

3G/4G LTE Super Modem III

User's Manual

Version: 1.2

Date: September 03, 2013

Revision History

Version	Date	Changes
1.0	06/21/2013	First Release of Super Modem III User's Manual
1.1	07/22/2013	Revise the Specification of Super Modem III's Adaptor
1.2	09/03/2013	Add the Description of Bridge Mode and New Functions upon firmware ver. 10019

Table of Contents

Revision History	2
TABLE OF CONTENTS.....	3
CHAPTER 1. PRODUCT OVERVIEW	5
1.1 INTRODUCTION	5
1.2 FEATURES	6
1.3 PACKAGE CONTENTS	6
CHAPTER 2. PHYSICAL DESCRIPTION	7
2.1 PANELS	7
2.1.1 Front Panel.....	7
2.1.2 Rear Panel.....	8
2.2 ILLUSTRATION	9
2.2.1 Front Panel Information.....	9
USB Connector	9
LAN Port	9
Reset Button	9
Power Supply Connector.....	10
LEDs.....	10
2.2.2 Rear Panel Information.....	10
3G ANT SMA Connector	10
SIM Card Slot.....	10
Switch.....	10
2.2.3 LED Description on Super Modem III	11
CHAPTER 3. WEB-BASED MANAGEMENT.....	12
3.1. INTERNET SETTINGS	14
3.1.1 WAN	14
3.1.1.1 3G Settings	14
3.1.2 LAN.....	15
3.1.3 DHCP Clients.....	17
3.1.4 VPN	18
3.1.4.1 L2TP VPN.....	18
3.1.4.2 PPTP VPN	20
3.1.5 Advanced Routing Settings.....	21
3.2 WIRELESS SETTINGS	23
3.2.1 Basic Wireless Settings.....	23
3.2.2 Wireless Security/Encryption Settings.....	28

- 3.2.2.1 Disable Mode 28
- 3.2.2.2 WEPAUTO(WEP) Mode..... 29
- 3.2.2.3 WPA-PSK / WPA2-PSK Mode 31
- 3.2.3 AP Client Settings 33
- 3.2.4 Station List 34
- 3.2.5 Wireless Statistics 35
- 3.3 FIREWALL SETTINGS 36
 - 3.3.1 MAC/IP/Port Filtering Settings 36
 - 3.3.2 Port Forwarding Settings 38
 - 3.3.2.1 Create a Port Forwarding 38
 - 3.3.3 DMZ Settings..... 41
 - 3.3.4 System Security Settings 42
- 3.4 MANAGEMENT 44
 - 3.4.1 System Management..... 44
 - 3.4.2 SIM Card Control 47
 - 3.4.3 Firmware Upgrade 50
 - 3.4.4 Configuration Management..... 51
 - 3.4.5 Status..... 52
 - 3.4.6 Statistics..... 53

1. Product Overview

1.1 Introduction

3G/4G LTE Super Modem III, a HSUPA/ HSDPA/ EDGE/ CDMA 1X/ EVDO/ EVDO Rev A 2G/3G modem, is built in an Ethernet port and WIFI module. Not only could it be used to connect to Internet devices such as vending machines or our IP cameras to get on the Internet through the modem dialup but also a WIFI access point.



1.2 Features

- Use 3G modem dialup as the WAN connection, RJ45 interface as the LAN connection.
- Multimode operation – HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM.
- Triple-band HSPA/UMTS 850/1900/2100 MHz.
- Quad-band EDGE/GPRS/GSM 850/900/1800/1900 MHz.
- HSUPA uplink up to 2.0 Mbps.
- HSDPA downlink up to 7.2 Mbps.
- WCDMA (UMTS) uplink data rate up to 384 kbps.
- EDGE data up to 237 Kbps DL and 118Kbps UL, 3GPP Release4, class 12.
- GPRS data up to 85.6 Kbps DL and 42.8 Kbps UL.
- Supports the remote reboot of the device through web-based user interface.
- Offer a slide switch to change the Router/Bridge operation mode.
- Offer the built-in module for WIFI Access Point.

1.3 Package Contents

- 1 x 3G/4G LTE Super Modem III
- 1 x RJ45 Ethernet Cable
- 1 x 3G Antenna
- External 3G Antenna with 3M Antenna Cable (*Optional*)
- 1 x Power Adapter
- 1 x CD with this User's Manual
- Quick Setup Guide

2. Physical Description

The following information contains the physical description of Super Modem III. This includes the functions and the locations of each connector and indicator. This information provides useful reference when installing the product. Please familiarize yourself with this device.

2.1 Panels

2.1.1 Front Panel

For more related description, please refer to the Section 2.2 and Section 2.2.1.

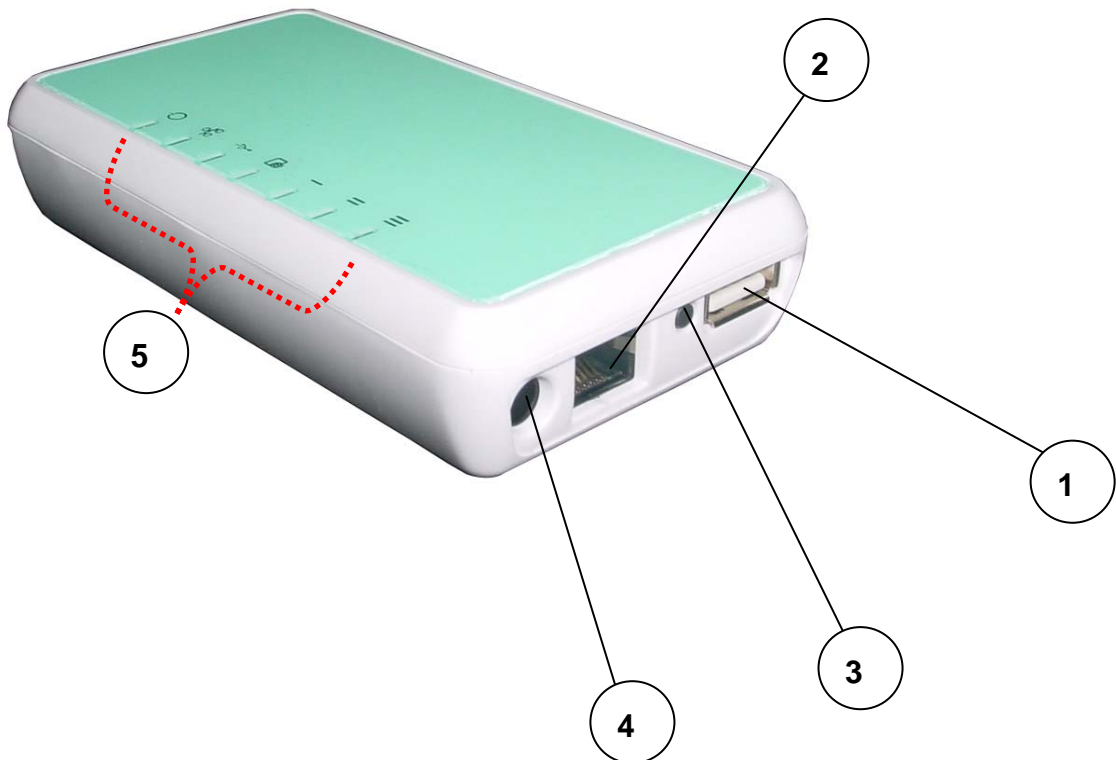


Fig. 1 Front View of 3G/4G LTE Super Modem III

2.1.2 Rear Panel

For more detailed description, please refer to the Section 2.2 and Section 2.2.2.



Fig. 2 Rear View of 3G/4G LTE Super Modem III

2.2 Illustration

No. in Figures	Name on Super Modem III	Description	Remark
1	USB Connector	Function reserved	Refer to section 2.2.1 for the front panel information
2	LAN Port	To connect to the device and Ethernet port via RJ45 cable	Refer to section 2.2.1 for the front panel information
3	Reset Button	To reset the Super Modem III to its factory defaults	Refer to section 2.2.1 for the front panel information
4	Power Supply Connector	To connect with the Super Modem III and the power adapter	Refer to section 2.2.1 for the front panel information
5	LEDs	To display the status of Super Modem III	Refer to section 2.2.3 for the LED description on the front panel
6	3G ANT SMA Connector	To connect with the 3G antenna	Refer to section 2.2.2 for Real panel information
7	SIM Card Slot	To connect with the internal modem for the access of Internet	Refer to section 2.2.2 for Real panel information
8	Switch	To change the operation environment between the "Router" and "Bridge" modes	Refer to section 2.2.2 for Real panel information

2.2.1 Front Panel Information

USB Connector

Function reserved.

LAN Port

Super Modem III is designed for 10/100Mbps Ethernet networks. Super Modem III connects to the network via category 5 cable.

Reset Button

Support the hardware reset function. Press 5 seconds around will reboot and reset the device to factory defaults. For the software reset of the device, you may refer to Section 3.4.4 for "Configuration Management".

Power Supply Connector

Plug the power adapter. The specifications of Super Modem III's power adapter are as follows:

- Input: 100 ~ 240V AC, 50/60Hz
- Output: 8V DC / 1A

LEDs

Include the LEDs of POWER, LAN Link/Activity, WLAN(Wireless LAN), 3G Dialup Status and Cellular Signal Strength.

2.2.2 Rear Panel Information

3G ANT SMA Connector

Support modem for wireless access.

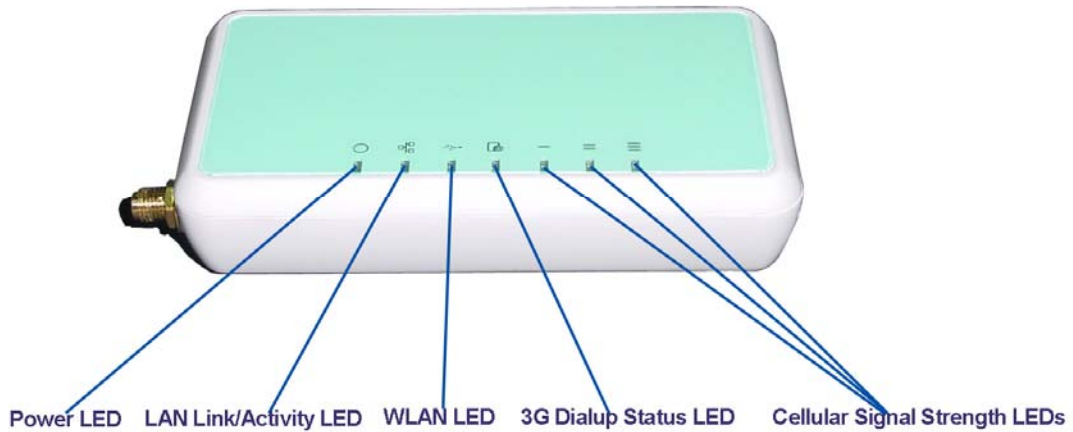
SIM Card Slot








Plug the SIM card chip.

Switch

- **Router Mode:** Switching the button into the “**3G**” position will have Super Modem III enter this operation mode, and PC will get the virtual IP address assigned by Super Modem III. For more details on the network connection of this mode, you may refer to the Quick Setup Guide coming with the package.
- **Bridge Mode:** Switching the button into the “**Bridge**” position will have Super Modem III enter this operation mode. Especially, it is designed for some kind of the routers that are not equipped with any USB connector to connect with wireless modem. In this mode, PC will get the virtual IP address assigned by Super Modem III as well as a new IP address from the PPPoE connection respectively. For more details on the network connection of this mode, you may refer to the Quick Setup Guide coming with the package.

2.2.3 LED Description on Super Modem III



LED	Color	Status
POWER ()	Green	Lit when 8V DC power is on and working.
LAN Link/Activity ()	Green	Lit when the cable connection with device exists. Flash when the data is transmitting. Off when no cable connection exists.
WLAN(Wireless LAN) ()	Green	Lit when the WiFi function is enabled. Flash when the data is transmitting. Off when the WiFi function is disabled.
3G Dialup Status ()	Green	Lit when the data is transmitting in 2G networks. Flash when the data is transmitting in 3G networks. Off when dialup is disconnected.
3 Cellular Signal Strength LEDs		
Low ()	Green	All 3 LEDs lit when the signal strength is good. (The LEDs lit would decrease progressively upon the signal strength)
Medium ()		
High ()		

3. Web-Based Management

This chapter instructs you how to configure and manage the Super Modem III through the web user interface it supports. With this facility, you can easily access and monitor through the LAN port of the Super Modem III.

After the Super Modem III has been connected to your PC via RJ45 network cable, type <http://192.168.0.254> in IE browser, it will show the following screen and ask you to input the user name and password in order to login and access authentication. The default user name and the password are both “**admin**”. For the first time to use, please enter this default user name and the password, then click the **OK** button. The root setup page for Super Modem III will be displayed once the login process is successful. The user will be able to fully access and configure the system.



In the router, it supports a simple user management function to configure the system. As the figure below shows, for example, left section is the whole function tree with web user interface while each of main functions, including INTERNET SETTINGS, WIRELESS SETTINGS, FIREWALL(only exists in the "Router" operation mode), and MANAGEMENT is selected.

In this root setup page, user can select his favorite language by pulling down the list. The languages we offer include English and Portuguese. The setting will be taken effect after clicking on the **Apply** button. By means of the hyperlink of Status, Statistic or Management, you can directly jump to the related pages if you would like to realize the basic information of the system.



3.1. Internet Settings

3.1.1 WAN

The WAN (Wide Area Network) section is where you configure your Internet connection type. The Super Modem III supports 3G dialup connection type to access Internet. Please contact your Internet Service Provider before configuring the required parameters.

Wide Area Network (WAN) Settings

3G Mode	
APN	<input type="text" value="internet"/>
Dial Number	<input type="text" value="*99#"/>
Username	<input type="text" value="user"/>
Pasword	<input type="text" value="passwd"/>
Auth Mode	PAP <input type="button" value="v"/>
Connection Type	3G + 2G(3G Preferred) <input type="button" value="v"/>

3.1.1.1 3G Settings

This section is where you configure your dialup up connection type. There are 2 modem types to choose from: Cellular 2G and 3G.

2G/3G ISP Settings: Your 2G/3G service provider will provide you with the values to fill in for the required fields of **Access Point Name (APN Gateway)**, **PPP User Name**, **PPP Password** and **Dial Number**.

Dial Number: The 2G/3G dial command. Default is *99#.

Authentication Mode: The mode for PPP authentication.

Connection Type: There are four types of operation mode supported: 3G only, 3G+2G(3G Preferred), 2G only, and 2G+3G(2G Preferred). Default is 3G + 2G (3G Preferred).

3.1.2 LAN

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	<input type="text" value="10.10.10.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	00:0A:EB:38:B8:85
DHCP Type	Server <input type="button" value="v"/>
Start IP Address	<input type="text" value="10.10.10.100"/>
End IP Address	<input type="text" value="10.10.10.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="168.95.1.1"/>
Secondary DNS Server	<input type="text" value="8.8.8.8"/>
Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

IP Address: The IP address of your router's LAN port. Default: 192.168.0.254.

Subnet Mask: Subnet Mask of your LAN (default: 255.255.255.0). All devices on the network must have the same subnet mask to communicate on the network.

DHCP Type: DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN). When you select **Server** item from this pull-down list to enable this function, the following parameters will be displayed. You must enter the IP address, Subnet Mask, Primary DNS Server and/or Secondary DNS Server.

Start IP Address: Specify the DHCP Client IP address that will start.

End IP Address: Specify the DHCP Client IP address that will end.

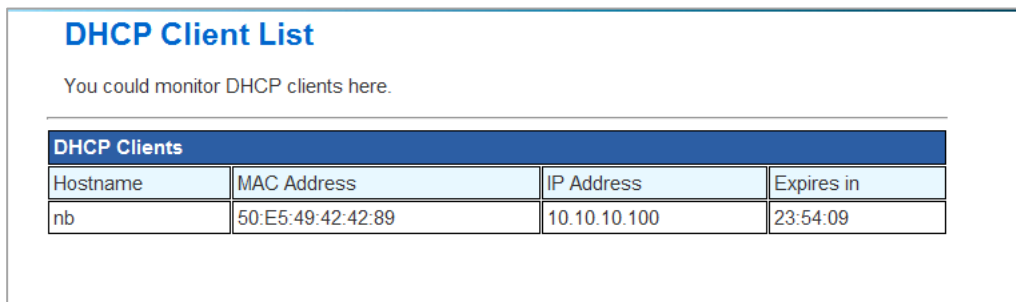
Note: The number of the "End IP" must be greater than "Start IP", and cannot be the same as the router's IP address.

DHCP Lease Time: Designate the amount of the time for the device to recycle and give out the IP addresses to the devices in your network (default: 86400).

Statically Assigned: You can statically assign the client MAC and IP address. Up to three IPs and MACs can be assigned.

3.1.3 DHCP Clients

In this section, you can see clearly which devices are currently leasing IP addresses that you had defined for the DHCP Server's allocation of addresses to computers and devices on your Local Area Network.



DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
nb	50:E5:49:42:42:89	10.10.10.100	23:54:09

Host Name: A name for each computer or device that is given an IP address by the DHCP Server. This may help you keep track of which computers are assigned this way.

MAC Address: A MAC address is usually located on a sticker at the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33.

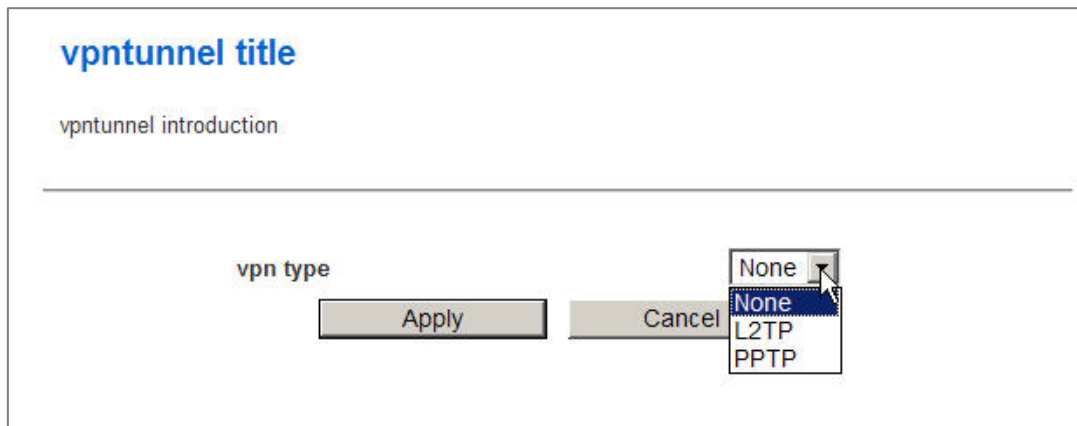
IP Address: The address which is obtained from the DHCP Server.

Expires in: The remaining time of the IP address's lease. A specific LAN device no longer needs the leased IP address when the time ends up, and this device will also free the IP address it had leased.

3.1.4 VPN

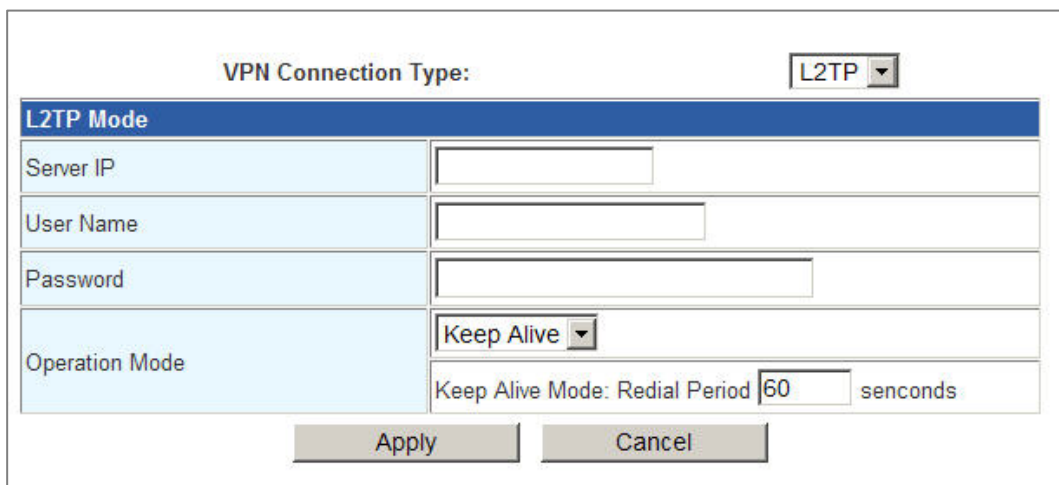
The Super Modem III supports L2TP and PPTP VPN (Virtual Private Network) communication protocols. VPN is a technology commonly used in different private networks between companies or groups. It allows the intranet message to be transmitted using the public network such as Internet. Through VPNs, the user is able to access resources on remote networks, for example, files, printers, databases, internal websites and so on.

To select the desired VPN, just pull down the list of **VPN Type** and then click on the **Apply** button. You may refer to the following description of parameters to set up your VPN.



3.1.4.1 L2TP VPN

L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a **User Name** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.



Server IP: The IP address of the L2TP server. The ISP will provide the value of this parameter.

Operation Mode: Typically, L2TP connections are not always on. The router allows you to set the reconnection mode. The setting is:

- **Keep Alive:** A connection to the Internet is always maintained. When this option is selected, please enter a value in the field of **Redial Period** which is the time interval the machine will be redialed before the L2TP connection is disconnected.

3.1.4.2 PPTP VPN

PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a **User Name** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

VPN Connection Type: PPTP	
PPTP Mode	
Server IP	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password"/>
Operation Mode	Keep Alive
Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds	
Apply Cancel	

Server IP: The IP address of the PPTP server. The ISP will provide the value of this parameter.

Operation Mode: Typically, PPTP connections are not always on. The router allows you to set the reconnection mode. The setting is:

- **Keep Alive:** A connection to the Internet is always maintained. When this option is selected, please enter a value in the field of **Redial Period** which is the time interval the machine will be redialed before the PPTP connection is disconnected.

3.1.5 Advanced Routing Settings

In Static Routing Settings, the user can set up a route rule (table) here. Refer to the description of the following parameters to set up the necessary route rule, and click the **Apply** button when you complete.

Static Routing Settings

You may add and remote custom Internet routing rules.

Add a routing rule

Destination	<input type="text"/>
Range	Host <input type="button" value="v"/>
Gateway	<input type="text"/>
Interface	LAN <input type="button" value="v"/>
Comment	<input type="text"/>

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	192.168.122.122	255.255.255.255	0.0.0.0	5	0	0	0	WAN (ppp0)	
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	
4	0.0.0.0	0.0.0.0	192.168.122.122	3	0	0	0	WAN (ppp0)	

Destination: The IP address of packets that will take this route.

Range: Includes **Host** and **Net** options. When selecting “Net”, there is another “Netmask” column that needs to be filled out.

Netmask: The bits in the mask specify which bits of the IP address must match.

Gateway: The gateway for the routing.

Interface: Specifies the interface -- **LAN** or **WAN** -- that the IP packet must use to transit out of the router when this route is used. Or you can choose the user-defined way by selecting the **Custom** option.

Comment: Memo for the routing rule.

Routing Table: Lists the current route rules you have added before. Click on the **Delete** button to delete the selected route rule.

3.2 Wireless Settings

The wireless section is used to configure the wireless settings for your router. Please note that changes made on this section may also need to be duplicated on your wireless client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP(WEPAUTO), WPA-PSK, and WPA2-PSK. WEP is the original wireless encryption standard. WPA provides a higher level of security. In WPA encryption, it supports TKIP or AES of WPA-PSK/WPA2-PSK.

3.2.1 Basic Wireless Settings

Through the basic wireless setting page, the user can control the ON/OFF status of WiFi function, and set up the 802.11 mode, Network Name (SSID) as well as Channel. Besides, you can do the further settings related to the HT Physical Mode.

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
WiFi On/Off	WiFi OFF
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	3Jtech WiFi Hidden <input type="checkbox"/>
Multiple SSID1	<input type="text"/> Hidden <input type="checkbox"/>
Multiple SSID2	<input type="text"/> Hidden <input type="checkbox"/>
Multiple SSID3	<input type="text"/> Hidden <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Frequency (Channel)	2437MHz (Channel 6) ▾

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Wireless Network Settings:

WiFi On/Off: This option turns on and off the wireless connection feature of the router. Simply click on the **WiFi ON / WiFi OFF** button. The system will automatically detect the current status of the router and switch the button accordingly.

Network Mode: There are 5 modes including, 802.11b/g mixed mode, 802.11b only, 802.11g only, 802.11/b/g/n mixed mode, and 802.11n only(2.4G) can be chosen.

Network Name(SSID): When you are browsing for available wireless networks, this is the name that will appear in the list (unless you set it to Hidden, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Default is 3Jtech WiFi.

Hidden: The option allows you to hide your wireless network. When this option is unchecked, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When you click on this checkbox to enable this function, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Multiple SSID 1 ~ 3: Up to three SSIDs you can additionally set up for this wireless network.

Broadcast Network Name (SSID): Enable/Disable the SSID broadcast function. This function is used to control the broadcast status of all SSIDs. If this function is disabled, all SSIDs you had set up for the router will be hidden. To cancel the hidden status for the specific SSID, you can uncheck the "Hidden" option in the back of your desired SSID.

AP Isolation: Enable/Disable this function. Create a separate virtual network for your wireless network. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.

MBSSID AP Isolation: Enable/Disable the MBSSID AP Isolation function. The router supports multiple SSIDs. You can decide whether the clients associated to different SSIDs on the device can see each other or not. Enable the option to block it. Default is "Disable".

Frequency (Channel): A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. If you select **AutoSelect**, the router automatically finds the channel with least interference and uses that channel for wireless networking.

Rate: Exist only when selecting 802.11b/g mixed mode, 802.11b only, 802.11g only as the Network Mode for the router. You can set up the desired transmitting rate for these network modes. Default is Auto.

HT Physical Mode Settings: This mode settings exist only when 802.11b/g/n mixed mode or 802.11n only(2.4G) is chosen as your router's Network Mode.

Operating Mode: Select the option to enable the Mixed Mode or the Green Field Mode for physical layer transceivers. Default: Mixed Mode.

Mixed mode: In this mode the device transmits the packets with preamble compatible legacy (802.11g), so they can be decoded by legacy devices. The device receives and decodes both Mixed Mode packets and legacy packets.

Green Field mode: The device transmits HT packets without legacy compatible part. But the device receives and decodes both Green Field and legacy packets.

Channel BandWidth: This option only works when selecting Network mode in 11b/g/n mixed mode and 11n mode. Select the option to choose 20 MHz or 20/40MHz. This option affects the Phy data rate of radio. Please refer to the table below, which shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Guard Interval: The 11n device inserts the Guard Interval into the signal. You can choose the interval between "Long" and "Auto". This option affects the Phy data rate of radio. For more details, please refer to the table below.

MCS: It means "Modulation Coding Scheme". The available options are "Auto, 0, 1, ...15, and 32". It changes the modulation of this device and effect the maximum Phy data rate. We recommend "Auto" setting. For more details, please refer to the table below.

The table below shows the relationship among Phy data rate, Bandwidth and Guard Interval.

Data Rate Mbps MCS	Bandwidth = 20MHz		Bandwidth = 40MHz	
	Short Guard Interval	Long Guard Interval	Short Guard Interval	Long Guard Interval
0 (1S)	7.2	6.5	15	13.5
1	14.4	13	30	27
2	21.7	19.5	45	40.5
3	28.9	26	60	54
4	43.3	39	90	81
5	57.8	52	120	108
6	65	58.5	135	121.5
7	72.2	65	150	135
8 (2S)	14.4	13	30	27
9	28.9	26	60	54
10	43.3	39	90	81
11	57.8	52	120	108
12	86.7	78	180	162
13	115.6	104	240	216
14	130	117	270	243
15	144.4	130	300	270
32	Not Supported	Not Supported	6.7	6

MCS: Modulation Coding Scheme
MCS=0~7 (1S, One Tx Stream)
MCS=8~15 (2S, Two Tx Stream)
MCS 32: BPSK

Reverse Direction Grant(RDG): This is the 11n performance parameter. Enable it if needed.

Extension Channel: Exist only when selecting "20/40" as the Channel BandWidth for the router. For example, if channel 6 is selected, it means you can select channel 2 or channel 10 as the extension channel. Choose the unused channel as the extension channel.

Aggregation MSDU(A-MSDU): The multiple HT packets can be transmitted with single ACK reply packet. Enable it to apply this function and reduce the network congestion.

Auto Block ACK: It is another aggregation technique which prevents sending ACK in the communication to increase the throughput. If this option is enabled, the device will activate this function when transmitting massive data.

Decline BA Request: Enable this option to decline the Block ACK request addressed by the other devices.

3.2.2 Wireless Security/Encryption Settings

In this section, you can configure the wireless security and encryption to prevent from unauthorized access and monitoring. Please choose a SSID you had created for this router in the *Wireless Settings* → *Basic* setting page from the **SSID Choice** pull-down list.

There are 4 encryption modes, including **Disable**, **WEPAUTO(WEP)**, **WPA-PSK** and **WPA2-PSK** offered for your selection. Please also pull down the **Security Mode** list and select the desired mode for your router's wireless security. For more details about the setup in these different modes, please refer to the following sections.

3.2.2.1 Disable Mode

In this mode, wireless clients can directly connect to the router without inputting any key.

The screenshot displays the 'Wireless Security/Encryption Settings' configuration page. At the top, the title 'Wireless Security/Encryption Settings' is shown in blue. Below the title is a subtitle: 'Setup the wireless security and encryption to prevent from unauthorized access and monitoring.' The main configuration area contains two sections. The first section, titled 'Select SSID', has a dropdown menu labeled 'SSID choice' with '3Jtech WiFi' selected. The second section, titled '"3Jtech WiFi"', has a dropdown menu labeled 'Security Mode' with 'Disable' selected. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

3.2.2.2 WPAUTO(WEP) Mode

WEP is a method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F(a-f)) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

Example,

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF12340012225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)



WEP Keys: Select "ASCII" or "Hex" from the pull-down list to set up the key value. ASCII (American Standard Code for Information Interchange) is a code for representing char as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F (a-f).

3.2.2.3 WPA-PSK / WPA2-PSK Mode

WPA (Wi-Fi Protected Access) is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard.

PSK(Pre-Shared Key) is the key which is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or 64 digits in HEX format at both ends of the wireless connection. When inputting ASCII strings, it cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Wireless Security/Encryption Settings	
Setup the wireless security and encryption to prevent from unauthorized access and monitoring.	
<hr/>	
Select SSID	
SSID choice	3Jtech WiFi
<hr/>	
"3Jtech WiFi"	
Security Mode	WPA-PSK
<hr/>	
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)
<hr/>	
Apply Cancel	

WPA Algorithms: Mark the option to enable modes of TKIP or AES.

Pass Phrase: This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ASCII characters or 64 digits in HEX format.

Key Renewal Interval: Enter a value to set up the WPA key renewal interval. The device regenerates the key in every interval seconds that you have setup without disconnection. The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds, and you can adjust the time interval (Valid Range: 0 ~ 4194303).

3.2.3 AP Client Settings

With the AP Client function, the Super Modem III could connect to other remote WiFi AP(AP1) as a WiFi station, and it will be bridged with Super Modem III WiFi AP and LAN, which means that PC WiFi clients under AP1 and PCs clients under Super Modem III LAN and WiFi could communicate with each other.

Just fill in the network name (SSID) and the pass phrase (security key) of the WiFi AP that Super Modem III would like to connect. Please note that the setup of **Network Mode** as well as **Frequency Channel No.** for the Super Modem III in the *Wireless Settings* → *Basic* setting page must match the values used on this WiFi AP.

AP Client Feature

You could configure AP Client parameters here.

AP Client Parameters	
SSID	<input type="text" value="SM3G3AP"/>
MAC Address (Optional)	<input type="text"/>
Security Mode	<input type="text" value="WPA2PSK"/>
Encryption Type	<input type="text" value="AES"/>
Pass Phrase	<input type="text" value="12345678"/>
Auto Select WIFI channel for FlashAir	<input type="text" value="Disable"/>

3.2.4 Station List

From the list of Station, you can see which devices are currently connecting to your Super Modem III in the wireless way through the MAC address. You also can have a clear realization of status, including Aid, PSM, MimoPS, MCS, BW(Bandwidth), SGI and STBC for each Wifi connection.

Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
74:2F:68:90:35:F4	1	0	0	7	20M	0	0

3.2.5 Wireless Statistics

The Super Modem III offers the counter function to collect all wireless traffic counting information about the transmitting / receiving packets of this router. The system will automatically update these wireless data per 3 seconds. To restart the counting, please click on the **Reset Counters** button.

The screenshot shows a web interface titled "AP Wireless Statistics" with the subtitle "Wireless TX and RX statistics". It contains a table with transmit and receive statistics, and a "Reset Counters" button at the bottom.

Transmit Statistics	
Tx Success	54
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	313760
Frames Received With CRC Error	243, PER=0.1%
SNR	
SNR	n/a, n/a, n/a

Tx Success: Display the transmitted number of the successful packets.

Tx Retry Count: Display the transmitted number of the retry packets.

Tx Fail after retry: Display the transmitted number of the unsuccessful packets after retry.

RTS Successfully Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets successfully.

RTS Fail To Receive CTS: Display the transmitted number of RTS(Request To Send) packets which receive CTS(Clear To Send) packets unsuccessfully.

Frames Received Successfully: Display the received number of the successful frames.

Frames Received With CRC Error: Display the received number of frames with CRC error packets.

SNR: Signal-to-Noise ratio (SNR). It stands that how fast wireless data of the router can travel and how far a wireless signal of the router can reach.

3.3 FireWall Settings

Please skip this section if you are using the “Bridge” operation mode.

3.3.1 MAC/IP/Port Filtering Settings

The router could filter the outgoing packets for security or management consideration. You can set up the filter against the IP addresses to block specific internal users from accessing the Internet. The firewall could not only obstruct outside intruders from intruding your system, but also restricting the LAN users. Port filter restricts certain type of data packets from your LAN to Internet through the router.

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering	Disable ▾
Default Policy -- The packet that don't match with any rules would be:	Dropped ▾

MAC/IP/Port Filter Settings

Source MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	None ▾
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Accept ▾
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

Basic Settings:

MAC/IP/Port Filtering: Enable/Disable the function of MAC/IP/Port Filtering.

Default Policy - The packet that don't match with any rules would be: Dropped/Accepted. For example, if you select "Dropped", all packets that do not match the rule you set up in the following **MAC/IP/Port FilteringSettings** would be dropped.

MAC/IP/Port Filtering Settings:

Source MAC address: Fill out the MAC address that you wish to filter.

Dest IP Address: Fill in the destination IP address that you wish to filter.

Source IP Address: Fill in the source IP address that you wish to filter.

Protocol: Select the protocol type of TCP, UDP or ICMP.

Dest Port Range: Fill in the destination port range that you wish to filter.

Source Port Range: Fill in the source port range that you wish to filter.

Action: You can either choose "Accept" or "Drop" to permit or prevent the action.

Comment: Input any text to describe this mapping, up to 16 alphanumerical characters.

MAC/IP/Port Filter Rule List: Lists the MAC/ IP / Port Filter Settings you have added before. Click on the **Delete Selected** button to delete the selected list.

3.3.2 Port Forwarding Settings

This function offers the way of Port Forwarding / Virtual Server in order to help redirect requests from computers on the LAN to a server set up on the LAN. You can set up an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.

3.3.2.1 Create a Port Forwarding

In this section, you can add a new port forwarding to the port forwarding table below or delete an existing entry from this table.

Port Forwarding				
Port Forwarding	Enable <input type="button" value="v"/>			
IP Address	<input type="text"/>			
Port Range	<input type="text"/> - <input type="text"/>			
Protocol	TCP&UDP <input type="button" value="v"/>			
Comment	<input type="text"/>			
(The maximum rule count is 32.)				
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				
Current Port Forwarding in system:				
No.	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	192.168.0.100	100 - 111	TCP + UDP	
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

Port Forwarding: Enable/Disable the function of Port Forwarding.

IP Address: Fill in the IP address of your LAN Server.

Port Range: Fill in the port range that you wish to filter.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

Comment: Input any text to describe this mapping. Up to 16 alphanumeric characters can be filled in.

Port Forwarding Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Port Forwarding you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.2.2 Create a Virtual Server

In this section, you can add a new virtual server to the virtual server table below or delete an existing entry from this table.

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port. For Example,

You are hosting a Web Server on a PC that has LAN IP Address of 192.168.0.50 and your ISP is blocking Port 80.

1. Enter the IP Address of the machine on your LAN (for example: **192.168.0.50**)
2. Enter the Public Port as [8888]
3. Enter the Private Port as [80]
4. Select the Protocol - TCP
5. Click the **Apply** button to add the settings to the Virtual Server Table
6. Repeat these steps for each Virtual Server Rule you wish to add. With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.0.50.

Virtual Server					
Virtual Server	Enable ▾				
IP Address	<input type="text"/>				
Public Port	<input type="text"/>				
Private Port	<input type="text"/>				
Protocol	TCP&UDP ▾				
Comment	<input type="text"/>				
<small>(The maximum rule count is 32.)</small>					
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					
Current Virtual Servers in system:					
No.	IP Address	Public Port	Private Port	Protocol	Comment
1 <input type="checkbox"/>	192.168.0.50	8888	80	TCP	Web
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>					

Virtual Server: Enable/Disable the function of Virtual Server.

IP Address: The IP address of the system on your internal network that will provide the virtual service, for example, **192.168.0.50**.

Public Port: The port that will be accessed from the Internet.

Private Port: The port that will be used on your internal network.

Protocol: Select the protocol type, including TCP, UDP or TCP&UDP used by the service.

Comment: Input any text to describe this mapping. Up to 16 alphanumerical characters can be filled in.

Virtual Server Mapping List: After completing the above settings, please click on the **Apply** button. The entry of Virtual Server you had added will be listed on this table if it is created successfully. Clicking on the **Delete Selected** button will remove the existing entry you select from this table.

3.3.3 DMZ Settings

The DMZ (Demilitarized Zone) is used to enable protocols, which needs to open ports on the router. The router will forward all unspecified incoming traffic to the host specified in this setting page. To configure it, mark to enable virtual DMZ and then enter the Host IP (private IP address) and click the **Apply** button to enact the setting.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ Settings	
DMZ Settings	Enable
DMZ IP Address	<input type="text"/>

Except TCP port 80

DMZ Settings: Enable/Disable the function of DMZ.

DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation in the field of **Statically Assigned** on the *Internet Settings* → *LAN* setting page so that the IP address of the DMZ machine does not change.

Except TCP port 80: If you click on the checkbox in front of **Except TCP port 80** function, it means that TCP port 80 cannot be used for DMZ; otherwise, you can use this port for DMZ.

3.3.4 System Security Settings

To improve the safety of the internal network environment, the Super Modem III offers a variety of basic firewall management functions, including Remote management (via WAN), Ping from WAN Filter, Block port scan, Block SYN Flood and SPI Firewall. By the configuration the following system security settings, you can protect the router itself from being attacked, scanned or intruded.

The screenshot shows the 'System Security Settings' configuration page. At the top, there is a title 'System Security Settings' and a subtitle 'You may configure the system firewall to protect AP/Router itself from attacking.' Below this, there are five sections, each with a blue header and a light blue background:

- Remote management**: The 'Remote management (via WAN)' dropdown menu is set to 'Allow'.
- Ping from WAN Filter**: The 'Ping from WAN Filter' dropdown menu is set to 'Disable'.
- Block Port Scan**: The 'Block port scan' dropdown menu is set to 'Disable'.
- Block SYN Flood**: The 'Block SYN Flood' dropdown menu is set to 'Disable'.
- Stateful Packet Inspection (SPI)**: The 'SPI Firewall' dropdown menu is set to 'Disable'.

At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Remote management (via WAN): Allow or Not Allow the user to log in the system with the WAN IP.

Ping from WAN Filter: Enable/Disable the function of Ping from WAN Filter. If the function is enabled, the system will reject to response the ICMP(ping) packets coming from the WAN.

Block port scan: Enable/Disable the function of Block port scan. The port scan actions will be dropped if you enable this function.

Block SYN Flood: Block TCP SYN Flood or not. If this function is enabled, it can prevent the system from being attacked by a large amount of SYN packets.

SPI Firewall: SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.

3.4 Management

3.4.1 System Management

You may configure language, administrator's account and password, NTP and DDNS settings here.

Language Settings	
Select Language	English <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Administrator Settings	
Account	admin
Password	•••••
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
NTP Settings	
Current Time	Sat Jan 1 03:57:21 UTC 20 <input type="button" value="Sync with host"/>
Time Zone:	(GMT-11:00) Midway Island, Samoa <input type="button" value="v"/>
NTP Server	<input type="text"/> ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
DDNS Settings	
Dynamic DNS Provider	www.no-ip.com <input type="button" value="v"/>
Account	ydchao3jtech
Password	•••••
DDNS	ydchao3jtech.no-ip.org
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Language Settings: Select the language which you would like. It includes English and Portuguese.

Administrator Settings: Modify the account and password to set up and manage the Super Modem III. The default settings for administrator are as follows:

Username: admin

Password: admin

NTP Settings: Set up the system time by syncing from the NTP server or your PC.

Sync with Host: Click on the button of **Synchronize with host** to synchronize the timer built in the router with the computer you are using.

Current Time: Show the system time of the router. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Wed, Aug. 29, 12:10:10, 2012.

Time Zone: It is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the router will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The router supports configurable time zone from -11 to +12 step 1 hour. Default Time zone: -11 Hrs.

NTP Sever: NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If you manually specify an IP address of user-defined NTP server as well as Time Zone, the router will sync the time immediately after pressing the **Apply** button.

NTP Synchronization (hours): Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing. You can set up the time interval (Valid range: 1 ~ 300 hours) to have the assigned NTP server do the synchronization of time for your router.

DDNS (Dynamic DNS) Settings: The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have registered (www.dyndns.com or www.no-ip.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your domain name to connect to your server, no matter what your IP address is.

Dynamic DNS Provider: Select a dynamic DNS service provider from the pull-down list.

Account: Enter the username or key provided by your service provider.

Password: Enter the password or key provided by your service provider.

DDNS: Enter the hostname you have registered.

Note: After configuring Super Modem III for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example **http://www.mydomain.info**) and Super Modem III will attempt to forward the request to port 80 on your LAN.

3.4.2 SIM Card Control

On this SIM Card Control settings page, you can set up the password for SIM card's authentication. The Super Modem III will detect automatically the current limit times of PIN code and PUK input for your SIM card. If the remaining times of PIN code input are less than 3 times, the system will stop all related functions. You should configure the PIN code of the SIM card on this web setting page, and enter the correct PIN code again before the reboot of the device.

Note 1: The wrong input of PIN code and PUK in the following setup will decrease the allowable input times of PIN code and PUK.

Note 2: Any changes on this webpage, the user needs to reset to power to have all related functions work normally.

Information	
SIM Card Status	READY
Remaining attempts to enter PIN	3
Remaining attempts to enter PUK	10
<input type="checkbox"/> Automatic PIN CODE insertion on boot Type the PIN CODE for automatic insertion: <input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Enable PIN request for inicialization	
Enable	No <input type="button" value="v"/>
PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Enter PIN	
PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Change PIN	
Old PIN	<input type="text"/>
New PIN	<input type="text"/>
Confirm New PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
PIN Unlock	
PUK	<input type="text"/>
New PIN	<input type="text"/>
Confirm New PIN	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Information Table: This table will show all information about the SIM card used in your Super Modem III. For more details, please refer to the following parameters below:

SIM Card Status: It includes “SIM not inserted”, “READY”, “SIM PIN”, “SIM PUK”, “ERROR” five statuses.

- **SIM not inserted:** It stands that the SIM card has not been inserted into the router yet.
- **READY:** It stands that the SIM card works normally.
- **SIM PIN:** It stands that the user needs to input the correct PIN code due to the wrong PIN code value of system.
- **SIM PUK:** It stands that the SIM card has already been locked. The user needs to request ISP and input the correct PUK to unlock the SIM card.
- **ERROR:** This message will be shown if the system fails to detect the information of the SIM card.

Remaining attempts to enter PIN: It shows the remaining times that you are allowed to input the PIN code for the SIM card inserted into the router. Once the times exceeds 3 times, the SIM card will be locked.

Remaining attempts to enter PUK: It shows the remaining times that you are allowed to input the PUK for the SIM card inserted into the router. Once the times exceeds 10 times, the SIM card will be useless.

Automatic PIN CODE insertion on boot: Decide that whether to use the value filled in the field of **Type the PIN CODE for automatic insertion** to do the authentication of SIM card or not while the router is powered on. To enable it, please click on the checkbox in front of this function.

Enable PIN request for initialization: Enable/Disable the PIN code function. In case this function is enabled and your SIM card has the PIN code setup, you must input the correct pin code and press the **Apply** button for the authentication. Three successively incorrect input of Pin Code will make the SIM card locked.

Enter PIN: In case the field of SIM Card Status in the Information Table is at the “SIM PIN” status, you should enter the correct PIN code in the **PIN** field of this function and press the **Apply** button for authentication. The system will return the message in the pop-up window for you to realize whether your setting is successful or not.

Change PIN: Besides the cell phone, you are also allowed to modify your PIN code of the SIM card through this function. To modify this password, please fill in your old password and your desired new password accordingly, then re-key this new password into the **Confirm New PIN** field. The new settings will be taken effect immediately after you press the **Apply** button. You also can realize whether this change is successful or not from the message returned by the system in the pop-up window.

PIN Unlock: As we had mentioned above the “SIM PUK” status displayed in the field of SIM Card Status in the Information Table, it means that the SIM card is locked. To unlock the SIM card, you should enter the correct PUK in the **PUK** field of this function and new PIN code accordingly. Also re-key this new PIN into the **Confirm New PIN** field of this function before pressing the **Apply** button for authentication. The system will return the message in the pop-up window for you to realize whether your setting is successful or not.

3.4.3 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. User can upgrade the firmware in this page. Please note that power cannot be off in the process of the software upgrade. You must do it carefully.

Specify the filename and directory where the file is located via the **Browse...** button, and click on the **Apply** button when it is completed. When the upload is finished, the router will start upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the router to have the new software worked.

If your upload is unsuccessful, an error message will be shown in the webpage, and it will not upgrade the software as well.

Upgrade Firmware

Upgrade the FWT AP firmware to obtain new functionality. The update process takes approximately 1 minute. Wait for the program to complete the update.

Upload Firmware

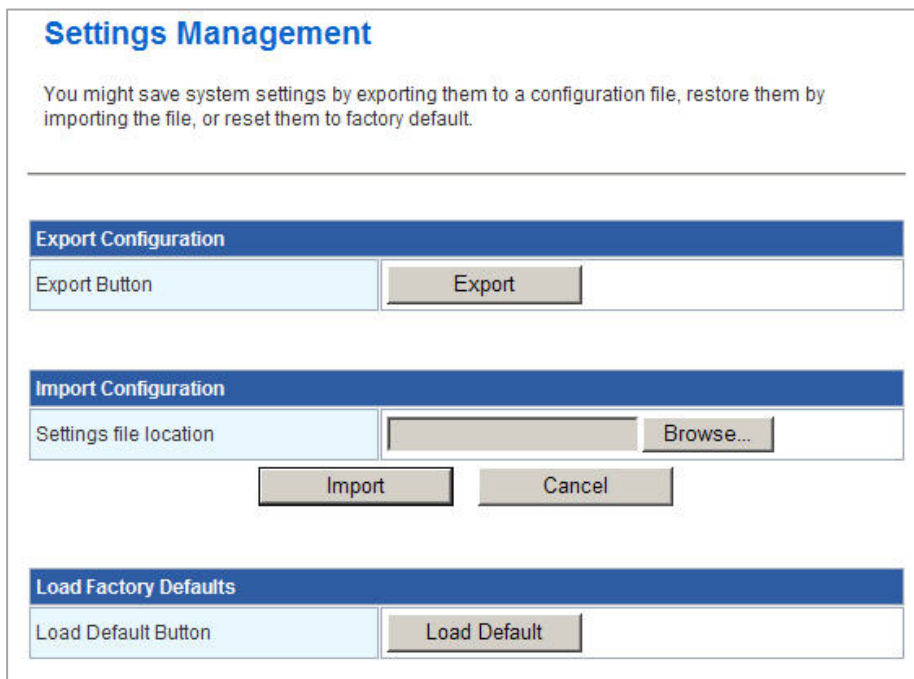
Location:

Location: File path and filename stored the image file you would like to upgrade.

3.4.4 Configuration Management

With this function, user can back up or reload the config files by exporting/ importing settings.

Besides through the press of the **RESET** button in the front panel to execute the hardware reset function as we had mentioned in Section 2.2.1 for the router. The software reset function provided here takes the same effect as the **RESET** button on the front panel of the router. It will take about 30~60 seconds to complete the system boot.



Export: To export the current settings stored in the flash to a config file, just press the **Export** button.

Import: Import the config file into your router. Specify the filename and directory where the file is located via the **Browse...** button, and press the **Import** button when completed.

Load Default: Restoring the unit to the factory default settings will erase all settings, including any rules that you had created. To have the router's settings be returned to the factory default, just press the **Load Default** button. Please note that the router cannot be powered off while resetting to the factory default.

3.4.5 Status

In the Status page, it tells you the basic information of the system. You can check the device status, including the firmware version, system up time, current operation mode, WAN/Local IP address, MAC address and so on. They will be refreshed per 3 seconds. With these information, it is helpful while malfunctioning.

SM3G III Status	
System Info	
Firmware Version	1.0.0.19
System Up Time	10 mins, 38 secs
Operation Mode	3G Router Mode
Internet Configurations	
WAN IP Address	111.80.70.225
Subnet Mask	255.255.255.255
Default Gateway	192.168.122.122
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.192.1
Local Network	
Local IP Address	192.168.0.254
Local Netmask	255.255.255.0
MAC Address	00:0A:EB:38:0C:18
IMEI	352347031828667
Registration Network	Local
CSQ	17
PLMN	Chunghwa Telecom(46692)
Connection Type	HSUPA
MyLoc (MCC:MNC:LAC:CI)	466:92:10291:74522

3.4.6 Statistics

The Super Modem III offers the counter function to collect all counting information about the memory status and all interfaces' receiving/transmitting packets of this router.

Statistic	
Take a look at the statistics	
Memory	
Memory total:	28400 kB
Memory left:	7476 kB
All interfaces	
Name	lo
Rx Packet	4
Rx Byte	360
Tx Packet	4
Tx Byte	360
Name	eth2.1
Rx Packet	5035
Rx Byte	646958
Tx Packet	5715
Tx Byte	3676984
Name	eth2.2
Rx Packet	0
Rx Byte	0
Tx Packet	120
Tx Byte	17989
Name	br0
Rx Packet	5023
Rx Byte	625237
Tx Packet	5711
Tx Byte	3653824
Name	ppp0
Rx Packet	2437
Rx Byte	1493346
Tx Packet	2349
Tx Byte	334147