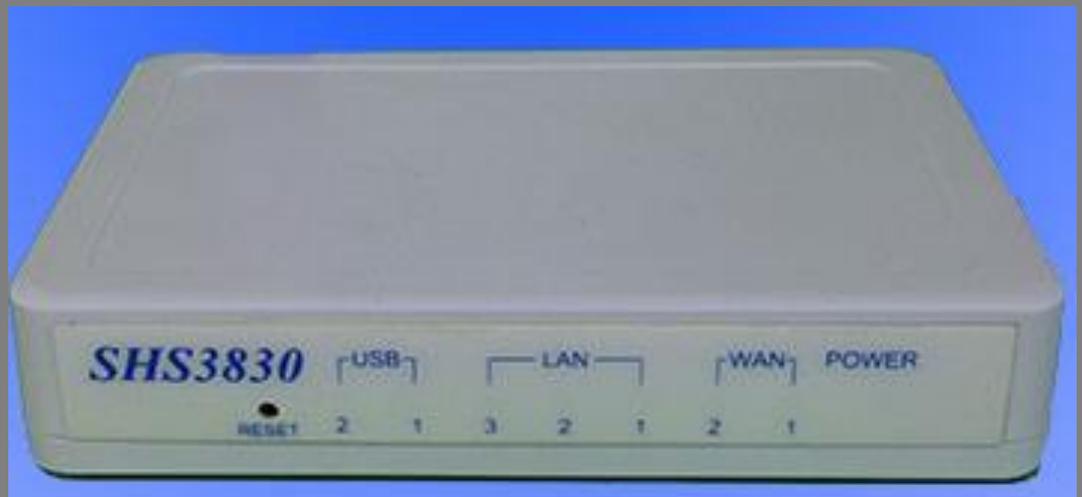


2014

SHS 3830

User Manual

SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features.



Avadesign Technology Co. Ltd

www.avadesign.com.tw

2014/11/25



WELCOME

Congratulations on purchasing the SHS 3830. The SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features. The SIP-based IP-PBX can create telephony systems for home and small-to-medium enterprises.

Manual version V1.00 25-11-2014
Avadesign Technology Co. Ltd

4F.-10, No.351, Sec. 2, Zhongshan
Rd., Zhonghe Dist., New Taipei City
23504, Taiwan R.O.C.

www.avadesign.com.tw

Table of Contents

Chapter 1 Introduction	5
1.1 SHS-3830 Specification.....	5
1.1.1 SIP IP-PBX Function	5
1.1.2 IP Network connection	6
1.1.3 Management	7
1.1.4 Environmental	7
1.1.5 Approvals	7
1.2 Hardware Overview	7
1.2.1 Front Panel and LED Indicator	7
1.2.2 Back Panel	8
Chapter 2 Start to configure SHS3830.....	9
2.1 Unpacking.....	9
2.2 Plug in DC power adapter to SHS 3830.....	9
2.3 Connect to LAN Port.....	9
2.4 Open Web Browser	9
2.5 Basic and Advance Configurations for IP-PBX.....	10
2.5.1 WAN configuration	10
2.5.2 LAN configuration	20
2.5.2.1 LAN configure.....	20
2.5.2.2 DHCP reserved IP	21
2.5.3 IP-PBX	23
2.5.3.1 Group.....	23
2.5.3.2 Subscribers.....	27
2.5.3.3 SIP Trunk.....	32
2.5.3.4 Dial Plan	33
2.5.3.5 SIP status	36
2.5.3.6 Queue	37
2.5.3.7 Paging.....	39
2.5.3.8 Preview	42

2.5.3.9 Download Log.....	44
2.5.3.10 Download CDR.....	45
2.5.3.11 Debug Capture	46
2.5.3.12 Update IPPBX	49
Chapter 3 Web configuration for Router functions.....	50
3.1 System status	50
3.1.1 Link status.....	50
3.1.2 Data monitor	50
3.1.3 DHCP clients table	51
3.1.4 NAT table	52
3.1.5 Current routing table.....	52
3.2 Load balance	53
3.2.1 Outbound.....	53
3.2.2 Inbound.....	55
3.3 Firewall	57
3.3.1 Super Users.....	58
3.3.2 DoS defense.....	61
3.3.3 ARP protection.....	64
3.3.4 Local IP filtering.....	64
3.3.5 Remote IP filtering.....	67
3.3.6 URL filtering.....	71
3.3.7 Intrusion security	74
3.3.8 Messenger blocking	78
3.3.9 IP session limit.....	79
3.4 Quality control	79
3.4.1 QoS.....	79
3.4.2 Bandwidth control.....	81
3.4.3 Outgoing Route	84
3.4.4 LAN IP speed limit	87
3.5 Advance	90
3.5.1 VPN pass through	90
3.5.2 DMZ	91
3.5.3 Virtual server.....	95
3.5.4 DDNS.....	99
3.5.5 Mac done	100
3.5.6 Multi-NAT	101

3.5.7 Inner DNS	104
3.5.8 Routing configure	107
3.6 System	111
3.6.1 Password	111
3.6.2 Time.....	112
3.6.3 Mail alert.....	113
3.6.4 System log	114
3.6.5 Remote configure.....	115
3.6.6 Load default	117
3.6.7 Config backup	118
3.6.8 Firmware update	119
3.7 Save & Reboot.....	120
Chapter 4 In-bound function	121
Chapter 5 Hardware load default.....	122
Chapter 6 Appendix.....	123
6.1 TCP/IP Protocol Port Number List	123

Chapter 1 Introduction

SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features. The Firewall and QoS improves VoIP network voice quality.

The IP-PBX module of SHS 3830 is a SIP-based IP-PBX that can create telephony systems for home and small-to-medium enterprises. It is also designed to operate on a variety of VoIP applications, such as auto-attendant, call transfer, and IP-based communications. Since it supports industry-standard SIP, it works with all SIP-supported products and devices available today. The key features of SHS 3830 are quiet, power saving, stability and small volume box.

1.1 SHS-3830 Specification

1.1.1 SIP IP-PBX Function

- RFC3261 compliance
- SIP UDP/TCP Protocol
- MD5 Digest Authentication (RFC2069/RFC2617)
- Allow FXO/FXS gateway, IP Phone and the DP-104 SIP IP video door phone to register.
- Support 50 registered extensions
- Easy install APP on smart phone to become SIP IP-PBX client extension
- Support SIP Trunk
- Support Audio Codec G.711 A-law/ μ -law
- Support pass through Video Call
- Out Band DTMF (RFC4733, RFC2833 / SIP INFO)
- Adaptive Jitter Buffer
- Automatic voice attendant
- Record your own greeting voice messages via voice file up-load from Web
- NAT Traversal configurable
- Blind Transfer
- Configurable Call and Pickup group
- Block Anonymous Call
- Call Hold
- Call Transfer
- Call Park
- Call Queuing
- Call Routing (DID & ANI) (in dial-plan function)
- Caller ID
- Route by Caller ID (in dial-plan function)
- Music On Hold
- Music On Transfer

- Time and Date
- Flexible Dial Plan
- Support Multi call rule to configure
- Outgoing Routing Rule (Drop, Replace, Add) and Routes selection
- Incoming Routing Rule (Drop, Replace, Add)
- Dial Group Setting
- Call Group, Pick up group setting
- Configure maximum concurrent SIP calls
- RTP Routed or Direct mode selection
- SIP Trunk setting
- Cellular Phone resonance setting
- Video preview setting
- Flexible Routing Plan
- Voice broadcasting over IP Phone with separated group
- Provide CDR log file

1.1.2 IP Network connection

- IPv4 (RFC 791) for WAN and LAN ports
- IP/ICMP/ARP/RARP/SNTP
- NTP Server and Time Zone setting
- WAN: DHCP, Fixed, PPPoE, DDNS
- LAN : Static Private IP or DHCP Server
- NAT allows users to surf internet by means of a single broadband user account
- Multiple DMZ Host (PPPoE, static IP)
- Multiple Virtual Server
- Multiple NAT function
- Protocol Route Control (IP Binding Function, by IP & port number)
- Protocol Bandwidth Control (by application protocol port number)
- IP/URL Blocking
- User Bandwidth control Function (by user IP address)
- Outgoing wan link selected (by user IP address)
- Remote Configuration through Internet
- Mail Alert: H32 WAN up
 - WAN down
 - System Log
- System Log: local event logging – log send to remote server
- Firewall
- Backup / Restore Router configuration file from PC
- Outbound Load Balance: provide 2 working mode: (1) session (2) weight round robin
- Inbound Load Balance: provide 2 working mode: (1) session (2) weight round

robin

- TCP/UDP (RFC 793/768)
- RTP/RTCP (RFC 1889/1890)

1.1.3 Management

- Administrative HTTP and port number configuration
- Subscriber information display
- HTTP port and user ID, Password control
- Firmware and Library upload
- Configuration Backup/Restore
- Reset to Factory default setting
- Soft-Reset or Reboot System
- Status display: Network, Line, SIP Trunk status

1.1.4 Environmental

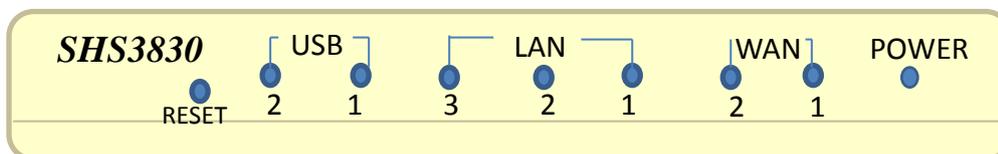
- Dimensions: 155(W) x 106(H) x 29(D) mm
- Weight: 300g
- Power Adaptor: INPUT: AC100V~240V, 50/60Hz 0.8A
OUTPUT: DC 12V, 2.0A

1.1.5 Approvals

- CE
- FCC
- RoHS

1.2 Hardware Overview

1.2.1 Front Panel and LED Indicator



RESET: If SHS 3830 encounters any system crash, you may press this button to reload factory default value as press the button over 3 seconds or reset back to latest configuration file while pushing the button.

USB: SHS 3830 provides two USB 2.0 ports. Light on when SHS 3830 detects USB device and active.

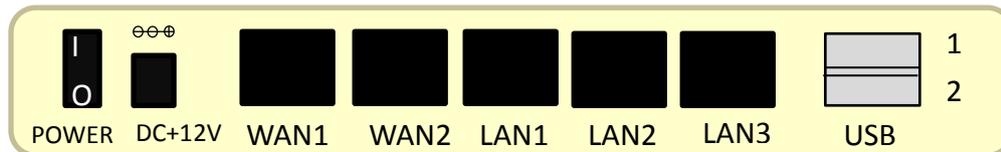
LAN: SHS 3830 provides three RJ45 type LAN ports connecting to your computer or network device such as Hub/Switch via RJ45 cable. Light on means link 100 Mbps. Flash when data is transmitting or receiving with 100 Mbps. Light off means

disconnected or undetected.

WAN: SHS 3830 provides two RJ45 type WAN ports connecting to broadband transmission equipment such as ADSL or Fiber or CABLE Modem via RJ45 cable. Light on means link 100 Mbps. Flash when data is transmitting or receiving with 100 Mbps. Light off means disconnected or undetected.

POWER: Light on when SHS3830 is powered by on.

1.2.2 Back Panel



POWER: A switch for power on or off

DC 12V/2A: Connecting to AC adapter. Input AC 100V~240V, 50/60Hz 0.8A;
Output DC12V 2.0A

LAN/WAN: RJ-45 socket, complied with Ethernet 10/100base-T.

USB: USB 2.0 ports, USB Type A.

Chapter 2 Start to configure SHS3830

2.1 Unpacking

Unpack the items. Your package should include:

- One SHS 3830
- One external power adaptor INPUT: AC100V~240V, 50/60Hz 0.8A
OUTPUT: DC 12V, 2.0A

If items are missing or damaged, notify your Avadesign representative. Keep the carton and packing material.

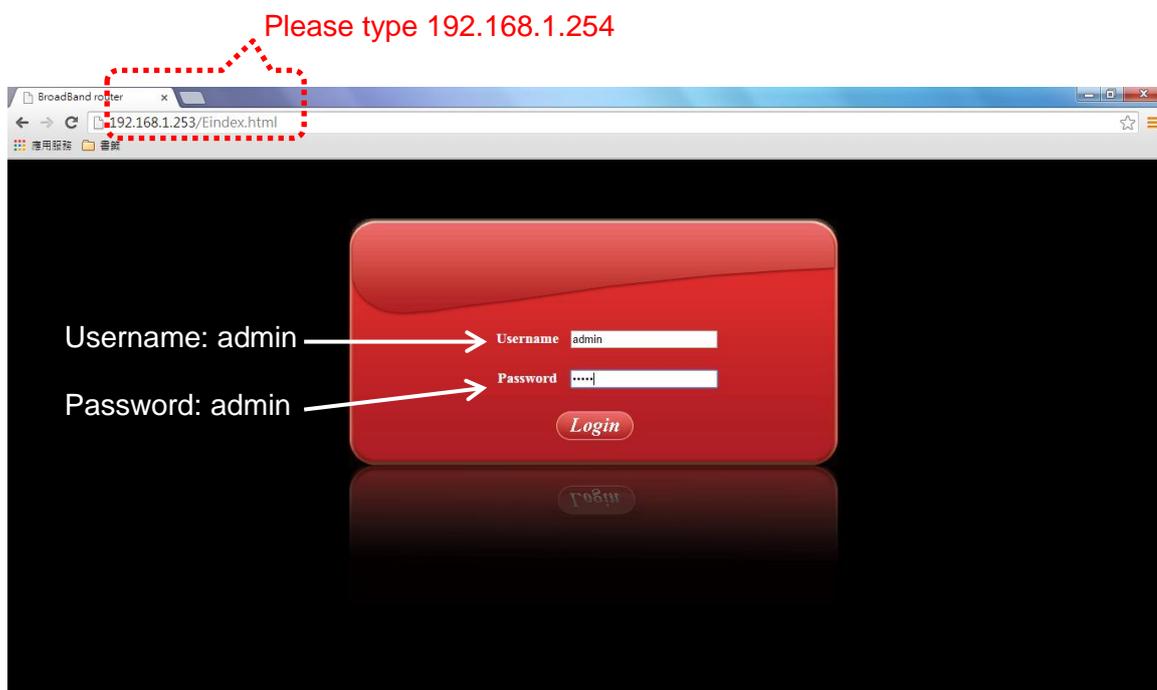
2.2 Plug in DC power adapter to SHS 3830

2.3 Connect to LAN Port

LAN port of SHS3830 connects to user's computer or Hub/Switch port via RJ45 cable. Then plug in AC power cord to power source and switch on the SHS 3830.

2.4 Open Web Browser

Type the default IP address <http://192.168.1.254> in the address bar of the Chrome browser to open web configuration. The screen shows as below:



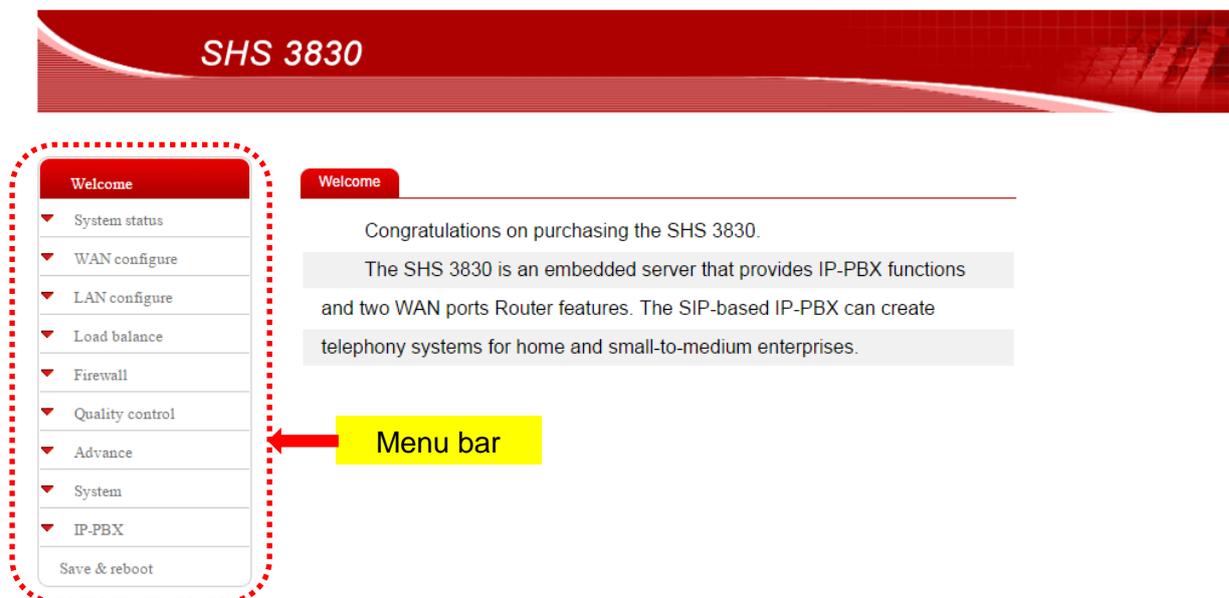
Please input with username: admin and password: admin then click “Login” button on the screen. After login SHS3830, user can start to do basic and advance configurations.

After Login SHS 3830 user will see screen as below, and there are ten main categories, user can click on each category to extend detail items.

- Welcome
- System Status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

The various configuration menus are explained below. You can select various function listed in the left side of Welcome page display.

Welcome Home Page



2.5 Basic and Advance Configurations for IP-PBX

To make SHS 3830 work smoothly you have to set up some basic and advance configurations that include router and IP-PBX features.

The first, you have to configure WAN and LAN IP for network enable.

2.5.1 WAN configuration

There are two WAN ports for the SHS 3830. You can select “WAN configure” in the menu bar on the left side of screen to configure WAN1/WAN2 as shown below.

There are several WAN functions can be made in this display, you can configure functions to each WAN port separately.

WAN Configure – WAN1 – Dynamic IP



WAN1 configure →

Welcome
System status
WAN configure
WAN1
WAN2
3G USB modem
LAN configure
Load balance
Firewall
Quality control
Advance
System
IP-PBX
Save & reboot

WAN1

WAN1 TYPE	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> PPPoE <input type="radio"/> Static IP
VPN client	<input checked="" type="radio"/> Disable <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> L2TP-PSK
Internet Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Healthy check:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

WAN1/WAN2 TYPE

Three kinds of WAN types to let you select for each WAN port:

1. Dynamic IP - connect to Cable Modem.

Obtain an IP address from ISP automatically. Usually it's used to connect CABLE modem. You won't need to assign an IP address. The SHS 3830 will get the IP address for user automatically.

2. PPPoE - connect to Dial Up DSL

Some ISPs require use of PPPoE to connect to their service. Connect to ISP via dial-up connecting, ISP will assign a legal IP to you after the user ID and password had been passed when the connection is made (The user ID and password here are provided by your ISP.)

3. Static IP - Connect to Leased DSL

ISP assigns you a static IP address. When used the leased line of ADSL. ISP will provide you the relative IP, Subnet Mask, Gateway and DNS. You need to indicate the static IP manually.

VPN Client

User can select either Disable or PPTP or L2TP or L2TP over IPsec. With PPTP/L2TP/L2TP-PSK dial up features to help construct a complete Client/Server topology for need of enterprise network, it improves security in connecting links in public network.

Internet Schedule

This function allows you to control each WAN port link up/down time by

daily/weekly. Available time: WAN port link up time. For example : The link time is from AM 9:30 – PM 6:30. User can fill 09:30 : 18:30

Select Weekly: choose by day

Note: When enable SCHEDULE function, the line will up/down following the timer set, no matter DOD function is enable or not.

Healthy check

User can select either Enable or Disable.

When choose Dynamic IP, you only need to save this selection by clicking on “Apply” button shown as below. When finish setting all parameter, reboot SHS 3830.

WAN Configure – WAN2 – Dynamic IP

SHS 3830

Welcome

- System status
- WAN configure
 - WAN1
 - WAN2
 - 3G USB modem
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

WAN2

WAN2 TYPE	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> PPPoE <input type="radio"/> Static IP
VPN client	<input checked="" type="radio"/> Disable <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> L2TP-PSK
Internet Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Healthy check:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Click on “Apply” button to save the configuration what you choose.

The content and usage of WAN2 is the same as WAN1.

WAN Configure – WAN1 – PPPoE

The screenshot shows the WAN configuration page for WAN1 on the SHS 3830 device. The interface is divided into several sections:

- Navigation Menu:** Includes Welcome, System status, WAN configure (selected), WAN1, WAN2, 3G USB modem, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, and Save & reboot.
- WAN1 Configuration:**
 - WAN1 TYPE:** Radio buttons for Dynamic IP, PPPoE (selected), and Static IP.
 - Account:** Text input field.
 - Password:** Text input field.
 - Service name (option):** Text input field.
 - Max idle time (mins):** Text input field with value 0.
 - Connect mode:** Radio buttons for Manual, Dial-on-demand, and Always on (selected).
 - LCP echo:** Checkmark for Enable.
 - Interval:** Text input field with value 20.
 - Counter:** Text input field with value 3.
- VPN client:** Radio buttons for Disable (selected), PPTP, L2TP, and L2TP-PSK.
- Internet Schedule:** Radio buttons for Enable and Disable (selected).
- Healthy check:** Radio buttons for Enable and Disable (selected).

An **Apply** button is located at the bottom center of the configuration area.

PPPoE/Dial up DSL Type

Select “PPPoE” and you will need to enter the ID and Password. Sometimes you also need to input the Service Name if ISP requires for it. Max Idle Time is using to disconnect the ADSL connection automatically after the idle period you define. The unit is minute and the default is 0. This default value let SHS 3830 remain connecting all the time unless disconnected by user manually or ISP. If you define the period as 3 and the SHS 3830 will auto disconnect after idling 3 minutes. Supposing that you don't have the Service Name, you may ask your ISP for it.

Account: User Name, provide by ISP, up to 60 characters can be enter.

Password: provide by ISP, up to 60 characters can be enter.

Max Idle Time: 0 =no check, check by minutes

Connect mode:

- **Manual:** You need to initiate WAN connection manually, by clicking "WAN1 connect" or "WAN2 connect" button in "System Status" - "Link status" menu. However, power up or reset also can initiate the WAN connection.
- **Dial-on-demand:** Whenever a user is trying to access the Internet from his computer, this WAN port will start connection automatically if it is disconnected.
- **Always-on:** The WAN port will try to establish the connection as long as it is disconnected, no matter this port is used or not.

LCP echo: To send LCP (Link Control Protocol) echo request at regular interval to ISP for checking PPPoE connection active.

Interval: Editable for need between 0 ~ 65535.

Counter: the number of LCP echo request to be sent.

about "always on " function, normally you need to combine "Health check " function together, then "always on" will be work more prefect because there have a ADSL modem between router & ISP equipment. in physical layer, if ADSL line fail but ADSL modem still alive , SHS 3830 can't detect line is broken unless ISP send a disconnect packet to SHS 3830 so if ADSL line is in abnormal up-down, sometimes router module of SHS 3830 does not get disconnect message from ISP, so connected line is deemed to still connection by SHS 3830.

If you enable "Health check " in each line. then the SHS 3830 can automatically send packet out through WAN to detect whether line is active or not (1 packet/30 sec) this function will cover entire network to secure packet will not lose in defect-line , include router-->ADSL modem--> ADSL line--> ISP Equipment---> Interest.

It's better to enable at least 2 options in "Health Check", in order to avoid misjudgments when only 1 option selected and that "option Server fail".

Static IP/Leased DSL Type

If you select "Static IP", you will need to input the IP address, Subnet Mask, Primary DNS, Secondary DNS and Gateway provided by your ISP. The picture below is an example of static IP's settings.

WAN Configure – WAN1 – Static IP

The screenshot shows the WAN1 configuration interface for the SHS 3830 router. The left sidebar contains a navigation menu with options like Welcome, System status, WAN configure (selected), LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, and Save & reboot. The main content area is titled 'WAN1' and displays the following configuration options:

WAN1 TYPE	<input type="radio"/> Dynamic IP <input type="radio"/> PPPoE <input checked="" type="radio"/> Static IP
IP address:	<input type="text" value="192.168.11.100"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Primary DNS:	<input type="text" value="168.95.1.1"/>
Secondary DNS:	<input type="text" value="168.95.192.1"/>
Gateway:	<input type="text" value="192.168.11.254"/>
VPN client	<input checked="" type="radio"/> Disable <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> L2TP-PSK
Internet Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Healthy check:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

An 'Apply' button is located at the bottom center of the configuration area.

3G Access (3G USB Modem)

In order to prevent any case in losing wired line connections, 3G wireless line for backup seems the best way to keep line alive to make your business not affected. Just a few steps for configured page as below, and then it soon can be online with no obstacle.

Disable/Enable of 3G USB modem is subject to be deactivated or activated all the time since the device turns on, so make sure 3G USB modem attached before device power on. All necessary parameters for configuration can be acquired from ISPs offering for account.

WAN configure – 3G USB modem configure

The screenshot shows the configuration interface for the SHS 3830 device. On the left is a navigation menu with options: Welcome, System status, WAN configure (selected), WAN1, WAN2, 3G USB modem, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, and Save & reboot. The main content area is titled '3G USB modem Configure' and contains the following settings:

3G USB modem	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Device name	Device NOT found
SIM card PIN code	<input type="text" value="0000"/>
APN	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
AT dial scripts	<input type="text" value="*99#"/>
Connect mode	<input checked="" type="radio"/> Manual <input type="radio"/> Always on

An 'Apply' button is located at the bottom of the configuration area.

PPTP Dial Up

PPTP dial up for WAN access type as below, need some parameters from ISPs to complete configuration page.

Ensure to key in user name and password as same as ISP offering. PPTP Server IP can be URL type or IP address that both are acceptable for device due to able to distinguish which one of them.

WAN Configure – WAN1 – Dynamic IP - PPTP



- Welcome
- System status
- WAN configure
- WAN1
- WAN2
- 3G USB modem
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

WAN1

WAN1 TYPE	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> PPPoE <input type="radio"/> Static IP
-----------	---

VPN client	<input type="radio"/> Disable <input checked="" type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> L2TP-PSK
------------	---

User Name	<input type="text"/>
Password	<input type="text"/>
PPTP Server IP	<input type="text"/>

Request options	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Pap</td> <td><input checked="" type="radio"/> Require <input type="radio"/> refuse</td> </tr> <tr> <td>Chap</td> <td><input type="radio"/> Require <input checked="" type="radio"/> refuse</td> </tr> <tr> <td>Mschap</td> <td><input checked="" type="radio"/> Require <input type="radio"/> refuse</td> </tr> <tr> <td>Mschap_v2</td> <td><input type="radio"/> Require <input checked="" type="radio"/> refuse</td> </tr> <tr> <td>Mppe_128</td> <td><input type="radio"/> Require <input checked="" type="radio"/> refuse</td> </tr> </table>	Pap	<input checked="" type="radio"/> Require <input type="radio"/> refuse	Chap	<input type="radio"/> Require <input checked="" type="radio"/> refuse	Mschap	<input checked="" type="radio"/> Require <input type="radio"/> refuse	Mschap_v2	<input type="radio"/> Require <input checked="" type="radio"/> refuse	Mppe_128	<input type="radio"/> Require <input checked="" type="radio"/> refuse
Pap	<input checked="" type="radio"/> Require <input type="radio"/> refuse										
Chap	<input type="radio"/> Require <input checked="" type="radio"/> refuse										
Mschap	<input checked="" type="radio"/> Require <input type="radio"/> refuse										
Mschap_v2	<input type="radio"/> Require <input checked="" type="radio"/> refuse										
Mppe_128	<input type="radio"/> Require <input checked="" type="radio"/> refuse										

Internet Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
-------------------	---

Healthy check:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
----------------	---

Below status shown established PPTP links for example.



- Welcome
- System status
- Link status
- Data monitor
- DHCP clients table
- NAT table
- Current routing table
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

Link status

Port	IP address	MAC address	Subnet mask	DHCP
LAN	192.168.1.253	00:09:2C:10:1B:6D	255.255.255.0	Disable

Port	IP address	MAC address	Subnet mask	Status	Button
WAN1	DHCP	00:09:2C:10:1B:6B	255.255.255.0	Disconnected	<input type="button" value="Connect"/>
WAN1-PPTP	0.0.0.0	Remote IP address :	0.0.0.0	Disconnected	
WAN2	DHCP	00:09:2C:10:1B:6C	255.255.255.0	Disconnected	<input type="button" value="Connect"/>

Firmware	Version number	Release date
SHS3830	V0028	2014-09-25 10:10:46+08:00

L2TP Dial Up

If ISPs ask for L2TP for dial up, then user can choose and enable it just follow below page to fill in necessary items to launch Internet service.

WAN Configure – WAN1 – Dynamic IP – L2TP

Welcome

System status

WAN configure

WAN1

WAN2

3G USB modem

LAN configure

Load balance

Firewall

Quality control

Advance

System

IP-PBX

Save & reboot

WAN1

WAN1 TYPE: Dynamic IP PPPoE Static IP

VPN client: Disable PPTP L2TP L2TP-PSK

User Name:

Password:

L2TP Server IP:

Request options:

Chap: Require refuse

Pap: Require refuse

Authentication: Require refuse

Internet Schedule: Enable Disable

Healthy check: Enable Disable

Apply

L2TP over IPSec. Dial up (L2TP-PSK) (Option)

It is L2TP over IPSec. dial up to offer a better protection for Internet access. Although not many devices support the feature in market, it is a choice for user to adopt for specific requirement if necessary.

Regarding above various VPN Clients for dial up to Server to establish secured connection to access data or contents, many of them have been wildly adopted by enterprises for their resources share no matter in between branch and headquarter , or employee carry portable devices outside to online import and export data for business.

Basically, the SHS 3830 does NOT provide this feature. User has to pay for this option.

Internet Schedule

Scheduling Internet connection with time period to save cost and manage access internet for workers to improve efficiency.

WAN Configure – Internet schedule



Welcome	WAN1
System status	
WAN configure	WAN1 TYPE: <input checked="" type="radio"/> Dynamic IP <input type="radio"/> PPPoE <input type="radio"/> Static IP
LAN configure	VPN client: <input checked="" type="radio"/> Disable <input type="radio"/> PPTP <input type="radio"/> L2TP <input type="radio"/> L2TP-PSK
Load balance	Internet Schedule: <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Firewall	Available Time: 0 : 0 - 23 : 59
Quality control	Select Week: <input checked="" type="checkbox"/> SUN <input checked="" type="checkbox"/> MON <input checked="" type="checkbox"/> TUE <input checked="" type="checkbox"/> WED <input checked="" type="checkbox"/> THU <input checked="" type="checkbox"/> FRI <input checked="" type="checkbox"/> SAT
Advance	Healthy check: <input type="radio"/> Enable <input checked="" type="radio"/> Disable
System	<input type="button" value="Apply"/>
IP-PBX	
Save & reboot	

Healthy check

1. Enable:

SHS 3830 will check ADSL link automatically to check whether link alive or not, if link fail, the Router will switch packet to another exist link(except TCP packet), the router will switch back to ADSL link again after router check ADSL line link again.

SHS 3830 provides 3 methods to check ADSL link. You can choose it with each method or both as follows:

- ✓ DNS : test DNS in Internet
- ✓ Ping IP : to test IP in Internet
- ✓ Time Server

Suggest select at least 2 method to check ADSL link, in order to avoid router making wrong action due to Internet Server disable.

2. Disable: no Healthy check function

If without "Time Server" existing, this function will disable automatically.

Healthy check can be set up to test 3 different destination IP, in order to avoid wrong operation (in case destination server is fail).

WAN Configure – Healthy check

SHS 3830

- Welcome
- System status
- WAN configure
- WAN1
- WAN2
- 3G USB modem
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

WAN1

WAN1 TYPE: Dynamic IP PPPoE Static IP

VPN client: Disable PPTP L2TP L2TP-PSK

Internet Schedule: Enable Disable

Healthy check: Enable Disable

Counter:

Mode	DNS server	URL	Enable	Test
DNS:	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Test"/>

Mode	IP address	Gateway	Enable	Test
Ping:	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Test"/>

Mode	User define NTP server	NTP server	Enable	Test
NTP:	<input type="text" value="207.46.232.182"/>	<input type="text" value="none"/>	<input type="checkbox"/>	<input type="button" value="Test"/>

Mode	IP address	Gateway:	Enable	Test
ARP gateway	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Test"/>

2.5.2 LAN configuration

LAN configure includes two functions. One configures LAN port. Include DHCP. The other set the DHCP Reserved IP.

2.5.2.1 LAN Configure

This function configures the LAN ports

- IP address
- Subnet Mask
- DHCP.

You can choose using DHCP server or not, the Dynamic Host Configuration Protocol (DHCP) allows the SHS 3830 to dynamically assign IP addresses to network devices. Dynamic IP assignment alleviates the need for the network administrator to maintain and monitor IP address assignments and simplifies IP use because the IP addresses are automatically and dynamically assigned when a station powers-on. You will need to indicate the range of DHCP server and DNS address if you enable DHCP server function.

When enable DHCP Server in “From”, ”TO” field, user **assigns** class A,B,C IP which suit for network topology. Fill in local DNS Server IP address in “**DNS Address**” field, you can ask your local ISP to provide this information.

LAN Configure – LAN Configure

The screenshot displays the SHS 3830 LAN Configure web interface. The sidebar on the left contains the following navigation items: Welcome, System status, WAN configure, LAN configure (highlighted), LAN configure, DHCP reserved IP, Load balance, Firewall, Quality control, Advance, System, IP-PBX, and Save & reboot. The main configuration area is titled 'LAN Configure' and includes the following fields:

LAN IP address	192.168.1.253
Subnet Mask	255.255.255.0
DHCP server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Start IP address	192.168.1.10
End IP address	192.168.1.249
Primary DNS	168.95.1.1
Secondary DNS	168.95.192.1
DHCP release time(seconds)	864000
Gateway IP	192.168.1.254

An 'Apply' button is located at the bottom of the configuration area.

LAN IP address: Input IP address for LAN port of SHS 3830. If user set up SHS 3830 be static IP mode, user need to input IP address of LAN and Subnet Mask.

Subnet Mask: Input Subnet Mask for LAN port of SHS 3830.

DHCP server: User can select either Enable or Disable.

Start IP address: Input Start IP address.

End IP address: Input End IP address.

Primary DNS: Input Primary DNS address.

Secondary DNS: Input Secondary DNS address.

DHCP release time (seconds): Input the number of seconds

Gateway IP: If user set up SHS 3830 be static IP mode, user need to input IP address of Gateway. The default Gateway IP address is 192.168.1.254

At last, user needs to click on “Apply” button to save configuration.

2.5.2.2 DHCP reserved IP

The second submenu of LAN configure is DHCP reserved IP.

You can also reserve some IP’s to specific computers. You need to enter the name (MAC address) of the network card installed in your computer to assign a particular IP to it. Click **ADD** to enter a new web page for adding a reserved IP.

For example : Add a new item.

Step 1: Enter **DHCP reversed IP** web page. Then click “Add” to enter the added page.

LAN Configure – DHCP reserved IP



Step 2: Fill data to MAC address and IP. Then Click “Add” then SHS 3830 goes back to **DHCP reversed IP** list table. The input screen shows as follows.

LAN Configure – DHCP reserved IP – ADD

Welcome

- System status
- WAN configure
- LAN configure**
 - LAN configure
 - DHCP reserved IP**
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

DHCP Reserved IP

Add DHCP Reserved IP Item

MAC address : : : : :

IP address

Apply

Step 3: Then click “Apply” to save. You will see the screen of DHCP reserved IP list table as below.

Welcome

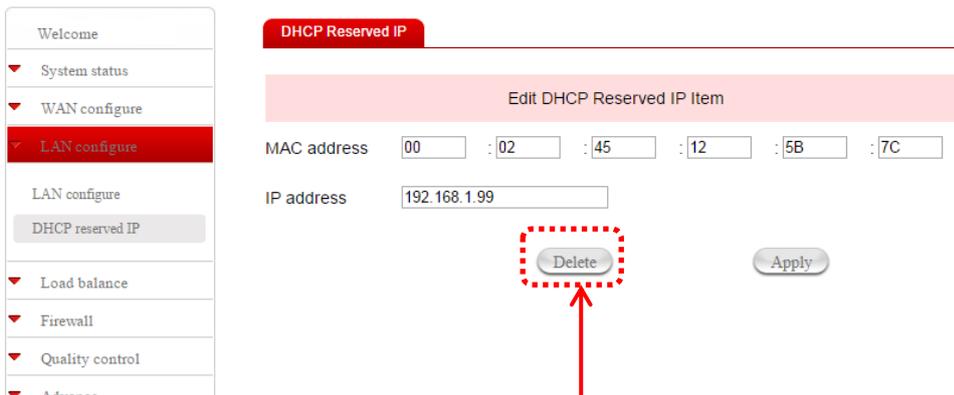
- System status
- WAN configure
- LAN configure**
 - LAN configure
 - DHCP reserved IP**
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

DHCP Reserved IP

Item	MAC address	IP address	Edit
1	00:02:45:12:5B:7C	192.168.1.99	<input checked="" type="checkbox"/>

Add Apply

User also can edit or delete an item by clicking the check square of “Edit” item.



If user wants to delete it, click "Delete", then go back to DHCP reversed IP list table.

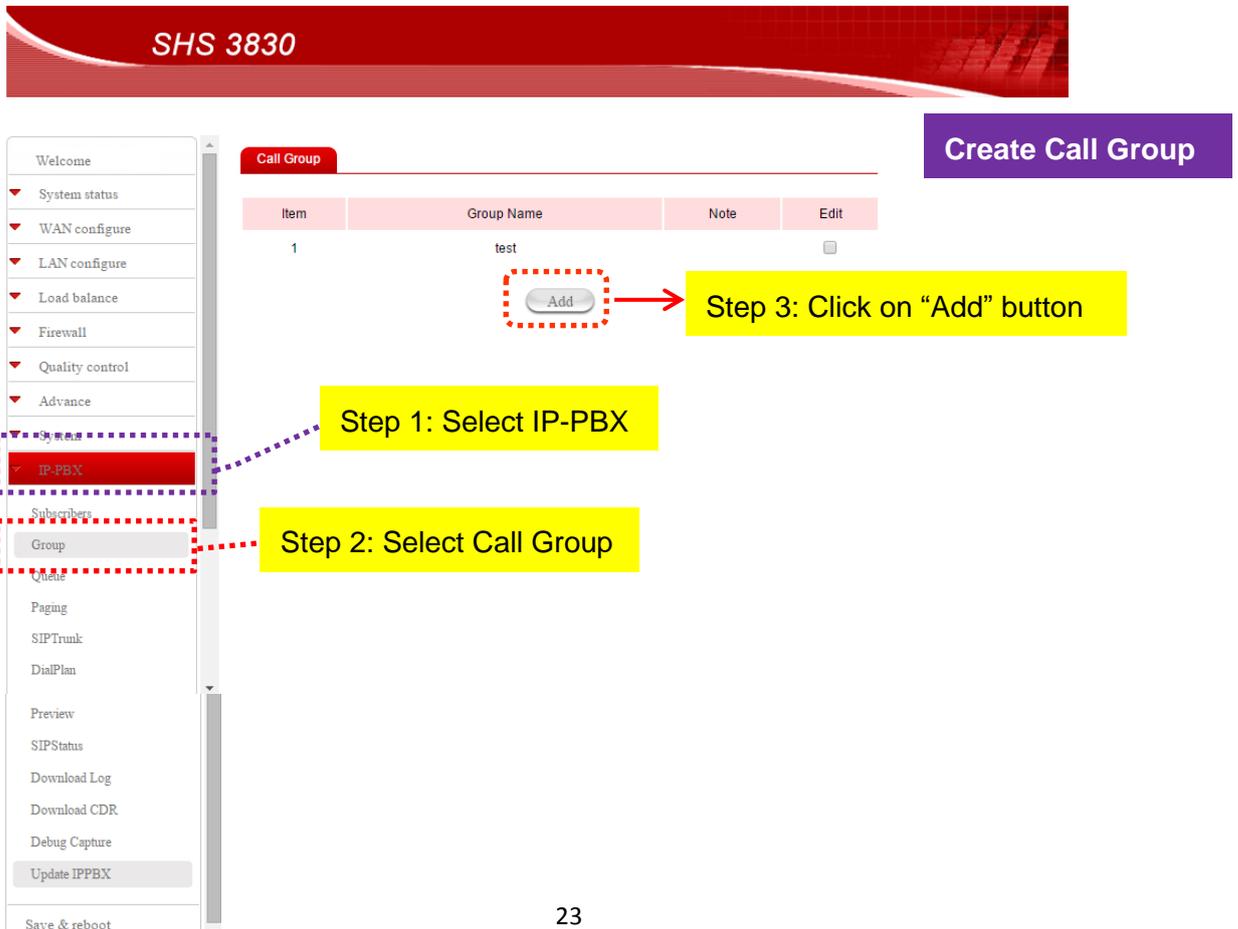
2.5.3 IP-PBX

At first, user needs to create call group. User can select "IP-PBX" in the menu bar on the left side of screen as shown below.

2.5.3.1 Group

Then step by step to set up call group as shown below.

IP-PBX – Group



Then user will see the screen of add SIP group. Please input group name and note to create a SIP group.

IP-PBX – Group – Add SIP Group

SHS 3830

Call Group

Add SIP Group

Group Name 123 Note 11

Apply

Step 4: Input group name and note then click "Apply" button to save configuration.

Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

SHS 3830

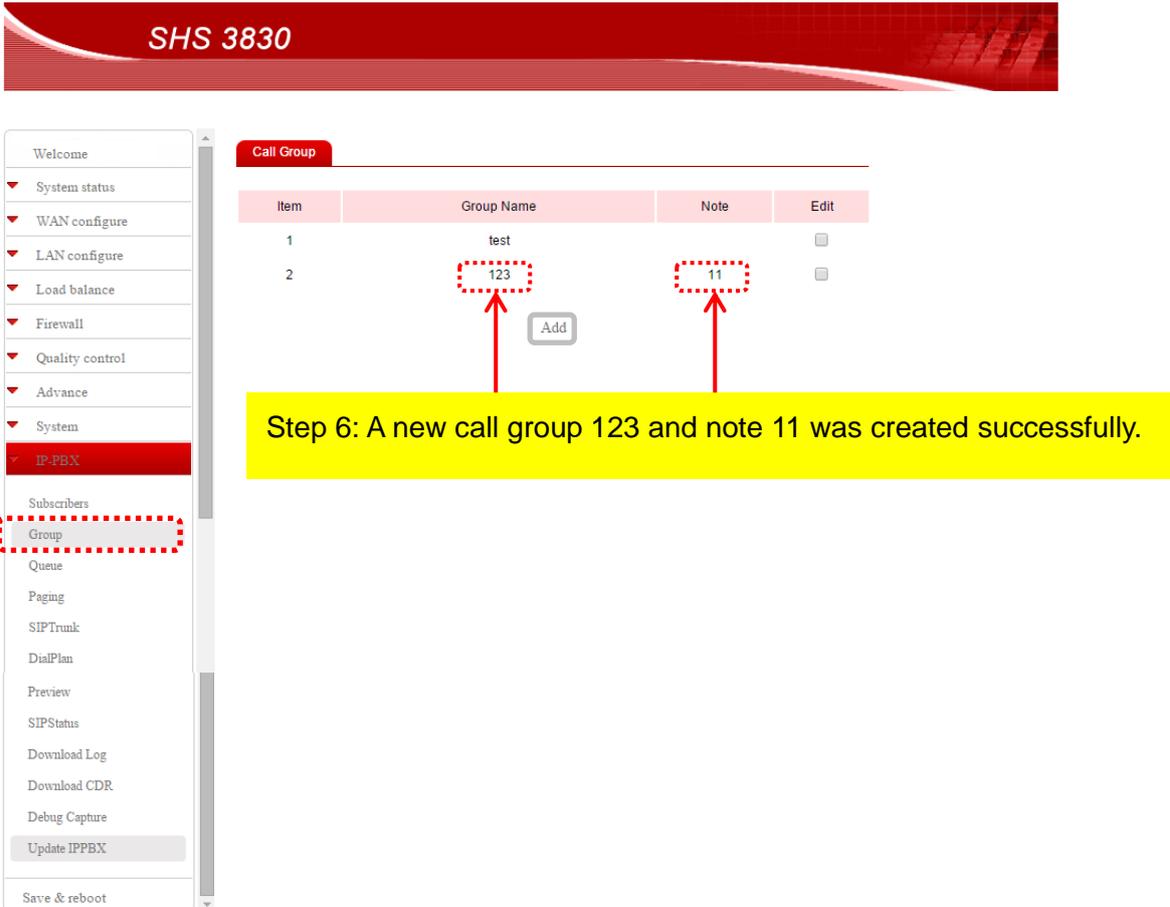
192.168.1.253 的網頁顯示 :
SIP Group configure saved success!

確定

Step 5: Click "Yes" button to complete the procedure of call group setting.

Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

Then user will see a new call group and note was created successful and display on the screen as below.



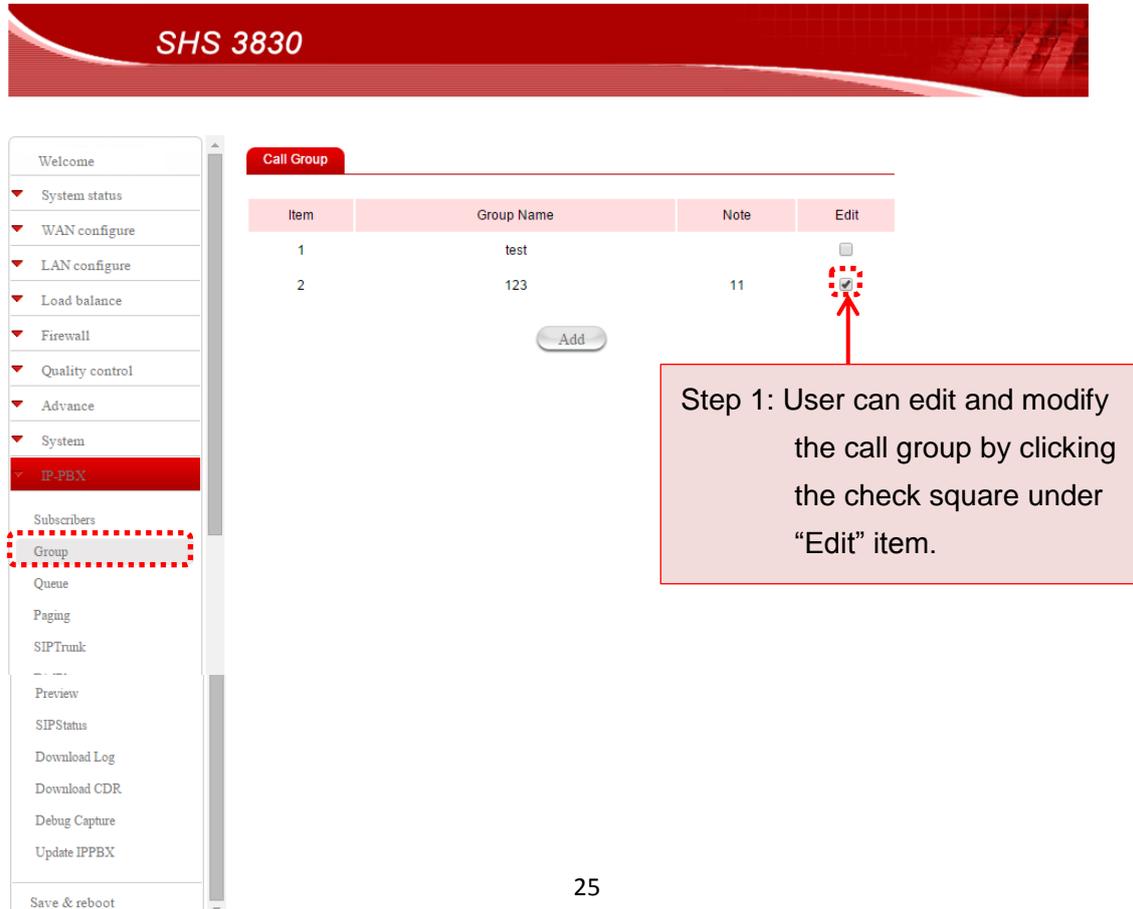
SHS 3830

Call Group

Item	Group Name	Note	Edit
1	test		<input type="checkbox"/>
2	123	11	<input type="checkbox"/>

Step 6: A new call group 123 and note 11 was created successfully.

User also can edit and modify the call group by clicking the check square under “Edit” item.



SHS 3830

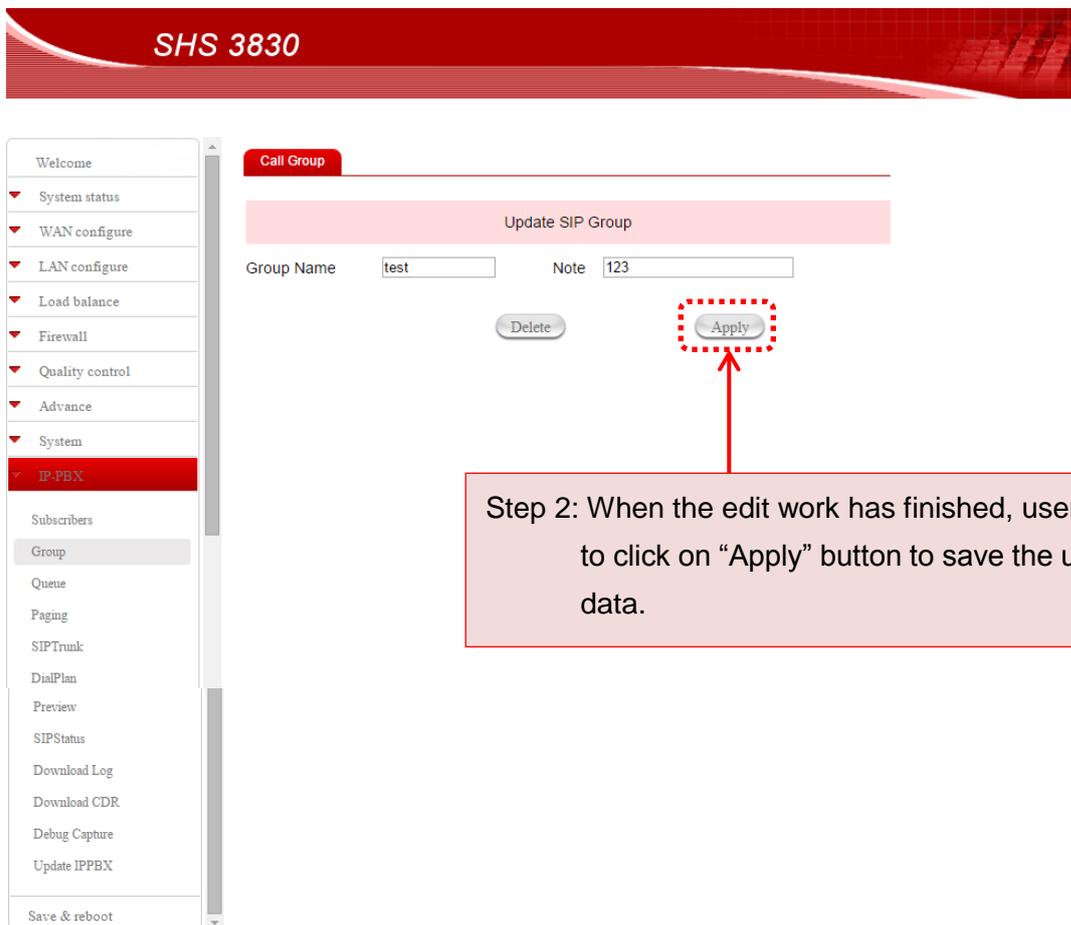
Call Group

Item	Group Name	Note	Edit
1	test		<input type="checkbox"/>
2	123	11	<input checked="" type="checkbox"/>

Step 1: User can edit and modify the call group by clicking the check square under “Edit” item.

Then user can see the screen of update SIP group as below. User can modify or delete the group to meet user's requirement. When the edit work has finished, user need to click on "Apply" button to save the updated data.

IP-PBX – Group – Updated SIP Group



Step 2: When the edit work has finished, user need to click on "Apply" button to save the updated data.



Step 3: Click "Yes" button to complete the procedure of call group updating.

2.5.3.2 Subscribers

In the next step, user has to create new subscriber for IP-PBX operating. The operation procedure is shown as following diagrams.

IP-PBX – Subscribers

The screenshot shows the SHS 3830 web interface. On the left is a navigation menu with 'IP-PBX' selected and 'Subscribers' highlighted. On the right, the 'Subscribers' page is displayed with a table containing one entry: SIP Account 2001, User Name, Pickup Group test, and an Edit button. A yellow callout box points to the 'Add' button with the text 'Step 3: Click on "Add" button'. Another yellow callout box points to the 'Subscribers' menu item with the text 'Step 2: Select Subscribers'. A third yellow callout box points to the 'IP-PBX' menu item with the text 'Step 1: Select IP-PBX'. A green button labeled 'Create Subscribers' is visible in the top right corner.

After click "Add" button, user can see the screen as below.

The screenshot shows the 'Add SIP Account' form in the SHS 3830 web interface. The form includes fields for SIP Account (2002), Password, User Name (2002), Group (test), Mobile Extension, NAT (Yes selected), Routing-Group (R1), Audio Codec (G711µ selected), Video Codec (h264, mpeg4, h263p, h263), Voice Mail Enable (ON selected), User Mail, Call Limit (2), and Quality (checked). A yellow callout box points to the 'Apply' button with the text 'Step 4: Input data to each field then click "Apply" button to save configuration.'

192.168.1.253 的網頁顯示 :
SIP Account configure saved success!

確定

Subscribers

Step 5: Click “Yes” button to complete the procedure of subscribers creating.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
 - Subscribers
 - Group
 - Queue
 - Paging
 - SIPTrunk
 - DialPlan
 - Preview
 - SIPStatus
 - Download Log
 - Download CDR
 - Debug Capture
 - Update IPPBX
- Save & reboot

Then user will see a new SIP account with user name and pickup group was created successful and display on the screen as below.

SHS 3830

Subscribers

SIP Account	User Name	Pickup Group	Edit
2001		test	<input type="checkbox"/>
2002	2002	test	<input type="checkbox"/>

Add

Step 6: A new SIP account and user name was created successfully.

“Edit” step 1:
User can edit and modify the subscriber data by clicking the check square under “Edit” item.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
 - Subscribers
 - Group
 - Queue
 - Paging
 - SIPTrunk
 - DialPlan
 - Preview
 - SIPStatus
 - Download Log
 - Download CDR
 - Debug Capture
 - Update IPPBX
- Save & reboot

User can edit and modify the subscriber data by clicking the check square under “Edit” item as shown above. Then user will see the screen of update SIP account as below.

IP-PBX – Subscribers – Update SIP account

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX**
 - Subscribers**
 - Group
 - Queue
 - Paging
 - SIPTrunk
 - DialPlan
 - Preview
 - SIPStatus
 - Download Log
 - Download CDR
 - Debug Capture
 - Update IPPBX
- Save & reboot

Subscribers

Update SIP 2002

SIP Account: 2002 Password: [masked]

User Name: 2002 Group: test

Mobile Extension: [empty]

NAT: Yes NO Routing-Group: R1

Audio Codec: G711µ G711a

Video Codec: h264 mpeg4 h263p h263

Voice Mail Enable: ON OFF User Mail: [empty]

Call Limit: 2 Quality:

Delete Apply

“Edit” step 2:
After the edit work has finished, please click “Apply” button to save the updated data.

SHS 3830

192.168.1.253 的網頁顯示 :

SIP Account configure saved success!

確定

Subscribers

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX**
 - Subscribers**
 - Group
 - Queue
 - Paging
 - SIPTrunk
 - DialPlan
 - Preview
 - SIPStatus
 - Download Log
 - Download CDR
 - Debug Capture
 - Update IPPBX
- Save & reboot

Step 3: Click “Yes” button to complete the procedure of subscribers updating.

Mobile extension setting

Except create and edit subscribers as above description, now we would like to introduce how to set up mobile extension for user. For example, there are two SIP account 2002 and 2003. **If user wants to use account 2002 as mobile extension,** please set up it as following steps.

The screenshot shows the SHS 3830 web interface. A red banner at the top contains the text "SHS 3830". On the right side, a red box contains the text "Mobile Extension Setting". The main content area is titled "Subscribers" and contains a table with the following data:

SIP Account	User Name	Pickup Group	Edit
2001		test	<input type="checkbox"/>
2002	2002	test	<input type="checkbox"/>
2003	2003	test	<input checked="" type="checkbox"/>

Below the table is an "Add" button. On the left side, there is a navigation menu with the following items: Welcome, System status, WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, Subscribers, Group, Queue, Paging, SIPTrunk, DialPlan, Preview, SIPStatus, Download Log, Download CDR, Debug Capture, Update IPPBX, and Save & reboot. The "IP-PBX" and "Subscribers" items are highlighted with a blue dashed box. Three orange callout boxes provide instructions: "Step 1: select IP-PBX" points to the "IP-PBX" menu item; "Step 2: select Subscribers item" points to the "Subscribers" menu item; "Step 3: Edit SIP account 2003 by clicking the check square under 'Edit' item." points to the checked checkbox in the table.

Subscribers

Update SIP 2003

SIP Account Password

User Name Group

Mobile Extension ← Step 4: Input account number 2002 here

NAT Yes NO Routing-Group

Audio Codec G711µ G711a

Video Codec h264 mpeg4 h263p h263

Voice Mail Enable ON OFF User Mail

Call Limit Quality

Delete Apply

Step 5: Click "Apply" button to save the configuration.

Once user has finished above configuration, someone call 2003, the extension 2002 will ring too. One of call answer, the other call will hang up automatically.

Call Transfer

The SHS 3830 supports call transfer now. During talk over the phone, you can press * and **9** for call transfer. After hearing the transfer voice, dial the extension number that you want to transfer.

Blind Transfer

The SHS 3830 supports blind transfer now. You can press * and **0** for blind transfer.

Call Group

You can use the Call Group parameter to assign an Extension to one or more groups.

Pick up Group

The SHS 3830 supports call pickup to allow a ringing phone to be answered from another extension. If you set up some extensions in the same group, one of extension is ringing, but nobody answer, then you can pick up this call on your extensions by press *8 to answer. For example: Ext-A is ringing, Ext-B can press * and **8** for call pick up.

2.5.3.3 SIP Trunk

User has to set up some necessary configuration for SIP trunk. Please select “SIPTrunk” under IP-PBX item of menu bar. Then click “Add” button as below. Alias is also a Trunk name. User also can click the check square of **Edit** to delete the specified Trunk or modify configured Trunk data.

IP-PBX – SIP Trunk

The screenshot shows the SHS 3830 web interface. The sidebar menu on the left includes 'System' > 'IP-PBX' > 'SIPTrunk'. The main content area displays a table of SIP Trunks with columns: Alias, Account, Proxy:Port, Status, and Edit. A table with one row is shown: Alias: test_trunk, Account: 2002, Proxy:Port: (empty), Status: State, Edit: (checkbox). An 'Add' button is located below the table. Annotations include: 'Step 1: Select IP-PBX' pointing to the IP-PBX menu item; 'Step 2: Select SIP Trunk item' pointing to the SIPTrunk menu item; 'Step 3: Please click "Add" button to create SIP Trunk.' pointing to the Add button; and a yellow box stating 'User can edit and modify the SIP trunk by clicking the check square under "Edit" item.' pointing to the checkbox in the Edit column.

Alias	Account	Proxy:Port	Status	Edit
test_trunk	2002		State	<input type="checkbox"/>

Then user will see the following screen:

IP-PBX – SIP Trunk – Add SIP Trunk

SHS 3830

SIP Trunk

Step 4: Please input data to each field.

Add SIP Trunk

Alias

Host:Port Domain:Port

Account Password

Numbers Routing-Group

AudioCodec Max Calls

Video Codec h264 mpeg4 h263p h263

Forward Trunk Reg

Quality

Max Calls: Blank express unlimited number of calls

Backup Router

SIP registration mode or peer to peer mode

Step 5: Click "Apply" button to save the configuration

Apply

2.5.3.4 Dial Plan

Define the dialing plan for Extension. It specifies the location of the instruction used to control what the phone is allowed to do, and what to do with incoming calls for this extension.

When users want to create their dial plan, please select "DialPlan" under IP-PBX item of menu bar. Then click "Add" button.

In the Dial Plan page, you should define the destination of prefix route. When you define the prefix route, you should set the Alias (Trunk ID) in the SIP Trunk page first; then you could input the correct Trunk ID in the Destination field. You also can input IP-Phone or Queue name or DISA.

Routing group allows you to set up call routing from route level 1 to 7 and DISA. The application of DISA performs as automated attendant. The SHS 3830 supports Automated Attendant. You can record the default greeting and the other announcements, for example: invalid call or call is busy or no answer, for use. And click the check square of DISA. So the caller will hear greeting because the called number will be routed to auto attendant.

IP-PBX – Dial Plan



Create Dial Plan

Prefix	Drop	Add Front	Add Back	Routing-Group	Edit
2XXX				r1	□

Add

IP-PBX

DialPlan

Step 1: Select IP-PBX

Step 3: Please click "Add" button to create user's dial plan.

Step 2: Select Dial Plan item

Then user will see the following screen "Add Dial Plan":



Create Dial Plan

Add Dial Plan

Prefix	1234	Drop	
Add Front		Add Back	
Routing-Group	<input checked="" type="checkbox"/> r1 <input type="checkbox"/> r2 <input type="checkbox"/> r3 <input type="checkbox"/> r4 <input type="checkbox"/> r5 <input type="checkbox"/> r6 <input type="checkbox"/> r7 <input type="checkbox"/> DISA		
Destination	test2 (Queue ▾)		
Ring Timer	<input style="width: 50px;" type="text"/> (s)		

Apply

Step 4: Set up a code for user's call group (the sample is 1234)

Step 5: Set up a routing-group for this call group (the example is r1)

Step 7: Click "Apply" button to save configuration.

Step 6: Here you can find some destination for choosing such as IP-Phone or alias of Trunk or queue name or DISA

Prefix	Drop	Add Front	Add Back	Routing-Group	Edit
2XXX	1234			r1	<input type="checkbox"/>
				r1	<input type="checkbox"/>

Step 8: Configuration! The dial plan of call group setting is successful now!

User can edit and modify the dial plan by clicking the check square.

Now we described each field of Dial Plan page as follows.

2! : All accounts with the first number is 2. Exclude 2 only.

1: Delete the first digit
-1: Delete the last digit

Add identified numbers at the end of telephone number.

DISA as described at page 31 of this manual.

Add identified number code before the telephone number. (for example: 886)

Dial Plan

The rule of Prefix is described as follows.

0 ~ 9: number for telephone number

x: any number from 0 to 9. For example: 02 2222 12xx means the telephone number range is from 02 2222 1200 to 02 2222 1299.

2!: all accounts (i.e. telephone number) with the first digit is 2 and exclude 2 only.

2.: all accounts (i.e. telephone number) with the first digit is 2 and include 2.

Add Front: To add assigned number before the telephone number. For example, you set 886 here and the called number is 0222221266, the SHS 3830 will add 886 then send 8860222221266 as the called number.

Add Back: To add assigned number at the end of telephone number. For example, you set 66 here and the called number is 02222212, the SHS 3830 will add 66 then send 0222221266 as the called number.

2.5.3.5 SIP status

User can select “SIP status” to look all of accounts on line.

The screenshot shows the SHS 3830 IP-PBX SIP Status page. The page title is "IP-PBX – SIP Status". The main content area displays a table with the following data:

Account	UserName	IP : PORT	Status
2001		0.0.0.0 : 0	
2002	2002	0.0.0.0 : 0	UNKNOWN
2003	2003	0.0.0.0 : 0	UNKNOWN

Navigation steps are indicated by red dashed boxes and yellow callout boxes:

- Step 1: Select IP-PBX** (points to the IP-PBX menu item in the left sidebar)
- Step 2: Select SIP Status item** (points to the SIPstatus menu item in the left sidebar)

2.5.3.6 Queue

You can set up some extensions in the queue. When a call is coming, all extensions in the queue will ring together. You can pick up anyone of extensions to answer. The other extensions will hang up automatically.

The screenshot shows the SHS 3830 interface with a sidebar on the left and a main content area. The sidebar has a menu with 'IP-PBX' and 'Queue' highlighted. The main content area has a 'Queue' tab and a form with 'Queue Name' and 'Add' buttons. A yellow box at the top right says 'Queue Setting'. Three green callout boxes provide instructions: 'Step 1: Select IP-PBX' points to the sidebar menu, 'Step 2: Select Queue' points to the 'Queue' menu item, and 'Step 3: Please click "Add" button to create call queuing.' points to the 'Add' button.

SHS 3830

Queue Setting

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX**
- Subscribers
- Group
- Queue
- Paging
- SIPTrunk
- DialPlan
- Preview
- SIPStatus
- Download Log
- Download CDR
- Debug Capture
- Update IPPBX
- Save & reboot

Queue

Queue Name Edit

Add

Step 3: Please click "Add" button to create call queuing.

Step 1: Select IP-PBX

Step 2: Select Queue

IP-PBX – Queue

The screenshot shows the SHS 3830 interface with the 'Queue' tab selected. The form is titled 'Add Queue' and has fields for 'Queue Name' (containing 'test 2') and 'Timeout to retry' (with a unit of 'sec'). Below these are two lists of SIP accounts. The left list contains 2001, 2002, 2003, 3001, 3002, and 3003. The right list is empty and labeled 'member'. There are '>>>>' and '<<<<' buttons between the lists, and an 'Apply' button at the bottom. A yellow box at the top right says 'Queue Setting'. Two green callout boxes provide instructions: 'Step 4: Input the queue name (the example is test 2)' points to the 'Queue Name' field, and 'Step 5: Shift these SIP accounts that user want to set up as a queue to member field at the right hand side.' points to the '>>>>' button.

SHS 3830

Queue Setting

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX**
- Subscribers
- Group
- Queue
- Paging
- SIPTrunk
- DialPlan
- Preview
- SIPStatus
- Download Log
- Download CDR
- Debug Capture
- Update IPPBX
- Save & reboot

Queue

Add Queue

Queue Name Timeout to retry sec

SIP Account

2001
2002
2003
3001
3002
3003

member

>>>>

<<<<

Apply

Step 4: Input the queue name (the example is test 2)

Step 5: Shift these SIP accounts that user want to set up as a queue to member field at the right hand side.

Then user will see the result as below.



Queue

Apply

Step 6: Click "Apply" button to save the configuration

IP-PBX – Queue

192.168.1.253 的網頁顯示:

SIP Queue configure saved success!

確定

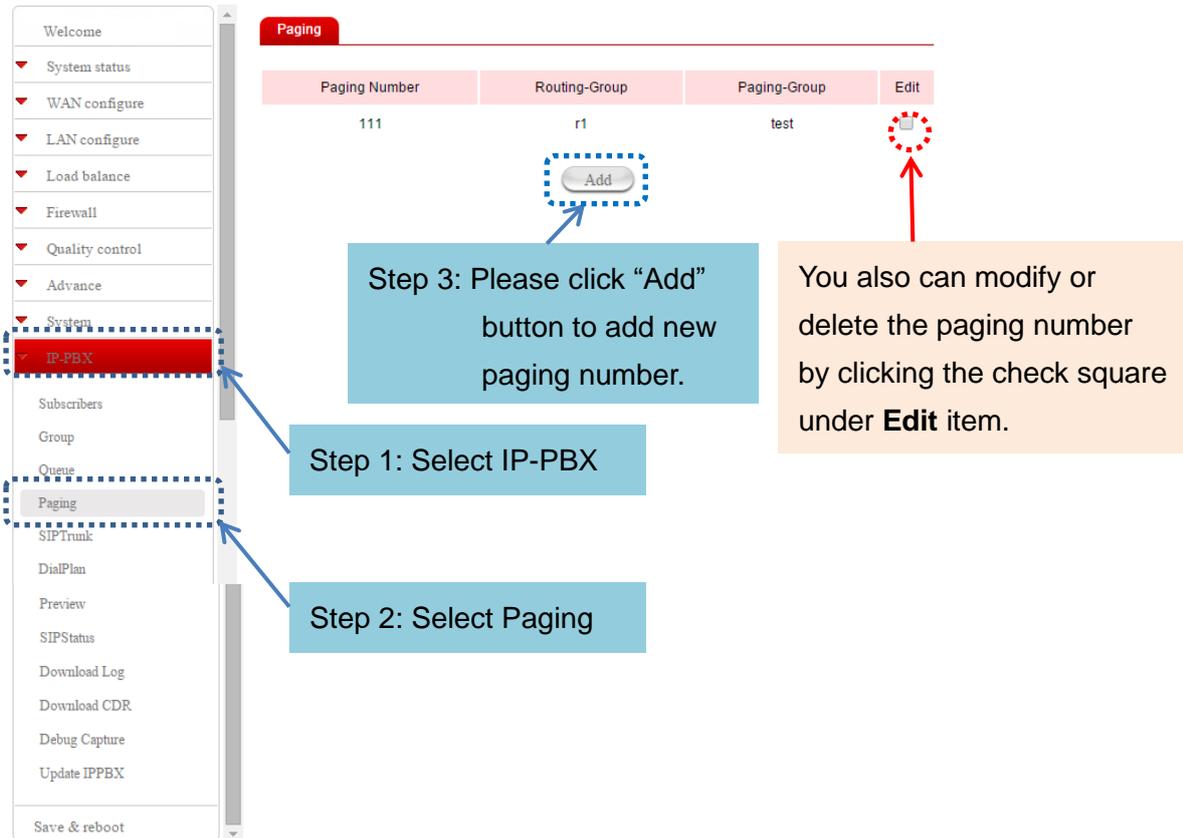
Step 7: Click "Yes" button to complete the procedure of queue setting.

Queue

2.5.3.7 Paging

In the page item of IP-PBX menu, you can add the extension number to perform broadcast function.

IP-PBX – Paging



The screenshot shows the 'Paging' configuration page. On the left is a navigation menu with 'IP-PBX' selected and 'Paging' highlighted. The main area contains a table with the following data:

Paging Number	Routing-Group	Paging-Group	Edit
111	r1	test	<input type="checkbox"/>

Annotations include: a blue box around 'IP-PBX' in the menu with the text 'Step 1: Select IP-PBX'; a blue box around 'Paging' in the menu with the text 'Step 2: Select Paging'; a blue box around the 'Add' button with the text 'Step 3: Please click "Add" button to add new paging number.'; and an orange box pointing to the 'Edit' column with the text 'You also can modify or delete the paging number by clicking the check square under Edit item.'

Then you will see the screen as below.

Quality control

Advance

System

IP-PBX

Subscribers

Group

Queue

Paging

SIPTrunk

DialPlan

Preview

SIPStatus

Download Log

Download CDR

Debug Capture

Update IPPBX

Save & reboot

Paging

Add Paging

Paging Number: 122

Routing-Group: r1 r2 r3 r4 r5 r6 r7 DISA

Paging-Group: test

Apply

Step 4: Input paging number, routing-group, and paging-group.

Step 5: Please click "Apply" button to save the configuration.

SHS 3830

Quality control

Advance

System

IP-PBX

Subscribers

Group

Queue

Paging

SIPTrunk

DialPlan

Preview

SIPStatus

Download Log

Download CDR

Debug Capture

Update IPPBX

Save & reboot

192.168.1.253 的網頁顯示 :
Paging configure saved success!

確定

Paging

Step 6: Click "Yes" button to complete the procedure of paging number setting.

Then you will see the extension 122 set up as paging number successfully that display on the screen as below.

Paging Number	Routing-Group	Paging-Group	Edit
111	r1	test	<input type="checkbox"/>
122	r1	test	<input checked="" type="checkbox"/>

Step 7: Extension 122 is set up as paging number now.

Edit step 1: You can modify or delete the paging number by clicking the check square under **Edit** item.

You also can modify or delete the paging number by clicking the check square under **Edit** item.

IP-PBX – Paging – Update Paging

Update Paging

Paging Number:

Routing-Group: r1 r2 r3 r4 r5 r6 r7 DISA

Paging-Group:

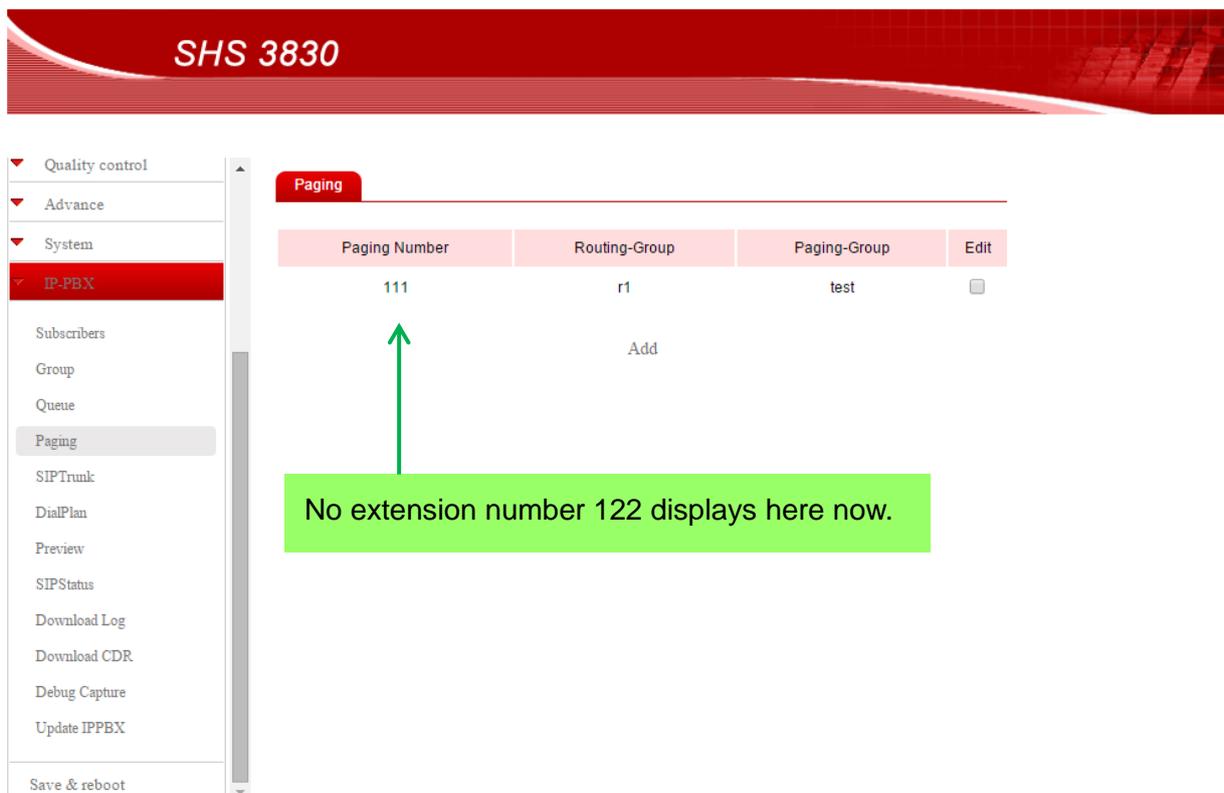
Edit Step 2: You can modify the paging number or routing-group or paging-group.

Otherwise you can adopt Edit Step 2: Click “Delete” button to delete the paging number.

Edit Step 3: Please click “Apply” button to save the configuration.



Then you will see the extension 122 was already deleted from paging number listing



2.5.3.8 Preview

The preview function is used with IP door phone. You can arrange some

extensions as member of preview group. You need to give a preview name for a preview group. The preview name listing is shown as below diagram.

When an IP door phone dial to a preview group, all of extensions, member, will ring. And you can answer the call from IP door phone by anyone of extensions to talk the person who at your door and open the door. The other extensions will hang up automatically.

IP-PBX – Preview

SHS 3830

Preview Number	Member	Edit
99990	2001,2002	<input type="checkbox"/>
99991		<input type="checkbox"/>
99992		<input type="checkbox"/>
99993		<input type="checkbox"/>
99994		<input type="checkbox"/>
99995		<input type="checkbox"/>
99996		<input type="checkbox"/>
99997		<input type="checkbox"/>
99998		<input type="checkbox"/>
99999		<input type="checkbox"/>

Step 1: Select IP-PBX

Step 2: Select Preview

You also can edit and modify the preview data by clicking the check square.

IP-PBX – Preview – Update Preview

SHS 3830

Update Preview

Preview Number : 99991

SIP Account

2001
2002
2003
3001
3002
3003

member

>>>>

<<<<

Apply

Shift one or some SIP accounts to be member at the right side.

Then you will see a member 3001 already add on the screen.

SHS 3830

Quality control
Advance
System
IP-PBX
Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

Preview

Preview Number	Member	Edit
99990	2001,2002	<input type="checkbox"/>
99991	3001	<input type="checkbox"/>
99992		<input type="checkbox"/>
99993		<input type="checkbox"/>
99994		<input type="checkbox"/>
99995		<input type="checkbox"/>
99996		<input type="checkbox"/>
99997		<input type="checkbox"/>
99998		<input type="checkbox"/>
99999		<input type="checkbox"/>

Add a new member in preview group 99991.

2.5.3.9 Download Log

You can download the log file of system by clicking “Download” button.

IP-PBX – Download Log

SHS 3830

Quality control
Advance
System
IP-PBX
Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

Download Log

Download Download&Delete

Step 1: Select IP-PBX

Step 2: Select Download Log

Step 3: Click “Download” button

You also can delete the log file from server.

The log file is shown as below for your reference. The maximum number of records is 1,000.

Example of System Log file

```
[Jan 31 22:25:51] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:26:51] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:26:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:27:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:27:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
```

2.5.3.10 Download CDR

You can download the Call Detail Record file by clicking “Download” button.

IP-PBX – Download CDR

The screenshot shows the SHS 3830 interface. On the left is a navigation menu with categories: Quality control, Advance, System, IP-PBX (selected), Subscribers, Group, Queue, Paging, SIPTrunk, DialPlan, Preview, SIPStatus, Download Log, Download CDR (highlighted), Debug Capture, Update IPPBX, and Save & reboot. At the top right, there is a red 'Download CDR' button. Below it are two buttons: 'Downlad' and 'Downlad&Delete'. Three callout boxes provide instructions: 'Step 1: Select IP-PBX' points to the IP-PBX menu item; 'Step 2: Select Download CDR' points to the Download CDR menu item; 'Step 3: Click "Download" button' points to the Downlad button. A pink box on the right states 'You also can delete the CDR file from server' with an arrow pointing to the Downlad&Delete button.

The CDR file is shown as below for your reference. The maximum number of CDR records is 1,000.

Example of CDR file

Caller ID	Caller Name	Caller State	Callee ID	Source SIP ID	Destination SIP ID	Command	Start time	Answer time
2001	s-BUSY	DialState	2001	SIP/2002-00000010	SIP/2002-00000011	Hangup	2/1/70 21:56	
2001	2002	r1	2001	SIP/2001-00000012	SIP/2002-00000013	Dial	SIP/2002,,rTk	2/1/70 22:00 2/1/70 22:00
2001	s-BUSY	DialState	2001	SIP/2002-00000014	SIP/2001-00000015	Hangup	2/1/70 22:00	
2001	2002	r1	2001	SIP/2001-00000016	SIP/2002-00000017	Dial	SIP/2002,,rTk	2/1/70 22:01 2/1/70 22:01
2002	2001	r1	2002	SIP/2002-00000018	SIP/2001-00000019	Dial	SIP/2001,,rTk	2/1/70 22:01 2/1/70 22:01
2002	2001	r1	2002	SIP/2002-0000001a	SIP/2001-0000001b	Dial	SIP/2001,,rTk	2/1/70 22:09 2/1/70 22:09

Start time	Answer time	End time	Duration	Billsec	Status
2/1/70 21:56		2/1/70 21:56	0	0	BUSY DOCUMENTATION 2757373.16
2/1/70 22:00	2/1/70 22:00	2/1/70 22:00	10	7	ANSWERED DOCUMENTATION 2757628.18
2/1/70 22:00		2/1/70 22:00	0	0	BUSY DOCUMENTATION 2757646.2
2/1/70 22:01	2/1/70 22:01	2/1/70 22:01	6	3	ANSWERED DOCUMENTATION 2757667.22
2/1/70 22:01	2/1/70 22:01	2/1/70 22:01	9	2	ANSWERED DOCUMENTATION 2757690.24
2/1/70 22:09	2/1/70 22:09	2/1/70 22:09	24	15	ANSWERED DOCUMENTATION 2758146.26

2.5.3.11 Debug Capture

When you have finished the configuration of SHS 3830 but the IP-PBX can NOT work smoothly or you get trouble in the usage of SHS 3830. Please select the function of Debug Capture to download the capture file for the network packet analysis and troubleshooting.

The capture file will be open and read by **Wireshark** software package. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting and analysis. You can free download from website www.wireshark.org.

Following diagrams will tell you how to download the capture file step by step.

IP-PBX – Debug Capture



Debug Capture

Step 1: Select IP-PBX

Step 3: Click "Start Capture" button

Start Capture

The screenshot shows the left-hand navigation menu of the SHS 3830 interface. The menu items are: Quality control, Advance, System, IP-PBX (highlighted with a red dashed box), Subscribers, Group, Queue, Paging, SIPTrunk, DialPlan, Preview, SIPStatus, Download Log, Download CDR, Debug Capture (highlighted with a red dashed box), Update IPPBX, and Save & reboot. A red box labeled "Debug Capture" is positioned above the main content area. A green box labeled "Step 1: Select IP-PBX" has an arrow pointing to the IP-PBX menu item. Another green box labeled "Step 3: Click 'Start Capture' button" has an arrow pointing to a "Start Capture" button, which is also highlighted with a red dashed box.



tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes

Step 4: Click "Stop Capture" button

StopCapture

The screenshot shows the SHS 3830 interface with the left-hand navigation menu. The menu items are: Quality control, Advance, System, IP-PBX (highlighted with a red dashed box), Subscribers, Group, Queue, Paging, SIPTrunk, DialPlan, Preview, SIPStatus, Download Log, Download CDR, Debug Capture (highlighted with a red dashed box), Update IPPBX, and Save & reboot. The main content area displays the text "tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes". A green box labeled "Step 4: Click 'Stop Capture' button" has an arrow pointing to a "StopCapture" button, which is also highlighted with a red dashed box.

SHS 3830

192.168.1.253 的網頁顯示 :
Capture Done!
確定

Quality control
Advance
System
IP-PBX
Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

Step 5: Click “Yes” button to confirm the capture file is complete.

SHS 3830

Debug Capture

Filename:hg3830_v702010_702012306.cap
Size:216.4K
Download Capture File: Download
Start Capture

Quality control
Advance
System
IP-PBX
Subscribers
Group
Queue
Paging
SIPTrunk
DialPlan
Preview
SIPStatus
Download Log
Download CDR
Debug Capture
Update IPPBX
Save & reboot

Step 6: Click “Download” button to download the capture file. Then you will get a file named hg3830_vxxxxxx_xxxxxxxxxx.cap p.s. x is any number from 0 to 9

2.5.3.12 Update IPPBX

You can update your SHS 3830 IP-PBX by clicking “Update IPPBX” in the main menu of IP-PBX as described below.

IP-PBX – Update IPPBX

The screenshot shows the SHS 3830 IP-PBX update interface. The left sidebar contains a menu with categories: Quality control, Advance, System, and IP-PBX. The IP-PBX category is expanded, showing options like Subscribers, Group, Queue, Paging, SIPTrunk, DialPlan, Preview, SIPStatus, Download Log, Download CDR, Debug Capture, Update IPPBX, and Save & reboot. The 'Update IPPBX' option is highlighted with a blue dashed box and labeled 'Step 2: Select Update IPPBX'. The main content area shows a red 'Update IPPBX' button at the top. Below it, a warning message reads: 'Attention: router will reboot after IPPS updated' and 'Current version is: v1410130preview'. A 'Choose file to update' dialog box is open, with the 'Choose' button highlighted by a blue dashed box and labeled 'Step 3: Choose file to update by clicking “choose file” button'. The 'Update' button in the dialog is also highlighted with a blue dashed box and labeled 'Step 4: Click “Update” button'. A blue arrow points from the 'Update' button in the dialog to the 'Update IPPBX' option in the sidebar, labeled 'Step 1: Select IP-PBX'.

Chapter 3 Web configuration for Router functions

3.1 System status

3.1.1 Link status

You can get the following information in **Link status** window

- LAN Status,
- WAN Status,
- Firmware Version

LAN Status: Shows the information of MAC Address, IP Address, Subnet Mask and DHCP Status (Enable/Disable).

WAN Status: Shows the information of MAC Address, IP Address, and Subnet Mask on each or all WAN ports

Firmware version: version of software and its released date.

System status - Link status

The screenshot shows the web configuration interface for the SHS 3830 router. The main content area is titled "Link status" and contains three tables:

Port	IP address	MAC address	Subnet mask	DHCP
LAN	192.168.1.253	00:09:2C:10:1B:6D	255.255.255.0	Disable

Port	IP address	MAC address	Subnet mask	Status	Button
WAN1	DHCP	00:09:2C:10:1B:6B	255.255.255.0	Disconnected	<input type="button" value="Connect"/>
WAN2	DHCP	00:09:2C:10:1B:6C	255.255.255.0	Disconnected	<input type="button" value="Connect"/>

Firmware	Version number	Release date
SHS3830	V0028	2014-09-25 10:10:46+08:00

Below the tables is a "Refresh" button.

3.1.2 Data monitor

Differ from "Link status", "Data monitor" indicates detailed packets transmitted and received status and system status at the moment.

System status

CPU usage / Memory usage / Live time

Packet transfer status

Current Session / TCP Session / UDP Session / Accumulative Session

Bandwidth

Current Bandwidth / Download Speed / Upload Speed
Load Balance
 Load balance / Byte Received / Byte Transmitted / Total Bytes
System status - Data monitor

SHS 3830

System status menu items: Welcome, System status (selected), Link status, Data monitor (selected), DHCP clients table, NAT table, Current routing table, WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, Save & reboot.

Data Monitor

CPU usage%	Memory usage%	Live time
0.0%	66.9%	20:19:27 up 20:19

Current session	TCP Session	UDP Session	Accumulative session
WAN1	0	0	0
WAN2	0	0	0

Current Bandwidth	Download Speed (bytes/sec)	Upload Speed (bytes/sec)
WAN1	0	0
WAN2	0	0

Load balance	Rate(%)	Bytes Received (K bytes)	Bytes Transmitted (K bytes)	Total Bytes (K bytes)
WAN1	0	0	0	0
WAN2	0	0	0	0

1K bytes=8K bits

3.1.3 DHCP Clients table

You can get the detail information of DHCP clients in following window.

System status – DHCP Clients table

SHS 3830

System status menu items: Welcome, System status (selected), Link status, Data monitor, DHCP clients table (selected), NAT table, Current routing table, WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, Save & reboot.

DHCP clients Table

Item	Mac Address	IP Address	Host Name	Expires In
------	-------------	------------	-----------	------------

3.1.4 NAT table

Display NAT (Network Address Translation) sessions occurred at the moment in router. NAT is widely implemented in router in order to resolve not sufficient IPs in IPv4, and functions as IP translation between public IP and private IP. Time means life time for each session type while session active.

System status – NAT table

Protocol	Time	Local IP	Local Port	Destination IP	Destination Port	Gateway IP	Gateway Port
UDP	12	192.168.1.249	5060	192.168.1.253	5060	192.168.1.249	5060
UDP	10	192.168.1.50	138	192.168.1.255	138	192.168.1.50	138
UDP	13	192.168.1.169	17500	255.255.255.255	17500	192.168.1.169	17500
UDP	1	192.168.1.44	56219	192.168.1.255	8612	192.168.1.44	56219
UDP	5	192.168.1.44	17500	255.255.255.255	17500	192.168.1.44	17500
UDP	9	192.168.1.44	54306	224.0.0.1	8612	192.168.1.44	54306
UDP	59	192.168.1.253	5060	85.25.73.181	5060	192.168.1.253	5060
UDP	9	192.168.1.76	17500	255.255.255.255	17500	192.168.1.76	17500
UDP	3	192.168.1.50	137	192.168.1.255	137	192.168.1.50	137
TCP	1799	192.168.1.45	49658	192.168.1.253	80	192.168.1.45	49658
UDP	5	192.168.1.44	17500	192.168.1.255	17500	192.168.1.44	17500
UDP	16	192.168.1.44	56603	224.0.0.1	8612	192.168.1.44	56603
UDP	15	192.168.1.45	17500	255.255.255.255	17500	192.168.1.45	17500
UDP	16	192.168.1.44	59131	192.168.1.255	8612	192.168.1.44	59131

3.1.5 Current routing table

This display shows the valid routing paths in router. Users can view the information about current routing paths.

System status – Current routing table

The screenshot shows the SHS 3830 web interface. At the top, there is a red banner with the text "SHS 3830". Below the banner is a navigation menu on the left with the following items: Welcome, System status (selected), Link status, Data monitor, DHCP clients table, NAT table, Current routing table (highlighted), WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System, IP-PBX, and Save & reboot. The main content area displays the "Current Routing Table" with the following data:

Destination network	Subnet mask	Gateway
192.168.1.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	192.168.1.1

3.2 Load balance

3.2.1 Outbound

Load Balance Router provides two load balance work modes:

Session	All the enabled WAN ports have the same (1:1) bandwidth rate.
Weight round robin	Configure the WAN ports bandwidth rate manually.

Session mode:

When choose this mode, the router will assign each coming session to each WAN port one by one, no matter how traffic loading on each WAN port.

LOAD BALANCE – Outbound (1)

SHS 3830

Welcome

▼ System status

▼ WAN configure

▼ LAN configure

▼ Load balance

Outbound

Inbound

▼ Firewall

▼ Quality control

▼ Advance

▼ System

▼ IP-PBX

Save & reboot

Outbound Load balance

Load balance by Session by IP

W1:W2:W3:W4=1:1:1:1

Weight round robin mode(ex x:2x:2x:3x)

Weight Round Robin mode:

Configure the WAN ports bandwidth rate manually, means you can distribute each coming session from users to each WAN port, following the rate that you assign in each WAN port.

The session number in each WAN can be numbered from **1 to 100**, the suggest number is under 1 ~10. If rate is 1:1 for each WAN port, the router function will act like Session mode

LOAD BALANCE – Outbound (2)

SHS 3830

Welcome

▼ System status

▼ WAN configure

▼ LAN configure

▼ Load balance

Outbound

Inbound

▼ Firewall

▼ Quality control

▼ Advance

▼ System

▼ IP-PBX

Save & reboot

Outbound Load balance

Load balance by Session by IP

W1:W2:W3:W4=1:1:1:1

Weight round robin mode(ex x:2x:3x)

WAN1:

WAN2:

USB3G:

3.2.2 Inbound

Inbound function allows incoming traffic to be allocated by inbound load balance policy so that increasingly all broadband bandwidth usage and balancing load among connected lines. Refer to Chapter 4 for more information.

For example, please follow these steps as below for adding an item.
 Step 1: Enter **inbound** web page. Then click “Add” to enter the added page.

LOAD BALANCE – Inbound

Welcome

- System status
- WAN configure
- LAN configure
- Load balance**
- Outbound
- Inbound
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

Inbound Load balance

Item	Domain	Seq.	Address	Weight	Enable	Edit
------	--------	------	---------	--------	--------	------

Add Apply

Step 2: Fill data to Domain name. If Type is IP, user must fill an IP for selected WAN port. If Type is WAN, User does NOT fill IP address. Then Click “Add” then router go back to **Inbound** list table.

Welcome

- System status
- WAN configure
- LAN configure
- Load balance**
- Outbound
- Inbound
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

Inbound Load balance

Edit Inbound Item 1

Domain name

Seq.	Type	WAN	Ip Address	Weight
1	<input type="radio"/> None <input type="radio"/> Wan <input checked="" type="radio"/> Ip	WAN1	172.168.1.10	1
2	<input type="radio"/> None <input type="radio"/> Wan <input checked="" type="radio"/> Ip	WAN2	172.168.1.11	1
3	<input type="radio"/> None <input checked="" type="radio"/> Wan <input type="radio"/> Ip	WAN1		1
4	<input type="radio"/> None <input checked="" type="radio"/> Wan <input type="radio"/> Ip	WAN2		2
5	<input type="radio"/> None <input checked="" type="radio"/> Wan <input type="radio"/> Ip	USB3G		3
6	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	WAN1		1
7	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	WAN1		1
8	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	WAN1		1

Delete Add

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance**
 - Outbound
 - Inbound**
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

Inbound Load balance

Item	Domain	Seq.	Address	Weight	Enable	Edit
1	www.tl.in	1	172.168.1.10	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		2	172.168.1.11	1	<input type="checkbox"/>	<input type="checkbox"/>
		3	WAN1	1	<input type="checkbox"/>	<input type="checkbox"/>
		4	WAN2	2	<input type="checkbox"/>	<input type="checkbox"/>

Add Apply

Option: Edit or Delete

Step 1: Enter **Inbound** web page. Then click “Enable” check square of item 2 to enter the edited page.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance**
 - Outbound
 - Inbound**
- Firewall
- Quality control
- Advance
- System
- Save & reboot

Inbound Load balance

Item	Domain	Seq.	Address	Weight	Enable	Edit
1	www.tl.in	1	172.168.1.10	1	<input type="checkbox"/>	<input type="checkbox"/>
		2	172.168.1.11	1	<input type="checkbox"/>	<input type="checkbox"/>
		3	WAN1	1	<input type="checkbox"/>	<input type="checkbox"/>
		4	WAN2	2	<input type="checkbox"/>	<input type="checkbox"/>
2	www.t2.in	1	WAN1	1	<input type="checkbox"/>	<input type="checkbox"/>
		2	WAN2	2	<input type="checkbox"/>	<input type="checkbox"/>
		3	172.16.1.100	3	<input type="checkbox"/>	<input type="checkbox"/>

Add Apply

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router go back to **Inbound** list table. If users want to edit, click “add” when user finish editing job. Then router go back to **Inbound** list table.

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Outbound
- Inbound
- Firewall
- Quality control
- Advance
- System
- Save & reboot

Inbound Load balance

Edit Inbound Item 2

Domain name

Seq.	Type	WAN	Ip Address	Weight
1	<input type="radio"/> None <input checked="" type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="3"/>
2	<input type="radio"/> None <input checked="" type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN2"/>	<input type="text"/>	<input type="text" value="2"/>
3	<input type="radio"/> None <input type="radio"/> Wan <input checked="" type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text" value="172.16.1.200"/>	<input type="text" value="1"/>
4	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="1"/>
5	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="1"/>
6	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="1"/>
7	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="1"/>
8	<input checked="" type="radio"/> None <input type="radio"/> Wan <input type="radio"/> Ip	<input type="text" value="WAN1"/>	<input type="text"/>	<input type="text" value="1"/>

Step 3: Go back to **Inbound** list table

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Outbound
- Inbound
- Firewall
- Quality control
- Advance
- System
- Save & reboot

Inbound Load balance

Item	Domain	Seq.	Address	Weight	Enable	Edit
1	www.t1.in	1	172.168.1.10	1	<input type="checkbox"/>	<input type="checkbox"/>
		2	172.168.1.11	1		
		3	WAN1	1		
		4	WAN2	2		
2	www.t2.in	1	WAN1	3	<input type="checkbox"/>	<input type="checkbox"/>
		2	WAN2	2		
		3	172.16.1.200	1		

3.3 Firewall

Firewall indeed is a big issue in networking, not only protect router from attack, but also complex inspection cause not so friendly usage experience while configured. Therefore how to make it easily and highly workable by user is an important issue for designer. Below supported functions by router are the most useful for deployment in real networking environment.

- Super Users

- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- Intrusion security
- Messenger blocking
- IP session limit

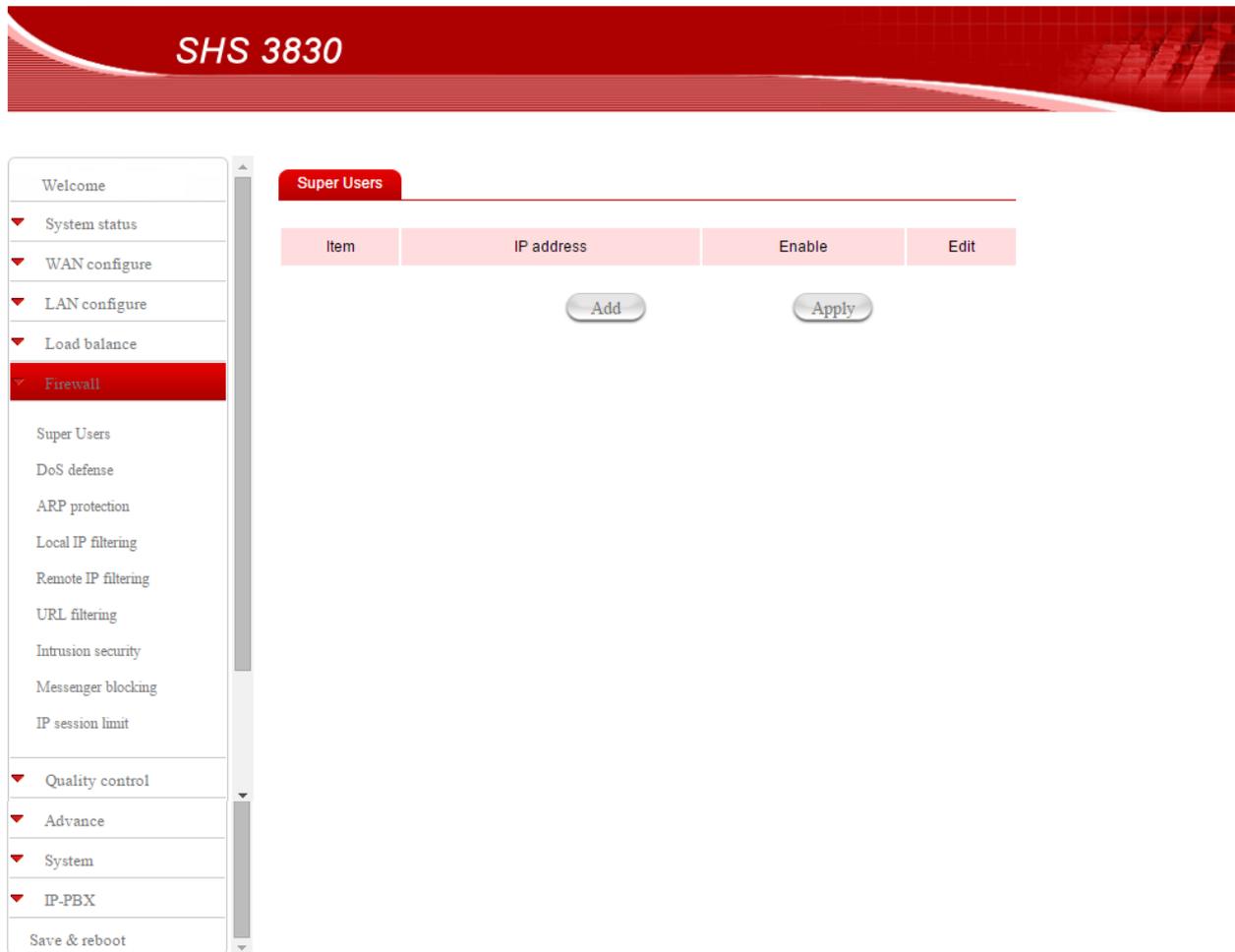
3.3.1 Super Users

The SHS 3830 allows super users IP can access Internet without limitation when enable block function.

Option: Add a new item.

Step 1: Enter **Super Users** web page. Then click “Add” to enter the added page.

Firewall – Super users



Step 2: Fill data to IP address. Then Click “Add” then router goes back to **Super Users** list table.

The screenshot shows the 'Super Users' configuration page. On the left is a navigation menu with 'Firewall' expanded to show 'Super Users'. The main content area is titled 'Super Users' and 'Edit Super Users Item 1'. It features a form with an 'IP address' field containing '192.168.1.99' and two buttons: 'Delete' and 'Apply'.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

The screenshot shows the 'Super Users' configuration page in list view. The left navigation menu is the same. The main content area is titled 'Super Users' and displays a table with the following data:

Item	IP address	Enable	Edit
1	192.168.1.99	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Below the table are two buttons: 'Add' and 'Apply'.

Option: Edit or Delete

Step 1: Enter **Super Users** web page. Then click “Enable” check square of item 2 to enter the edited page.

Item	IP address	Enable	Edit
1	192.168.1.99	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.100	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.200	<input type="checkbox"/>	<input type="checkbox"/>

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Super Users** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Super Users** list table.

Edit Super Users Item 2

IP address

Step 3: Router go back to **Super Users** list table.

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

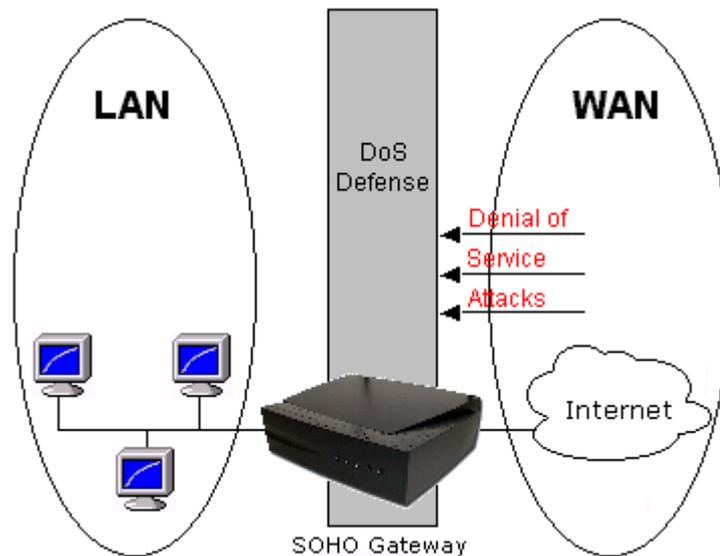
Super Users

Item	IP address	Enable	Edit
1	192.168.1.99	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.150	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.200	<input type="checkbox"/>	<input type="checkbox"/>

Add
Apply

3.3.2 DoS defense

The SHS 3830 also provides with DoS (Denial of Service Defense) function to protect your network servers, hosts, routers and other devices from the attacking of villain using mass data transmission. The default value in the display is the optimize parameter for Router.



Firewall – DoS defense – LAN DoS Defense

SHS 3830

- LAN configure
- Load balance
- Firewall
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security
 - Messenger blocking
 - IP session limit
- Quality control
- Advance
- System

LAN DoS Defense
WAN DoS Defense

LAN DoS Defense Enable Disable

Function	Enable
Disable Ping(ICMP) respond	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Fragments Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Function	Parameter	Lock Time	Enable
Port Scan	<input type="text" value="50"/> times/sec	<input type="text" value="6"/> sec	<input type="checkbox"/>

Function	Parameter	Burst	Enable
TCP SYN Flooding	<input type="text" value="500"/> times/sec	<input type="text" value="50"/> times	<input checked="" type="checkbox"/>
ICMP Flooding	<input type="text" value="10"/> times/sec	<input type="text" value="1"/> times	<input checked="" type="checkbox"/>
Oversized Ping	<input type="text" value="1"/> times/sec	<input type="text" value="1"/> times	<input checked="" type="checkbox"/>
UDP Flooding	<input type="text" value="500"/> times/sec	<input type="text" value="50"/> times	<input checked="" type="checkbox"/>

Firewall – DoS defense – WAN DoS Defense

SHS 3830

- LAN configure
- Load balance
- Firewall
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security
 - Messenger blocking
 - IP session limit
- Quality control
- Advance
- System
- IP PRV

LAN DoS Defense
WAN DoS Defense

WAN DoS Defense Enable Disable

Function	Enable
Disable Ping(ICMP) respond	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Fragments Checking	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address spoofing	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Function	Parameter	Lock Time	Enable
Port Scan	<input type="text" value="50"/> times/sec	<input type="text" value="6"/> sec	<input type="checkbox"/>

Function	Parameter	Burst	Enable
TCP SYN Flooding	<input type="text" value="500"/> times/sec	<input type="text" value="50"/> times	<input checked="" type="checkbox"/>
ICMP Flooding	<input type="text" value="10"/> times/sec	<input type="text" value="1"/> times	<input checked="" type="checkbox"/>
Oversized Ping	<input type="text" value="1"/> times/sec	<input type="text" value="1"/> times	<input checked="" type="checkbox"/>
UDP Flooding	<input type="text" value="500"/> times/sec	<input type="text" value="50"/> times	<input checked="" type="checkbox"/>

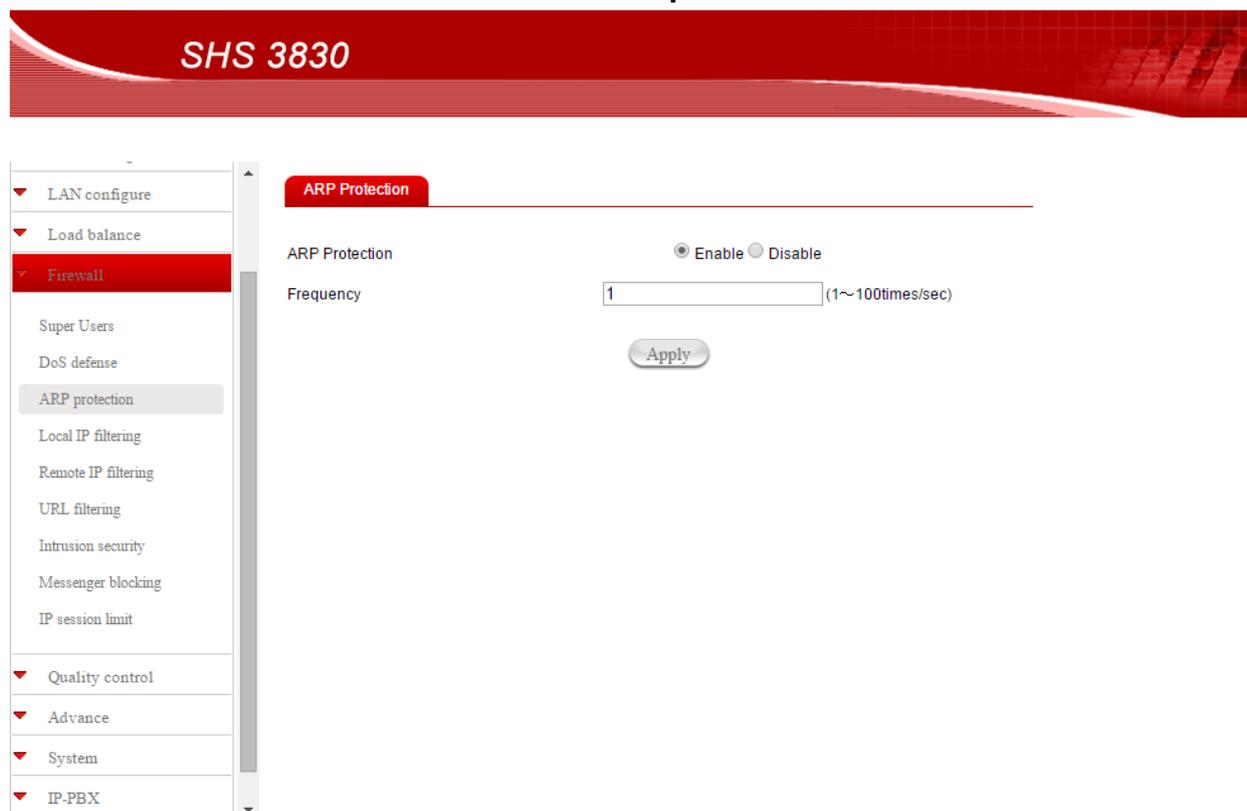
* Some virus are using “PING” command to attack network, this Router can be defined as accept or reject “PING” command from WAN or LAN.

Function	Description
IP Fragments Checking	Checking the IP fragments. When it finds someone from WAN side tries to attack your network using overlap IP fragments in a bad attention, this function will check over these packets and drop them.
IP Address spoofing	Finding out whether the source address(s) and destination address(s) are legal IP's or not. If they are illegal IP's or multicast addresses, this function will cast these packets away.
Port Scan	When an IP from Internet tries to scan the IP of Load Balance Router up to 10000ports/sec (default value), this function will drop all the packets from this IP within 5 minutes (default value).
TCP SYN Flooding (WAN)	When a destination address and destination port of Load Balance Router receives TCP SYN packet from WAN over 10000 times (default value) in one second, Load Balance Router will close this address and port for 5 minutes (default value) temporarily.
TCP SYN Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send TCP SYN packet over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.
ICMP Flooding (WAN)	When a destination address of Load Balance Router receives ICMP from WAN over 10000 times (default value) in one second, Load Balance Router will close this address for 5 minutes (default value) temporarily.
ICMP Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send ICMP over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.
UDP Flooding (WAN)	When a destination address of Load Balance Router receives UDP from WAN over 10000 times (default value) in one second, Load Balance Router will close this address for 5 minutes (default value) temporarily.
UDP Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send UDP over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.

3.3.3 ARP protection

It prevents network hosts from ARP spoofing attack so that enable the function to immune any ARP spoofing. So router updates ARP message for hosts to keep accurate ARP table restoring in hosts due to attacker sending spoofed ARP while attacking.

Firewall – ARP protection



3.3.4 Local IP filtering

SHS 3830 allows you to do accessed restriction of block/allow outgoing IP packets by protocol (port number).

You may restrict some IP's only to perform limited protocols or allow them to execute partial protocols. And the first thing you have to know is the port numbers and their usages.

Option: Add a new item.

Step 1: Enter **Local IP filtering** web page. Then click “Add” to enter the added page.

Firewall – Local IP filtering

SHS 3830

Local IP Filtering

Item	Local start IP address	Local stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
------	------------------------	-----------------------	-------	------------------------	-----------------------	--------	------

Add Apply

Step 2: Fill data to Local Start IP, Local Stop IP, Protocol, Local Port and Local Stop Port. Then click “Add” then router goes back to **Local IP filtering** list table.

SHS 3830

Local IP filtering

Edit Local IP Filtering Item 1

Local start IP address: 192.168.1.13

Local stop IP address: 192.168.1.15

TCP/UDP: TCP

Destination start port: 5000

Destination stop port: 5020

Delete Apply

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

Item	Local start IP address	Local stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	192.168.1.13	192.168.1.15	TCP	5000	5020	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Option: Edit or Delete

Step 1: Enter **Local IP filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.

Item	Local start IP address	Local stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	192.168.1.13	192.168.1.15	TCP	5000	5020	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.30	192.168.1.50	UDP	7000	7020	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.100	192.168.1.200	TCP	10000	11000	<input type="checkbox"/>	<input type="checkbox"/>

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Local IP filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Local IP filtering** list table.

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Local IP filtering

Edit Local IP Filtering Item 2

Local start IP address:

Local stop IP address:

TCP/UDP:

Destination start port:

Destination stop port:

Step 3: Router go back to **Local IP filtering** list table.

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Local IP Filtering

Item	Local start IP address	Local stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	192.168.1.13	192.168.1.15	TCP	5000	5020	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.30	192.168.1.50	UDP	7000	8000	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.100	192.168.1.200	TCP	10000	11000	<input type="checkbox"/>	<input type="checkbox"/>

3.3.5 Remote IP filtering

As name implied, router filters remote IP user desire to and set below.

Option: Add a new item.

Step 1: Enter **Remote IP filtering** web page. Then click “Add” to enter the added page.

Firewall – Remote IP filtering

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security
 - Messenger blocking
 - IP session limit
- Quality control

Remote IP Filtering

Item	Remote start IP address	Remote stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
------	-------------------------	------------------------	-------	------------------------	-----------------------	--------	------

Add Apply

Step 2: Fill data to Remote Start IP, Remote Stop IP, Protocol, Remote Port and Remote Stop Port. Then Click “Add” then router goes back to **Remote IP filtering** list table.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security
 - Messenger blocking
 - IP session limit
- Quality control

Remote IP Filtering

Edit Remote IP Filtering Item 1

Remote start IP address: 172.16.1.13

Remote stop IP address: 172.16.1.15

TCP/UDP: TCP

Destination start port: 1000

Destination stop port: 1010

Delete Apply

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

Remote IP Filtering

Item	Remote start IP address	Remote stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	172.16.1.13	172.16.1.15	TCP	1000	1010	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Option: Edit or Delete

Step 1: Enter **Remote IP filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.

Remote IP Filtering

Item	Remote start IP address	Remote stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	172.16.1.13	172.16.1.15	TCP	1000	1010	<input type="checkbox"/>	<input type="checkbox"/>
2	172.16.1.100	172.16.1.200	UDP	2000	2010	<input type="checkbox"/>	<input type="checkbox"/>
3	172.16.1.30	172.16.1.50	ALL	1700	1800	<input type="checkbox"/>	<input type="checkbox"/>

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Remote IP filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Remote IP filtering** list table.

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Remote IP Filtering

Edit Remote IP Filtering Item 2

Remote start IP address

Remote stop IP address

TCP/UDP

Destination start port

Destination stop port

Step 3: Router go back to **Remote IP filtering** list table.

- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Remote IP Filtering

Item	Remote start IP address	Remote stop IP address	Proto	Destination start port	Destination stop port	Enable	Edit
1	172.16.1.13	172.16.1.15	TCP	1000	1010	<input type="checkbox"/>	<input type="checkbox"/>
2	172.16.1.80	172.16.1.90	UDP	2000	2010	<input type="checkbox"/>	<input type="checkbox"/>
3	172.16.1.30	172.16.1.50	ALL	1700	1800	<input type="checkbox"/>	<input type="checkbox"/>

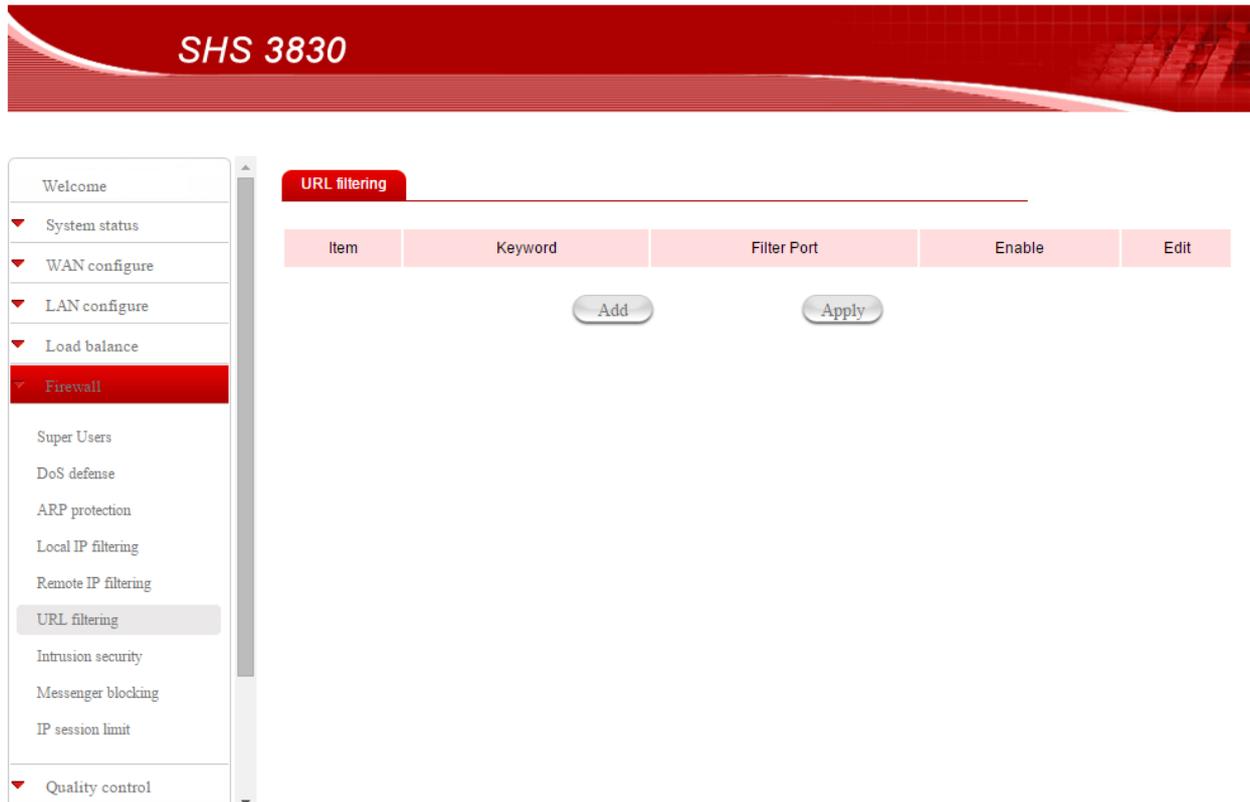
3.3.6 URL filtering

Besides restrict users by local/destination IP, the SHS 3830 provides you to do accessed restriction for user by URL as well. You may restrict some URL address that are not allow to reach

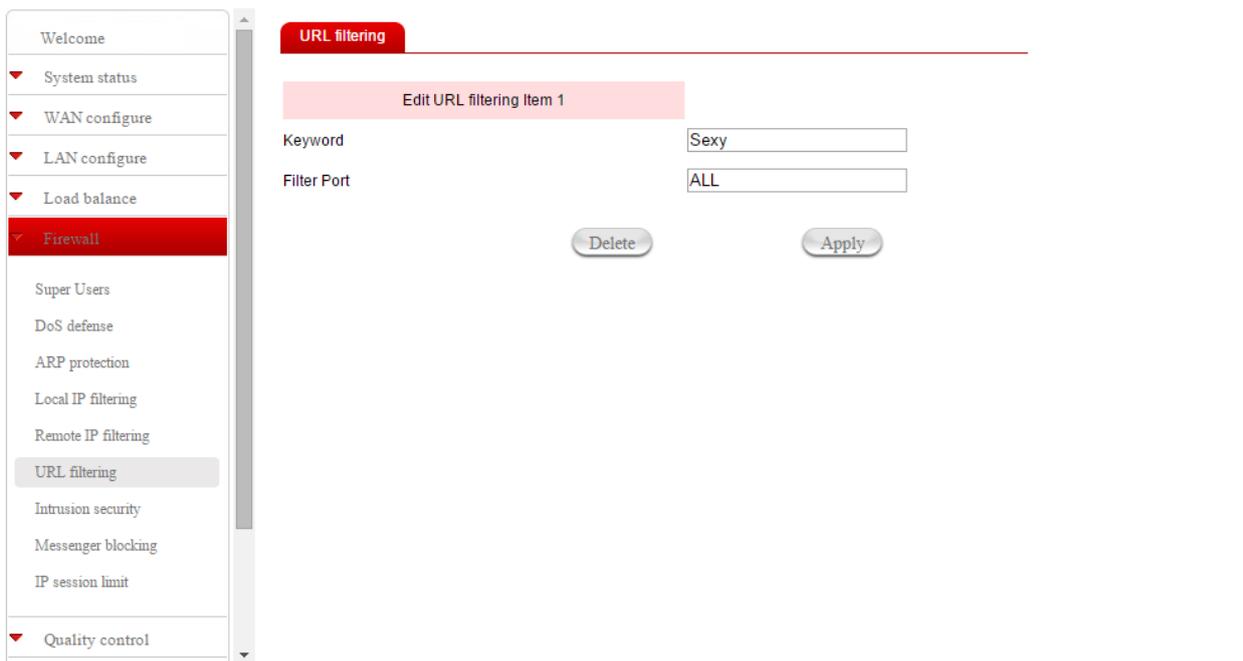
Option: Add a new item.

Step 1: Enter **URL filtering** web page. Then click “Add” to enter the added page.

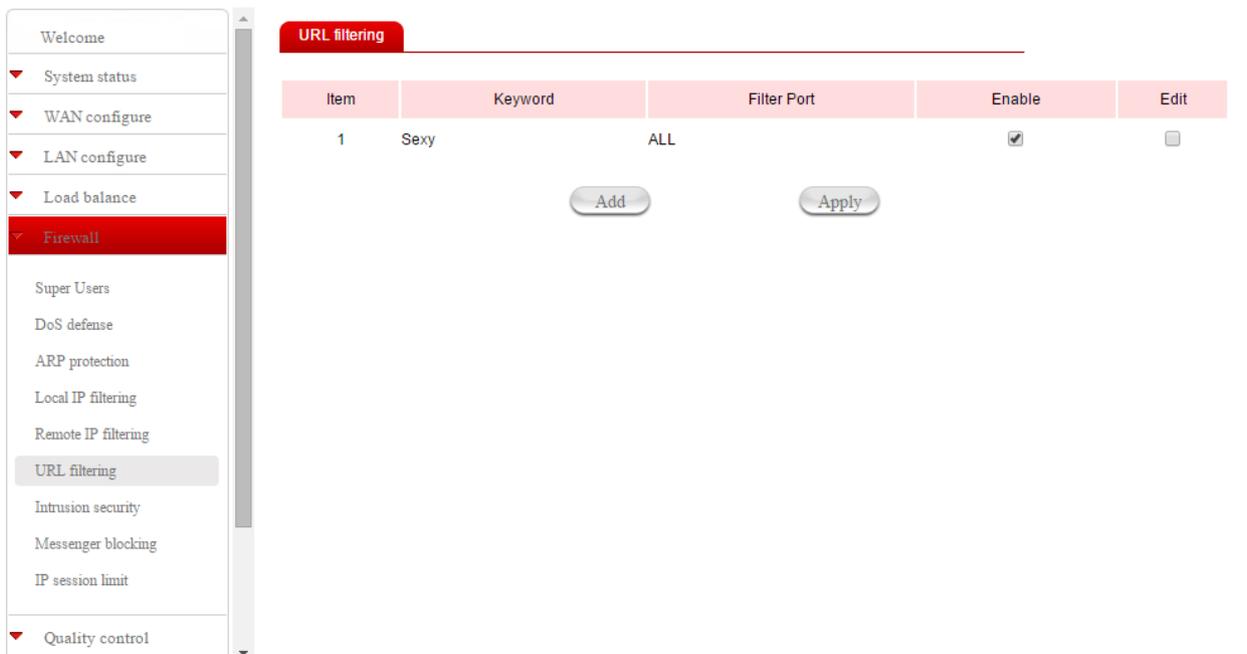
Firewall – URL filtering



Step 2: Fill data to Keyword and Filter Port. You can write a number or ALL to Filter Port. Then Click “Add” then router goes back to **URL filtering** list table.



Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Option: Edit or Delete

Step 1: Enter **URL filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.

Item	Keyword	Filter Port	Enable	Edit
1	Sexy	ALL	<input type="checkbox"/>	<input type="checkbox"/>
2	abc	80	<input type="checkbox"/>	<input type="checkbox"/>
3	check	1000	<input type="checkbox"/>	<input type="checkbox"/>

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **URL filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **URL filtering** list table.

Edit URL filtering Item 2

Keyword

Filter Port

Step 3: Router go back to **URL filtering** list table.



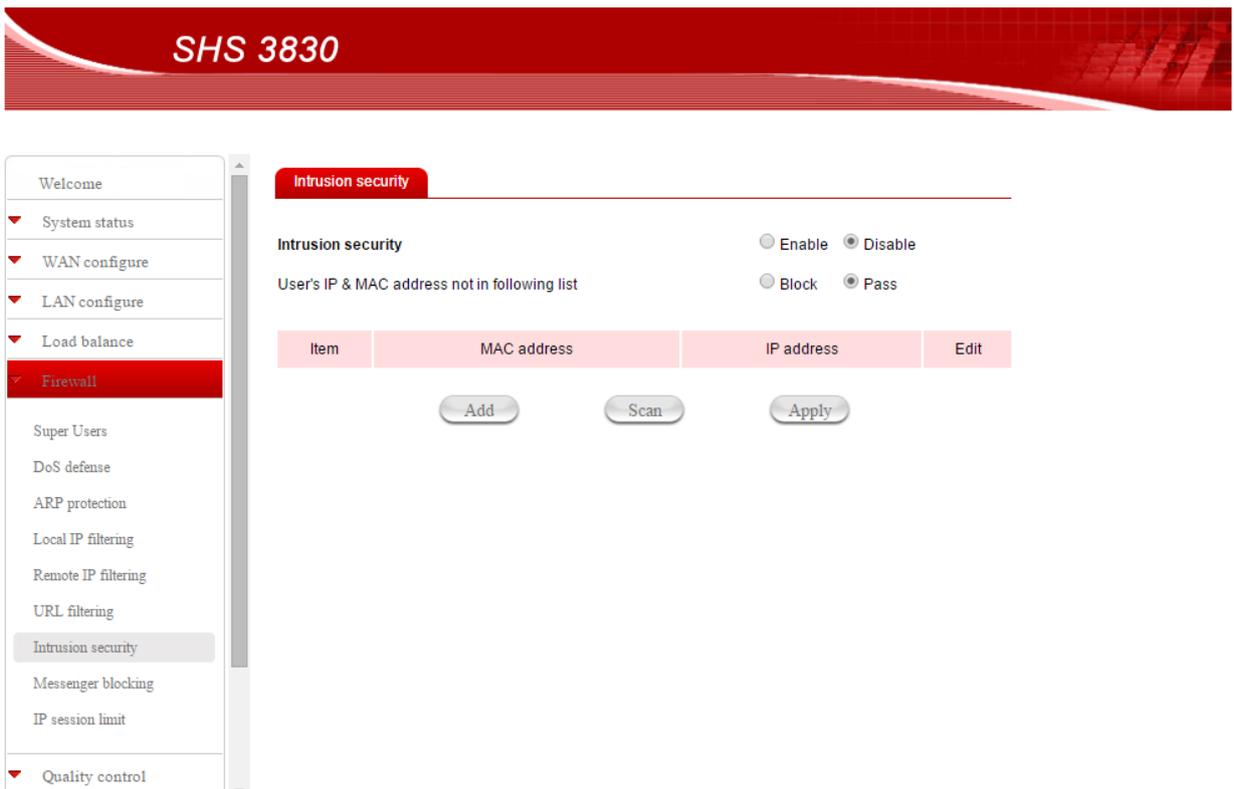
3.3.7 Intrusion security

Pre-setting IP & MAC mapping to prevent from not anticipate association for security consideration. By setting up this table router will perform “BLOCK” or “PASS” function according to the option.

Option: Add a new item.

Step 1: Enter **Intrusion security** web page. Then click “Add” to enter the added page.

Firewall – Intrusion security



Step 2: Fill data to MAC address and IP. Then Click “Add” then router go back to **Intrusion security** list table.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security**
 - Messenger blocking
 - IP session limit
- Quality control

Intrusion Security

Add Intrusion Security Item

MAC address : : : : :

IP address

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
 - Super Users
 - DoS defense
 - ARP protection
 - Local IP filtering
 - Remote IP filtering
 - URL filtering
 - Intrusion security**
 - Messenger blocking
 - IP session limit
- Quality control

Intrusion security

Intrusion security Enable Disable

User's IP & MAC address not in following list Block Pass

Item	MAC address	IP address	Edit
1	00:01:02:45:5B:2A	192.168.1.99	<input type="checkbox"/>

Option: Edit or Delete

Step 1: Enter **Intrusion security** web page. Then click “Enable” check square of item 2 to enter the edited page.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Intrusion security

Enable Disable

Block Pass

User's IP & MAC address not in following list

Item	MAC address	IP address	Edit
1	00:01:02:45:5B:2A	192.168.1.99	<input type="checkbox"/>
2	00:03:02:46:6B:7C	192.168.1.199	<input checked="" type="checkbox"/>
3	00:12:45:67:9B:2C	192.168.1.100	<input type="checkbox"/>

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Intrusion security** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Intrusion security** list table.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall**
- Super Users
- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- URL filtering
- Intrusion security
- Messenger blocking
- IP session limit

Intrusion Security

Edit Intrusion Security Item 2

MAC address: 00 : 03 : 02 : 46 : 6B : 7C

IP address: 192.168.1.150

Step 3: Router go back to **Intrusion security** list table.

Intrusion security

Enable Disable

Block Pass

User's IP & MAC address not in following list

Item	MAC address	IP address	Edit
1	00:01:02:45:5B:2A	192.168.1.99	<input type="checkbox"/>
2	00:03:02:46:6B:7C	192.168.1.150	<input type="checkbox"/>
3	00:12:45:67:9B:2C	192.168.1.100	<input type="checkbox"/>

Add Scan Apply

Example: Scan all PC connect with Router. Directly click scan. It will clear all old data. Replace it with scanned data. But it need some time to scan all PC. The delay time depend on PC quantity.

SHS 3830

Intrusion Security

Intrusion Security auto scan configure saved success!

確定

Intrusion security

Enable Disable

Block Pass

User's IP & MAC address not in following list

Item	MAC address	IP address	Edit
1	00:23:54:74:DB:EB	192.168.1.10	<input type="checkbox"/>

3.3.8 Messenger Blocking

Router can block below traffic packet from LAN to WAN. For some exception Router allow **Super users** IP can access Internet without limitation when enable block function Instant Message Blocking/ P2P BT Blocking

Firewall – Messenger blocking

Messenger Blocking

- YAHOO Blocking
- QQ Blocking
- QQ GAME Blocking
- PAOPAO Blocking
- eMUTE Blocking
- BT Blocking

3.3.9 IP session limit

For each user IP default session limit is 200. Session amounts per each IP can be change from 200 to 65,000.

Firewall – IP session limit

SHS 3830

IP Session limit

Item	IP address	Session Limit (50~65535)	Enable
0	All IP	200	<input type="checkbox"/>

Item	Exception IP	Session Limit (50~65535)	Enable
1	<input type="text"/>	200	<input type="checkbox"/>
2	<input type="text"/>	200	<input type="checkbox"/>
3	<input type="text"/>	200	<input type="checkbox"/>
4	<input type="text"/>	200	<input type="checkbox"/>
5	<input type="text"/>	200	<input type="checkbox"/>

Apply

3.4 Quality control

- QoS
- Bandwidth control
- Outgoing route
- LAN IP speed limit

3.4.1 QoS

With this function, you can set up **USER BANDWIDTH** with Maximum & Minimum bandwidth value.

Configure WAN Speed

The WAN speeds must be configured for the QoS configuration to take effect.

IP MAX/MIN Limit

Allocate bandwidths to users.

- IP: IP address of specified user.
- MAX: Bandwidth limitation to this user.
- MIN: Minimal Bandwidth kept for this user before allocating any bandwidth from this user to others.
- Down Rate: Download speed.

- Up Rate: Upload speed.
- WAN Apply: Which WAN you want the allocation to take effect. (Do not use this option to specify which WAN to use for this user.)

Quality Control – QoS

SHS 3830

Welcome

- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- ▼ IP-PBX
- Save & reboot

QoS

When QoS enabled, router allocated average WAN bandwidth to each IP automatically

QoS Enable Disable

Quality control – QoS Enable

SHS 3830

Welcome

- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- ▼ IP-PBX
- Save & reboot

QoS

When QoS enabled, router allocated average WAN bandwidth to each IP automatically

QoS Enable Disable

* Please fill in each WAN real speed

WAN	WAN speed Upload(k bits/s)	WAN speed Download(k bits/s)
WAN 1	<input type="text" value="100000"/>	<input type="text" value="100000"/>
WAN 2	<input type="text" value="100000"/>	<input type="text" value="100000"/>
USB 3G modem	<input type="text" value="100000"/>	<input type="text" value="100000"/>

Default WAN speed is 100M bits/s

3.4.2 Bandwidth Control

This is a very useful function, it can let you to control WAN port bandwidth usage by each protocol. Like FTP

When someone uses FTP to transfer file, it will occupied heavy bandwidth, by using this function, you can limit allocated bandwidth.

Dedicated application bandwidth

For example:

In following display, FTP, HTTP & Mail bandwidth will be limit in certain percentage. This router provide 3 most often use protocol in the table, Just fill in port number and % usage for each application.

Protocol ... name of protocol data packet will be limit.

Port ... protocol port number

Usage: % of WAN speed can be used.

Protocol % usage cannot exceed 100% for each WAN port.

Router provides another 4-user self-define port number for easy use, just fill in port number for each protocol.

Step 1: Enter **Quality Control** web page.

Quality Control – Bandwidth usage control

Description	PROTO	PORT	MAX Upload rate (k bits)	MAX Download rate (k bits)	Enable	Edit
HTTP	TCP	80	0	0	<input type="checkbox"/>	<input type="checkbox"/>
POP3	TCP	110	0	0	<input type="checkbox"/>	<input type="checkbox"/>
SMTP	TCP	25	0	0	<input type="checkbox"/>	<input type="checkbox"/>
FTP	TCP	21	0	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Step 2: Click the “Edit” check square of FTP. Then enter its edit page

Welcome

- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- ▼ IP-PBX
- Save & reboot

Bandwidth Usage control

Edit Bandwidth Usage control Item 4

Description	<input type="text" value="FTP"/>
TCP/UDP	<input type="text" value="TCP"/>
Port	<input type="text" value="21"/>
MAX Upload speed(k bits/s)	<input type="text" value="0"/>
MAX Download speed (k bits/s)	<input type="text" value="0"/>

Delete
Apply

Step 3: There are 5 fields in the page.

Description: It will be display in bandwidth table.

TCP/UDP: The AP use protocol. Example: FTP use TCP.

Port: The AP use port.

MAX Upload speed: The AP's maximum upload speed. Its unit is kbit.

MAX Download speed: The AP's maximum download speed. Its unit is kbit.

Finish the job then click "Apply" to save parameter and go back Bandwidth control table.

Welcome

- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- ▼ IP-PBX
- Save & reboot

Bandwidth Usage Control

* Using this function need to enable QoS

Description	PROTO	PORT	MAX Upload rate (k bits)	MAX Download rate (k bits)	Enable	Edit
HTTP	TCP	80	0	0	<input type="checkbox"/>	<input type="checkbox"/>
POP3	TCP	110	0	0	<input type="checkbox"/>	<input type="checkbox"/>
SMTP	TCP	25	0	0	<input type="checkbox"/>	<input type="checkbox"/>
FTP	TCP	21	10000	10000	<input type="checkbox"/>	<input type="checkbox"/>

Add
Apply

Step 4: Click the “Enable” check square of FTP. Then Click “Apply”.

If user would like to create a new protocol, please follow below steps:

Step 1: Enter Bandwidth control web page.

Step 2: Click the “Add” then enter its added page. Set parameters in below page.
Then click “Apply”.

Step 3: Click the “Enable” check square of APP1. Then Click “Apply”.

Description	PROTO	PORT	MAX Upload rate (k bits)	MAX Download rate (k bits)	Enable	Edit
HTTP	TCP	80	0	0	<input type="checkbox"/>	<input type="checkbox"/>
POP3	TCP	110	0	0	<input type="checkbox"/>	<input type="checkbox"/>
SMTP	TCP	25	0	0	<input type="checkbox"/>	<input type="checkbox"/>
FTP	TCP	21	10000	10000	<input type="checkbox"/>	<input type="checkbox"/>
APP1	UDP	1000	2000	2000	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3.4.3 Outgoing route

This function can let you arrange data packet from specific IP address to access Internet by designated WAN port. With this function, you can easily let VOIP packet or other special applications with high bandwidth in designated WAN port in order to have best performance.

Example: Add a new item.

Step 1: Enter **Outgoing route** web page. Then click “Add” to enter the added page.

Quality Control – Outgoing route

The screenshot shows the SHS 3830 web interface. At the top, there is a red header with the text "SHS 3830". Below the header, there is a navigation menu on the left side with the following items: Welcome, System status, WAN configure, LAN configure, Load balance, Firewall, Quality control (highlighted), QoS, Bandwidth control, Outgoing Route (highlighted), LAN IP Speed limit, Advance, System, IP-PBX, and Save & reboot. The main content area is titled "Outgoing route" and contains a table with the following columns: Item, Start IP address, End IP address, PROTO, Destination start port, Destination stop port, Select WAN, Enable, and Edit. Below the table, there are two buttons: "Add" and "Apply".

Step 2: Fill data to Destination network, Netmask and Gateway IP. Then Click “Add” then router goes back to **Outgoing route** list table.

The screenshot shows the 'Outgoing route' configuration page. On the left is a navigation menu with 'Quality control' selected. The main area is titled 'Edit Outgoing route Item 1' and contains the following fields:

- Start IP address: 192.168.1.10
- Stop IP address: 192.168.1.12
- TCP/UDP: TCP
- Destination start port: 3000
- Destination stop port: 3020
- Select WAN: AUTO

At the bottom of the form are 'Delete' and 'Apply' buttons.

Note: Select WAN has 7 items. They are AUTO, WAN1 first, WAN2 first, USB3G first, WAN1 only, WAN2 only and USB3G only.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

The screenshot shows the 'Outgoing route' configuration page in a list view. The navigation menu is the same as in the previous screenshot. The main area displays a table with the following data:

Item	Start IP address	End IP address	PROTO	Destination start port	Destination stop port	Select WAN	Enable	Edit
1	192.168.1.10	192.168.1.12	TCP	3000	3020	AUTO	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Below the table are 'Add' and 'Apply' buttons.

Example: Edit or Delete

Step 1: Enter **Outgoing route** web page. Then click “Enable” check square of item 2 to enter the edited page.

SHS 3830

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- Save & reboot

Outgoing route

Item	Start IP address	End IP address	PROTO	Destination start port	Destination stop port	Select WAN	Enable	Edit
1	192.168.1.10	192.168.1.12	TCP	3000	3020	AUTO	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.100	192.168.1.102	UDP	4000	4040	WAN1first	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.200	192.168.1.220	TCP	5000	5010	WAN2only	<input type="checkbox"/>	<input type="checkbox"/>

Add
Apply

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Outgoing route** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Outgoing route** list table.

SHS 3830

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- Save & reboot

Outgoing route

Edit Outgoing route Item 2

Start IP address

Stop IP address

TCP/UDP

Destination start port

Destination stop port

Select WAN

Delete
Apply

Step 3: Router go back to **Outgoing route** list table.

Welcome
▼ System status
▼ WAN configure
▼ LAN configure
▼ Load balance
▼ Firewall
▼ Quality control
QoS
Bandwidth control
Outgoing Route
LAN IP Speed limit
▼ Advance
▼ System
Save & reboot

Outgoing route

Item	Start IP address	End IP address	PROTO	Destination start port	Destination stop port	Select WAN	Enable	Edit
1	192.168.1.10	192.168.1.12	TCP	3000	3020	AUTO	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.100	192.168.1.120	UDP	4000	4040	WAN1first	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.200	192.168.1.220	TCP	5000	5010	WAN2only	<input type="checkbox"/>	<input type="checkbox"/>

Add

Apply

3.4.4 LAN IP Speed limit

To limit each IP bandwidth allocation in LAN so that an IP may need high data rates for specific application can be satisfied to fulfill all demands. Before the feature is effective then user need to enable QoS first.

Example: Add a new item.

Step 1: Enter **LAN IP Speed limit** web page. Then click “Add” to enter the added page.

Quality Control – LAN IP Speed limit

Welcome
▼ System status
▼ WAN configure
▼ LAN configure
▼ Load balance
▼ Firewall
▼ Quality control
QoS
Bandwidth control
Outgoing Route
LAN IP Speed limit
▼ Advance
▼ System
▼ IP-PBX
Save & reboot

LAN IP speed limit

* Using this function need to enable QoS

Item	IP address	MAX download rate kbits	MAX upload rate kbits	MIN download rate kbits	MIN upload rate kbits	Enable	Edit
------	------------	-------------------------	-----------------------	-------------------------	-----------------------	--------	------

Add

Apply

Step 2: Fill data to IP address, upload speed and Download speed. Then Click “Add” then router goes back to **LAN IP Speed limit** list table.

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control**
 - QoS
 - Bandwidth control
 - Outgoing Route
 - LAN IP Speed limit
- Advance
- System
- IP-PBX
- Save & reboot

LAN IP speed limit

Edit LAN IP speed limit Item 1

IP address: 192.168.1.11

MAX download rate kbits: 1000

MAX upload rate kbits: 1000

MIN download rate kbits: 2000

MIN upload rate kbits: 2000

Delete Apply

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable

SHS 3830

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control**
 - QoS
 - Bandwidth control
 - Outgoing Route
 - LAN IP Speed limit
- Advance
- System
- IP-PBX
- Save & reboot

LAN IP speed limit

* Using this function need to enable QoS

Item	IP address	MAX download rate kbits	MAX upload rate kbits	MIN download rate kbits	MIN upload rate kbits	Enable	Edit
1	192.168.1.11	1000	1000	2000	2000	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Apply

Example: Edit or Delete

Step 1: Enter **LAN IP Speed limit** web page. Then click “Enable” check square of item 2 to enter the edited page.

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- Save & reboot

LAN IP speed limit

* Using this function need to enable QoS

Item	IP address	MAX download rate kbits	MAX upload rate kbits	MIN download rate kbits	MIN upload rate kbits	Enable	Edit
1	192.168.1.11	1000	1000	2000	2000	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.100	1200	1200	3000	3000	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.13	1300	1300	1200	1200	<input type="checkbox"/>	<input type="checkbox"/>

Add
Apply

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **LAN IP Speed limit** list table. If user wants to edit, click “add” when user finish editing job. Then router goes back to **LAN IP Speed limit** list table.

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- Save & reboot

LAN IP speed limit

Edit LAN IP speed limit Item 2

IP address	<input style="width: 90%;" type="text" value="192.168.1.12"/>
MAX download rate kbits	<input style="width: 90%;" type="text" value="1200"/>
MAX upload rate kbits	<input style="width: 90%;" type="text" value="1200"/>
MIN download rate kbits	<input style="width: 90%;" type="text" value="3000"/>
MIN upload rate kbits	<input style="width: 90%;" type="text" value="3000"/>

Delete
Apply

Step 3: Router go back to **LAN IP Speed limit** list table.

Welcome

- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- QoS
- Bandwidth control
- Outgoing Route
- LAN IP Speed limit
- ▼ Advance
- ▼ System
- Save & reboot

LAN IP speed limit

*Using this function need to enable QoS

Item	IP address	MAX download rate kbits	MAX upload rate kbits	MIN download rate kbits	MIN upload rate kbits	Enable	Edit
1	192.168.1.11	1000	1000	2000	2000	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.12	1200	1200	3000	3000	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.13	1300	1300	1200	1200	<input type="checkbox"/>	<input type="checkbox"/>

Add
Apply

3.5 Advance

- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure

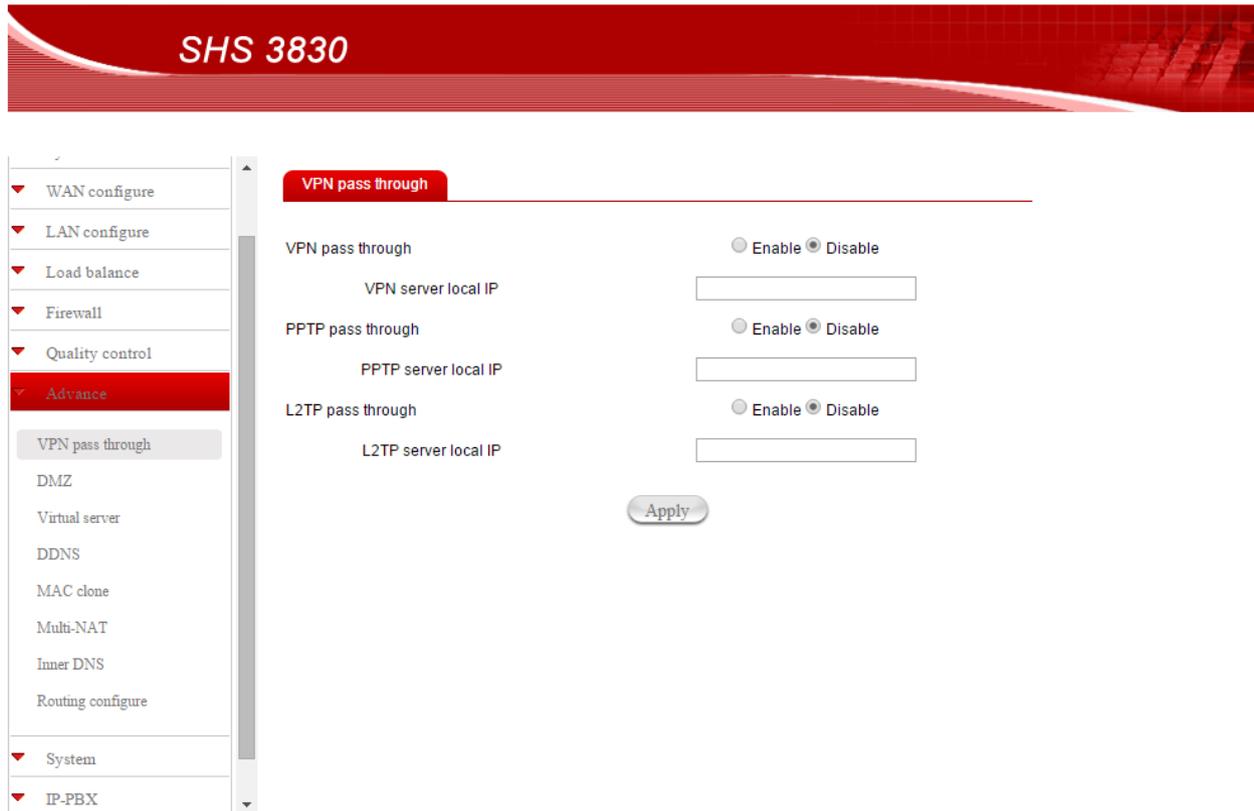
3.5.1 VPN pass through

VPN is the abbreviation for Virtual Private Network, which provide a secured link through public network by encrypting data between local and remote sides.

In order to pass through VPN traffic, router needs to recognize VPN packets and pass them in transparent way. VPN packets like IP Sec., PPTP and L2TP will not be affected and passed to the destination for appropriate process as desired.

Example: Select Pass through protocol and fill its local IP.

Advance – VPN pass through



3.5.2 DMZ

The Demilitarized Zone (DMZ) function provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers configured in DMZ Host list but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you keep all sensitive information off of the public servers. Please store sensitive information in computers on LAN.

If you would like to grant remote users the right to access one of your computers on LAN to perform some actions such as Internet games, you must enable the function of DMZ. When remote users access your legal IP(s), Load Balance Router will transmit these packets to the corresponding virtual IP(s).

Share-IP-DMZ

WAN: Host IP Address (PPPoE Mode)

When WAN port IP assigned by ISP obtained by PPPoE (**Dynamic IP**), you can fill

in DMZ host that inside the network, the router will mapping WAN IP to internal DMZ host automatically.

Example: Set the IP of WAN1 or WAN2. Click the “Enable” check square then click “Apply”

Advance – Share IP-DMZ

SHS 3830

Share-IP-DMZ Multi-DMZ

WAN	Host IP address	Enable
WAN1	<input type="text"/>	<input type="checkbox"/>
WAN2	<input type="text"/>	<input type="checkbox"/>

Apply

Multi-DMZ

When using this function, the WAN port IP need to be **FIX IP** assigned by ISP.

Example: Add a new item.

Step 1: Enter **Multi-DMZ** web page. Then click “Add” to enter the added page.

Advance – Multi-DMZ

The screenshot shows the SHS 3830 router configuration interface. The left sidebar contains a menu with the following items: WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance (highlighted), VPN pass through, DMZ (highlighted), Virtual server, DDNS, MAC clone, Multi-NAT, Inner DNS, Routing configure, System, and IP-PBX. The main content area is titled "Multi-DMZ" and features a table with the following columns: Item, DMZ host IP address, ISP provided IP address, WAN, Enable, and Edit. Below the table are "Add" and "Apply" buttons.

Step 2: Fill data to DMZ host IP address, ISP provided IP address and WAN. Then Click “Add” then router goes back to **Multi-DMZ** list table.

The screenshot shows the SHS 3830 router configuration interface. The left sidebar is the same as in the previous screenshot. The main content area is titled "DMZ" and shows the "Edit Multi-DMZ Item 1" form. The form contains the following fields: DMZ host IP address (192.168.1.31), ISP provided IP address (172.16.1.10), and WAN (WAN1). Below the form are "Delete" and "Apply" buttons.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Example: Edit or Delete

Step 1: Enter **Multi-DMZ** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Multi-DMZ** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Multi-DMZ** list table.

System status

WAN configure

LAN configure

Load balance

Firewall

Quality control

Advance

VPN pass through

DMZ

Virtual server

DDNS

MAC clone

Multi-NAT

Inner DNS

Routing configure

System

DMZ

Edit Multi-DMZ Item 2

DMZ host IP address 192.168.1.51

ISP provided IP address 172.19.1.2

WAN WAN2

Delete Apply

Step 3: Router go back to **Multi-DMZ** list table.

System status

WAN configure

LAN configure

Load balance

Firewall

Quality control

Advance

VPN pass through

DMZ

Virtual server

DDNS

MAC clone

Multi-NAT

Inner DNS

Routing configure

System

Share-IP-DMZ Multi-DMZ

Item	DMZ host IP address	ISP provided IP address	WAN	Enable	Edit
1	192.168.1.31	172.16.1.10	WAN1	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.51	172.19.1.2	WAN2	<input type="checkbox"/>	<input type="checkbox"/>

Add Apply

3.5.3 Virtual server

You may have FTP, MAIL, VPN or other server on your LAN. If you would like to allow the global users access some servers providing special services on your LAN. This function can help you to do this.

Provide with global port & local port mapping function, let you easily configure internal server with same port number mapping to WAN IP different port number.

Global port: WAN virtual protocol number

Local port: used by internal server port number

Local IP: local server IP address

For multi-wan port router, no matter data packet coming in from which WAN port (WAN IP address), router will check incoming data port number only.

For example:

Global port number 1021 map into local server IP 192.168.1.10 port 21

Global port number 8080 map into local server IP 192.168.1.10 port 80

Global port number 2323 map into local server IP 192.168.1.25 port 23

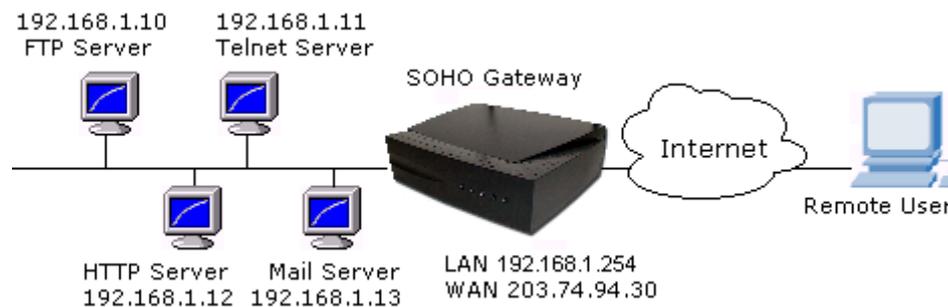
Global port number 1100 map into local server IP 192.168.1.13 port 21

You also can configure

Global port number 1022 map into local server IP 192.168.1.20 port 21

same port number in local server with different global port number

Virtual server



For example,

Supposing you want to have four servers providing FTP, HTTP, Mail and Telnet services, you must enter four virtual servers and enable them.

If users key in ftp://203.74.94.30, Load Balance Router will send the data of FTP protocol to the server of 192.168.1.10.

If users use telnet software to connect to 203.74.94.30, they will connect to the server of 192.168.1.11.

If users key in http://203.74.94.30, Load Balance Router will send the data of HTTP protocol to the server of 192.168.1.12.

If users use the email to connect to 203.74.94.30, they can receive the mails in Mail server of 192.168.1.13.

Group Virtual server eases user to configure a range of ports for some applications.

Example: Add a new item.

Step 1: Enter **Virtual server** web page. Then click “Add” to enter the added page.

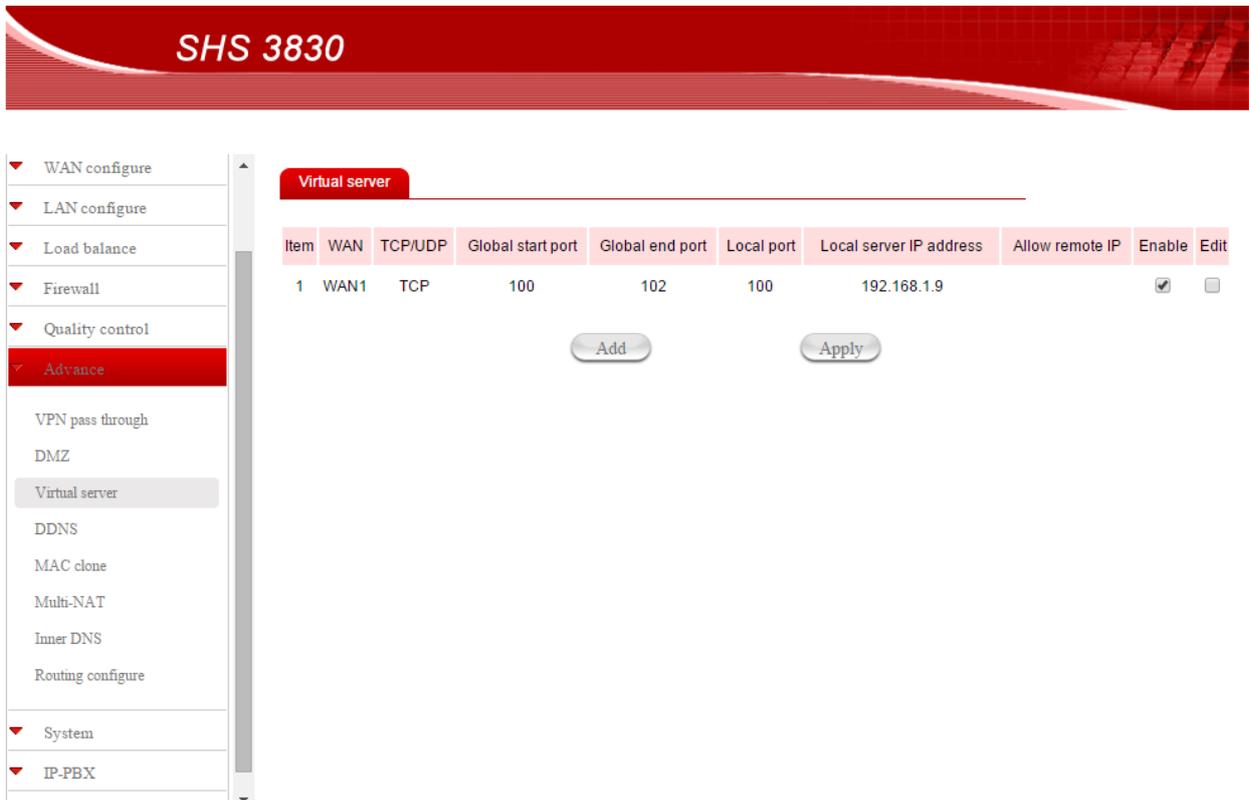
Advance – Virtual server

The screenshot shows the SHS 3830 web interface. The left sidebar has a menu with 'Advance' selected, and 'Virtual server' is highlighted. The main content area is titled 'Virtual server' and contains a table with the following columns: Item, WAN, TCP/UDP, Global start port, Global end port, Local port, Local server IP address, Allow remote IP, Enable, and Edit. Below the table are two buttons: 'Add' and 'Apply'.

Step 2: Fill data to WAN, TCP/UDP, Global port, local port and local server address IP. Then Click “Add” then router goes back to **Virtual server** list table.

The screenshot shows the SHS 3830 web interface. The left sidebar has a menu with 'Advance' selected, and 'Virtual server' is highlighted. The main content area is titled 'Virtual server' and contains a form for editing a virtual server. The form has the following fields: WAN (dropdown menu with 'WAN1' selected), TCP/UDP (dropdown menu with 'TCP' selected), Global start port (text input with '100'), Global end port (text input with '102'), Local port (text input with '100'), Local server IP address (text input with '192.168.1.9'), and Allow remote IP address (text input). Below the form are two buttons: 'Delete' and 'Add'.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Example: Edit or Delete

Step 1: Enter **Virtual server** web page. Then click “Edit” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Virtual server** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Virtual server** list

table.

SHS 3830

Virtual server

Edit virtual server Item 2

WAN: WAN2

TCP/UDP: ALL

Global start port: 1200

Global end port: 1202

Local port: 1200

Local server IP address: 192.168.1.10

Allow remote IP address:

Delete Add

Step 3: Router go back to **Virtual server** list table.

SHS 3830

Virtual server

Item	WAN	TCP/UDP	Global start port	Global end port	Local port	Local server IP address	Allow remote IP	Enable	Edit
1	WAN1	TCP	100	102	100	192.168.1.9		<input type="checkbox"/>	<input type="checkbox"/>
2	WAN2	ALL	1200	1202	1200	192.168.1.10		<input type="checkbox"/>	<input type="checkbox"/>
3	USB3G	TCP	3000	3005	3010	192.168.1.111		<input type="checkbox"/>	<input type="checkbox"/>

Add Apply

3.5.4 DDNS

You need to apply for a free DNS domain name from DNS provider.

Example: dyndns.org. The SHS 3830 will update the WAN IP address to DDNS's

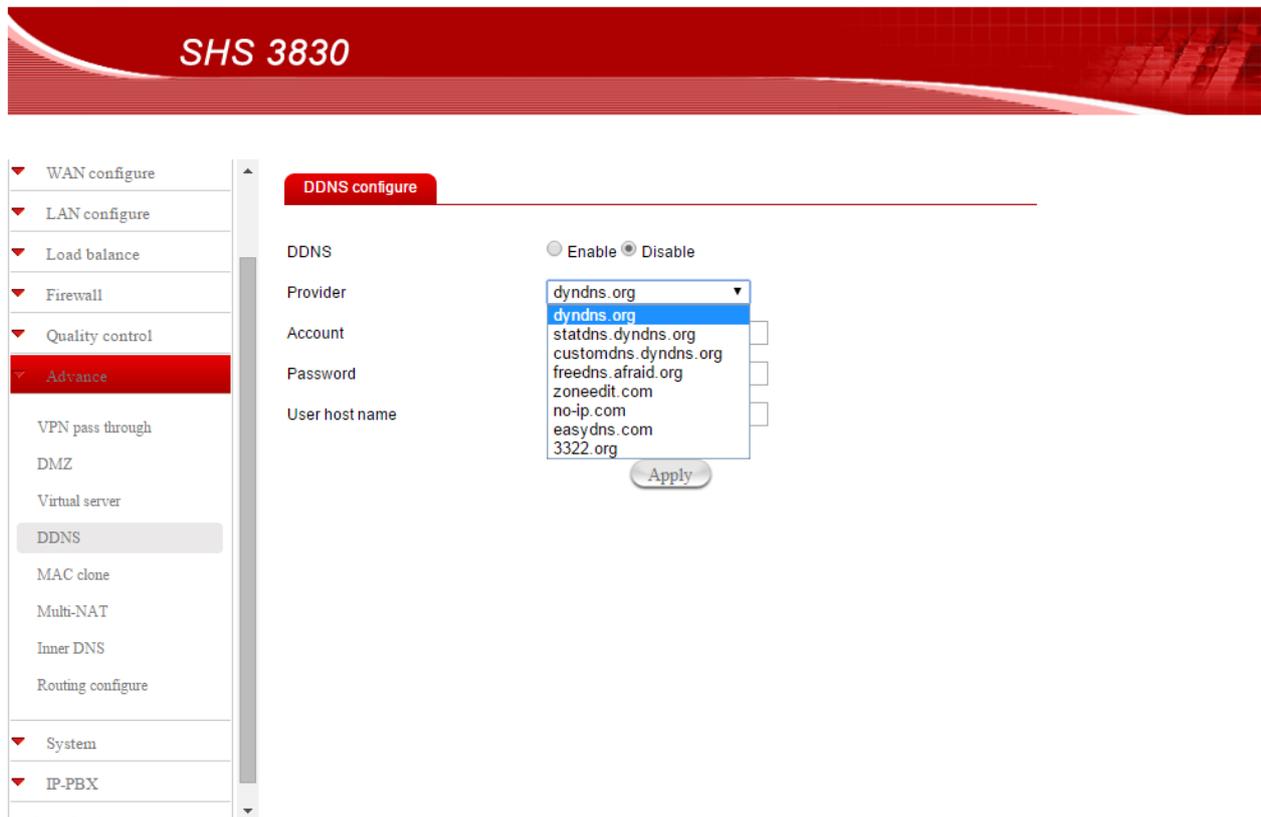
database once a WAN port was connected to Internet if DDNS function is enabled. And the users in Internet can find out the SHS 3830 via this domain name.

User Name: please apply from DNS provider.

Password: please apply from DNS provider.

User Hostname: please apply from DNS provider.

Advance – DDNS Configure



3.5.5 MAC clone

If your ISP blocked the MAC address of WAN port in router, you may use MAC Address Clone to duplicate the MAC address of PC in LAN to replace the Mac address in each WAN port.

Remove all Ethernet cable on Load Balance Router LAN port except for the PC you want to clone. Then press **Ok** when you ready.

Example: Select LAN or WAN1 or WAN2. Then fill a new MAC to MAC address

Advance – MAC Clone

The screenshot displays the SHS 3830 web interface. The top header is red with the text 'SHS 3830'. On the left, a sidebar menu is visible with the following items: WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance (highlighted), VPN pass through, DMZ, Virtual server, DDNS, MAC clone (highlighted), Multi-NAT, Inner DNS, Routing configure, System, and IP-PBX. The main content area is titled 'MAC Clone' and contains the following configuration fields:

- Select port: LAN1 (dropdown menu)
- MAC address default value: 00:09:2C:10:1B:6D
- MAC address: 00:09:2C:10:1B:6D
- Apply (button)

3.5.6 Multi-NAT

Multi-NAT function allow you to configure multiple LAN IP Domain to each WAN port, after configure multiple NAT function It will act like have virtual router connect to SHS 3830 LAN port, all traffic between each LAN IP domain , will send and receive through SHS 3830. SHS 3830 provides following benefit.

Example: Add a new item.

Step 1: Enter **Multi-NAT** web page. Then click “Add” to enter the added page.

Advance – Multi-NAT

The screenshot shows the SHS 3830 Multi-NAT configuration page. On the left is a navigation menu with categories: WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance (selected), VPN pass through, DMZ, Virtual server, DDNS, MAC clone, Multi-NAT (highlighted), Inner DNS, Routing configure, System, and IP-PBX. The main content area is titled "Multi-NAT" and contains a table with the following columns: Item, LAN IP address, Subnet mask, WAN IP, Select WAN, Enable, and Edit. Below the table are two buttons: "Add" and "Apply".

Step 2: Fill data to LAN IP address, Subnet mask, WAN IP and Select WAN. Then Click “Add” then router goes back to **Multi-NAT** list table.

The screenshot shows the SHS 3830 Multi-NAT configuration page in edit mode. The navigation menu is the same as in the previous screenshot. The main content area is titled "Multi-NAT" and shows "Edit Multi-NAT Item 1". The form contains the following fields: LAN IP address (192.168.1.2), Subnet mask (255.255.255.248), WAN IP (172.16.1.10), and Select WAN (AUTO). Below the form are two buttons: "Delete" and "Add".

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

SHS 3830

Multi-NAT

Item	LAN IP address	Subnet mask	WAN IP	Select WAN	Enable	Edit
1	192.168.1.2	255.255.255.248	172.16.1.10	AUTO	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add Apply

Left sidebar menu: WAN configure, LAN configure, Load balance, Firewall, Quality control, **Advance**, VPN pass through, DMZ, Virtual server, DDNS, MAC clone, Multi-NAT, Inner DNS, Routing configure, System, IP-PBX.

Example: Edit or Delete

Step 1: Enter **Multi-NAT** web page. Then click “Edit” check square of item 2 to enter the edited page.

SHS 3830

Multi-NAT

Item	LAN IP address	Subnet mask	WAN IP	Select WAN	Enable	Edit
1	192.168.1.2	255.255.255.248	172.16.1.10	AUTO	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.5	255.255.255.248	172.16.1.11	WAN1	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.7	255.255.255.248	172.16.1.12	WAN2	<input type="checkbox"/>	<input type="checkbox"/>

Add Apply

Left sidebar menu: WAN configure, LAN configure, Load balance, Firewall, Quality control, **Advance**, VPN pass through, DMZ, Virtual server, DDNS, MAC clone, Multi-NAT, Inner DNS, Routing configure, System.

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Multi-NAT** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Multi-NAT** list table.

- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- ▼ Advance
- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure
- ▼ System

Multi-NAT

Edit Multi-NAT Item 2

LAN IP address

Subnet mask

WAN IP

Select WAN

Step 3: Router go back to **Multi-NAT** list table.

- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- ▼ Advance
- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure
- ▼ System

Multi-NAT

Item	LAN IP address	Subnet mask	WAN IP	Select WAN	Enable	Edit
1	192.168.1.2	255.255.255.248	172.16.1.10	AUTO	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.1.7	255.255.255.248	172.16.1.11	WAN1	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.1.7	255.255.255.248	172.16.1.12	WAN2	<input type="checkbox"/>	<input type="checkbox"/>

3.5.7 Inner DNS

In order to speed out DNS request process for quick surfing internet, Inner DNS works as a cache to retain DNS information for hosts DNS lookup.

Example: Add a new item.

Step 1: Enter **Inner DNS** web page. Then click “Add” to enter the added page.

Advance – Inner DNS

SHS 3830

Inner DNS

Item	Domain name	IP address	Enable	Edit
------	-------------	------------	--------	------

Add Apply

Step 2: Fill data to Domain Name and its IP. Then Click “Add” then router goes back to **Inner DNS** list table.

SHS 3830

Inner DNS

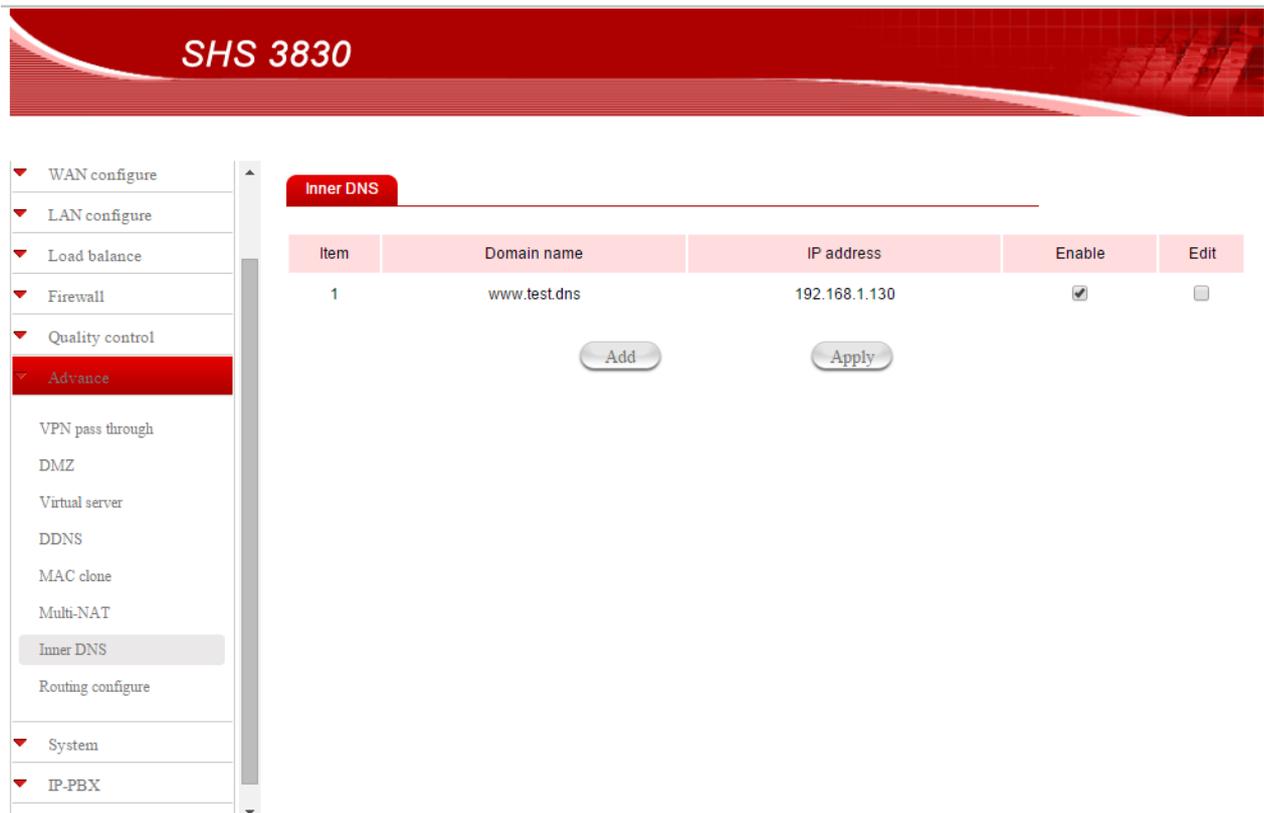
Edit Inner DNS Item 1

Domain name

IP address

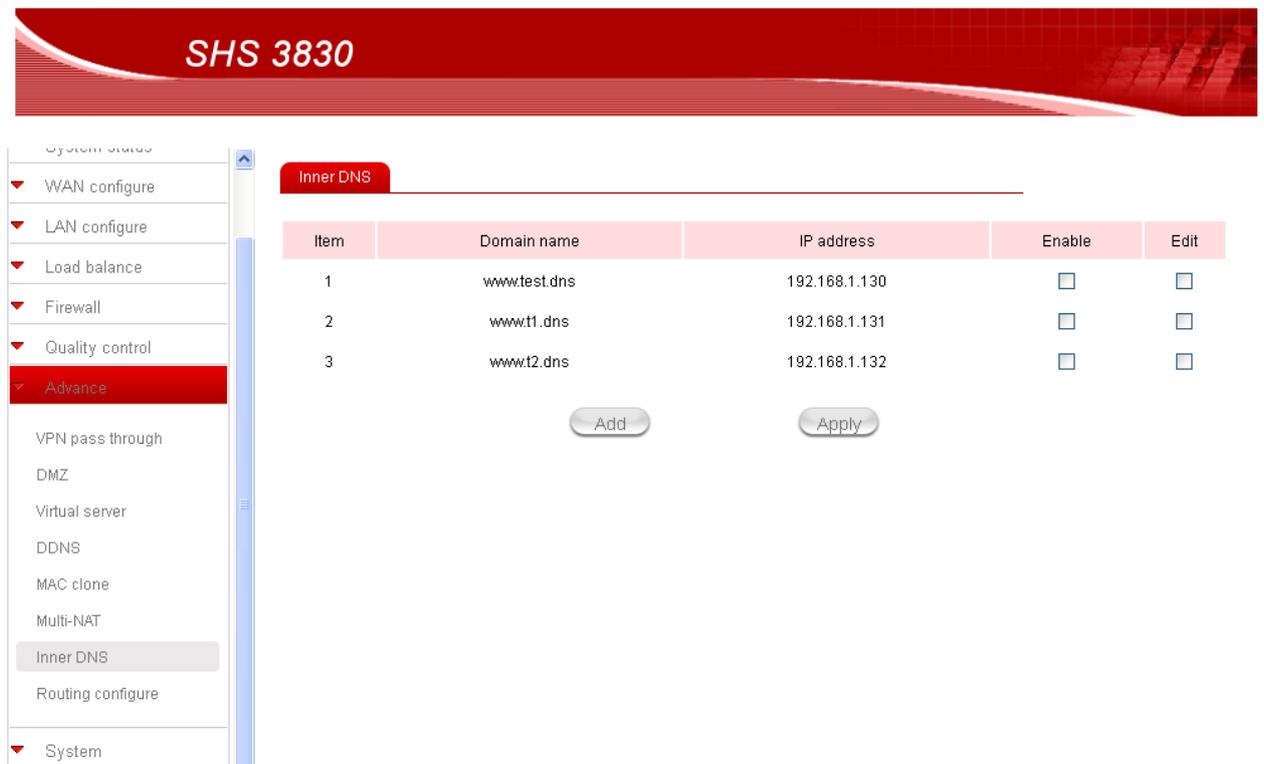
Delete Apply

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Example: Edit or Delete

Step 1: Enter **Inner DNS** web page. Then click “Edit” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Inner DNS** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Inner DNS** list table.



System status

- WLAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance**
- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure
- System

Inner DNS

Edit Inner DNS Item 2

Domain name:

IP address:

Step 3: Router go back to **Inner DNS** list table.



System status

- WLAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance**
- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure
- System

Inner DNS

Item	Domain name	IP address	Enable	Edit
1	www.test.dns	192.168.1.130	<input type="checkbox"/>	<input type="checkbox"/>
2	www.t1.dns	192.168.1.141	<input type="checkbox"/>	<input type="checkbox"/>
3	www.t2.dns	192.168.1.132	<input type="checkbox"/>	<input type="checkbox"/>

3.5.8 Routing configure

There are two routing methods can be applied in various network environments, so choose one of them (**Static routing/Dynamic routing**) for need.

Static routing

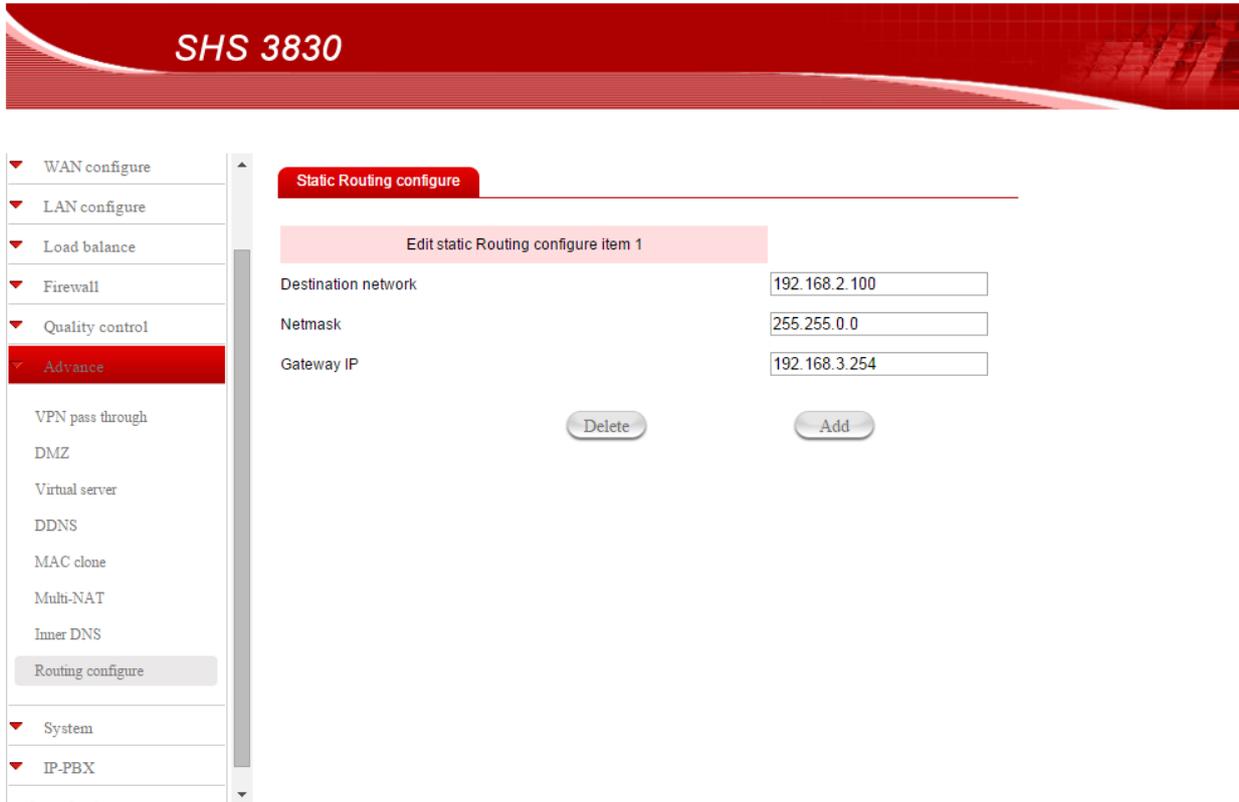
This function allows manually defined by users as the only path to the

destination. Users can configure the static routing path to Load Balance Router.

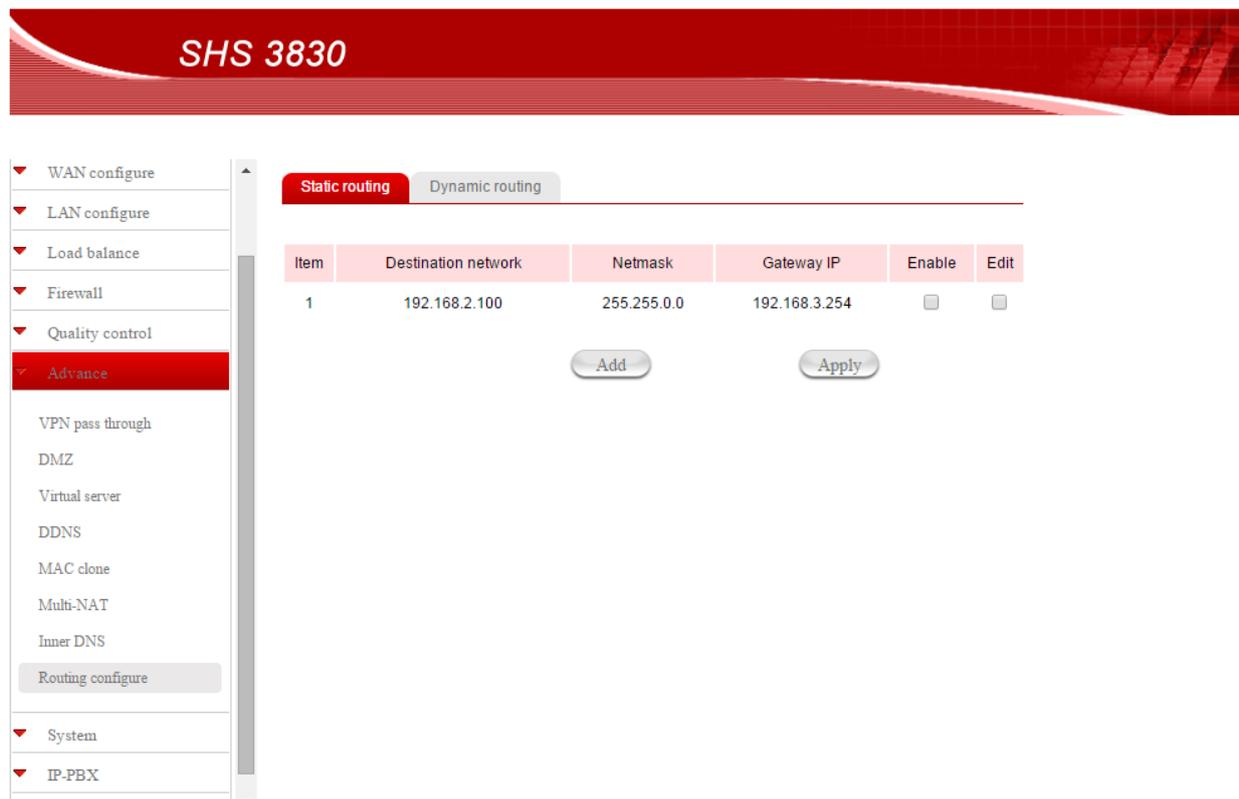
Example: Add a new item.

Step 1: Enter **Static routing** web page. Then click “Add” to enter the added page.

Advance – Static routing



Step 2: Fill data to Destination network, Netmask and Gateway IP. Then Click “Add” then router goes back to **Static routing** list table.



Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and

enable.

Example: Edit or Delete

Step 1: Enter **Static routing** web page. Then click “Edit” check square of item 2 to enter the edited page.

The screenshot displays the SHS 3830 router's configuration interface. The main content area is titled "Static routing" and contains a table with the following data:

Item	Destination network	Netmask	Gateway IP	Enable	Edit
1	192.168.2.100	255.255.0.0	192.168.3.254	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.2.102	255.255.0.0	192.168.4.254	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.2.104	255.255.0.0	192.168.5.254	<input type="checkbox"/>	<input type="checkbox"/>

Below the table are two buttons: "Add" and "Apply". The left sidebar shows a navigation menu with "Advance" selected, and "Routing configure" highlighted at the bottom.

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Static routing** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Static routing** list table.

Dynamic routing

Dynamic routing allows router learns of path to destination by receiving periodic updates from others. The protocol used in communication between routers is RIP 1/2 (Routing Information Protocol). RIP1 supports only broadcast mode while RIP2 supports broadcast and multicast mode.

Advance – Dynamic routing

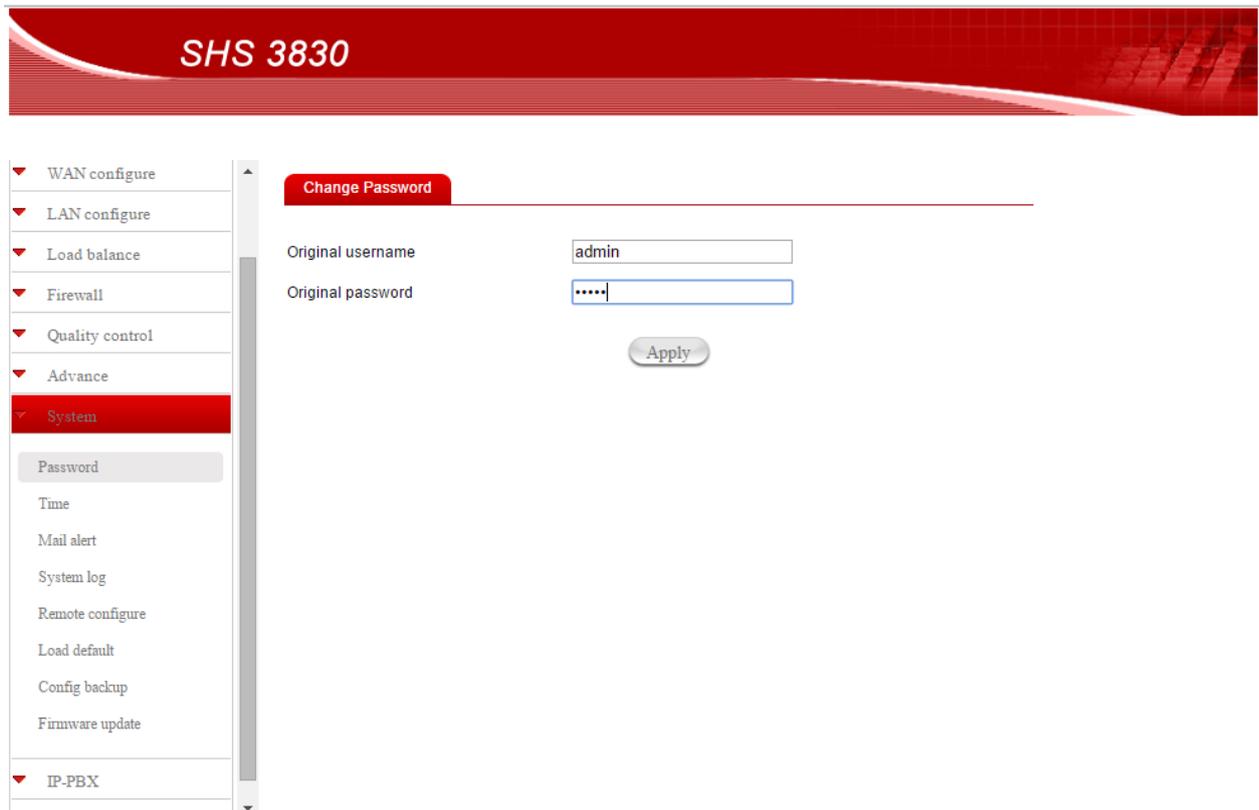
3.6 System

3.6.1 Password

Use this function to change the **Password** that is used for access the web configuration.

Step 1: Type in the **Original username** and **Original Password** then click “Apply” button. Router will display a change password web page.

System – password (1)



The screenshot shows the web configuration interface for the SHS 3830 router. The top banner is red with the text "SHS 3830". On the left, there is a navigation menu with the following items: WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System (highlighted in red), Password, Time, Mail alert, System log, Remote configure, Load default, Config backup, Firmware update, and IP-PBX. The main content area is titled "Change Password" and contains two input fields: "Original username" with the value "admin" and "Original password" with masked characters ".....". Below the fields is an "Apply" button.

Step 2: Type in the “**Input new username**”, “**Input new Password**” and **Re-input new Password** in their respective fields and then click **Apply**, the password will be changed to new one after re-boot.

System – password (2)

SHS 3830

Change Password

Change system username & password

Input new username: admin

Input new password:

Reinput new password:

Apply

System menu items: Password, Time, Mail alert, System log, Remote configure, Load default, Config backup, Firmware update, IP-PBX

“Password length can up to 30 alphanumeric characters with case sensitive”

WE SUGGESTED YOU TO CHANGE SHS 3830 PASSWORD AND KEEP IT IN SAFETY PLACE AFTER YOU RECEIVED SHS 3830 AND FINISH ALL ROUTER PARAMETER SETTING.

3.6.2 Time

The SHS 3830 will obtain the GMT (Greenwich Mean Time) after connected to Internet. You need to indicate the local time so that the system could show the correct time. For example, Taiwan’s local time is GMT + 8 hours.

Select “Automatic adjust clock for daylight saving changes” will display the time one hour earlier than local time.

System – System time

Welcome

- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System**
- Password
- Time
- Mail alert
- System log
- Remote configure
- Load default
- Config backup

System time

Time zone: GM+0:00

Update mode: NTP PC

Interval: 1440 Minutes (Range : 30 - 1440)

Select NTP server

User define NTP server:

Primary server: time.nist.gov

Second server: stdtime.gov.hk

Current time: Sun Jan 4 1970, 01:54:56

3.6.3 Mail alert

Enter the **Receiver/ Sender** e-mail Address in the fields and check the items you want. System will send e-mails to **Receiver** address once the conditions meet the setting.

Receiver mail address: The mail address that will receive alert mail

Sender mail address: The mail address that send out alert mail, you should fill in a legal format address (ex. router@yahoo.com)

The SHS 3830 provides four condition selections:

WAN Up	System will send the mail, once WAN port(s) is connected to Internet.
WAN Down	System will send the mail, once WAN port(s) is disconnected from Internet.
Router Reboot	System will send the mail, once the router reboot.
CONFIG save	System will send the mail of log information, once the system configuration is saved.
DHCP Fail	System will send the mail of log information, once the WAN Port status is DCHP and it can't get an IP from DHCP server.
PPPoE Fail	System will send the mail of log information, once the WAN Port status is PPPoE and its connect is fail.

System – Mail alert

SHS 3830

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- ▼ Advance
- ▼ System
- Password
- Time
- Mail alert
- System log
- Remote configure
- Load default
- Config backup

Mail Alert

Enable mail alert

Sender mail address

Mail server address

Authentication

 Account

 Password

Receiver mail address

Enable	Alert condition
<input checked="" type="checkbox"/>	WAN up
<input checked="" type="checkbox"/>	WAN down
<input checked="" type="checkbox"/>	Router reboot
<input checked="" type="checkbox"/>	CONFIG save
<input checked="" type="checkbox"/>	DHCP fail
<input checked="" type="checkbox"/>	PPPOE fail

3.6.4 System log

Show all the records after SHS 3830 Power on, such as WAN port up/down, WAN IP address, the obtained time, DDNS current corresponding WAN IP address and so forth. You can also save these data to files.

System – System log configure

SHS 3830

- Welcome
- ▼ System status
- ▼ WAN configure
- ▼ LAN configure
- ▼ Load balance
- ▼ Firewall
- ▼ Quality control
- ▼ Advance
- ▼ System
- Password
- Time
- Mail alert
- System log
- Remote configure
- Load default
- Config backup

System Log configure

Log content

Send log to specify PC Enable Disable

PC IP address:

Remote port

Interval(seconds)

System – Log content

The screenshot displays the SHS 3830 web interface. The left sidebar contains a navigation menu with the following items: Welcome, System status, WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System (highlighted), Password, Time, Mail alert, System log, Remote configure, Load default, and Config backup. The main content area is titled 'System Log configure' and 'Log content'. It features a table with the following data:

Item	Time	Event
1	Jan-1-00:00:15	LAN interface bootup, IF=eth0.40 , IP=192.168.1.253
2	Jan-1-00:00:15	WAN interface bootup, IF=eth0.1 , IP=192.168.11.100
3	Jan-1-00:00:15	WAN interface bootup, IF=eth0.2 , IP=192.168.12.100
4	Jan-1-00:00:38	LAN port start up

3.6.5 Remote Configure

The SHS 3830 can be managed from any PC from INTERNET. If enable **Remote configure** function in this display, access to the Web-based interface is available via the INTERNET, If not enabled, access is only available to PCs from LAN.

Access from LAN specific 192.168.1.254 in the URL field

Access from INTERNET ...specific WAN port IP address in the URL field

ROUTER provide easy method to access from INTERNET via “Dynamic IP” & “Dynamic port”

Remote IP: specific dedicated PC can be remote access ROUTER

- Leaving these fields blank will allow access by all PCs.
- if enter specific IP address, only this address PC can access from remote
- The address must be Internet IP addresses.

Remote Port: The port number used when connecting remotely.

Example: If the local user

- . Enable the **Remote configure** function
- . Remote port is **8888 (default is 8888, can be different port number)**
- . Remote IP is blank.
- . ROUTER WAN port IP is **110.111.112.1**

When the user of remote side want to access the ROUTER web configure, the remote user only need to enter ***http:// 110.111.112.1:8888***

System – Remote configure



- Welcome
- System status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System**
- Password
- Time
- Mail alert
- System log
- Remote configure
- Load default
- Config backup

Remote configure

Remote configure Enable Disable

Service port

8888

Apply

3.6.6 Load default

Use this function to reset all the settings to their factory default values or latest configuration file. Click **Apply** after selection, the ROUTER will restart automatically.

System – Load default

The screenshot displays the web interface for the SHS 3830 router. At the top, a red banner contains the text "SHS 3830". On the left side, there is a vertical navigation menu with the following items: Welcome, System status, WAN configure, LAN configure, Load balance, Firewall, Quality control, Advance, System (highlighted in red), Password, Time, Mail alert, System log, Remote configure, Load default (highlighted in grey), and Config backup. The main content area on the right is titled "Load Default" and contains the following text: "Attention: This function will load factory default value, and LAN IP will be back to 192.168.1.254". Below this text is a single "Apply" button.

3.6.7 Configure backup

Use **Configure backup** function to save all the settings parameter to PC for safety issue, in order to avoid all parameters lose when system crush or SHS 3830 is loaded the default parameters.

System – Configure backup



3.6.8 Firmware update

The SHS 3830 allows you to easily update the embedded firmware.

We will occasionally provide new firmware on the web site to help you updating the firmware of your SHS 3830.

Follow the procedure to update your firmware after downloaded the new code.

System – Firmware update



You will see the updating processing. After finishing update procedure, you must **reboot** SHS 3830 to run new code.

3.7 Save & Reboot

In order to save the configuration changes that have been made to the SHS 3830 you must save them to the SHS 3830's Flash memory. If you do not save the changes, the configuration settings will be lost in the event of a power loss or system reboot to the SHS 3830.

Save and reboot



Welcome
▼ System status
▼ WAN configure
▼ LAN configure
▼ Load balance
▼ Firewall
▼ Quality control
▼ Advance
▼ System
▼ IP-PBX

Save and reboot

Save and reboot Save new parameters and reboot router

Save new parameters Save new parameters without reboot router

Chapter 4 In-bound function

Authorities DNS is just a fancy term for the official IP address keeper/provider of particular Domain (or Internet) name, such as www.example.com is analogous to a telephone book where a person's name is associated with his telephone number. Wikipedia, the free encyclopedia has a good general discussion of DNS: http://en.wikipedia.org/wiki/Domain_Name_System

This IN-BOUND ROUTER DNS server contains the names and Internet addresses of servers that you wish to host. In order for all DNS requests for your domain names to be ultimately routed to your IN-BOUND ROUTER, it has to be setup at the registrar of your Internet name. In general, logon to your registrar site, and manage your domain name. For example, www.example.com Current is located at a WEBhosting company:

Domain servers in listed order: NS0.DNSMADEEASY.COM
NS1.DNSMADEEASY.COM NS2.DNSMADEEASY.COM
NS3.DNSMADEEASY.COM NS4.DNSMADEEASY.COM We need to change
www.example .com to be hosted by IN-BOUND ROUTER; so we follow the registrar's
instructions and delete: NS2, NS3, and NS4, and assign:

Domain servers as below

Name	IP address
NS0.EXAMPLE.COM	WAN1
NS1.EXAMPLE.COM	WAN2

The name is arbitrary; what are important are the IP addresses. It is absolutely necessary for WAN1 to be a static address, and for redundant, fault-tolerant accesses, WAN2 should also be a static address. It would take approximately 24 – 48 hours for this change to take effect throughout the Internet.

Chapter 5 Hardware load default

If you need to reset the settings of the SHS 3830 to factory default values or back to latest configuration file, please follow the description step by step to load the factory default settings or back to latest configuration file for the device. Please be careful. Do not press the **Factory Reset** button unless you want to clear the current data.

1. Plug in the power code and then press on the **Factory Reset** button **3 seconds**
2. Release the **Factory Reset** button.
3. The SHS 3830 will load the default settings or back to latest configuration file and do self-test
4. Complete the reset procedure.

Chapter 6 Appendix

6.1 TCP/IP Protocol Port Number List

Protocol Port No. List

Protocol	Service	Port no.	Protocol	Service	Port no.
TCP	FTP	21	TCP	LADP	389
TCP	SSH	22	TCP	HTTPS	443
TCP	TELNET	23	UDP	IKE	500
TCP	SMTP	25	TCP	RLOGIN	513
UDP	DNS	53	UDP	SYSLOG	514
UDP	TFTP	69	UDP	TALK	517,518
TCP	GOTHER	70	UDP	RIP	520
TCP	FINGER	79	TCP	AFPOWERTCP	548
TCP	HTTP	80	TCP	Net-Meeting	1503,1702
TCP	POP3	110	TCP	L2TP	1701
UDP	NFS	111	TCP	PPTP	1723
TCP	NNTP	119	TCP	AOL	5190~5194
UDP	NTP	123	UDP	PC Anywhere	5631~5632
TCP	IMAP	143	TCP	XWINDOW	6000-6063
UDP	SNMP	161	TCP	IRC	6660~6669
TCP	BGP	179	TCP	Real-Media	7070
TCP	WAIS	210	TCP		6000-6063