

Uniway2000 Uniway2100

User Manual

Version 1.8.0

Synway Information Engineering Co., Ltd www.synway.net



Content

Content		i
Copyright I	Declaration	iii
Revision H	istory	iv
Chapter 1	Product Introduction	1
1.1 Typica 1.2 Featu 1.3 Hardw <i>1.3.1 Ap</i> <i>1.3.2 Ha</i> 1.4 Alarm	al Application Ire List ware Description ppearance & Interface Description ardware Structure in Info	1 2 3 5 6
Chapter 2	Quick Guide	7
Chapter 3	WEB Configuration	9
3.1 System 3.2 Opera 3.2.1 Sy 3.2.2 Bo 3.2.3 W 3.3 Gatew 3.3.1 Bo 3.3.2 Bo	m Login ation Info ystem Info oard State /arning Info way Setting oard Setting	9 10 11 12 12 12 12 12 13
3.4 Board 3.5 Route 3.5.1 IP 3.6 Syster 3.6.1 Ne 3.6.2 Ma	d Group e Settings <i>to TEL/PSTN</i> m Tools <i>etwork</i> lanagement	13 14 14 16 18 19
3.6.3 IP 3.6.4 Ac 3.6.5 Ce 3.6.6 Cc 3.6.7 Si 3.6.8 Pi	P Routing Table ccess Control entralized Manage onfiguration File ignaling Capture	21 22 24 27 28 28
3.6.9 FF 3.6.10 M 3.6.11 Ba 3.6.12 Fa 3.6.13 Up 3.6.14 Ar	RACERT Test Iodification Record ackup & Upload actory Reset	30 31 32 32 32 32 32 32 32
3.6.15 Cl 3.6.16 Re	hange Password estart	34 35



Appendix A Technical Specifications	36
Appendix B Troubleshooting	37
Appendix C Technical/sales Support	38



Copyright Declaration

All rights reserved; no part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without prior written permission from Synway Information Engineering Co., Ltd (hereinafter referred to as 'Synway').

Synway reserves all rights to modify this document without prior notice. Please contact Synway for the latest version of this document before placing an order.

Synway has made every effort to ensure the accuracy of this document but does not guarantee the absence of errors. Moreover, Synway assumes no responsibility in obtaining permission and authorization of any third party patent, copyright or product involved in relation to the use of this document.



Revision History

Version	Date	Comments
Version 1.6.3	2017-3	Initial publication
Version 1.8.0	2019.11	New revision

Note: Please visit our website http://www.synway.net to obtain the latest version of this document.



Chapter 1 Product Introduction

Thank you for choosing Synway UMG Series Gateway!

The Synway UMG series gateway products (hereinafter referred to as 'UMG gateway') integrate the analog, digital and wireless subboards. It can connect the traditional phone sets, the fax machines, the PSTN and the enterprise PBX as well as the wireless network to implement multiple features of analog, digital and wireless gateways, providing a powerful, reliable and cost-effective VoIP solution for such occasions as IP call centers and multi-branch agencies.

1.1 Typical Application



Figure 1-1 Typical Application



1.2 Feature List

Basic Features	Description		
IP Call	Call initiated from IP to a designated SIP trunk for voice communication, via routing and number manipulation.		
Number Manipulation	Peels off some dig phone number.	its of a phone number from left/right, or adds a prefix/suffix to a	
VoIP Routing	Routing path: from	IP to PSTN or from PSTN to IP.	
Fax	Multiple fax parame correction mode, e	eters: fax mode, maximum fax rate, fax train mode, error tc.	
Echo Cancellation	Provides the echo	cancellation feature for a call conversation.	
IMS Network	Registers the gate	way to a server under IMS network.	
Simultaneous Register to Multiple Servers	Registers the gateway to a master registrar server and a spare registrar server simultaneously.		
Signaling & Protocol	Description		
SIP Signaling	Supported protocol	I: SIP V1.0/2.0, RFC3261	
Voice	CODEC G.711A, G.711U, G.729, G723, G722, AMR, iLBC DTMF Mode RFC2833, SIP INFO, INBAND, RFC2833+Signaling, In-band+Signaling		
Network	Description		
Network Protocol	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN		
Static IP	IP address modification	ation support	
DNS	Domain Name Service support		
Security	Description		
Admin Authentication	Support admin authentication to guarantee the resource and data security		
Maintain & Upgrade	Description		
WEB Configuration	Support of configurations through the WEB user interface		
Language	Chinese, English		
Software Upgrade	Support of user interface, gateway service, kernel and firmware upgrades based on WEB		
Tracking Test	Support of Ping and Tracert tests based on WEB		
SysLog Type	Three options available: ERROR, WARNING, INFO		

1.3 Hardware Description

The UMG gateway features 2U rackmount design and integrates embedded LINUX system within



the POWERPC+DSP hardware architecture. It has 2 Megabit Ethernet ports (LAN1 and LAN2) on the chassis, two fan boxes with removable fans and independent air passages respectively on the front and back panels.

1.3.1 Appearance & Interface Description











Figure 1-6 Rear View for Uniway2100



Screw Holes for Foot Bracket

Figure 1-7 Left View for Uniway2100

The table below gives a detailed introduction to the interfaces, buttons and LEDs illustrated above:

Interface	Description		
	Amount: 2		
	Type: RJ-45		
LAN	Bandwidth: 10/100Mbps		
	Self-Adaptive Bandwidth Supported		
	Auto MDI/MDIX Supported		
	Amount: 1		
	Type: RS-232		
	Baud Rate: 115200 bps		
	Connector: Mini-USB connecting line		
Console Port	Data Bits: 8 bits		
	Stop Bit: 1 bit		
	Parity Unsupported		
	Flow Control Unsupported		
Button	Description		
Power Key	The power key for the board power supply		
Reset Button	Restore the gateway to factory settings.		
LED	Description		
Davison la alla a fa a	Indicates the power state. It lights up when the gateway starts up with the power		
Power Indicator	cord well connected.		
Run Indicator	Indicates the running status. For more details, refer to Alarm Info.		
Alarm Indicator	Alarms the device malfunction. For more details, refer to Alarm Info.		
Link Indicator	The green LED on the left of LAN, indicating the network connection status.		



ACT Indicator	The orange LED on the right of LAN, whose flashing tells data are being
Actimateutor	transmitted.

1.3.2 Hardware Structure

The UMG gateway features 2U rackmount design, which can be inserted with the CPU board, the switching board, analog gateway subboards, digital gateway subboards and wireless gateway subboards. For the Uniway2000 gateway, it designs 6 service board slots in the front, 2 service board slots together with 1 switching board slot at the back. The wider one among the 9 slots is only for the switching board, and the other 8 slots are optional; for the Uniway2100 gatewaym ut designs 6 service board slots in the front, 1 switching board slot at the back. The descriptions about the subboards are listed below:

The CPU board (Occupied a height of two service boards) based on the X86 architecture is used to run the IVR and other programs developed by customers.

The switching board (Uniway2000: UMG-X08G) based on the MCU03 processor and the 1.2G quad-core ARM processor, is used to run the front-end gateway service program. The assembled switching board of Uniway2000 has 3 independent Kilomega-Ethernet ports which can be self-adaptive the 10/100M network. It provides a high-performance, embedded CPU to manage all the devices. The switching board for Uniway2100 (UMG-X06) has 2 independent Million-Ethernet ports. The service boards interact with the exterior via the switching board.

The digital gateway subboards (UMG2120) support 1E1, 2E1s and 4E1s, with the type of UMG-2030, UMG-2060 and UMG-2120.

The analog gateway subboards (UMG1016) now support up to 16 analog channels, with the types of UMG1016-16S (16-channels FXS port), UMG1016-8S8O (8-channels FXS port and 8-channels FXO port) and UMG1016-16O (16-channels FXO port).

The wireless gateway subboards (UMG4008) now support up to 8 wireless channels, with the type of UMG-4008_8G, UMG-4008_8C, UMG-4008_8W, UMG-4008_4G, UMG-4008_4C and UMG-4008_4W.

The 8 optional slots can be inserted with any subboards according to your requirement. The ordinary settings are: 1 CPU board + 1 switching board + 6 available service boards; 2 CPU boards + 1 switching board + 4 available service boards; 1 switching board + 8 available service boards.

See the hardware architecture below:



Figure 1-8 UMG Gateway Hardware Architecture



1.4 Alarm Info

The UMG gateway is equipped with two indicators denoting the system's running status: Run Indicator (green) and Alarm Indicator (red). The table below explains the states and meanings of the two indicators.

LED	State	Description	
	Go out	System is not yet started.	
Run Indicator	Light up and flash fast	System is starting.	
	Flash slowly	System is normal.	
Go out		System is normal.	
		Upon startup: System is normal.	
Alarm Indicator	Light up	In runtime: System is abnormal.	
Flash		System is abnormal.	

Note:

- The startup process consists of two stages: System Booting and Gateway Service Startup. The system booting costs about 1 minute and once it succeeds, both the run indicator and the alarm indicator light up. Then after the gateway service is successfully started and the device begins to work normally, the run indicator flashes and the alarm indicator goes out.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Go to <u>Appendix C Technical/sales Support</u> to find the contact way.



Chapter 2 Quick Guide

This chapter is intended to help you grasp the basic operations of the UMG gateway in the shortest time.

Step 1: Confirm that your packing box contains all the following things.

- UMG Gateway *1
- Angle Bracket *2, Rubber Foot Pad *4, Screw for Angle Bracket *8
- 220V Power Cord *2
- Warranty Card *1
- Installation Manual *1

Step 2: Properly fix the UMG gateway.

If you do not need to place the gateway on the rack, simply fix the 4 rubber foot pads. Otherwise, you should first fix the 2 angle brackets onto the chassis and then place the chassis on the rack.

Step 3: Connect the power cord.

Make sure the device is well grounded before you connect the power cord. Check if the power socket has the ground wire.

Note: Each UMG gateway has two power interfaces to meet the requirement for power supply hot backup. As long as you properly connect and turn on these two power keys, either power supply can guarantee the normal operation of the gateway even if the other fails.

Step 4: Connect the network cable.

Step 5: Log in the gateway.

Enter the original IP address of the UMG gateway (Uniway2000 WAN1, Uniway2100 ETH1: 192.168.1.101 or Uniway2000 WAN2, Uniway2100 ETH2: 192.168.0.101) in the browser to go to the WEB interface. The original username and password of the gateway are both 'admin'. For detailed instructions about login, refer to <u>System Login</u>. We suggest you change the initial username and password via 'System Tools \rightarrow Change Password' on the WEB interface as soon as possible after your first login. For detailed instructions about changing the password, refer to <u>Change Password</u>. After changing the password, you are required to log in again.

Step 6: Modify IP address of the gateway.

You can modify the IP address of the gateway via 'System Tools \rightarrow Network' on the WEB interface to put it within your company's LAN. Refer to <u>Network</u> for detailed instructions about IP modification. After changing the IP address, you shall log in the gateway again using your new IP address.

Step 7: Check the connection of subboards.

After the gateway starts successfully with the subboards, you can go 'Gateway→Subboard Gateway' on the WEB interface to check if all the subboards are well connected.

Step 8: Set routing rules for calls.

Go to the route setting interface of each subboard to set the routing rules. Please refer to the user manual of each gateway for detailed information.

Special Instructions:

• The chassis of the UMG gateway must be grounded for safety reasons, according to standard industry requirements. A simple way is earthing with the third pin on the plug.



No or improper grounding may cause instability in operation as well as decrease in lightning resistance.

- As the device will gradually heat up while being used, please maintain good ventilation to prevent sudden failure, ensuring that the ventilation holes (see Figure 1-4) are never jammed.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Otherwise it may lead to a drop in performance or unexpected errors.

Chapter 3 WEB Configuration

3.1 System Login

Type the IP address into the browser and enter the login interface. See Figure 3-1.



Figure 3-1 Login Interface

The gateway only serves one user, whose original username and password are both 'admin'. You can change the username and the password via 'System Tools \rightarrow Change Password' on the WEB interface. For detailed instructions, refer to <u>Change Password</u>.

After login, you can see the main interface as below.

Operation Info	*
System Info	le l
Board State	
\&(arning Info	
•••uning into	
	~
; Gateway Set	۲
Board Group	8
Route	۲
System Tools	*

Figure 3-2 Main Interface

3.2 Operation Info

Operation Info shows the current running status of the gateway. See Figure 3-3.

Figure 3-3 Operation Info

3.2.1 System Info

	System In	fo	
1.0.5.1.4			
LAN I	00.50.40.00.05.00		
MAC Address	00:50:43:60:3F:32	000 000 000 0	470.40.00.054
IP Address	172.16.30.149	255.255.255.0	172.16.30.254
DINS Server	0.0.0.0	F	Durau 0
Receive Packets	AII:2995972	Error:U	Drop:0
Fransmit Packets	All:6698	Error:U	Drop:0
Current Speed	Receive:1.8 KB/s	Transmittu B/s	
Work Mode	100Mb/s Full Duplex		
LAN 2			
MAC Address	00:50:43:60:48:32		
IP Address	192.168.0.101	255.255.255.0	192.168.0.254
DNS Server	0.0.0.0		
Receive Packets	All:0	Error:0	Drop:0
Transmit Packets	All:0	Error:0	Drop:0
Current Speed	Receive:0 B/s	Transmit:0 B/s	
Work Mode	Disconnected		
Runtime	1d 23h 7m 32s		
Current Version			
Serial Number	22092(uniwav2100)		
WEB	1.8.0 2019103109		
Gateway	1.8.0 2019103109		
Uboot	2.1.7 201707		
Kernel	#151 SMP Wed Sep 11 16:20	3:23 CST 2019	
Firmware 0			

Figure 3-4 System Info Interface

See Figure 3-4 for the system info interface. You can click *Refresh* to obtain the latest system information, click *Version Detail* to obtain the detailed information of WEB, Gateway, Uboot and Kernel. The table below explains the items shown in Figure 3-4.

ltem	Description		
MAC Address	MAC address of LAN 1 or LAN 2.		
IP Addross	The three parameters from left to right are IP address, subnet mask and default		
IF Address	gateway of LAN 1 or LAN 2.		

DNS Server	DNS server address of LAN 1 or LAN 2.		
Receive Packets,	The amount of receive/transmit packets after the gateway's startup, including three		
Transmit Packets	categories: All, Error and Drop.		
Current Speed	The current speed of data receiving and transmitting.		
	The work mode of the network, including six options: 10 Mbps Half Duplex, 10 Mbps		
	Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 1000 Mbps Full Duplex		
Work Mode	and Disconnected.		
	Note: The mode of 1000 Mbps Full Duplex is unavailable for the Uniway2100		
	gateway.		
Devertime	Time of the gateway keeping running normally after startup. This parameter		
Runtime	updates every 2s.		
CPU Temperature	Display the real time temperature of the CPU.		
Serial Number	Unique serial number of an UMG gateway.		
WEB	Current version of the WEB interface.		
Gateway	Current version of the gateway service.		
Uboot	Current version of Uboot.		
Kernel	Current version of the system kernel on the gateway.		
Firmware	Current version of the firmware on the gateway.		

3.2.2 Board State

Board Status				
Slot No.	Туре	Status		
1		Disconnected		
2		Disconnected		
3		Disconnected		
4		Disconnected		
5		Disconnected		
6		Disconnected		

Figure 3-5 Board Status List

See Figure 3-5 for the Board Status List. It displays the online status of each board connected to the gateway, telling the board type for each slot number as well as if the board is connected or not.

3.2.3 Warning Info

Warning Log	
2019-10-09 08:40:09 Warning:Internal MCU5 maybe down,please check!	~
2019-10-15 09:20:52 eth0 is down!	
2019-10-17 08:28:45 Warning:Internal MCU0 maybe down,please check!	
2019-10-17 08:28:45 Warning:Internal MCU1 maybe down,please check!	
2019-10-17 08:28:45 Warning:Internal MCU2 maybe down,please check!	
2019-10-17 08:28:45 Warning:Internal MCU3 maybe down,please check!	
2019-10-17 08:28:45 Warning:Internal MCU5 maybe down,please check!	-
2019-10-17 08:47:57 Warning:Internal MCU0 maybe down,please check!	
2019-10-17 08:47:57 Warning:Internal MCU1 maybe down,please check!	
2019-10-17 08:47:57 Warning:Internal MCU2 maybe down,please check!	
2019-10-17 08:47:57 Warning:Internal MCU3 maybe down,please check!	
2019-10-17 08:47:57 Warning:Internal MCU5 maybe down,please check!	
2019-10-24 15:31:32 Warning:Internal MCU0 maybe down,please check!	
2019-10-24 15:31:32 Warning:Internal MCU1 maybe down,please check!	
2019-10-24 15:31:32 Warning:Internal MCU2 maybe down,please check!	
2019-10-24 15:31:32 Warning:Internal MCU3 maybe down,please check!	
2019-10-24 15:31:32 Warning:Internal MCU5 maybe down,please check!	
2019-10-28 10:18:43 Warning:Internal MCU0 maybe down,please check!	
2019-10-28 10:18:43 Warning:Internal MCU1 maybe down,please check!	
2019-10-28 10:18:43 Warning:Internal MCU2 maybe down,please check!	
2019-10-28 10:18:43 Warning:Internal MCU3 maybe down,please check!	
2019-10-28 10:18:43 Warning:Internal MCU5 maybe down,please check!	
2019-10-29 08:31:50 Warning:Internal MCU0 maybe down,please check!	
2019-10-29 08:31:50 Warning:Internal MCU1 maybe down,please check!	
2019-10-29 08:31:50 Warning:Internal MCU2 maybe down,please check!	4
2019-10-29 08:31:50 Warning:Internal MCU3 maybe down,please check!	
Download	

Note: Only the latest 100 pieces of warning information will be displayed. To check all the information, please click the Download button.

Figure 3-6 Warning Info Interface

See Figure 3-6 for the Warning Information interface. It displays all the warning information on the gateway.

3.3 Gateway Setting

SIP Settings includes *Board Setting* and *Board Information*. See Figure 3-7.

🚆 Gateway Set	۶
Board Set	
Board Info	

Figure 3-7 Gateway Settings

3.3.1 Board Setting

The Board Setting interface displays all the board types of the UMG gateway. See Figure 3-8. Click *Configuration* to go to the configuration interface of each board. You can refer to the

corresponding gateway's manual for detailed operations.

Subboard Gateway					
Slot No.	Subboard IP	Gateway Type	Configuration		
1					
2					
3					
4	169.254.1.104	UMG-2120			
5					
6	169.254.1.106	UMG-2120			

Figure 3-8 Board Setting Interface

3.3.2 Board Information

The Board Information interface displays all the route and port information. See Figure 3-9 below.

Route Info Port Info						
	IP->TEL/PSTN					
IP/SIP Trunk Group	Port Group/P0	CM Trunk Group	Subboard			
SIP Trunk Group[0]	PCM True	nk Group[0]	1UMG-2120			
TEL/PSTN->IP						
Port Group/PCM Trunk Group	Port Group/PCM Trunk Group IP/SIP Trunk Group		Subboard			
PCM Trunk Group[0]		SIP Trunk Group[0]	1UMG-2120			

Figure 3-9 Board Information Interface

3.4 Board Group

Board Group					
Check Index Boards Description			Modify		
	0	1,2,3,4,5,6	default		
Check All 🗄 Uncheck All 🗄 Inverse 🗄 Delete 🗏 Clear All					
ltems Total 20 ltems/Page 1/1 First Previous Next Last Go to Page 1 ⊻ 1 Pages Total					

Figure 3-10 Board Group Settings

See Figure 3-10 for the Board Group Setting interface. A new board group can be added by the *Add New* button on the bottom right corner of the list in the above figure. See Figure 3-11 for the Board Group Adding interface.

Board Group				
Index:	0			
Description:	default			
Board :	Check All			
B1 (Unknown)	🗹 B2(Unknown) 🗹 B3(Unknown)			
B4(Unknown)	🗹 B5(Unknown) 🗹 B6(Digit)			
Save	Close			

Figure 3-11 Add New Board Group

The table below explains the items shown in Figure 3-11.

ltem	Description			
Index	The unique index of each board group, which is mainly used in the configuration of			
Index	routing rules and number manipulation rules to correspond to board groups.			
Description	More information about each board group.			
	The boards in the board group. If the checkbox before a board is grey, it indicates			
Boards	that the board has been occupied. The ticked boards herein will be displayed in the			
	column 'Boards' in Figure 3-10.			

After configuration, click *Save* to save the settings into the gateway or click *Close* to cancel the settings.

Click *Modify* in Figure 3-10 to modify a board group. The configuration items on the board group modification interface are the same as those on the *Board Group Adding* interface.

To delete a board group, check the checkbox before the corresponding index in Figure 3-10 and click the **Delete** button. **Check All** means to select all available items on the current page; **Uncheck All** means to cancel all selections on the current page; **Inverse** means to uncheck the selected items and check the unselected. To clear all board groups at a time, click the **Clear All** button in Figure 3-10.

3.5 Route Settings

Route Settings is used to specify the routing rules for calls from IP to TEL/PSTN. See Figure 3-12.

🔁 Route	۶
IP->TEL/PSTN R	oute

Figure 3-12 Route Settings

3.5.1 IP to TEL/PSTN

By default, there is no IP→TEL/PSTN routing rule available on the gateway. Click Add New to

add some manually. See Figure 3-13 for the IP \rightarrow TEL/PSTN routing rule adding interface.

IP->PSTN Routing Rule				
Index:	254 🔹			
Source IP:	*			
CallerId Prefix:	*			
CalleeID Prefix:	*			
Call Destination:	Subboard Group[0] -			
Description:	default			
Save	Close			

Figure 3-13 Add New Routing Rule (IP→TEL/PSTN)

The table below explains the items shown in the above figure.

ltem	Description
	The unique index of each routing rule, which denotes its priority. A routing rule with
Index	a smaller index value has a higher priority. If a call matches several routing rules, it
	will be processed according to the one with the highest priority.
Source IP	The IP address where the calls come from.

	A string of numbers at the beginning of the calling/called party number.						
	can be set	can be set to a specific string or "*" which indicates any string. These two					
	configuration	items together with Call Initiator can specify the calls which apply to a					
	routing rule.						
	Rule Explana	ation:					
	Characte	r Description					
	"0"~"9"	Digits 0~9.					
		'[]' is used to define the range for a number. Values within it only					
CallerID Prefix,	"[]"	can be digits '0~9', punctuations '-' and ','. For example,					
CalleeID Prefix		[1-3,6,8] indicates any one of the numbers 1, 2, 3, 6, 8.					
		'-' is used only in '[]' between two numbers to indicates any					
		number between these two numbers.					
	""	',' is used to separate numbers or number ranges, representing					
	,	alternatives.					
	Example: Ru	le "0[0-3,7][6-9]" denotes the prefix is 006, 016, 026, 036, 007, 017,					
	027, 037, 00	3, 018, 028, 038, 009, 019, 029, 039, 076, 077, 078, 079.					
	Note: Multiple rules are supported for CallerID/CalleeID prefix. They are separated						
	by ":".						
Call Destination	Board group	to which the call will be routed.					
Description	More informa	tion about each routing rule.					

After configuration, click **Save** to save the settings into the gateway or click **Close** to cancel the settings. See Figure 3-14 for the IP→TEL/PSTN Routing Rule Configuration Interface.

Default Routing Rule: Image: Turning by Subboard Gateway: Subboard Slot No. Priority: Subboard Idle Channels Priority:							
			F	Routing Rules			
Check	Index	Call Initiator	CallerID Prefix	CalleeID Prefix	Call Destination	Description	Modify
	254	201.123.116.197	*	*	Subboard Group[6]	default	
	255	201.123.112.140	*	*	Subboard Group[1]	default	
	253	201.123.111.82	*	*	Subboard Group[1]	default	
Check All 🗮 Uncheck All 🗄 Inverse 🗮 Delete 🗮 Clear All				Add New			
3 Items Total 2	3 Items Total 20 Items/Page 1/1 First Previous Next Last Go to Page 1 ▼ 1 Pages Total						

Figure 3-14 IP→TEL/PSTN Routing Rule Configuration Interface

Click **Modify** in Figure 3-14 to modify a routing rule. The configuration items on the $IP \rightarrow TEL/PSTN$ routing rule modification interface are the same as those on the **Add New Routing Rule (IP \rightarrow TEL/PSTN)** interface. Note that the item **Index** cannot be modified.

To delete a routing rule, check the checkbox before the corresponding index in Figure 3-14 and click the **Delete** button. **Check All** means to select all available items on the current page; **Uncheck All** means to cancel all selections on the current page; **Inverse** means to uncheck the selected items and check the unselected. To clear all routing rules at a time, click the **Clear All** button in Figure 3-14.

3.6 System Tools

System Tools is mainly for gateway maintenance. It provides such features as IP modification, time synchronization, data backup, log inquiry and connectivity check. See Figure 3-15 for details.

Figure 3-15 System Tools

3.6.1 Network

	Network Settin	gs	
	SIP IP Address	LAN 1:172.16.30.149	~
	SIP Port	5060	
LAN 1	IP Address (I):	172.16.30.149	
	Subnet Mask (U):	255.255.255.0	
	Default Gateway (D):	172.16.30.254	
LAN 2	IP Address (I):	192.168.0.101	
	Subnet Mask (U):	255.255.255.0	
	Default Gateway (D):	192.168.0.254	
DNS Server S	Get		
	Preferred DNS Server (P)	0.0.0.0	
	Standby DNS Server (P)	0.0.0.0	
Note1: After IP	Save Save Save Save Save Save Save Save	Reset g your new IP address.	
Note2: If you fa log on to it aga	ail to log on to the web after changing the networ ain.	k type to PPPoP, please modify the web port an	id

Figure 3-16 Network Settings Interface

See Figure 3-16 for the network settings interface. A gateway has two LANs, each of which can be configured with independent IP address, subnet mask, default gateway and DNS server. On this interface, SIP Address is used to select the IP address for SIP signaling, using LAN 1 by default; SIP Signaling Port is used to set the monitoring port for SIP signaling, with the value range of 5001~65535 and the default value of 5060.

Note: 1. The two configuration items IP Address and Default Gateway cannot be the same for NET 1 and NET 2.

2. By default, *Speed and Duplex Mode* is hidden, set to Automatic Detection, and you can click 'F' to let it display. We suggest you do not modify it because the non-automatic detection may cause abnormity in network interface.

After configuration, click **Save** to save the above settings into the gateway or click **Reset** to restore the configurations. After changing the IP address, you shall log in the gateway again using your new IP address.

3.6.2 Management

	Managemen	t Parameters
NEB Mana	gement	
	WEB Port	80
	Access Setting	Allow All IPs
	Time to Log out	1800 s
SSH Manag	ement Config	
	SSH	OYes ONo
	SSH Port	22
Remote Dat	a Canture Config	
	Remote Data Capture	⊙Yes ONo
	Capture RTP	LAN 1(172.16.30.149)
FTP Config		
	FTP	●Yes ONo
SYSLOG P	arameters	
	SYSLOG	⊙Yes ONo
	Server Address	127.0.0.1
	SYSLOG Level	ERROR
CDR Param	eters	
	Convex Address	160.054.1.100
	Server Address	169.254.1.100
	Server Port	3
Parameter (Config	
	NAT Traversal	🗹 Enable
	Traversal Type	Port Mapping
	LAN2 Mapping Address	
	LAN2 Mapping Address	
	RTP Self-adaption	Enable
	Auto Reply of Source Address	
	Send Response By Former Via	
	RTP Port	6000,20000
Send Numb	er Classification Information	
	Send Number Classification Data	⊙Yes ONo
	Server Ip	127.0.0.1
	Server port	4
Time Demo	otoro	
nine Param	NTP	
	NTP Server Address	127.0.0.1
	Pupelyconizing Cuele	2000
	Synchronizing Cycle	Source S
	Dally Restart Restart Time	
	Restart Hille	
	System Time	V DUCTION VITTIN TO VE S STOLES A
	System Time	Modily 2019-11-2513:30:13

Figure 3-17 Management Parameters Setting Interface

See Figure 3-17 for the Management Parameters Setting interface. The table below explains the items shown in the above figure.

ltem	Description	
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.	
	Sets the IP addresses which can access the gateway via WEB. By default, all IPs	
A	are allowed. You can set an IP whitelist to allow all the IPs within it to access the	
Access Setting	gateway freely. Also you can set an IP blacklist to forbid all the IPs within it to access	
	the gateway.	
Time to Leav Out	The gateway will log out automatically if it is not operated during a time longer than	
Time to Log Out	the value of this item, calculated by s, with the default value of 1800ms.	
66H	Sets whether to enable the gateway to be accessed via SSH, with the default value	
350	of No.	
SSH Port	The port which is used to access the gateway via SSH.	
Remote Data	After this feature is enabled, you can obtain the gateway data via a remote capture	
Capture	tool. The default value is <i>No</i> .	
Conturo BTB	Sets whether to capture RTP. Once this feature is enabled, the RTP package will	
	also be captured by the selected network.	
FTP	Sets whether to enable the FTP server, with the default value of Yes.	
SVSI OC	Sets whether to enable SYSLOG. It is required to fill in SYSLOG Server Address	
373200	and SYSLOG Level in case SYSLOG is enabled. By default, SYSLOG is disabled.	
Server Address	Sets the SYSLOG server address for log reception.	
SYSLOG Level	Sets the SYSLOG level. There are three options: ERROR, WARNING and INFO.	
	Sets whether to enable the feature of sending CDR. It is required to fill in Server	
Send CDR	Address and Server Port in case Send CDR is enabled. By default, Send CDR is	
	disabled.	
Server Address	The address of the server to receive CDR.	
Server Port	The port of the server to receive CDR.	
NAT Traversal,	Sets whether to enable the NAT traversal. By default this feature is disabled. There	
Traversal	is only one traversal type: Port Mapping.	
Туре		
LAN1 Mapping	The mapping addresses of LAN1 and LAN2 in case the NAT traversal is enabled. If	
Address,	the port mapping is selected as the traversal type, you are required to set the	
LAN2 Mapping	mapping address on the router and fill in the corresponding information here as well.	
Address	By default, only the IP address need be filled in, and the port value is just the same	
	as the SIP signaling port.	
	When this feature is enabled, the RTP reception address or port carried by the	
RTP Self-adaption	signaling message from the remote end, if not consistent with the actual state, will	
	be updated to the actual RTP reception address or port. By default, this feature is	
	disabled.	
Auto Reply of	Once this feature is enabled, the gateway will reply the source address in the invite	
Source Address	message. The default value is <i>disabled</i> .	
Send Response By	To IP->PSTN calls, enabling this feature means to close the automatic modification	
Former Via	on the Via header of the response message. By default it is disabled.	

RTP Port	Supported RTP port range for the IP end to establish a call conversation. Range of value: 5000~60000, with the lower limit of 6000 and the upper limit of 20000 by default The difference between is not less than 4096		
	Sets whether to enable the NTP time synchronization feature. It is required to fill in		
NTP	NTP Server Address, Synchronizing Cycle and Time Zone in case NTP is		
	enabled. By default, NTP is disabled.		
NTP Server Address	Sets the Server address for NTP time synchronization.		
Synchronizing Cycle	Sets the cycle for NTP time synchronization.		
Daily Restart	Sets whether to restart the gateway regularly every day at the preset Restart Time .		
	By default, this feature is disabled.		
Restart Time	Sets the time to restart the gateway regularly.		
System Time	The system time. Check the checkbox before <i>Modify</i> and change the time in the edit		
	box.		
Time Zone	The time zone of the gateway.		

3.6.3 IP Routing Table

IP Routing Table is allowed to be set. The gateway will, according to the IP routing table, send the IP packages via a specified route to the destination network segment. By default, there is no routing information available on the gateway, click *Add New* to add manually. See Figure 3-18.

Rou	ting Table	
No.:	0	
Destination:		
Subnet Mask:		
Network Port:	NET 2(201.123.111.158 -	
Save	Close	

Figure 3-18 Add Routing Table Interface

The table below explains the items shown in above figures.

Item	Description
No.	The number of the routing for the LAN in routing table.
Destination	The network segment the in which the IP address is accessible for the network port.
Subnet Mask	The subnet mask of the network segment.
Network Port	The corresponding network port of the routing.

After configuration, click *Save* to save the settings into the gateway or click *Close* to cancel the settings. See Figure 3-19 for the Routing Table List.

Synway Information Engineering Co., Ltd

			IP Routing Table		
Check	No.	Destination	Subnet Mask	Network Port	Modify
	0	201.123.112.0	255.255.255.0	NET 2(201.123.111.158)	
Delete 🗮 🕻	Clear All				Add New

Figure 3-19 Routing Table List

Click *Modify* in Figure 3-19 to modify a routing. The configuration items on the routing table modification interface are the same as those on the *Add Routing Table* interface. Note that the item *No.* cannot be modified.

To delete a routing, check the checkbox before the corresponding index in Figure 3-19 and click the **Delete** button. To clear all number manipulation rules at a time, click the **Clear All** button in Figure 3-19.

3.6.4 Access Control

Access Control List						
Check	Check Index Command Modi			Modify		
	0	iptables -I INPUT -s 172.16.30.31 -p udp -j ACCEPT				
Check All 🗮 Uncl	heck All	e = Delete = ClearAll	Apply	Cancel		Add New
I Items Total 20 Items/Page 1/1 First Previous Next Last Go to Page 1 🕑 1 Pages Total						
Note: Application and cancel application buttons are for all current set rules,not direct at a certain rule.						

Figure 3-20 Access Control List Interface

On the Access Control List interface, once you add a piece of command to ACL, the network flow will be restricted, only the particular devices allowed to visit the gateway and only the data packages on the designated ports be forwarded. Click *Add New* to add a new piece of command.

	Access Control Command
Index:	1
Command:	
	Close

Input a piece of command into the Command item and click *Save* to save the settings to the gateway. Click *Close* to cancel your settings. After that, click *Apply* to make the new command

valid.

Click *Modify* to modify a command. The configuration items on the Access Control Command Modification interface are the same as those on the *Add Access Control Command* interface. Note that the item *Index* cannot be modified.

To delete an Access Control Command, check the checkbox before the corresponding index and click the **Delete** button, and then click the **Apply** button to make the deleted command invalid. **Check All** means to select all available items on the current page; **Uncheck All** means to cancel all selections on the current page; **Inverse** means to uncheck the selected items and check the unselected. To clear all access control commands at a time, click the **Clear All** button.

Note: 1. Currently, only the command iptables is supported by the gateway.

2. When you add or modify or delete commands manually, don't forget to click the *Apply* button to make your settings valid. However, when the gateway restarts or the configuration is leading-in, you need not click the *Apply* button and the commands will get valid automatically.

3.6.5 Centralized Manage

Centralized Manag	ge
Centralized Manage	Enable
Notification Setting:	🗹 Enable
Trap Server Port:	162
CPU Temperature Threshold("C):	60
CPU Usage Threshold(%):	90
Memory Usage Threshold(%):	90
High CPS Threshold(%):	90
Low Connection Rate Threshold(%):	20
Auto Change Default Gateway:	🗹 Enable
Management Platform:	DCMS
Company Name:	
Gateway Description:	
SNMP Server Address:	127.0.0.1
Community String:	public
Authorization Code :	Please input authorization code
Working Status:	Not Enabled
Save	Download MIB

Figure 3-22 Centralized Management Setting Interface

The Centralized Management Setting interface is used to configure parameters about centralized management. The gateway can register to a centralized management platform and accept the management of the platform. The table below explains the items shown in this interface.

Item	Description
Notification	If it is enabled, the gateway will send the SNMP TRAP warning information
Setting	automatically.
Trap Server Port	The server port to receive the warning information, with the default value of 162.

CPU			
Temperature	The warning on high CPU temperature.		
Threshold			
CPU Usage	The warning on high CDU utilization		
Threshold			
Memory Usage	The warping on high moment upage		
Threshold			
High CPS	The warning on high CDS		
Threshold			
Low Connection	The warping on low connection rate		
Rate Threshold			
Auto Change	Once this feature is enabled, the gateway will connect the DCMS via another network		
Default	port automatically once the connected network cable is loosen or drawn out. The		
Gateway	default value is disabled.		
Management	Colort a management platform for the activity to register		
Platform	Select a management platform for the gateway to register.		
Compony Nome	The company name used to register the gateway to DCMS, only valid when DCMS is		
Company Name	selected.		
Cotoway	The description displayed on DCMS after the gateway is registered to DCMS, giving an		
easy identification of the gateway in device grouping. This item is only va			
Description	DCMS is selected.		
Centralized			
Management Sets the centralized management protocol. It only supports SNMP currently			
Protocol			
	Sets the version of SNMP, three options available: V1, V2 and V3, with the default		
SNMP Version	value of V2.		
SNMP Server	ID address of SNMD		
Address			
Monitoring Port	Monitoring Port for SNMP on the gateway.		
Community	Community string used for information acquisition		
String			
Account	The account of SNMP, only valid when the SNMP version is set to V3.		
	The grade of SNMP, three options available: Neither authenticated nor encrypted,		
Grade	Authenticated but not encrypted and Authenticated and encrypted, with the default		
	value of Neither authenticated nor encrypted. It is only valid when the SNMP version is		
	set to V3.		
Authentication	The authentication password required to enter when the item Grade is set to		
Password	Authenticated but not encrypted or Authenticated and encrypted.		
Encryption	The encryption password required to enter when the item Grade is set to Authenticated		
Password	and encrypted.		

	The maximum length of the authorization code is 64 bits. There is no limitation on the				
	input content. When connecting to the centralized management server for the first time,				
Authorization	you can enter the connection by entering the correct authorization code. After the				
Code	connection is successful, you can always connect even if you change to the wrong				
	authorization code, but the centralized management feature with the wrong				
	authorization code cannot be turned off.				
Westing Oteran	The status of the connection between the gateway and the centralized management				
working Status	server. It is only valid when DCMS is selected.				

3.6.6 Configuration File

	SMGConfig.ini	*
Config File		
Dereion		_
		-
0000000-1.0.1 Komel/-1 inux mee9200com 2.6.24 #95 Thu Dee 6.10:12:40 CST 2012		
Remerv=Linux mpt650950m 2.6.34 #65 Thu Det 6 T0.12.49 CST 2012		
Cpluv=45021.580		
HWaddr1=00.04.9F.EF.03.02		
HWV80012=00.04.8F.EF.03.02		
[Cilent]		
Ip1=109.204.1.101		
Ipz=109.204.1.102		
FUIL2=00		
Ip3=109.204.1.103		
FURJ=80		
Ip4=109.204.1.104		
FUIL4=00		
Ip3=109.234.1.103		
In6-160 254 1 106		
Port6=80		
In7=169 254 1 107		
Port7=80		
In8=169 254 1 108		
Port8=80		
Reference in the second s		
LincalAddress=0.0.0.0		
UserName=BgtTPNLUr/23x1wC/w		
Pwd=BatTPNLUr/23x1wC/w		
[Monitor]		
LocalAddress=0.0.0.0		
LocalPort=1002		
AutoExec=1		
UpgradeExecPath=/usr/local/apache/htdocs/RecUpgrade		
IniFilePath=/mnt/flash		
(DigitsMapRulesInfo)		
DigitsMapRulesNum=2		
INetConfig1		
arpMode=1		
BondFlag=0		
lpAddr1=172.16.30.149		
subnet1=255.255.255.0		~
Gateway1=172.16.30.254		
Save		
Note: You shall restart the service or system to validate the modified configuration f	ile!	
Note2: Non-professional person do not modify the hosts file.		
Note3: In case of manual modification, avoid the appearance of duplicate confiduration	n item.	
Note4: Please set a line at the end of the file to avoid missing reading valid data from the last	line of the file!	

Figure 3-23 Configuration File Interface

See Figure 3-23 for the Configuration File interface where you can check and modify some relative configuration files, including SMGConfig.ini and ShConfig.ini. Configurations about the gateway server, such as route rules, number manipulation, number filter and so on, are included in SMGConfig.ini; Configurations about the board are included in ShConfig.ini. You can modify these configurations on the interface directly, and then click **Save** to save the above settings into the gateway or click **Reset** to restore the configurations.

3.6.7 Signaling Capture

	Data Capture				
Choose a network interface to capture Data	LAN 1(172.16.30.149)	Start			
Destination address for syslog 172.16.30.254 Stop					
Note:If capture,the function 'Remote Data Capture Config' in 'Management' would be closed.					
	Clean Data Download Log				

Figure 3-24 Signaling Capture Interface

See Figure 3-24 for the Signaling Capture interface. Data Capture is used to capture data on the network interface you choose. Click *Start* to start capturing data (1024000 packets at most) on the corresponding network interface. SIP and SysLog are supported at present. You can enter the Syslog destination address to send Syslog to wherever required. Click *Stop* to stop data capture and download the captured packets.

Click *Clean Data* to clean all the captured packages. Click *Download Log* to download such logs as core files, configuration files, error information and so on.

3.6.8 PING Test

Ping ⁻	Test
Source IP Address	LAN 1: 198.254.1.200 -
Destination Address	127.0.0.1
Ping Count (1-100)	4
Package Length (56-1024 bytes)	56
Start	End
lafa	
	h.

Figure 3-25 Ping Test Interface

See Figure 3-25 for the Ping Test interface. A Ping test can be initiated by the gateway on a designated IP address to check the connection status between them. The table below explains the configuration items shown in the above figure.

Item Description			
Source IP Address	Source IP address where the Ping test is initiated.		
Destination Address Destination IP address on which the Ping test is executed.			
Ping Count The number of times that the Ping test should be executed. Range of value:			
Package Length Length of a data package used in the Ping test. Range of value: 56~1024 t			
	The information returned during the Ping test, helping you to learn the network		
ΙΠΤΟ	connection status between the gateway and the destination address.		

After configuration, click Start to execute the Ping test; click End to terminate it immediately.

3.6.9 TRACERT Test

Tracert Tes	it
Source IP Address	LAN 1: 198.254.1.200 -
Destination Address	127.0.0.1
Maximum Jumps (1-255)	30
Start	End
Info	

Figure 3-26 Tracert Test Interface

See Figure 3-26 for the Tracert Test interface. A Tracert test can be initiated by the gateway on a designated IP address to check the routing status between them. The table below explains the configuration items shown in the above figure.

ltem	Description				
Source IP Address	Source IP address where the Tracert test is initiated.				
Destination Address	Destination IP address on which the Tracert test is executed.				
Maximum Jumps	Maximum number of jumps between the gateway and the destination address, which can be returned in the Tracert test. Range of value: 1~255.				
Info	The information returned during the Tracert test, helping you to learn the detailed information about the jumps between the gateway and the destination address.				

After configuration, click *Start* to execute the Tracert test; click *End* to terminate it immediately.

3.6.10 Modification Record

Modification Record	
2019-11-21 09:01:10 Add:Config/SMGConfig.ini6-SysInfo-Language:-1>1 from 172.16.30.70	^
2019-11-21 09:38:10 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.30.70	
2019-11-21 09:38:39 Mod:Config/SMGConfig.ini-SysInfo-Language:0>1 from 172.16.30.70	
2019-11-21 09:39:15 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_max:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup-1:-1>0 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup0:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup1:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup2:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup3:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup4:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMTRUNKS-pcmtrunk_isusedbygroup5:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_used0:-1>1 from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_portselecttype0:-1> from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_backup0:-1> from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_description0:-1>default from 172.16.30.70	
2019-11-21 09:44:51 Add:/Config/SMGConfig.ini-PCMGROUPS-pcmgroup_trunks0:-1>0,1,2,3,4,5 from 172.16.30.70	
2019-11-21 09:48:04 Mod:/Config/SMGConfig.ini-ROUTE_IP2TEL-RouteNum:-1>1 from 172.16.30.70	
2019-11-21 09:48:04 Add:/Config/SMGConfig.ini-ROUTE_IP2TEL-Route0:-1>255 * * * 0 default 0 from 172.16.30.70	
2019-11-21 10:09:56 Mod:Config/SMGConfig.ini-SysInfo-Language:0>1 from 172.16.30.70	
2019-11-21 10:11:08 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.30.70	
2019-11-21 10:17:21 Mod:Config/SMGConfig.ini-SysInfo-Language:0>1 from 172.16.30.70	_
2019-11-21 10:20:21 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.30.70	
2019-11-21 10:28:00 Mod:Config/SMGConfig.ini-SysInfo-Language:0>1 from 172.16.30.70	
2019-11-21 10:29:52 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.30.70	
2019-11-21 10:32:45 AllDel:/Config/SMGConfig.ini-WebUser from 172.16.30.70	
2019-11-21 10:32:45 AllDel:/Config/SMGConfig.ini4-WebUser from 172.16.30.70	
2019-11-21 10:32:45 AllDel:/Config/SMGConfig.ini6-WebUser from 172.16.30.70	
2019-11-21 12:41:54 Mod:Config/SMGConfig.ini-SysInfo-Language:0>1 from 172.16.30.70	
2019-11-22 16:10:37 Mod:/Config/SMGConfig.ini-SysInfo-Language:1>0 from 172.16.60.27	~
	лł
Check Download	
Note: Only the latest 100 pieces of modification record will be displayed.To check all the records, please click the Download button.	
Figure 3-27 Modification Record Interface	

The Modification Record interface is used to check the modification record on the web configuration. Click *Check* and the modification record will be shown on the dialog box. See Figure 3-27. Click *Download* to download the record file.

3.6.11 Backup & Upload

Data Backup				
Choose a file to backup: Configuration file Click the 'Backup' button on the right to backup the file.				
Data Upload				
To upload a file, select it and click the button 'Upload' on the right to start. Choose a file to upload: Configuration file	Upload			

Figure 3-28 Backup & Upload Interface

See Figure 3-28 for the Backup and Upload interface. To back up data to your PC, you shall first choose the file in the pull-down list and then click **Backup** to start. To upload a file to the gateway, you shall first choose the file type in the pull-down list, then select it via **Browse...**, and at last click **Upload**. The gateway will automatically apply the uploaded data to overwrite the current configurations.

3.6.12 Factory Reset

Factory Reset
Click the button 'Reset' below to restore to factory settings.
Reset

Figure 3-29 Factory Reset Interface

See Figure 3-29 for the Factory Reset interface. Click *Reset* to restore all configurations on the gateway to factory settings.

3.6.13 Upgrade

Current Version					
Serial Number	22092				
WEB	1.8.0_2019103109				
Service	1.8.0_2019103109				
Uboot	2.1.7_201707				
Kernel	#151 SMP Wed Sep 11 16:28:23 CST 2019				
Firmware	0-0				
Select an Update File Browse					
Update Reset					

Figure 3-30 Upgrade Interface

See Figure 3-30 for the upgrade interface where you can upgrade the WEB, gateway service, kernel and firmware to new versions. Select the upgrade package "*.tar.gz" via **Browse...** and click **Update** (The gateway will do MD5 verification before upgrading and will not start to upgrade until it passes the verification). Wait for a while and the gateway will finish the upgrade automatically. Note that clicking **Reset** can only delete the selected update file but not cancel the operation of **Update**.

3.6.14 Account Manage

	Empty!		
	ADD		

Figure 3-31 Account Management Interface

See Figure 3-31 for the Account Management interface. By default, there is no user information available on the gateway, click *Add* to add a piece of information.

User Information		
Index:	0	
User Name:		
Password:		
Authority:	Read 🔽	
Save	Close	

Figure 3-32 User Information Adding Interface

The table below explains the configuration items shown on the interface.

Item	Description	
	The unique index of each user information, starting from 0 and supporting up to 64	
Index	pieces of user information to add.	
User Name/Password	User name and password for WEB login. Only numbers, letters and underscores	
	are supported.	
Authority	ority Operation rights, including two options Read and Read/Write.	

After configuration, click *Save* to save the settings into the gateway or click *Close* to cancel the settings. See Figure 3-33 for the user information list.

info					
Choose	Id	User	Permission	Modify	
	0	123	Read		
Check All E Uncheck All E Inverse E Delete E Clear All Add New					
1 Items Total 20 Items/Page 1/1 First Previous Next Last Go to Page 1 💌 1 Pages Total					

Figure 3-33 User Information List

Click *Modify* in Figure 3-33 to modify a piece of user information. The configuration items on the user information modification interface are the same as those on the *User Information Adding* interface. Note that the item *Index* cannot be modified.

To delete a piece of user information, check the checkbox before the corresponding index in Figure 3-34 and click the **Delete** button. **Check All** means to select all available items on the current page; **Uncheck All** means to cancel all selections on the current page; **Inverse** means to uncheck the selected items and check the unselected. To clear all user information at a time, click the **Clear All** button.

3.6.15 Change Password

Change Password		
Current Username	admin	
Current Password	•••••	
New Username		
New Password		
Confirm New password		
Save Reset Note1: The username and the password can consist only of numbers,letters or the underline.		

Figure 3-35 Password Changing Interface

See Figure 3-35 for the Password Changing interface where you can change username and password of the gateway. Enter the current password, the new username and password, and then confirm the new password. After configuration, click **Save** to apply the new username and password or click **Reset** to restore the configurations. After changing the username and password, you are required to log in again.

3.6.16 Restart

Service Restart		
Click the button 'Restart' to restart the service.		
System Restart		
Click the button 'Restart' to restart the system.	Restart	

Figure 3-36 Service/System Restart Interface

See Figure 3-36 for the Restart interface. Click *Restart* on the service restart interface to restart the gateway service or click *Restart* on the system restart interface to restart the whole gateway system.

Appendix A Technical Specifications

Dimensions

Uniway2000: 440×88×470 mm³

Uniway2100: 440×88×372 mm³

Weight:

UMG-1016: about 0.5kg

UMG-4008: about 0.5kg

Sucker antenna (singleton): about 0.045kg

Uniway2000 (one switching board included): about 8.5kg

Uniway2100 (one IPPBX board included): about 5.4kg

Environment

Operating temperature: 0 °C---40 °C

Storage temperature: -20 $^\circ\!\!C\text{---85}\,^\circ\!\!C$

Humidity: 8%— 90% non-condensing

Storage humidity: 8%— 90% non-condensing

LAN

Amount: 2 (10/100 BASE-TX (RJ-45)) Self-adaptive bandwidth supported Auto MDI/MDIX supported

Console Port

Amount: 1 (RS-232) Baud rate: 115200bps Connector: Mini USB connecting line Data bits: 8 bits Stop bit: 1 bit Parity unsupported

Flow control unsupported

Note: Follow the above settings to configure the console port; or it may work abnormally.

Power Requirements

Input power: 100~240V AC

Maximum power consumption : ≤360W

Signaling & Protocol

SS7: TUP, ISUP

ISDN: ISDN User Side, ISDN Network Side

SS1: SS1 Signaling

SIP signaling: SIP V1.0/2.0, RFC3261

Audio Encoding & Decoding

G.711A	64 kbps
G.711U	64 kbps
G.729A/B	8 kbps
G723	5.3/6.3 kbps
G722	64 kbps
AMR	4.75/5.15/5.90/6.70/7.40/7.9 5/10.20/12.20 kbps
iLBC	13.3/15.2 kbps

Sampling Rate

8kHz

Safety

Lightning resistance: Level 4

Appendix B Troubleshooting

1. What to do if I forget the IP address of the UMG gateway?

Long press the Reset button on the gateway to restore to factory settings. Thus the IP address will be restored to its default value:

Uniway2000 WAN1: 192.168.1.101 Uniway2000 WAN2: 192.168.0.101 Uniway2100 ETH1: 192.168.1.101 Uniway2100 ETH2: 192.168.0.101

2. In what cases can I conclude that the UMG gateway is abnormal and turn to Synway's technicians for help?

a) During runtime, the run indicator does not flash or the alarm indicator lights up or flashes, and such error still exists even after you restart the device or restore it to factory settings.

Other problem such as failed registrations is probably caused by configuration errors. We suggest you refer to <u>Chapter 3 WEB Configuration</u> for further examination. If you still cannot figure out or solve your problems, please feel free to contact our technicians.

3. What to do if I cannot enter the WEB interface of the UMG gateway after login?

This problem may happen on some browsers. To settle it, follow the instructions here to configure your browser. Enter 'Tools > Internet Options >Security Tab', and add the current IP address of the gateway into 'Trusted Sites'. If you change the IP address of the gateway, add your new IP address into the above settings.

Appendix C Technical/sales Support

Thank you for choosing Synway. Please contact us should you have any inquiry regarding our products. We shall do our best to help you.

Headquarters

Synway Information Engineering Co., Ltd

http://www.synway.net/

9F, Synway D&R Center, No.3756, Nanhuan Road, Binjiang District, Hangzhou, P.R.China, 310053

Tel: +86-571-88860561

Fax: +86-571-88850923

Wechat QR Code: Scan the QR code below to add us on Wechat.

Technical Support

Tel: +86-571-88864579 Mobile: +86-18905817070 Email: techsupport@sanhuid.com Email: techsupport@synway.net MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561 Tel: +86-571-88864579 Fax: +86-571-88850923 Email: sales@synway.net