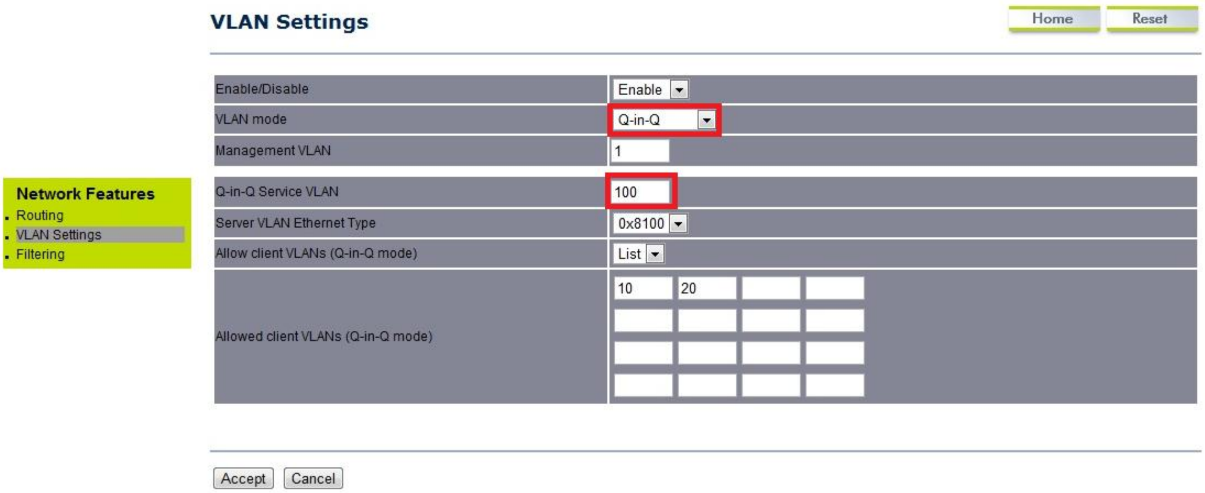
VLAN Settings

Enable/Disable	Enable
VLAN mode	Trunk
Management VLAN	1
Allow trunk VLANs (trunk mode)	List
Allowed trunk VLANs (trunk mode)	10 20

Enable/Disable	Select Enable or Disable function from the drop down list.
VLAN Mode	Select as Trunk for configuring in Access VLAN mode.
Management VLAN	Select the ID as one.
Allow trunk vlans (trunk mode)	Select 'ALL' option for allowing all the tagged packets. Select 'List' option for allow the VLANs mentioned in the boxes
Allowed trunk vlans (trunk mode)	Specify the trunk VLAN IDs. (maximum 16 VLANs allowed)
Note	All the VLAN related changes will take effect immediately after clicking on 'accept' tab.

6.0.3 QinQ mode

Under the VLAN settings, select the mode as QinQ.



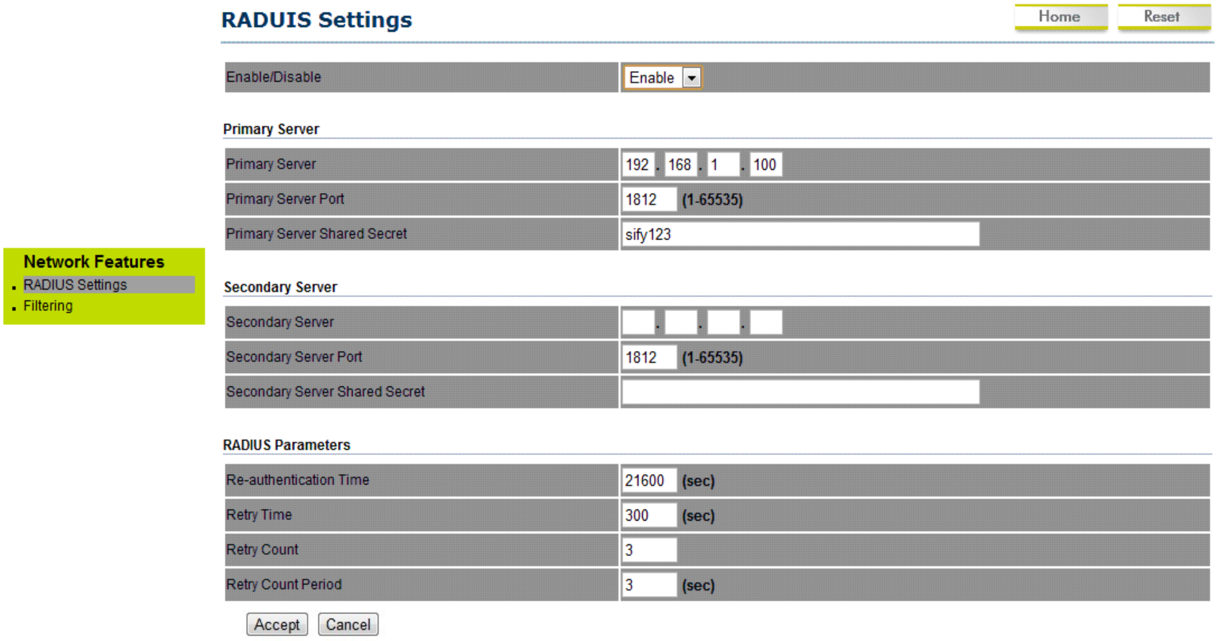
VLAN Settings

Enable/Disable	Enable
VLAN mode	Q-in-Q
Management VLAN	1
Q-in-Q Service VLAN	100
Server VLAN Ethernet Type	0x8100
Allow client VLANs (Q-in-Q mode)	List
Allowed client VLANs (Q-in-Q mode)	10 20

Enable/Disable	Select Enable or Disable function from the drop down list.
VLAN Mode	Select as QinQ for configuring in QinQ mode.
Management VLAN	Select the ID as one.
Q-in-Q service VLAN	Specify the service vlan id (outer vlan id)
Server VLAN Ethernet Type	Specify the Ethernet type
Allow client VLANs (Q-in-Q mode)	Select 'ALL' option for allowing all the tagged packets. Select 'List' option for allow the VLANs mentioned in the boxes
Allowed client VLANs(Q-in-Q mode)	Specify the client VLAN IDs. (maximum 16 VLANs allowed)
Note	All the VLAN related changes will take effect immediately after clicking on 'accept' tab.

7.0.0 Radius

Whenever a new subscriber tries to associate with AP, the AP will forward this request to the primary radius server and if Primary server is down, the request will be forwarded to the secondary server. If SU details are valid in the RADIUS server, it will associate with AP or else it will be rejected. Radius server option will be available in the outdoor Base mode (AP) only.



RADUIS Settings

Enable/Disable	Enable

Primary Server

Primary Server	192 . 168 . 1 . 100
Primary Server Port	1812 (1-65535)
Primary Server Shared Secret	sify123

Secondary Server

Secondary Server	. . .
Secondary Server Port	1812 (1-65535)
Secondary Server Shared Secret	

RADIUS Parameters

Re-authentication Time	21600 (sec)
Retry Time	300 (sec)
Retry Count	3
Retry Count Period	3 (sec)

7.0.1 Primary Server

This configuration is used to specify the primary radius server IP address.

Enable/Disable	Select Enable or Disable function from the drop down list.
Primary server	Specify the primary server IP (Data Type: IP address).
Primary server port	Specify the primary server ort (Data Type: Integer, range 1 – 65535)
Primary shared server secret	Specify the primary secret (Data Type: String)

7.0.2 Secondary Server

This configuration is used to specify the primary radius server IP address.

Request timeout	Specify the secondary server IP (Data Type: IP address).
Secondary server port	Specify the secondary server ort (Data Type: Integer, range 1 – 65535)
Secondary shared server secret	Specify the secondary secret (Data Type: String)

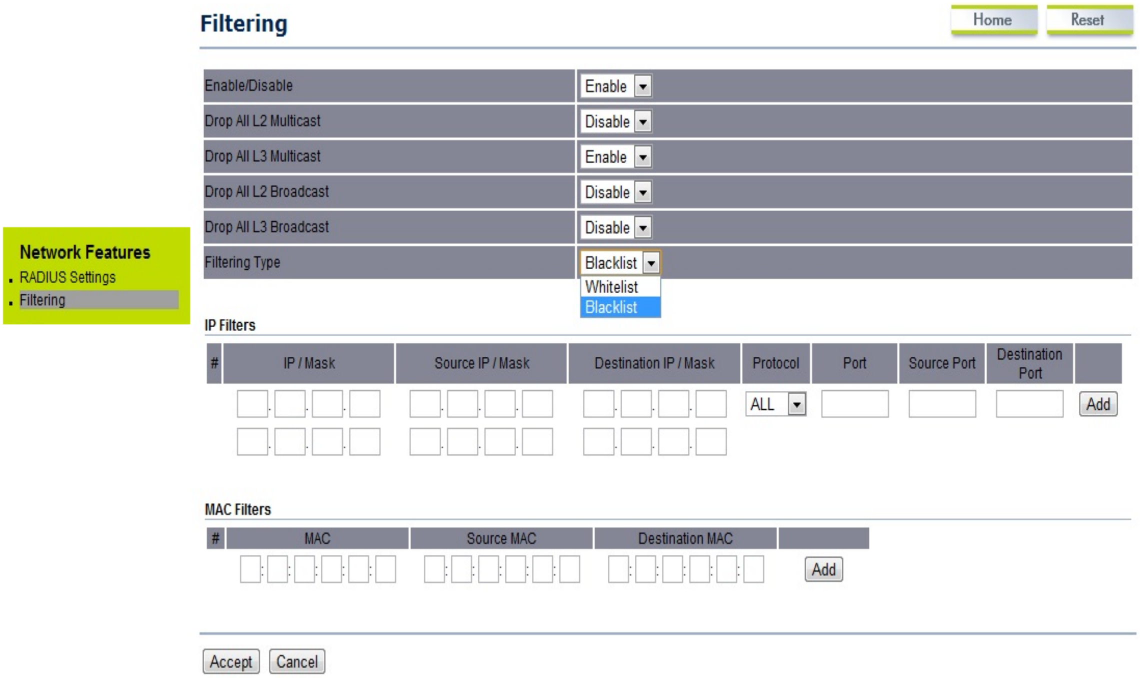
7.0.3 Radius settings

Re-authentication time	Specify the number of seconds after which the SU is re-authenticated in case of successful/unsuccessful authentications. Data Type: Integer (default 300 seconds)
Retry Time	Specify the number of seconds after which an attempt will be made to reach the primary and secondary server. AP will not forward any request to primary and secondary server for the time duration configured in retry time. Data Type: Integer (default 300 seconds)
Retry count	Specify the number of times Radius Client should try to connect to the Radius Server before giving up. Data Type: Integer (default 3 times)
Request count period	Specify the time gap between two requests retries. Data Type: Integer (default 3 seconds)

Note	All the radius related changes will take effect immediately after clicking on 'accept' tab.

8.0 Filtering

Click on the filtering option under the Network features menu. This page displays IP, MAC, multicast, broadcast, etc based filtering options. Filtering option is available in Outdoor base (AP) and Subscriber mode (SU).



Enable/Disable	Enable
Drop All L2 Multicast	Disable
Drop All L3 Multicast	Enable
Drop All L2 Broadcast	Disable
Drop All L3 Broadcast	Disable
Filtering Type	Blacklist

IP Filters

#	IP / Mask	Source IP / Mask	Destination IP / Mask	Protocol	Port	Source Port	Destination Port	
				ALL				Add

MAC Filters

#	MAC	Source MAC	Destination MAC	
				Add

8.0.1 Global filtering

Enable/Disable	Select Enable or Disable function from the drop down list.
Drop All L2 Multicast	Select Enable or Disable function from the drop down list. By default it's disabled.
Drop All L3 Multicast	Select Enable or Disable function from the drop down list. . By default it's enabled.
Drop All L2 Broadcast	Select Enable or Disable function from the drop down list. By default it's disabled.
Drop All L3 Broadcast	Select Enable or Disable function from the drop down list. . By default it's disabled.
Filtering Type	Select White list/Blacklist from the drop down list. Black list – By default all the data traffic is allowed, it will block the traffic based on the filter rule is applied. White list – By default all the data traffic is blocked, it will allow the traffic based on the filter rule is applied.
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab.

8.0.2 IP Filtering

IP	Specify the IP address.
MASK	Specify the IP sub mask.
SOURCE IP	Specify the Source IP address.
SOURCE MASK	Specify the Source sub mask.
DESTINATION IP	Specify the Destination IP address
DESTINATION MASK	Specify the Destination sub mask
Protocol	Specify the protocol name

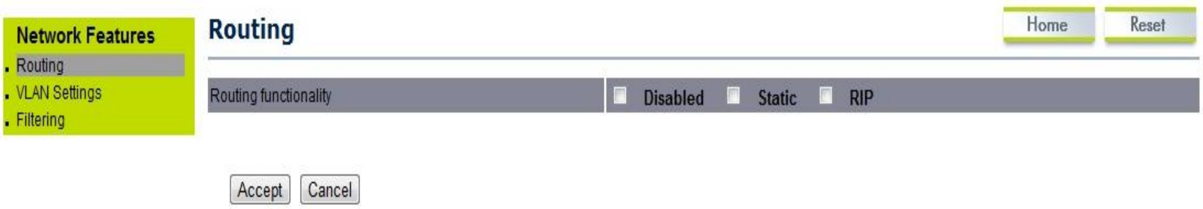
Port	Specify the port number.
Source port	Specify the Source port number
Destination port	Specify the Source port number
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab.

8.0.3 MAC Filtering

MAC	Specify the MAC address.
SOURCE MAC	Specify the Source MAC address.
DESTINATION MAC	Specify the Destination MAC address
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab.

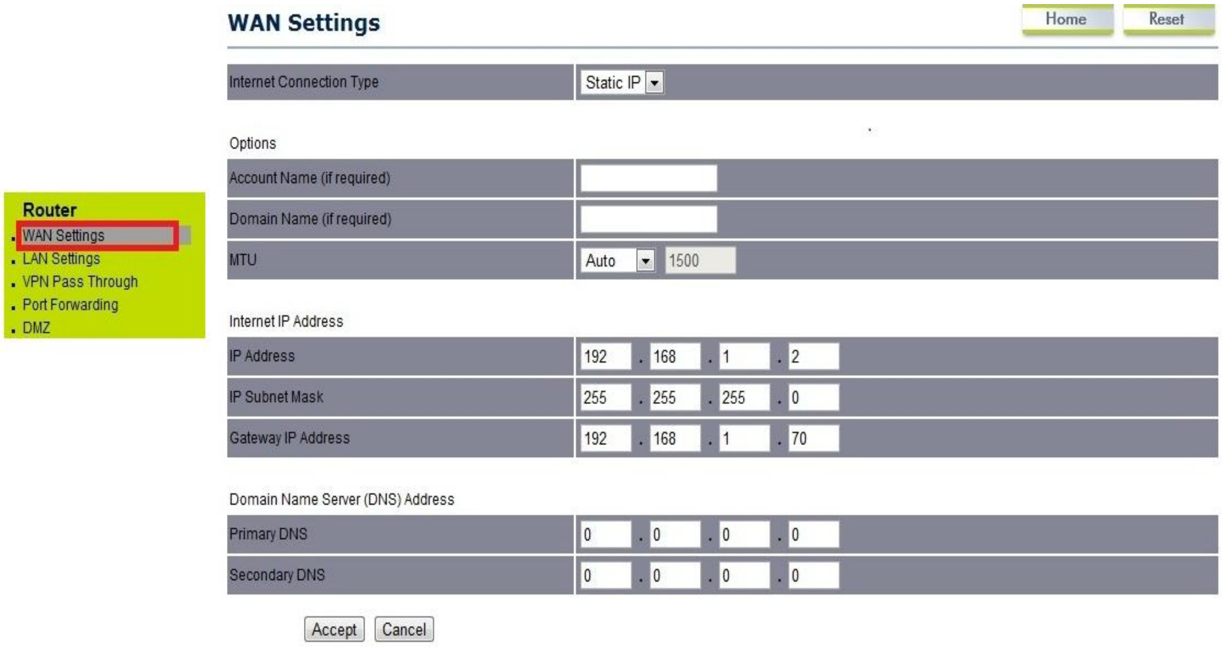
9.0 Routing

Click on the Routing option under the Network features menu and uncheck the disabled dialogue box. This page displays Static, RIP functions; Routing option will be available in Outdoor Subscriber (SU mode only)



Routing functionality ☐ Disabled ☐ Static ☐ RIP

Click on the WAN Settings option under the Router menu for configuring the Wireless IP address.



WAN Settings

Internet Connection Type: Static IP

Options

Account Name (if required):

Domain Name (if required):

MTU: Auto 1500

Internet IP Address

IP Address: 192 . 168 . 1 . 2

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 1 . 70

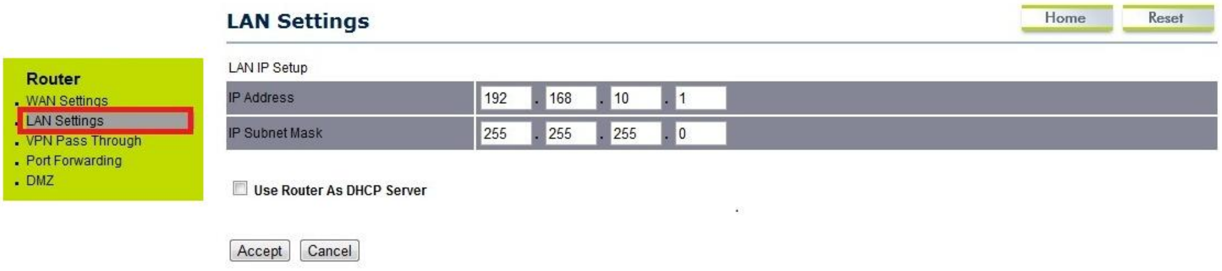
Domain Name Server (DNS) Address

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

Internet Connection Type	Specify the Internet connection type from the drop down menu. Default is Static IP.
Account Name (If required)	Specify the Account Name if required.
Domain Name(If required)	Specify the Domain Name if required.
MTU	Specify the MTU value. Suggest remain in Auto configuration
IP Address	Specify the IP address.
IP Subnet Mask	Specify the Subnet Mask.
Gateway IP Address	Specify Gateway IP address.
Primary DNS	Specify Primary DNS server IP address
Secondary DNS	Specify Secondary DNS server IP address

Click on the LAN Settings option under the Router menu for configuring the LAN IP address.



LAN Settings

LAN IP Setup

IP Address: 192 . 168 . 10 . 1

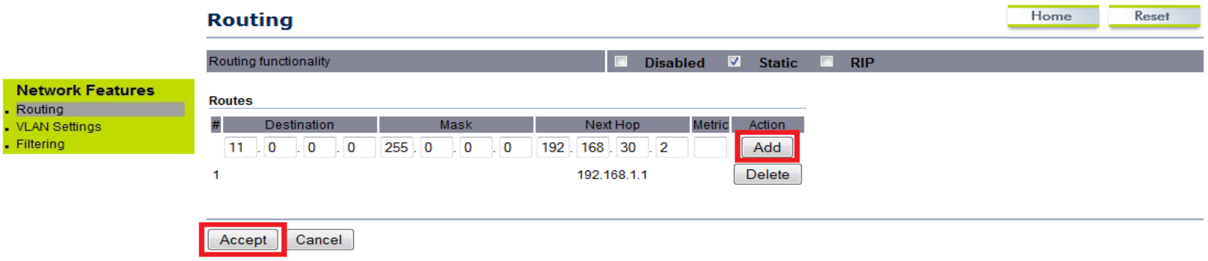
IP Subnet Mask: 255 . 255 . 255 . 0

□ Use Router As DHCP Server

IP Address	Specify the IP address.
IP Subnet Mask	Specify the Subnet Mask.
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab. Maximum it can support 100 routes in static routing mode.

9.0.1 Static Routing

Check the dialogue box of static option for enabling the static routing function. RIP dialogue box has to be unchecked.



Routing

Routing functionality: □ Disabled ☑ Static □ RIP

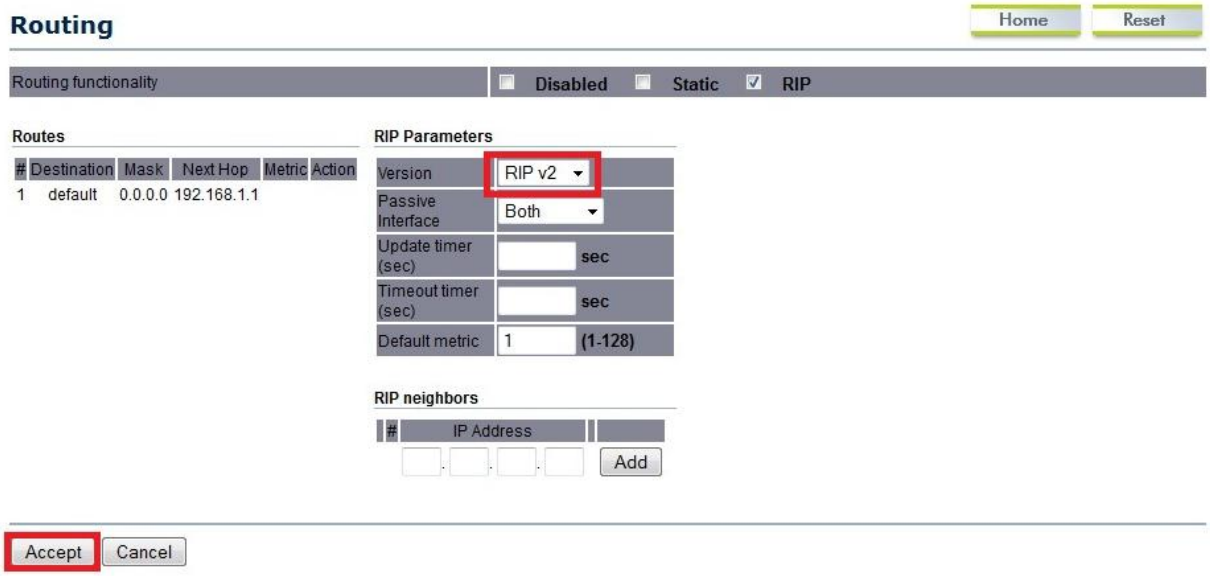
Routes

#	Destination	Mask	Next Hop	Metric	Action
	11 . 0 . 0 . 0	255 . 0 . 0 . 0	192 . 168 . 30 . 2		Add
1			192.168.1.1		Delete

Destination	Specify the Destination IP address.
Mask	Specify the Destination Mask.
Next Hop	Specify the next hop IP address.
Metric	Specify the metric value if required.
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab. Maximum it can support 100 routes in static routing mode.

9.0.2 RIP (Routing Information Protocol)

Check the dialogue box of RIP option for enabling the static routing function. Static dialogue box has to be unchecked.



Routing functionality □ Disabled □ Static ☑ RIP

Routes

#	Destination	Mask	Next Hop	Metric	Action
1	default	0.0.0.0	192.168.1.1		

RIP Parameters

Version	RIP v2
Passive Interface	Both
Update timer (sec)	sec
Timeout timer (sec)	sec
Default metric	1 (1-128)

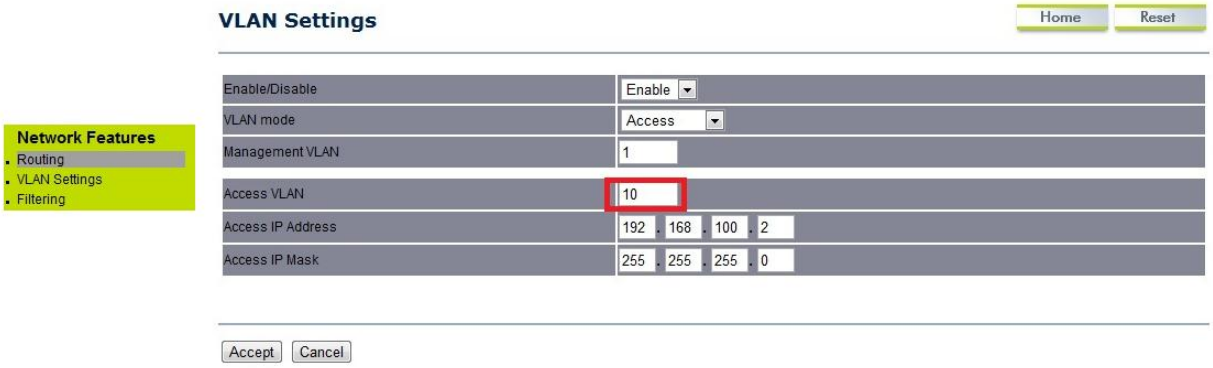
RIP neighbors

#	IP Address

Version	Specify the version 1 or 2 from the drop down menu
Passive interface	Specify the passive interface as Both/Wireless/Ethernet from the drop down menu
Update timer(sec)	Specify the update timer in seconds. Suggest remain in default configuration
Default Metric	Specify the default metric value if required. Suggest remain in default configuration value as one.
RIP Neighbour	Specify the neighbor IP address. Suggest remain in default configuration value as one.
Note	All the filter related changes will take effect immediately after clicking on 'accept' tab. Maximum it can support 100 routes in static routing mode.

9.0.3 Routing mode access VLAN

Routing mode access VLAN option will get enabled after configuring the Outdoor Subscriber (SU) in Routing mode only. Click on the VLAN settings under the Network features menu for access VLAN settings option.



VLAN Settings

Enable/Disable	Enable
VLAN mode	Access
Management VLAN	1
Access VLAN	10
Access IP Address	192 . 168 . 100 . 2
Access IP Mask	255 . 255 . 255 . 0

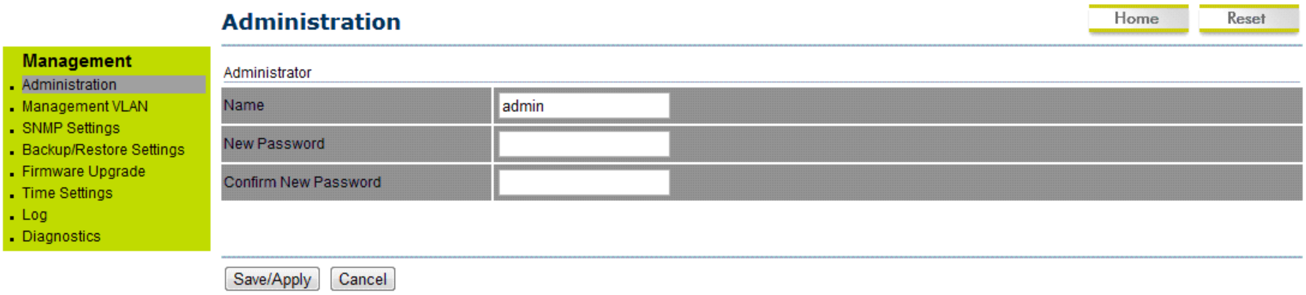
Enable/Disable	Select Enable or Disable function from the drop down list.
VLAN Mode	Select as Access for configuring in Access VLAN mode.
Management VLAN	Select the ID as one.
Access VLAN	Specify the access VLAN ID
Access IP Address	Specify the access IP Address
Access IP Mask	Specify the access IP MASK
Note	All the VLAN related changes will take effect immediately after clicking on 'accept' tab.

10 Management Settings

Management section is on the navigation drop-down menu. You will then see seven options: administration, management VLAN, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

10.1 Administration

Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured with a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



Administrator

Name	admin
New Password	
Confirm New Password	

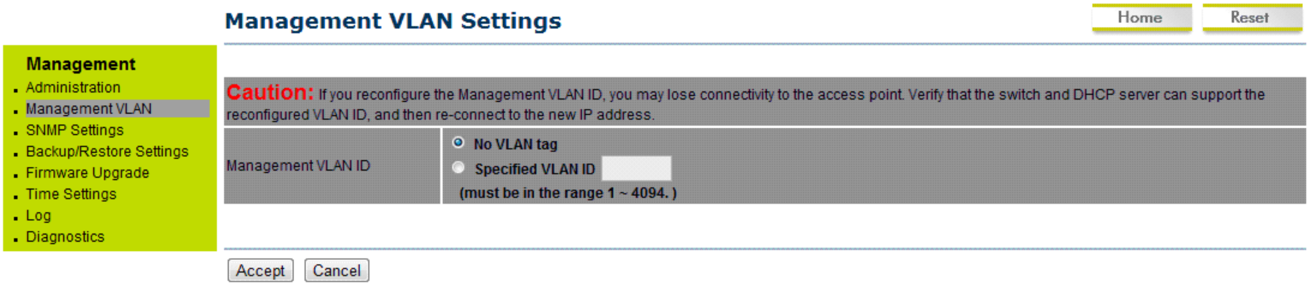
Name	Specify Username for login.
Password	Specify a Password for login
Confirm Password	Re-enter the Password for confirmation. Password length should be minimum 8 and maximum 16.
Save/Apply / Cancel	Press Save/Apply to apply the changes or Cancel to return previous settings.

CAUTION

Press Save/Apply will change the setting immediately. It will not be able to undo the action.

10.2 Management VLAN

Click on the **Management VLAN** link under the **Management** menu. This option allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN



Management VLAN Settings

Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID
● No VLAN tag
○ Specified VLAN ID
(must be in the range 1 ~ 4094.)

Management VLAN ID	If your network includes VLANs and if tagged packets need to pass through the Access Point, specify the VLAN ID into this field. If not, select the **No VLAN tag** radio button.
Accept / Cancel	Press Accept to confirm the changes or Cancel to return previous settings.

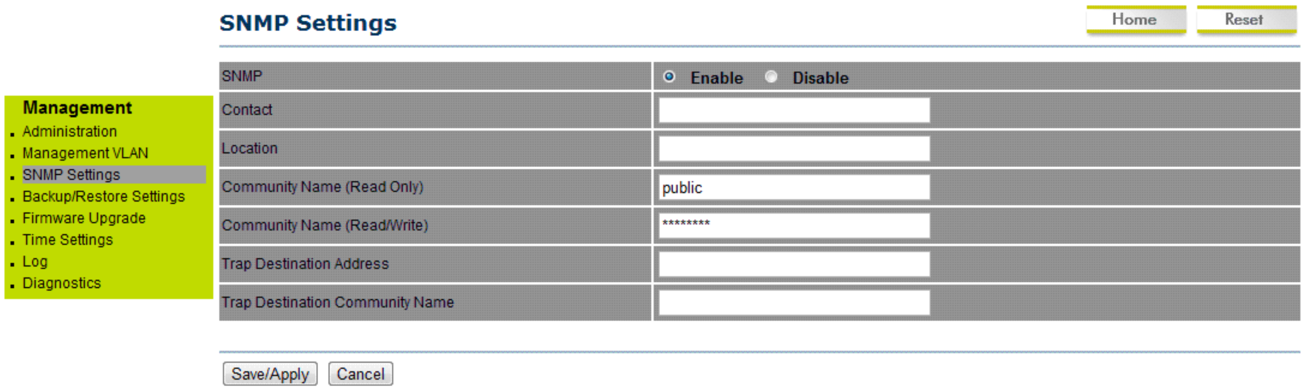
CAUTION

1. If you reconfigure the Management VLAN ID, you may lose connection to the SMAC5800. Verify DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

2. Accept does not compile the changes; you must go to Status -> Save/Load to apply the new settings. Please refer to the chapter 4.1 for more detail.

10.3 SNMP Settings

Click on the **SNMP Settings** link under the **Management** menu. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.



SNMP	● Enable ○ Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	********
Trap Destination Address	
Trap Destination Community Name	

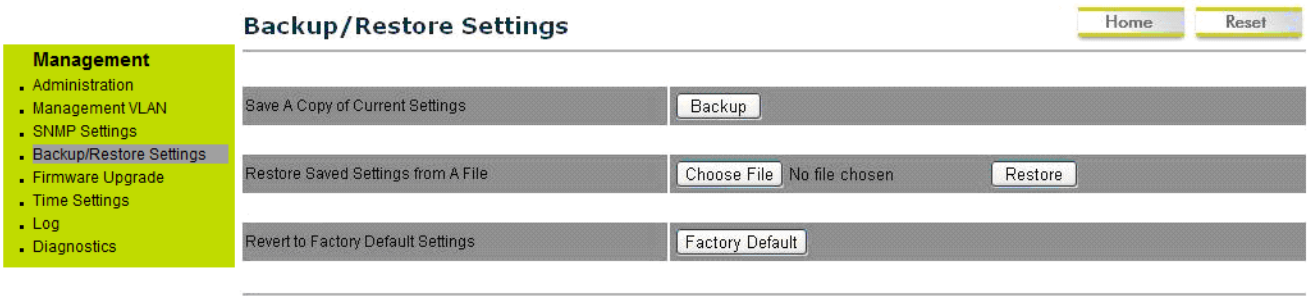
Enable/Disable	Select the Radio button to Enable or Disable SNMP function.
Contact	Specify the contact details of the device.
Location	Specify the location of the device.
Community Name(Read only)	Specify the password for access the SNMP community for read only access. By default its public; better keep it in default password.
Community Name(Read/Write)	User cant able to change the default SNMP Read/Write password.
Trap Destination IP Address	Specify the IP address that will receive the SNMP trap.
Trap Destination Community Name	Specify the Destination Community name.
Save/Apply / Cancel	Press Save/Apply to apply the changes or Cancel to return previous settings.

CAUTION

Press Save/Apply will change the setting immediately. It will not be able to undo the action.

10.4 Backup/Restore Settings

Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.



Backup/Restore Settings

Save A Copy of Current Settings

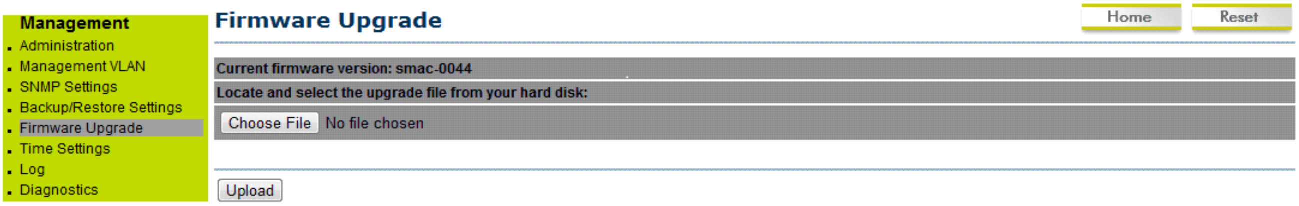
Restore Saved Settings from A File — No file chosen

Revert to Factory Default Settings

Save A Copy of Current Settings	Click on **Backup** to save current configured settings.
Restore Saved Settings from a File	SMAC5800 can restore a previous setting that has been saved. Click on Browse to select the file and Restore.
Revert to Factory Default Settings	Click on Factory Default button to reset all the settings to the default values.

10.5 Firmware Upgrade

Click on the **Firmware Upgrade** link under the **Management** menu. This page is used to upgrade the firmware of the device. Make sure that downloaded the appropriate firmware from your vendor.



Firmware Upgrade

Current firmware version: smac-0044

Locate and select the upgrade file from your hard disk:

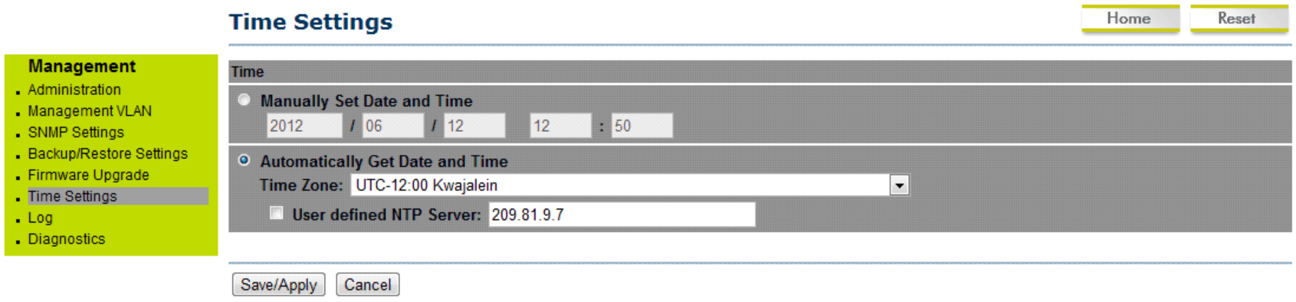
No file chosen

CAUTION

Upgrade process may take few minutes (approximate 3 minutes); please do not power off the device and it may cause the device crashed or unusable. SMAC5800 will restart automatically once the upgrade is completed.

10.6 Time Settings

Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.



Time Settings

Time

○ Manually Set Date and Time
2012 / 06 / 12 12 : 50

● Automatically Get Date and Time
Time Zone: UTC-12:00 Kwajalein
□ User defined NTP Server: 209.81.9.7

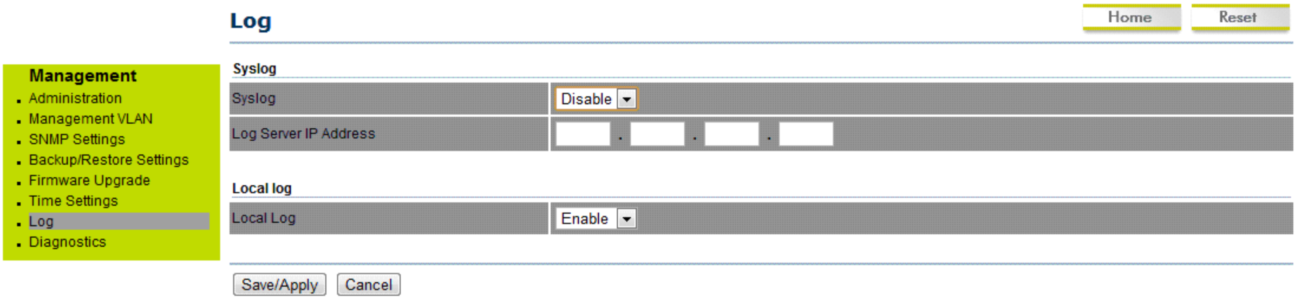
Manually Set Date and Time	Manually setup the date and time.
Automatically Get Date and Time	Specify the Time Zone from the drop down list and Place a **Check** to specify the IP address of the NTP Server manually or uses default NTP Server.
Save/Apply / Cancel	Press Save/Apply to apply the changes or Cancel to return previous settings.

CAUTION

Press Save/Apply will change the setting immediately. It will not be able to undo the action.

10.7 Log

Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.



Syslog

Syslog	Disable
Log Server IP Address	. . .

Local log

Local Log	Enable

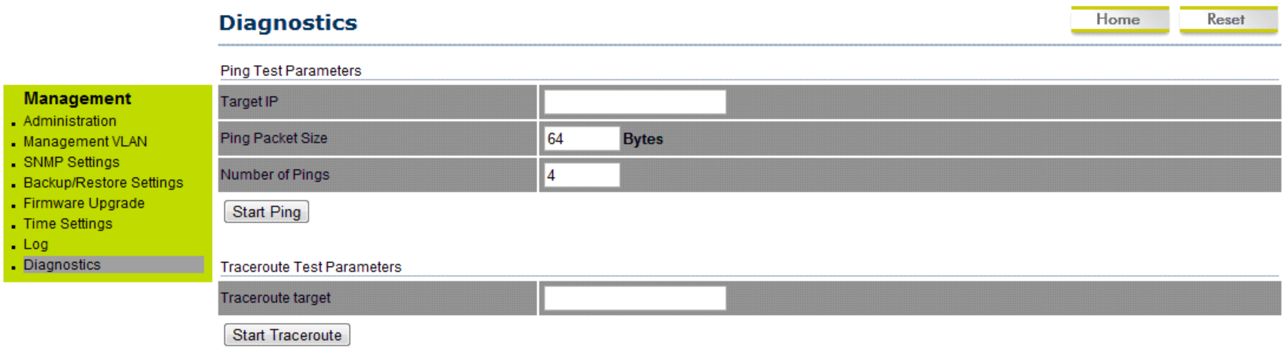
Syslog	Select Enable or Disable Syslog function from the drop down list.
Log Server IP Address	Specify the Log Server IP address.
Local Log	Select Enable or Disable Local Log service.
Save/Apply / Cancel	Press Save/Apply to apply the changes or Cancel to return previous settings.

CAUTION

Press Save/Apply will change the setting immediately. It will not be able to undo the action.

10.8 Diagnostics

Click on the **Diagnostics** link under the **Management** menu. This function allows you to detect connection quality and trace the routing table to the target.



Diagnostics

Ping Test Parameters

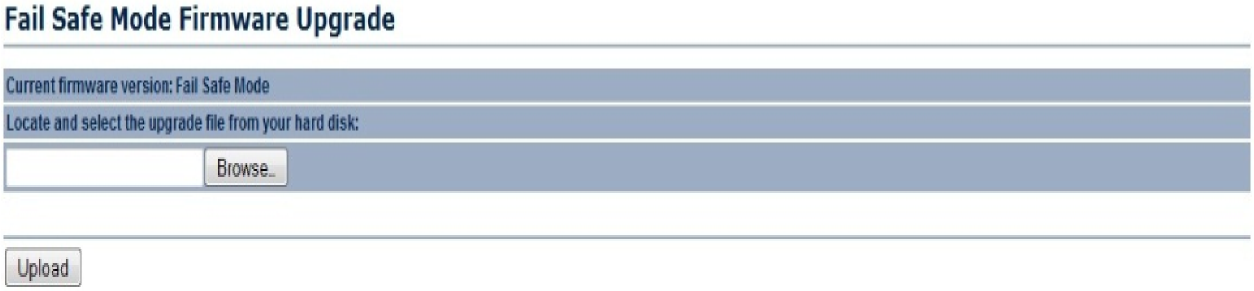
Target IP	
Ping Packet Size	64 Bytes
Number of Pings	4

Traceroute Test Parameters

Traceroute target	

11. Failsafe Mode

Any interruption is happening while firmware upgrade, device will go to failsafe mode. In this mode radio will be reachable with default ip – 192.168.1.1/24. Only web access can be done in this stage and firmware can upload through web. Click on Browse and select the firmware from the storage location and click on upload button.



Fail Safe Mode Firmware Upgrade

Current firmware version: Fail Safe Mode

Locate and select the upgrade file from your hard disk:

12. LED Indication

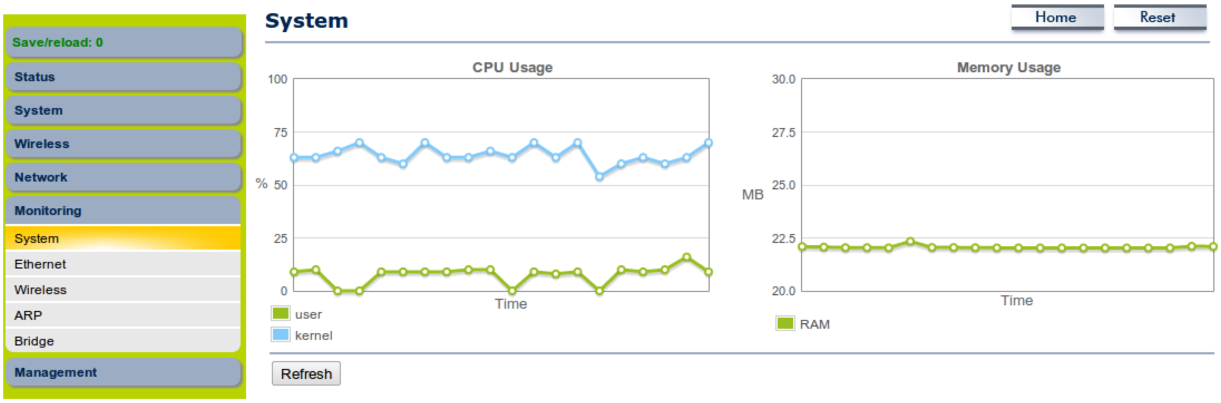
LED indication in Outdoor Subscriber (SU) mode and LED blinking format is given below.

NAME	Condition	Signal Strength
WLAN_LED	GREEN blinking fast	Excellent (less than -63)
	GREEN blinking slow	Good (-64 to -74 dBm)
	Alternate GREEN and AMBER	Average (-75 to -80 dBm)
	AMBER blinking	Poor (above -81 dBm)
	OFF	Wireless Link DOWN

12. Monitoring

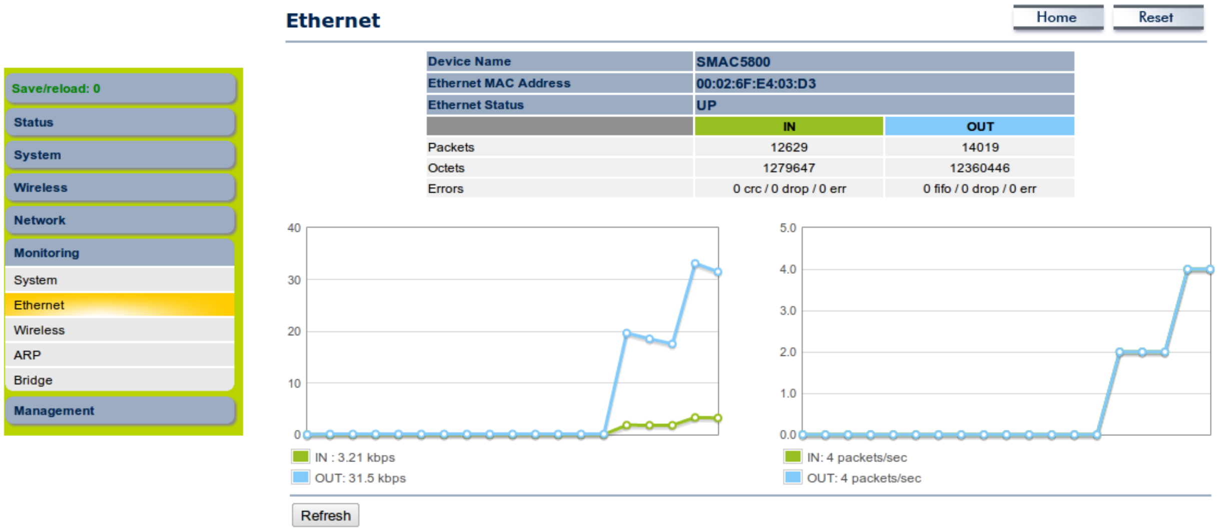
12.1 System

Click on the **System** link under the **Monitoring** menu for monitoring the CPU and Memory usage of AP/SU in the System tab. The graph representation will help to find out the current usage of CPU and Memory in percentage.



12.2 Ethernet

Click on the **Ethernet** link under the **Monitoring** menu for monitoring the Drop/error counts increasing in the IN and OUT tab of Ethernet side. Based on the counters we can able to conclude any ethernet side issue on the AP/SU side. We can able to check the Ethernet status (UP/Down) in the ethernet tab. Graphical representation of current utilization and PPS of IN and OUT can be monitored in the Ethernet interface.



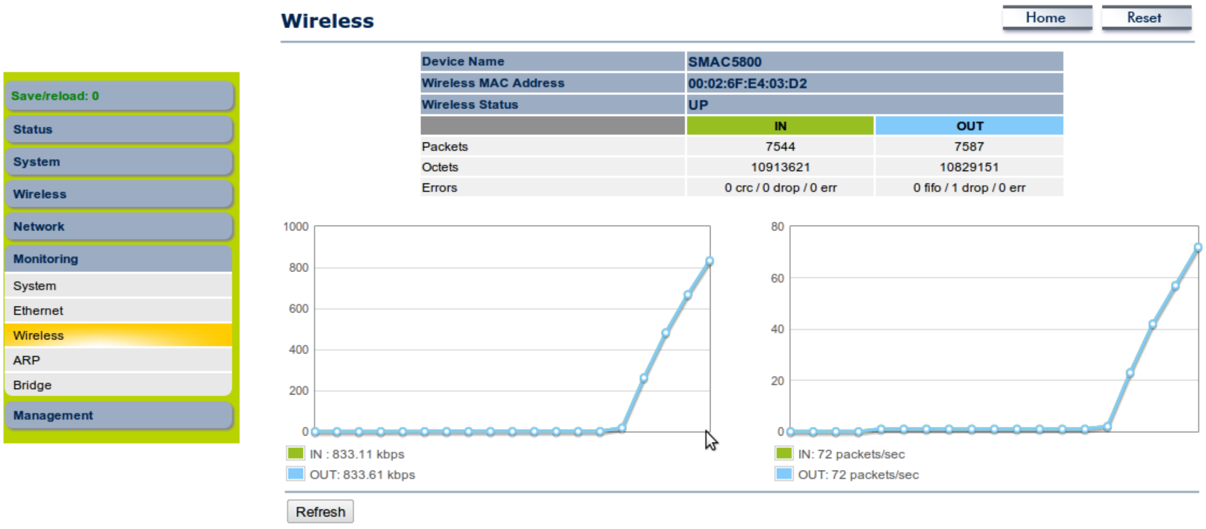
Device Name	SMAC5800	
Ethernet MAC Address	00:02:6F:E4:03:D3	
Ethernet Status	UP	
	IN	OUT
Packets	12629	14019
Octets	1279647	12360446
Errors	0 crc / 0 drop / 0 err	0 fifo / 0 drop / 0 err

🟩 IN : 3.21 kbps
🟦 OUT: 31.5 kbps

🟩 IN: 4 packets/sec
🟦 OUT: 4 packets/sec

12.3 Wireless

Click on the **Wireless** link under the **Monitoring** menu for monitoring the Drop/error counts increasing in the IN and OUT tab of wireless side. Based on the counters we can able to conclude any wireless side issue on the AP/SU side. We can able to check the wireless status (UP/Down) in the wireless tab. Graphical representation of current utilization and PPS of IN and OUT can be monitored in the wireless interface.



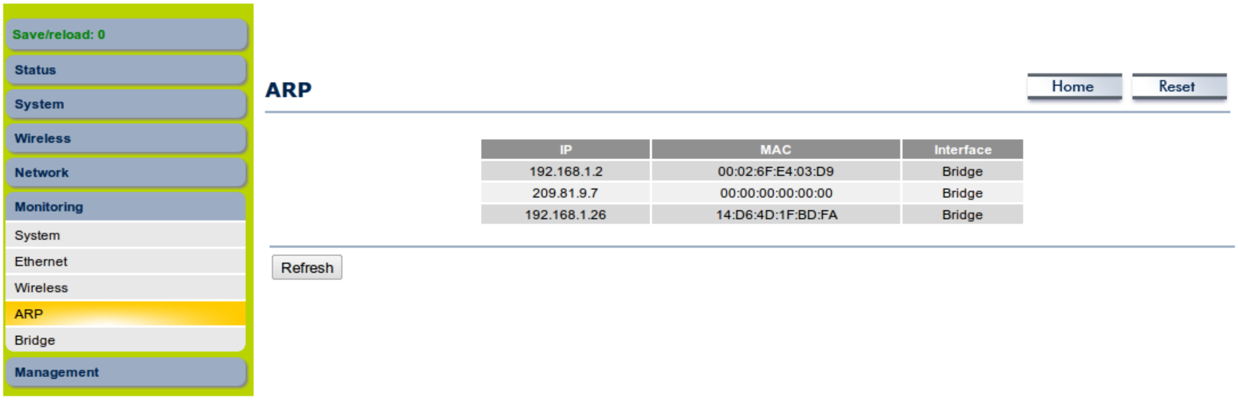
Device Name	SMAC5800	
Wireless MAC Address	00:02:6F:E4:03:D2	
Wireless Status	UP	
	IN	OUT
Packets	7544	7587
Octets	10913621	10829151
Errors	0 crc / 0 drop / 0 err	0 fifo / 1 drop / 0 err

🟩 IN : 833.11 kbps
🟦 OUT: 833.61 kbps

🟩 IN: 72 packets/sec
🟦 OUT: 72 packets/sec

12.4 ARP Table

Click on the **ARP** link under the **Monitoring** menu for ARP entries learned in AP/SU.

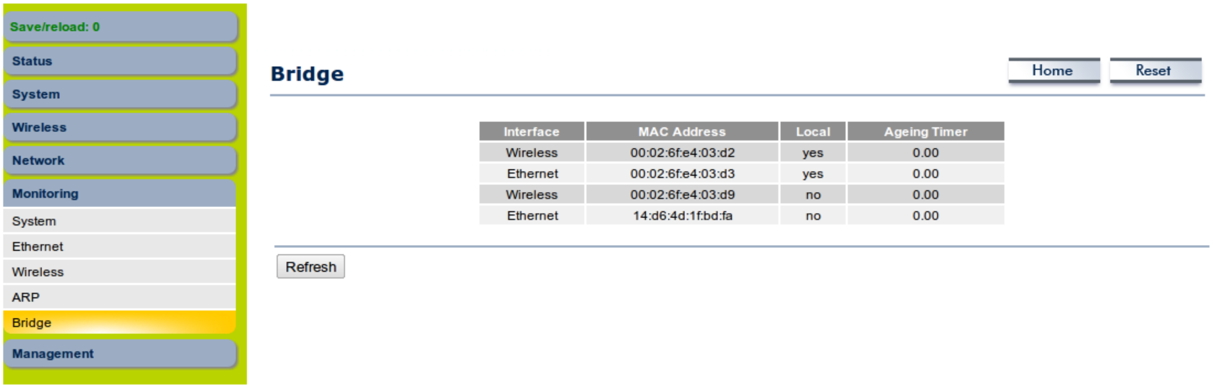


ARP

IP	MAC	Interface
192.168.1.2	00:02:6F:E4:03:D9	Bridge
209.81.9.7	00:00:00:00:00:00	Bridge
192.168.1.26	14:D6:4D:1F:BD:FA	Bridge

12.5 Learn Table

Click on the **Learn** link under the **Monitoring** menu for learn entries in AP/SU.



Bridge

Interface	MAC Address	Local	Ageing Timer
Wireless	00:02:6f:e4:03:d2	yes	0.00
Ethernet	00:02:6f:e4:03:d3	yes	0.00
Wireless	00:02:6f:e4:03:d9	no	0.00
Ethernet	14:d6:4d:1f:bd:fa	no	0.00