SIP-Based Wireless Gateway SS38

FCC ID: Q5S-SS38

Thank you for your purchase of SIP-Based Wireless Gateway

Notice regarding electromagnetic signal interference

If this equipment is used near a radio or television receiver in a domestic environment, it may cause radio interference.

Install and use the equipment according to the instruction manual.

Notice regarding WLAN electromagnetic waves

Users with artificial heart pacemaker implants should not make use of this device.
This device emits radio waves which could interfere with the correct functionality of such medial devices and be potentially harmful to their users.
Do not use this device near any medical equipment.
Do not use this device near a microwave oven. Electromagnetic waves generated by appliances such as microwave ovens could interfere with the functionality of this device.

Notice regarding 2.4GHz WLAN Electromagnetic wave interference

The bandwidth of this device is identical to the bandwidth for RFID readers using in factory production line (wireless transmission station permit required), low-power wireless transmission stations (wireless transmission station permit non-required), and amateur wireless transmission stations (wireless transmission station permit required).
Before using this device, please ensure that there are no RFID readers, specific low-power wireless transmission stations, or amateur wireless transmission stations nearby. If this device is interfering with RFID readers, please change bandwidth or stop use immediately, and contact your sales representative.

⚠ Operation Safety Guide

Safety-related precautions

The following are some safety-related precautions. Please read carefully.

- Please follow the instructions and procedures in this document to perform the operations properly.
- Please be sure to follow this product's and this manual's precaution items. Omitting these items can cause bodily harm or damage to the device.
- Do not operate the device in methods not stated in this manual.
- For questions regarding this product or this manual, please inquire the place of purchase or the sales clerk.
- This manual contains precaution items that may need further review. It does not guarantee it contains all the situations that might occur. It is recommended to not only follow the instructions contained in this document, but to handle the product carefully at all times.
- The safety related precaution items are listed below. They include"Warnings" "Cautions" and "Notes".

⚠ Warning	Indicates a potentially hazardous situation, which if not avoided, could result in death or serious injury.
⚠ Caution	Indicates a potentially hazardous situation, which if not avoided, may result in minor or moderate injury.
⚠ Notice	This precaution signal is utilized in titles and safety related situations, to enhance attention.
	Provides important information unrelated to security.

◆ Caution about operations (Prohibition)

⚠Warning

⚠ Warning **Never attempt to disassemble the phone cover or AC adapter cover**

Never attempt to disassemble the phone cover or the AC Adapter cover. Disassembly or modification could cause ignition, electric shock, as well as damage to the phone itself.

⚠ Warning **Discontinue the use of the phone if any unusual conditions occur**

If battery is leaking fluid, emitting gas, producing a peculiar smell, or making strange sounds, discontinue use immediately for this may cause ignition or electric shock.
Please remove the battery immediately for safety reasons.

⚠ Warning **Never attempt to perform modifications to the phone**

Never attempt to make any modifications to the phone.
Disassembly or modification could cause ignition, electric shock, as well as damage to the phone itself.

⚠ Operation Safety Guide

⚠Warning Do not damage the power cord

Do not damage, tug, or make modifications to the power cord.
Do not bend the power cord to prevent damage. Do not expose the power cord to heat and never place heavy equipment onto the power cord.
Pulling the power cord excessively might also lead to ignition or electric shock.

⚠Warning Keep away from high humidity

In case the device is immersed in water, power off the device immediately. Continued use of the device under this condition could cause fire or exposure to electric shock. Please consult the place of purchase or sales clerk about the disposal.

⚠Warning Do not insert other objects into the device

Do not insert metallic or inflammable objects into the device for it might cause ignition or electric shock.

⚠Warning Always maintain the charger in a clean status

Please ensure there is no dust on the power cord before plugging it to the outlet to prevent electric shock.

⚠Warning Do not touch the plug or electrical cord with damp hands

Do not touch the plug or electrical cord with damp hands to prevent electric shock.

⚠Warning Do not use accessories from other manufacturers

Using accessories that are not compatible could cause ignition, electric shock or damage to the device.

⚠Warning Do not touch the device when lightning occurs

Please power off and shift to a safe location to reduce risk of electric shock.

⚠Warning Do not insert other objects into the device

Do not insert metallic or inflammable objects into the venthole or fall it to the ground for it might cause ignition or electric shock. If an object is accidentally inserted it, please take out the objest immediately and consult the place of purchase or sales clerk.

⚠Warning Do not place in unstable location

Do not place device on slanting or unstable tables, and other unstable spots for this product may fall, causing serious damage to the device.

⚠Warning Do not place objects on the top of device

Do not place objects such as vases, pots, glasses, medicine bottles, or containers on top of the device. These objects might either cause rupture to the device, or leak liquids that might penetrate the device and lead to fire or electric shock. Placing the device on an unbalanced table, causing the device to drop, will also damage to the device.

Warning **Please hold the plug when pulling out of outlet**

Please hold the plug when pulling out of outlet because pulling on the power cord excessively might lead to damage, electric shock, fire, or damage to the device.

◆ Caution about operations (Prohibition) Related with AC adaptor

Warning **Do not use AC adapters from other manufacturers**

Do not use AC adapters other than the one included with your device for they could cause ignition, electric shock or damage to the device.

Warning **Do not insert plug into an outlet with voltage other than AC240V**

Do not insert plug into an outlet with voltage other than AC240V for it could cause ignition, electric shock or damage to the device.

⚠ Operation Safety Guide

⚠Caution

⚠Caution Don't close up the venthole

Venthole is designed to prevent producing heat inside the device. Do not put the device in the airless condition or erect the device, and close up the venthole for they will cause ignition, electric shock or damage to the phone.

⚠Caution Do not combine or integrate with other equipment or hardware

Do not combine or integrate with other equipment or hardware for it might cause fire or damage to the device.

⚠Caution No not expose the phone to high pressure

Keep phone away from contact with other metallic objects, Heavy weight could cause phone damage.

⚠Caution Pull out plug when in movement

When in movement, please ensure the plug has been pulled out of the outlet.

⚠Caution Please pull out plug when not in use

For your safety, unplug the battery charger from wall outlet if it will not be used for a long time in summer; otherwise it may cause fire.

⚠Caution Do not expose the phone in unfavorable environment conditions

Do not expose the phone near gas leakage. Keep the device in a clean, dust-free environment. Avoid exposure to smoke, erosive gases. Avoid placing the device in locations subject to severe vibration. Do not expose device directly to sunlight. Keep away from heat sources such as stoves, or other products that produce heat. Do not expose the device to fire or high temperature for this could shorten the lifetime of the device.

⚠Caution Do not place heavy equipment onto the power cord

Do not place heavy equipment onto AC adapter for it might lead to fire or damage.

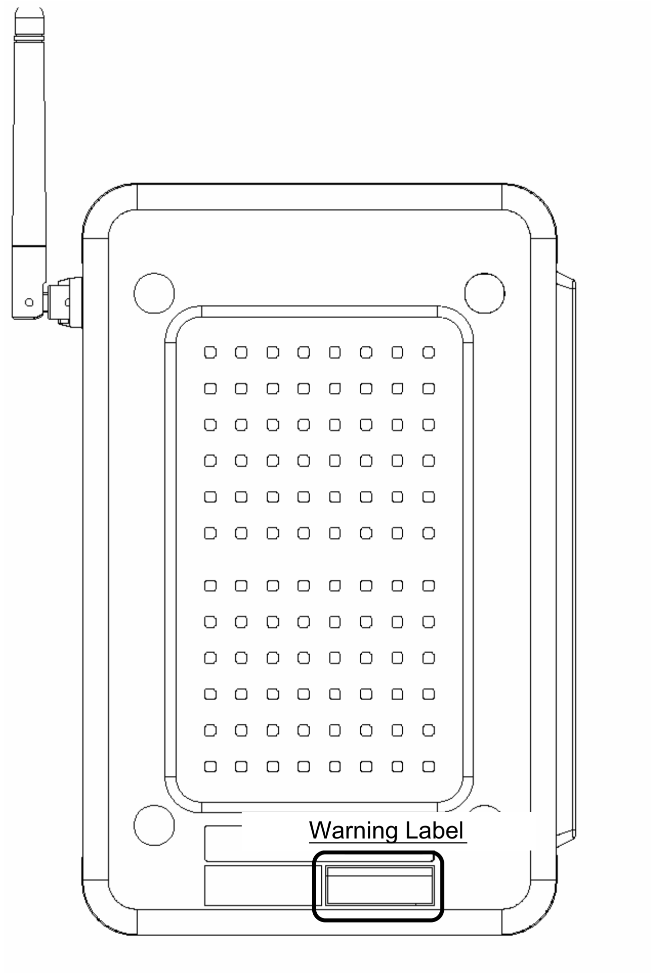
⚠Caution Discarding the device

Please regard to the related legislation and return the obsolete device to the place of purchase or to the nearest recycling facility.

Operation Safety Guide

The warning labels are adhered the device and the AC adapter in the parts shown in the figure below:

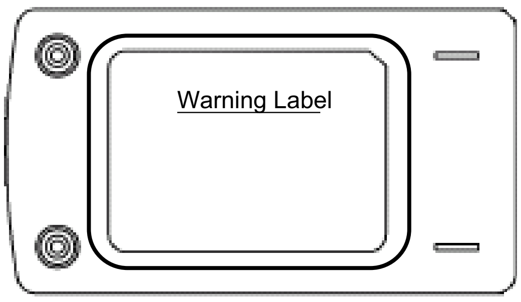
(1) AP

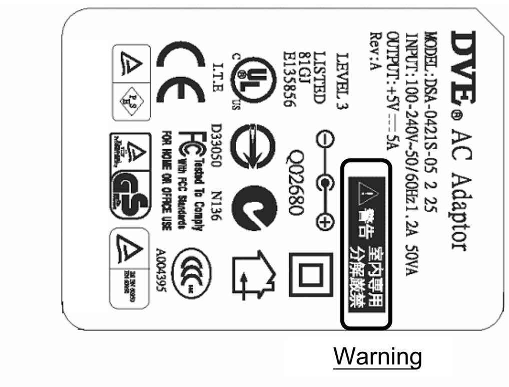


(a) Warning Label (Back View)

(b) Warning Label

(2) Bottom of Adaptor Cover





(a) Warning Label (Back View)

(b)Warning Label

Table of Contents

Table of Contents

Table of Contents

1 Important Safety Precautions

1.1 Warning/Caution

- This manual is for use with the SIP-Based Wireless Gateway (Server Mode) and (AP Mode)
- The manufacturer disclaims any liability for damage resulting as a consequence of improper use, or damage due to external causes, such as power outage, or unfavorable environmental conditions. Please handle your phone with care.
- The repair and maintenance of this product must be handled by a qualified professional service technician. Please be noted that by not being done by a qualified technician might violate the law or result in an accident.
- This product generates, uses, and can radiate radio frequency energy might cause interference to radio or television signals when near these devices. The user is encouraged to increase the distance between the phone and the other devices.
- This product is made and designed for office operations. Please do no use it for any unfair purpose. Please read all instructions and safety precautions described in this document before operating the product/appliance. Please follow the instructions carefully and ensure you are aware of correct handling procedures.
- It is recommended that this manual is kept at a proper location for quick reference. If misplaced or damaged, please request a new one from the place of purchase (dealer). The contents in this manual are subject to change without notification.

Regarding some advice in this manual

(1) This label indicates caution items or restrictions regarding the use of this product.

Caution

(2) This label is used for items the user should pay attention to when using or setting this product.

MEMO

(3) This label indicates to regard to related information.

☞ Regarding to xxx
Please refer to "xxx

(4) This label indicates which function doesn't support in AP Mode.

~~AP~~

1.2 Applicable machine type

Product Name	Type Model	Title of this manual	Technical Standard Identification Number
SIP-Based Wireless Gateway(Server Mode)		Server Mode	
SIP-Based Wireless Gateway(AP Mode)		AP Mode	

1.3 Confirm objects contained in package

Please ensure the package contains the following items:
Please contact the place of purchase if any items are missing.

Contents	SIP-Based Wireless Gateway(Server Mode) SIP-Based Wireless Gateway(AP Mode)
Body	1
Safety precaution booklet	1
User manual	1
AC adapter	1
Stand	1
Power cord	1
CD-ROM	1

1.4 External Appearance

1.4.1 Front view

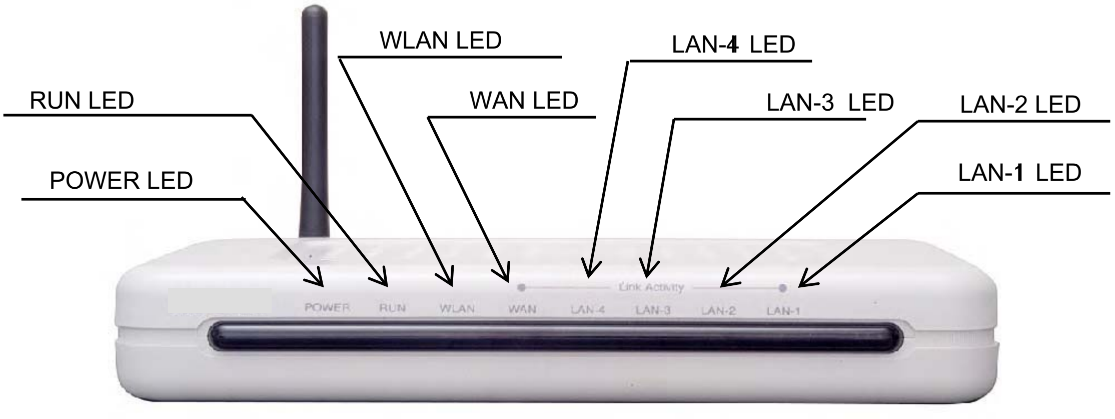


Figure 1.4.1 Front view

Table 1.4.1 Functions Overview

No.	Menu	Description	Remark
1	Power LED Green	Lighting: The power supply of this device is turned on. Turning off: The power supply of this equipment is turned off.	
2	Run LED Green	Lighting: The device is operating normally. Blinking (quickly): The device can't start (cycle : 0.5 secs). Blinking (slowly): The start is under processing.(cycle : 1 secs). Turning off: The device is unusual.	
3	WLAN LED Green	Lighting: WLAN is operating normally. Blinking: WLAN is transmission wireless LAN data. Turning off: WLAN is unusual.	
4	WAN LED Green ~~AP~~	Lighting: The link of a WAN port is established. Blinking: Data transmission in a WAN port. Turning off: Link of a WAN port is not established.	SS38 (Server Mode)
5	LAN-1 LED Green	Lighting: Link of LAN-1 port is established. Blinking: Data transmission in the LAN-1 port. Turning off: Link of the LAN-1 port is not established.	
6	LAN-2 LED Green	Lighting: Link of LAN-2 port is established. Blinking: Data transmission in the LAN-2 port. Turning off: Link of the LAN-2 port is not established.	
7	LAN-3 LED Green	Lighting: Link of LAN-3 port is established. Blinking: Data transmission in the LAN-3 port. Turning off: Link of the LAN-3 port is not established.	
8	LAN-4 LED Green	Lighting: Link of LAN-4 port is established. Blinking: Data transmission in the LAN-4 port. Turning off: Link of the LAN-4 port is not established.	

1.4.2 Back view

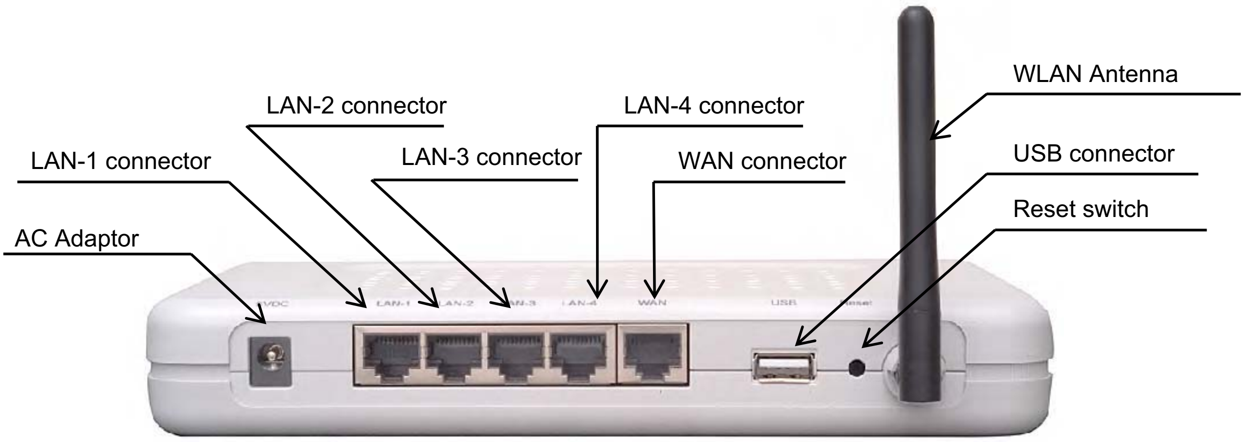


Figure 1.4.2 Back view

Table 1.4.2 Functions overview

No.	Menu	Description	Remark
1	AC adaptor	Connect to the attached AC/DC adaptor (DC+5V, 2A). ❗Caution **Please do not use another AC/DC adaptor.** **It will cause the damage.**	
2	LAN-1 connector	RJ-45 connector (straight cross automatically) Connect to IP fixed-line phone or VoIP gateway. Moreover, it is used also for connecting SS38 (Server Mode)~(AP Mode)	LAN-4
3	LAN-2 connector	RJ-45 connector (straight cross automatically) Connect to IP fixed-line phone or VoIP gateway. Moreover, it is used also for connecting SS38 (Server Mode)~(AP Mode)	
4	LAN-3 connector	RJ-45 connector (straight cross automatically) Connect to IP fixed-line phone or VoIP gateway. Moreover, it is used also for connecting SS38 (Server Mode)~(AP Mode)	
5	LAN-4 connector	RJ-45 connector (straight cross automatically) Connect to IP fixed-line phone or VoIP gateway. Moreover, it is used also for connecting SS38 (Server Mode)~(AP Mode)	
6	LAN connector ~~AP~~	RJ-45 connector (straight cross automatically) Connect to the circuit from IP phone network (A WAN connector cannot be used in SS38 ~(AP Mode)	SS38 (Server Mode)
7	USB connector	This device doesn't support.	
8	Reset switch	Switch for initializing the device (by long pressing).	
9	WLAN antenna	An antenna for wireless LAN transmission and reception.	

1.5 WLAN Safety Notice / Precautions

The signal strength on the WLAN IP phone and the parameters set by the network operator will greatly affect the talk and standby times of the phone, as well as the range and quality of the phone call.
Please read the following precaution items careful.

(1) Notice regarding environment

① Please use it indoor or in a high and viewable place.

② Electric waves can penetrate a wall and glass, but it can't penetrate the metal. if this device is accommodated in a metal rack, the transmission range may become narrow.

(2) Communication Range of wireless IP phone

When using an IP phone, the phones settings will affect the communication range and quality. Suggest to keep with in 30 meters.

(3) Notice regarding 2.4GHz WLAN Electromagneticwave interference

The bandwidth of this device is identical to the bandwidth for RFID readers using in factory production line (wireless transmission station permit required), low-power wireless transmission stations (wireless transmission station permit non-required), and amateur wireless transmission stations (wireless transmission station permit required).

① Before using this device, please ensure that there are no RFID readers, specific low-power wireless transmission stations, or amateur wireless transmission stations nearby.

②If this device is interfering with RFID readers, please change bandwidth or stop use immediately, and contact your sales representative.

Table 1.5.1 Device wireless LAN overview

No.	Menu	Description
1	Bandwidth	2.4GHz Wireless Device
2	Modulation	DS-SS OFDM
3	Default Interference distance	Under 40m
4	Change bandwidth	4 Change bandwidthUses full bandwidth. Avoid RFID readers and low-power wireless transmission station bandwidths.

The content on the above table are displayed on the Warning label at the back of the phone

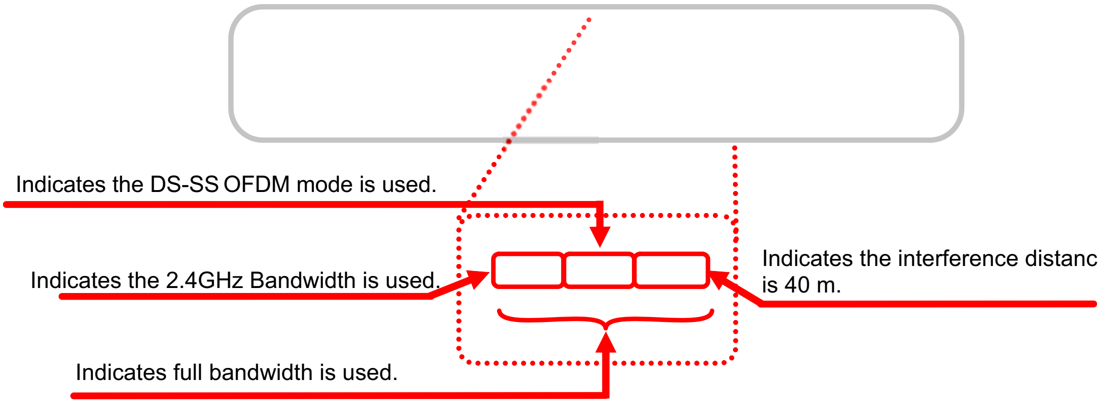

Indicates the DS-SS OFDM mode is used.
Indicates the 2.4GHz Bandwidth is used.
Indicates the interference distance is 40 m.
Indicates full bandwidth is used.

Figure 1.5.1 Lable notation

1.6 Specification

Menu			Specification	Remark
Interface	WAN		10BASE-T/100BASE-TX(10/100Mbit/s) x 1 circuit	~~AP~~
	LAN		10BASE-T/100BASE-TX(10/100Mbit/s) x 4 circuits	
	WLAN	Mode	IEEE802.11b/g(11/54 Mbit/s)	
		Change bandwidth	OFDM-BPSK QPSK 16QAM 64QAM DBPSK DQPSK CCK	
		Reset	Reset	
Indication of moving			Displayed by LED	
System summary			(1)Setup by web management (2)Download the system summary file from Web management	
AC adaptor	Input Current		AC100-240V+/-10V 50/60Hz +/- 1Hz	
	Charge Output		5.0V/5A	
Dimensions [W x D x H]	AP (mm)		207 x 136 x 32	
	Stand (mm)		100 x 136 x 32	
	AC adaptor (mm)		92 x 55 x 30	
AC adaptor cord length	AC (M)		1.3	Without the plug
	DC (M)		0.8	
Weight			AP under 350g, stand under 25g	
Environmental Conditions	Temperature		5~40℃	Non-dew condition
	Humidity		20~80%RH	

2 Functions

2.1 About functions of the device

◎ IP cellar phones connecting to this product can be used as IP phones (VoIP) with broadband network.
◎ Cellar Phones connecting to this product can be used as interphones or transfer extension number.
◎ Wireless IP phone can login up to 100 VoIP devices, so it's easy to expand.
◎ This product uses 2.4GHz bandwidth (802.11b/g wireless network).
◎ This product provides various wireless network security settings including registering MAC address and shared key authentication.
>Supports WEP RC4 (64/128bit)
>Network authentications support "WPA-PSK", "WPA" , "IEEE802.1X. It can configure RADIUS server to use wireless network If using" WPA" and "IEEE802.1X".
◎ IP filter can control access restriction.
◎ This product has firewall function.
◎ Network Address Port Translation function (NAPT).
◎ DHCP Server function.
◎ DNS Proxy function.
◎ SIP Proxy server / SIP Registrar function.
◎ Wire LAN supports 10BASE-T/100BASE-TX (autoswitch).
◎ "LAN" port supports 4 port switching hub.
◎ "WAN" port x 1 and "LAN" port x 4 can auto negotiation MDI (straight) / MDI-X (cross).
◎ This product can configure whole functions through WWW browser.
◎ This product is non-licensed WLAN AP.

SS38(AP Mode)doesn't support a part of functions as above.
Please refer to next page **"Table 2.1.1 Function"**.

Chart 2 Functions

Table 2.1.1 Functions

●:support

	Menu	Description	Server Model	AP Model
Interface	WAN port	Port quantity (RJ-45)	1	(※1)
		10/100BASE-TX auotswitching	●	
		MDI/MDI-X auto negotiation	●	
	LAN port	Port quantity (RJ-45)	4	4
		10/100BASE-TX auotswitching	●	●
		MDI/MDI-X auto negotiation	●	●
	WLAN port	IEEE802.11b/g(2.4GHz bandwidth-11/54Mbit/s)	●	●
		Wireless channel quantity	US (1~11 Ch) Europe (1~13Ch) Japan (1~14 Ch)	US (1~11 Ch) Europe (1~13Ch) Japan (1~14 Ch)
		The max number of sessions of WLAN	10(※2)	10
Functions	SIP functions	SIP Proxy server	●	(※1)
		SIP Registrar	●	
		The maximum number of registered users	100	
		The maximum number of concurrent calls	20	
		Call pickup function (auto-replay)	●	
		Multiple gateway connecting	●	
	DNS Proxy function	Refreshing	●	(※1)
		The maximum number of conditions	16	
	DHCP function	Server function	●	(※1)
		The maximum number of available IP Address (server function)	253	
		Client	●	
	NAPT	IP address refreshing	●	(※1)
	Wireless LAN function	Disable WLAN	●	(※1)
		CAC controlling	●	●
	IP login	Default WAN port	●	(※1)
		Statically	●	
	IP connecting ways	Ethernet	●	●
		PPPoE	●	(※1)
Security	WLAN Security	WEP(RC4):64/128 bit	●	●
		WEP/802.1x	●	●
		WPA/802.1x	●	●
		WPA-PSK	●	●
	MAC address filtering function	L2 ACL	●	●
	IP Packet filtering function	Inbound	●	(※1)
		Outbound	●	
	Firewall function	DoS Prevention	●	(※1)
		Intrusion detection	●	
Information	System summary	Display MAC address or version info	●	●
	Interface information	Display the status of WAN port	●	(※1)
		Display the status of LAN port	●	●
		Display the status of WLAN port	●	●
	SIP information	Display SIP server information	●	(※1)
		Display registrars	●	
		Display on-line callers	●	
	Log information	Display System log	●	●
		Display SIP log	●	(※1)
	Others	WWW browser user interface (GUI)	●	●

(※1) : SS38 (AP Mode) doesn't support.

(※2) : It switches as well as the maximum number of concurrent calls (Max Calls) when disabling CAC controlling.

2.2 MDI/MDI-X

This device features 4-port Ethernet LAN port(LAN-1~LAN-4) and 1-port WAN up to 5 Ethernet ports inside.

These 5 Ethernet ports support auto negotiation of 100BASE-TX/10BASE-T, and MDI (straight) / MDI-X(cross).

Please use the cable over Category 5 to connect the ports.

2.3 Wireless LAN specification (IEEE802.11b/g)

This device provides the specification of WLAN as below:

>IEEE Std 802.11b-1999 and IEEE Std 802.11g -2003
Using 2.4GHz bandwidth.
The max speed of transmission is 54Mbit/s.

This function can be used regarding to System Configuration.

Regarding WLAN settings,
Please refer to **" 5.1.4 WLAM Port Settings "**

2.4 Support various securities

2.4.1 Wireless LAN security

This device provides four security functions as below.
These securities can be configured through System Summary or Settings.

（1）WEP

RC4, 64bit and 128bit network authentication.

（2）WEP/802.1x

RADIUS authentication and WEP security.

（3）WPA/802.1x

A security combining with RADIUS authentication and WPA (Wi-Fi Protected Access).

（4）WPA-PSK

A security combining with WPA (Wi-Fi Protected Access) codec and WPA-PSK authentication (Pre-Sheared Key).

Regarding to the settings of WLAN Security functions,
" 5.1.4 WLAN Port Settings " .

2.4.2 Other securities

Except the WLAN security functions in 2.4.1, this device provides the securities (packet filtering)
This security can be configured in System Summary.

（1）L2 ACL

It is the function, which registers the access control list (ACL) of the layer 2 (MAC of the WLAN device), and carries out packet filtering regarding to the registered ACL.
Access of the WLAN device to this equipment is controllable by using this function.

（2）Packet Filtering (Inbound) ~~AP~~

This function performs filtering control regarding the packet relayed from the WAN side circuit to the LAN/ WLAN side circuit to IP packet level (IP address or protocol type) regarding to the security policy rule defined in advance.

（3）Packet Filtering (Outbound) ~~AP~~

This function performs filtering control regarding the packet relayed from the LAN / WLAN side circuit to the WAN side circuit t o IP packet level (IP address or protocol type) regarding to the security policy rule defined in advance.

Regarding to the settings of L2 ACL and a Packet Filtering function
Please refer to**"5.2 System Security ".**

2.5 Firewall

~~AP~~

This device is supporting the following firewall functions.
The inaccurate packet detected by the firewall function cancels.
The firewall function can be used by setting the "Firewall" status of the "System Security" menu to enable.

> Regarding to the settings of firewall function,
> Please refer to **"5.2 System Security".**

2.5.1 DoS Prevention (DoS:Denial of Services)

DoS is the general term of the attack from a malicious third-party through the network, and inaccurate data is transmitted to disable a computer or a router to paralyze the network traffic flow.

The functions which can detect Dos attacks are the following six types and Packet Violating (violation of a packet).

◎ IP Spoofing — To masquerade the self-IP as a IP address of the target to attack or break through firewall.

◎ Land Attack — To transmit a SYN packet and to make the device lapse into a endless loop.

◎ Ping of Death — To use Ping and send the huge and oversize IP packet to the device, and to crash the target.
The attack way for the bug of a TCP/IP protocol stack.

◎ Smurf Attack — By sending ping requests to a broadcast address on the target network or an intermediate network. The return address is spoofed to the target address. Since all nodes on the subnet pick up a broadcast address, generating hundreds of responses from one request and eventually causing a traffic overload.

◎ Ping Flood — A simple Denial of service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.

◎ UDP Flood — An attacker sends a UDP packet to a random port on the target system.

◎ Packet Violating — To send the packet of the inaccurate format created in order to crash the TCP/IP protocol stack.

> Regarding to the result of detection by this device,
> It will display in **"(1)Security Log "of "6.1.2 System Log"**

2.5.2 Intrusion detection

Detect the inaccurate access to this device

> Regarding to the result of detection by this device,
> It will display in **"(1)Security Log "of "6.1.2 System Log"**

2.6 SIP Functions

~~AP~~

This device supports SIP Proxy server and SIP Registrar functions.

Regarding to the settings of SIP functions,
Please refer to**" 5.3 SIP Configuration "**.

Table 2.6.1 Transmission types of SIP functions

No	Types	Description	Moving of transmission
1	Busy forward	Busy forward	Transfer the call of the registered SIP user in a call.
2	Unavailable forward	Unavailable forward	Transfer the call if the registered SIP users or the registered callee doesn't answer.
3	Unconditional forward	Unconditional forward	Transfer the call from the registered SIP user unconditionally.
4	No answer forward	No answer forward	Any call to the registered SIP user will be transferred within 1-999 seconds automatically if no respond.
5	Attended transfer	Attended transfer	Transfer the call by following procedure. (Take A, B, C registered in this device for example) (1) The call between device A and device B (2) Hold the current call from device B or A (3) Device B makes a call to device C (4) The call between device B and device C (5) Device B terminated the call (6) The call between device A and device C

2.6.1 Call pickup function

This device supports call pickup function.

This device can transfer the call from the extension numbers which registered in "SIP User" to the other substitute extension number to respond.

The call pickup function of this device can become enhance call pickup function.

If the extension number is registered in this device, the extensions can pickup the call except the special group.

(1) Set up the extension number for a call pickup party as a special group.

(2) The maximum, which can be set up 10.

(3) Each special group can set up to 5 extension numbers. (Except Outbound Call)

(4) The extension numbers which are set up in special group and "call pickup" extension numbers will take the extension numbers which are registered in the "SIP User" information as the targets.

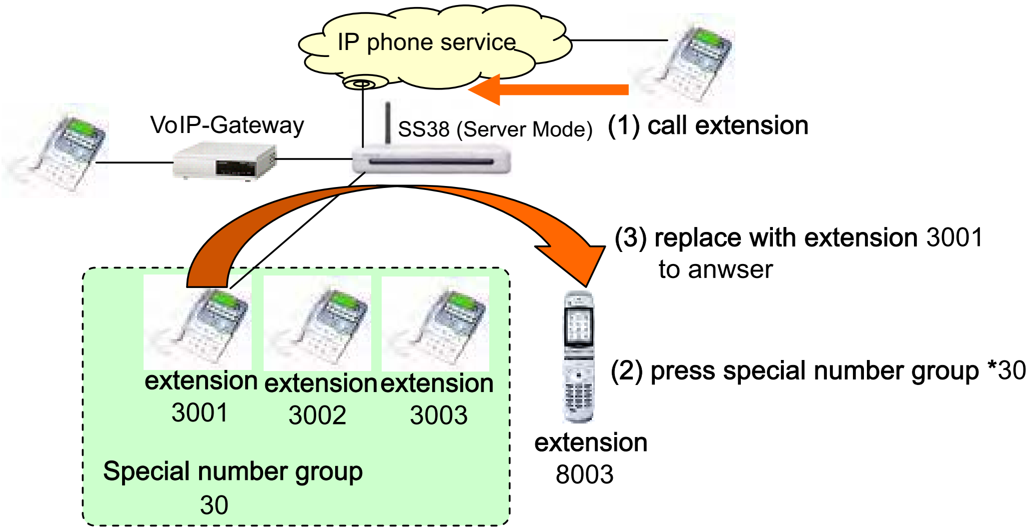


Figure 2.6.1 Call pickup function

Regarding to the settings of Call pickup function,
Please refer to " **5.3.2.1 SIP Call Pickup Management** ".

2.6.1 Connect multiple Gateway

This device supports multiple gateway as below.

(1) Use PBX and VoIP gateway at the same time.

(2) By the increase in the number of connection circuits, the maximum of calls is up to 20. (at the same time).

The maximum of 4 Gateway IP addresses can be set to one group.

A Gateway address will be searched by the sequence of registration. When the address of front Gateway can't be used (all circuits are busy), the address of the next Gateway will be used.

The maximum of 2 groups can be set up with the device.

This setting will just be used if the number is one of the "SIP User" registrars.

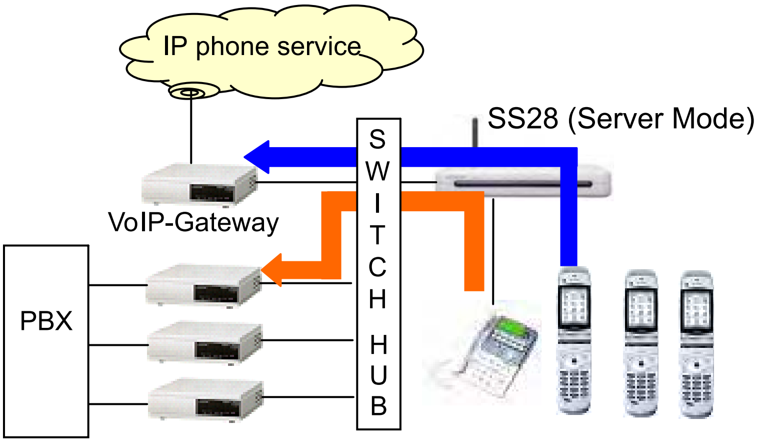


Figure 2.6.2 Multiple Gateway

Regarding to the settings of multiple Gateway,
Please refer to **" 5.3.5 SIP Gateway "**.

2.7 DNS Proxy

~~AP~~

This device supports DNS (Domain Name System) Proxy.

This function can change a domain name and a website name into an IP address or URL.

It can set up "DNS Proxy Table", and conversion conditions can be registered up to 16 entries.

Regarding to the settings of DNS Proxy,
Please refer to **" 5.1.2 LAN Port Settings "**.

2.8 Modify IP Address

~~AP~~

This function is to change the IP address of a local subnet (LAN side) into the IP address of a global subnet (WAN side) .

Caution

(1) When perform this function, please use the IP address of a local subnet (LAN side) within Class C.

(2) Although this device supports NAPT (IP masquerades) , neither the protocol type nor port number can be ordered arbitrarily.

Regarding to the settings of Modify IP Address,
please refer to "**5.1.2 LAN Port Settings**".

2.9 DHCP functions

~~AP~~

This device supports DHCP server (LAN side) and DHCP client function (WAN side).
DHCP server gives a dynamical IP address to the DHCP client device connected to the local subnet (LAN side).

DHCP client can get an IP address from the server on a global subnet (WAN side).

MEMO

About DHCP functions

(1) DHCP server can operate by only a LAN port. Only the client which connected to the LAN side will be distributed.

(2) The IP addresses, which a DHCP server distributes, are up to 253.

(3) As for a DHCP client can operate by only a WAN port.

Regarding to the settings of DHCP function
please refer to "**5.1.2 LAN Port Settings**"&
"**5.1.3 WLAN Port Settings**".

2.10 Control CAC

This function can deter new calls in case the number of wireless session exceeds 10 calls. (example: 5 calls in the WLAN device.).

This function will deny the wireless session command from another wireless device in a 10-sessions group, and respond busy automatically.

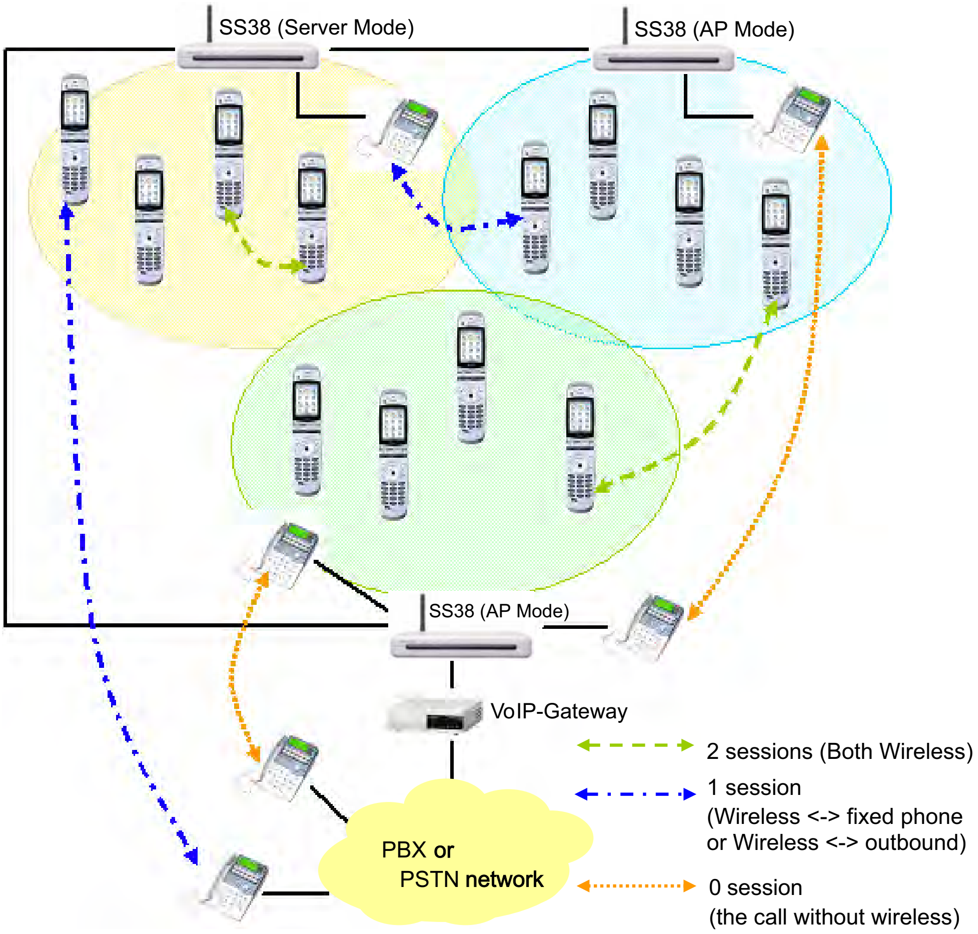

SS38 (Server Mode)
SS38 (AP Mode)
SS38 (AP Mode)
VoIP-Gateway
PBX or
PSTN network
2 sessions (Both Wireless)
1 session
(Wireless <-> fixed phone
or Wireless <-> outbound)
0 session
(the call without wireless)

Figure 2.10.1 Control CAC

2.11 User interface of WWW browser

This device supports the user interface of WWW browser.
User can setup any command and system summary of this device from the WWW browser.

Regarding to the user interface of WWW browser,
please refer to " 3 Preparations for settings"

3 Preparations for settings

This equipment can display the configuration and system information in the utility setting of WWW browser.
Furthermore, if using a setting wizard, it's easier than a guidebook to set this device .
This chapter will explain the setting of PC and the access to the utility setting.

3.1 Applicable software (WWW browser)

Internet Explorer 5.0
Netscape 6.0

3.2 Start the device

If finish the preparations for settings, please insert connector into slot at the back of the device.
This device will start.
Please use Category 5 cable and connect the LAN port to PC.

3.3 Setup the PC

Please setup the manual PC network setting to connect the PC and this device.
Regarding to SS38 (Server Mode), please refer to 3.3.1. Regarding to SS38 (AP Mode), please refer to 3.3.2.

Please ensure that the LAN port has connected to the PC through category 5 cable in advance.

3.3.1 Setup the DHCP client

Initial setting of this device operates as a DHCP server.
In the setting of PC network (TCP/IP), please check if IP address will be configured automatically, and setup the PC as DHCP client.

Step 1

Please open a "**control panel"** from the "**start**" button of PC, and double-click "Network and Dialup". ("**Network and Internet connections**"will display on OS, please double-click "**Network connections**".)

Step 2

Right-click on the "**Local area connection**" button, and select **"Properties"**

Step 3

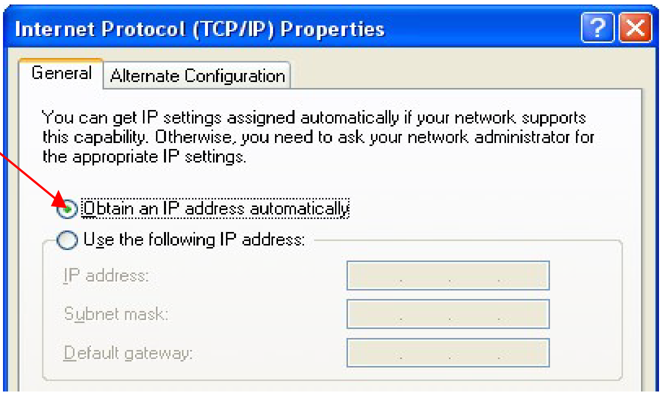
Please choose "**Internet protocol (TCP/IP)**"from the pop-up window, and click the "**Properies**" button.

Step 4

Select " **Got an IP address automatically** " on the right screen.

Click the "**OK**"button to save the configuration.

The PC is set up as a DHCP client.


Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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:
Subnet mask:
Default gateway:

3.3.2 Setup the fixed IP

If you want to setup the fixed IP address, the address besides the range of the IP address, which the DHCP server has reserved, can be assigned.

Step 1~3

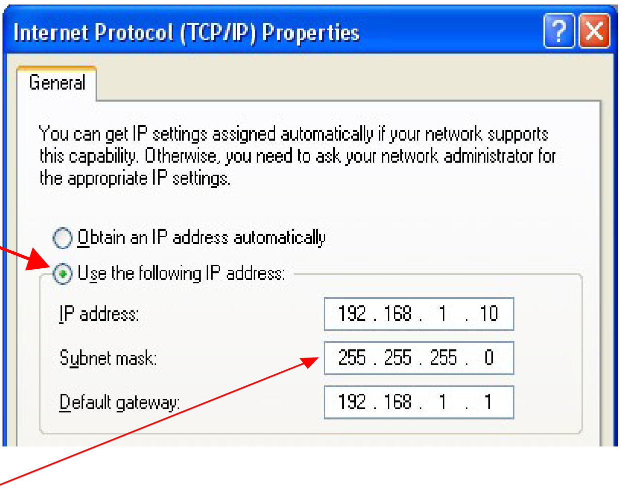
Follow the step as well as "3.3.1 Setup DHCP client".

Step 4

On the right screen, please select "Use the following IP address", and enter subnet mask and default geteway.

Ensure the PC IP address and the IP of network are in the same subnet network.

The default IP address of the LAN port is **192.168.1.1**.



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: 192 . 168 . 1 . 1

Example for the setting of PC IP address

IP address: 192.168.1.10

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

Caution

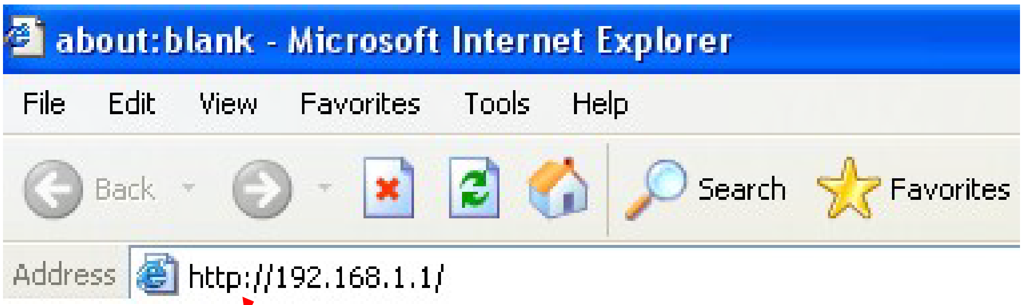
SS38 (AP Mode) doesn't support DHCP server function.

If you want to connect to **SS38 (AP Mode)**, please set a fixed IP address.

3.3.3 Access to utilities setting

Caution

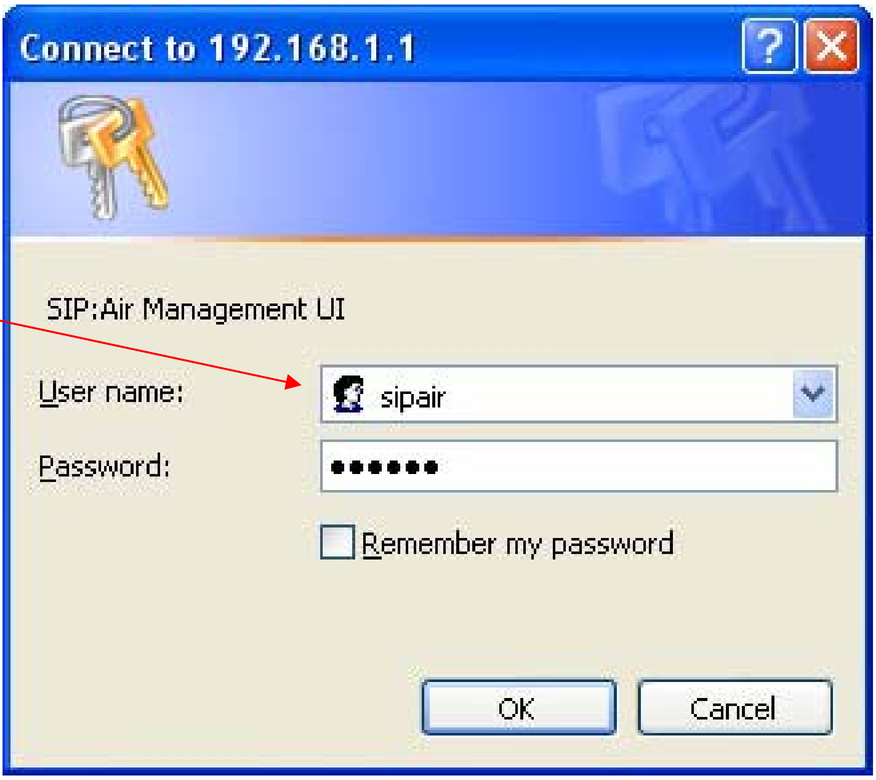
Please setup is as "not via Proxy" through WWW browser.



Address: http://192.168.1.1/

step1

Enter the IP address of this device in the address box (default value is **192.168.1.1**), and press "**Enter**".



User name: sipair

Password: ••••••

step2

It will display the page needs to enter the password. Enter the username "**sipair**", and password "**sipair**".

Press "**OK**" button, and then the first page will display and the process is finished.

3.4 Founctions of setting utilities

Quick Link Selector

For viewing the page and setting the summary quickly, you can edit your favorite page to the link list.

Regarding to Quick Link Selector, please refer to "**3.5 Quick Link Selector**".

Display system summary

Display the system information incluind WAN, WLAN, LAN port, System status, statistic and system log of the device.

Regarding to system information, please refer to "**6 Ensure the status of the device**".

Setting Wizard

You can follow this guideline to setup this device.
In Configuration Wizard, you can setup WAN, LAN and WLAN.
in Wireless Security Wizard, you can setup WLAN security.

Regarding to Setting Wizard, please refer to "**7.1 System Tool Box**".

System summary menu

It can setup various system summary of this device.

Regarding to system summary, please refer to "**5 Setup the device**".

Checking input date

If an wrong data has be input, the check function will notify an error message to a WWW browser.
It will display an error message and resets the input field.

Firmware upgrade

The firmware of this device can be updated to the newest version.

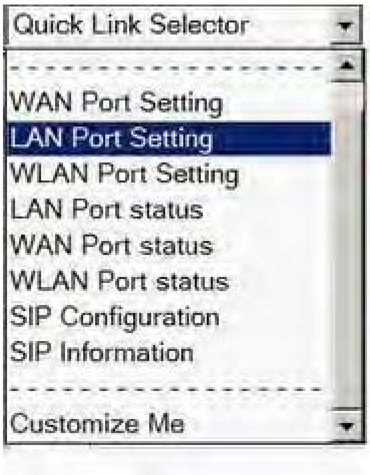
Upgrade and download the system configuration file

You can download the system configuration to save it, and upgrade new configuration via PC.

Regarding to fireware upgarde, upgrade and download the system configuration file, please refer to "**7.1 System Tool Box**".

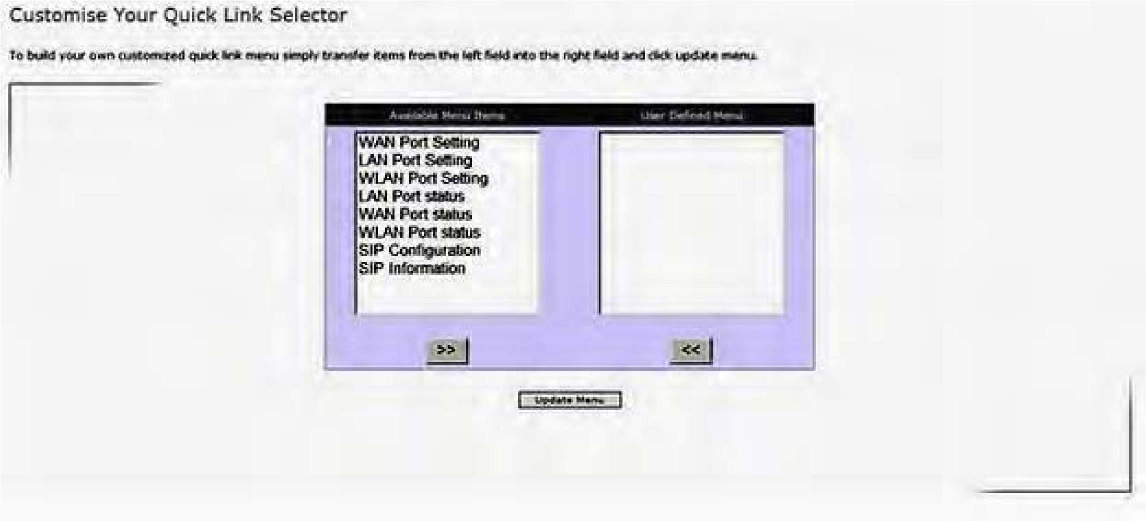
3.5 Quick Link Selector

There is a pull down menu called **Quick Link Selector** (quick link selector) on the upper left of each page. If displays the default status on the right figure.



It can customize the list. Select "**Customize Me**", and please move from left column from right column. These items displays "**Quick Link Selector**"

Press "**Update Menu**" button to apply the configuration.


Customise Your Quick Link Selector

To build your own customized quick link menu simply transfer items from the left field into the right field and click update menu.

3.6 Button functions

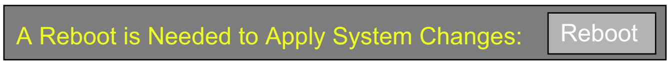
After configuration of setting, please press "**Apply**" button.(always display on the button of the page.)

It can return to the last page of setting menu.
The button will displays when using setting wizard.

It can go to the next page of setting menu.
The button will displays when using setting wizard.

Return to system tool box page.
The button will display when using setting wizard.

If pressing the "**Apply**" button or "**Finish**" button, but it displays this signal on the screen as left, You have to restart the device for the result of configuration.
Please press "**Reboot**" button to restart.


A Reboot is Needed to Apply System Changes:

4 System Configuration

The system configuration of this device is as below:

(AP:SS38(AP Mode), ー:none, △:none in part)

No	Menu	Description	AP (*1)
1	System Configuration	(1) Administration (Password for system management) (2) LAN Port Settings (LAN port setting) (3) WAN Port Settings (WAN port setting) (4) WLAN Port Settings (WLAN port setting)	△
2	System Security	(1) Access Control (Firewall, packet filter)	△
3	SIP Configuration	(1) SIP Configuration (SIP option information) (2) SIP Group (SIP group information) (3) SIP User (SIP user information) (4) SIP Domain (SIP domain information) (5) SIP Gateway (SIP gateway information)	－

(*1) Indicates if SS38 (AP Mode) can setup (SS38 (Server Mode) can setup all items)

Caution

After changing system configuration, to see the contents please press Apply

After pressing the Apply button, it will display "A Reboot is Needed to Apply System Changes" and Reboot will be displayed at the same time.

After pressing the Reboot button, the device will restart.

MEMO

Regarding to SS38 (AP Mode) WLAN Port Settings, L2 ACL

(1) **WLAN Port Settings of SS38 (AP Mode)**
It's not in "System Configuration". Please setup in the "Configuration Wizard" of "System Tool Box (refer to "**7.1.1 Setting Wizard**") !!

(2) **L2 ACL of SS38 (AP Mode)**
It's not in "System Security" menu. Please setup in the "System Security Wizard" of "System Tool Box (refer to "**7.1.1 Setting Wizard**") !!

4 System Configuration

4.1 System Configuration

4.1.1 Administration

（AP：SS38 (AP Mode)，●：support，－：none）

Item	Default value	Range	AP
Modify Password (For system management)	sipair	The maximum of 31 letters	●

4.1.2 LAN Port Settings

4.1.2.1 LAN Port Connection

（AP：SS38 (AP Mode)，●：support，－：none）

Item	Default value	Range	AP
NAT (Address modification)	Enable	Enable, Disable	－
IP Address Assignment			●
IP Address (IP address)	192.168.1.1	IP address format	●
Subnet Mask (Subnet mask)	255.255.255.0	IP address format	●

4.1.2.2 DHCP Server

（AP：SS38 (AP Mode)，●：support，－：none）

Item	Default value	Range	AP
Status (Enable DHCP server)	Enable	Enable Disable	－
Server Setting			－
Start IP Address (The head of the IP address to assign)	192.168.1.21	IP address format	－
Supported Host Number (The max number of the IP address to assign)	150	0-253 (Change according to Start IP Address)	－
Subnet Mask (Subnet mask address to assign)	255.255.255.0	IP address format	－
Default Gateway (The default gateway IP address to assign)	192.168.1.1	IP address format	－
WINS Server (The WINS server IP address to assign)	(none)	IP address format	－

4.1.2.3 DNS Proxy

（AP：SS38 (AP Mode)，●：support，－：none）

Item	Default value	Range	AP
Status (Enable DNS Proxy)	Enable	Enable, Disable	－
DNS Proxy Table	(none)	The maximum of 16 entries	－
Host Name (Local DNS host name)	(none)	The maximum of 31 letters	－
IP Address (Local DNS hot IP address)	(none)	IP address format	－

4.1.3 WAN Port Settings

4.1.3.1 WAN Port Connection

(AP:SS38 (AP Mode), ●：support, －：none)

Item	Default value	Range	AP
Connection Mode	DHCP	DHCP Manual Settings PPPoE Settings	–
WAN Access	Enable	Enable, Disable	–

(1) Manual Settings

(AP:SS38 (AP Mode), ●：support, －：none)

Item	Default value	Range	AP
IP Address	10.1.1.1	IP address format	–
Subnet Mask	255.255.0.0	IP address format	–
Default Gateway	10.1.1.254	IP address format	–
Primary DNS Server	168.95.1.1	IP address format	–
Secondary DNS Server	168.95.192.1	IP address format	–

(2) PPPoE Settings

(AP:SS38 (AP Mode), ●：support, －：none)

Item		Default value	Range	AP
User Account（PPPoE account)		(none)	The maximum of 39 letters	–
User Password（PPPoE password)		(none)	The maximum of 39 letters	–
Authentication Method		PAP	PAP, CHAP, MS-CHAP（※1）	–
Auto-connect on Demand		Disable	Enable, Disable	–
Auto-Dialing After Busy		Disable	Enable, Disable	–
	Number of Times	1	1~10 times	–
	Retry Interval	5 secs.	1~60 secs	–
Auto-disconnect Idle Time		Off (1 min.)	off, on (1~60 mins.)	–

(*1) MS-CHAP is an authentication which extends CHAP of PPP by Microsoft RAS.

4.1.3.2 Routing

(AP:SS38(AP Mode), ●: support, ー: none)

Item	Default value	Range	AP
Status (Enable static routing)	Disable	Disable, Static Routing (Enable)	–
Routing Table (Static routing table)	(none)	The maximum of 16 entries	–
Network Destination	(none)	IP address format	–
NetMask	(none)	IP address format	–
NextHop	(none)	IP address format	–

4.1.4 WLAN Port Settings

4.1.4.1 WLAN Port Radio Settings

(AP:SS38(AP Mode), ●: support, ー: none)

Item	Default value	Range	AP
Wireless Mode	11B only (11M)	11G only (54M) 11G only (54M)/11B(11M)-Mix 11B only (11M)	●
SSID	sipair	The maximum of 32 letters	●
Modification of WIFI	Enable	Enable, Disable	–
Limitation of one AP Access	10	0:Disable 1-10: The number of current accesses	●
Hide Beacon SSID & Block Unspecified SSID	Disable	Enable, Disable	●
Channel	1	1-14	●
Burst Mode	on (3000)	off, on (1-3000)	●
RTS Threshold	off (2300)	off, on (1-2347)	●
RTS Retries	5	1-255	●
Fragmentation Threshold	off	off, on	●
	(2000)	(256-2346)	●
Beacon Period	100 ms	20-1000 ms	●

Wireless Mode

Caution

Please do not use this device in "11G only" mode, when there have 802.11b WLAN client.

4.1.4.2 WLAN Advance Security

（AP：SIP:Air@AP, ●：support, －：none）

Item	Default value	Range	AP
Security Mechanism	Disable	Disable WEP WEP/802.1x WPA/802.1x WPA/PSK	●

(1) WEP

（AP：SIP:Air@AP, ●：support, －：none）

Item	Default value	Range	AP
WEP Key Input Mode	Hex	Hex, ASCII	●
Key Length	64-bits	64-bits, 128-bits	●
WEP Key Selection	KEY1	KEY1,KEY2, KEY3, KEY4	●
WEP Keys	(none)	13 letters in ASCII, 26 letters in Hex (*1)	●

(*1) WEP Keys information can set up a maximum of 4 entries.

(2) WEP/802.1x

（AP：SIP:Air@AP, ●：support, －：none）

Item	Default value	Range	AP
Use of Local Server	No	No, Yes	●
Local Server Table	(none)	The maximum of 128 entries	●
Account (Local CHAP username)	(none)	The maximum of 31 letters	●
Password (Local CHAP username)	(none)	The maximum of 31 letters	●
Authentication Server Address (IP address of RADIUS server)	(none)	IP address format	●
Authentication Server Port (The number of RADIUS server)	1812	1~65535	●
Authentication Key (Key shared with RADIUS server)	(none)	The maximum of 16 letters	●
NAS ID	(none)	The maximum of 16 letters	●
Re-Auth Interval	3600 secs.	60~99999 secs.	●
WEP Key Input Mode	Hex	Hex, ASCII	●
Key Length	64-bits	64-bits, 128-bits	●
WEP Key Selection	KEY1	KEY1,KEY2, KEY3, KEY4	●
WEP Keys	(none)	13 letters in ASCII, 26 letters in Hex (*1)	●

(*1) WEP Keys information can set up a maximum of 4 entries.

(3) WPA/802.1x

(AP:SS38(AP Mode), ●：support, ー：none）

Item	Default value	Range	AP
Authentication Server Address (IP address of RADIUS server)	(none)	IP address format	●
Authentication Server Port (The number of RADIUS server)	1812	1~65535	●
Authentication Key (Key shared with RADIUS server)	(none)	The maximum of 16 letters	●
NAS ID (NAS ID)	(none)	The maximum of 16 letters	●
Re-Auth Interval	3600 secs.	60~99999 secs.	●
Group Key Renewal Interval (Updating interval of Group Key)	3600 secs.	60~99999 secs.	●

(4) WPA/PSK

(AP:SS38(AP Mode), ●：support, ー：none）

Item	Default value	Range	AP
Pre-Shared Key Input Mode (WPA/PSK key type)	Hex	Hex, ASCII	●
Pre-Shared Key	(none)	8~63 letters in ASCII, 64 letters in Hex	●
Group Key Renewal Interval	3600 secs.	60~99999 secs.	●

4.2 System Security

4.2.1 Access Control

4.2.1.1 Firewall

(AP:SS38(AP Mode), ●：support, －：none）

Item	Default value	Range	AP
Firewall Enable (L2 ACL(※1), enable Packet Filtering)	Disable	Enable, Disable	－

(※1) There is no Firewall Enable setting in SS38(AP Mode)
IF you want to use L2 ACL function, please start "System Security Wizard "(refer to 7.1.1 Setting Wizard) to enable "L2 ACL Status".

4.2.1.2 L2 ACL

(AP:SS38(AP Mode), ●：support, －：none）

Item	Default value	Range	AP
Status (Enable ACL function)	Disable	Enable, Disable	●
Table Policy (Table policy)	Deny	Grant, Deny	●
L2 ACL Table	(none)	The maximum of 256 entries	●
MAC Address(MAC address for L2 ACL)	(none)	MAC address format	●

4.2.1.3 Packet Filtering (inbound)

(AP:SS38(AP Mode), ●：support, －：none）

Item	Default value	Range	AP
Status (Enable Inbound Filter)	Disable	Enable, Disable	－
Table Policy (Inbound table policy)	Grant	Grant, Deny	－
Packet Filtering Inbound Table (Inbound table list)	(none)	The maximun of 64 entries	－
Source IP From (The head of the source IP address of the policy)	(none)	IP address format	－
Source IP To (The last of the source IP address of the policy)	(none)	IP address format	－
Source Port From (The head of the source port number of the policy)	(none)	0~65535	－
Source Port To (The last of the source port number of the policy)	(none)	0~65535	－
Destination IP From (The head of the IP address of the policy)	(none)	IP address format	－
Destination IP To (The last of the IP address of the policy)	(none)	IP address format	－
Destination Port From (The head of the address port number of the policy)	(none)	0~65535	－
Destination Port To (The last of the address port number of the policy)	(none)	0~65535	－
Protocol Type (The protocol type of the policy)	(none) (*1)	TCP, UDP, ICMP	－

(*1)TCP is set up automatically at the time of new entry generated.

4.2.1.4 Packet Filtering (Outbound)

(AP:SS38(AP Mode)，●：support，－：none）

Item	Default value	Range	AP
Status (Enable Inbound Filter)	Disable	Enable, Disable	–
Table Policy (Inbound table policy)	Grant	Grant, Deny	–
Packet Filtering Outbound Table (Inbound table list)	(none)	The maximun of 64 entries	–
Source IP From (The head of the source IP address of the policy)	(none)	IP address format	–
Source IP To (The last of the source IP address of the policy)	(none)	IP address format	–
Source Port From (The head of the source port number of the policy)	(none)	0~65535	–
Source Port To (The last of the source port number of the policy)	(none)	0~65535	–
Destination IP From (The head of the IP address of the policy)	(none)	IP address format	–
Destination IP To (The last of the IP address of the policy)	(none)	IP address format	–
Destination Port From (The head of the address port number of the policy)	(none)	0~65535	–
Destination Port To (The last of the address port number of the policy)	(none)	0~65535	–
Protocol Type (The protocol type of the policy)	(none) (*1)	TCP, UDP, ICMP	–

(*1) TCP is set up automatically at the time of new entry generated.

4.3 SIP Configuration

4.3.1 SIP Configuration

(AP:SS38(AP Mode), ●：support, ー：none）

Item	Default value	Range	AP
SIP Proxy Type (SIP Server mode)	Proxy	Proxy	－
SIP Authentication (Authentication mode fo SIP Proxy)	Disable	Enable, Disable	－
Loop Detection (Loop detection of SIP Proxy)	Enable	Enable, Disable	－
Log function (SIP log extraction of SIP Proxy)	Disable	Enable, Disable	－
Transport Type (Transmission type of SIP message of SIP Proxy)	UDP	TCP, UDP	－
Max Calls (Current calls)	20	1~20	－
Request Timeout (Registration effective time of SIP Proxy)	3600 secs.	3600~999999 secs.	－
Outbound Proxy Domain	(none)	The maximum of 50 letters	－
Outbound Proxy Setting	0.0.0.0	IP address format	－
Authentication Timeout (Authentication timeout time of SIP Proxy)	180000ms	180000~99999999ms	－
Call Timeout (Call timeout time at the time of oral transmission)	150 secs.	15~150secs.	－

4.3.2 SIP Group

(AP:SS38(AP Mode), ●：support, ー：none）

Item	Default value	Range	AP
SIP group management (SIP Group information)	administrator	Can't change	－
Call Pickup	(none)	The maximum of 10 entries	－
Call Pickup Number	(none)	The maximum of 15 letters	－
User1~User5 (Extension numbers of the group)	(none)	The maximum of 5 numbers	－

4.3.3 SIP User

SIP User information can be set up a maximum of 100 entries.

(AP:SS38(AP Mode), ●：support, －：none)

Item	Default value	Range	AP
User Name (Internal) (SIP username)	(none)	The maximum of 15 letters	－
User Name (Global) (SIP global username)	(none)	The maximum of 15 letters	－
Domain Name (SIP user domain name)	(none)	Select from 4.3.4.2 Registrar Domain	－
Group Name (SIP user group name)	administrator	administrator	－
Password (SIP user password)	(none)	The maximum of 15 letters	－
Busy Forward (SIP user busy transfer URL)	(none)	The maximum of 15 letters before @ The maximum of 31 letters after @	－
Unavailable Forward (SIP user unavailable transfer URL)	(none)	The maximum of 15 letters before @ The maximum of 31 letters after @	－
Unconditional Forward (SIP user unconditional transfer URL)	(none)	The maximum of 15 letters before @ The maximum of 31 letters after @	－
No Answer Forward (SIP user no answer transfer URL)	(none)	The maximum of 15 letters before @ The maximum of 31 letters after @	－
No Answer Timeout	(none)	1~999 secs.	－

Caution

"**Domain Name**" and "**@xxx**" of each transfer URL, the IP address specified by "**Registrar Domain Table**" is set up automatically.

4.3.4 SIP Domain

4.3.4.1 Domain forwarding

This device doesn't support this item. Please do not use it.

(AP:SS38(AP Mode) , ●：support, －：none）

Item	Default value	Range	AP
SIP Domain (Transfer SIP Domain)			
Default Proxy IP Address (Transfer IP address)			

4.3.4.2 Registrar Domain

Caution

Please input the "LAN IP Address" value of SS38(Server Mode) into Registrar Domain Table.
(Although a maximum of 3 entries input is possible, please note that the first entry is effective.)

(AP:SS38(AP Mode), ●：support, －：none）

Item	Default value	Range	AP
Registrar Responsible Domain (Registrar domain)	(none)	A maximum of 31 letters (Specifies by the IP address)	－

4.3.5 SIP Gateway

(AP:SS38(AP Mode), ●：support, －：none）

Item	Default value	Range	AP
SIP Gateway Group	(none)	A maximum of 2 groups	－
Gateway Name (The name of VoIP gateway)	(none)	A maximum of 8 letters A maximum of 4 entries	－
SIP Gateway IP (The IP address of VoIP gateway)	0.0.0.0	IP address format A maximum of 4 entries	－
Dial plan management	(none)	A maximum of 20 entries	－
Route Pattern (The dial number transmitted to SIP Gateway)	(none)	A maximum of 15 letters	－

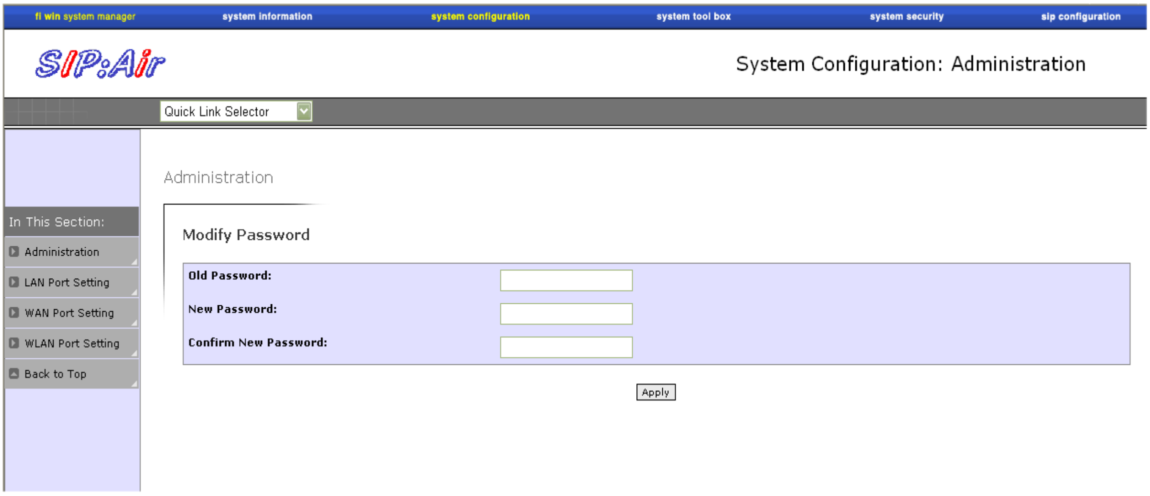
5 Setup the device

5.1 System Configuration

Please click "**system configuration**" of the screen above. (The "**system configuration**" will reverse to yellow display after selection.)

It displays on the screen as below:

Please click
system configuration



Administration

Modify Password

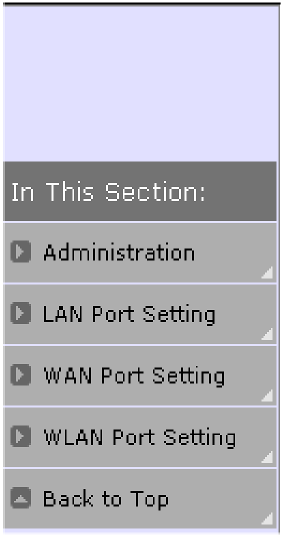
Old Password:

New Password:

Confirm New Password:

Then, please choose the menu arbitrarily displayed on "**In This Selection**".

Regarding to the functions of each menu, please refer to below.



5.1.1 Administration

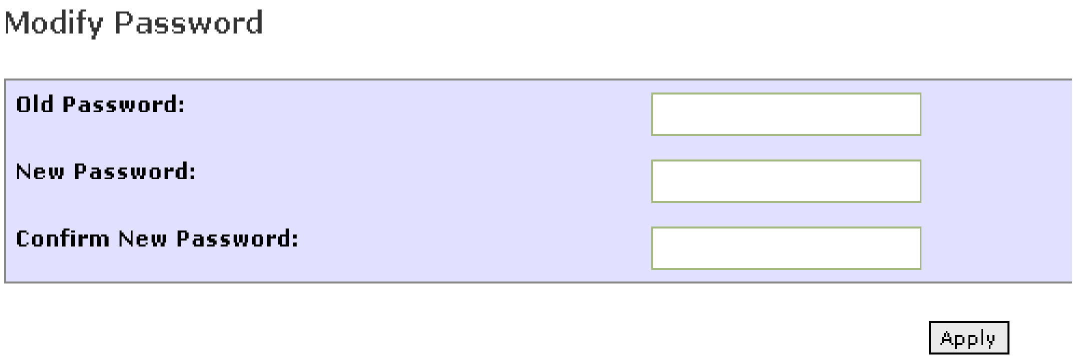
5.1.2 LAN Port Setting

5.1.3 WAN Port Setting

5.1.4 WLAN Port Setting

5.1.1 Administration

Please click "**Administration**" in the menu displayed on left side of the screen of "**5.1 System Configuration**".



Modify Password

Old Password:	
New Password:	
Confirm New Password:	

Modify Password

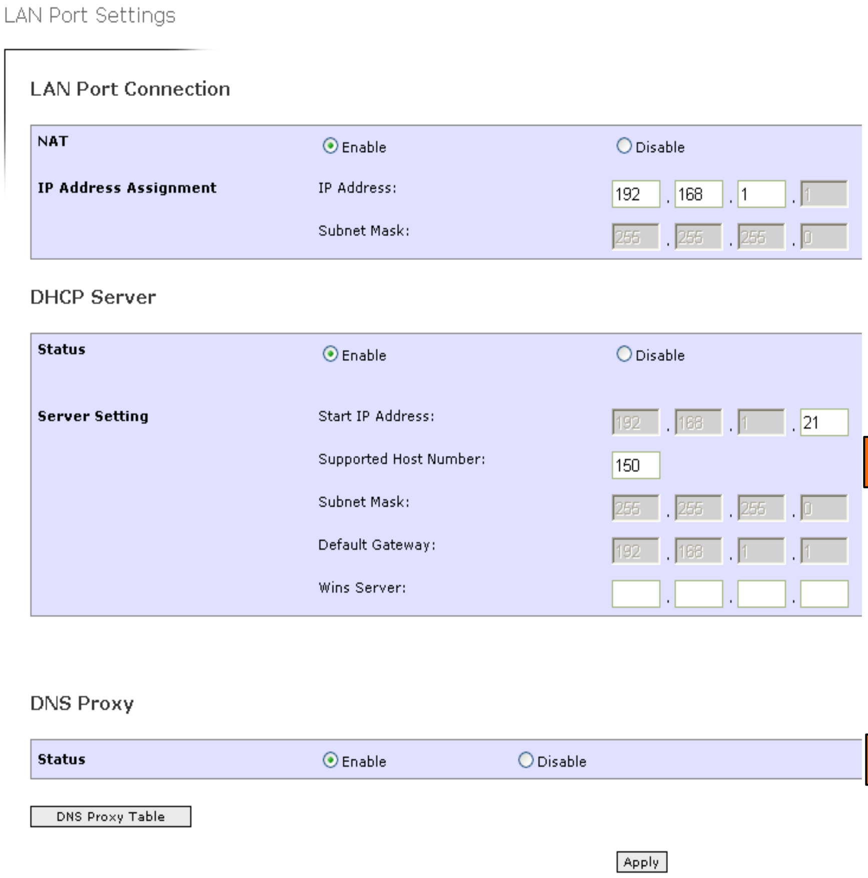
Enter the old password and the new password, and click the "**Apply**" button to modify the password.

Caution

If the password is changed, please note that a password window will be displayed and needs to re-login.

5.1.2 LAN Port Settings

Please click "**LAN Port Settings**" in the menu displayed on left side of the screen of "**5.1 System Configuration**".



LAN Port Settings

LAN Port Connection

NAT	● Enable	○ Disable
IP Address Assignment	IP Address:	192 . 168 . 1 . 1
	Subnet Mask:	255 . 255 . 255 . 0

DHCP Server

Status	● Enable	○ Disable
Server Setting	Start IP Address:	192 . 168 . 1 . 21
	Supported Host Number:	150
	Subnet Mask:	255 . 255 . 255 . 0
	Default Gateway:	192 . 168 . 1 . 1
	Wins Server:	. . .

DNS Proxy

Status	● Enable	○ Disable

DNS Proxy Table

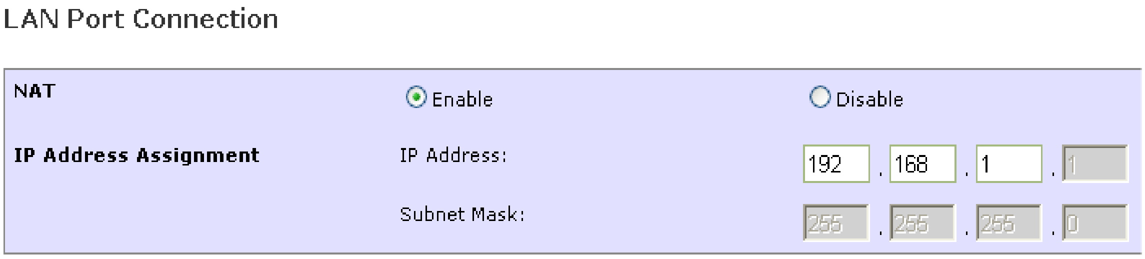
Apply

To 5.1.2.1

To 5.1.2.2

To 5.1.2.3

5.1.2.1 LAN Port Connection



LAN Port Connection

NAT	● Enable	○ Disable
IP Address Assignment	IP Address:	192 . 168 . 1 . 1
	Subnet Mask:	255 . 255 . 255 . 0

~~AP~~

NAT

Please enable / disable NAT function. The default value is Enable.

Enable : Global IP address can be shared by multiple users.
The address is convertible in the range of Class C.

Disable: Please set the IP address and subnet mask in the LAN port of this device.

IP Address Assignment

IP address: The IP address of the LAN port of this device

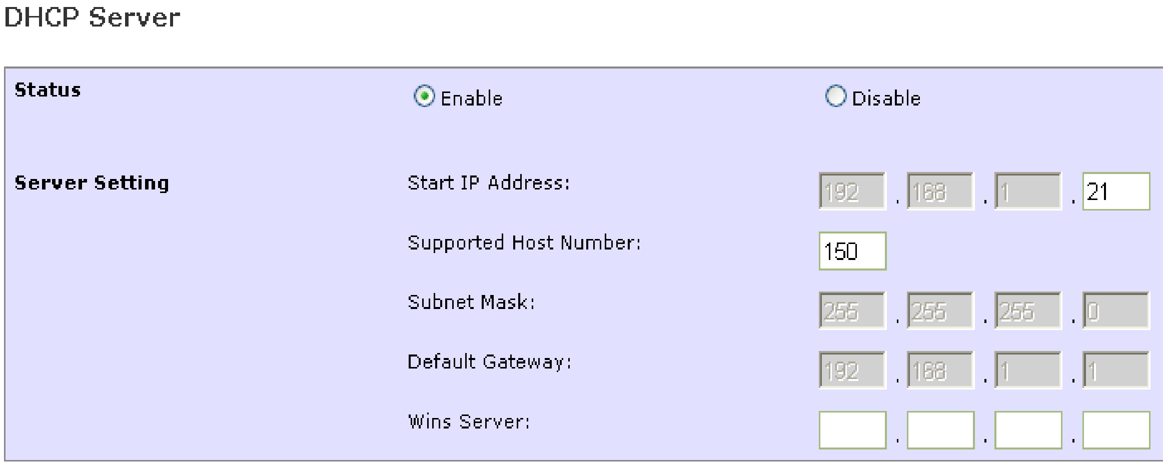
NAT: It's convertible when Disable

Subnet mask: The subnet mask of the LAN port

NAT: It's convertible when Disable

5.1.2.2 DHCP Server

~~AP~~



DHCP Server

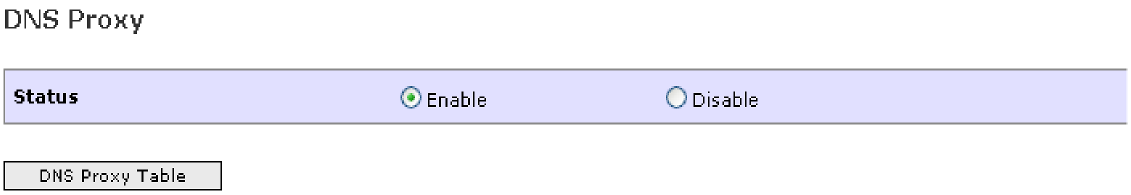
Status	● Enable	○ Disable
Server Setting	Start IP Address:	192 . 168 . 1 . 21
	Supported Host Number:	150
	Subnet Mask:	255 . 255 . 255 . 0
	Default Gateway:	192 . 168 . 1 . 1
	Wins Server:	. . .

Status

Please enable / disable DHCP server function. The default value is Enable.
DHCP server will assign a IP address automatically to the device connected to LAN/WLAN.
Please check if the device is a DHCP client (can be setup in "**IP Address Assignment** " of the TCP/IP setting).

5.1.2.3 DNS Proxy

~~UAP~~



DNS Proxy

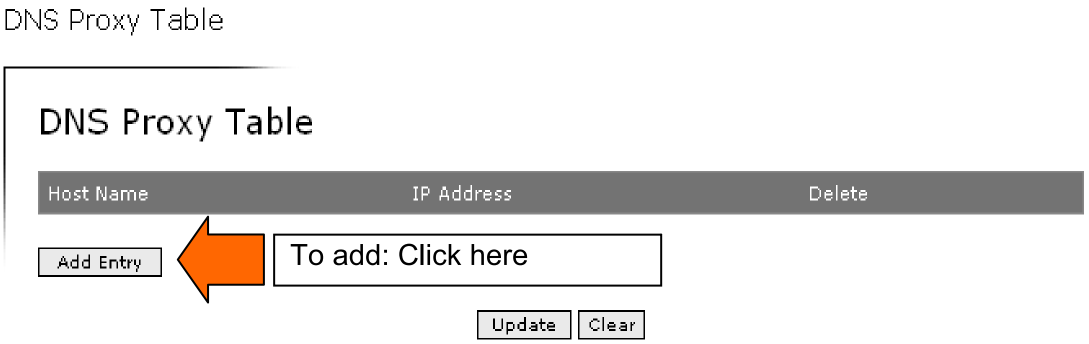
Status	● Enable	○ Disable

DNS Proxy

Enable / Disable the DNS Proxy.

If click the **DNS Proxy Table** button, a pop-up window will be display and you can edit the **DNS Proxy table**.

If the DNS Proxy is effective, a domain / website name will be reversed to an IP address / URL from the DNS Proxy table.



DNS Proxy Table

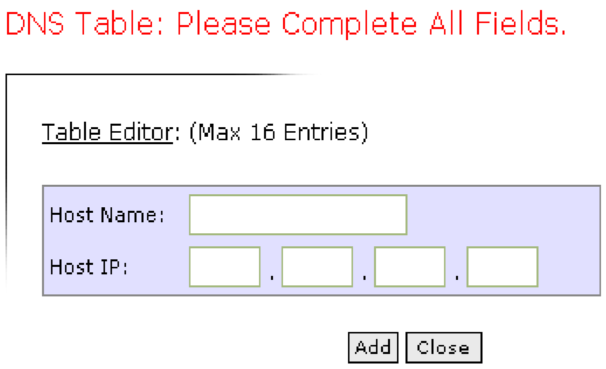
DNS Proxy Table

Host Name	IP Address	Delete

To add: Click here

DNS Proxy Table (Before the edition)

Add Entry If click the button, **Table Editor** window will pop up and you can login the DNS Proxy.



DNS Table: Please Complete All Fields.

Table Editor: (Max 16 Entries)

Host Name:	
Host IP:	. . .

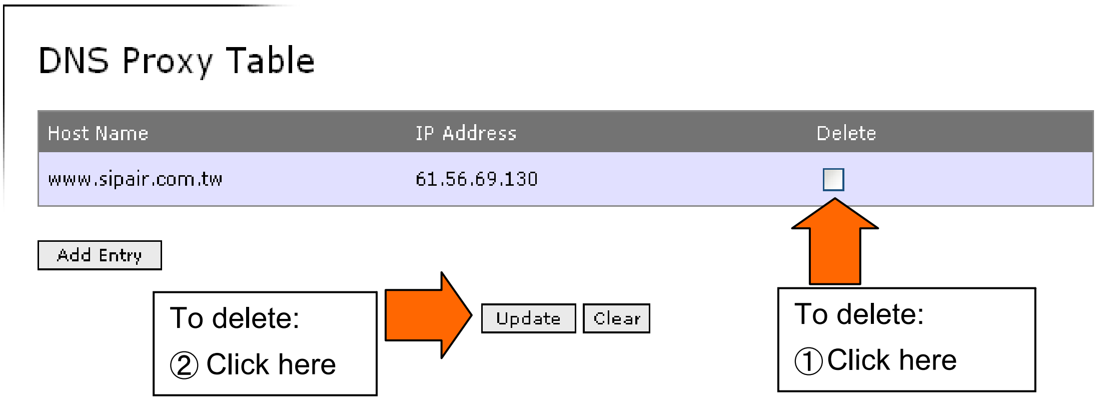
Table Editor

Enter the new DNS Proxy.

Please press the "**Add**" button when entering the IP address. The new data will be displayed on the **DNS Proxy Table**.

The maximun of entries are 16 letters.

DNS Proxy Table



DNS Proxy Table

Host Name	IP Address	Delete
www.sipair.com.tw	61.56.69.130	□

To delete:
② Click here

To delete:
①Click here

DNS Proxy Table (After the edition)

After the edition, the new data will be displayed as above.

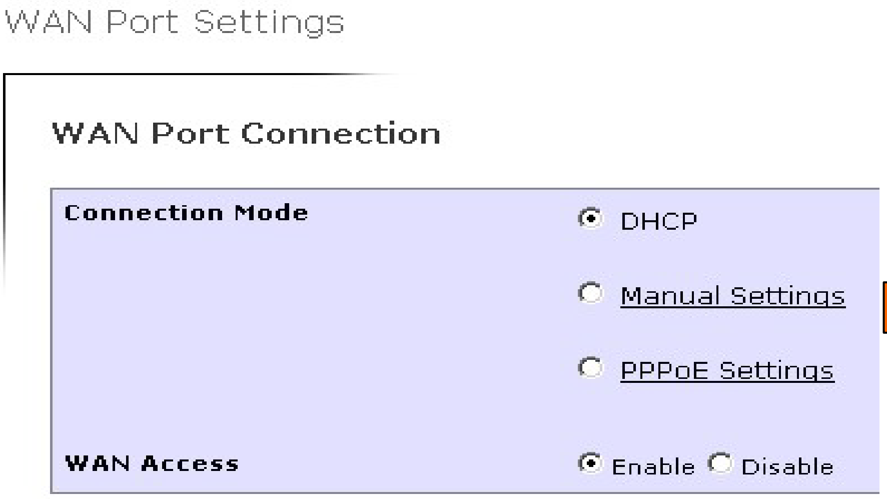
If you want to delete the entry, please select the "**Delete**" button and press the "**Update**" button.

If click the "**Clear**" button, it will clear the "**Delete**" box.

5.1.3 WAN Port Settings

~~AP~~

Please click "**WAN Port Settings**" in the menu displayed on left side of the screen of "**5.1 System Configuration**". It will display as below.



WAN Port Settings

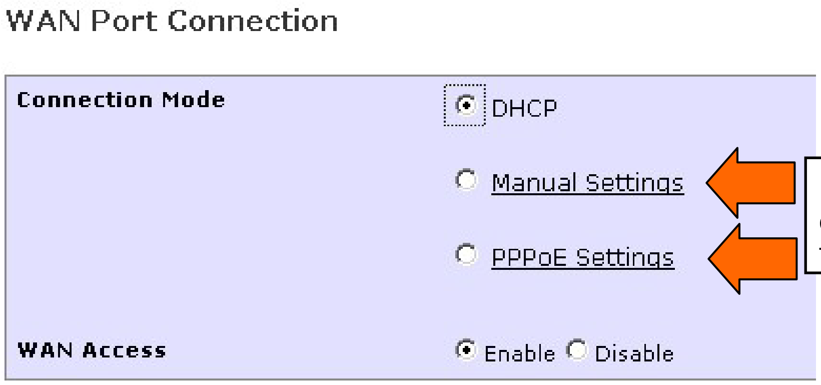
WAN Port Connection

Connection Mode	● DHCP ○ Manual Settings ○ PPPoE Settings
WAN Access	● Enable ○ Disable

To 5.1.3.1

To 5.1.3.2

5.1.3.1 WAN Port Connection



WAN Port Connection

Connection Mode	● DHCP ○ Manual Settings ○ PPPoE Settings
WAN Access	● Enable ○ Disable

If you want to change the configuration, please click the hyperlink.

Connection Mode

You can select 3 connection Modes from the options as below.

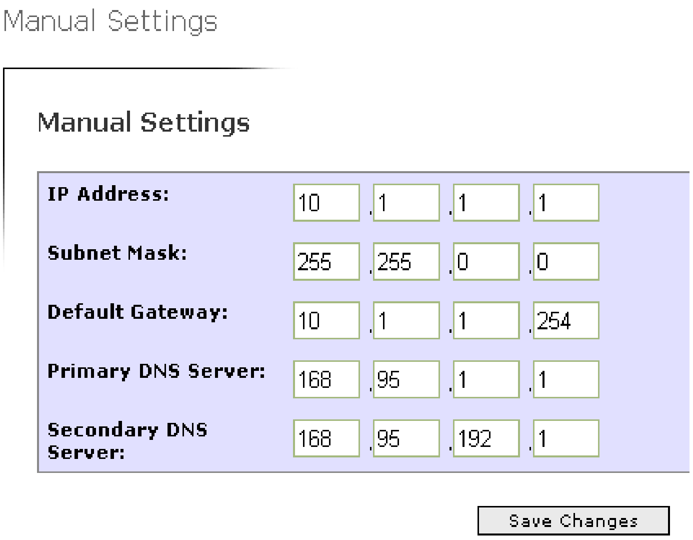
· DHCP	(DHCP client)
· Manual Settings	(Manual connection settings)
· PPPoE Settings	(PPPoE connection)

The initial status of connection mode is DHCP client.

In Manual Settings or PPPoE Settings, if you click the hyperlink, a window will pop up and the setting will be changed.

WAN Access

The connection to the WAN port from LAN or WLAN can be set as Enable/Disable.



Manual Settings

Manual Settings

IP Address:	10	1	1	1
Subnet Mask:	255	255	0	0
Default Gateway:	10	1	1	254
Primary DNS Server:	168	95	1	1
Secondary DNS Server:	168	95	192	1

If selecting "Manual Settings", the pop up window will display as above and you can select the configurations as below.

IP address

To setup the IP address of WAN port.

Subnet Mask

To setup the subnet mask of the network for connecting to WAN port.

Default Gateway

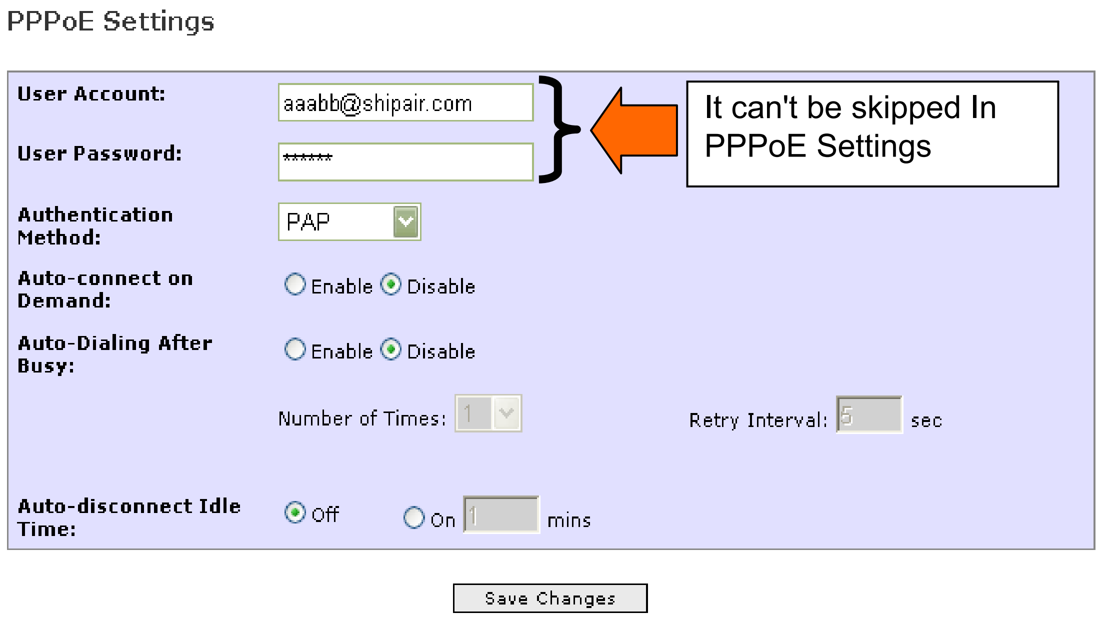
To setup the default gateway IP address.

Primary DNS Server

To setup the primary DNS server IP address.

Secondary DNS Server

To setup the secondary DNS server IP address.



PPPoE Settings

User Account: aaabb@shipair.com

User Password: ******

It can't be skipped In PPPoE Settings

Authentication Method: PAP

Auto-connect on Demand: ○ Enable ● Disable

Auto-Dialing After Busy: ○ Enable ● Disable

Number of Times: 1 Retry Interval: 5 sec

Auto-disconnect Idle Time: ● Off ○ On 1 mins

If selecting the "PPPoE Settings", the screen will be displayed as above and you can select the configurations as below.

User Account

To setup the client for connecting to PPPoE.

User Password

To setup the password for connecting to PPPoE.

Authentication Method

To setup the authentication method to connect to PPPoE.
To select from PAP, CHAP or MS-CHAP.

Auto-connect on Demand

To setup the function of Auto-Dialing on demand Enable/Disable.
If enable the function, PPPoE will be connected automatically.

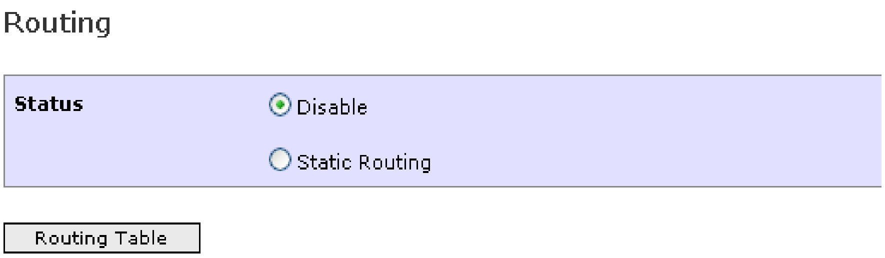
Auto-Dialing After busy

To setup auto-dialing function Enable/Disable during talking.
The user can setup the re-dialing times for 1~10, and can set up a re-dialing interval in the range for 1~60 seconds.

Auto-disconnect Idle Time

To setup auto-disconnect OFF / ON when the call is disconnected.
If On, it can setup the Idle time until the call is disconnected automatically.

5.1.3.2 Routing



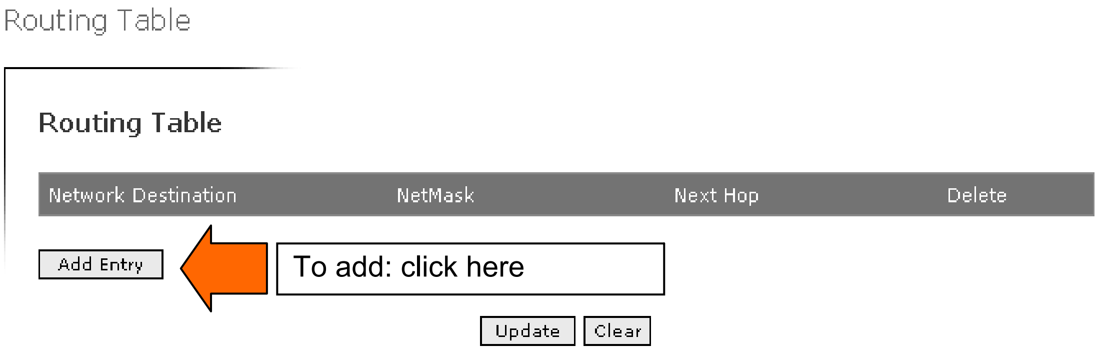
Routing

Status	● Disable ○ Static Routing

Status

If selecting **Disable**, WAN interface will be used as a default route.

If using **Static routing**, please select "**Static routing**" and click "**Routing Table**" button for editing Routing table.



Routing Table

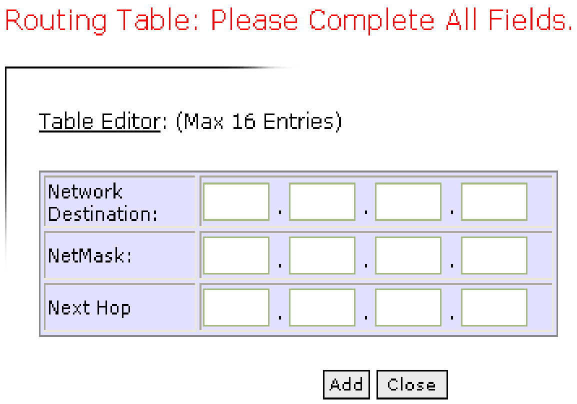
Routing Table

Network Destination	NetMask	Next Hop	Delete

Routing Table (Before the edition)

It displays the current Routing Table.

When adding the entry, if click the "**Add Entry**" button, the "**Table Editor**" window will pop up.



Routing Table: Please Complete All Fields.

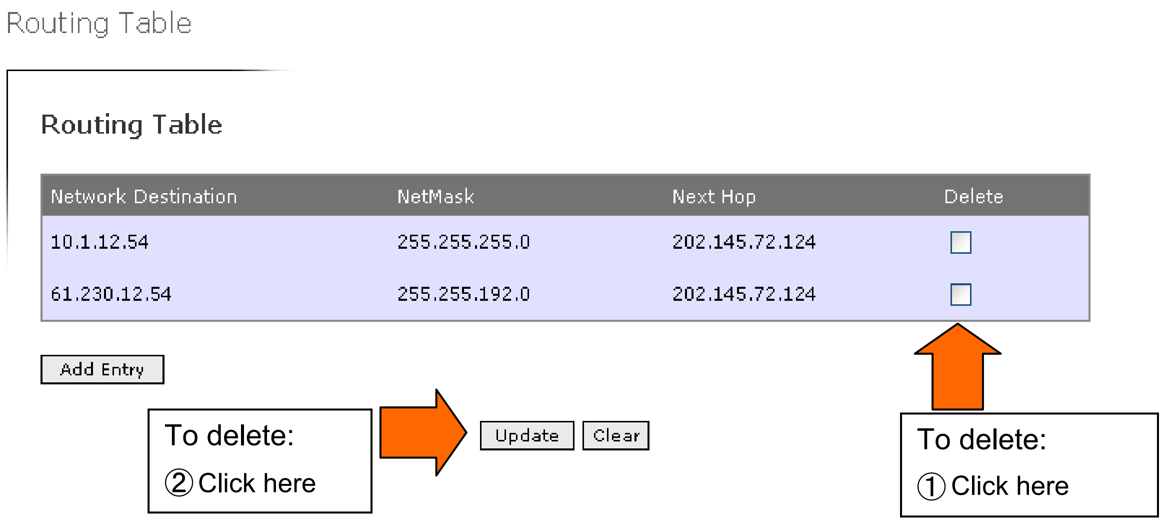
Table Editor: (Max 16 Entries)

Network Destination:	. . .
NetMask:	. . .
Next Hop	. . .

Table Editor

The entry can be added to static routing table from this window.

Enter the *Network Destination, NetMask,* and *Next Hop* information. (Max 16 entries)



Routing Table

Routing Table

Network Destination	NetMask	Next Hop	Delete
10.1.12.54	255.255.255.0	202.145.72.124	□
61.230.12.54	255.255.192.0	202.145.72.124	□

To delete:
② Click here

To delete:
① Click here

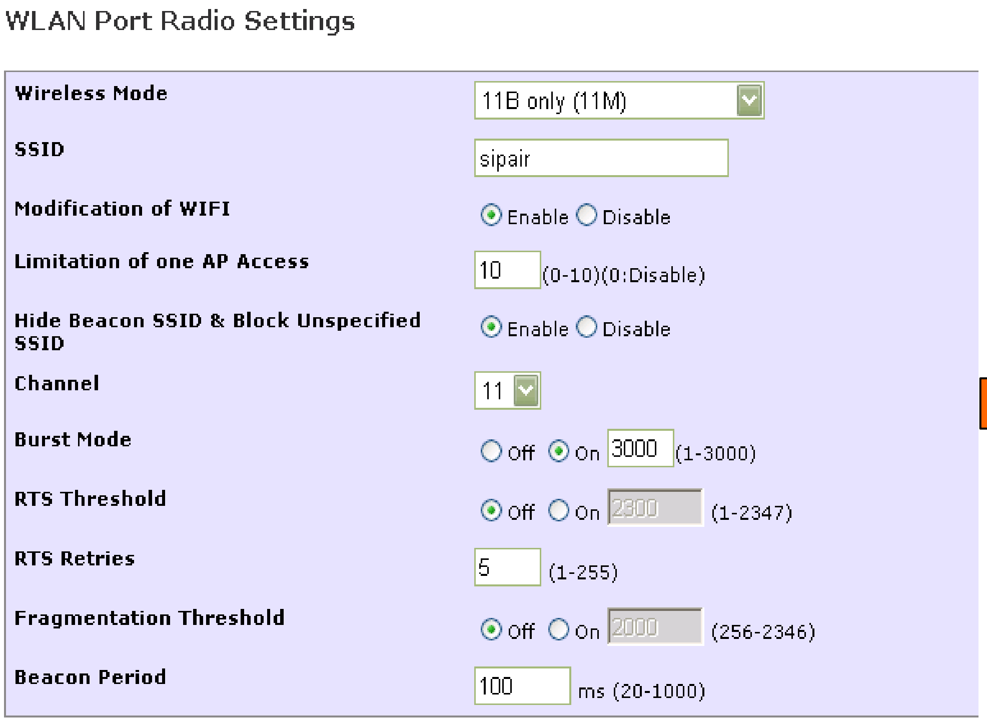
Routing Table (After the edition)

After the edition, the new data will display as above.

If you want to delete the entry, please check the "**Delete**" box in advance and click the "**Update**" button. If clicking "**Clear**", it might clear the "**Delete**" box.

5.1.4 WLAN Port Settings

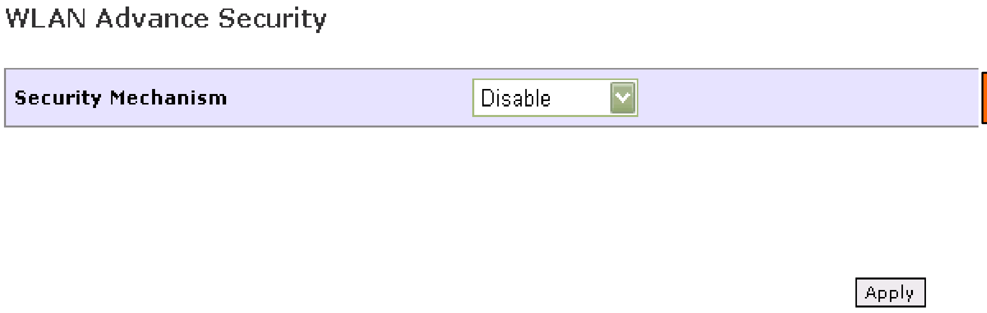
Please click "**WLAN Port Settings**" in the menu displayed on left side of the screen of "**5.1 System Configuration**". It will display as below.



WLAN Port Radio Settings

Wireless Mode	11B only (11M)
SSID	sipair
Modification of WIFI	● Enable ○ Disable
Limitation of one AP Access	10 (0-10)(0:Disable)
Hide Beacon SSID & Block Unspecified SSID	● Enable ○ Disable
Channel	11
Burst Mode	○ Off ● On 3000 (1-3000)
RTS Threshold	● Off ○ On 2300 (1-2347)
RTS Retries	5 (1-255)
Fragmentation Threshold	● Off ○ On 2000 (256-2346)
Beacon Period	100 ms (20-1000)

To 5.1.4.1



WLAN Advance Security

Security Mechanism	Disable

To 5.1.4.2

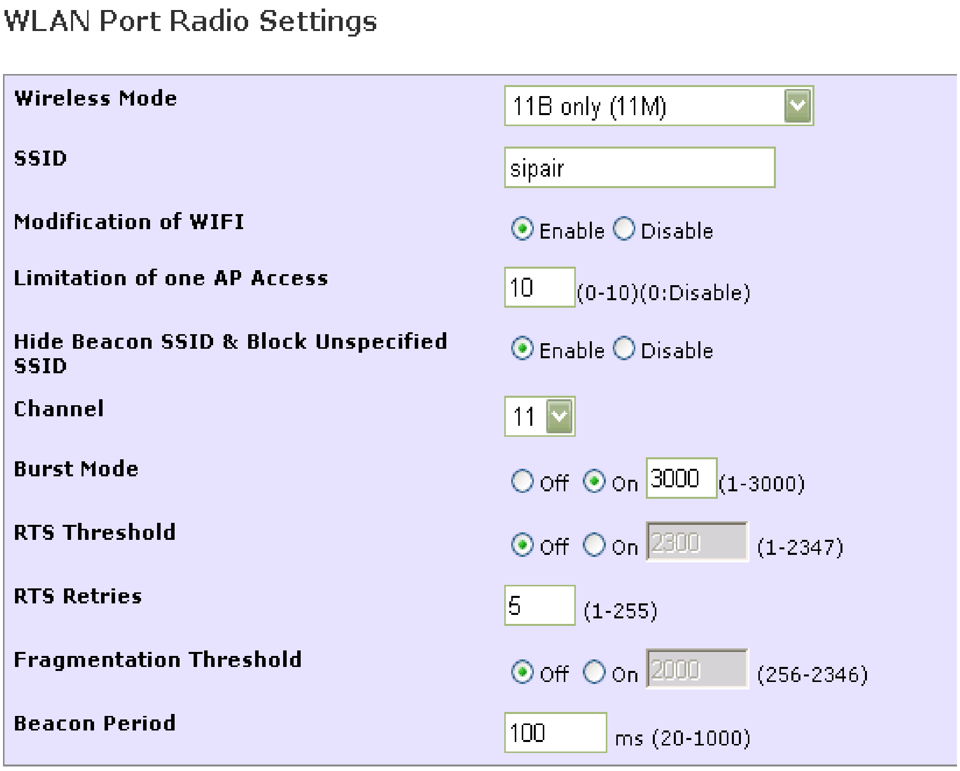
MEMO

Regarding to the WLAN Port Settings of SS38 AP Mode

"**System Configuration**" is not in the menu. Please refer to "**Configuration Wizard**" of the "**Configuration Wizard"** menu.

(Refer to **"7.1.1 Setting Wizard**")

5.1.4.1 WLAN Port Radio Setting



WLAN Port Radio Settings

Wireless Mode	11B only (11M)
SSID	sipair
Modification of WIFI	● Enable ○ Disable
Limitation of one AP Access	10 (0-10)(0:Disable)
Hide Beacon SSID & Block Unspecified SSID	● Enable ○ Disable
Channel	11
Burst Mode	○ Off ● On 3000 (1-3000)
RTS Threshold	● Off ○ On 2300 (1-2347)
RTS Retries	5 (1-255)
Fragmentation Threshold	● Off ○ On 2000 (256-2346)
Beacon Period	100 ms (20-1000)

SSID

SSID (Service Set Identifier) can enter up to 32 letters.
Please setup the same SSID as the wireless device connecting to this device.
The initial value of SSID is sipair.

Modification of WIFI ~~AP~~

Enable: enabling the WLAN access point function of Server Mode
Disable: disabling the WLAN access point function of Server Mode
When only using Server Mode of the SIP server, please setup "Disable" and suspend the WLAN access point function.

Limitation of one AP Access

The number of concurrent accesses to the WLAN access point can be restricted.
Default = 10 will be the maximum for 11 Mbit/s communication environment. When customer's speed can't reach 11 Mbit/s (in a blind spot and wants to use the phone in 30m radius), please restrict the number of connection for better communication quality.

Hide Beacon SSID & Block Unspecified SSID

Setup the SSID stealth function and ANY connection refusal as Enable/Disable.
The initial value of SSID is Disable.
If it's setup as Enable, this device will stop the beacon of broadcasting assignment, and block the wireless device without SSID to connect to this device.(ex: Block "any" connection)

Channel

The default value is channel "1".

Caution

The range on the adjacent access point and the parameters set by the network operator will greatly affect the talk and standby times of the phone, as well as the range and quality of the phone call. Please set adjacent access point at least for 5 channels apart.

Burst Mode

Setup Burst Mode as Off/On.

Please specify a Setup Burst when the Setup Burst is On.

The default value of Burst Mode "**On**" is "3000".

RTS Threshold

Setup RTS (Request To Send parameter) as Off/On.

Please specify a parameter if the RTS is On.

The default value of "RTS parameter" is Off.

RTS Retries

Specify the frequency of RTS retries of connection.

Fragmentation Threshold

Setup Fragmentation parameter as Off/On.

Please specify a parameter if the Fragmentation parameter is On. The default value is Off.

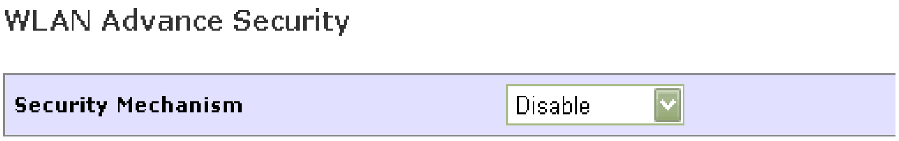
Beacon Period

Setup the interval of the beacon signal. The default value is a 100ms.

5.1.4.2 WLAN Advance Security

This device can support up to 5 WLAN securities as (1)~(5).
This chart will explain the detailed configuration of each security.

(1) Disable

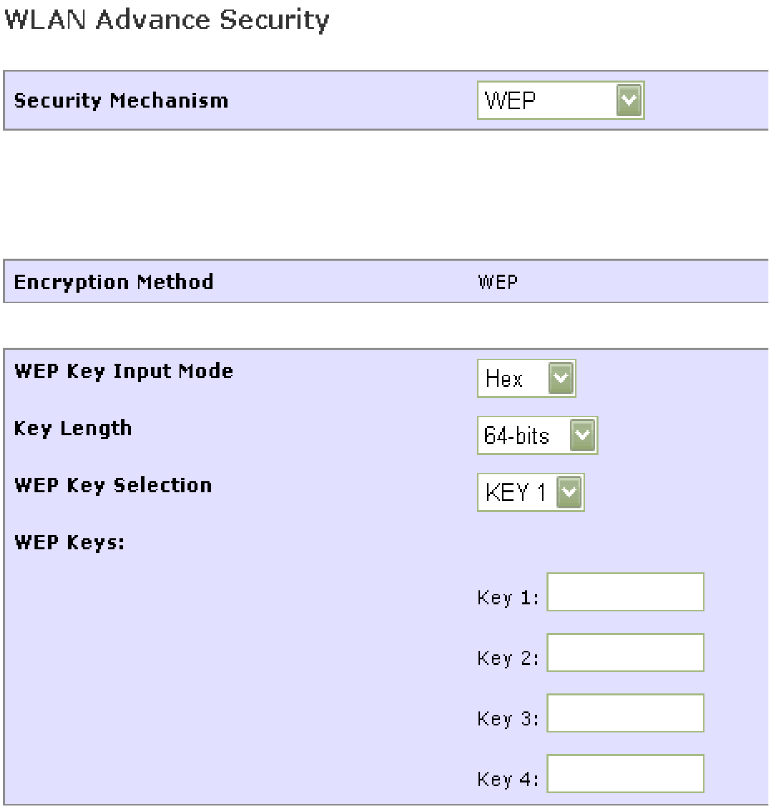


WLAN Advance Security

Security Mechanism	Disable

Security Mechanism:
The default value of security is Disable. Authentication or codec is invalid.

(2) WEP



WLAN Advance Security

Security Mechanism	WEP

Encryption Method	WEP

WEP Key Input Mode	Hex
Key Length	64-bits
WEP Key Selection	KEY 1
WEP Keys:	
	Key 1:
	Key 2:
	Key 3:
	Key 4:

Security Mechanism
Setup WEP (Wired Equivalent Privacy) as effective.
Setup the key info for coding.
This device supports 2 coding methods. Defines as IEEE 802.11, it can setup 64 bit WEP Key or extended 128 bits Key.

Encryption Method
Display the current selected data coding method.

WEP key Input Mode

Select ASCII (alphanumeric letter) or Hex (hexadecimal number) as a Key input mode.

Key Length

Select 64 bits or 128 bit coding method.

WEP Key Selection

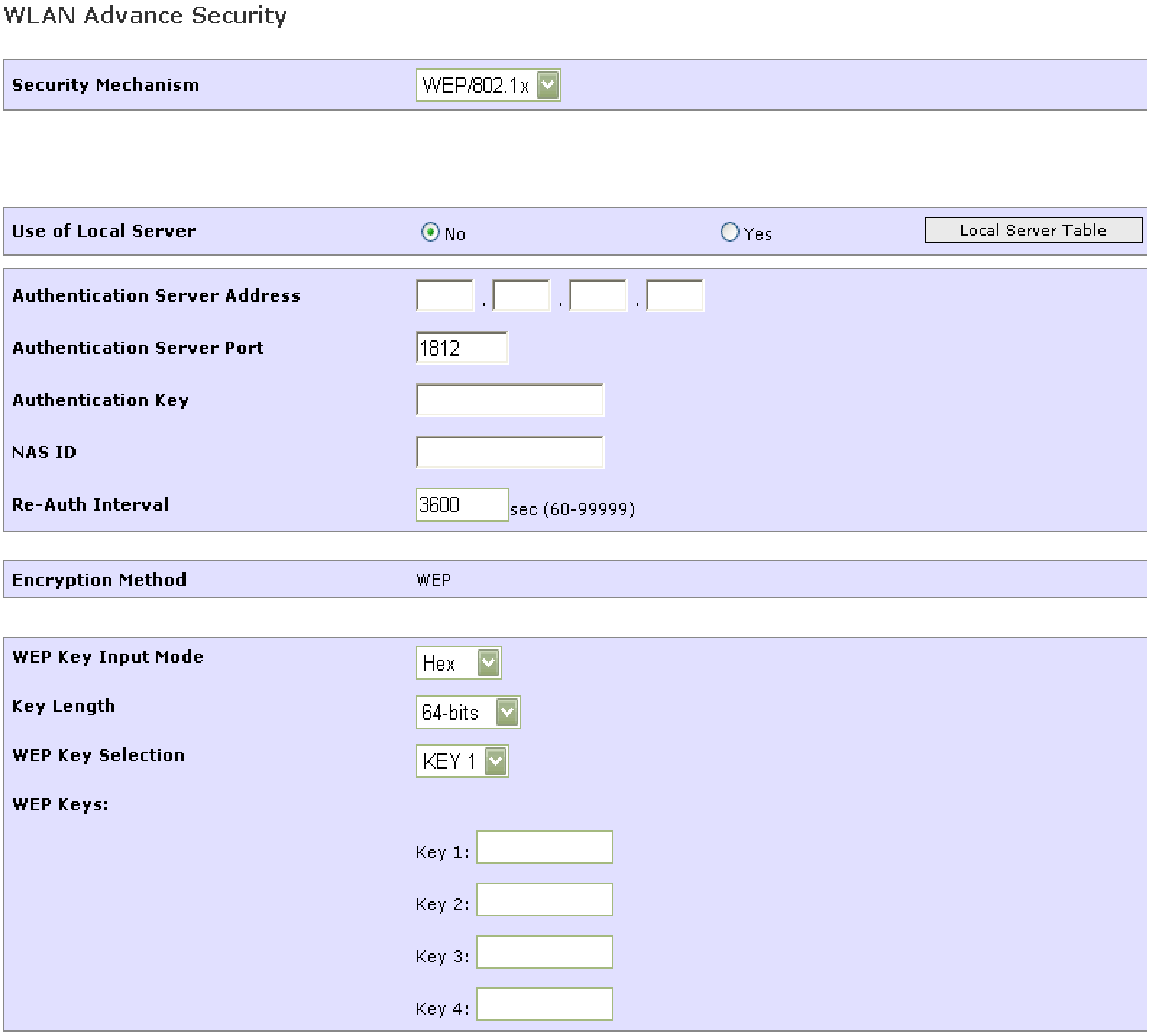
Select one from the maximum of 4 coded keys.

WEP Key

You can enter up to 4 keys.

When the **Key Length** is 64 bits, ASCII can inputs ５ letters and Hex inputs 10 digits.
If 128 bits, ASCII can inputs 13 letters, and Hex inputs 26 digits.

(3) WEP/802.1x



WLAN Advance Security

Security Mechanism	WEP/802.1x		
Use of Local Server	● No	○ Yes	Local Server Table
Authentication Server Address	. . .		
Authentication Server Port	1812		
Authentication Key			
NAS ID			
Re-Auth Interval	3600 sec (60-99999)		
Encryption Method	WEP		
WEP Key Input Mode	Hex		
Key Length	64-bits		
WEP Key Selection	KEY 1		
WEP Keys:	Key 1: Key 2: Key 3: Key 4:		

Security Mechanism

Use 802.1x authentication and WEP coding to make a safer wireless communication.

Use of Local Server

If selecting "Yes", this device can be used as the local authenticated server.
If selecting "Yes", Please click the "**Local Server Table**" button and edit the entry.

Caution

Local server supports **EAP-MD5** authentication. (Max 128 entries)

Authentication Server Address

Enter the IP address of the authenticated server connecting to this device(RADIUS server).

Authentication Server Port

Enter the port number of the authenticated server connecting to this device(RADIUS server).

Authentication Key

Please enter the authenticated key shared with authenticated server.(RADIUS server).

NAS ID

NAS ID (the Network Attached Server Identity) is used as a parameter of authentication.

MEMO

Regarding to authentication configuration

The configurations of the following four items will be effective if "No" is chosen in Use of Local Server.

- Authentication Server Address
- Authentication Server Port
- Authentication Key
- NAS ID

Re-Auth Interval

Specify the cycle of a re-authentication.(in the range from 60 to 99999 secs.)

Encryption method

Display the encryption method used in the current security function.
WEP supports transmitting data encryption.

WEP Input Mode

Either ASCII or Hex can be chosen as a Key input mode.

Key Length

Either 64 bits or 128-bit encryption can be specified.

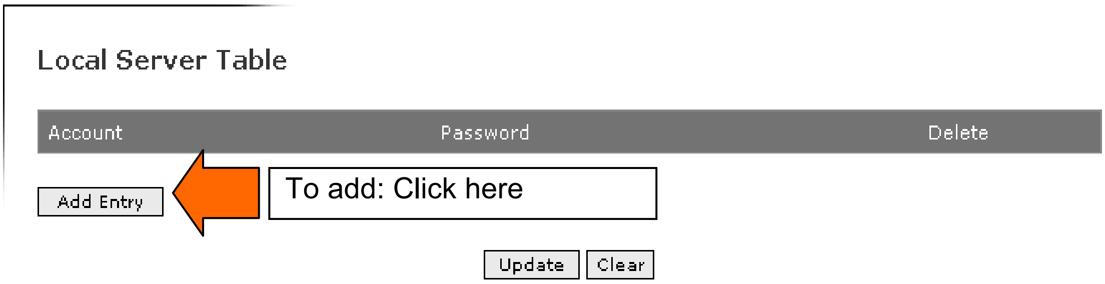
WEP Key Selection

Please select one from a maximum of 4 set up encryption Keys.

WEP Key

The maximum of 4 keys can be entered.
If the **Key Length** is 64 bits, ASCII inputs 5 letters and Hex inputs the letters of 10 digits.
If 128 bits, ASCII inputs 13 letters and Hex inputs the letters of 26 digits.

Local Server Table

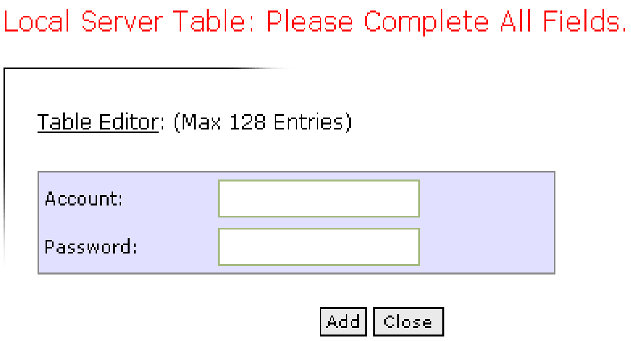


Local Server Table

Account	Password	Delete

Local Server Table (Before the edition)

Please refer to, edit and delete **Local Server Table**.
If adding entry, please click **Add Entry**.



Local Server Table: Please Complete All Fields.

Table Editor: (Max 128 Entries)

Account:	
Password:	

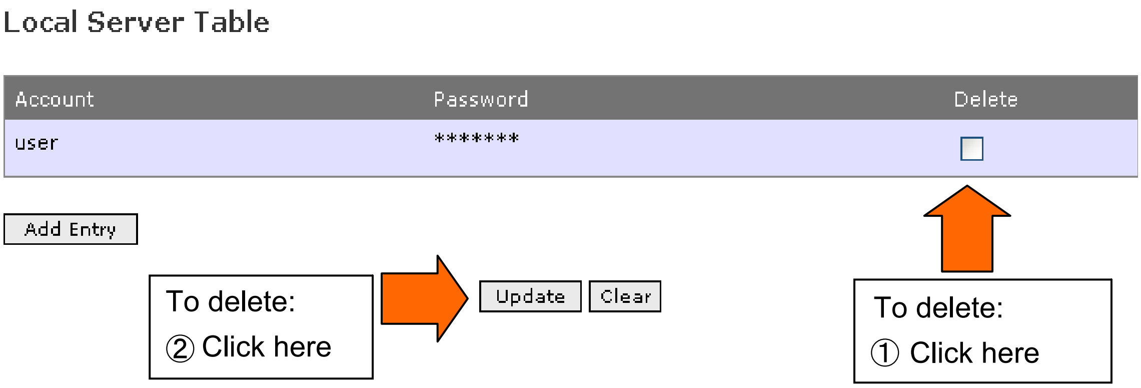
Table Editor

For adding registration,please enter the date in the table editor and click "Add" button.

It can add to Local Server Table a maximum of 128 entries.

Caution

The system configuration related to an authentication server is used as the information related to a RADIUS server. RADIUS client can be used as a security function while using WEP/802.1x and WPA/802.1x.



Local Server Table

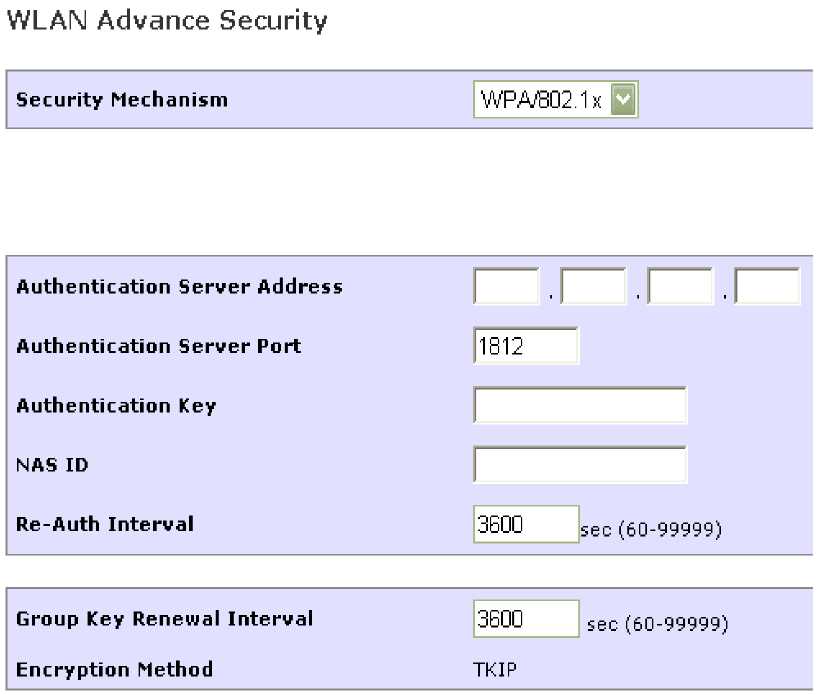
Account	Password	Delete
user	*******	□

Local Server Table (After the edition)

After the edition, the new data will display as above.

If you want to delete the entry, please check the "**Delete**" box in advance and click the "**Update**" button. If clicking "**Clear**", it might clear the "**Delete**" box.

(4) WPA/802.1x



WLAN Advance Security

Security Mechanism	WPA/802.1x

Authentication Server Address	. . .
Authentication Server Port	1812
Authentication Key	
NAS ID	
Re-Auth Interval	3600 sec (60-99999)

Group Key Renewal Interval	3600 sec (60-99999)
Encryption Method	TKIP

Security Mechanism

The connection of an external RADIUS server is established by this device in WPA/802.1x.
Furthermore, before applying this security function, downloading authentication is required from a RADIUS server.

Authentication Server Address

Enter the IP address of the authentication server (RADIUS server).

Authentication Server Port

Enter the port number of the authentication server (RADIUS server).

Authentication Key

Enter the authenticated key shared with the authentication server (RADIUS server).

NAS ID

NAS ID (the Network Attached Server Identity) is used as a parameter of authentication.

Re-Auth Interval

Specify the cycle of a re-authentication.(in the range from 60 to 99999 secs.)

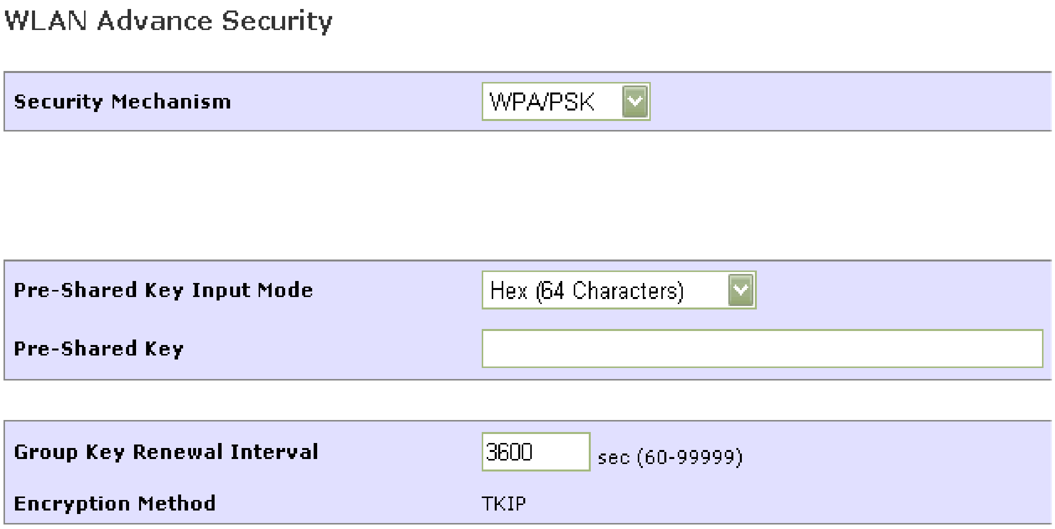
Group Key Renewal Interval

Specify the cycle of group key renewal.
Group key is updated required by the user.
(in the possible range from 60 to 99999 secs.)

Encryption Method

Display the encryption method. The encryption method of WPA/802.1x is TKIP.

(5) WPA/PSK



WLAN Advance Security

Security Mechanism	WPA/PSK
Pre-Shared Key Input Mode	Hex (64 Characters)
Pre-Shared Key	
Group Key Renewal Interval	3600 sec (60-99999)
Encryption Method	TKIP

Security Mechanism

The prior share Key shared between this device and the other is set up in WPA/PSK.
This key generates keys for the data protection between this device and the other.
There are the 2 input modes incluing ASCII and Hex.

Pre-Shared Key Input Mode

It is the input mode of **Pre-Shared Key**. Select either ASCII or Hex.

Pre-Shared Key

About Hex input mode, please enter 64 digits (fixed).
About ASCII input mode, please input alphanumeric letters within the limits from 8 to 63.

Group Key Renewal Interval

Specify the cycle of group key renewal.
Group key is updated required by the user.
(in the possible range from 60 to 99999 secs.)

Encryption Method

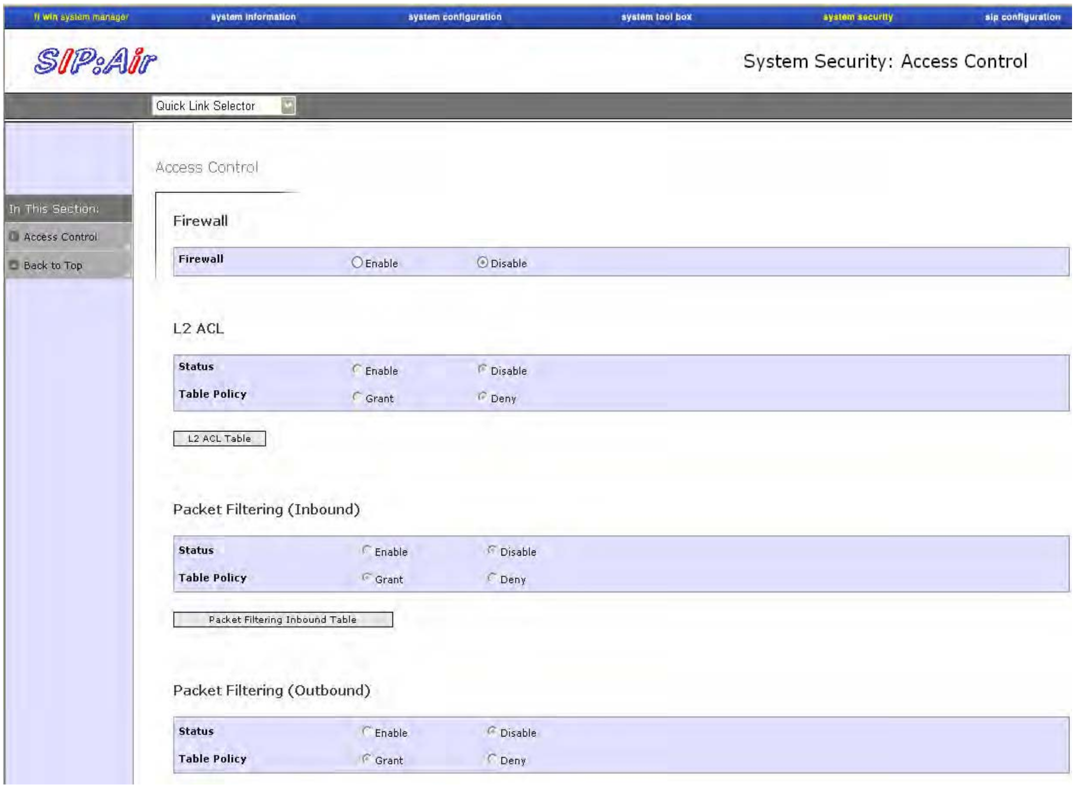
Display the encryption method. The encryption method of WPA/802.1x is TKIP.

5.2 System Security

~~AP~~

Please click "**system security**" in the menu displayed on upper side of the screen. (The "**system security**" will reverse to yellow after selection).
It will display as below.

Please select
system security



System Security: Access Control

Access Control

Firewall

Firewall	○ Enable	● Disable

L2 ACL

Status	○ Enable	● Disable
Table Policy	○ Grant	● Deny

Packet Filtering (Inbound)

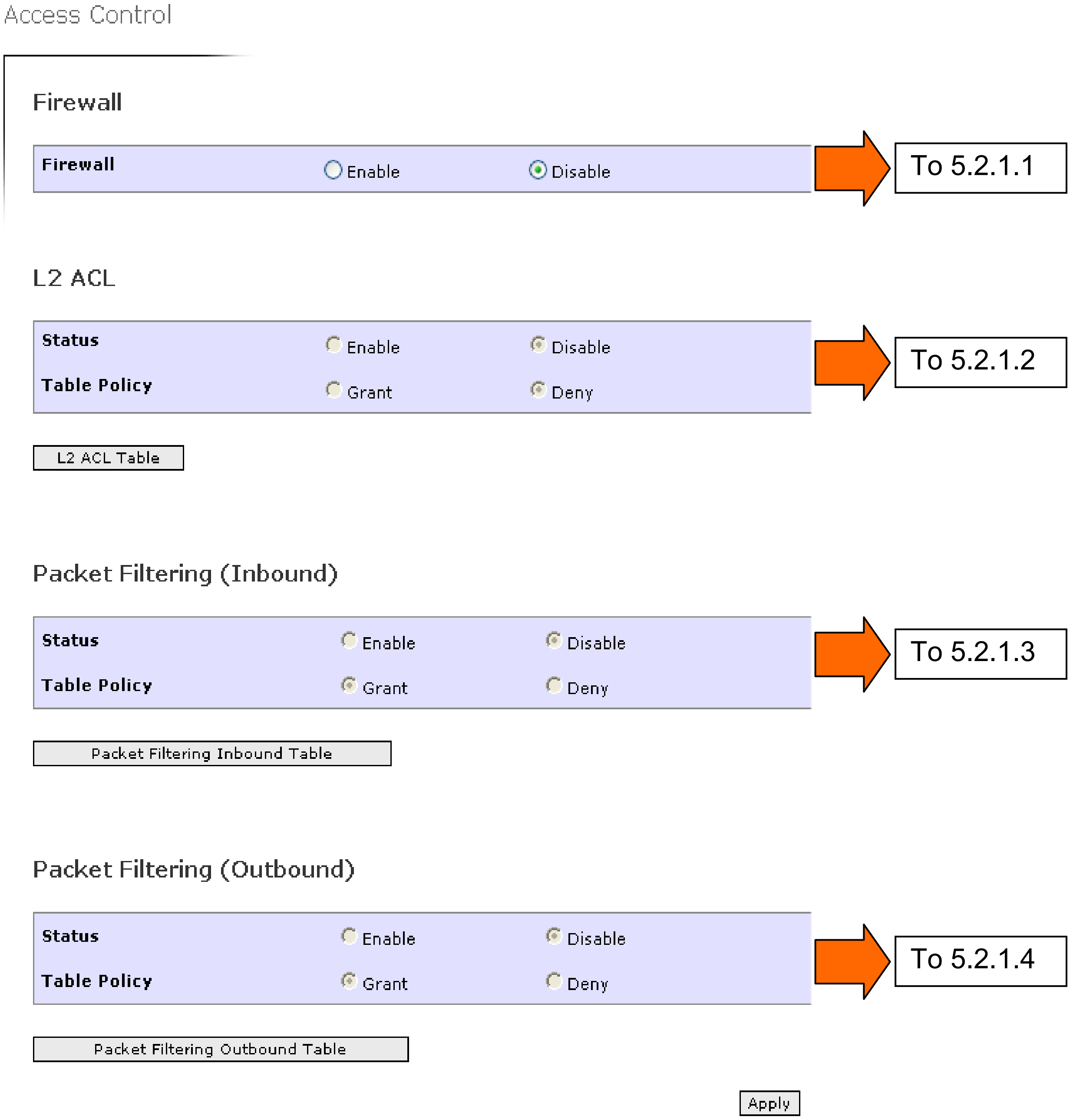
Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

Packet Filtering (Outbound)

Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

5.2.1 Access Control

Please click "**Access Control**" from "**5.2 System Security**" menu displayed on the left side of the screen.



Access Control

Firewall

Firewall	○ Enable	● Disable

To 5.2.1.1

L2 ACL

Status	○ Enable	● Disable
Table Policy	○ Grant	● Deny

To 5.2.1.2

Packet Filtering (Inbound)

Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

To 5.2.1.3

Packet Filtering Inbound Table

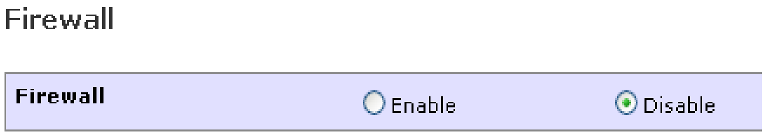
Packet Filtering (Outbound)

Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

To 5.2.1.4

Packet Filtering Outbound Table
Apply

5.2.1.1 Firewall



Firewall

Firewall ○ Enable ● Disable

Firewall

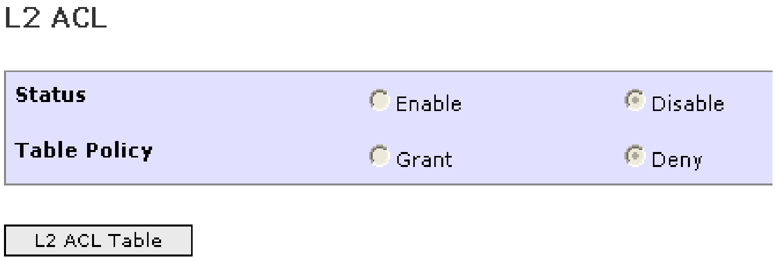
Setup the firewall (L2 ACL, packet filtering) as Enable / Disable. The default value is Disable. If enabling firewall, the following items can be setup.

5.2.1.2 L2 ACL

MEMO

Regarding to L2 ACL setting of SS38 (AP Mode)

It's not in the "**System Security**" menu. Please setup in "**System Security Wizard**" menu of the "**System Tool Box**" ("**7.1.1 Setting Wizard**")



L2 ACL

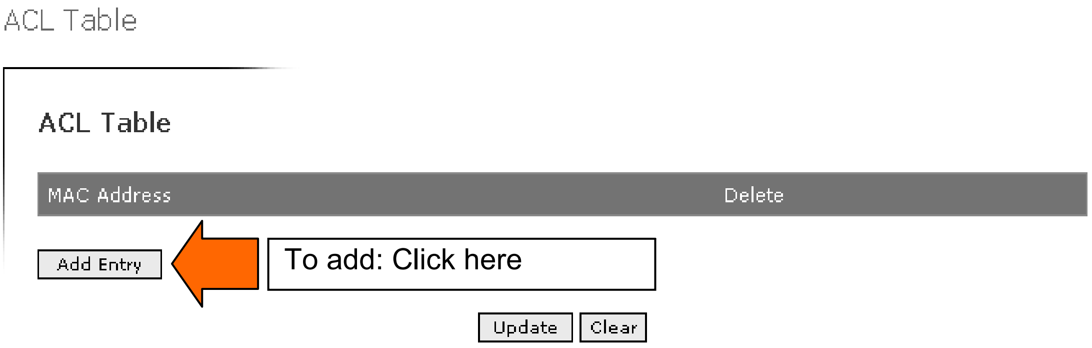
Status ○ Enable ● Disable

Table Policy ○ Grant ● Deny

L2 ACL

Setup the policy of layer 2 access control list (L2 ACL) .
There are 2 configurations of Grant and Deny.
When setting as Grant, it permits that the device with the registered layer 2 MAC Address connects to the network.
No devices which are not registered into other ACL can connect to the network.

If set as Deny, the device with the registered layer 2 MAC Address refuses to connect to the network.
All the terminals that are not registered into other ACL make network connection.
No devices which are not registered into other ACL can connect to the network.



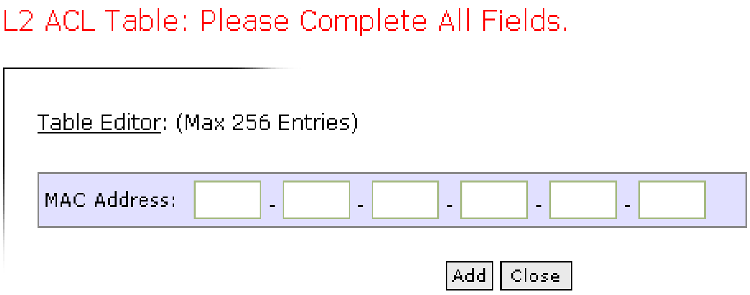
ACL Table

ACL Table

MAC Address	Delete

ACL Table

The window which displays the current registration status will show as above if clicking **L2 ACL Table**, If you want to add new entry, please click the "**Add Entry**" button in the left side of the window.



L2 ACL Table: Please Complete All Fields.

Table Editor: (Max 256 Entries)

MAC Address: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

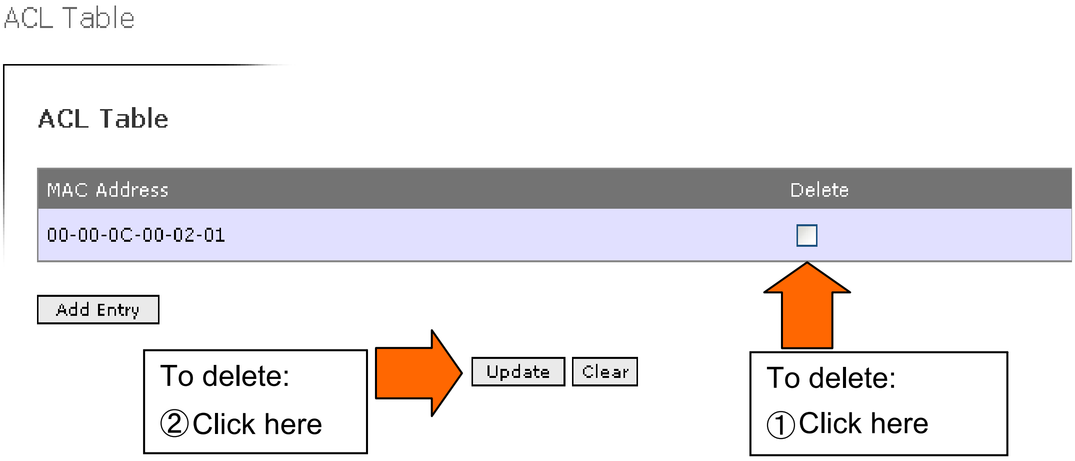
Table Editor

Please add the data, and click "**Add**" button to register.

ACL table can be registered a maximum of 256 addresses.

Caution

ACL is effective only at the WLAN interface.



ACL Table

ACL Table

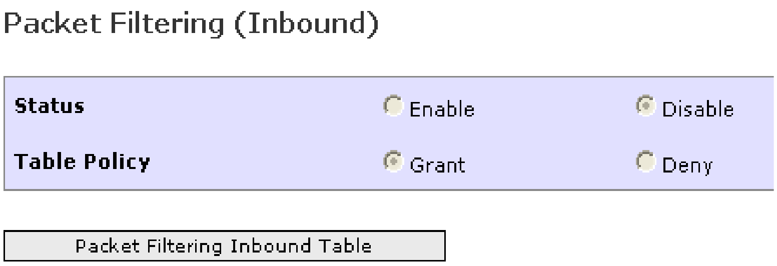
MAC Address	Delete
00-00-0C-00-02-01	□

ACL Table (After the edition)

After the edition, the new data will display as above.

If you want to delete the entry, please check the "**Delete**" box in advance and click the "**Update**" button. If clicking "**Clear**", it might clear the "**Delete**" box.

5.2.1.3 Packet Filtering (Inbound)



Packet Filtering (Inbound)

Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

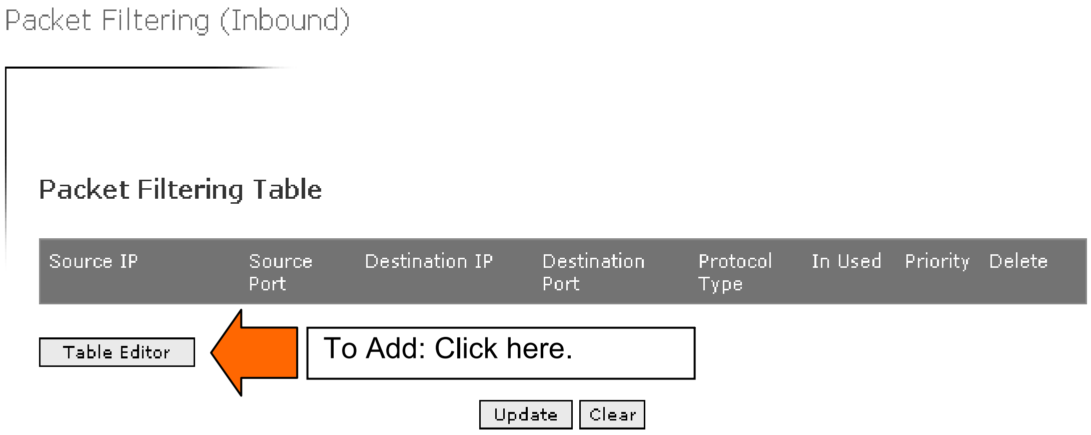
Packet Filtering (Inbound)

According to the security policy, it filters when using the header information of the layer 3 (L3) and layer 4 (L4) of an inbound packet.

The security policy will be setup according to **Packet Filtering Inbound Table**.

If set as Grant, the packet, which was the same with the registered filter conditions, will be relayed. The packet, which doesn't correspond to filter conditions, will be canceled.

If set as Deny, the packet, which was the same with the registered filter conditions, will be canceled. The packet, which doesn't correspond to filter conditions, will be relayed.



Packet Filtering (Inbound)

Packet Filtering Table

Source IP	Source Port	Destination IP	Destination Port	Protocol Type	In Used	Priority	Delete

To Add: Click here.

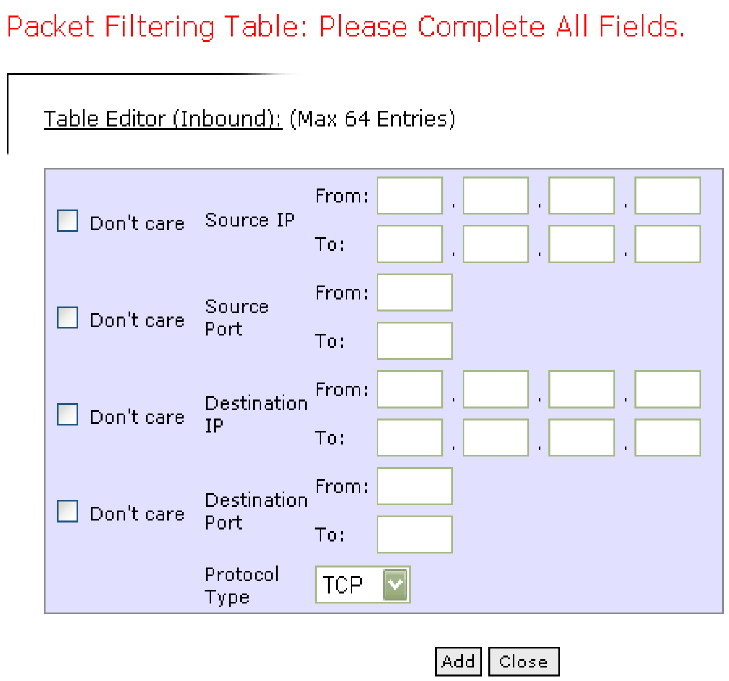
Packet Filtering Table (Before the edition)

Displays the existing entries. Each entry contains a source IP, source port, destination IP, destination port, protocol type and the priority.

You can edit the priority and delete the entry from this table.

The entry, which checked in the "**In Used**" box is used for packet filtering, and the entry without the check, will be ignored.

If you want to change the value of "Priority" box, please click "**Update**" button and the priorty of each entry will be changed.



Packet Filtering Table: Please Complete All Fields.

Table Editor (Inbound): (Max 64 Entries)

☐ Don't care	Source IP	From:	. . .
		To:	. . .
☐ Don't care	Source Port	From:	
		To:	
☐ Don't care	Destination IP	From:	. . .
		To:	. . .
☐ Don't care	Destination Port	From:	
		To:	
	Protocol Type	TCP	

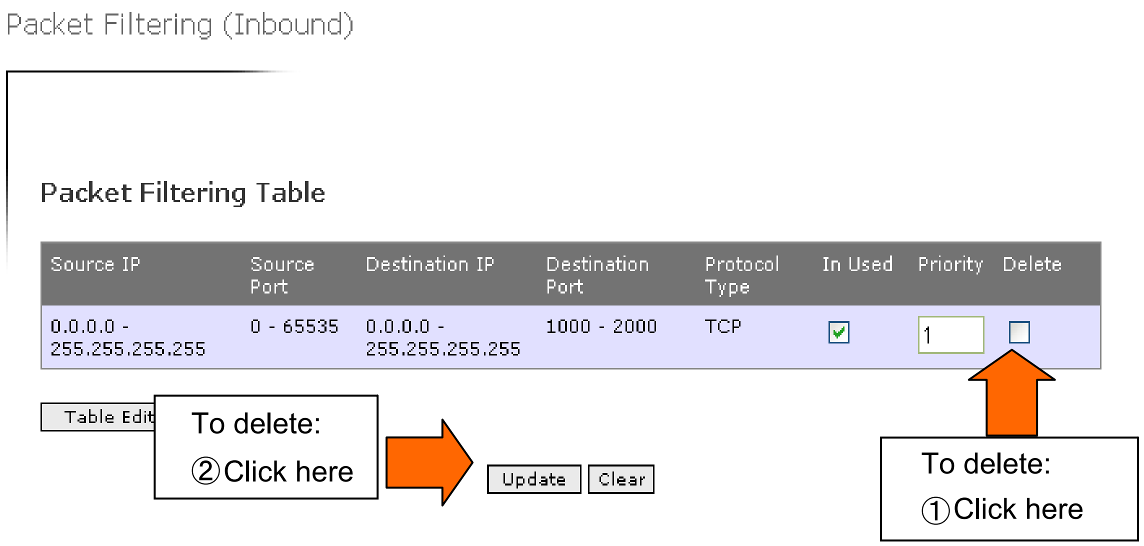
Table Editor

Setting up an IP address, specific port or a specific protocol type can define a packet-filtering policy.
The entry which checked the "Don't care" box will be ignored.
All the additional policies are displayed on Packet Filtering Table.

MEMO

Regarding to "Inbound" packet

"Inbound" packet means the packet transmitted to internal LAN/WLAN from the external WAN side.



Packet Filtering (Inbound)

Packet Filtering Table

Source IP	Source Port	Destination IP	Destination Port	Protocol Type	In Used	Priority	Delete
0.0.0.0 - 255.255.255.255	0 - 65535	0.0.0.0 - 255.255.255.255	1000 - 2000	TCP	☑	1	☐

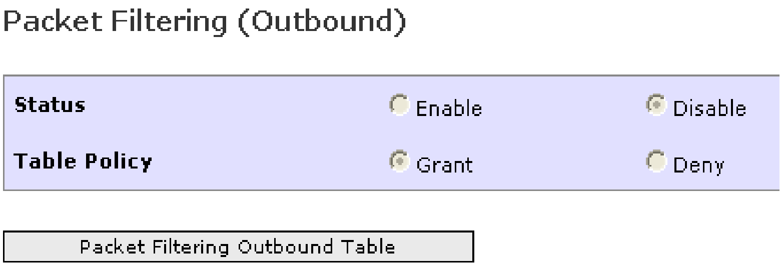
To delete: ②Click here

To delete: ①Click here

Packet Filtering Table (After the edition)

After the edition, the new data will display as above.
If you want to delete the entry, please check the "**Delete**" box in advance and click the "**Update**" button. If clicking "**Clear**", it might clear the "**Delete**" box.

5.2.1.4 Packet Filtering (Outbound)



Packet Filtering (Outbound)

Status	○ Enable	● Disable
Table Policy	● Grant	○ Deny

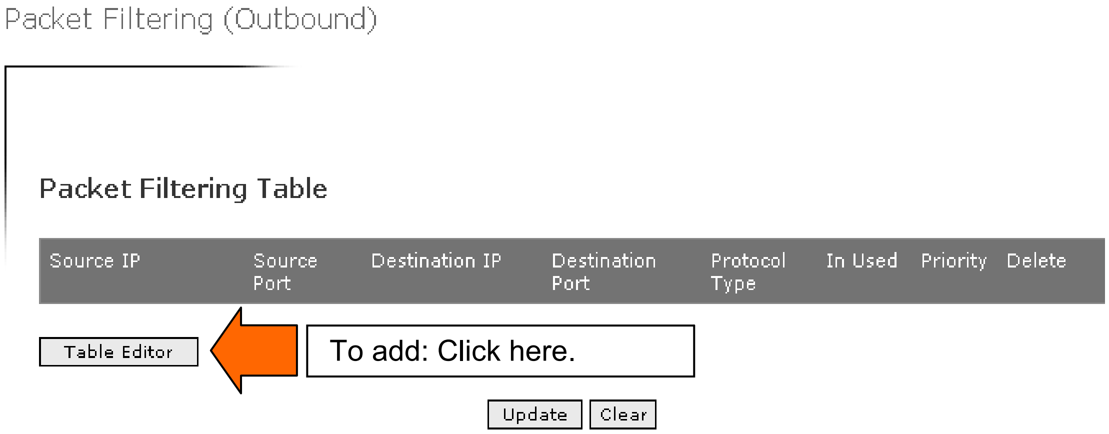
Packet Filtering (Outbound)

According to the security policy, it filters when using the header information of the layer 3 (L3) and layer 4 (L4) of an outbound packet.

The security policy will be setup according to **Packet Filtering Outbound Table**.

If set as Grant, the packet, which was the same with the registered filter conditions, will be relayed. The packet, which doesn't correspond to filter conditions, will be canceled.

If set as Deny, the packet, which was the same with the registered filter conditions, will be canceled. The packet, which doesn't correspond to filter conditions, will be relayed.



Packet Filtering (Outbound)

Packet Filtering Table

Source IP	Source Port	Destination IP	Destination Port	Protocol Type	In Used	Priority	Delete

To add: Click here.

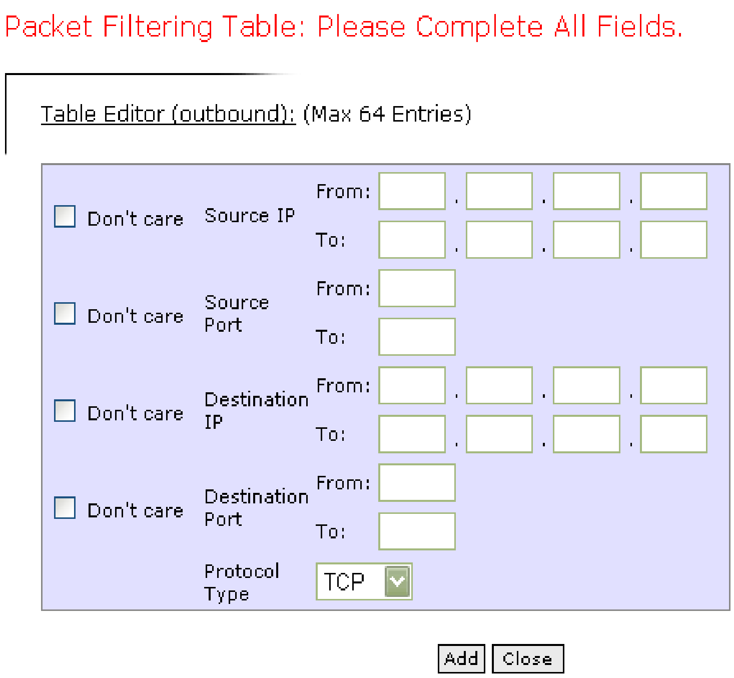
Packet Filtering Table (Before the edition)

Displays the existing entries. Each entry contains a source IP, source port, destination IP, destination port, protocol type and the priority.

You can edit the priority and delete the entry from this table.

The entry which checked in the "**In Used**" box is used for packet filtering, and the entry without the check will be ignored.

If you want to change the value of "Priority" box, please click "**Update**" button and the priorty of each entry will be changed.



Packet Filtering Table: Please Complete All Fields.

Table Editor (outbound): (Max 64 Entries)

□ Don't care	Source IP	From:	. . .
		To:	. . .
□ Don't care	Source Port	From:	
		To:	
□ Don't care	Destination IP	From:	. . .
		To:	. . .
□ Don't care	Destination Port	From:	
		To:	
	Protocol Type	TCP	

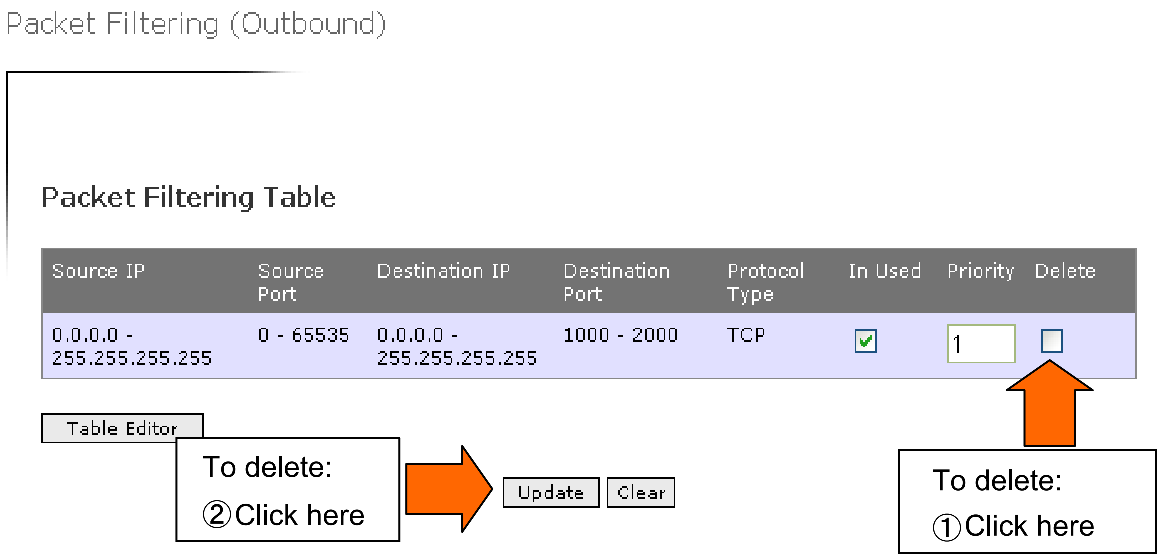
Table Editor

Setting up an IP address, specific port or a specific protocol type can define a packet-filtering policy.
The entry which checked the "Don't care" box will be ignored.
All the additional policies are displayed on Packet Filtering Table.

MEMO

Regarding to "Outbound" packet

"Outbound" packet means the packet transmitted to external WAN from the internal LAN / WLAN side.



Packet Filtering (Outbound)

Packet Filtering Table

Source IP	Source Port	Destination IP	Destination Port	Protocol Type	In Used	Priority	Delete
0.0.0.0 - 255.255.255.255	0 - 65535	0.0.0.0 - 255.255.255.255	1000 - 2000	TCP	☑	1	□

To delete:
②Click here

To delete:
①Click here

Packet Filtering Table (After the edition)

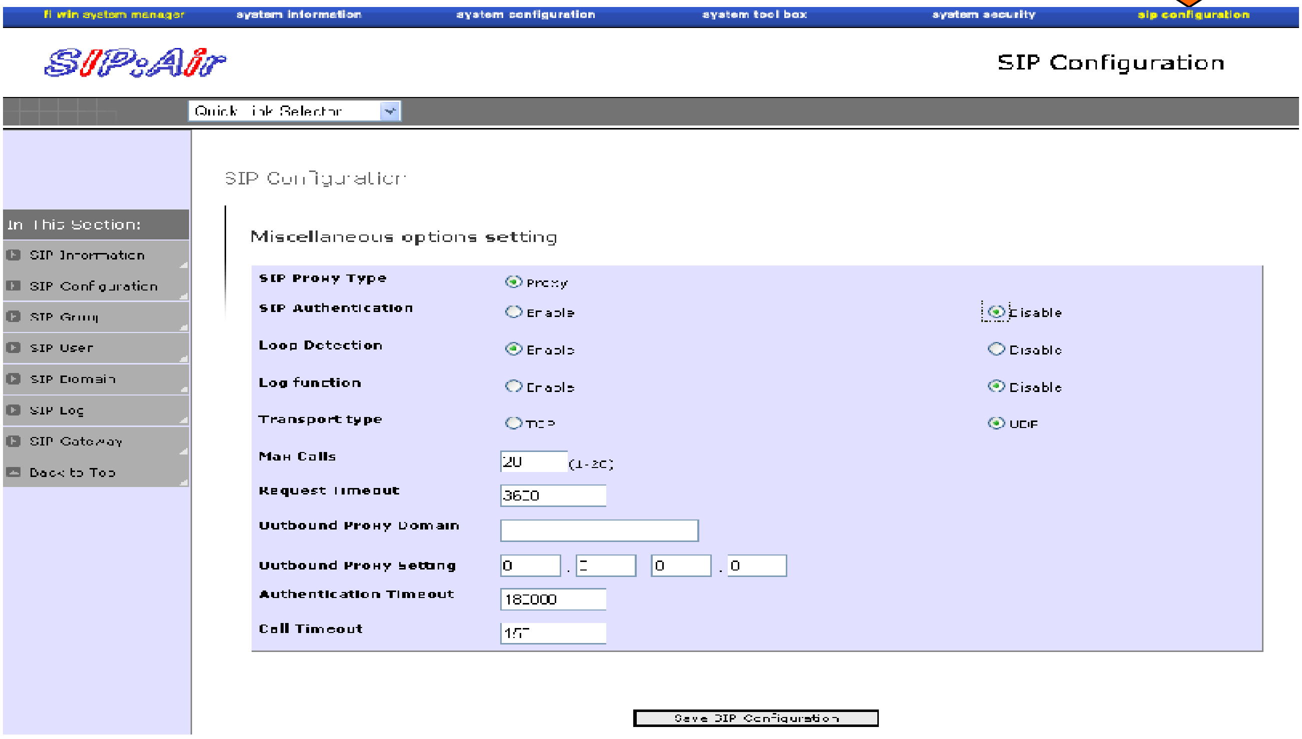
After the edition, the new data will display as above.
If you want to delete the entry, please check the "**Delete**" box in advance and click the "**Update**" button. If clicking "**Clear**", it might clear the "**Delete**" box.

5.3 SIP Configuration

~~@AP~~

Please click "**sip configuration**" in the menu displayed on upper side of the screen.
(The "**sip configuration**" will reverse to yellow after selection).
It will display as below.

Please click
sip configuration



SIP Configuration

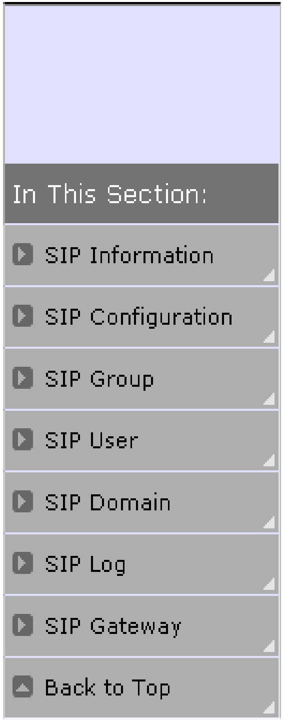
SIP Configuration

Miscellaneous options setting

SIP Proxy Type	● Proxy	
SIP Authentication	○ Enable	● Disable
Loop Detection	● Enable	○ Disable
Log function	○ Enable	● Disable
Transport type	○ TCP	● UDP
Max Calls	20 (1-20)	
Request Timeout	3600	
Outbound Proxy Domain		
Outbound Proxy Setting	0 . 0 . 0 . 0	
Authentication Timeout	180000	
Call Timeout	[illegible]	

Save SIP Configuration

Then, please choose the menu arbitrarily displayed on "**In This Selection**".
Please refer to the following explanation for operations as below.

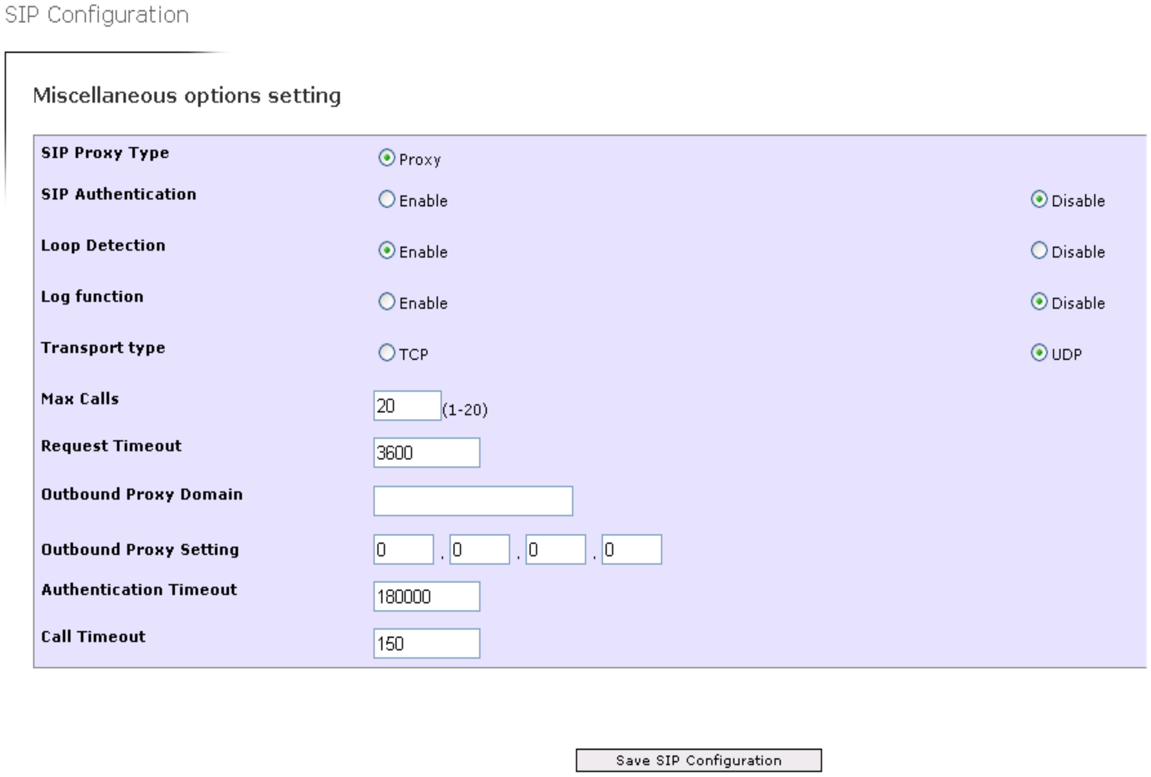


In This Section:

- SIP Information
- SIP Configuration → **5.3.1 SIP Configuration**
- SIP Group → **5.3.2 SIP Group**
- SIP User → **5.3.3 SIP User**
- SIP Domain → **5.3.4 SIP Domain**
- SIP Log
- SIP Gateway → **5.3.5 SIP gateway**
- Back to Top

5.3.1 SIP Configuration

Please click "**SIP Configuration**" from "**5.3 SIP Configuration**" menu displayed on the left side of the screen.



SIP Configuration

Miscellaneous options setting

SIP Proxy Type	● Proxy	
SIP Authentication	○ Enable	● Disable
Loop Detection	● Enable	○ Disable
Log function	○ Enable	● Disable
Transport type	○ TCP	● UDP
Max Calls	20 (1-20)	
Request Timeout	3600	
Outbound Proxy Domain		
Outbound Proxy Setting	0 . 0 . 0 . 0	
Authentication Timeout	180000	
Call Timeout	150	

SIP Proxy Type

This version supports Proxy mode.

In Proxy mode, when SIP server process receives a request, it will be transferred to UA or other Proxy servers.

SIP Authentication

Enable/Disable the SIP authentication. The default value is Disable.

Enable : Authentication information is required when SIP User connects to this device.

Disable: Authentication information isn't required when SIP User connects to this device.

Loop Detection

Enable/Disable the loop detection function of SIP Proxy server. The default value is Enable.

Enable : When the loop is detected, this device doesn't transmit SIP messages.

Disable: Whether a loop status is generated or not, this device still transmits SIP messages.

Log function

Enable/Disable SIP log function of this device.

The default value is Disable

Enable :100 newest SIP messages are held in the database.

Disable: No SIP message is held.

Transport type

Setup the transport type (TCP or UDP) of the SIP message from this device.

The default value is UDP.

TCP: Use TCP to send the SIP message.

UDP: Use UDP to send the SIP message.

Max Calls

Combine the external and internal lines, and specify the number of current phone calls.
The default value is 20. (The possible range is from 1 to 20.)

Request Timeout

Specifiy the SIP registration effective time (secs.). The default value is 3600 secs.
SIP registration is effective until the registration effective time is timeout.
Using the default value of 3600 is recommended. (The possible range is from 3600 to 999999 secs.)

Caution

Request Timeout is effective only when SIP User doesn't specify registration effective time.

Outbound Proxy Domain

Setup the domain name of Outbound Proxy server.
Regarding to the detail, please refer to Outbound Proxy Setting.

Outbound Proxy Setting

Setup the IP address of Outbound Proxy server. The default value is 0.0.0.0.
Please set an effective value only when the Outbound Proxy server exists.
If setting 0.0.0.0, Outbound Proxy server will be invalid.
SIP Proxy server will transmit a SIP message to the Outbound Proxy server.

Authentication Timeout

Specify the waiting time for authentication information of a SIP Proxy server (millisecond).
The default value is 180000ms.
SIP Proxy server will wait for authentication information until time is timeout.
Using the default value of 180000 is recommended. (The possible range is from 180000 to 99999999 ms.)

Call Timeout

Setup the time of transfer URL timeout for attended transfer.
The default value is 150. (The possible range is from 15 to 150.)

Save SIP Configuration

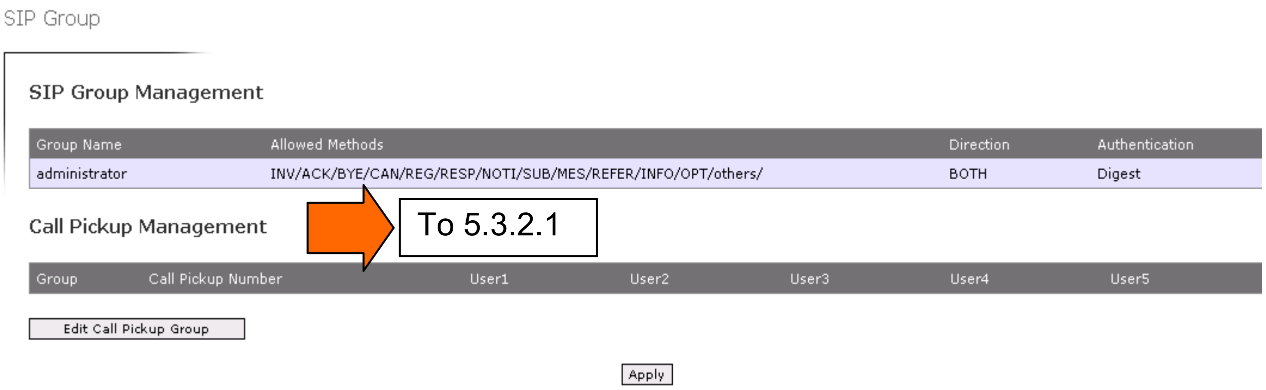
If clicking this button, the configuration for Miscellaneous options setting (as above) will be saved.

Caution

If the device is rebooted without saving change, the contents of change will be lost.

5.3.2 SIP Group

Please click "**SIP Group**" from "**5.3 SIP Configuration**" menu displayed on the left side of the screen. It will display as below.



SIP Group

SIP Group Management

Group Name	Allowed Methods	Direction	Authentication
administrator	INV/ACK/BYE/CAN/REG/RESP/NOTI/SUB/MES/REFER/INFO/OPT/others/	BOTH	Digest

Call Pickup Management

To 5.3.2.1

Group	Call Pickup Number	User1	User2	User3	User4	User5

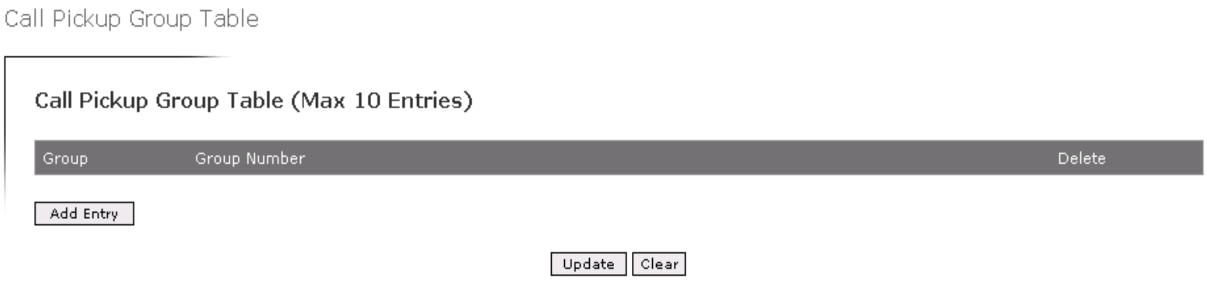
SIP Group management

Display the group information of SIP Proxy server.

This version only supports "**administration**" group.

5.3.2.1 Call Pickup Management

Please press "**Edit Call Pickup Group**" button in the "**5.3.2 SIP Group**".

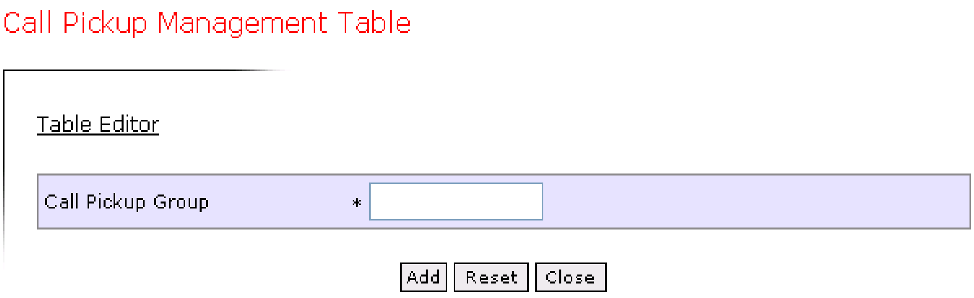


Call Pickup Group Table

Call Pickup Group Table (Max 10 Entries)

Group	Group Number	Delete

Please click "**Add Entry**" button.



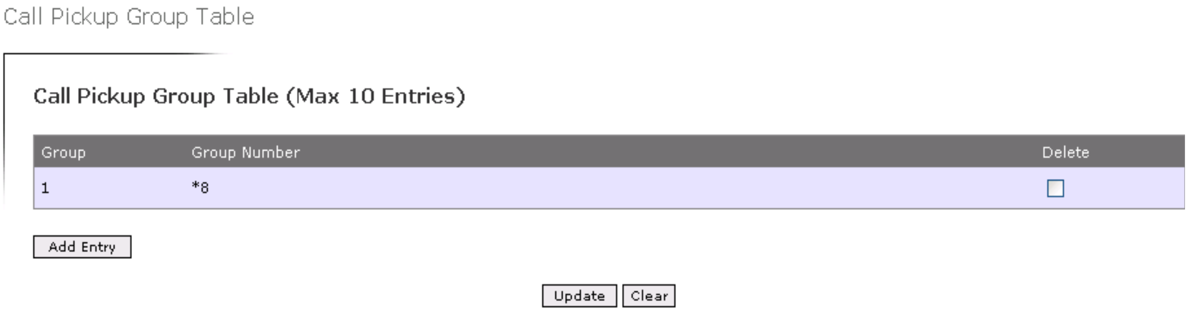
Call Pickup Management Table

Table Editor

Call Pickup Group *

Call Pickup Group

Please enter the number for call pickup.

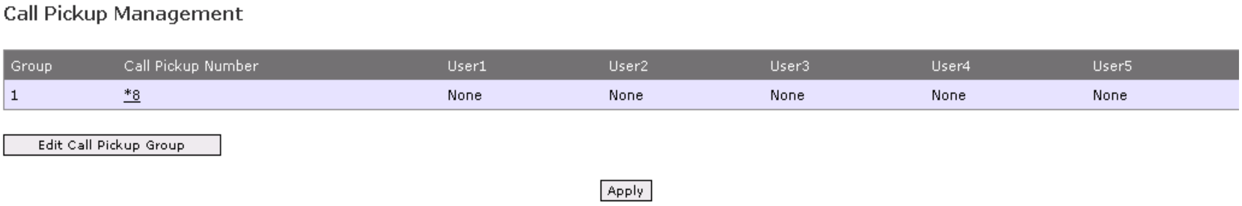


Call Pickup Group Table

Call Pickup Group Table (Max 10 Entries)

Group	Group Number	Delete
1	*8	□

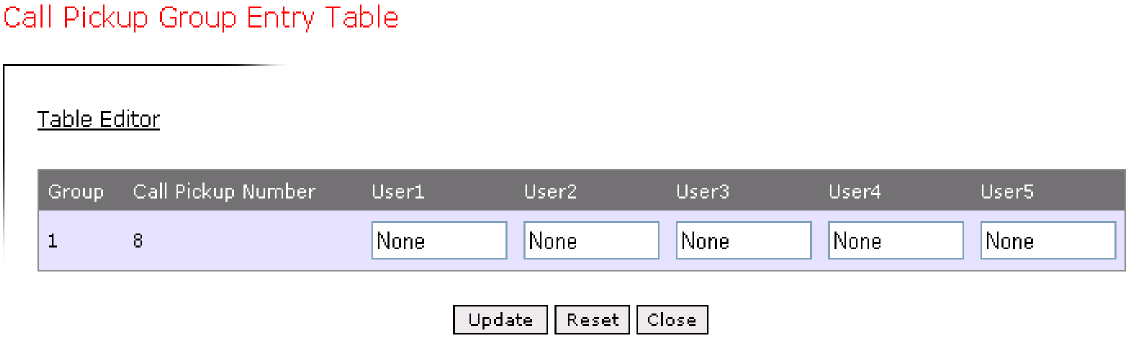
After ensuring the input content, please click "**Update**" button.



Call Pickup Management

Group	Call Pickup Number	User1	User2	User3	User4	User5
1	*8	None	None	None	None	None

Then, please setup the extension numbers to a grouping. (User1 ~ User5)
Please click the number of **"Call Pickup Number**" (The number with an underline).



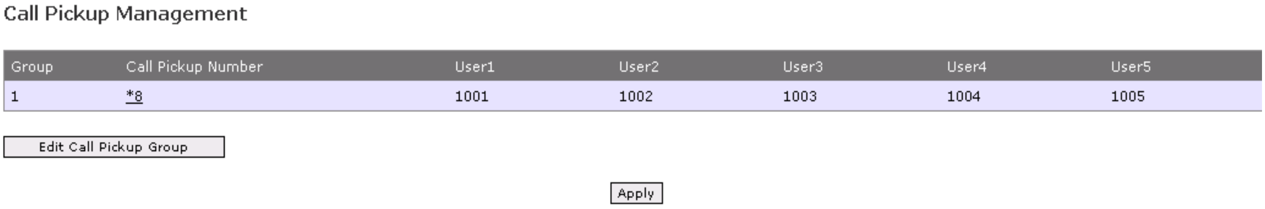
Call Pickup Group Entry Table

Table Editor

Group	Call Pickup Number	User1	User2	User3	User4	User5
1	8	None	None	None	None	None

User1~User5

Please setup the extension numbers of "**Call Pickup Number**" to a grouping.
After entering, please click "**Update**" button.



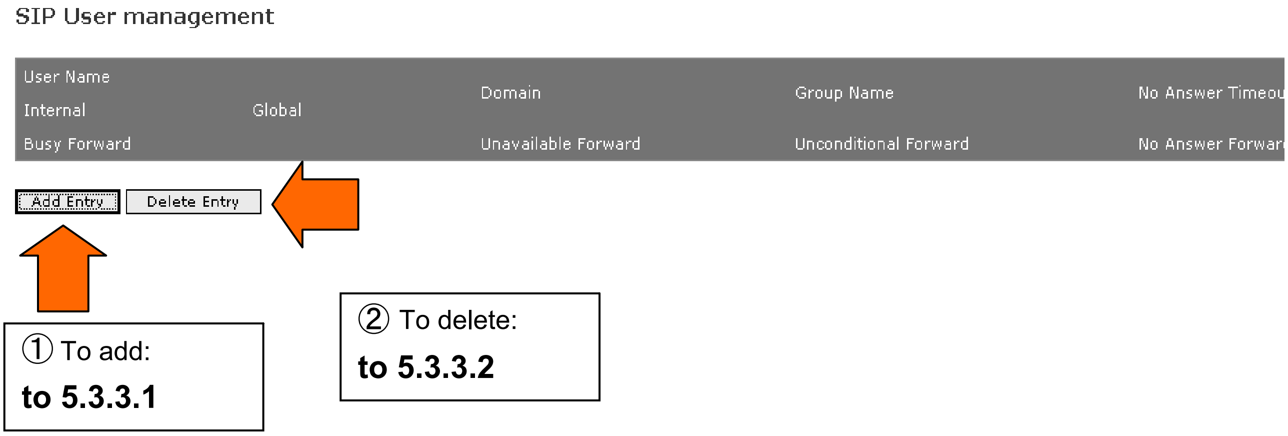
Call Pickup Management

Group	Call Pickup Number	User1	User2	User3	User4	User5
1	*8	1001	1002	1003	1004	1005

The screen after editing.

5.3.3 SIP User

Please click "SIP User" from "5.3 SIP Configuration" menu displayed on the left side of the screen.
It will display as below.



SIP User management

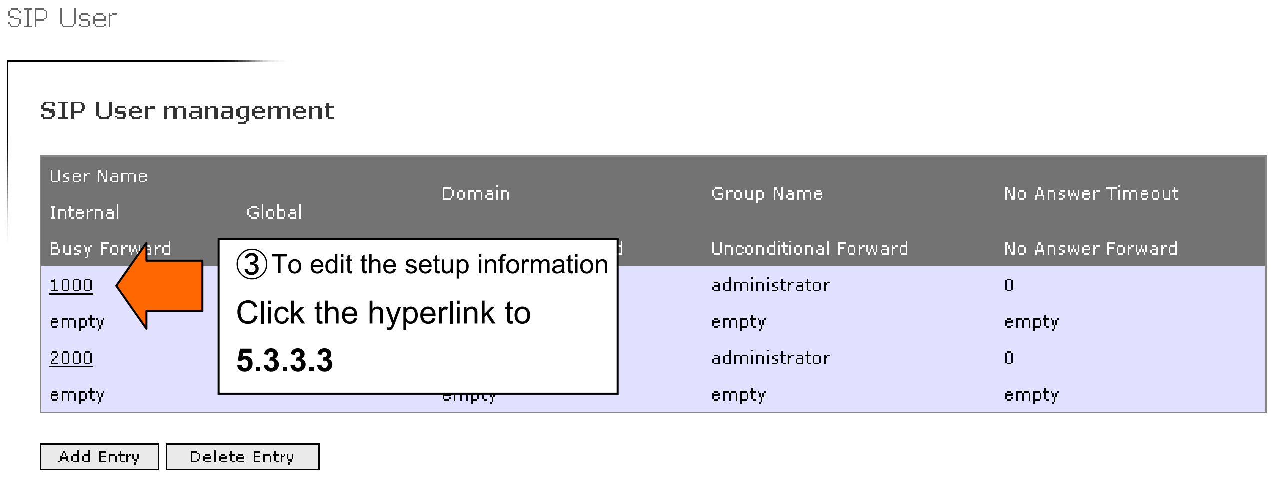
User Name Internal Busy Forward	Global	Domain Unavailable Forward	Group Name Unconditional Forward	No Answer Timeou No Answer Forwar

① To add:
to 5.3.3.1

② To delete:
to 5.3.3.2

SIP User management

Display the user information of this device.
If adding the user entry, please cilck "**Add Entry**" .(as figure ①)
If deleting the user entry, please click "**Delete Entry**".(as figure ②)
If editing the user entry, please click the hyperlink of "**User Name**".(as figure ③)



SIP User

SIP User management

User Name Internal Busy Forward	Global	Domain Unavailable Forward	Group Name Unconditional Forward	No Answer Timeout No Answer Forward
1000			administrator	0
empty			empty	empty
2000			administrator	0
empty		empty	empty	empty

③To edit the setup information
Click the hyperlink to
5.3.3.3

5.3.3.1 Add SIP User

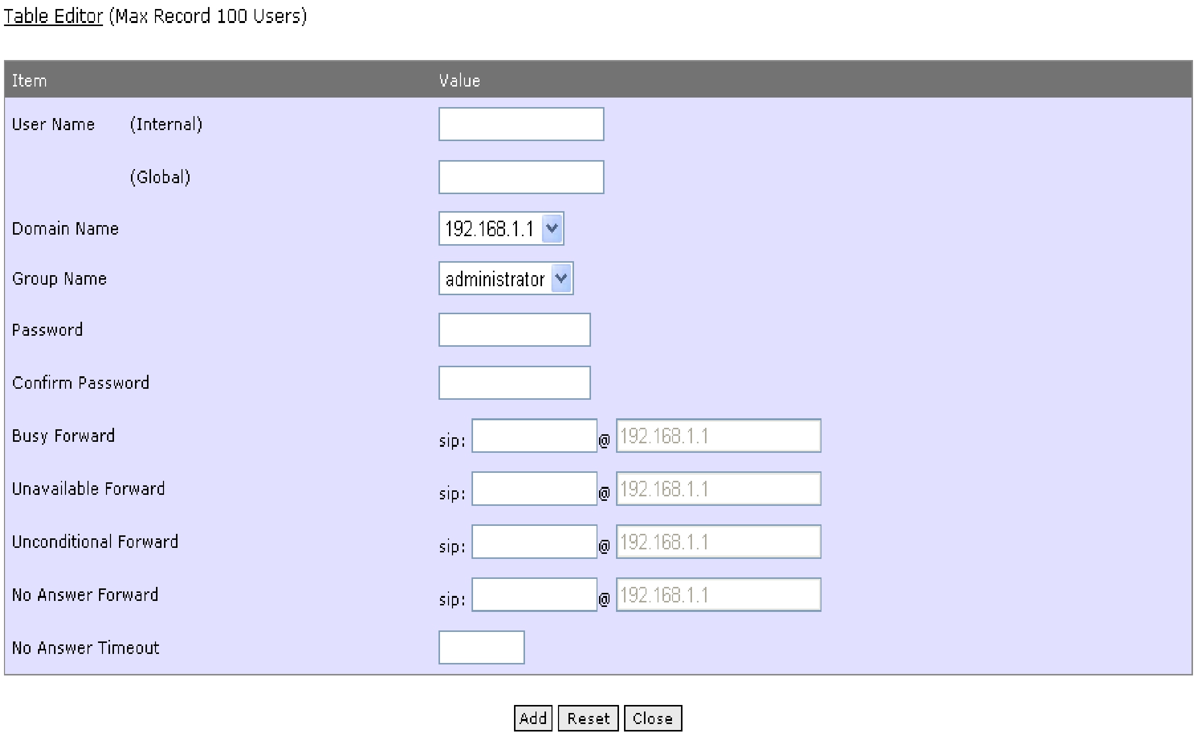


Table Editor (Max Record 100 Users)

Item	Value
User Name (Internal)	
(Global)	
Domain Name	192.168.1.1
Group Name	administrator
Password	
Confirm Password	
Busy Forward	sip: @ 192.168.1.1
Unavailable Forward	sip: @ 192.168.1.1
Unconditional Forward	sip: @ 192.168.1.1
No Answer Forward	sip: @ 192.168.1.1
No Answer Timeout	

Table Editor

Add the new user. If clicking "**Add**" button after entering the user data, it will display the result of the additional registration.

This device can set up the SIP user of a maximum of 100 entries.

User Name (Internal)

Setup the internal number of the new user.

This user name will be registered as the internal number.

User Name (Global)

Setup the external number of the new user.

It will registered as the external number of the device.

Domain Name

Specify a domain name of the user.

Group Name

Specify the group name of the user.

Password

Enter the password for SIP authentication.

If SIP Authentication is Enable, you have to enter the password.

Confirm Password

Enter the password again.

Busy Forward

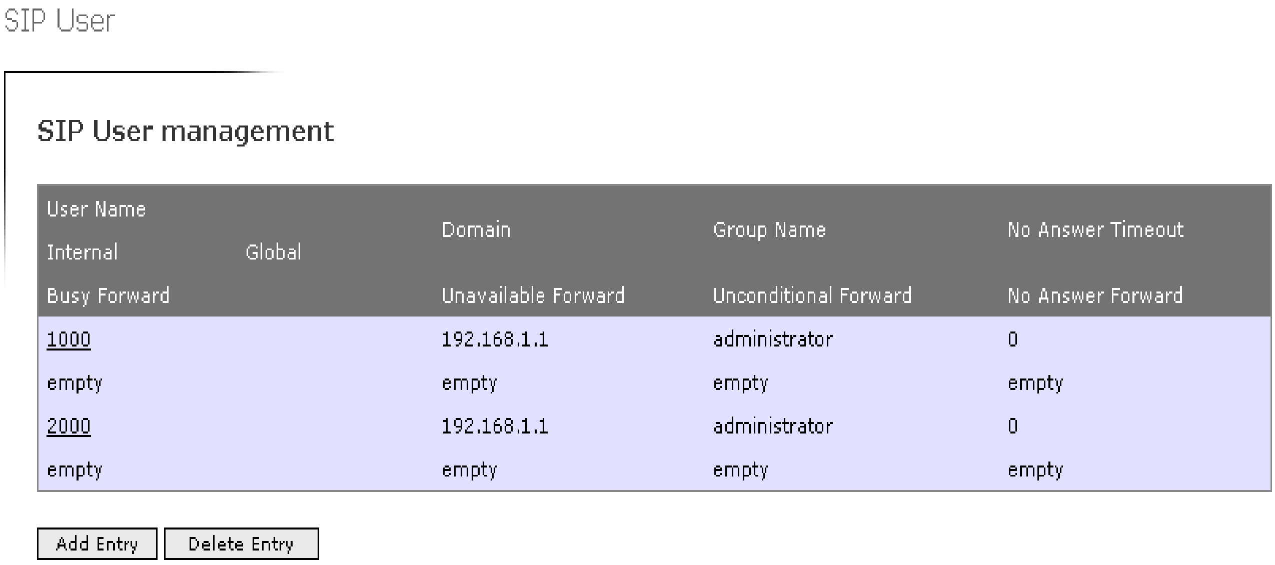
Enter the SIP URL of the Busy forward.

Unavailable Forward
Enter the SIP URL of Unavailable forward Previous (Unavailable transfer).

Unconditional Forward
Enter the SIP URL of Unconditional forward (Unconditional transfer).

No Answer Forward
Enter the SIP URL of No answer forward (No Answer transfer).

No Answer Timeout
Setup Timeout value of No answer (1~999)



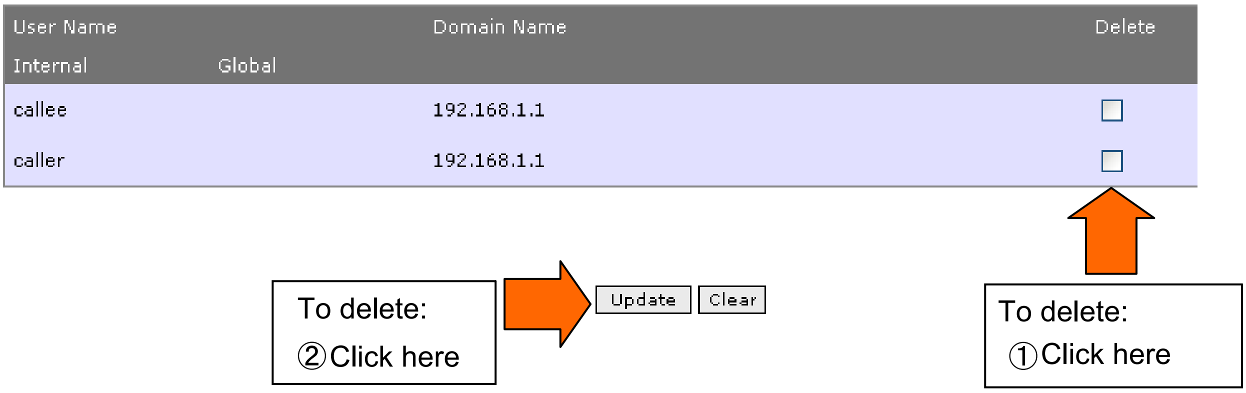
SIP User

SIP User management

User Name		Domain	Group Name	No Answer Timeout
Internal	Global			
Busy Forward		Unavailable Forward	Unconditional Forward	No Answer Forward
1000		192.168.1.1	administrator	0
empty		empty	empty	empty
2000		192.168.1.1	administrator	0
empty		empty	empty	empty

Regarding to "**Domain Name**" and "**@xxx**" of each Transfer URL, the specified IP addresses will be setup automatically in "**Registrar Domain Table**".

5.3.3.2 Delecte SIP User



User Name		Domain Name	Delete
Internal	Global		
callee		192.168.1.1	□
caller		192.168.1.1	□

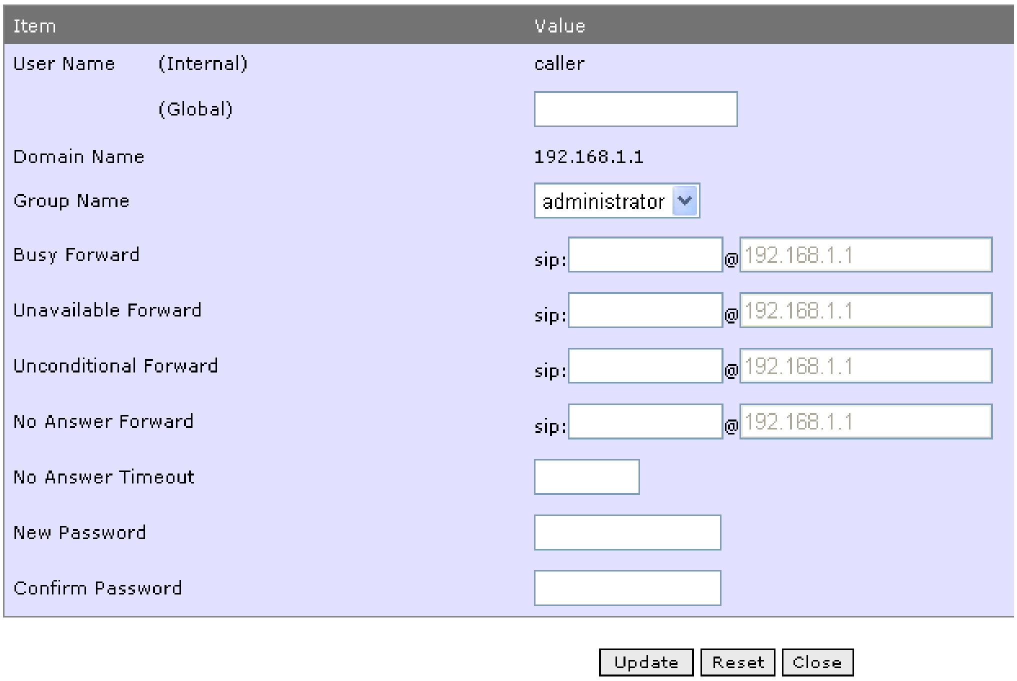
To delete:
②Click here

To delete:
①Click here

Table Editor

For delete the existing SIP user, please click "Delete" box and click "**Update**" button, it will display the result of starting message box.

5.3.3.3 Edit SIP User



Item		Value
User Name	(Internal)	caller
	(Global)	
Domain Name		192.168.1.1
Group Name		administrator
Busy Forward		sip: @ 192.168.1.1
Unavailable Forward		sip: @ 192.168.1.1
Unconditional Forward		sip: @ 192.168.1.1
No Answer Forward		sip: @ 192.168.1.1
No Answer Timeout		
New Password		
Confirm Password		

Table Editor

Enter the following information in Table Editor, and click "**Update**" button to display the result.

User Name (Global)
Specify the external number of the user.

Group Name
Specify the group name of the user.

Busy Forward
Enter the SIP URL of Busy forward (Busy transfer).

Unavailable Forward
Enter the SIP URL of Unavailable forward (Unavailable transfer).

Unconditional Forward
Enter the SIP URL of Unconditional forward (Unconditional transfer).

No Answer Forward
Enter the SIP URL of No answer forward (No Answer transfer).

No Answer Timeout
Setup the default value of No answer (1~999 secs.)

New Password
Enter the new password.

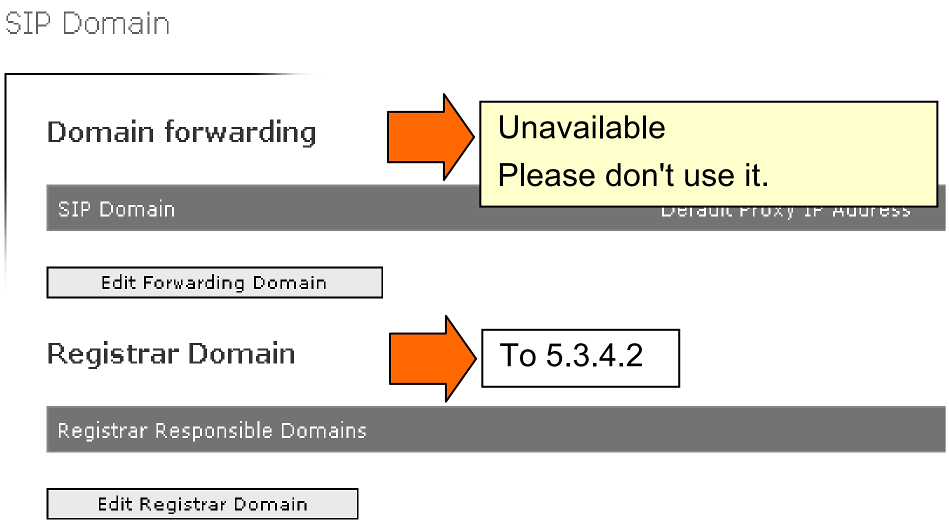
Confirm Password
Enter the new password again.

Caution

Regarding to "**Domain Name**" and "**@xxx**" of each Transfer URL, the specified IP addresses will be setup automatically in "**Registrar Domain Table**".•

5.3.4 SIP Domain

Please click "**SIP Domain**" from "**5.3 SIP Configuration**" menu displayed on the left side of the screen. It will display as below.



SIP Domain

Domain forwarding

Unavailable
Please don't use it.

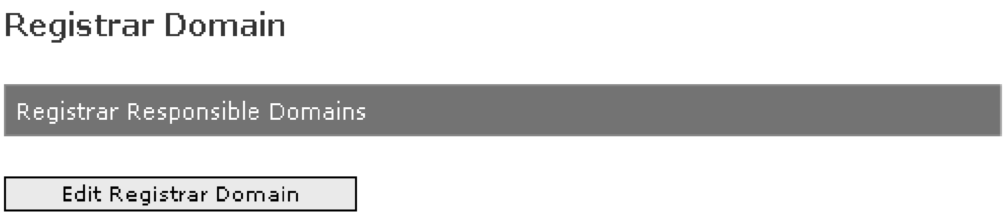
Registrar Domain

To 5.3.4.2

5.3.4.1 Domain forwarding

This device doesn't support this information. Please do not use it.

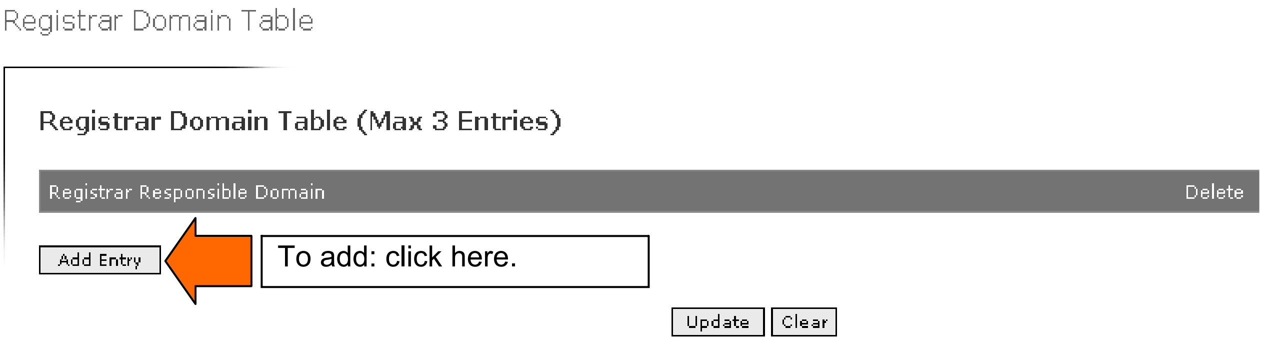
5.3.4.1 Registrar Domain


Registrar Domain

Registrar Responsible Domains

Registrar Domain

Display the current Registrar Domain name of this device.
This device can use a maximum of 3 Registrar domains.


Registrar Domain Table

Registrar Domain Table (Max 3 Entries)

Registrar Responsible Domain	Delete

To add: click here.

Registrar Domain Table

If clicking "**Add Entry**" button, the window for adding Registrar Domain will pop up. If you want to delete Registrar Domain name, please click "**Delete**" box and click "**Update**" button.

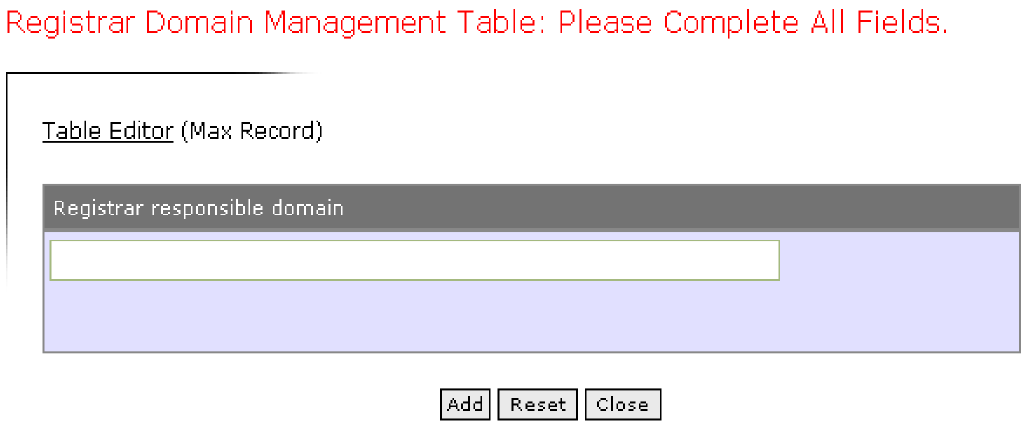

Registrar Domain Management Table: Please Complete All Fields.

Table Editor (Max Record)

Registrar responsible domain

Registrar responsible domain

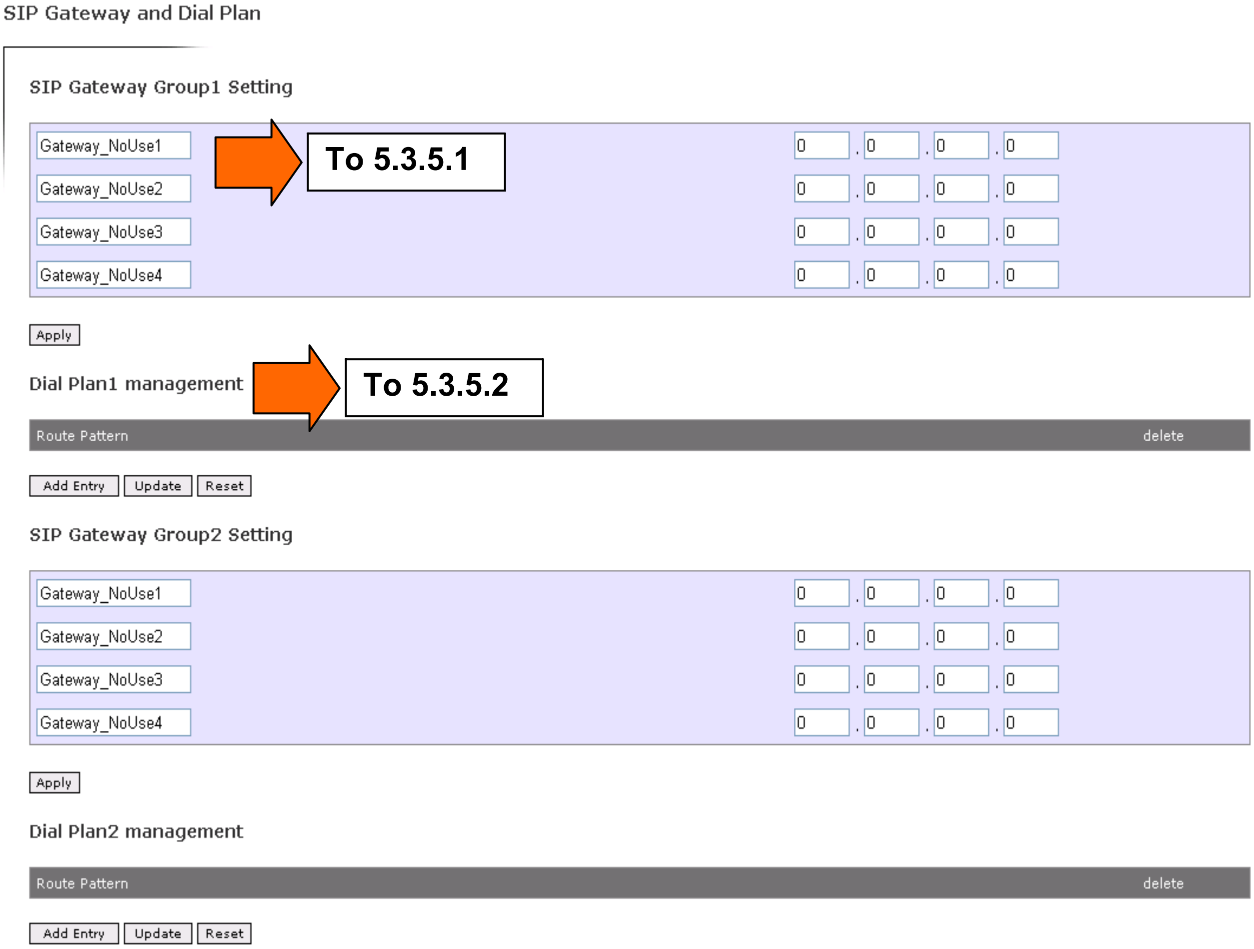
Please enter the IP address in Registrar domain.
After entering Registrar domain in Table Editor, please click "**Add**" button.

Caution

Please enter the "**LAN IP Address**" value of **Server Mode** in "**Registrar Domain Table**". (Although you can enter up to 3, please note that only the first one is effective.)

5.3.5 SIP Gateway

Please click "**SIP Gateway**" from "**5.3 SIP Configuration**" menu displayed on the left side of the screen. It will display as below.



SIP Gateway and Dial Plan

SIP Gateway Group1 Setting

Gateway_NoUse1	0	0	0	0
Gateway_NoUse2	0	0	0	0
Gateway_NoUse3	0	0	0	0
Gateway_NoUse4	0	0	0	0

To 5.3.5.1

Dial Plan1 management

To 5.3.5.2

Route Pattern	delete

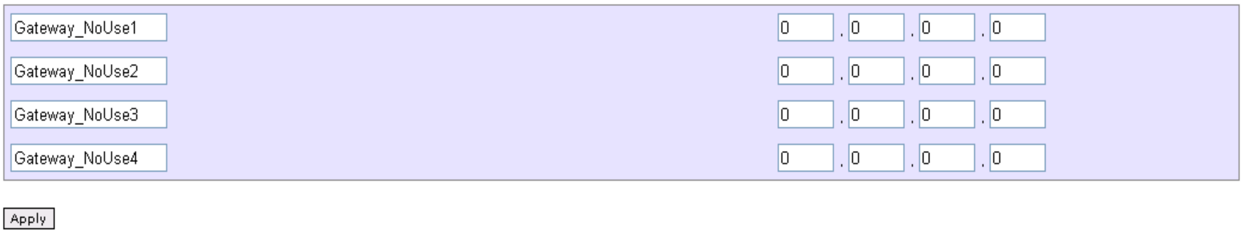
SIP Gateway Group2 Setting

Gateway_NoUse1	0	0	0	0
Gateway_NoUse2	0	0	0	0
Gateway_NoUse3	0	0	0	0
Gateway_NoUse4	0	0	0	0

Dial Plan2 management

Route Pattern	delete

5.3.5.1 SIP Gateway Group Setting



Gateway_NoUse1	0	0	0	0
Gateway_NoUse2	0	0	0	0
Gateway_NoUse3	0	0	0	0
Gateway_NoUse4	0	0	0	0

Enter the Gateway name in the left side (as the box of Gateway_NoUse1~Gateway_NoUse4), The maximum of entries are 1~8 letters.

Setup the IP address of SIP VoIP Gateway in the right side.

If setup 0.0.0.0, SIP Gateway will be invaild.

One group can accept up to 4 Gateway IP addresses.

But the maximum of groups are two.

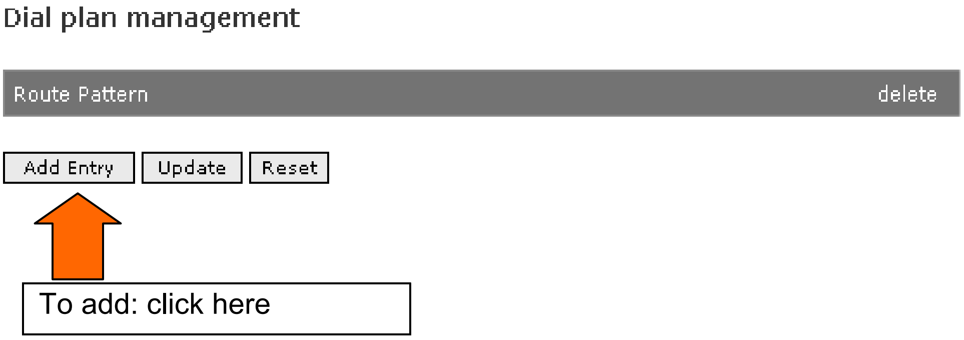
Apply

If clicking this button, the configuration of this SIP Gateway Group will be saved.

Caution

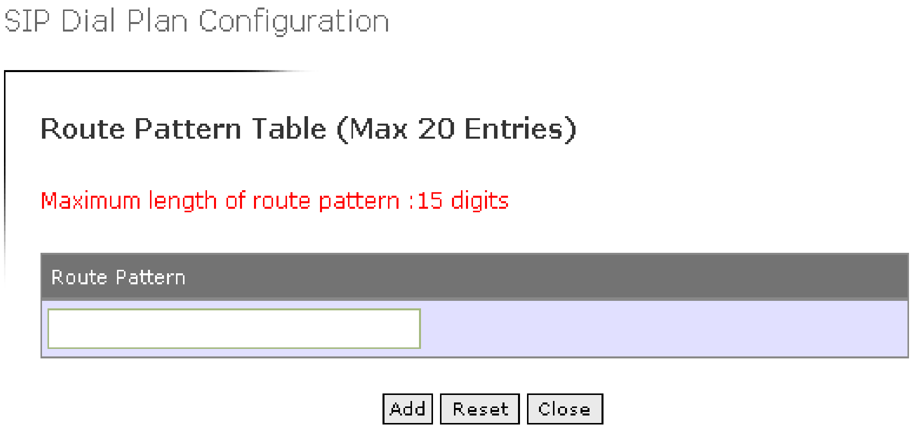
Please click the "**Apply**" buttons of **Group1/Group2** apart. For example, If you want to change the content of **Group1** but click the "**Apply**" button of **Group2**, the content of **Group 1** will be lost.

5.3.5.2 Dial plan management



Dial plan management

The caller number which is the same with the route pattern will be transferred to the SIP Gateway IP address setup in "**5.3.5.1 SIP Gateway Group Setting**".
Please setup each group apart.


SIP Dial Plan Configuration
Route Pattern Table (Max 20 Entries)
Maximum length of route pattern :15 digits
Route Pattern
Add
Reset
Close

Route Pattern Table

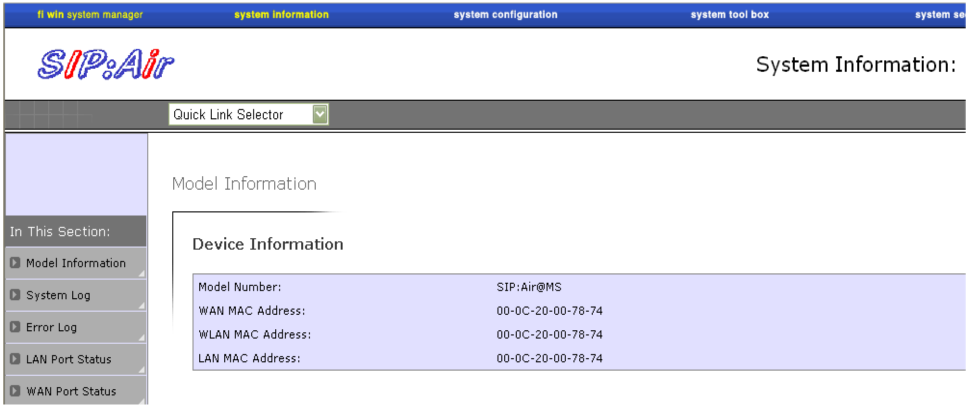
The route pattern table can be entered up to 20 entries.
Maximum length of route pattern is 15 digits.
A wild card letter can be used for a setup of a route pattern.(ex:03*)
After entering the callee number and click "**Add**" button.

6 Ensure the status of device

6.1 System Information

Please click "**system information**" in the menu displayed on upper side of the screen.
(The "**system information**" will reverse to yellow after selection).
It will display as below.

Please click system information

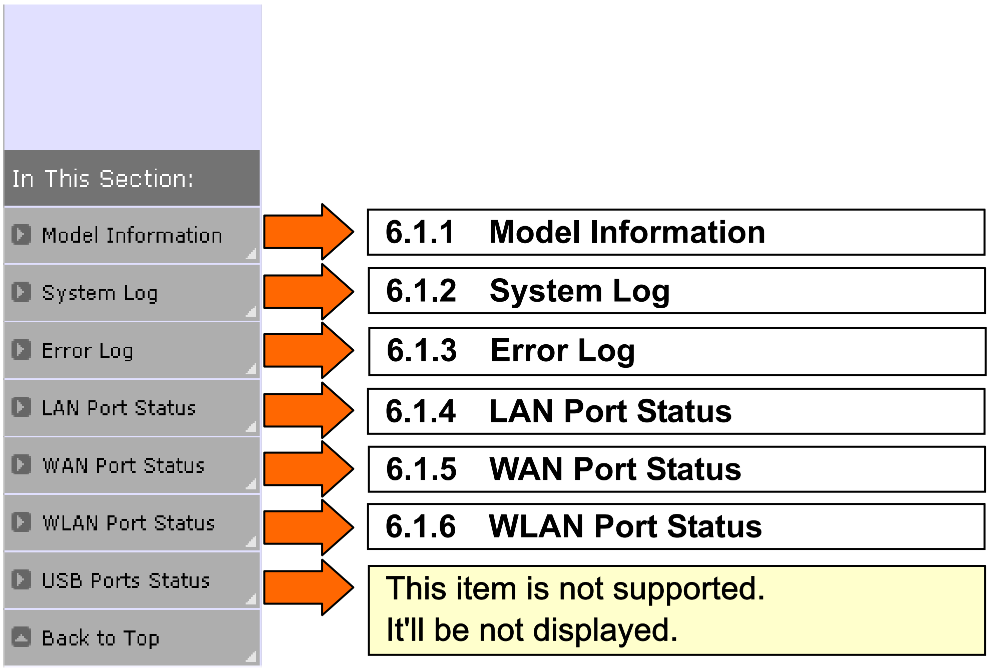


System Information:

Model Information

Device Information

Model Number:	SIP:Air@MS
WAN MAC Address:	00-0C-20-00-78-74
WLAN MAC Address:	00-0C-20-00-78-74
LAN MAC Address:	00-0C-20-00-78-74



6.1.1 Model Information

6.1.2 System Log

6.1.3 Error Log

6.1.4 LAN Port Status

6.1.5 WAN Port Status

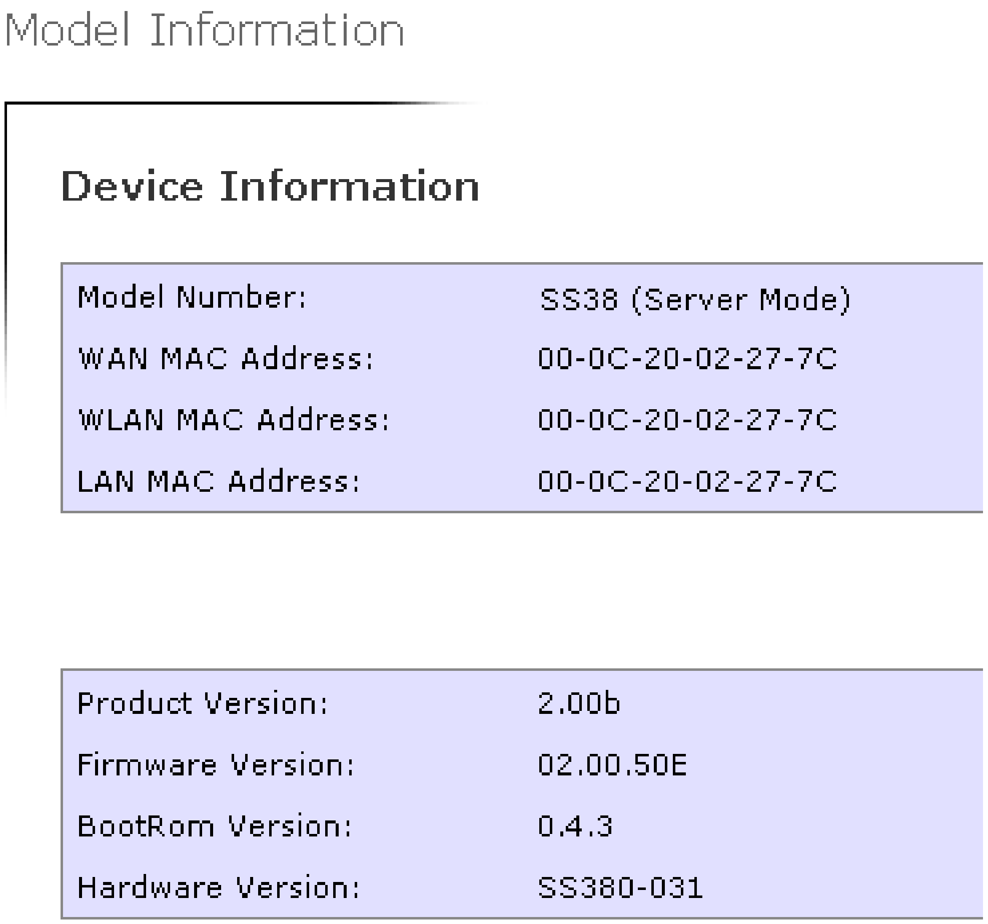
6.1.6 WLAN Port Status

This item is not supported.
It'll be not displayed.

6.1.1 Model Information

Please click "**Model Information**" from "**6.1 System Information**" menu displayed on the left side of the screen. It will display as below.

Model Information will display the following version information of this device:



Model Information

Device Information

Model Number:	SS38 (Server Mode)
WAN MAC Address:	00-0C-20-02-27-7C
WLAN MAC Address:	00-0C-20-02-27-7C
LAN MAC Address:	00-0C-20-02-27-7C

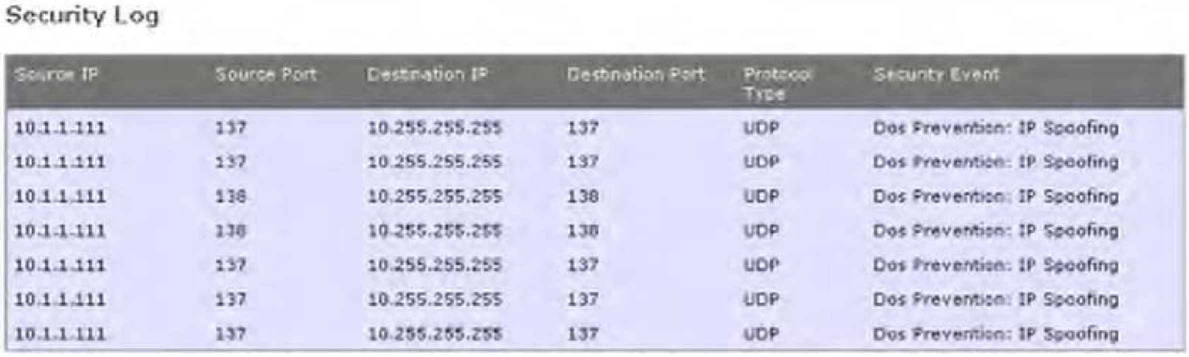
Product Version:	2.00b
Firmware Version:	02.00.50E
BootRom Version:	0.4.3
Hardware Version:	SS380-031

6.1.2 System Log

Please click "**System Log**" from "**6.1 System Information**" menu displayed on the left side of the screen.

(1) Security Log

It will display the result of detected security disturbance or the security attack here.
(Max 200 items)



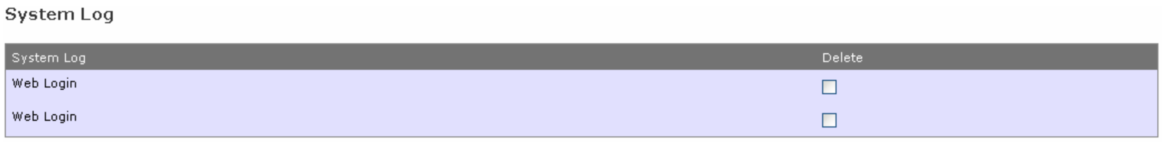
Security Log

Source IP	Source Port	Destination IP	Destination Port	Protocol Type	Security Event
10.1.1.111	137	10.255.255.255	137	UDP	Dos Prevention: IP Spoofing
10.1.1.111	137	10.255.255.255	137	UDP	Dos Prevention: IP Spoofing
10.1.1.111	138	10.255.255.255	138	UDP	Dos Prevention: IP Spoofing
10.1.1.111	138	10.255.255.255	138	UDP	Dos Prevention: IP Spoofing
10.1.1.111	137	10.255.255.255	137	UDP	Dos Prevention: IP Spoofing
10.1.1.111	137	10.255.255.255	137	UDP	Dos Prevention: IP Spoofing
10.1.1.111	137	10.255.255.255	137	UDP	Dos Prevention: IP Spoofing

Source IP	
Source Port	
Destination IP	
Destination Port	
Protocol Type	Destination Port (TCP/UDP) or Message type (ICMP)
Security Event	The content of event

(2) System Log

It will display the system event, system error, and system security log here.
(Max 200 items)



System Log

System Log	Delete
Web Login	□
Web Login	□

MEMO

Regarding to the log information

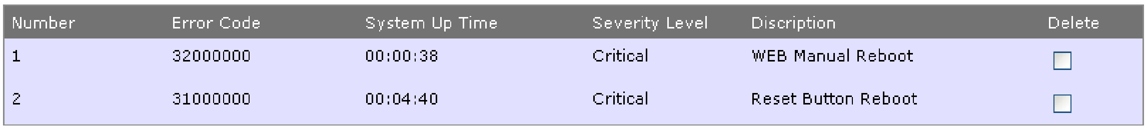
If the maximum numbers of item are exceeded, it will be deleted from the oldest log and new events will be registered.
If the device is rebooted, System Log and Security Log will be all deleted

Regarding to the displayed information of **Security Log** & **System Log**, please refer to "**8.2 Log Summary**".

6.1.3 Error Log

Please click "Error Log" from "6.1 System Information" menu displayed on the left side of the screen.

It will display events which pressed the reset button and then rebooted, and events of a system error here. (Max 100 items)



Number	Error Code	System Up Time	Severity Level	Discription	Delete
1	32000000	00:00:38	Critical	WEB Manual Reboot	□
2	31000000	00:04:40	Critical	Reset Button Reboot	□

MEMO

Regarding to the log information

If the maximum numbers of items are exceeded, it will be deleted from the oldest log and new events will be registered.

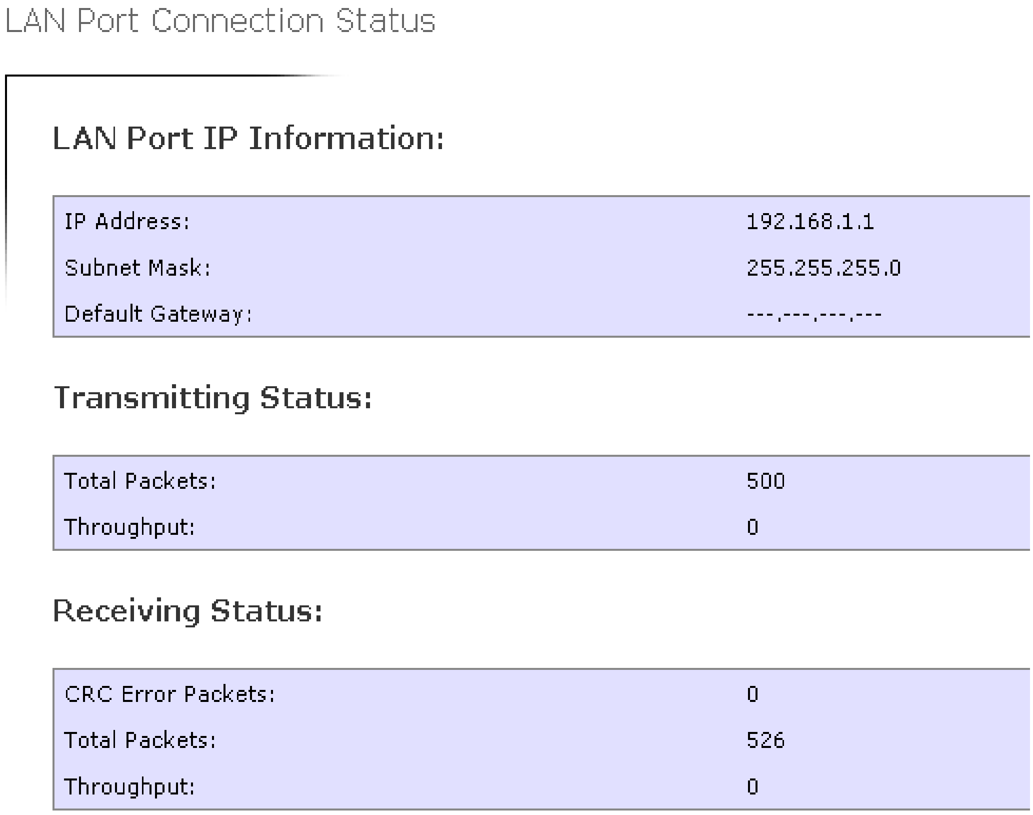
Even if the device is rebooted, Error Log will not be deleted.

Regarding to the displayed information of **Error Log**, please refer to "**8.2 Log Summary**".

6.1.4 LAN Port Status

Please click "**LAN Port Status**" from "6.1 System Information" menu displayed on the left side of the screen.

It will display the following connecting status of LAN port.



LAN Port Connection Status

LAN Port IP Information:

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	---.---.---.---

Transmitting Status:

Total Packets:	500
Throughput:	0

Receiving Status:

CRC Error Packets:	0
Total Packets:	526
Throughput:	0

LAN Port IP Information

Display the LAN Port IP address, Subnet Mask and Gateway IP Address.

Transmitting Status

Display the numbers of current transmitting packets and the throughput.

Receiving Status

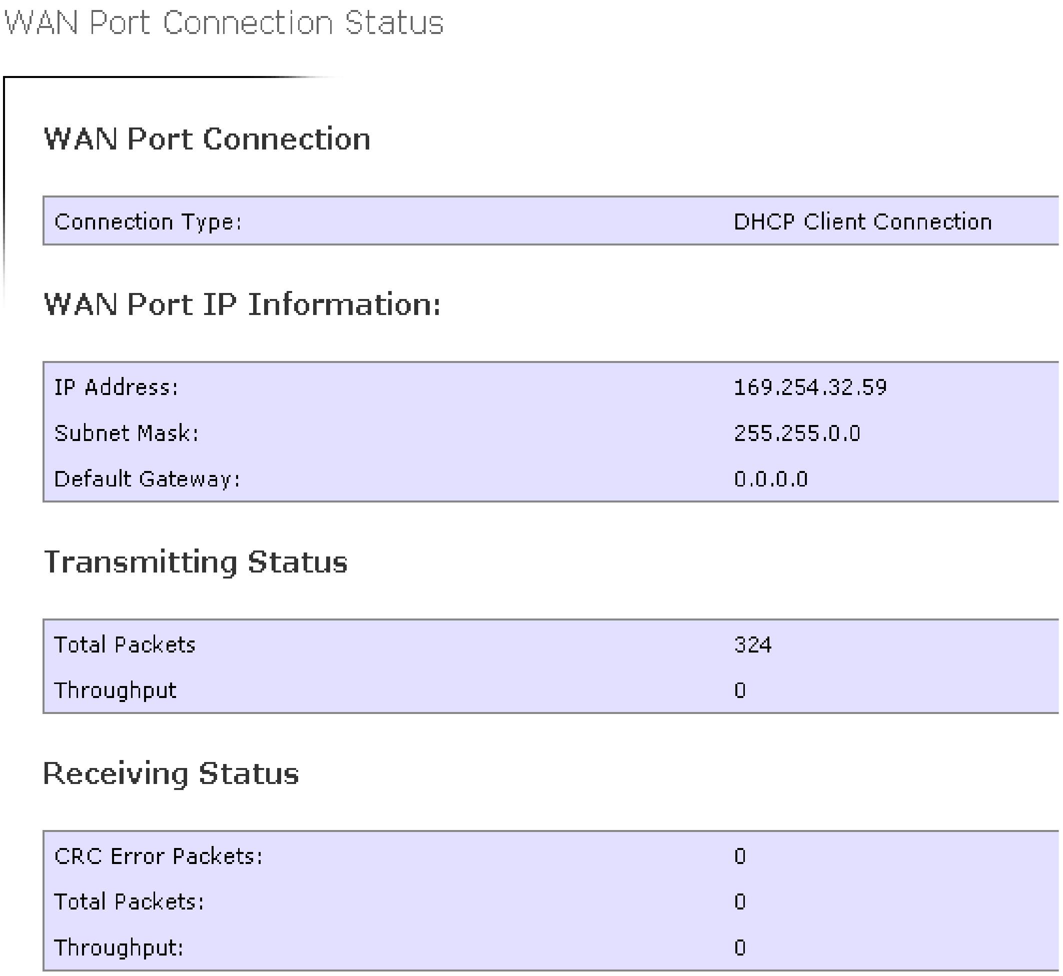
Display the numbers of current receiving packets and the throughput.

6.1.5 WAN Port Status

~~AP~~

Please click "**WAN Port Status**" from "6.1 System Information" menu displayed on the left side of the screen.

It will display the following connecting status of WAN Port.



WAN Port Connection Status

WAN Port Connection

Connection Type:	DHCP Client Connection

WAN Port IP Information:

IP Address:	169.254.32.59
Subnet Mask:	255.255.0.0
Default Gateway:	0.0.0.0

Transmitting Status

Total Packets	324
Throughput	0

Receiving Status

CRC Error Packets:	0
Total Packets:	0
Throughput:	0

WAN Port Connection

Regarding to current WAN Port connection, it will display as following messages.

(1) DHCP Client Connection
(2) Manual IP Connection
(3) PPPoE Dialing Connection

WAN Port IP Information

Display the current WAN Port IP address, Subnet Mask and Gateway IP Address.

Transmitting Status

Display the numbers of current transmitting packets and the throughput of WAN Port.

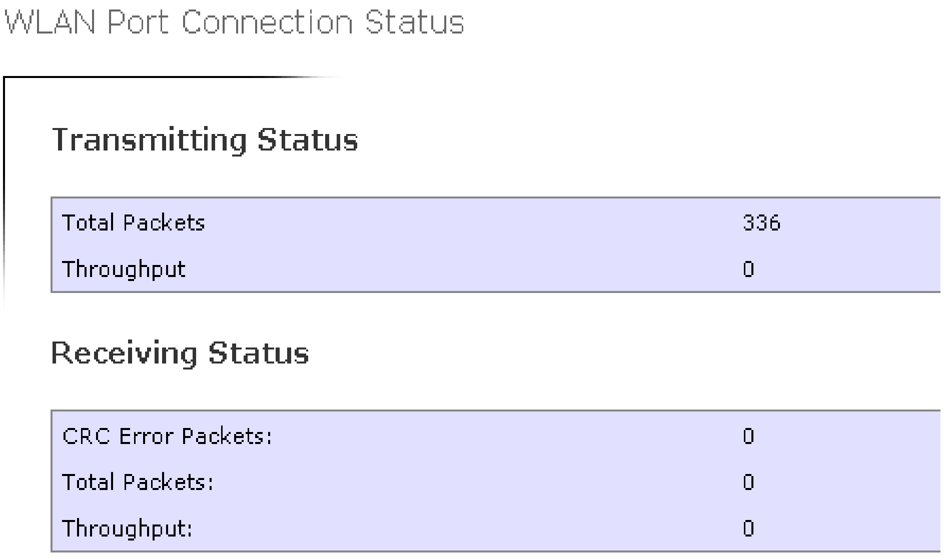
Receiving Status

Display the numbers of current receiving packets and the throughput of WAN Port.

6.1.6 WLAN Port Status

Please click "**WLAN Port Status**" from "6.1 System Information" menu displayed on the left side of the screen.

It will display the following connecting status of WLAN Port.



WLAN Port Connection Status

Transmitting Status

Total Packets	336
Throughput	0

Receiving Status

CRC Error Packets:	0
Total Packets:	0
Throughput:	0

Transmitting Status

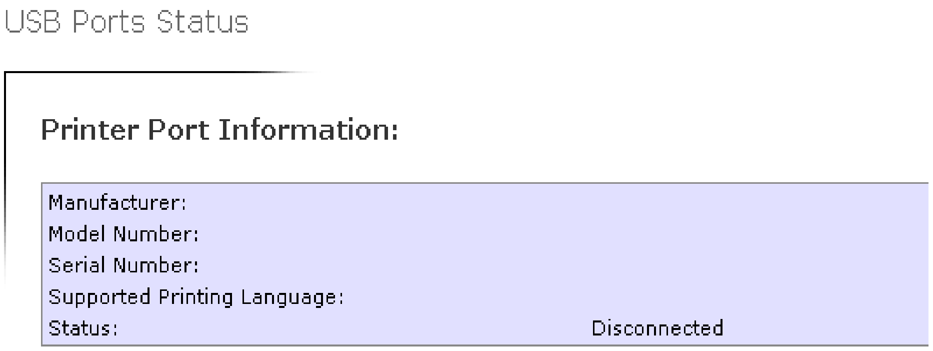
Display the numbers of current transmitting packets and the throughput of WLAN Port.

Receiving Status

Display the numbers of current receiving packets and the throughput of WLAN Port.

6.1.7 USB Port Status

This function is not supported yet. The information will not be displayed.



USB Ports Status

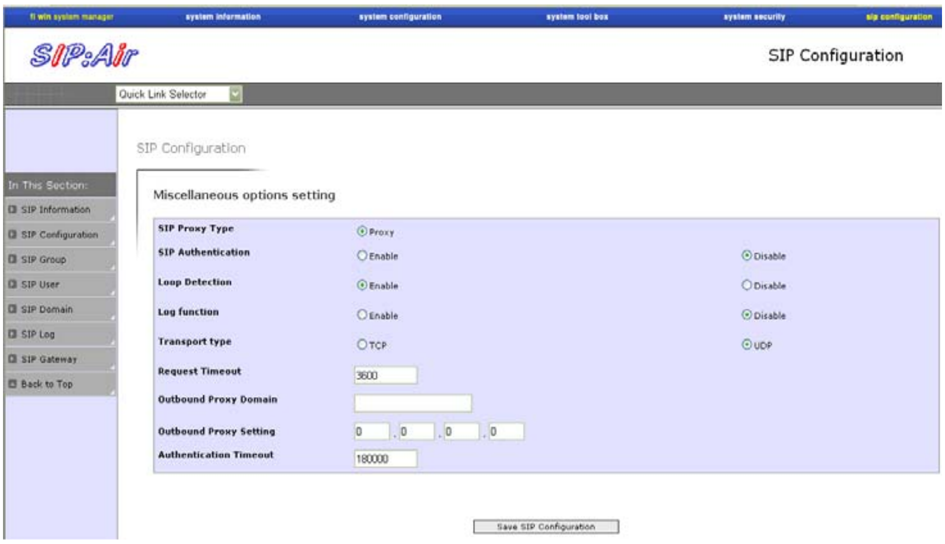
Printer Port Information:

Manufacturer:	
Model Number:	
Serial Number:	
Supported Printing Language:	
Status:	Disconnected

6.2 SIP Configuration

Please click "**sip configuration**" in the menu displayed on upper side of the screen.
(The "**sip configuration**" will reverse to yellow after selection).
It will display as below.

Please click SIP configuration



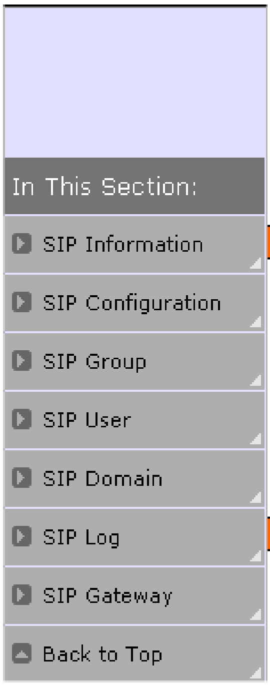
SIP Configuration

Miscellaneous options setting

SIP Proxy Type	● Proxy	
SIP Authentication	○ Enable	● Disable
Loop Detection	● Enable	○ Disable
Log function	○ Enable	● Disable
Transport type	○ TCP	● UDP
Request Timeout	3600	
Outbound Proxy Domain		
Outbound Proxy Setting	0 . 0 . 0 . 0	
Authentication Timeout	180000	

Then, please choose the menu arbitrarily displayed on "**In This Selection**".
Please refer to the following explanation for operations as below.

Moreover, since it is a system configuration menu except "**SIP Information**" and "**SIP Log**", please refer to "**5 Setup the device**".



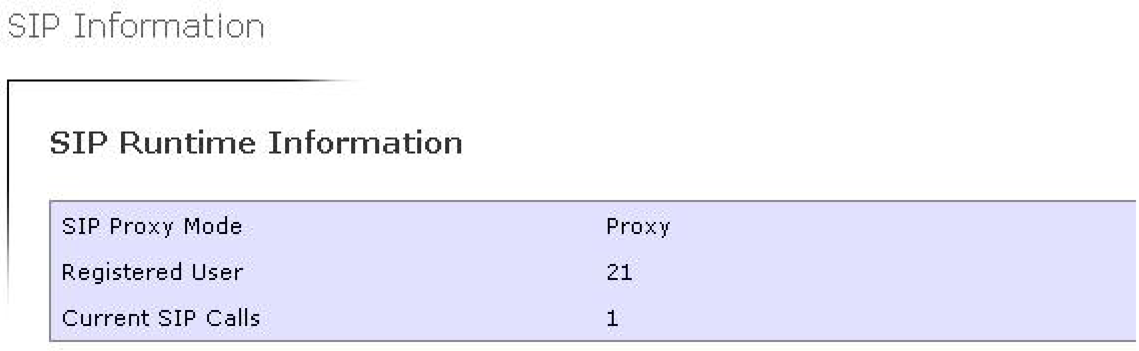
To 6.2.1 SIP Information

To 6.2.2 SIP Log

6.2.1 SIP Information

Please click "**SIP Information**" from "6.1 System Information" menu displayed on the left side of the screen.

It will display the following information of SIP Proxy server.



SIP Information

SIP Runtime Information

SIP Proxy Mode	Proxy
Registered User	21
Current SIP Calls	1

SIP Runtime Information

Display the information of SIP Proxy Mode, the number of registrars and current SIP Session.

SIP Registered User Information

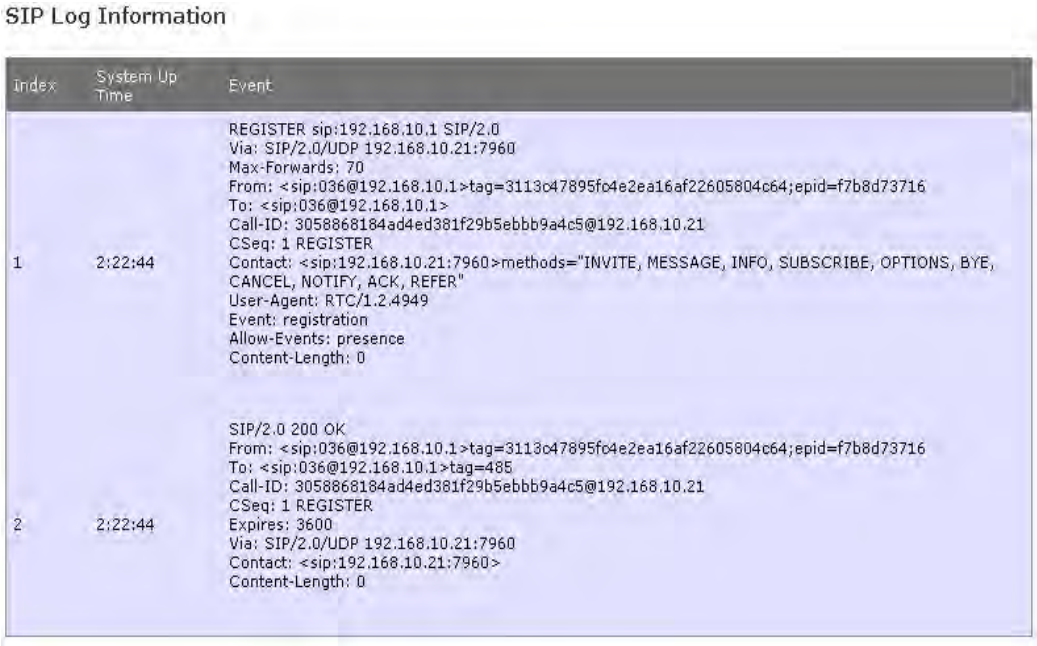
Display the detailed information of current registered users.

SIP Session Information

Display the detailed information of current SIP session.

6.2.2 SIP Log

Please click "**SIP Log**" from "**6.1 System Information**" menu displayed on the left side of the screen.



SIP Log Information

Index	System Up Time	Event
1	2:22:44	REGISTER sip:192.168.10.1 SIP/2.0 Via: SIP/2.0/UDP 192.168.10.21:7960 Max-Forwards: 70 From: <sip:036@192.168.10.1>tag=3113c47895fc4e2ea16af22605804c64;epid=f7b8d73716 To: <sip:036@192.168.10.1> Call-ID: 3058868184ad4ed381f29b5ebbb9a4c5@192.168.10.21 CSeq: 1 REGISTER Contact: <sip:192.168.10.21:7960>methods="INVITE, MESSAGE, INFO, SUBSCRIBE, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER" User-Agent: RTC/1.2.4949 Event: registration Allow-Events: presence Content-Length: 0
2	2:22:44	SIP/2.0 200 OK From: <sip:036@192.168.10.1>tag=3113c47895fc4e2ea16af22605804c64;epid=f7b8d73716 To: <sip:036@192.168.10.1>tag=485 Call-ID: 3058868184ad4ed381f29b5ebbb9a4c5@192.168.10.21 CSeq: 1 REGISTER Expires: 3600 Via: SIP/2.0/UDP 192.168.10.21:7960 Contact: <sip:192.168.10.21:7960> Content-Length: 0

If setting Log function as Enable in SIP Configuration, SIP message of SIP Proxy server will be displayed.

(Max 100 items)

MEMO

Regarding to the log information

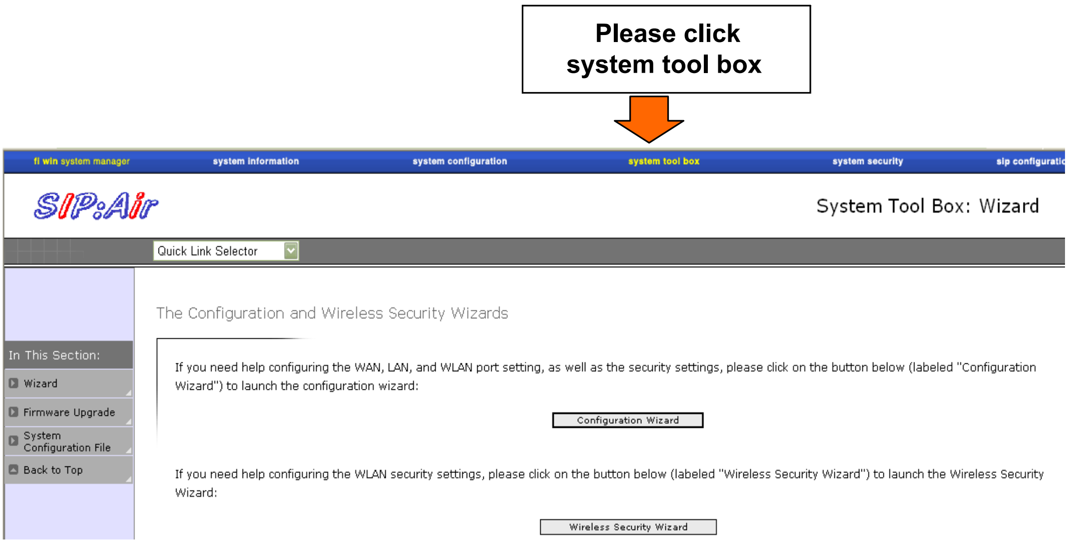
If the maximum numbers of items are exceeded, it will be deleted from the oldest log and new events will be registered.
If the device is rebooted, System Log will be all deleted.

Regarding to the confifuration of Log Function,
please refer to "**5.3.1 SIP Configuration**".

7 Maintenance

7.1 System Tool Box

Please click "**system tool box**" in the menu displayed on upper side of the screen.
(The "**system tool box**" will reverse to yellow after selection).
It will display as below.



Please click system tool box

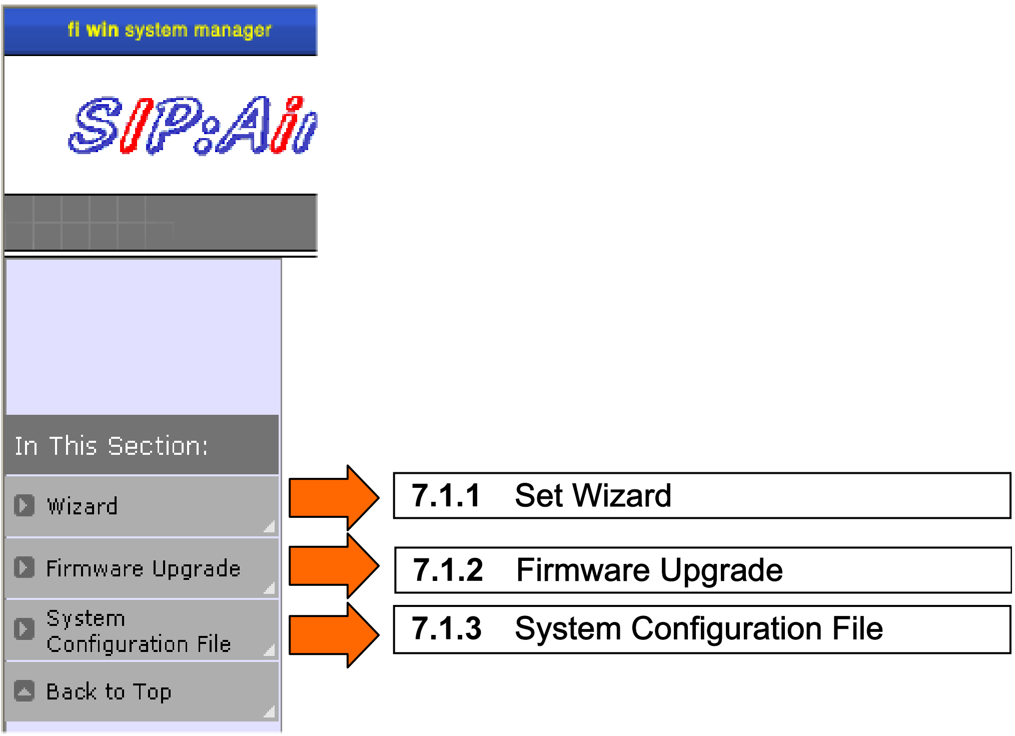
System Tool Box: Wizard

The Configuration and Wireless Security Wizards

If you need help configuring the WAN, LAN, and WLAN port setting, as well as the security settings, please click on the button below (labeled "Configuration Wizard") to launch the configuration wizard:

If you need help configuring the WLAN security settings, please click on the button below (labeled "Wireless Security Wizard") to launch the Wireless Security Wizard:

Then, please choose the menu arbitrarily displayed on "**In This Selection**".
Please refer to the following explanation for operations as below.



7.1.1 Set Wizard

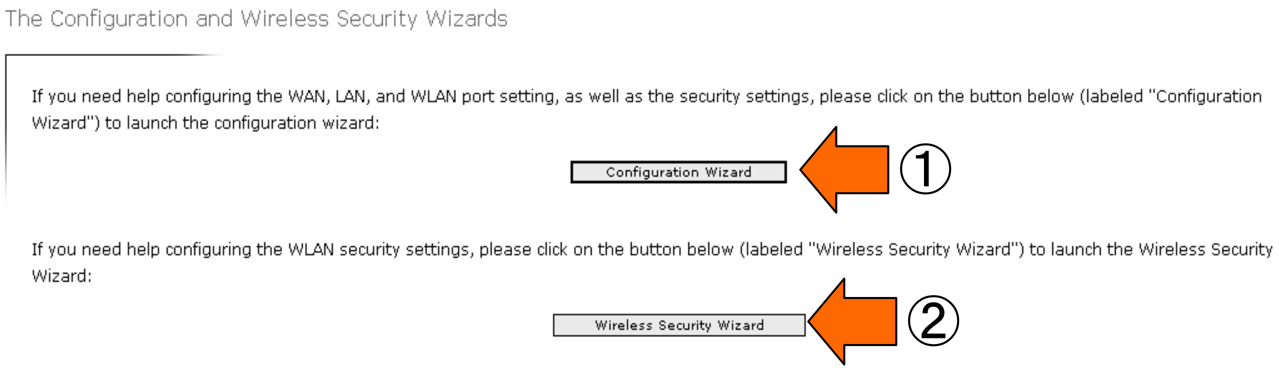
7.1.2 Firmware Upgrade

7.1.3 System Configuration File

7.1.1 Set Wizard

7.1.1.1 SS38 (Server Mode)

Please click "**Wizard**" from the menu displayed on the left side of the screen.



The Configuration and Wireless Security Wizards

If you need help configuring the WAN, LAN, and WLAN port setting, as well as the security settings, please click on the button below (labeled "Configuration Wizard") to launch the configuration wizard:

If you need help configuring the WLAN security settings, please click on the button below (labeled "Wireless Security Wizard") to launch the Wireless Security Wizard:

Configuration Wizard (as the ①)

WAN, LAN, and WLAN can be setup according to the guide.

Regarding to the detailed configuration,
please refer to "**5.1 System Configuration**".

Wireless Security Wizard (as the ②)

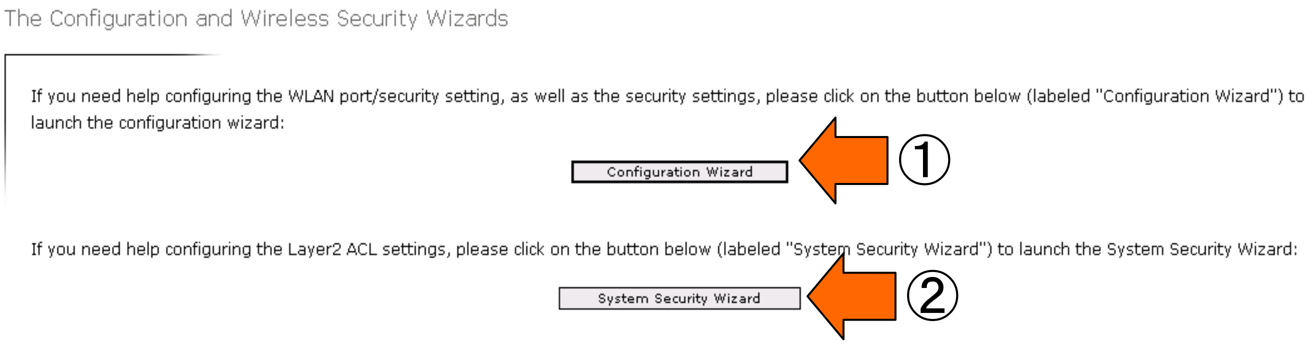
WLAN security can be setup according to the guide.

You can setup from Main menu -> System Configuration -> Wireless LAN Setting ->Advance Security Setting.

Regarding to detailed configuration,
please refer to "**5.1.4.2 WLAN Advance Security**".

7.1.1.2 SS38 (AP Mode)

Please click "**Wizard**" from the "**7.1 System Tool Box**" menu displayed on the left side of the screen.



The Configuration and Wireless Security Wizards

If you need help configuring the WLAN port/security setting, as well as the security settings, please click on the button below (labeled "Configuration Wizard") to launch the configuration wizard:

If you need help configuring the Layer2 ACL settings, please click on the button below (labeled "System Security Wizard") to launch the System Security Wizard:

Configuration Wizard (as the ①)

WLAN can be setup according to the guide.

If clicking "**Next**", WLAN security setting screen will be displayed.

After setting, please click "**Finish**" to return to the screen as above.

> ☞ Regarding to the detailed configuration,
> please refer to "**5.1.4 WLAN Port Settings**".

System Security Wizard (as the ②)

L2 ACL can be setup according to the guide.

After setting, please click "**Finish**" to return to the screen as above.

> ☞ Regarding to the detailed configuration,
> please refer to "**5.2.1.2 L2 ACL**".

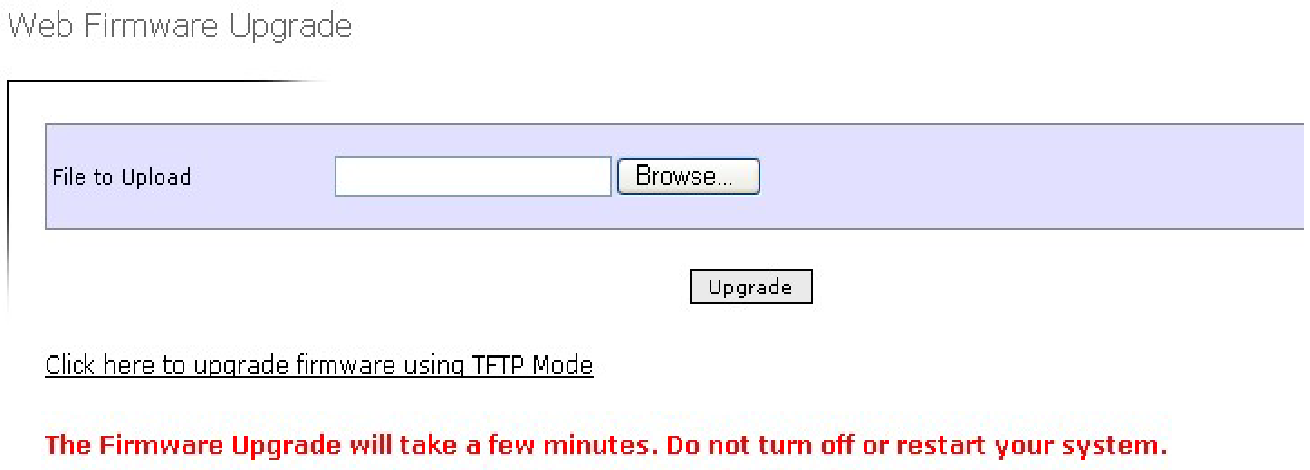
7.1.2 Firmware Upgrade

Please click "**Firmware Upgrade**" from the "**7.1 System Tool Box**" menu displayed on the left side of the screen.

There are the following two methods of upgrading firmware of this device.

7.1.2.1 File to Upload

The newest firmware file can be uploaded via PC.
Please press the " **Browse** " button to select the file to upload the firmware.



Web Firmware Upgrade

File to Upload

The Firmware Upgrade will take a few minutes. Do not turn off or restart your system.

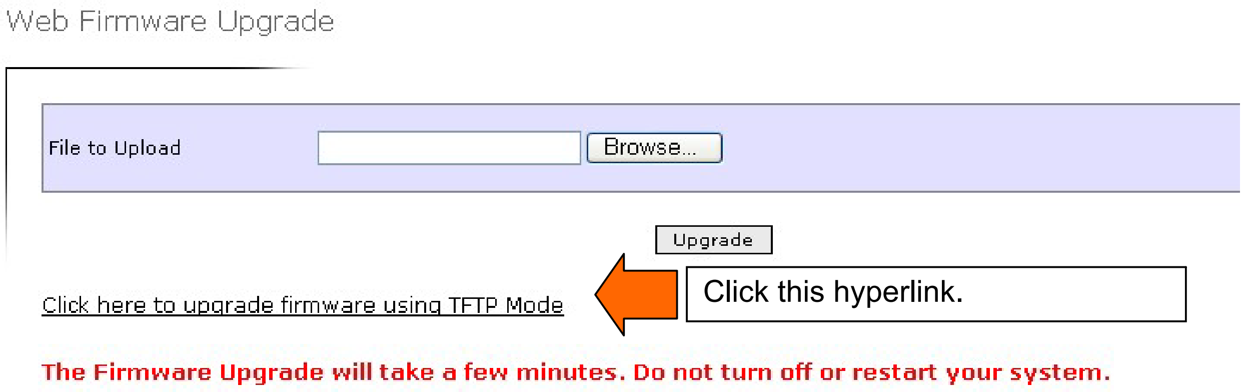
After selecting the file, please press "**Upgrade**" button.

Caution

After uploading, the screen which is needed to reboot will be displayed. Please press "Reboot" button to restart the device.

7.1.2.2 TFTP Firmware Upgrade

The firmware can be update to the newest version by using TFTP.
Please click the hyperlink (Click here to upgrade firmware using TFTP Mode) in "**7.1.2.1 File to Upload**".



Web Firmware Upgrade

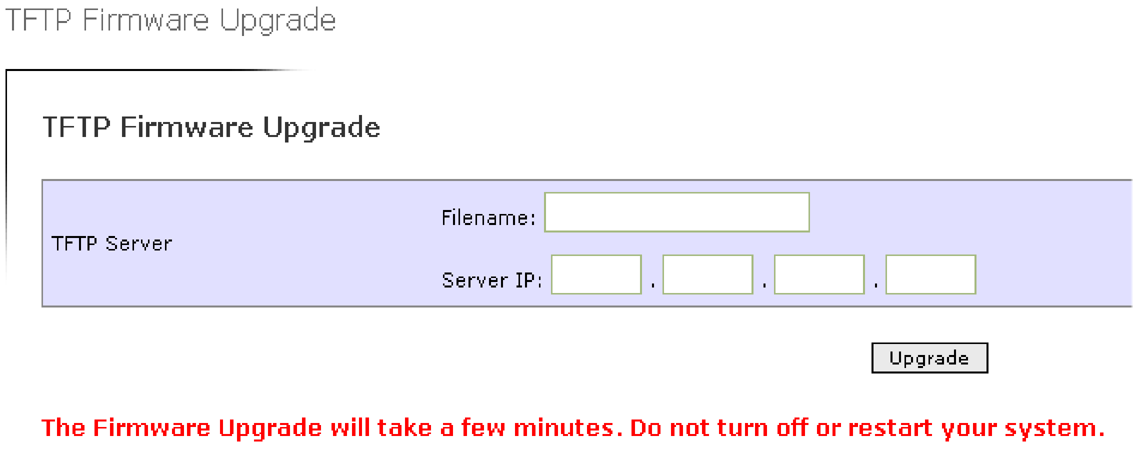
File to Upload

Click here to upgrade firmware using TFTP Mode

Click this hyperlink.

The Firmware Upgrade will take a few minutes. Do not turn off or restart your system.

Please enter the file name of the firmware, and the IP address of TFTP server.



TFTP Firmware Upgrade

TFTP Firmware Upgrade

TFTP Server

Filename:

Server IP: . . .

The Firmware Upgrade will take a few minutes. Do not turn off or restart your system.

Please press "**Upgrade**" after entering.

Caution

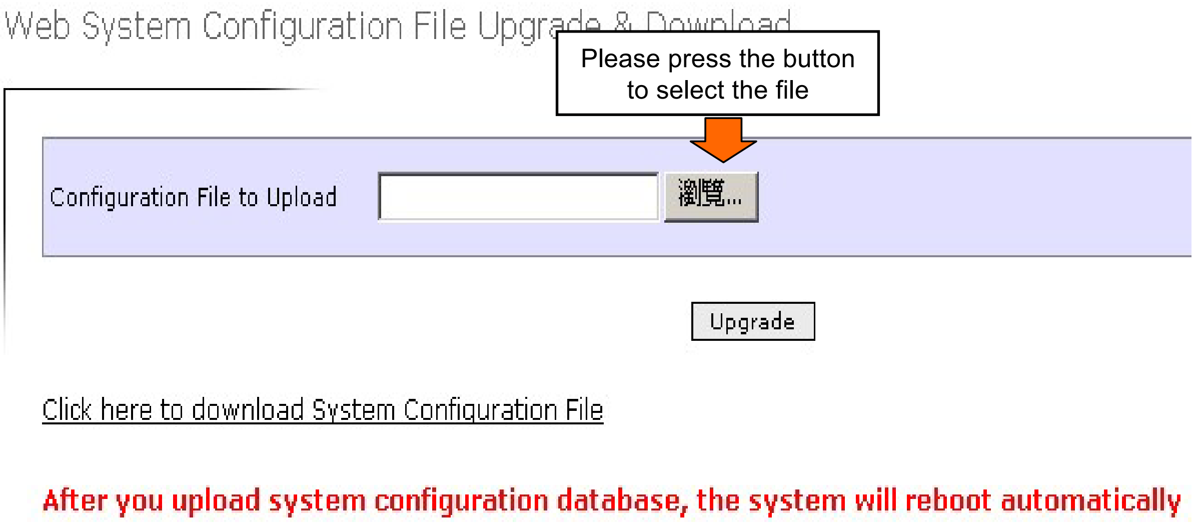
Please prepare a TFTP server if you want to perform TFTP Firmware Upgrade.

7.1.3 Upload & Download Device Summary

Please click "**System Configuration File**" from "**7.1 System Tool Box**" menu displayed on the left side of the screen.

7.1.3.1 Configuration File to Upload

The newest configuration file can be uploaded via PC.
Please press the " **Browse** " button to select the file to upload the configuration.



Web System Configuration File Upgrade & Download

Configuration File to Upload

Please press the button to select the file

After you upload system configuration database, the system will reboot automatically

After selecting the file, please press" **Upgrade** "buttom.

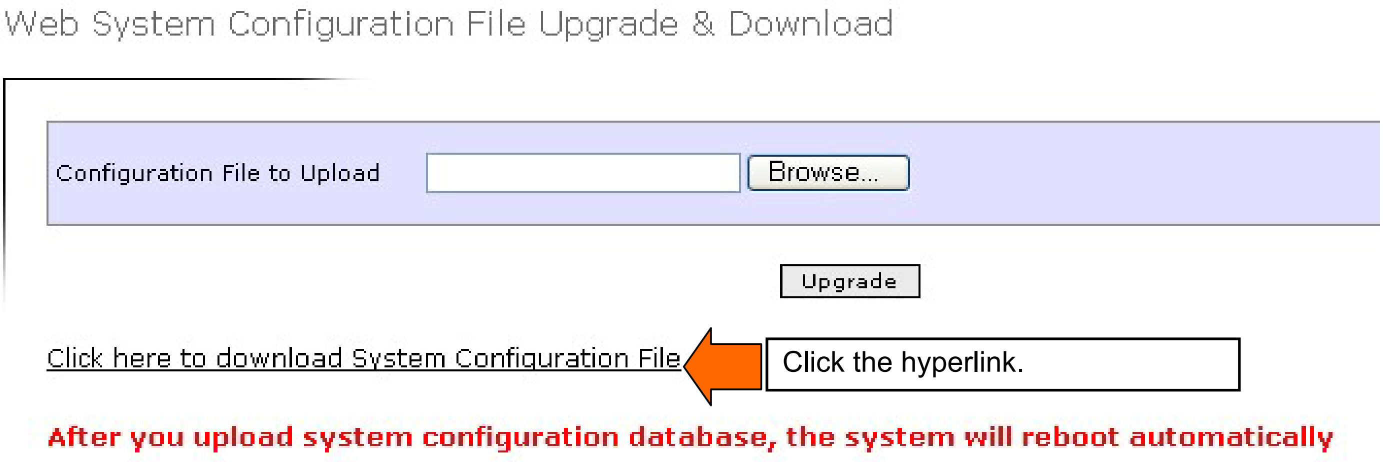
Caution

After the uploading, the dervcie will reboot automatically.

7.1.3.2 Download System Configuration File

The system configuration file of this device can be downloaded and saved in PC.

Please click the hyperlink to download in the screen of "**7.1.3.1 Configuration File to Upload**"
(Click here to download System Configuration File)
Please follow the displayed message.



Web System Configuration File Upgrade & Download

Configuration File to Upload

Click the hyperlink.

After you upload system configuration database, the system will reboot automatically

8 Troubleshooting

8.1 Troubleshooting

8.1.1 Can not access the setting utilities ?

Ensure the configuration of WWW browser.

Please check if WWW browser is setup as "Do not connect via Proxy".

Ensure the connection with this device

Please check if the PC can transmit PING to the device.
Enter [**Start**] -> [**Programs**] -> [**Accessories**] -> [**Command prompt**], and enter "ping 192.168.1.1" (*1)(Please enter from [**Start**] -> [**Programs**] -> [**MS-DOS prompt**] according to the operation system.)

(*1) 192.168.1.1 is the default value of LAN IP address.
Please enter the address when changing.

If no respond, please check if LAN LED is light on and LAN cable is connected ready.

If LAN LED is off, please ensure the cable which is connecting to Ethernet is plugged into the device.

Ensure the configuration of the device and PC

If it still can't connect to the network, please ensure if the subnet of PC is the same with this device. When the PC is setup as a DHCP client to acquire the IP automatically, please assign the fixed IP address of the same network as this device to the PC, and confirm that the DHCP server of the device is effective (Enable).

8.1.2 Forget Password ?

If you forget the password, please reset the configuration to the default value.

Regarding to the method of reset,
please refer to "**8.1.3 How to reset default** ?".

8.1.3 How to reset default ?

If you press the reset button over 10 secs, the system will be reset to the default configuration.
Since RUN LED of the front panel will blink after 10 secs, please leave the reset button.
The device will restart.

Caution

Please note that all configuration of this device will be initialized by this operation.

8.1.4 Can not connect the Wireless LAN ?

In order to establish WirelessLAN connection, please check that the configuration of WLAN device is the same as this device.

Wireless connection mode

Please do not use this device in "11G only" mode, when there have 802.11b WLAN client.

SSID

Ensure that SSID of the wireless LAN device is the same with this device.

WLAN security configuration

Ensure that the security configuration of the WLAN device is the same with this device.

Regarding to WEP coding

Ensure if this device and the WLAN device share the same configuration of key.

Regarding to WPA-PSK

Ensure that PSK (Pre-Shared Key) configuration of WLAN device is the same with this device.

Regarding to the Authentication of 802.1x

Ensure if the WLAN device is selected from RADIUS server and both use the same algorithm.

8.2 Log Summary

8.2.1 Security Log

Security Event	Condition
Dos Prevention: IP Spoofing	When "IP Spoofing" is received
Dos Prevention: Land Attack	When "Land Attack" is received
Dos Prevention: Ping of Death	When "Ping of Death" is received
Dos Prevention: Smurf Attack Begin	When "Smurf Attack" is received
Dos Prevention: Smurf Attack End	
Dos Prevention: PING Flooding Begin	When "Ping Flood" is received
Dos Prevention: PING Flooding End	
Dos Prevention: UDP Flooding Begin	When "UDP Flood" is received
Dos Prevention: UDP Flooding End	
Packet Violating	When "Packet Violating" is received

8.2.2 System Log

System Log	Condition	Solution
Error Login	The login password is wrong	Enter the correct password
Web Login	Login to SS38.	(None)
Password Change OK	Change the login password successfully	(None)
Password Change Error	Change the login password unsuccessfully ① Old Password is wrong ② New Password and Confirm New Password are not the same	① Enter the current password ② Enter the same digits of "New Password" & "Confirm New Password"
RADIUS Server not found (for 802.1x)	① RADIUS server can not be used ② The IP address of RADIUS server is wrong - The RADIUS Server is not available - The address of RADIUS Server is not correct	① Enter the correct RADIUS server IP
PPPoE Connection OK	PPPoE connection OK	(None)
PPPoE Connection Fail	PPPoE connection Failure	Check PPPoE Parameter again
Firmware Upgrade OK	Firmware Upgrade OK	(None)
Firmware Upgrade Fail	Firmware Upgrade Failure ① Problems of the firmware ② The error generates during the file transmission	Contact with the sales representative.
Memory Allocate Fail	①SDRAM error ②Use debug	
Access Configuration Data Fail	System configuration date reading Failure from the FLASH memory	
Flash Memory Access Error	FLASH ROM error	

8.2.3 Error Log

Code	Discription	Condition	RUN LED
1000 0000	ROM(FLASH) failure	The code check error of FLASH （*1）	RUN LED off
2000 0000	RAM failure	RAM check error （*1）	RUN LED off
3000 0000	CPU watchdog reboot	System crash (WDT) （*1）	Normal
3100 0000	System manual reboot	Rebooted by the reset button	Normal
3200 0000	WEB manual reboot	Rebooted by changing the setting from web utility	Normal
4000 0000	WAN error	WAN port error （*1）	Normal
5000 0001	LAN error	LAN port 1 error （*1）	Normal
5000 0002	LAN error	LAN port 2 error （*1）	Normal
5000 0003	LAN error	LAN port 3 error （*1）	Normal
5000 0004	LAN error	LAN port 4 error （*1）	Normal
6000 0000	WLAN error	WLAN module error （*1）	Normal

（*1） The error will be detected by the function when starting.

FEDERAL COMMUNICATIONS 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 or more 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.

CAUTION:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the 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.

RF exposure warning ·

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.