New Rock Technologies, Inc.

HX4E/MX8A Series Voice Gateway

User Manual

Website: http://www.newrocktech.com
Email: gs@newrocktech.com
Document Version: 201506

Amendent Records

Document Rev. 01 (Jun, 2015)

This manual is applicable to New Rock's HX4E/MX8A series Voice Gateway V340.

Contents

Amendent Records 2

Contents 3

Contents of Figure 5

Contents of Table 7

1 Overview 9

1.1 Product Introduction 9

1.2 Functions and Features 10

1.3 Equipment Structure 11

1.3.1 HX4E 11

1.3.2 MX8A 12

2 Parameters Setting 16

2.1 Login 16

2.1.1 Obtaining Gateway IP Address 16

2.1.2 Logging On 16

2.1.3 Gateway Administrator and Operator Rights 17

2.2 Buttons Used on Gateway Management Interface 18

2.3 Basic Configuration 18

2.3.1 Status 18

2.3.2 Network 18

2.3.3 VLAN 20

2.3.4 System 22

2.3.5 SIP 24

2.3.6 High Availability 26

2.3.7 MGCP 27

2.3.8 FoIP 29

2.4 Line 31

2.4.1 Phone Number 31

2.4.2 Subscriber Line Features 32

2.4.3 Subscriber Line Batch (Unavailable on the HX4E) 35

2.4.4 Subscriber Line Characteristics 36

2.5 Trunk 39

2.5.1 Phone Number 39

2.5.2 Trunk Features 40

2.5.3 Trunk Batch (Unavailable in the HX4E) 42

2.5.4 Trunk Characteristics 43

2.6 Routing 46

2.6.1 Digit Map 46

2.6.2 Routing Table 48

2.6.3 Examples of Routing Rules 51

2.6.4 IP Table 52
2.7 Advanced Configuration..... 53
2.7.1 System..... 53
2.7.2 Auto Provision 54
2.7.3 Management System Type..... 55
2.7.4 Security Configuration 56
2.7.5 White list for Accessing Web and Telnet 57
2.7.6 Media Stream 58
2.7.7 SIP Related Configuration 59
2.7.8 RADIUS (Unavailable on the HX4E)..... 62
2.7.9 Encryption..... 63
2.7.10 Greeting..... 65
2.7.11 Call Progress Tone Plan..... 65
2.7.12 Feature Codes..... 67
2.7.13 Clock Service..... 69
2.8 Status..... 72
2.8.1 Call Status 72
2.8.2 Call History on FXS 72
2.8.3 Call History on FXO..... 72
2.8.4 SIP Message Count..... 73
2.9 Logs..... 73
2.9.1 System Status 73
2.9.2 Call Message..... 75
2.9.3 System Startup 75
2.9.4 Manage Log..... 76
2.10 Tools..... 77
2.10.1 Change Password 77
2.10.2 Configuration Management 78
2.10.3 Upgrade..... 78
2.10.4 Restore Factory Settings 80
2.10.5 Capture Recordings on the Port 80
2.10.6 Ethereal Capture 81
2.10.7 Network Diagnosis..... 81
2.11 Product Information..... 82
2.12 Reboot 82
2.13 Logout..... 82
3 Appendix: VLAN Configuration..... 1
3.1 Manual Configuration..... 1
3.1.1 Single VLAN 1
3.1.2 Multi-service VLAN 2
3.2 Automatic Configuration..... 8
3.2.1 Handling Process for Automatically Enabling VLAN..... 8
3.2.2 Messages 9
4 Appendix: High availability configuration..... 11
5 Appendix: Auto provisioning configuration 12

Contents of Figure

Figure 1-1 HX4E Front Panel 11
Figure 1-2 HX4E Back Panel 11
Figure 1-3 MX8A Front Panel 13
Figure 1-4 MX8A Back Panel 14
Figure 1-5 RJ45 to RS232 Serial Cable 14
Figure 1-6 USB to RS232 Converter Cable 14
Figure 2-7 Login Interface for MX8A Gateway Configuration 17
Figure 2-8 Status Interface 18
Figure 2-9 Network Configuration Interface 19
Figure 2-10 VLAN Configuration Interface 21
Figure 2-11 System Configuration Interface 23
Figure 2-12 SIP Configuration Interface 25
Figure 2-13 High Availability Configuration Interface 26
Figure 2-14 MGCP Configuration Interface 28
Figure 2-15 Fax Configuration Interface 30
Figure 2-16 Configuration Interface for Phone Number 32
Figure 2-17 Subscriber Line Features Configuration Interface 33
Figure 2-18 Feature Batch Configuration Interface 36
Figure 2-19 Subscriber Line Characteristics Configuration Interface 37
Figure 2-20 Phone Number Configuration Interface 40
Figure 2-21 Trunk Line Features Configuration Interface 41
Figure 2-22 Trunk Batch Configuration Interface 43
Figure 2-23 Trunk Characteristics Configuration Interface 44
Figure 2-24 Configuration Interface for Digit map 46
Figure 2-25 Routing Table Configuration Interface 48
Figure 2-26 IP Table Configuration Interface 52
Figure 2-27 Interface of system advanced configuration 53
Figure 2-28 Interface of system advanced configuration (Remote management) 54
Figure 2-29 SNMP configuration interface 55
Figure 2-30 TR069 configuration interface 56
Figure 2-31 Security configuration interface 57
Figure 2-32 White List Configuration Interface 58
Figure 2-33 Media Stream Configuration Interface 58
Figure 2-34 SIP Related Configuration Interface 60
Figure 2-35 RADIUS Configuration Interface 63
Figure 2-36 Encryption Configuration Interface 64
Figure 2-37 Greeting Interface 65
Figure 2-38 Call Progress Tone Configuration Interface 66
Figure 2-39 Feature Codes Configuration Interface 67
Figure 2-40 Clock Service Interface 70
Figure 2-41 Call Status Interface 72
Figure 2-42 Interface of Call history on FXS 72
Figure 2-43 Interface of Call on FXO 73

Figure 2-44 SIP Message Count Interface ... 73
Figure 2-45 System Status Interface ... 74
Figure 2-46 Call Message Interface ... 75
Figure 2-47 Interface of System Startup ... 76
Figure 2-48 Manage Log Interface ... 76
Figure 2-49 Log Saving Interface ... 77
Figure 2-50 Path Saving Interface ... 77
Figure 2-51 Password Change Interface ... 78
Figure 2-52 Configuration Management Interface ... 78
Figure 2-53 Upgrade Interface ... 79
Figure 2-54 File Upload Interface ... 79
Figure 2-55 Upgrade Interface ... 79
Figure 2-56 Upgrade Process Screen ... 79
Figure 2-57 Interface for Completing Device Restart after Upgrade ... 80
Figure 2-58 Restore Factory Settings Interface ... 80
Figure 2-59 Interface for capturing Port Recordings ... 80
Figure 2-60 Ethereal Capture Interface ... 81
Figure 2-61 Automatic Diagnosis Interface ... 81
Figure 2-62 Ping Diagnosis Interface ... 81
Figure 3-63 Configuring the single VLAN ... 2
Figure 3-64 A Data Packet Carrying a Corresponding VLAN Tag in the Single VLAN Mode ... 2
Figure 3-65 Configuring Voice VLAN to Work in Mode 1 ... 3
Figure 3-66 Configuring Voice VLAN to Work in Mode 2 ... 4
Figure 3-67 Configuring Management VLAN ... 4
Figure 3-68 Network environment ... 5
Figure 3-69 Configuring Multi-service VLAN ... 6
Figure 3-70 IP Addresses of the Device in Multi-service VLAN ... 6
Figure 3-71 SIP Data Packet Carrying VLAN Tag of the Voice VLAN in the Multi-service VLAN Mode ... 7
Figure 3-72 RTP Data Packet Carrying VLAN Tag of the Voice VLAN in the Multi-service VLAN Mode ... 7
Figure 3-73 RTP Data Packet Carrying VLAN Tag of the Management VLAN in the Multi-service VLAN Mode ... 7
Figure 3-74 System Composition ... 8
Figure 3-75 Procedure of handling LLDP message carrying a VLAN ID ... 9
Figure 3-76 Procedure of handling the LLDP message with no VLAN ID ... 9
Figure 3-77 LLDP Message ... 10
Figure 3-78 Adding a VLAN ID to the message to be sent ... 10

Contents of Table

Table 1-1 MX8A and HX4E Series Gateway Hardware Specifications 9
Table 1-2 Configuration Combination of HX4E 11
Table 1-3 Description of HX4E Front Panel 11
Table 1-4 Description of HX4E Back Panel 12
Table 1-5 Indicator Status of HX4E 12
Table 1-6 Configuration Combination of MX8A 13
Table 1-7 Voice Interface Cards Supported by the MX8A 13
Table 1-8 Description of MX8A Front Panel 13
Table 1-9 Description of MX8A BackPanel 14
Table 1-10 Indicator Status of MX8A 14
Table 2-1 Default IP Address of Gateway 16
Table 2-2 Default Passwords of Gateway 17
Table 2-3 Network Configuration Parameters 19
Table 2-4 VLAN Configuration Parameters 21
Table 2-5 System Configuration Parameters 23
Table 2-6 Codec Methods Supported by Gateways 24
Table 2-7 SIP Configuration Parameters 25
Table 2-8 Parameters 26
Table 2-9 MGCP Configuration Parameters 28
Table 2-10 Fax Configuration Parameters 30
Table 2-11 Configuration Parameters of Phone Number 32
Table 2-12 Subscriber Line Features Configuration Parameters 33
Table 2-13 Subscriber Line Characteristics Configuration Parameter 37
Table 2-14 Configuration Parameters of FXO Phone Number 40
Table 2-15 Configuration Parameters of Trunk Features 41
Table 2-16 Trunk Characteristics Configuration Parameter 44
Table 2-17 Description of Digit Map 46
Table 2-18 Routing Table Format 49
Table 2-19 Number Transformations 49
Table 2-20 Routing Destination 51
Table 2-21 NAT Configuration Parameters 53
Table 2-22 Remote Management Configuration Parameters 54
Table 2-23 SNMP Configuration Parameters 55
Table 2-24 TR069 Configuration Parameters 56
Table 2-25 Security Configuration Parameters 57
Table 2-26 Media Stream Configuration Parameter 59
Table 2-27 SIP Related Configuration Parameter 61
Table 2-28 RADIUS Configuration Parameter 63
Table 2-29 Encryption Configuration Parameters 64
Table 2-30 Greeting Configuration Parameters 65
Table 2-31 Call Progress Tone Configuration Parameters 66
Table 2-32 Feature Codes Configuration Parameter 67
Table 2-33 Clock Service Parameters 71

Table 2-34 System Status Parameters 74
Table 2-35 Log Management Configuration Parameters 76

1 Overview

1.1 Product Introduction

MX8A and HX4E Series intelligent VoIP Gateways (MX Gateways) are designed to bridge the traditional telecom terminal device into IP networks through SIP or MGCP protocols. The main applications include:

- For carriers and value-added service providers to provide telephone, fax and voice-band data services to subscribers using IP access methods such as FTTB, HFC, and ADSL;
- Used to bridge the traditional telecom terminal equipment, such as PBXs, to the VoIP core networks of carriers;
- Connected with an enterprise PBX to provide IP-based voice private network solutions for institutions, enterprises and schools;
- Used as remote access equipment for IP-PBXs in call center deployment

The basic hardware specifications for the MX8A/HX4E are included in Table 1-1.

Table 1-1 MX8A and HX4E Series Gateway Hardware Specifications

Model	Voice ports	Chassis	Installation	CPU	RAM	Flash	Power
MX8A	4 - 8	Metal	Desktop or rack	MIPS34Kc, 700MHz, SOC	128MB	16MB	12 VDC
HX4E	2 - 4	Plastic Casing	Desktop	MIPS34Kc, 700MHz, SOC	64MB	16MB	12 VDC

Hardware for MX series gateways uses high-performance CPUs, ensuring that each product of the series can achieve full-capacity concurrent calls with high speech quality.

MX gateways software adopts the stable and reliable embedded Linux operating system (OS), implementing scores of business phone functions, including, call forwarding, call transfer, call hold, teleconference, caller identification, Do Not Disturb, ringback tone, hunt group simultaneous ring, distinctive ring, one phone with two numbers, and fax. In addition, MX gateways are featured with FXO port second stage dialing with voice prompt, routing table with a maximum of 500 entries, phone digit manipulation, and PSTN failover upon power-off or network disconnection.

MX gateways support local and remote management operations through Web GUI or Telnet/SSH, support SNMPv2-based and TR069/TR104/TR106-based centralized management schemes, and support auto provision. Maintenance tasks such as modifying configuration, upgrading software, collecting statistical data, downloading logs, and fault alarms can be performed.

1.2 Functions and Features

- Connect analog telephone, PBX, facsimile machine and POS machine to the IP core network, or PSTN
- Work with a service platform to provide various telephone supplementary services
- Support protocols: SIP, MGCP
- Support STUN. Detecting changes of the reflexive address of the device via STUN, and then triggering re-registration to the SIP registrar server.
- Flexible configuration of subscriber/trunk interfaces
- Support G.711, G.729
- Support echo cancellation
- Up to 500 routing rules can be stored in gateways
- Intercom
- Support concurrent calls under full load
- Support call progress tones for various countries and regions
- Support Line second stage dialing or voice prompt
- Support PSTN failover on power or network failure
- Security strategy: IP filter, encryption
- Support PSTN failover through FXO ports
- Support T.30/T.38 fax mode
- Support polarity inverse detection and busy tone detection
- 3-way calling
- Compatible with unified communication solutions, such as CallManager, Lync and Asterisk
- Support SNMPv2 and TR069/TR104/TR106
- Support Web GUI-based management , Telnet, automatic software upgrades, and configuration downloading
- Support high availability, implementing a cloud of SIP servers working in primary-standby or load balancing mode
- Support auto provision
- Support security settings such as whitelists
- Message waiting indications (MWI) with high voltage, FSK, or reversed polarity
- Support SSH
- Support Ping blocking
- Support IMS
- Modular FXS/FXO interface cards for MX8A

1.3 Equipment Structure

1.3.1 HX4E

The HX4E adopts a compact plastic structural design and can be placed on a desk.

It provides either two or four FXS/FXO ports.

The HX4E supports the following models:

Table 1-2 Configuration Combination of HX4E

Models	Number of FXS Ports	Number of FXO Ports
HX402E	2	0
HX420E	0	2
HX422E	2	2
HX412E	2	1
HX440E	0	4
HX404E	4	0

Figure 1-1 HX4E Front Panel

Table 1-3 Description of HX4E Front Panel

No.	Description
PWR	Power Indicator
WAN	Indicator of WAN interface
PC	Indicator of PC interface
FXO/FXS	Indicator of FXS port or FXO port

Figure 1-2 HX4E Back Panel

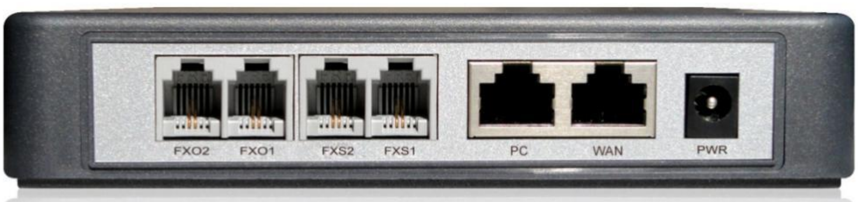


Table 1-4 **Description of HX4E Back Panel**

No.	Description
PWR	Power interface, 12 VDC input
WAN	10/100 M Ethernet Interface, RJ45
PC	10/100 M Ethernet Interface, RJ45
FXO/FXS	FXS port or FXO port

Table 1-5 **Indicator Status of HX4E**

Indicator	Status	Description
PWR(green)	Green Flashing	The device is starting.
	Steady green	The device is running.
	Off	The device is powered off or a power supply fault occurs.
STU (red, green)	Steady red	The WAN interface does not acquire the IP address. Possibly the WAN interface is not connected to a network cable, the WAN interface address fails to be acquired by using DHCP, the IP addresses are conflicted, and the PPPoE dialing fails.
	Red flashing	The device is starting or the Kupdate is upgrading.
	Steady green	Registration is successful.
	Blinking alternatively between red and green	Registration failed.
	Green flashing	Calling.
	Off	Registration has not started.
WAN (green)	Steady green	A WAN connection is established without any service flow.
	Green flashing	A WAN connection is established with service flow.
	Off	WAN interface is disconnected.
PC (green)	Steady green	A link is connected without any service flow.
	Green flashing	A service flow is being transmitted.
	Off	A link is not connected.
FXS/FXO (green)	Steady green	Off-hook or call established
	Green flashing	Ringing on incoming call
	Off	The port is in idle status

1.3.2 MX8A

The MX8A adopts a compact metal structural design. It can be placed on a desk or installed in a standard communications cabinet and provides eight analog ports. MX8A supports the following types of configuration.

Table 1-6 Configuration Combination of MX8A

Models	Number of FXS Ports	Number of FXO Ports
MX8A-4S/4	4	4
MX8A-6S/2	6	2
MX8A-8S	8	0
MX8A-8FXO	0	8

Table 1-7 Voice Interface Cards Supported by the MX8A

Voice Interface Card Types	Number of FXS Ports	Number of FXO Ports
401A-4FXS	4	0
401A-4FXO	0	4
401A-2FXS/2FXO	2	2

Figure 1-3 MX8A Front Panel

Table 1-8 Description of MX8A Front Panel

No.	Description
PWR	Power indicator
STU	Status indicator
WAN	Indicator of WAN interface
AUX	Indicator of AUX interface
VOICE	Indicators of FXS or FXO port

Figure 1-4 MX8A Back Panel

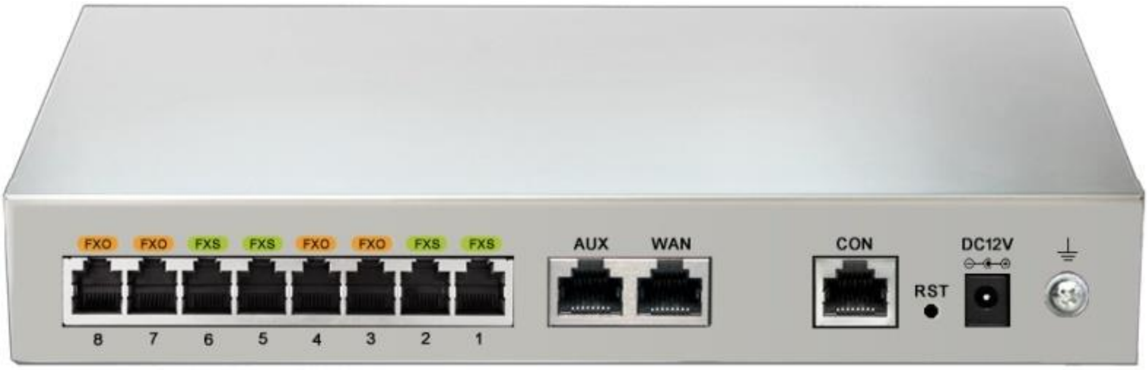


Table 1-9 Description of MX8A BackPanel

No.	Description
CON	The console port is used for local management and testing. PCs can be connected to device by linking the RS232 port to CON port. Connecting cables need to be produced or purchased. If the connection is established between the device and the mobile PC with no RS232 ports, please use the cable together with a USB to an RS232 converter cable. Cables are shown below in Figure 1-5 and Figure 1-6.
WAN	Ethernet interface
AUX	Auxiliary management interface
FXO/FXS	FXS port or FXO port

Figure 1-5 RJ45 to RS232 Serial Cable

Figure 1-6 USB to RS232 Converter Cable

Table 1-10 Indicator Status of MX8A

Indicator	Status	Description
PWR (green)	Green flashing	The device is starting.
	Steady green	The device is running.
	Off	The device is powered off or a power supply fault occurs.
STU (red, green)	Steady red	The WAN interface does not acquire the IP address. Possibly the WAN interface is not connected to a network cable, the WAN

Indicator	Status	Description
		interface address fails to be acquired by using DHCP, the IP addresses are conflicted, and the PPPoE dialing fails.
	Red flashing	The device is starting or the Kupdate is upgrading.
	Steady green	Registration is successful.
	Blinking alternatively between red and green	Registration is failed.
	Green flashing	Calling.
	Off	Registration has not started.
WAN (green)	Steady green	A WAN connection is established without any service flow.
	Green flashing	A WAN connection is established with service flow.
	Off	WAN interface is disconnected.
AUX (green)	Steady green	A link is connected without any service flow.
	Green flashing	A service flow is being transmitted.
	Off	A link is not connected.
VOICE (Green-FXS, yellow-FXO)	Indicates line type and device status:	
	Yellow flashing	The device is starting and the port is an FXO port.
	Green flashing	The device is starting and the port is an FXS port.
	Off	No line is detected. Possibly the voice interface card is not inserted or the port is damaged.
	Indicates running status:	
	Steady yellow	Calling in or out via an analog trunk.
	Yellow flashing	Ringing of calling in for an analog trunk.
	Steady green	Off-hook or call established
	Green flashing	Ringing on incoming call
	Off	The port is in idle status
	Note: The device starts up for approximate 30s to indicate line type, then indicates running status.	
Indicator of button:		
RST	To restore the MX8A to factory default, press the RST for more than 3 seconds and release it when STU turn blinking red. This setting will be valid after rebooting the device.	

2 Parameters Setting

2.1 Login

2.1.1 Obtaining Gateway IP Address

MX8A/HX4E Gateways start DHCP service by default, and automatically obtain an IP address on the LAN; you can use the factory-default gateway IP address if it is unable to be obtained (e.g. when connected directly with a computer).

To change the fixed IP address, you can use a telephone connected to the FXS port to dial ***90+the fixed IP address+#subnet mask#IP address of the gateway#0#**. The dots "." in the IP address need to be replaced with star keys "*".

To obtain an IP address through DHCP, you can use a telephone connecting to the FXS port to dial ***90###1#**, and after "The feature is now activated. " is heard, restart the device.

Table 2-1 Default IP Address of Gateway

Type	Default DHCP Service	Default IP Address	Default Subnet Mask
MX8A	Enabled	192.168.2.218	255.255.0.0
HX4E	Enabled	192.168.2.218	255.255.0.0

- You can dial ## to obtain the current gateway IP address, version information of firmware and port used to access the Web GUI using the telephone connected to the subscriber line (FXS ports) after the equipment is powered on.
- If the device does not have FXS ports (such as an MX8A-8FXO or HX440E), you can use New Rock's device IP address obtaining tool called "Finder" to obtain the IP address.
  You can get the "Finder" software by sending email to gs@newrocktech.com.

2.1.2 Logging On

Enter the gateway IP address in the browser address bar (e.g. 192.168.2.218). You can enter the gateway configuration login interface by entering a password on the login interface. Both Chinese and English Languages are provided for the Web GUI.

Figure 2-7 Login Interface for MX8A Gateway Configuration

2.1.3 Gateway Administrator and Operator Rights

Logon users are classified into administrator and operator. The default password is shown in Table 2-2. The password is shown in a cipher for safety.

Table 2-2 Default Passwords of Gateway

Type	Default Administrator Passwords (lowercase letters required)	Default Operator Password
MX8A	mx8	operator
HX4E	hx4	operator

The administrator can browse and modify all configuration parameters, and modify login passwords.

The operator can browse and modify a subset of the configuration parameters.

The gateways allow multiple users to log in if needed.

- If both an administrator and operator have logged in, the administrator can modify the configuration, while the operator is limited to browsing.
- When multiple users with the same level of permission log in, the first can modify, while others may only browse.

Note

- The system will confirm timeout if users do not conduct any operation within 10 minutes after login. They are required to log in again for continuing operations.
- Upon completion of configuration, click the **Logout** button to return to the login page, so as not to affect the login permission of other users.
- To ensure system security, please choose **Tools** > **Change password** and change the password when you log in for the first time. For details, see 2.10.1 Change Password.

2.2 Buttons Used on Gateway Management Interface

Save buttons are at the bottom of the configuration screens. It is used to submit configuration information. Users click the **Save** button after completion of parameter configuration on a page. A success prompt will appear if configuration information is accepted by the system; if **The configuration takes effect after the system is restarted** dialog box appears; it means that the parameters are valid only after a system restart. It is recommended that users press the **Reboot** button on top right corner to enable the configuration after changing all parameters to be modified.

2.3 Basic Configuration

2.3.1 Status

After login, open the **Basic** tab page to view device information. When the SIP port of the device is 5060, you are advised to modify it.

Figure 2-8 Status Interface

2.3.2 Network

After login, click **Basic** > **Network** tab to open the configuration interface.

Figure 2-9 Network Configuration Interface

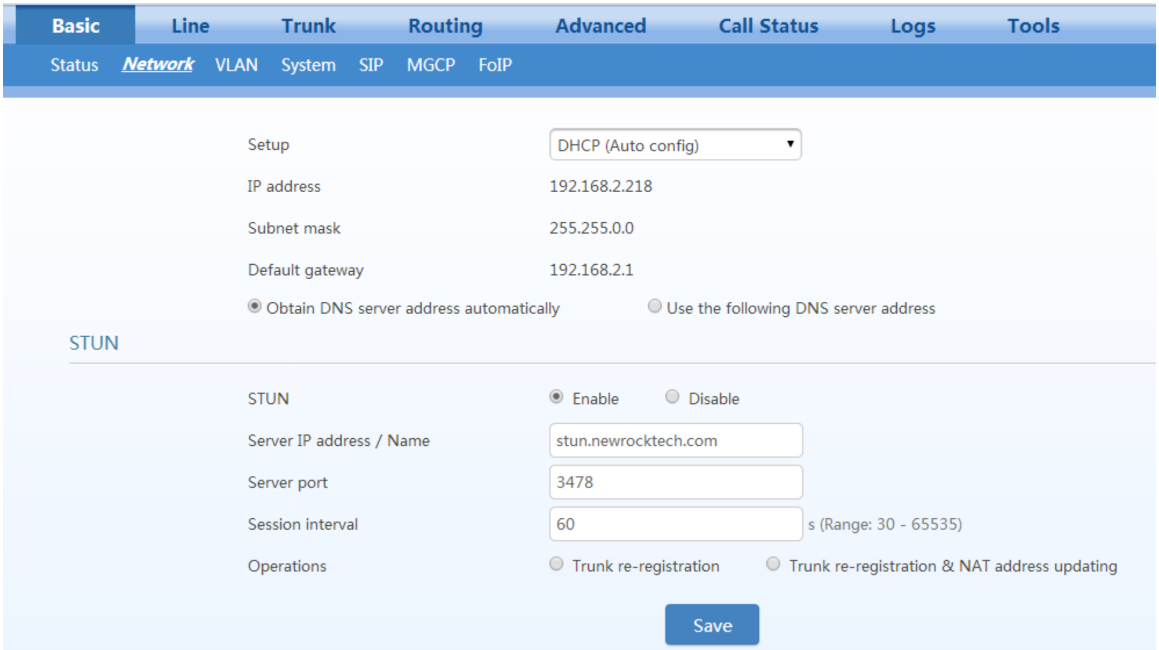


Table 2-3 Network Configuration Parameters

Name	Description
Setup	Methods for obtaining an IP address. • Static IP: static IP address is used; • DHCP: use the dynamic host configuration protocol (DHCP) to obtain IP addresses and other network parameters; • PPPoE: PPPoE service is used.
Username	Enter an authentication user name if PPPoE service is selected, and there is no default value.
Password	Enter an authentication password if PPPoE service is selected, and there is no default value.
IP address	If "Static IP" or "DHCP" is selected but an address fails to be obtained, the gateways will use the IP address filled in here. If the gateways obtain an IP address through DHCP, the system will display the current IP address automatically obtained from DHCP. This parameter must be set due to no default value.
Subnet mask	The subnet mask is used with an IP address. When the gateways uses a static IP address, this parameter must be entered; when an IP address is automatically obtained through DHCP, the system will display the subnet mask automatically obtained by DHCP. It has no default value.
Default gateway	The IP address of LAN gateway. When the gateways obtain an IP address through DHCP, the system will display the LAN gateway address automatically obtained through DHCP. It has no default value.
Obtain DNS server address automatically	When the connection mode is "DHCP" or "PPPoE", the device uses the automatically obtained IP address of the DNS server.
Use the following DNS server address	Use the DNS server addresses specified manually.

Name	Description
Primary DNS Server	If **Use the following DNS server address** is selected, the network IP address of the **Primary DNS server** must be entered, and there is no default value.
Secondary DNS Server	If **Use the following DNS server address** is selected, the network IP address of the **Secondary DNS server** can be entered, and there is no default value.
STUN	The device periodically sends a STUN request to the STUN server to obtain the public IP address for the front-end router. It is disabled by default.
Server IP address / Name	Set the IP address or domain name of the STUN server. The factory default STUN server is the New Rock STUN server.
Server port	Set the port of STUN server. It is 3478 by default.
Session interval	The interval at which the device sends a STUN request ranges from 30 to 3600 seconds.
Operations	• **Trunk re-registration**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. Normally, the session interval of STUN request should be shorter than the registration period. Note: The IP address obtained through STUN is used only for re-registration of SIP server, and it is not used in SIP message fields such as Via and Contact and SDP C field. • **Trunk re-registration & NAT address updating**: A re-registration of the SIP trunk is triggered upon the detection of the change of the public IP address of the device by using STUN query. And the IP address obtained through STUN is used in SIP message fields such as Via and Contact and SDP C field.

2.3.3 VLAN

After login, click **Basic** > **VLAN** tab to open the configuration interface.

Figure 2-10 VLAN Configuration Interface

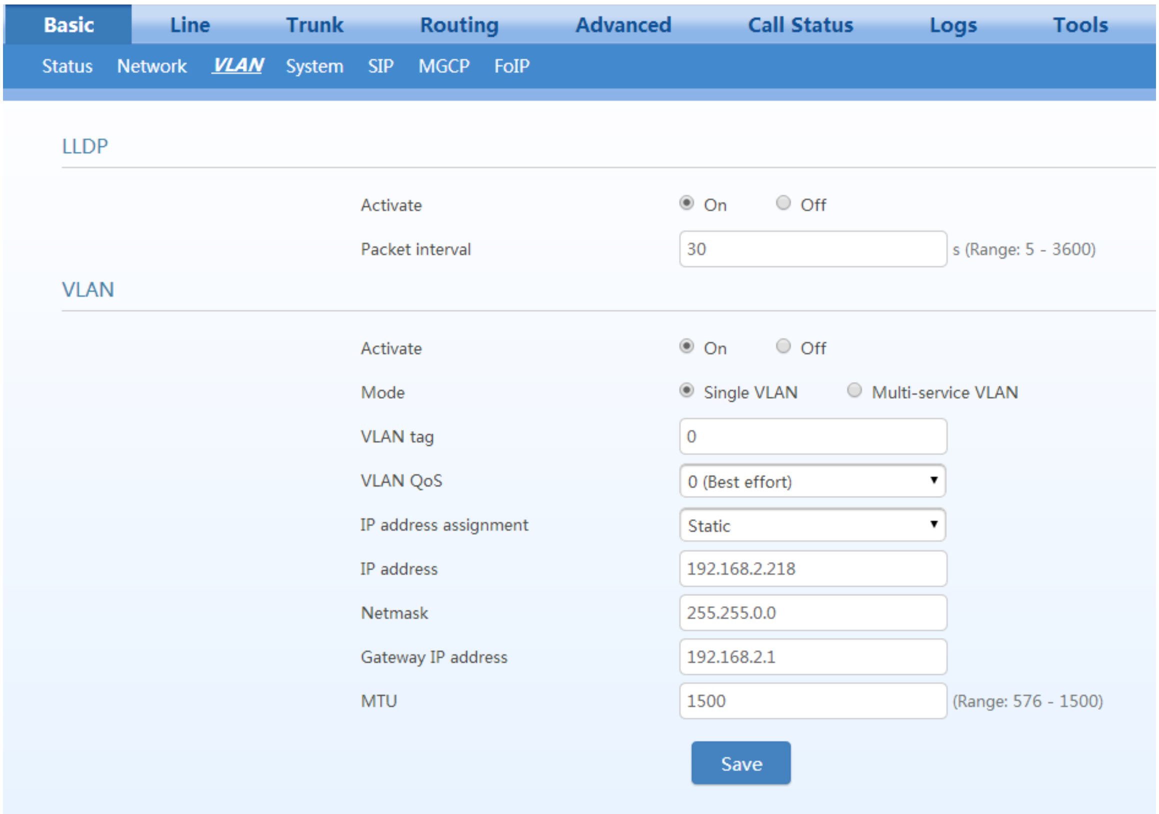


Table 2-4 VLAN Configuration Parameters

Name	Description
LLDP	
Activate	• **On**: Indicates that the LLDP is enabled. Then the device periodically sends LLDP messages, and parses received LLDP messages. • **Off** (default value): Indicates that the LLDP is disabled. The device does not send any LLDP messages, nor parses any received LLDP messages.
Packet interval	This parameter specifies the interval at which LLDP messages are sent after the LLDP is enabled. The value range is 5 to 3600 seconds. The default value is 30 seconds.
VLAN	
Activate	• **On**: enable VLAN • **Off**: disable VLAN
Mode	Select the VLAN mode: • **Single VLAN**: All services of the device are on the same VLAN, and the device receives only data packets carrying the VLAN and includes the VLAN tag in all sent data packets. • **Multi-service VLAN**: The device can configure different VLAN information for the voice service (SIP signaling and RTP/T.38 media stream) and the management service (HTTP, Telnet, TR069, and SNMP) and includes a different VLAN tag in a data packet of a different service.

Name	Description
Voice VLAN	VLAN to which the voice service (SIP signaling and RTP/T.38 media stream) belongs. • **None**: disable the voice VLAN • **Mode 1**: SIP and RTP/T.38 are on the same VLAN • **Mode 2**: SIP and RTP/T.38 are on different VLANs
Management VLAN	Selected: enable the management VLAN Deselected: disable the management VLAN
VLAN tag	Tag of the VLAN. The value ranges from 1 to 4094.
VLAN QoS	Priority of the VLAN. The value ranges from 0 to 7. A larger value indicates a higher priority of a to-be-sent data packet.
IP address assignment	Type for obtaining the IP address of the VLAN interface. • **Static**: set the IP address to a static IP address • **DHCP**: automatically obtain an IP address by using the DHCP protocol
IP address	IP address of the VLAN interface
Netmask	Subnet mask of the VLAN interface
Gateway IP address	IP address of the gateway of the VLAN interface
MTU	Maximum Transmission Unit value of the VLAN interface. The value ranges from 576 to 1500. The default value is 1500.

Note

- A reboot is required to enable the VLAN configuration.
- After a VLAN is configured, only PCs in the same VLAN can access the device.
- The device address used to log in to the Web GUI can be obtained by connecting a phone to an FXS (Phone) port of the device, and dialing "##". In the case of a single VLAN, the IP address of the single VLAN is voiced; in the case of a multi-service VLAN, the IP address of the management VLAN is voiced.

2.3.4 System

After login, click **Basic** > **System** tab to open the configuration interface.

Figure 2-11 System Configuration Interface

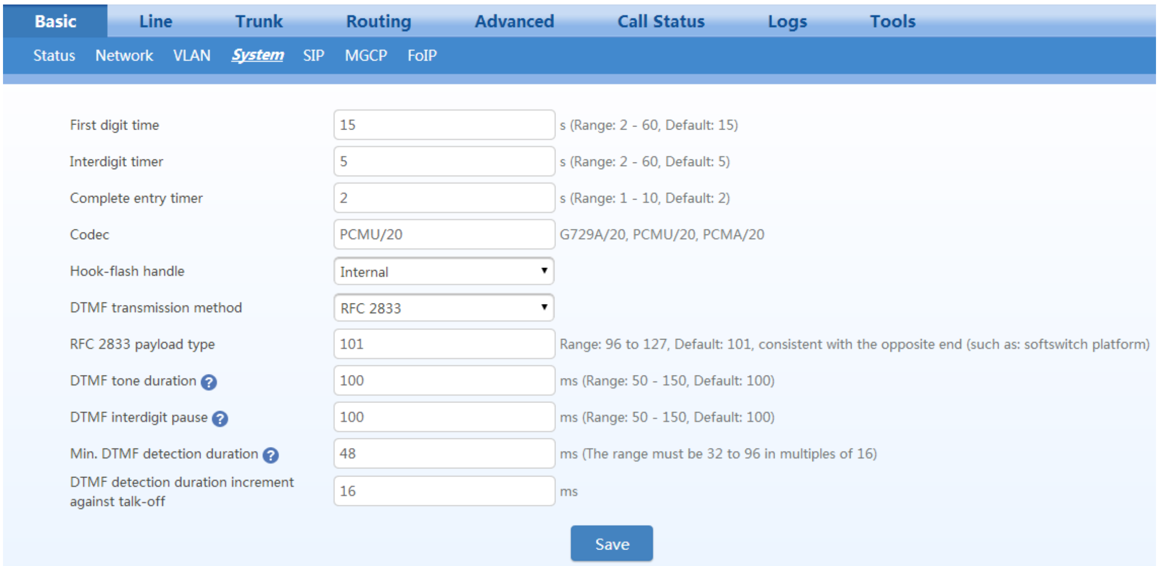


Table 2-5 System Configuration Parameters

Name	Description
First digit timer	If a subscriber does not dial any digit within the specified time by this parameter after off-hook, the gateways will prompt to hang up with a busy tone. The value must be an integer, and decimal points are not allowed. Unit: Seconds; Default value: 15 seconds.
Interdigit timer	The maximum time interval to dial the next digit. After timeout, the gateways will call out with the collected number. The value must be an integer, and decimal points are not allowed. Unit: Seconds; Default value: 5 seconds.
Complete entry timer	The value must be an integer, and decimal points are not allowed. Unit: second; Default value: 2 seconds. This parameter is used with the "x.T" rule set in dialing rules. For example, there is "021.T" in the dialing rules table. When a subscriber has dialed 021 and hasn't dialed the next number within a set time by this parameter (eg. 2 seconds), the gateways will consider that the subscriber has ended dial-up and call out the dialed number 021.
Codec	Codecs supported by the deivce include G729A/20, PCMU/20 and PCMA/20. This parameter must be set due to no default value. For details, see Table 2-6. Several encoding methods can be configured in this item at the same time, separated with "," in the middle; the gateways will negotiate with the platform in the order from front to back when configuring the codec methods.
Hook-flash handle	The gateways provide the following processing modes after detecting hook flash from subscriber terminals: Internal: the hook flash event will be handled internally; Server(RFC 2833): transmitting the hook flash to platform with RFC 2833; Server (SIP INFO): transmitting the flash-off to platform with SIP INFO.

Name	Description
DTMF transmission method	Transmission modes of DTMF signal supported by the gateways include RFC 2833, Audio and SIP INFO. The factory default value is RFC 2833. • **RFC 2833**: separate DTMF signal from sessions and transmit it to the platform through RTP data package in the format of RFC2833; • **Audio**: DTMF signal is transmitted to the platform with sessions; • **SIP INFO**: separate DTMF signal from sessions and transmit it to the platform in the form of SIP INFO messages. • **RFC2833+SIP INFO**: sending DTMF signals simultaneously via RFC 2833 and SIP INFO.
RFC 2833 payload type	Used with "RFC 2833" in the DTMF transmission modes. The default value of 2833 payload type is 101. The effective range available: 96 ~ 127. This parameter should match the setting of far-end device (eg. platform).
DTMF tone duration	This parameter sets the on time (in ms) of DTMF signal sent from FXO port. The default value is 100 ms. The duration time range is 50 ~ 150 ms.
DTMF interdigit pause	This parameter sets the off time (ms) of DTMF signal sent from port. The default value is 100 ms. The duration time range is 50 ~ 150 ms.
Min. DTMF detection duration	Minimum duration time of effective DTMF signal. Its effective range is 32 to 96 ms. The default value is 48 ms. The greater the value is set, the more stringent the detection is.
DTMF detection duration increment against talk-off	An actual detection threshold is determined jointly by using the **Min. DTMF detection duration** and this parameter. Actual detection threshold = **Min. DTMF detection duration** + **DTMF detection duration increment against talk-off**. The valid values are 16, 32, and 48 in million seconds. Increase the value can prevent false detection of DTMF signal.

Table 2-6 Codec Methods Supported by Gateways

Codec	Bit Rate (Kbit/s)	Time Intervals of RTP Package Sending (ms)
G729A	8	10/20/30/40
PCMU/PCMA	64	10/20/30/40

2.3.5 SIP

After login, click **Basic** > **SIP** tab to open the configuration interface.

Figure 2-12 SIP Configuration Interface

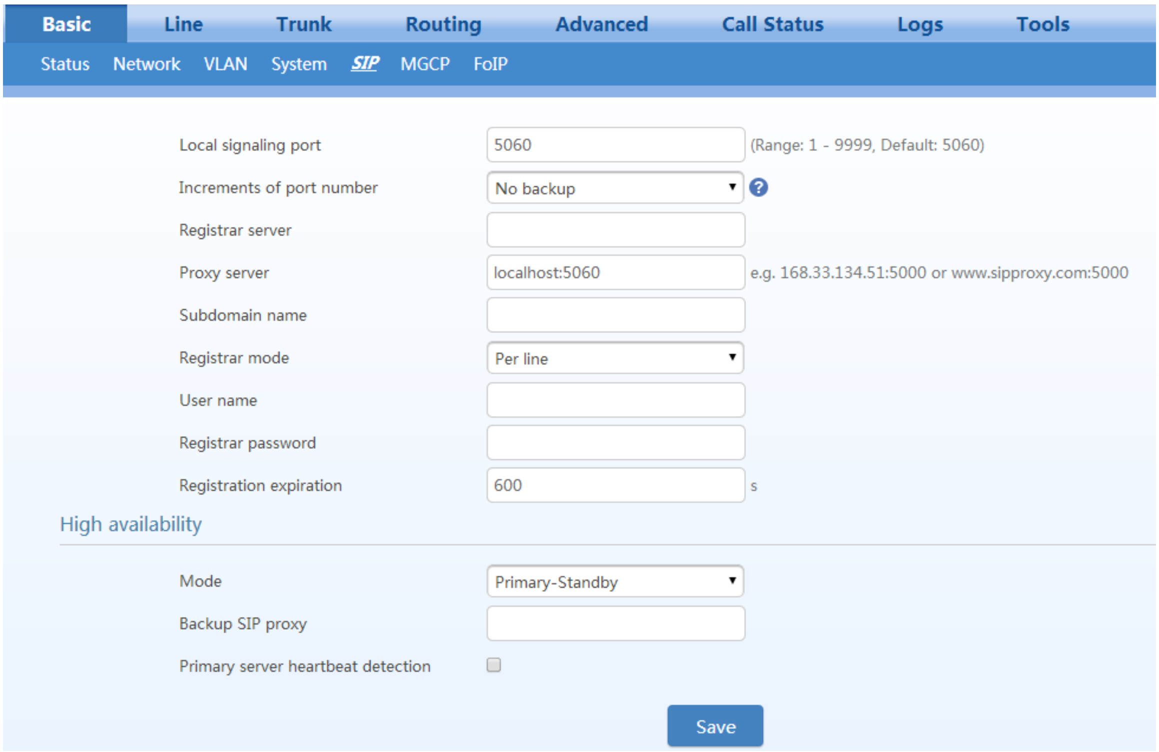


Table 2-7 SIP Configuration Parameters

Name	Description
Local Signaling port	Configure the UDP port for transmitting and receiving SIP messages, with its default value 5060. Note: The signaling port number can be set in the range of 1-9999, but cannot conflict with the other port numbers used by the equipment.
Increments of port number	If "n" (ranked from 1-10) is chosen, after the failure registration of signaling port's original configuration, the range of signaling port's change varies from "original signaling port, original signaling port +n". Register with the new signaling port value (signaling port +1) until it succeeds.
Registrar server	Configure the address and port number of the SIP registration server. The address and port number are separated by ":". It has no default value. The register server address can be an IP address or a domain name. e.g. 168.33.134.51:5000 or www.sipproxy.com:5000. When a domain name is used, you must activate DNS service and configure DNS server parameters on the network-configuration page.
Proxy server	Configure the IP address and port number of the SIP proxy server. The address and port number are separated by ":". It has no default value. The proxy server address can be set to an IP address or a domain name. e.g. 168.33.134.51:5000 or www.sipproxy.com:5000. When a domain name is used, you must activate DNS service and configure DNS server parameters on the network-configuration page. When a domain name is used, you can fill in a backup IP address in **Backup SIP proxy server** in the High Availability configuration. This allows the device to failover to the IP address if the domain name resolution service fails.

Name	Description
Subdomain name	This domain name will be used in INVITE messages. If it is not set here, the gateways will use the IP address or domain name of the proxy server as the user-agent domain name. It has no default value.
Registrar mode	The gateway supports three registration schemes: • **Per line** (default): authentication and register per line. • **Per gateway**: authentication and register per gateway. • **Per line/GW auth**: Enable registration per line. Use the number configuration per line. Use the global account and password in authentication.
User name	Configure the user name as part of the account for registration. It has no default value. Note: If **Per gateway** or **Per line/GW Auth** is selected for **Registrar mode**, the user name must be entered here. If **per line** is selected the user name should be set on “Line > Feature” page (Refer to 2.4.2 Subscriber Line Features).
Registrar password	Password as part of account information is used for authentication by platform. It has no default value. It is formed with either numbers or characters, and case sensitive. Note: If **Per gateway** or **Per Line/GW Auth** is selected for **Registrar mode**, the password must be entered here. If **Per line** is selected the password should be set on “Line > Feature” page (Refer to 2.4.2 Subscriber Line Features).
Registration expiration	Valid time of SIP re-registration in seconds. Its default value is 600.

2.3.6 High Availability

After login, click **Basic** > **SIP** tab to open the configuration interface.

For details, see http://website.newrocktech.com/Files/High%20Availability%20Configuration%20Guide.pdf.

Figure 2-13 High Availability Configuration Interface

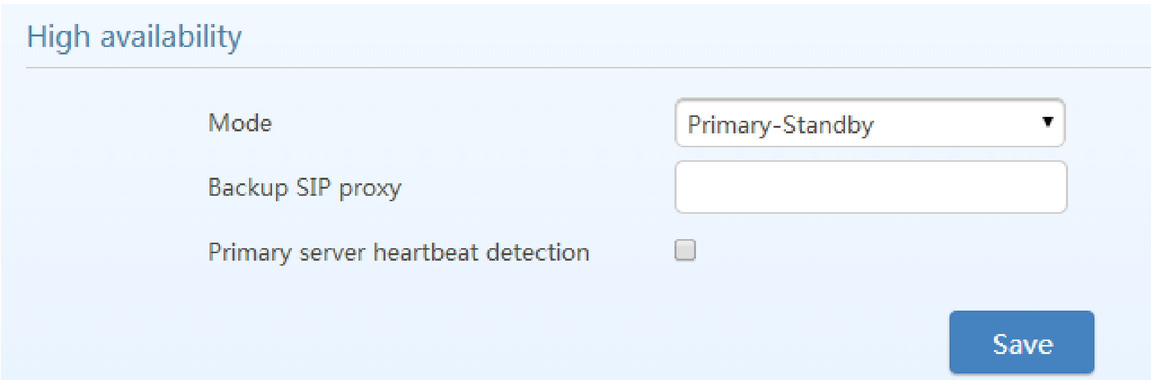


Table 2-8 Parameters

Name	Description
Mode	High availability can be configured as Primary-Standby, Active-Standby or Load Balancing mode.
Primary-Standby mode	

Name	Description
Backup SIP proxy	Configure the address and port number of the backup SIP proxy server. When the primary SIP server faults, the gateway failovers from the primary server to the backup server automatically.
Primary server heartbeat detection	Select it to send OPTIONS request to the primary SIP server all the time. If the gateway does not receive any response to OPTIONS request, it failovers to the backup server. After failover to the backup server, the gateway will still send OPTIONS to the primary server. It switches back to the primary server once the response to the OPTIONS request is received.
OPTIONS request period	The interval between receiving the response (200) from the SIP server to the previous OPTIONS and sending the next OPTIONS.
Active-Standby	
SIP proxy server setting	A maximum of five servers can be added.
OPTIONS Keep-alive	**Enable**: the device sends OPTIONS request to the current SIP server. **Disable**: the device doesn't send OPTIONS request to the current SIP server.
Active SIP server	This parameter displays the current SIP server address.
Switchover	If you click Switchover, the gateway performs switchover to the next available server in sequence based on the SIP server list.
Load balancing	
SIP proxy server setting	A maximum of five SIP servers can be added.
OPTIONS request period	The interval between receiving the response (200) from the SIP server to the previous OPTIONS and sending the next OPTIONS.
OPTIONS request timeout	The period since the sending of the last OPTIONS with no response by the SIP server.
REGISTER request timeout	The period of time from the sending of the first REGISTER with no response by the previous SIP server to the sending of REGISTER to the next SIP server.

2.3.7 MGCP

The gateways use SIP protocol by default. When the gateways need to interface with MGCP protocol -based softswitch platform, set the relevant parameters here.

After login, click **Basic > MGCP** tab to open the configuration interface.

Figure 2-14 MGCP Configuration Interface

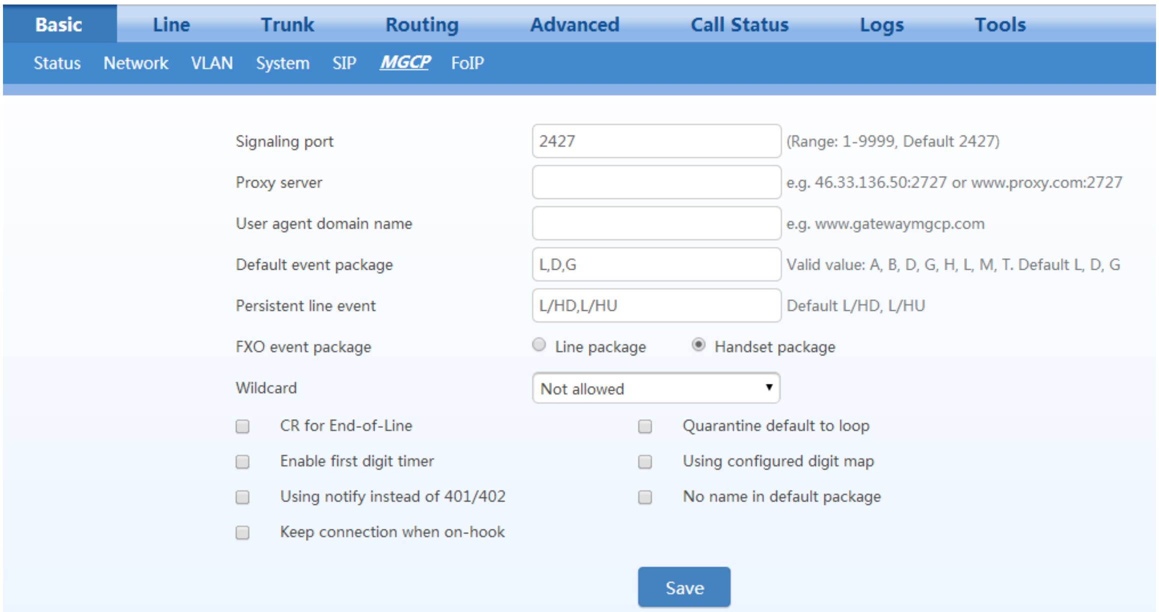


Table 2-9 MGCP Configuration Parameters

Name	Description
Signaling port	Configure the UDP port for transmitting and receiving MGCP messages, and the default value is 2427. Note: The signaling port number can be set in the range of 1-9999, but cannot conflict with the other port numbers used by the equipment.
Proxy server	Configure the IP address and port number of MGCP proxy server, separated by ":". It has no default value. The address can be set to an IP address or a domain name according to the subscribers' requirements. When a domain name is used, it is required to configure DNS server on the "**Basic** > **Network**" page. Examples of complete and effective configuration: **46.33.136.50:2727** or **www.proxy.com: 2727**.
User agent domain name	The domain name associated with the call agent, and it has no default value. DNS server is required to set. Example: www.gatewaymgcp.com.
Default event package	List all the types of default event packages supported by the HX4. Multiple package names are separated by",". The default value is L, D, G L: Line Package D: DTMF Package G: Generic Media Package
Persistent line event	List the event types that the gateway can report, with multiple types separated by ",". When gateways process the events listed here, they will report to the call agent. Note: This parameter must be set since there is no default value. The factory setting is L/HD, L/HU: L/HD: Offhook L/HU: Onhook

Name	Description
FXO event package	Handset Packag or Line Package
Wildcard	Select whether a wildcard with prefix is allowed when a gateway registers to the proxy server. The default value is **not allowed.** Partially allowed: gateways will use a wildcard with fixed prefix (e.g. aaln / *) when registering. For example, when configuring telephone numbers, if line 1 is set to aaln/1, line 2 is set to aaln/2 and line 3 is set to aaln/3, the gateways will register to the call agent in aaln/* without the need of registering the lines individually. Allowed: the gateways will use a wildcard in registering without prefix.
CR for End-of-Line	Select whether CR is used as the end of line in the MGCP messages. Default not selected.
Quarantine default to loop	Select the Quarantine handle of gateways making a request to the outside, and default not selected. Selected: quarantine using loop mode, the gateways will continually notify all events as requested after receiving a request.
Enable first digit timer	Select the processing mode when there is no timeout parameter in the outside request received by the gateways, and default not selected. Selected: the gateways will report timeout in terms of its own timeout setting (the time interval set in non-dial timeout of configuration system parameters) when subscribers hasn’t dialed up in time after offhook.
Using configured digit map	Select whether to activate the digit map configured by local gateway, and default value is not selected.
Using notify instead of 401/402	Set whether the gateways report “offhook events” to replace 401 messages in NTFY or report “onhook events” to replace 402 messages in NTFY when responding to messages sent by the proxy server. Default: not selected. Selected: the gateways will use NTFY messages to replace 401 and 402 messages.
No name in default package	Select if a package name is included when the gateways reply to the default package, and default not selected.
Keep connection when on-hook	Select if the gateways actively cancel connection disconnect when subscribers hook on, and default not selected.

2.3.8 FoIP

After login, click the label of **Basic** > **FoIP** to open this interface.

Figure 2-15 Fax Configuration Interface

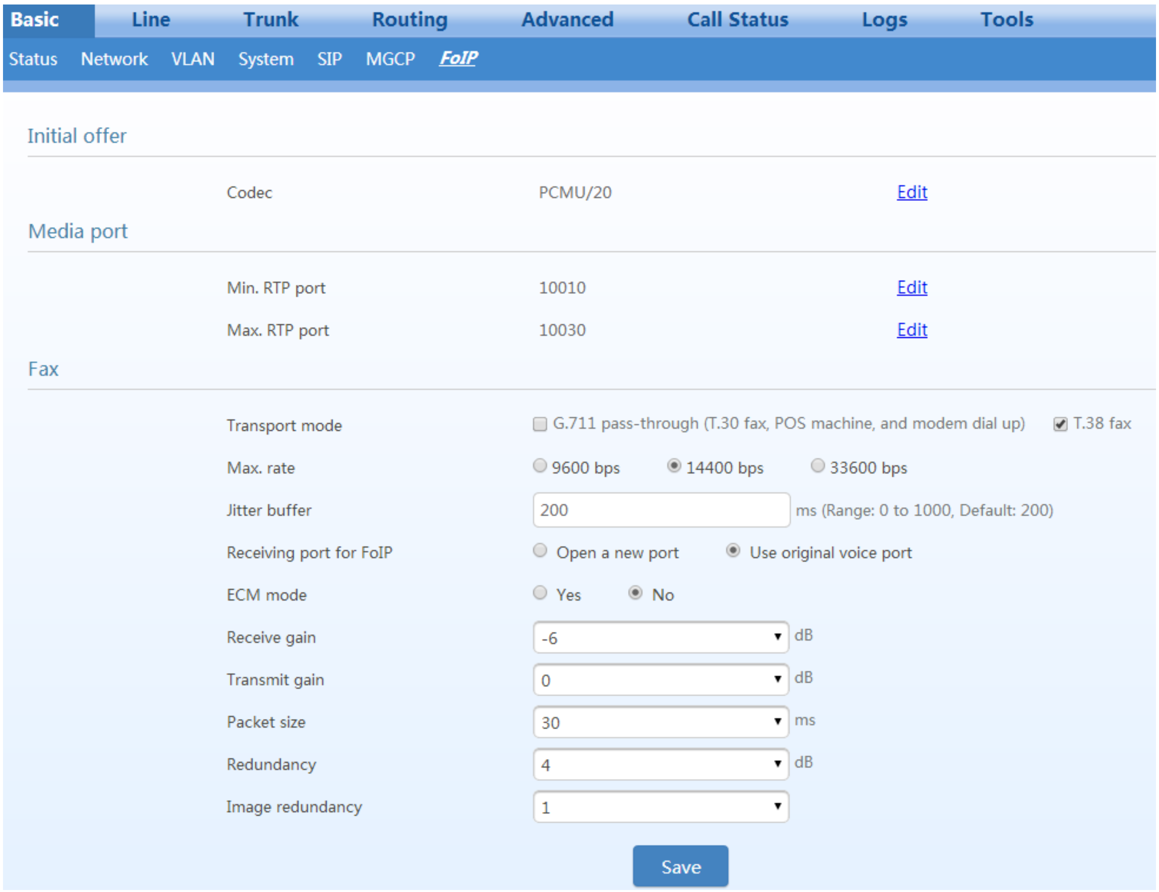


Table 2-10 Fax Configuration Parameters

Name	Description
Initial offer	
Codec	Go to **Basic** > **System** page to configure by clicking **Edit**. For details, see 2.3.4 System.
Media port	
Min. RTP port	Go to **Advanced** > **Media stream** page to configure by clicking **Edit**. For details, see 2.7.6 Media Stream.
Max. RTP port	Go to **Advanced** > **Media stream** page to configure by clicking **Edit**. For details, see 2.7.6 Media Stream.
Fax	
Only **G.711 pass-through** selected	This parameter applies only to the T.30, POS terminal, and MODEM service. In this mode, the voice codec must be set to G.711; otherwise the facsimile service fails.
Only **T.38 fax** selected	T.38 with CED T.38 with CNG
Both **G.711 pass-through** and **T.38 fax** selected	Both T.30 and T.38 Note: When received fax signaling carries both T.30 and T.38 media, preferentially use T.38.
Adjustable parameters when the T.38 is enabled (Default values are recommended.)	

Name	Description
Max. rate	Set the maximum fax transmission rate using these three options: • 9600: negotiates the transmission rate first in accordance with the V.29. The maximum value is 9600 bps. • 14400 (default value): negotiates the transmission rate first in accordance with the V.17. The maximum value is 14400 bps. • 33600: negotiates the transmission rate first in accordance with the V.34. The maximum value is 33600 bps. Otherwise, keep it the default value. You need to modify it only when the negotiation peer requires.
Jitter buffer	Set the extent of T.38 jitter buffer, and the default is 250. The valid range is 0~1000 in milliseconds.
ECM mode	Determine whether to use corrective mode of fax. By default, it is not selected. By default, it is not selected.
Packet size	Set the packet size of T.38. 30 milliseconds is the default value.
Redundancy	Set the number of the redundant frames in T.38 date package, default is 4.
Image redundancy	Set the number of the redundant image in T.38 date package, default is 1.
Parameters available only in the MX8A	
Receiving port for FoIP	Set whether to open a new port when the gateway is switching to T.38 mode, and by default, original voice port will be used. • **Open a new port**: use the new RTP port. • **Use original voice port**: use the original RTP port that created on call set.
Receive gain	Set the receiving gain of T.38 fax, with the default of -6dB.
Transmit gain	Set the transmission gain of T.38 fax, with the default of 0dB.

2.4 Line

2.4.1 Phone Number

Only a gateway with FXS ports can display this interface.

After login, click **Line > Phone number** tab to open the configuration interface.

Figure 2-16 Configuration Interface for Phone Number

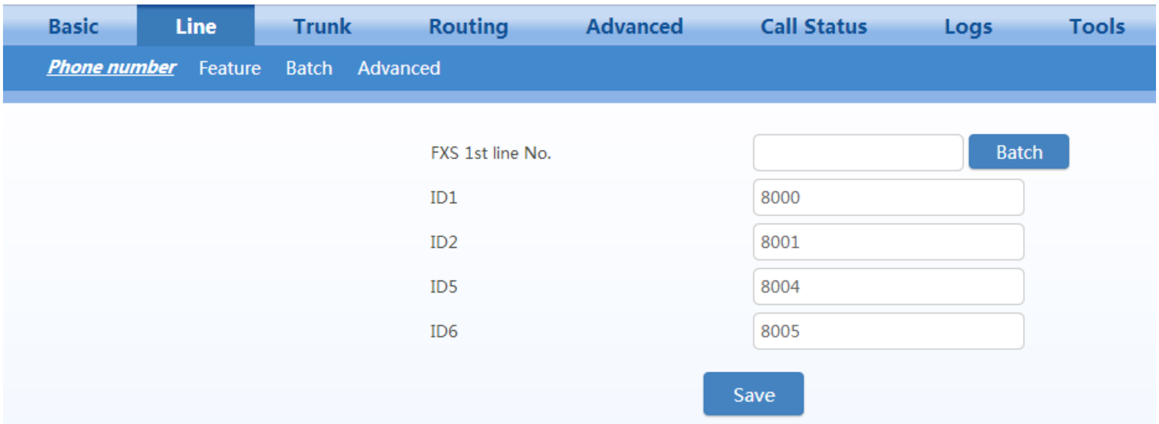


Table 2-11 Configuration Parameters of Phone Number

Name	Description
FXS 1st line No.	This number is used for the batch setup of consecutive number of subscriber line. Click Batch after filling in initial number, the number of Line 1 adopts initial number; that of Line 2 increases 1 progressively based on that of Line 1, and so on. You needn't fill in if you do not use batch configuration or the number is not consecutive.
ID n	Fill in the telephone number associated with the subscriber line n (FXS port). This should be manually performed if Batch mode is not used.

2.4.2 Subscriber Line Features

Only a gateway with FXS ports can display this interface.

After login, click **Line** > **Feature** tab to open the configuration interface.

Figure 2-17 Subscriber Line Features Configuration Interface

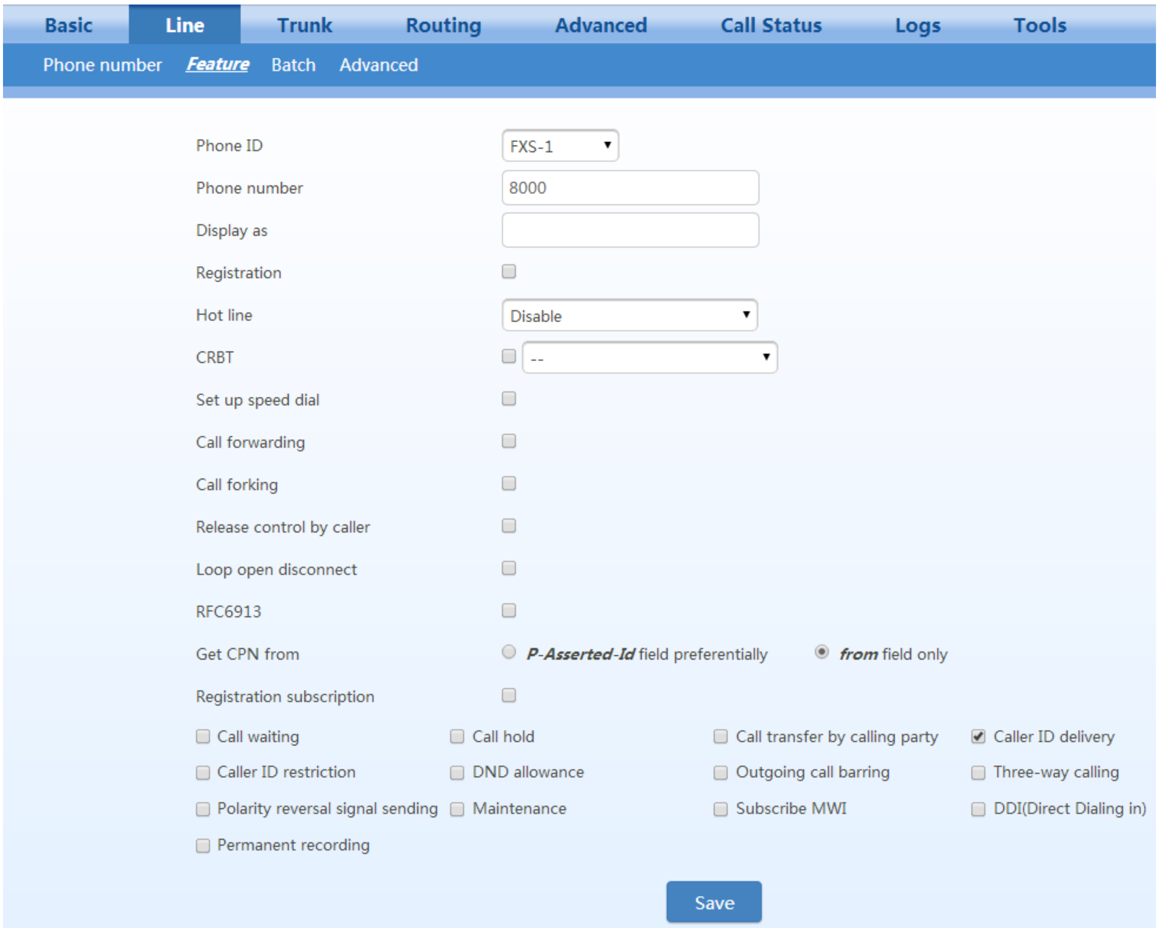


Table 2-12 Subscriber Line Features Configuration Parameters

Name	Description
Phone ID	Fill in the phone number associated with this port. “FXS-n” corresponds to the **Line** > **Phone Number** > **ID n**.
Phone number	Fill in the name associated with this port.
Display as	Fill in the display name which will be contained in the From field of SIP message. e.g. From: "Bob " <sip:8000@127.0.0.1>;tag=14340047091433920745-1, Bob is the display name.
Local SIP port	This parameter is displayed only when **multi port** is selected in page **Advanced** > **SIP**. Set the port used for receiving and sending SIP messages associated with the line. If this parameter is not specified, the local port configured in **Basic** > **SIP** is used.
Registration	Select if this line is required to register to a softswitch. This is selected as default.
User name	If **Registration** is selected, users must enter the user name for registering the line here. This is not mandatory. If this parameter remains blank, the phone number of the extension set is used.
Registrar password	If **Registration** is selected, users must enter the authentication password for registering of this line here.
Note: The following features are valid only in SIP protocol. When the gateways use MGCP protocol, features are controlled by the proxy server without the need for setting on the gateway.	

Name	Description
Hot line	Select if the gateway is required to automatically dial out the hotline number after offhook. By default, hot line is disabled. • **Disable hot line**: close this feature. • **Hot line**: automatically dial out the hotline number after offhook. • **Delay mode**: automatically dial out the hotline number when the offhook is timeout with a time delay of 5 seconds.
CRBT(Color ring back tone)	Select it to activate CRBT (Color Ring Back Tone), and choose an audio file as ring back tone. There are two.dat files in the G.729 coding format (fring1.dat and fring2.dat) storage in MX for factory default. You can upload .wav files through the Web GUI, for details, see **2.7.10 Greeting**.
Set up speed dial	Select if the Speed dials is activated on this line. By default, this is not selected.
Speed dial groups	Use "Abbreviated number-Phone number", such as 20-13812345678. Use a forward slash "/" to separate each group of abbreviated numbers. The abbreviated numbers range from 20 to 49. A maximum of 399 bytes can be configured.
Call forwarding	Select if Call forwarding is activated on this line. By default, it is not selected.
Unconditional	All incoming calls are forwarded to the telephone number specified in this parameter.
No Answer	All incoming calls are forwarded to the telephone number specified in this parameter when they are not answered.
Busy	All incoming calls are forwarded to the telephone number specified in this parameter when the extension is busy.
Call Forking	Select to activate call forking. Forking allows the device to initiate a call to another telephone terminal while ringing on this line terminal. Either terminal may answer, terminating ringing on the other terminal.
Release control by caller	Select if the call release is controlled by the caller. By default, this is not selected. Selected: the gateway will immediately release the call upon caller hanging up; the gateway will not release the call after the called party hanging up as long as the caller is still off-hook until timeout (60 seconds by default); Unselected: the gateway will immediately release the call upon either party hanging up the call.
Loop open disconnect	Select it only if the trunk of the PBX supports loop open signaling, in which the PBX takes the loop open as the indication of disconnection. Select it only if the trunk of the PBX supports loop open signaling, in which the PBX takes the loop open as the indication of disconnection. Note: Loop open interval can be configured on the Advanced > Line page.
RFC6913	If this item is selected, the Fax over IP label carried in INVITE is supported.
Get CPN from	If a received INVITE message carries **From** and **P-Asserted-Id** header fields, the caller identification number will be selected according to this parameter. If the received INVITE message does not carry the **P-Asserted-Id** header field, caller identification numbers are obtained from the **From** header field. • ***P-Asserted-Id* field preferentially**: The caller identification information is preferentially obtained from the P-Asserted-Id field in the INVITE message. • ***From* field only**: The caller identification information is obtained from the From field in the INVITE message. ***From* field only** is selected by default.

Name	Description
Registration subscription	The device subscribes the registration status of the line. If the subscription is successful, the SIP server sends a NOTIFY message for notification of the registration status of the line.
Call waiting	Select if Call waiting is activated on this line. By default this is not selected.
Call hold	Select it to enable Call Hold on this line. By default this is not selected. Note: If this function is enabled, the gateways will automatically activate Call Transfer.
Call transfer by calling party	Select if Caller Transfer is activated on this line. By default, this is not selected. When A calls B, B picks up the call and A transfers the call to C. Note: The call hold must be activated before caller transfer.
Caller ID delivery	Set whether the calling number is sent to the called party. This feature requires the support of softswtich. By default this is selected.
Caller ID restriction	Set whether the number of this telephone is sent to the called party with support from platform. By default this is not selected
Outgoing call barring	Select if outgoing calls are barred on this line. By default, this is not selected.
DND allowance	Select if **Do Not Disturb** is allowed to enable on this line. By default, this is not selected.
Three-way calling	Select if 3-way service is activated, and by default this is not selected.
Polarity reversal signal sending	Select if reverse polarity signal sending is activated on this line. By default, this is not selected. Note: The gateways will provide reverse polarity signal when the phone is connected after this feature is activated.
Maintenance	Select if the line is set to maintenance status, in which the FXS port no longer supplies current to the phone. By default, this is not selected.
Subscribe MWI	Select if voice mail service is activated, and by default this is not selected. (Also see **MWI Re-subscription** on page **Advanced** > **SIP**.)
DDI (Direct Dialing in)	Set whether DDI (Direct Dialing In) is activated, By default, this is not selected. Different from FXS, DDI is only used for incoming calls, and the gateways will not send dial tone after off-hook (calling in) on user side. Note: Reverse polarity signal must be activated on the gateways when DDI is used.
Permanent recording	Select if recording service is activated, and by default this is not selected.

2.4.3 Subscriber Line Batch (Unavailable on the HX4E)

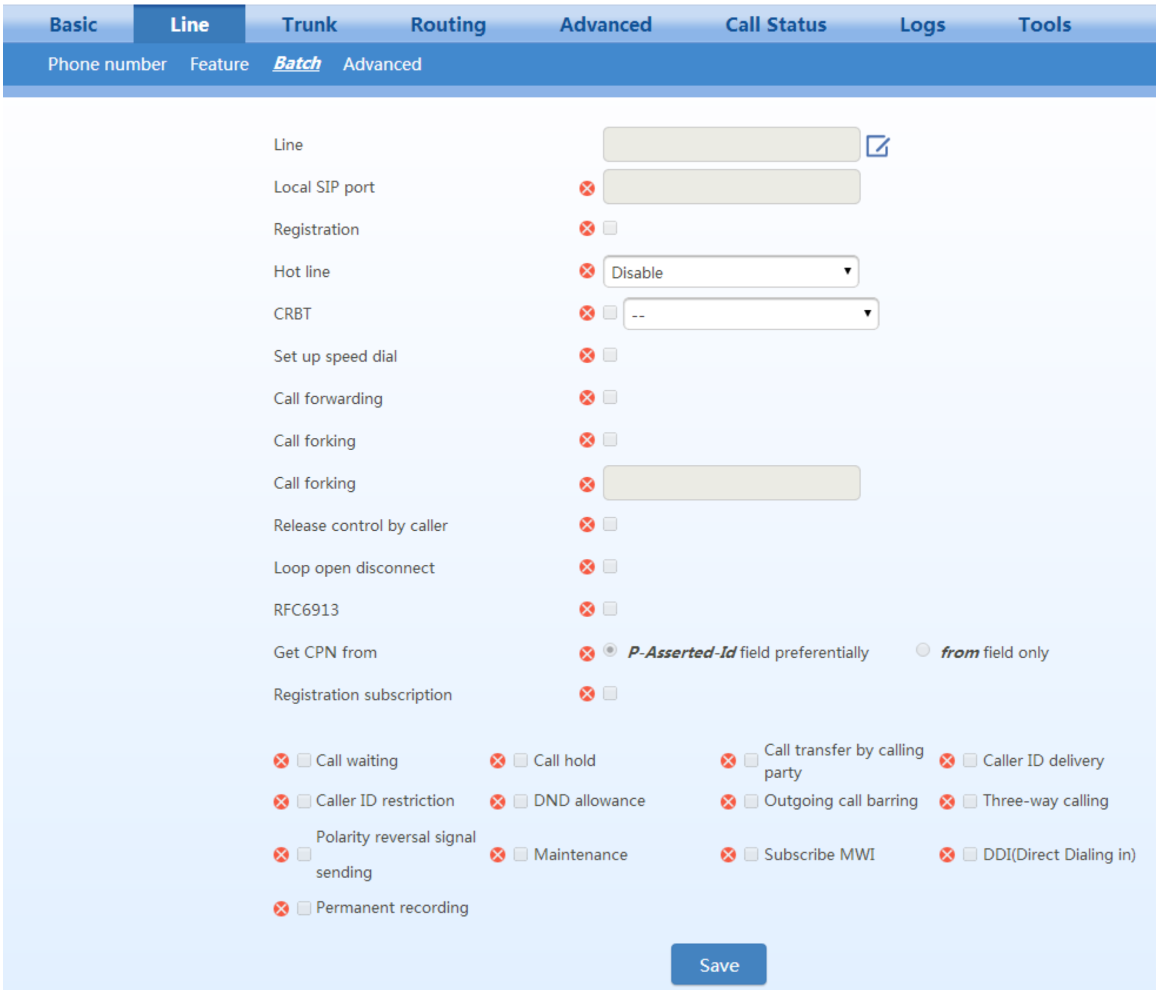
Only a gateway with FXS ports can display this interface.

After login, click **Line** > **Batch** tab to open the configuration interface.

Step 1 Click , the following interface is shown. Choose batch configured features and click **OK**.

Step 2 Click to activate this function to configure this parameter. For details of the parameter, see **Line** > **Feature**.

Figure 2-18 Feature Batch Configuration Interface



2.4.4 Subscriber Line Characteristics

Only a gateway with FXS ports can display this interface.

After login, click **Line** > **feature** tab to open the configuration interface.

Figure 2-19 Subscriber Line Characteristics Configuration Interface

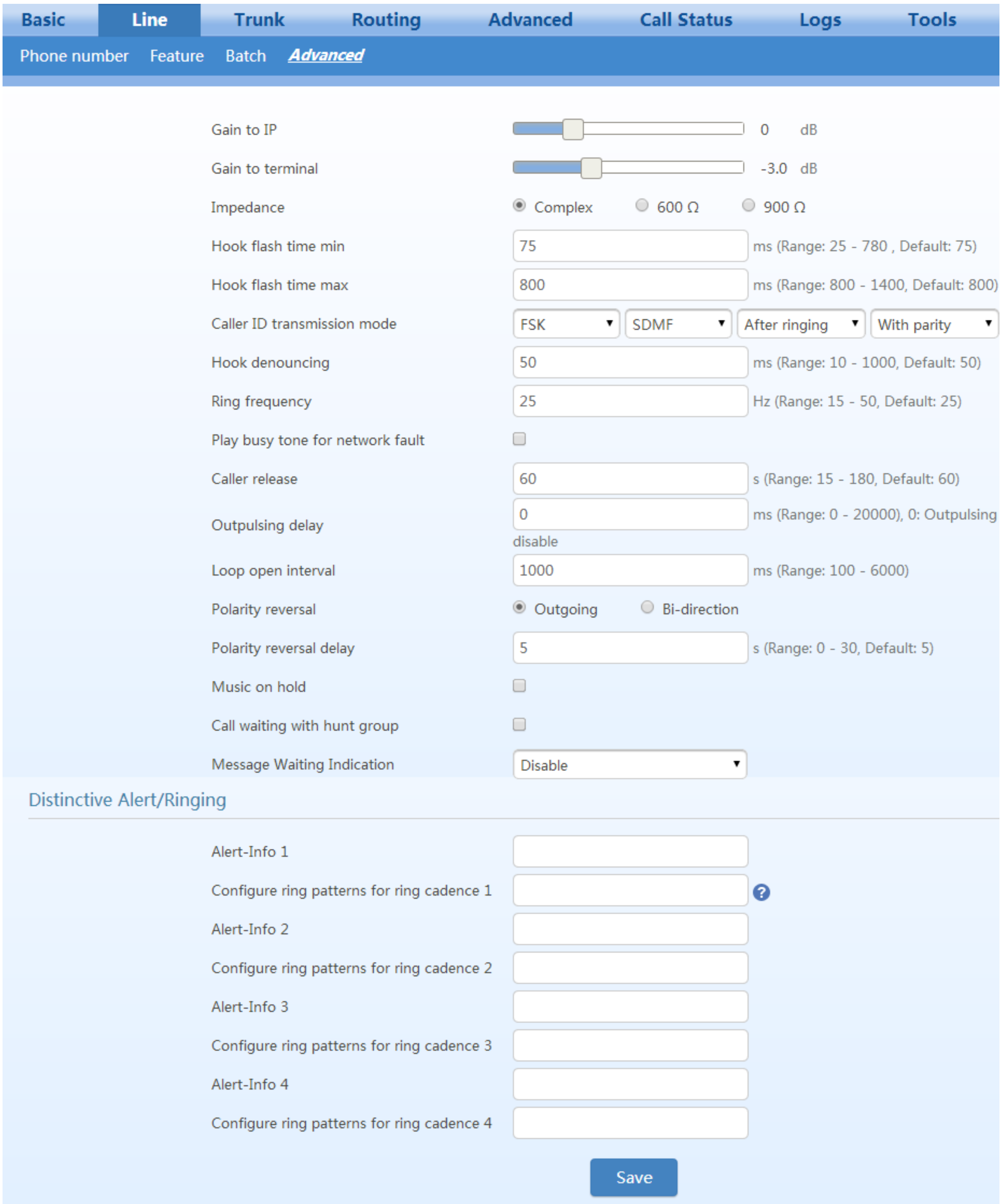


Table 2-13 Subscriber Line Characteristics Configuration Parameter

Name	Description
Gain to IP	Set the voice volume gain toward the IP side, the default is 0. Taking decibel as the unit, setting range is -3 ~ +3 decibels. -3 means declining of 3 decibels; +3 denotes the amplification of 3 decibels.
Gain to terminal	Set the voice volume gain toward FXS port side, the default is -3. Taking decibel as the unit, setting range is -6 ~ +3 decibels. -3 means declining of 3 decibels; +3 denotes the amplification of 3 decibels.

Name	Description
Impedance	Select the parameter of FXS port line impedance and the default value is 600 ohm. The optional values as below: • Complex (default value) • 600 (ohm) • 900 (ohm)
Hook flash time min	Used by the gateway to detect Hook Flash event, the default is 75 milliseconds. The gateway will ignore any flash that fall short of the shortest flash time. Generally, this value should not be less than 75 milliseconds.
Hook flash time max	Used by gateway to detect hook flash, the default is 800 milliseconds. The gateway will regard the flash duration between **Min.hookflash** and **Max.hookflash** as effective flash. Any flash lasting over the longest time will be considered by gateway as hang up. Generally, this value should not be less than 800 milliseconds.
Caller ID transmission mode	Select transmission mode of Caller ID signal from the FXS port to the phone. • FSK or DTMF • SDMF or MDMF • Sending Caller ID data before or after ringing • Sending Caller ID data with or without parity
Hook debouncing	Used by gateway to avoid a glitch of the phone status, with default of 50 milliseconds. When the duration from hang-up to off-hook falls short of this value, the gateway will ignore the status variation, and consider that the phone remains in hang-up status. In opposite case, the gateway will ignore the status variation, and consider the phone remains in off-hook status. Effective range of setting is 10~1000 milliseconds.
Ring frequency	Set the ringing frequency to be transmitted by gateway to the phone, ranging from 15 to 50 Hz, with default of 20 Hz.
Play busy tone for network fault	Play a busy tone upon off-hook when a network fault occurs.
Caller release	Set the delay release time of line as caller control method, with a default of 60 seconds. Effective range of setting is 15~180 seconds. This parameter is used in combination with the **Release control by caller** parameter in **Line** > **Feature**.
Outpulsing delay	Used when gateways' FXS port is connected with the trunk interface of PBXs. For calls from gateway to PBX, gateways will relay the extensions to PBX after the delay set here. Setting of 0 means no extension number relay. The default is **0** milliseconds.
Loop open interval	This parameter is used with the loop open disconnection request. The range is from 100 ms to 6000 ms.
Polarity reversal	Set the trigger for polarity reversal, the default is **Outgoing.** • **Outgoing**: transmit reverse polarity signal only when the outbound is connected; • **Bi-direction**: transmit reverse polarity signal for the connection of both inbound and out bound calls.
Polarity reversal delay	The delay time from a call being answered to the transmission of reverse polarity signal. The default value is 3 in seconds. Effective range of setting is 0 ~ 30 seconds.
Music on hold	Choose whether to play the background music while call waiting, and the default is not to play.
Call waiting with hunt group	Choose whether to activate hunt group feature for call waiting. Default not selected.

Name	Description
Message waiting indication (MWI)	Choose the lighting method of message waiting indicator of voice mail here: None, Polarity reversed, FSK, high voltage lighting. Message waiting indicator refers to the special LED on a phone, working with voice mail function. When user receives a voice message. The gateway will light this lamp upon receiving the notice from platform; the light goes off when there’s no unheard mail. It’s essential to understand whether the phone supports the indicators and lighting method when selecting the lighting method.
Distinctive Alert/Ringing	Set the parameter **Alert-Info *n*** according to the “Alert-Info” value provided on the SIP server. When the “Alert-info” value of received INVITE message matches with the **Alert-Info *n***, ring cadence *n* is activated.
Alert-Info 1	To match with ring cadence 1.
Configure ring patterns for ring cadence 1	Configure ring patterns for ring cadence 1. It is used with E.g 1: if the ring patterns are set to **2, 500, 500, 1000, 3000**, the ringing cadence is 0.5s on, 0.5s off; 1s on, 3s off. E.g 2: if the ring patterns are set to **2000, 4000,** the ringing cadence will be 2s on, 4s off.
Alert-Info 2	To match with ring cadence 2.
Configure ring patterns for ring cadence 2.	Configure ring patterns for ring cadence 2. It is used with **Alert-Info 2**.
Alert-Info 3	To match with ring cadence 3.
Configure ring patterns for ring cadence 3	Configure ring patterns for ring cadence 3
Alert-Info 4	To match with ring cadence 4.
Configure ring patterns for ring cadence 4	Configure ring patterns for ring cadence 4. It is used with **Alert-Info 4**.

2.5 Trunk

2.5.1 Phone Number

Only a gateway with FXO ports can display this interface.

After login, click **Trunk > Phone number** tab to open the configuration interface.

Figure 2-20 Phone Number Configuration Interface

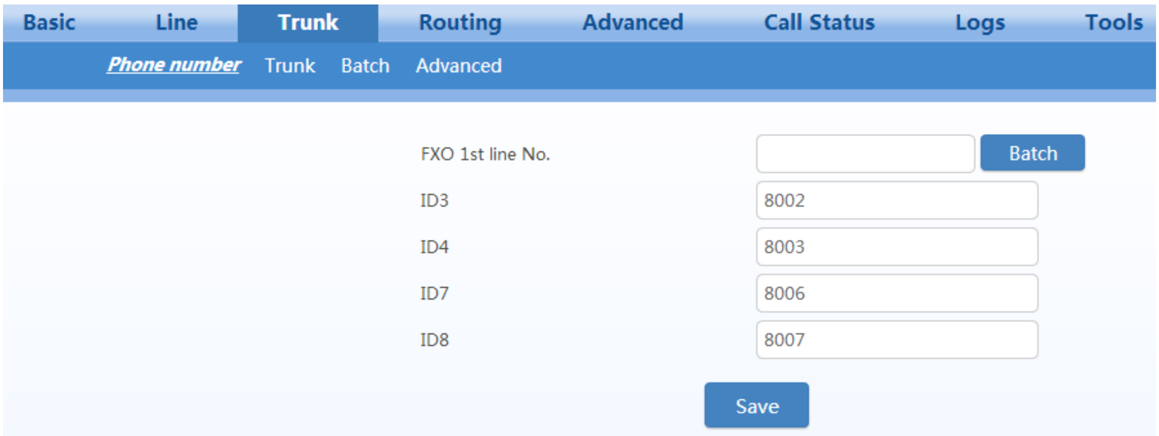


Table 2-14 Configuration Parameters of FXO Phone Number

Name	Description
FXO 1st line No.	This number is used for the fast setup of consecutive number of trunk line. Click **Batch** after filling in initial number, the number of Line 1 adopts initial number; that of Line 2 increases 1 progressively based on that of Line 1, and so on. You needn't fill in if you do not use batch configuration or the number is not consecutive.
ID n	Fill in the telephone number associated with the trunk n (FXO port). This should be manually performed if Batch mode is not used.

2.5.2 Trunk Features

Only a gateway with FXO ports can display this interface.

After login, click **Trunk** > **Trunk** tab to open the configuration interface.

Figure 2-21 Trunk Line Features Configuration Interface

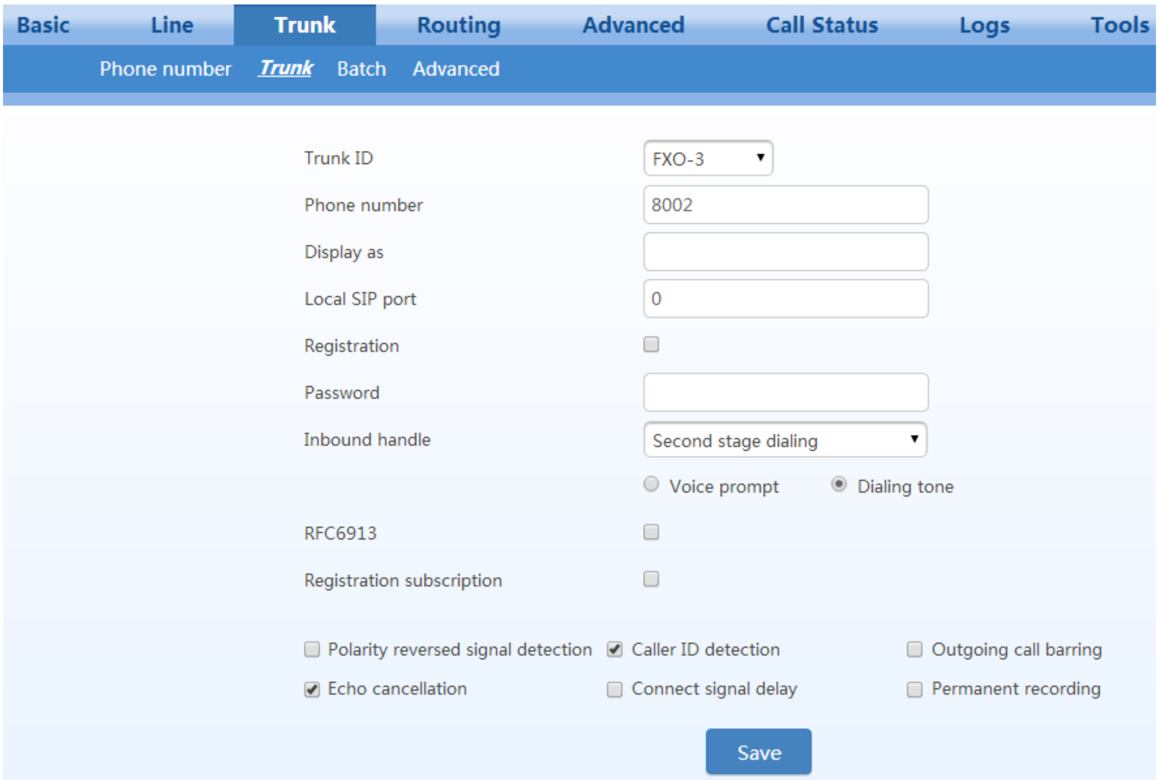


Table 2-15 Configuration Parameters of Trunk Features

Name	Description
Trunk ID	Select a trunk line required to configure. “FXO-n” corresponds to the **Trunk** > **Phone number** > **ID n**.
Phone number	Display phone number associated with the trunk set in **Trunk** > **Phone number**
Local SIP port	Set the port used for receiving and sending SIP messages on the line. If this parameter is not specified, the local port configured in **Basic** > **SIP** is used. This parameter is displayed only when **multi port** is selected in page **Advanced** > **SIP**.
Registration	Select if this trunk registers with the SIP registration server. By default, this is not selected.
Password	If **Registration** is selected, the authentication password for register of this line must be entered here.

Name	Description
Note: The following features are valid only in SIP protocol. When the gateways use MGCP protocol, the control of all call services is provided by the proxy server without the need of these setting.	
Inbound handle	The gateways provide three scenarios for handling incoming calls on the FXO trunk: • **Binding:** when a telephone call comes to the FXO port, the gateways will route the call to a FXS port according to the DID number bound with the port. Note: Setting a number to be bound is required or this setting is invalid. Note: Setting a number to be bound is required or this setting is invalid. • **Second-stage dialing**: when a telephone call comes to the Line port, the gateways will provide the second dial tone and route the call according to the extension number entered. Dialing tone or voice prompt file can be changed by user. • **Direct**: the gateways will route the incoming call on FXO port n to FXS port n.FXO ports map to FXS ports. For example, a call made to the first FXO port is forwarded to the first FXS port. Note: **Direct** applies only to a device having both FXO and FXS ports.
RFC6913	If this item is selected, the Fax over IP label carried in INVITE is supported.
Registration subscription	The device periodically sends subscription messages to the SIP server. The period of sending the subscription messages is the same as the **Registration expiration** in **Basic** > **SIP**.
Polarity reversal signal detection	If a PSTN line supports reverse polarity, make the selection here. Or this setting is invalid. By default, this is not selected.
Caller ID detection	Select to enable the detection function of caller ID for this FXO port. By default, this is not selected.
Outgoing call barring	Select if this FXO port bars outgoing call service to the PSTN. By default, this is not selected.
Echo cancellation	Select if echo cancellation is enabled for this FXO (Line).By default, this is selected.
Connect signal delay	After making an outgoing call from a FXO port, the gateway will send a 200 OK message to the platform with a delay if this parameter is selected. If unselected, the system sends a 200 OK message to the platform after off hook on the FXO port. Also see **Answer delay** on page **Trunk** > **Advanced**.
Permanent recording	Select if recording service is activated, and by default this is not selected.

2.5.3 Trunk Batch (Unavailable in the HX4E)

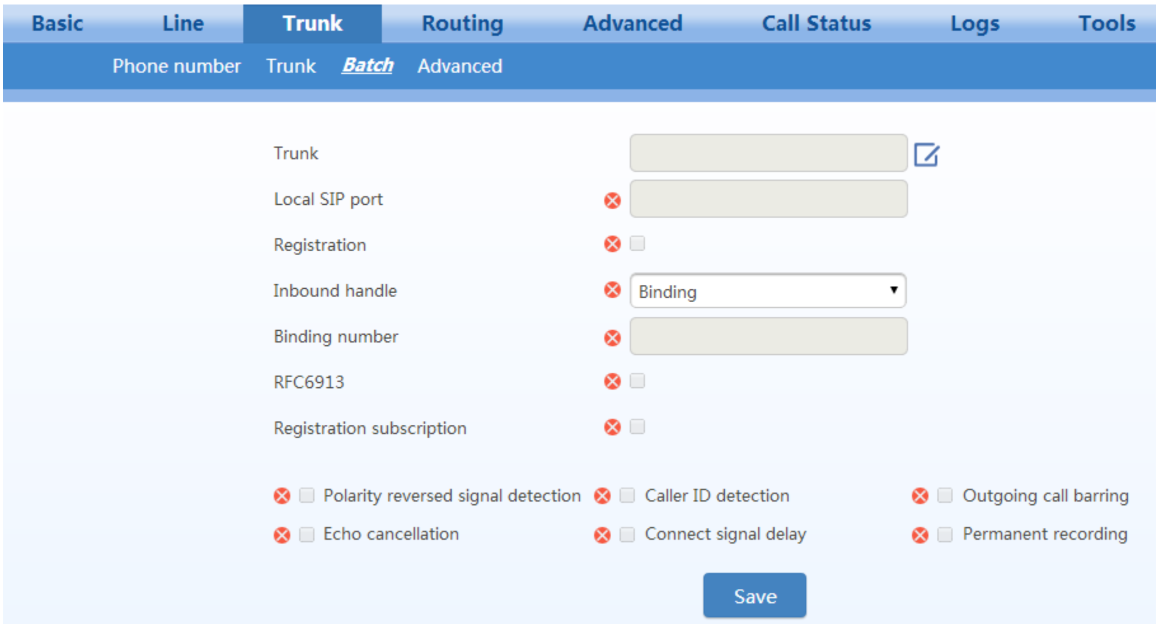
Only a gateway with FXO ports can display this interface.

After login, click **Trunk** > **Batch** to open the configuration interface.

Step 1 Click , the following interface is shown. Choose batch configured trunks and click **OK**.

Step 2 Click to activate this function to configure this parameter. For details of the parameter, see **Trunk > Feature**.

Figure 2-22 Trunk Batch Configuration Interface



2.5.4 Trunk Characteristics

Only a gateway with FXO ports can display this interface.

After login, click **Trunk** > **Advanced** tab to open the configuration interface.

Figure 2-23 Trunk Characteristics Configuration Interface

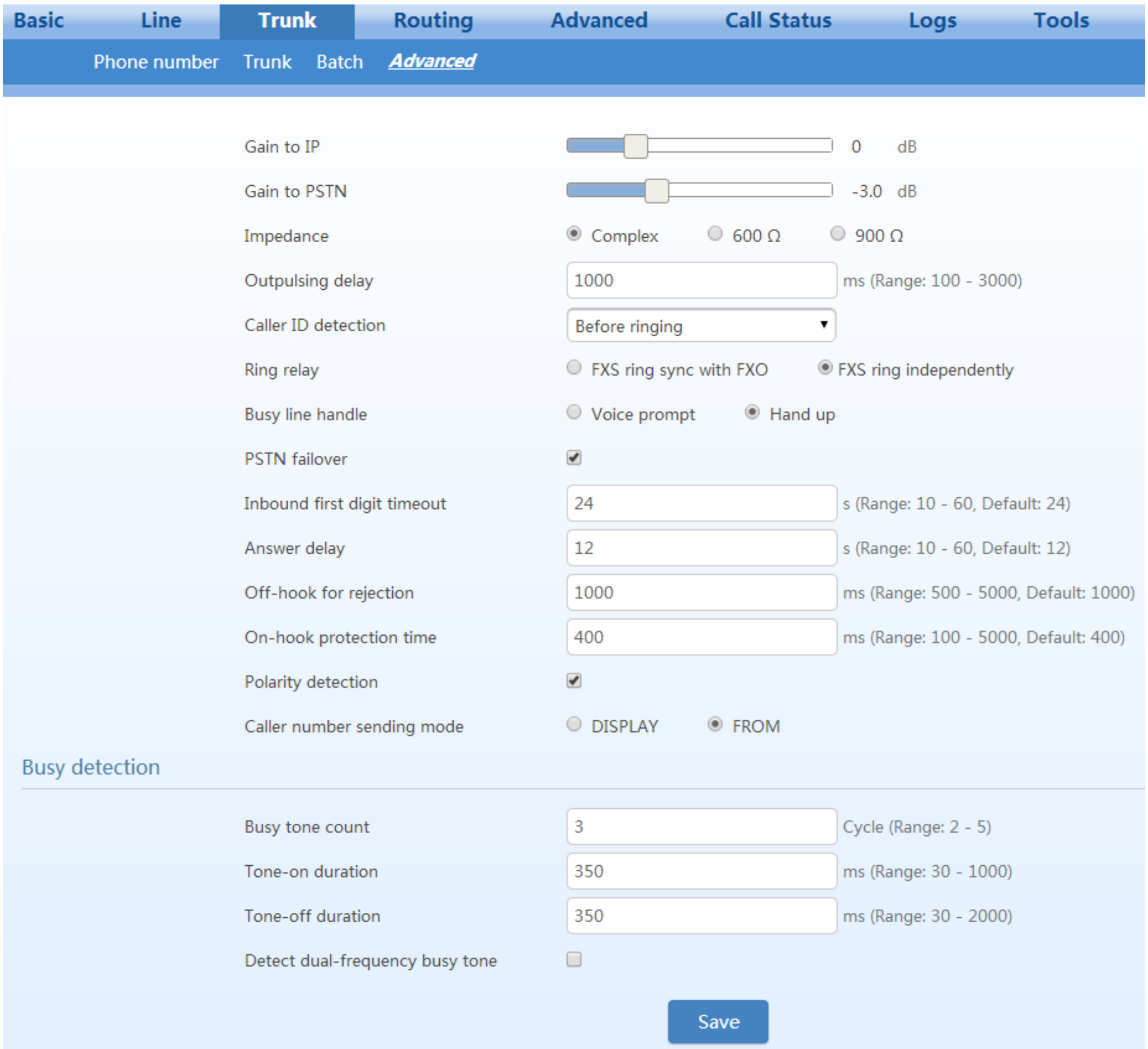


Table 2-16 Trunk Characteristics Configuration Parameter

Name	Description
Gain to IP	This parameter is used to adjust the volume of the voice sent from the PSTN to the device. When the call volume of the extension set is extremely low, you can increase the parameter value. When the call volume of the extension set is excessively high, you can decrease the parameter value. Range: -3.0 - +9.0 dB. It is set to 0 dB by default.
Gain to PSTN	This parameter is used to adjust the volume of the voice sent from the device to the PSTN. When the sound volume is extremely low, you can increase the parameter value. When the call volume of the extension set is excessively high, you can decrease the parameter value. Range: -6.0 - +3.0 dB.
Impedance	Set the parameter of FXO impedance, with the default of 600 ohm. The optional settings are below: • Complex (default value) • 600 (ohm) • 900 (ohm)

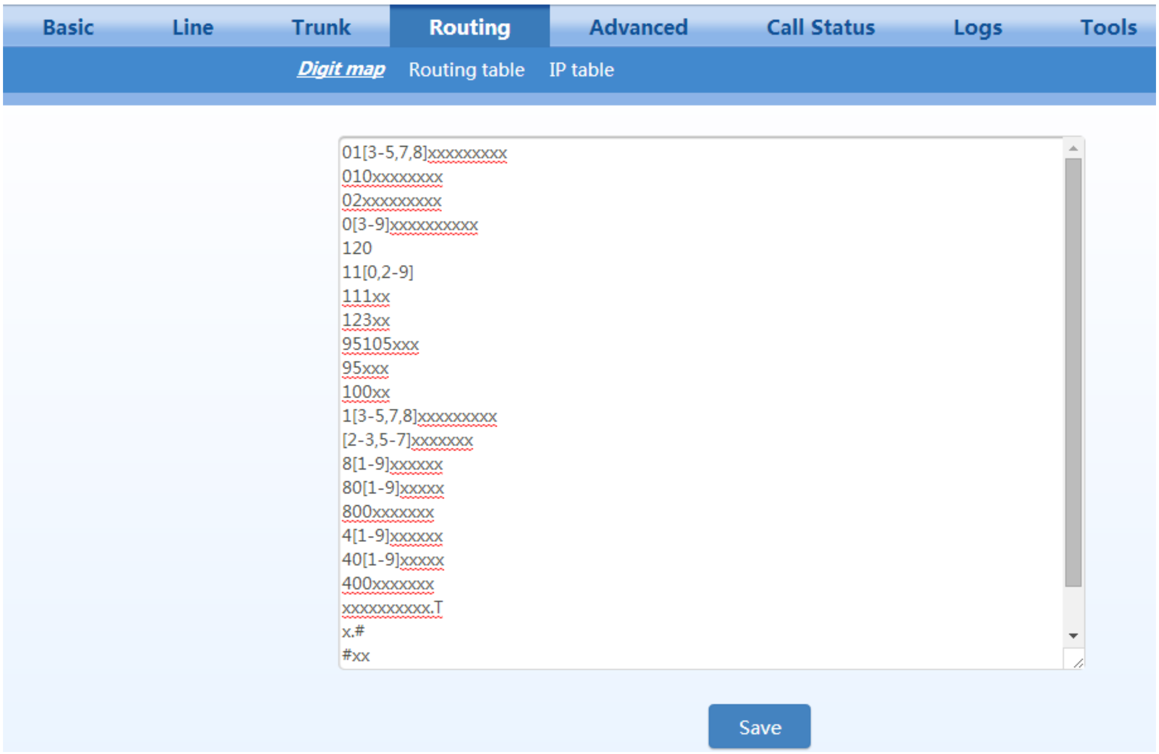
Name	Description
Outpulsing delay	Set the time interval between the FXO going off-hook and start for outpulsing of the first digit to the PSTN. The default is 600 in milliseconds. Note: This parameter is used to match the digit receiving response time of the PSTN PBX.
CallerID detection	Before ringing; After ringing. The **After ringing** mode is generally used.
Ring relay	Whether to relay the ring of inbound call to the FXS port when applying to DID. The default is **Phone ring independently**.
Busy line handle	Either a voice prompt or hanging up can be applied to FXO port when an incoming call goes to the FXS port which is in busy. This only applies to DID feature.
PSTN failover	Whether to route a call to the PSTN through an FXO port when the IP network faults or no response to the call request. Default selected.
Inbound first digit timeout	Set the timeout of calling DTMF on FXO port for inbound calls, ranging from 10-60 seconds, with default of 24 seconds.
Answer delay	Set the delay time for sending 200 OK. It rangs from 10-60 seconds, with default of 12 seconds. This parameter is used in combination with the **Connect signal delay** in **Trunk** > **Trunk** page. See Table 2-15.
Off-hook for rejection	This parameter is used to specify how to reject an incoming call in the **Direct** mode (see Table 2-15) for the FXO port. For inbound calls to an FXO port, if the associated FXS port is busy, the gateway will hang up after off hook according to the time set by the parameter, so as to refuse the upcoming call. The duration of the off hook is 500~5000 milliseconds, with a default of 600 milliseconds
On-hook protection time	Protection period following hang up of FXO port. During this period, gateway ignores any voltage variation of line. Value range is 100~5000 milliseconds, the default is 400 in milliseconds.
Polarity detection.	Choose whether to activate the detection of reverse polarity signal of FXO port. Note the detection will work only when the trunk supports polarity reversal.
Caller number sending mode	• **DISPLAY**: includes the incoming call number detected at the FXO port in the Display field and sends it to the peer end. The From field carries the phone number associated with the FXO port. • **FROM**: includes the incoming call number detected by FXO in the From field and sends it to the peer end. No Display information is carried.
Busy detection	
Busy tone count	Set the number of consecutive repeat times the gateway detects busy tone signals. Gateways will regard the busy tone signal with the repeat times specified here as a hang-up signal. Default is 2, effective range is 2 ~ 5(cycle).
Tone-on duration	Set duration of busy tone signal, the default is 350 in milliseconds.
Tone-off duration	Set the interval time of busy tone, the default is 350 in milliseconds.
Detect dual-frequency busy tones	To detect dual-frequency busy tones.
Busy tone frequency	If **Detect dual-frequency busy tones** is enabled, you need to specify the frequency to be detected. Unit: Hz.

2.6 Routing

2.6.1 Digit Map

After login, click **Routing** > **Digit Map** tab to open the dialing rules interface.

Figure 2-24 Configuration Interface for Digit map



Dialing rules are used to effectively judge if the received number sequence is completed for terminating receiving numbers and sending received numbers. The proper use of dialing rules can help to reduce the connection time of telephone calls.

The maximum number of rules that can be stored in gateways is 250. Each rule can hold up to 32 numbers and 38 characters. The total length of dialing rules table (the total length of all dialing rules) can be up to 2280 bytes.

The default digit map only contains system function rules. If you want set your own digit map, please choose the country in **Advanced** > **Tones** and input the rules you want to the text box. The following provides descriptions of typical rules:

Table 2-17 Description of Digit Map

Digit map	Description
x	Represents one digit between 0-9.
.	Represents more than one digit between 0-9.
##	After ## is detected, the gateway terminates the process of receiving digits. ## is a special dial string for users to receive gateway IP address and version number of firmware by default.

Digit map	Description
x.T	The gateways will detect any length of telephone number starting with any number between 0-9. The gateway terminates the process of receiving digits and sends detected numbers if the duration of no dialing period exceeded the value of the **Complete entry timer** parameter (in **Basic** > **System**. See Table 2-5).
x.#	If subscribers press # key after dial-up, the gateways will immediately terminate receiving digits and send all the numbers before # key.
*xx	Terminate after receiving * and any two-digit number. *xx is primarily used to activate function keys for supplementary services, such as CRBT, Call Transfer, Do not Disturb, etc.
#xx	Terminate after receiving * and any two-digit number. #xx is primarily used to stop function keys for supplementary services, such as CRBT, Call Transfer, Do not Disturb, etc.
[2-3,5-7]xxxxxxx	The gateway terminates receiving digits after receiving eight digits starting with any digits except 1, 4, or 9.
02xxxxxxxxx	The gateway terminates receiving digits after receiving 11 digits starting with 2.
013xxxxxxxxx	The gateway terminates receiving digits after receiving 12 digits starting with 013.
13xxxxxxxxx	The gateway terminates receiving digits after receiving 11 digits starting with 13.
11x	The gateway terminates receiving digits after receiving three digits starting with 11.
9xxxx	The gateway terminates receiving digits after receiving five digits starting with 9.
17911 (e.g.)	Send away when the set number, like 17911, is received.

Dial rules by default as follows:

01[3-5,7,8]xxxxxxxxx

010xxxxxxxx

02xxxxxxxxx

0[3-9]xxxxxxxxxx

120

11[0,2-9]

111xx

123xx

95105xxx

95xxx

100xx

1[3-5,7,8]xxxxxxxxx

[2-3,5-7]xxxxxxx

8[1-9]xxxxxx

80[1-9]xxxxx

800xxxxxxx

4[1-9]xxxxxx

40[1-9]xxxxx

400xxxxxxx

xxxxxxxxxx.T

x.#

#xx

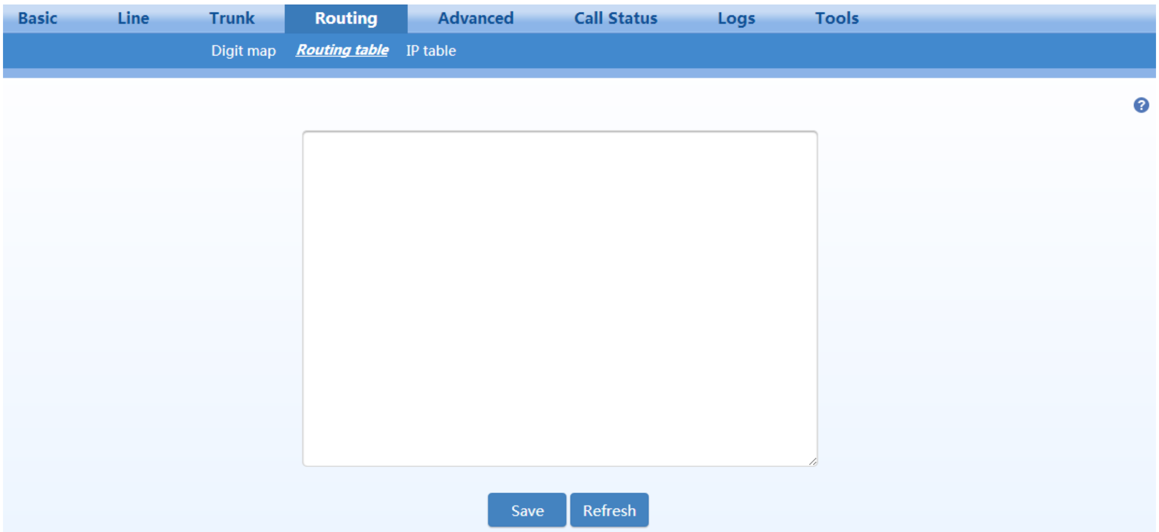
*xx

##

2.6.2 Routing Table

After login, click **Routing** > **Routing Table** tab to open the configuration interface.

Figure 2-25 Routing Table Configuration Interface



Click  to open the illustrative interface for routing configuration.

The routing table with a capacity of 500 rules provides two functions including number transformation and call routing assignment.

The device will match a rule from top to bottom. Shortest matching rule is performed for number.

Note

- Rules must be filled out without any blank at the beginning of each line; otherwise the data can't be validated even if the system prompts successful submittal.
- The routing table is empty by default. The gateways will point a call to the SIP proxy server when there is no matched rule for the call.

The format of number transformation is

Source Number Transformation Method

Take **FXS 021 REMOVE 3** as an example. It indicates that, for a call from the FXS port (on a subscriber line), the first three digits area code 021 is removed from the called number.
Where FXS is source, 021 is number, and REMOVE 3 indicates the method of number transformation.

The format of routing rules is

Source Number ROUTE Routing Destination

Take **IP 800[0-1] ROUTE FXO 1-2** as an example. It means that calls from IP with called number prefix 8000 or 8001 are routed to FXO port in a sequential order. Namely, FXO Port 2 is selected when FXO Port 1 is busy and so on.

For details of **Source** and **Number**, see Table 2-18.
For details of **Number Transformation** and **Routing Destination**, see Table 2-19 and Table 2-20 respectively.

Table 2-18 Routing Table Format

Name	Description
Source	There are three types of source: IP, FXS (Phone/fax) and FXO (Line). The IP indicates any IP addresses. IP [xxx.xxx.xxx.xxx] indicates a specific address. IP [xxx.xxx.xxx.xxx:port] indicates an specific IP address and a specific port number. The FXS or FXO indicates any FXS or FXO port. FXS1, FXO2, FXS [1-2], or similar indicates a specific port.
Number	a called party number with the form of number. It could be a calling party number with the form of CPN + number The number may be denoted with digit 0-9,"*",".","#"," x ", etc., and uses the same regular expression as that of dialing rules. Here are examples of the form of number: Designate a specific number: eg.114, or 61202700 Designate a number matching a prefix: such as 61xxxxxx. Specify a number scope. For example, **268[0-1, 3-9]** specifies any 4-digit number starting with 268 and followed by a digit between 0-1or 3-9 Number matching follows the principle of minimum matching. For example: x matches any number with at least one digit; xx matches any number with at least two-digit; 12x matches any number with at least 3-digit starting with 12.

Table 2-19 Number Transformations

Processing Mode	Description and Example
KEEP	Keep number. A positive number behind KEEP means to keep several digits in front of the number; a negative number means to keep several digits at the end of the number. Example: FXS 02161202700 KEEP -8 Keep the last 8 digits of the called number 02161202700 for calls from FXS. The transformed called number is 61202700.
REMOVE	Remove number. A positive number following REMOVE means to remove the first several digits of the number; a negative number means to remove the latter several digits of the number. For example: FXS 021 REMOVE 3 Remove 021 of the called number beginning with 021 for calls from FXS.
ADD	Add prefix or suffix to number. A positive number behind ADD is the prefix; a negative number is suffix. Example 1: FXS1 CPNX ADD 021 FXS2 CPNX ADD 010 Add 021 in front of calling numbers for calls from FXS port 1; add 010 in front of calling numbers for calls from FXS port 2. Example 2: FXS CPN6120 ADD -8888 Add 8888 at the end of the calling number starting with 6120 for calls from an FXS (Phone/fax) port.
REPLACE	Number replacement. The replaced number follows REPLACE. Example: FXS CPN88 REPLACE 2682000 Replace the calling number beginning with 88 for calls from FXS port with 2682000.

Processing Mode	Description and Example
REPLACE	Another use of REPLACE is to replace the specific number based on another number associated with the call. For example, replace the calling number according to the called number. Examples: FXS 12345 REPLACE CPN-1/8621 FXS CPN13 REPLACE CDPN0/0 For calls from FXS ports with called party number of 1234, remove one digit at the end of the calling number and add 8621; for calls from FXS ports with calling party number starting with 13, add 0 at the beginning of the called number.
END or ROUTE	End-of-number transformation. From top to bottom, number transformation will be stopped when END or ROUTE is encountered; the gateways will route the call to the default routing upon detecting END, or route the call to the designed routing after detecting ROUTE. Example 1: FXS 12345 ADD -8001 FXS 12345 REMOVE 4 FXS 12345 END Add suffix 8001 to the called number starting with 12345 for calls from FXS ports, then remove four digits in front of the number to end number transformation yielding 58001. Example 2: IP [222.34.55.1] CPNX. REPLACE 2680000 IP [222.34.55.1] CPNX. ROUTE FXS 2 For calls from IP address 222.34.55.1, calling party number is replaced by 2680000, and then the call is routed to FXS port 2 with the new calling party number.
CODEC	Designate the use of a codec, such as PCMU/20/16, where PCMU denotes G.711, /20 denotes RTP packet interval of 20 milliseconds, and /16 denotes echo cancellation with 16 milliseconds window. PCMU/20/0 should be used if echo cancellation is not required to activate. Example: IP 6120 CODEC PCMU/20/16 PCMU/20/16 codec will be applied to calls from IP with called party number starting with 6120.
RELAY	Insert prefix of called party number when calling out. The inserted prefix number follows behind RELAY. Example: IP 010 RELAY 17909 For calls from IP with called party number starting with 010, digit stream 17909 will be outpulsed before the original called party number is sent out. Example: IP 010 RELAY 17909 ,,, For a call from the IP end with the called number starting with 010, before the call is made, 17909 is automatically dialed first and three seconds later, the called number is dialed. One comma "," represents one second.

Table 2-20 Routing Destination

Destination	Description and Example
ROUTE NONE	Calling barring (also known as "blacklist") . Example: IP CPN[1,3-5] ROUTE NONE Bar all calls from IP, of which the calling numbers start with 1, 3, 4, and 5.
ROUTE FXS	Route a call to FXS ports. Example 1: IP 800[0-3] ROUTE FXS 1-2 Select a port in sequential order. Example 2: IP 800[0-3] ROUTE FXS 1 Point this call to FXS port 1. Example 3: IP 800[0-3] ROUTE FXS 1-2/R Select a port in round robin order Example 4: IP 800[0-3] ROUTE FXS 1-2/G Select all idle ports and provide ringing.
ROUTE FXO	Route a call to FXO port. Example 1: IP x ROUTE FXO 1-2 Select a port in sequential order. Example 2: IP 800[0-1] ROUTE FXO 1-2/R Select a port in round robin order.
ROUTE IP	Route a call to the SIP proxy server Example: FXS 021 ROUTE IP 228.167.22.34:5060 228.167.22.34:5060 is the IP address and port of the platform.

2.6.3 Examples of Routing Rules

This section provides examples of how routing table can be used to implement features.

1) Assigning One Phone with Dual Numbers
2) Hunt Group
3) Outbound Call Barring
4) Trunk Group for Outbound Calling

Assigning One Phone with Dual Numbers

An analog extension of an FXS port, FXS1 for example, of HX4E can be associated with two phone numbers, a PSTN number 61202701 and an extension number 1001for example. The PSTN number is used for direct inward dialing and the extension number is used for intercom. This feature can be supported by configuring the FXS1 number as 61202701 and adding the following routing rule to the routing table:

FXS 1001 ROUTE FXS 1

Hunt Group

A hunt group is a group of extensions, to which an inbound call is terminated following certain rules. Here is an example of how to terminate incoming calls from analog trunks to a hunt group consisting of ports FXS1 and FXS2 in round-robin fashion:

FXO x ROUTE FXS 1-2/R

Outbound Call Barring

Restrict users to from dialing certain telephone numbers, such as an international call. Examples are as follows:

Routing Setting	Description
FXS[1] 0 ROUTE NONE	A calling starting with 0 is barred from dialing using the phone set at FXS1 port
FXS[1-2] 00 ROUTE NONE	A calling starting with 00 is barred from dialing using the phone set at FXS1 to FXS2 port. International call is not allowed.
FXS CPN2 ROUTE NONE	The telephone whose calling number starts with 2 at a FXS port is barred to call out.

Trunk Group for Outbound Calls

An outbound trunk group consists of a set of trunks which are used for outbound calling following certain rules. Here is an example of routing all outbound calls from analog extensions to the trunk group consisting of ports FXO1 to FXO4 in sequential fashion:

FXS x ROUTE FXO 1-4

Further, we set up the trunk group such that it is used only by calls to destinations with prefix 6120:

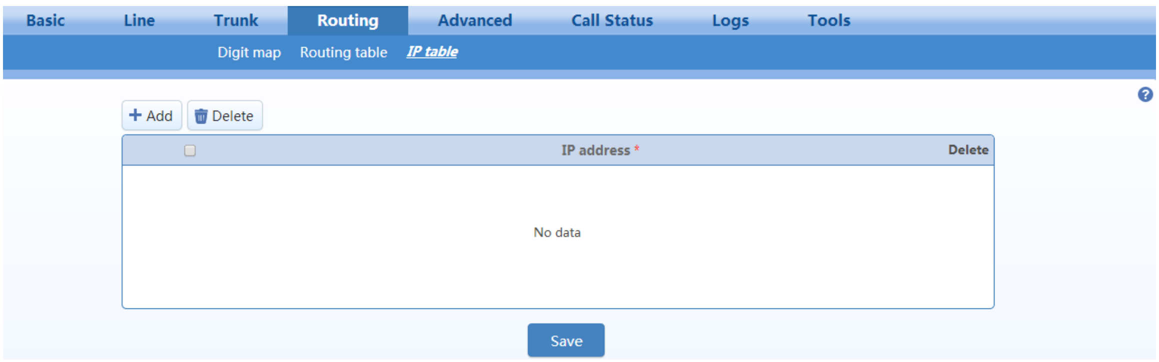
FXS 6120 ROUTE FXO 1-4

2.6.4 IP Table

The IP filtering function is used to ignore the VoIP messages from untrusted network.

After login, click **Routing** > **IP Table** tab to open the configuration interface.

Figure 2-26 IP Table Configuration Interface



Add the authorized IP addresses to this table, and the gateways will only process the VoIP signaling from authorized IP addresses. If the IP table is empty, the gateways will not perform IP address-based message filtering.

Note

If the gateway is deployed in a public network, you are advised to set IP filtering to prevent call theft.

2.7 Advanced Configuration

2.7.1 System

After login, click the label of **Advanced** > **System** to open this interface.

Figure 2-27 Interface of system advanced configuration

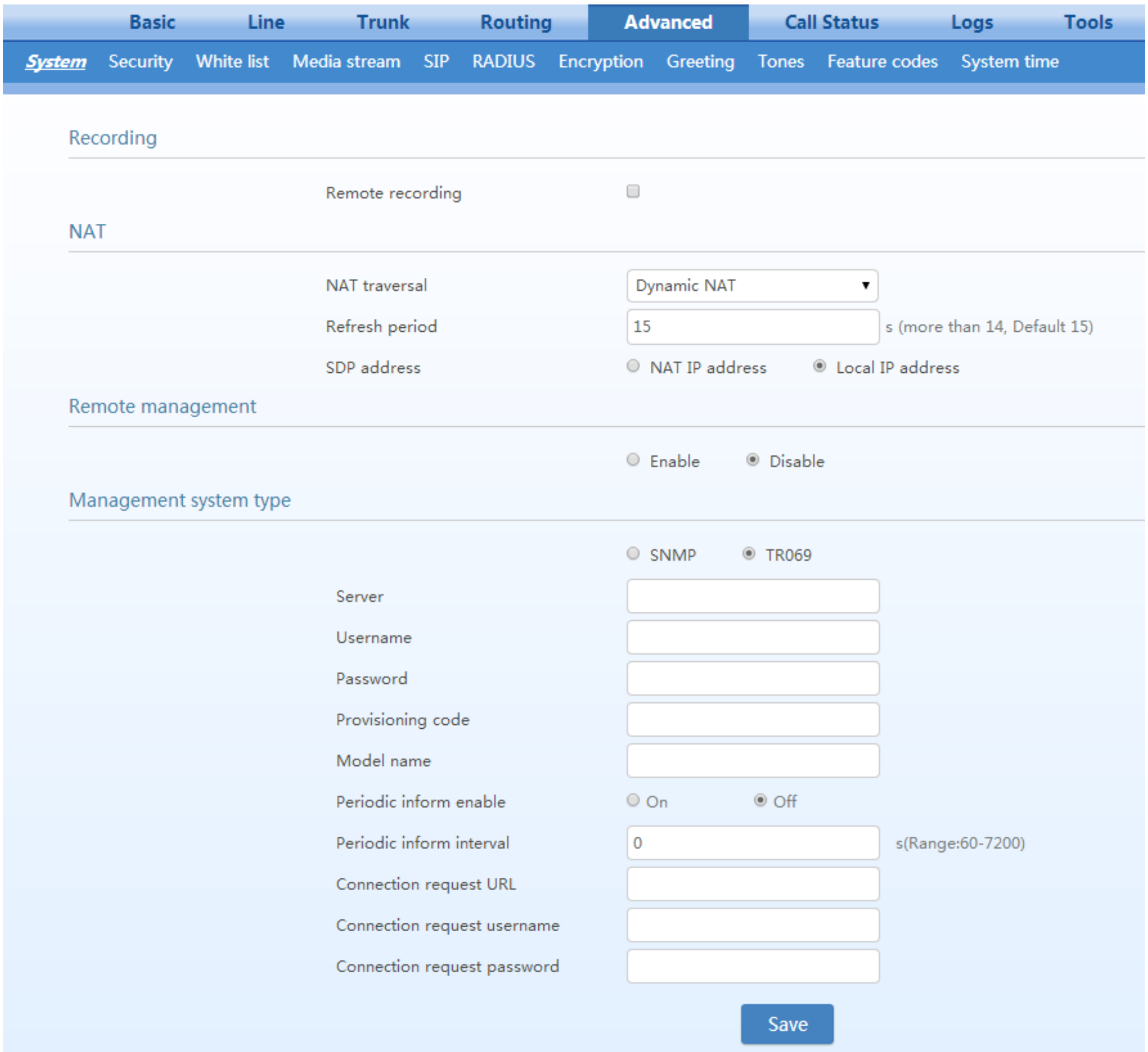


Table 2-21 NAT Configuration Parameters

Name	Description
Remote recording	Call recordings are stored on an external Windows or Linux based recording server, on which the agent provided by New Rock collects and stores the call recording files. For more information, see the Recording Agent User Guide in *http://www.newrocktech.com/ViewProduct_E.asp?id=64*. Set this parameter to the IP address of the server. Note: The recording function needs to be enabled for the subscriber line.
NAT traversal	Gateways support several mechanisms for NAT traversal. Usually, static NAT is used when a fixed public IP address is available. It's necessary to perform port mapping or DMZ function on router when choosing dynamic or static NAT.

Name	Description
Refresh period	The refresh time must be filled in here when choosing dynamic NAT or STUN traversal. Refresh time interval shall be determined by giving consideration to the NAT refresh time of the LAN router where the gateway is located. Gateway's NAT holding function and STUN function will carry out periodic operation according to this parameter. With seconds as its unit, default value of 60 seconds.
SDP Address	• **NAT IP Address**: apply NAT public address into the transmitted SDP; • **Local IP Address**: apply the gateway's IP address into the transmitted SDP. Note: The parameter **NAT IP Address** should come into effect only on condition that gateway successfully obtained NAT public address.

2.7.2 Auto Provision

After login, click the label of **Advanced** > **System** to open this interface.

For specific configurations, see: http://website.newrocktech.com/Files/MX%20Gateway%20Auto%20Provisioning%20Configuration%20Manual.pdf.

Figure 2-28 Interface of system advanced configuration (Remote management)

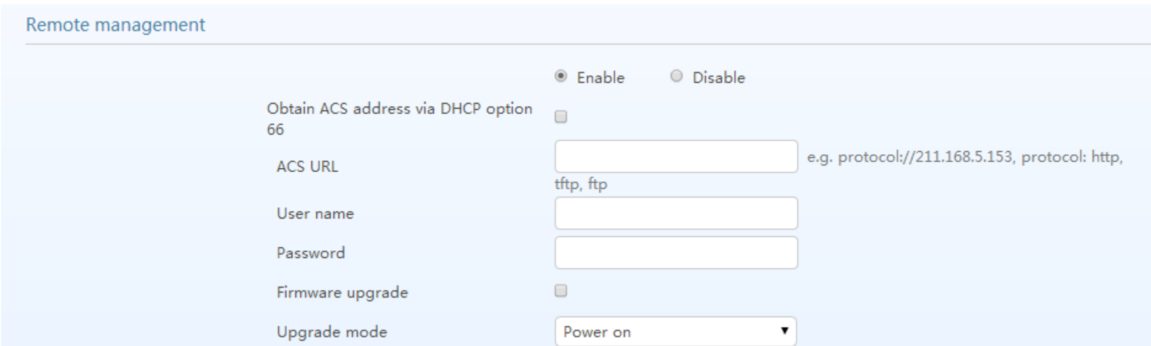


Table 2-22 Remote Management Configuration Parameters

Name	Description
Remote management	This parameter specifies whether to enable or disable auto provisioning.
Obtain ACS address via DHCP option 66	ACS (Auto Provisioning Server) address is obtained by using option 66 of the DHCP.
ACS URL	Manually configure the ACS address, which can be the TFTP, FTP, or HTTP server. • tftp://ACS address • ftp:// ACS address • http://ACS address
User name	Input a user name for accessing the ACS.
Password	Input a password for accessing the ACS.
Firmware upgrade	Supports firmware download and update using ACS.

Name	Description
Update mode	The following modes are available. • **Power on**: the gateway detects whether there are configurations and firmware to be updated when the device is powered on. • **Power on + Periodical**: when the device is powered on, the gateway first checks whether there are configurations and firmware to be updated, and then periodically performs checking based on the set times.
Upgrade period	When **Power on+Periodical** is set, this parameter specifies the interval for periodic automatic upgrades. The default is 3600 seconds.

2.7.3 Management System Type

After login, click the label of **Advanced** > **System** to open this interface.

Figure 2-29 SNMP configuration interface

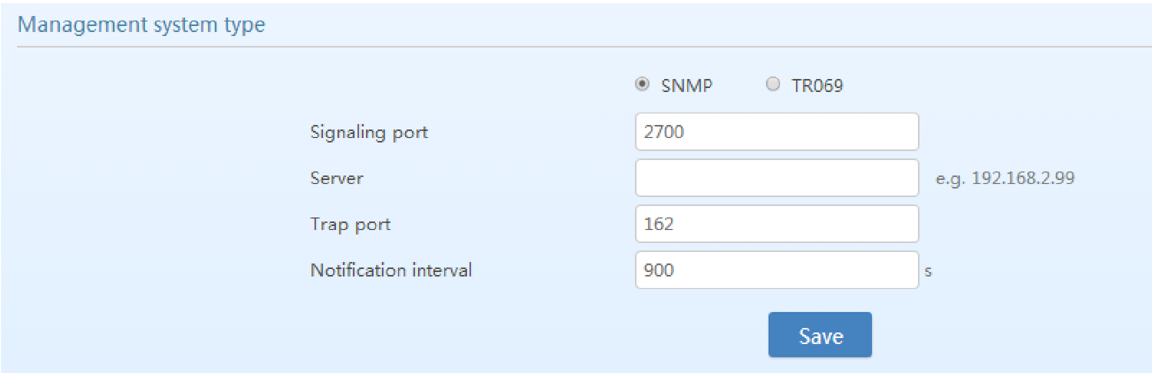


Table 2-23 SNMP Configuration Parameters

Name	Description
Signaling port	Enter the SNMP local port. The default value is 2700. If **SNMP** is selected, the following three parameters need to be specified.
Server	Enter the address of the SNMP server.
Trap port	Enter the port number of the SNMP server. The default value is 162.
Notification interval	The default value is 900 seconds. The default value is 900 seconds.

Figure 2-30 TR069 configuration interface

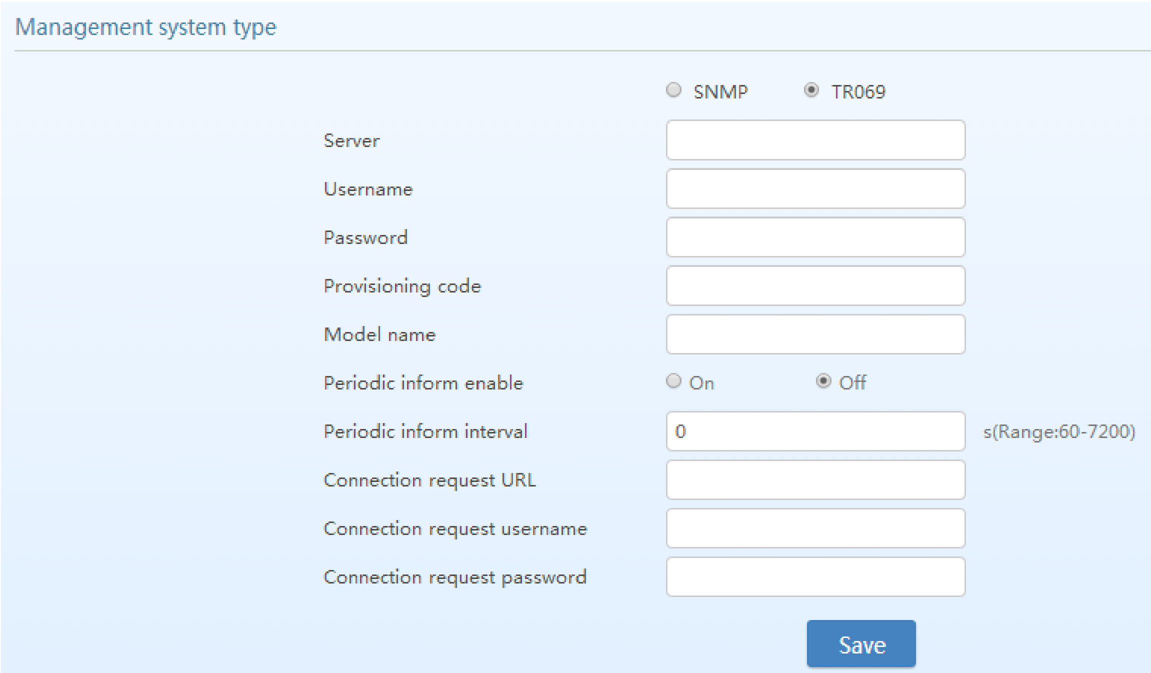


Table 2-24 TR069 Configuration Parameters

Name	Description
Server	Specify the URL of the ACS.
User name	Specify the user name to be used by the device to authenticate with the ACS.
Password	Specify the password to be used by the device to authenticate with the file server
Provisioning code	Information of the device vendor, which may be used to indicate the primary service provider and other provisioning information to the ACS. It can be numbers or English letters.
Model name	A brief description of the interface type or name. It is a string of characters.
Periodic inform enable	A switch used to specify whether to periodically report to the ACS.
Periodic inform interval	The interval for reporting to the ACS.
Connection request URL	The address used for the ACS to connect back to the device.
Connection request username	The account used for the ACS to connect back to the device, for example, admin.
Connection request password	The password used for the network management server to connect back to the device.

2.7.4 Security Configuration

After login, choose **Advanced** > **Security** to open the security configuration interface.

Figure 2-31 Security configuration interface

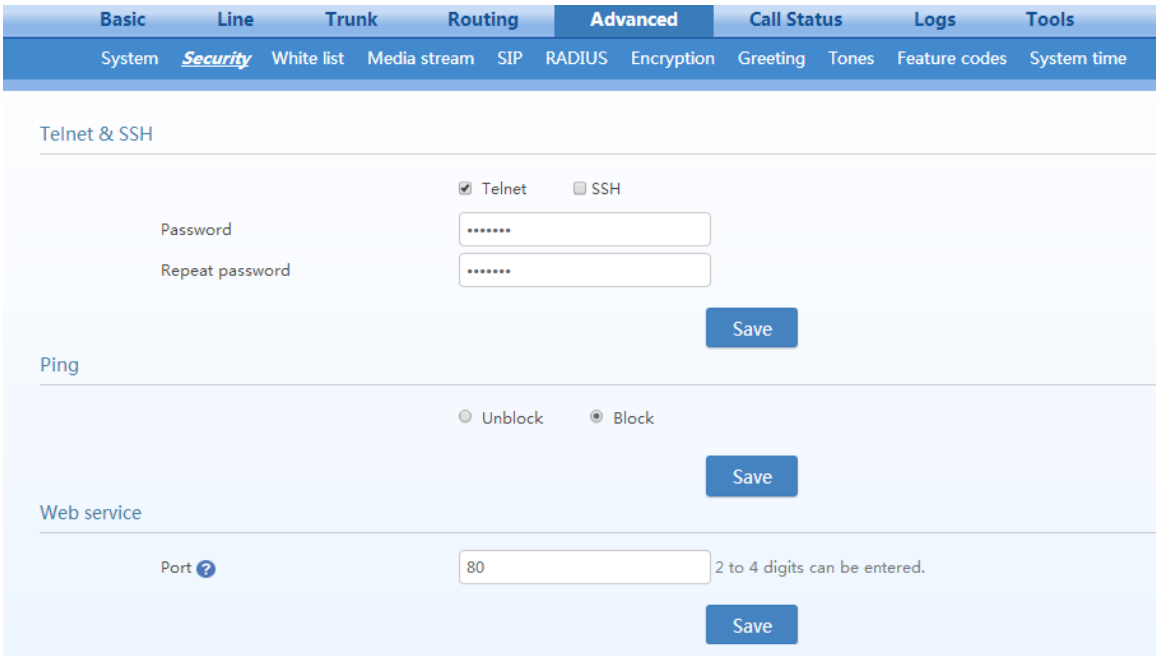


Table 2-25 Security Configuration Parameters

Name	Description
Telnet &SSH	
Telnet	If this parameter is selected, the Telnet service is enabled to allow a terminal to log in to the device through Telnet.
SSH	If this parameter is selected, the SSH service is enabled to allow a terminal to log in to the device through SSH.
Password	Specify the password for logging in to the device through Telnet or SSH. If both the Telnet and SSH services are enabled, the password will be shared. The password consists of 6 to 20 characters (letters, digits, or !@#$%^) and is case-sensitive.
Repeat password	Re-enter the specified password.
PING	
	Block: The device is forbidden to respond to a Ping message. Unblock: The device is allowed to respond to a Ping message.
Web service	
Port	This parameter specifies the number of a HTTP port used for accessing the Web management interface of the device. It is 80 by default.

Note

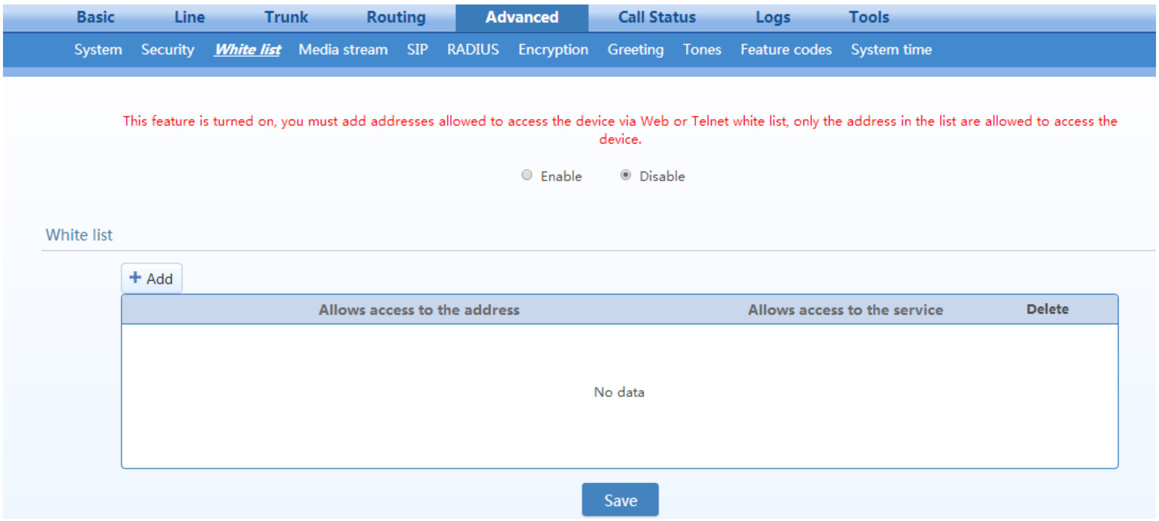
If the gateway is placed in a public network environment, you should disable the Telnet function to prevent hacker attacks.

2.7.5 White list for Accessing Web and Telnet

The white list is used to specify the IP addresses from which access to the device through Web or Telnet are allowed.

After login, choose **Advanced** > **White list** to open the white list configuration interface.

Figure 2-32 White List Configuration Interface



Step 1 Click **Add**.

Step 2 In the input box, enter IP addresses and types of services and click **Save**.

Step 3 Select **enable**.

Note

- This function takes effect after the device restarts.
- The device allows a white list of 20 entries.

2.7.6 Media Stream

After login, click the label of **Advanced** > **Media Stream** to open this interface.

Figure 2-33 Media Stream Configuration Interface

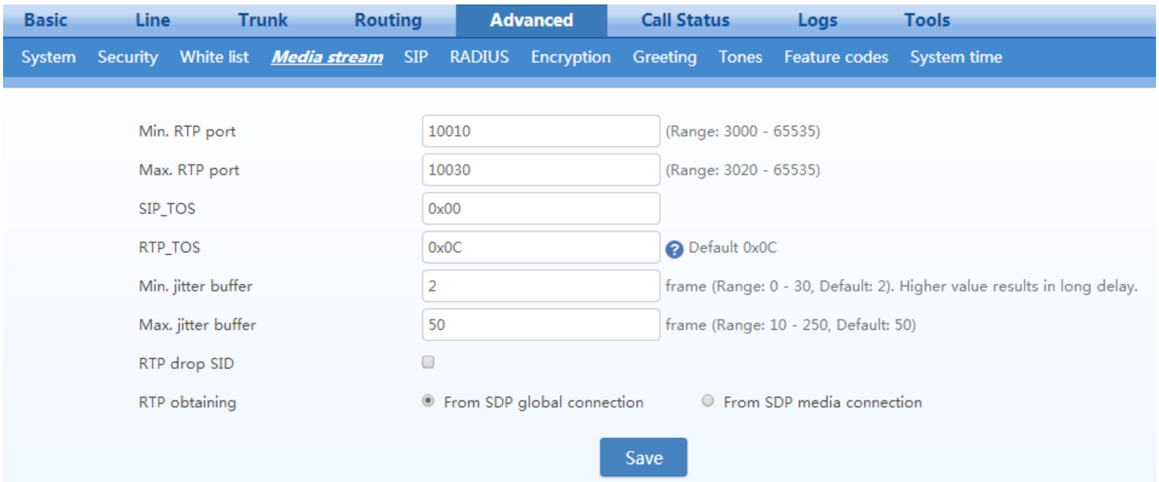


Table 2-26 Media Stream Configuration Parameter

Name	Description
Min. RTP port	The lowest port number of UDP ports for RTP transmission and receiving. The parameter must be greater than or equal to 3000. This is a required field. Note: each phone call will occupy RTP and RTCP ports. If the gateway is equipped with 4 subscriber lines (or trunk line), then at least 8 UDP ports are needed.
Max. RTP port	The highest port number of UDP ports for RTP's transmission and receiving. This is a required field. The value must be greater than or equal to "2 ×number of lines + min. RPT port". The value must be greater than or equal to "2 ×number of lines + min. RPT port".
SIP_TOS	For SIP signaling, set the service level quality guarantee for different priorities. The default value is 0x00.
RTP_TOS	For RTP voice streams, set the service level quality guarantee for different priorities. The default value is 0x0c.
Min. jitter buffer	RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This default value is 3.
Max. jitter buffer	RTP Jitter Buffer helps to reduce the influence brought by network jitter. The default value is 50.
RTP drop SID	Determine whether to discard received RTP SID voice packets. By default, SID voice packets will not be dropped. Note: RTP SID packets should be dropped only when they are in nonconformity to the specifications. Nonstandard RTP SID data could generate noise for calls.
RTP obtaining	• **From SDP global connection** (default value): obtain the IP address from SDP global connection; • **From SDP media connection**: obtain the IP address from SDP Media Description.

2.7.7 SIP Related Configuration

SIP messages consist of request message and response message. Both include a SIP message-header field and SIP message-body field. The SIP message header mainly describes the message sender and receiver; SIP message body mainly describes the specific implementation method of the dialog.

Message of request: the SIP message sent by a client to the server, for the purpose of activating the given operation, including INVITE, ACK, BYE, CANCEL, OPTION and UPDATE etc.

Message of response: the SIP message sent by a server to the client as response to the request, including 1xx, 2xx, 3xx, 4xx, 5xx, and 6xx responses.

Message header: Call-ID.

Parameter line: Via, From, To, Contact, Csq, Content-length, Max-forward, Content-type, White Space, and SDP etc.

MX gateways provide good flexibility in content setting in order to improve compatibility with the SIP register server.

After login, click the label of **Advanced > SIP** to open this interface.

Figure 2-34 SIP Related Configuration Interface

Table 2-27 SIP Related Configuration Parameter

Name	Description
SIP related configuration	
MWI subscription	The default is 86400 seconds. The gateway will send the platform a message to confirm that it has subscribed to MWI service at intervals of the time period set here. This parameter should be used in conjunction with voice mail subscription on the page of the subject subscriber line.
PRACK	Determine whether to activate Reliable Provisional Responses. (RFC 3262)
Session timer	Choose to activate session refresh (RFC 4028). By default, session timer is not activated. By default, this is not selected.
Session interval	Set the session refresh interval, the gateway will enclose the value of Session-Expires into INVITE or UPDATE messages. Default value is 1800 seconds.
Minimum timer	Set the minimum value of session refresh interval.
Request/Response message configuration	
Port for sending response	Select the port for sending SIP signaling responses: • Using received port to send response • Using 5060
Contact field in REGISTER	Choose the registration mode of gateway under LAN traversal circumstance, the default is **NAT IP Address.** • **NAT IP address**: use the NAT information returned by registration server. • **LAN IP address**: keep original content of Contact when register.
Domain name in REGISTER	The default is **Domain name**. • **Domain name**: complete domain name used for registration (for example: 8801@registrar.newrock.com); • **Sub domain name**: only use the common part of the name of domain (for example: 8801@newrock.com).
Via field	Choose whether to use NAT IP address or LAN IP address for **Via** header field value, the default is **NAT IP address.**
To header field	Choose whether to apply Sub domain name or Outbound proxy to the To header field, the default is **Sub domain name**.
Call-ID header field	Choose whether to fill Call ID field with Host name or Local IP address, the default is **Local IP address.**
Obtain Called party number from	Choose whether the gateway acquires the called number from Request Line field or To field. The default is **From *Request line* field**.
Calling party number in call transfer	Under call forwarding, the calling party number sent can be chosen from Originating number or Forwarding number being set for sending, the default is **Forwarding number**. For example: the subscriber line 2551111 on the gateway activates call forwarding feature and set the destination to 3224422. When caller with 13055553333 calls 2551111, the call will be forwarded to 3224422: • if **Originating number** is chosen, the number 13055553333 will be sent to 3224422 as calling party number; • if **Forwarding number** is chosen, the number 2551111 will be sent to 3224422 as calling party number.

Name	Description
Do not validate Via	Set whether to ignore Via field, By default, Via is ignored.
Register upon invite timeout	Set whether to activate registration when SIP message of INVITE is failed or time expired, and by default, re-registration is not selected.
Selecting the receiving port for response	Use the receiving port of proxy or use the sending port of proxy.
IMS	
IMS	Select the IMS mode or the NGN mode for use.
Multi port	A local SIP port can be assigned to each line.
SIP timer	
Timer A	INVITE request retransmit interval, for UDP only. It is 1000 ms by default.
Timer B	INVITE transaction timeout timer. It is 16000 ms by default.
Timer D	Wait time for response retransmits. It is 16000 ms by default.
Timer E	non-INVITE request retransmit interval, UDP only. It is 500 ms by default.
Timer F	non-INVITE transaction timeout timer. It is 17000 ms by default and ranges from 2000 to 32000 ms.
Timer G	INVITE response retransmit interval. It is 2000 ms by default.
Timer H	Wait time for ACK receipt. It is 16000 ms by default.
Timer I	Wait time for ACK retransmits. It is 5000 ms by default.
Timer J	Wait time for non-INVITE request retransmits. It is 16000 ms by default.
Timer K	Wait time for response retransmits. It is 5000 ms by default.
URI RFC 3966	
Calling party number	Select the address scheme for calling party: • SIP: SIP URI is used, such as “From: <sip:212@172.16.10.126>;tag=143349062153-1”. • TEL: tel URL is used, such as “From: <tel:212>;tag=143349065857-1”.
Called party number	Select the address scheme for called party: • SIP: SIP URI is used, such as “To: <sip:212@172.16.10.126>”. • TEL: tel URI is used, such as “To: <tel:212>”.
user=phone Parameter	Carrying the user=phone field precede SIP version in the INVITE request. e.g. INVITE sip:212@172.16.10.126;user=phone SIP/2.0

2.7.8 RADIUS (Unavailable on the HX4E)

After login, click the label of **Advance**d > **RADIUS** to open this interface.

Figure 2-35 RADIUS Configuration Interface

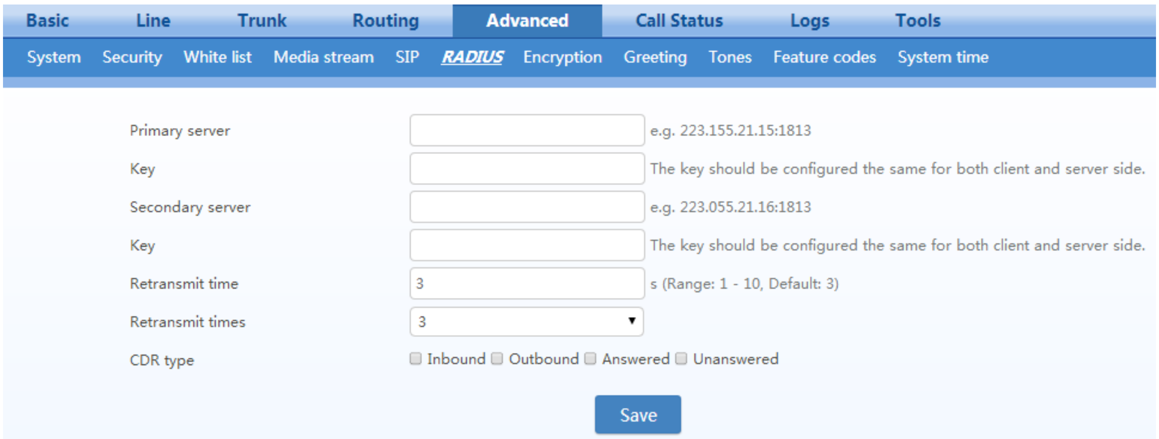


Table 2-28 RADIUS Configuration Parameter

Name	Description
Primary Server	Set IP address and port number of preferred Radius server. Note: if the port number is not configured yet, please use Radius default port number of 1813.
Key	Set the share key to be used for encrypted communications between Radius client and server. Note: The share key should be configured the same for both client and server side.
Secondary Server	Set the IP address and port number of standby Radius server. When the fault appears in communications between gateway and preferred Radius server, the gateway will automatically activate standby Radius server. Note: In case of no configuration of port number, use default port number of 1813.
Key	The share key for communications between Radius client and standby Radius server. Note: The key should be configured the same for both client and server side
Retransmit timer	Set the amount of overtime on response after transmission of Radius message, the default is 3 seconds. The retransmission will be performed If no response is given after the timeout.
Retransmit times	Set the times of retransmission of Radius message when no response is received default is 3 times.
CDR type	• Outbound: set whether to send RADIUS charge message for outbound calls; • Inbound: set whether to send RADIUS charge message for inbound calls; • Answered: set whether to send RADIUS charge message when calls are connected; • Unanswered: set whether to send RADIUS charge message for unanswered calls.

2.7.9 Encryption

After login, click the label of **Advanced** > **Encryption** to open this interface.

Figure 2-36 Encryption Configuration Interface

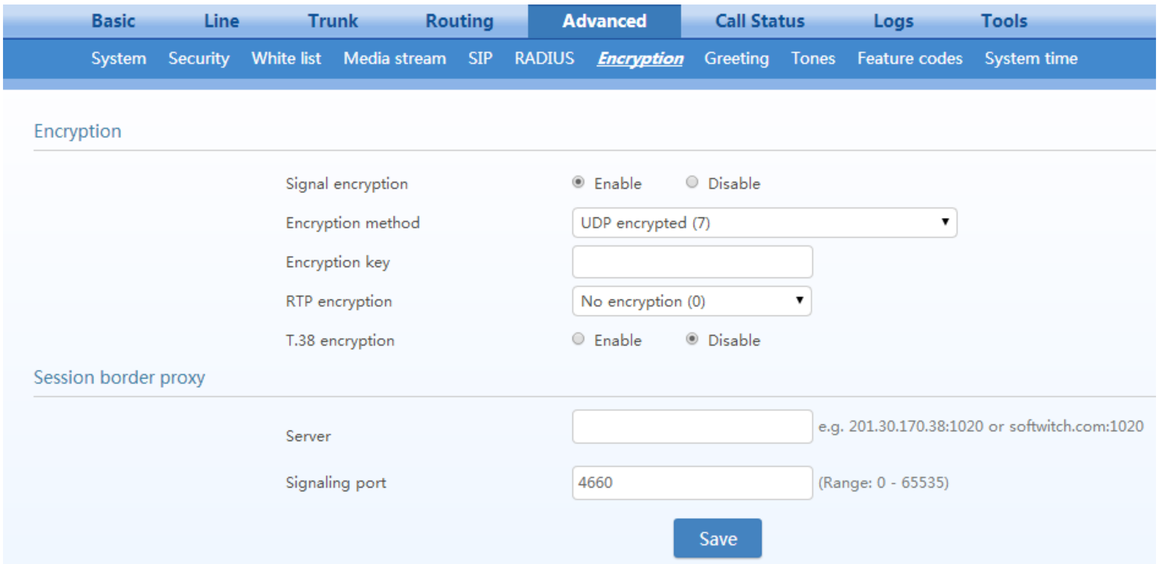


Table 2-29 Encryption Configuration Parameters

Name	Description
Signal encryption	Choose whether to encrypt signaling. By default, this is not selected.
Encryption method	Set the gateway encryption method, default is 7. The optional parameters as below: • 2:TCP not encrypted • 3: TCP encrypted • 6: UDP not encrypted • 7: UDP not encrypted • 8: Using keyword • 10: RC4 • 13: Encrypt13 • 14: Encrypt14 • 16: Word reverse(263) • 17: Word exchange(263) • 18: Byte reverse(263) • 19: Byte exchange(263) • 20:VOS
Encryption key	You may obtain it from service provider
RTP encryption	Choose whether to encrypt RTP voice pack, the default is 0. • 0: no encryption • 1: entire message • 2: header only • 3: the data body only
T.38 encrypt	Select to encrypt T.38 fax media stream packets. By default, this is not selected.
Session Border Proxy	

Name	Description
Server	Set the IP address and port number of session border proxy server. The character of “:” must be used between IP address and port number. Server address could be set into IP address or domain name. When a domain name is used, it is required to configure DNS server on the "Basic > Network" page. Example: 201.30.170.38:1020 or sbc.com:1020.
Signaling port	Signaling port assignment of the gateway, the default value is 4660. Signaling port number may be set at will, but cannot conflict with other ports of equipment.

2.7.10 Greeting

After login, choose **Advanced** > **Greeting** to open the audio files interface.

Figure 2-37 Greeting Interface

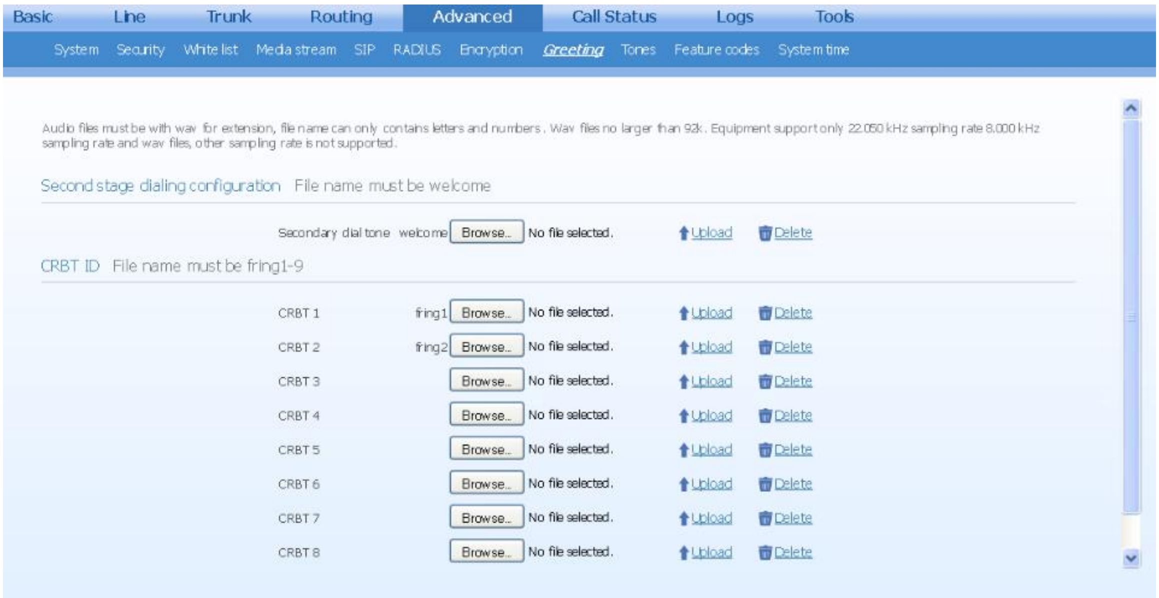


Table 2-30 Greeting Configuration Parameters

Name	Description
Second Stage Dialing Configuration	Click **Browse,** and then select the local audio file named **welcome.wav**. Click **Upload**. The uploaded audio file overwrites the original one. If you want to delete the current customized second stage dialing tone, click **Delete**. After the gateway restarts, the default second stage dialing tone is used.
CRBT ID	Click **Browse**, and then select the local audio file named **fring1/2/3/4/5/6/7/8/9.wav**. Click **Upload**. The uploaded audio file overwrites the original one. If you want to delete the current color ringback tone, you can click **Delete.** After the gateway restarts, the default color ringback tone is used.

2.7.11 Call Progress Tone Plan

After login, click the label of **Advanced > Tones** to open this interface.

Figure 2-38 Call Progress Tone Configuration Interface

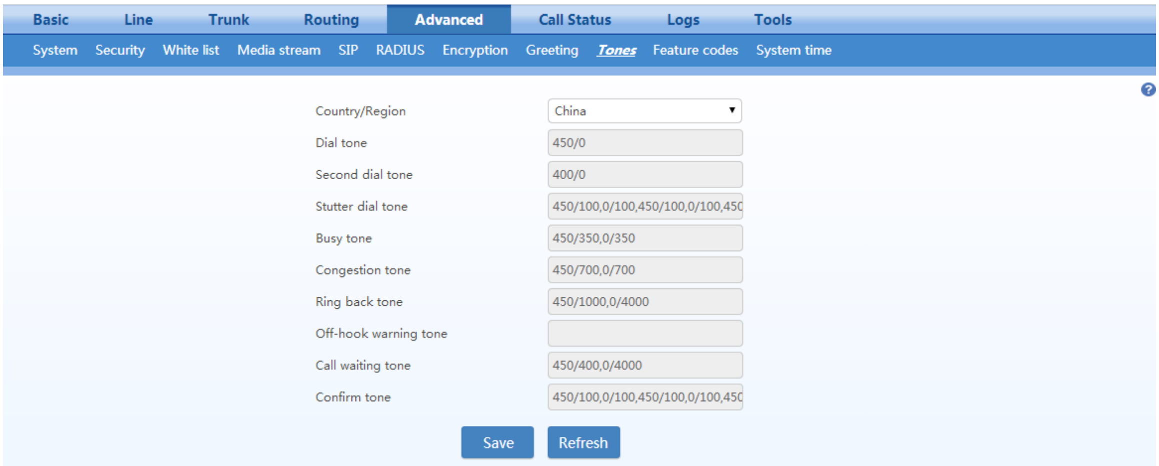


Table 2-31 Call Progress Tone Configuration Parameters

Name	Description
Country/Region	There are progress tone plans for several countries and regions which are pre-programmed in gateways. Users may also specify the tone plan according to the national standard. Gateways provide tone plans for the following countries and regions: China; the United States; France; Italy; Germany; Mexico; Chile; Russia; Japan; South Korea; Hong Kong; Taiwan; India; Sudan; Iran; Algeria; Pakistan; Philippines; Kazakhstan, Singapore, Israel, Malaysia, Indonesia, United Arab Emirates, Zimbabwe, Australia. User-defined: define the call progress tones by yourself.
Dial tone	Prompt tone of off-hook dial tone.
Second dial tone	Used for the second stage dial tone.
Stutter dial tone	Used for prompt of voice mail, or when the subscriber line is set with “Don’t Disturb Service and Call Transfer”.
Busy tone	Used for busy line prompt.
Congestion tone	Used for notification of call set up failure due to resource limit.
Ring back tone	The tone sent to caller when ringing is on.
Off-hook warning tone	Used for reminding the subscriber of off-hook and no dialup status of the phone.
Call waiting tone	Used for notification in call waiting.
Confirm tone	Used for confirming function keys being entered.

Here are examples that illustrate the various call-progress tones

- 350+440 (dial tone)

  Indicates the dual–frequency tone consisting of 350 and 440 Hz

- 480+620/500,0/500 (busy)

  Indicates the dual–frequency tone consisting of 480 and 620 Hz, repeated playing with 500 milliseconds on and 500 milliseconds off.

Note: 0/500 indicates 500 milliseconds mute.

- 440/300,0/10000,440/300,0/10000

  Indicates 440 Hz single frequency tone, repeated twice in terms of 300 milliseconds on and 10 seconds off.

- 950/333,1400/333,1800/333,0/1000

  Indicates repeated playing 333 milliseconds of 950 Hz, 333 milliseconds of 1400 Hz, 333 milliseconds of 1800 Hz, and mute of 1 second.

2.7.12 Feature Codes

The feature codes consist of system feature codes and service feature codes. The system feature codes are used for acquiring gateway information, and the latter is used for users to activate and inactivate supplementary services.

After login, click the label of **Advanced** > **Feature** codes to open this interface.

The following are the examples of the dialing rule for the feature codes:

Using *xx (dial * and 2 digits number) to activate a service

Using #xx (dial # and 2 digits number) to cancel a service. This is illustrated with the following defaults for various parameters, which may be modified according to requirements.

It is highly recommended not to modify the default configuration in **System feature codes**.

Figure 2-39 Feature Codes Configuration Interface

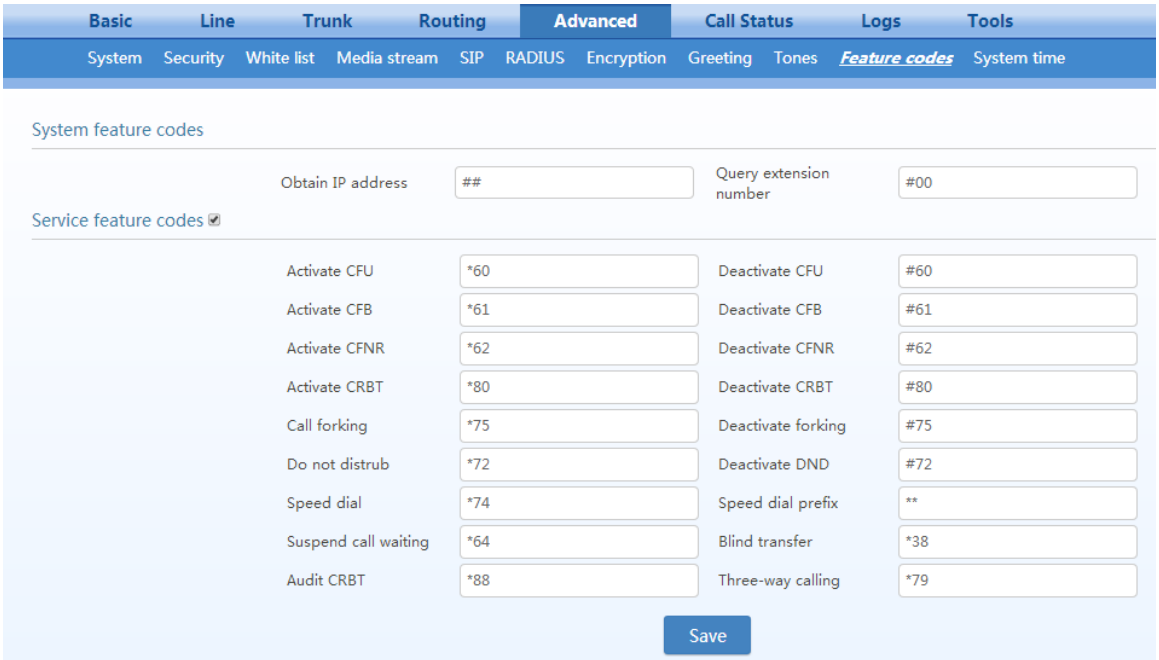


Table 2-32 Feature Codes Configuration Parameter

Name	Description
System feature codes	

Name	Description
Obtain IP address	The function key for determining the IP address of gateway, with a default of ##. When this function key is dialed, you can hear the device IP address, the web port number for accessing the device, the IP address of the gateway, the subnet mask, and the system software version number. Note: If the device has only the FXO port, you can use Finder, a tool developed by New Rock, to obtain the IP address. If you want to have a copy of Finder, please send an email to gs@newrocktech.com.
Query extension number	The function key for determining the phone number of this subscriber line, with default of #00. By dialing this key, your will hear the phone number of the subscriber line voiced by the gateway.
Service feature codes	You can click to enable the service function key, or deselect the checkbox to disable the service function key.
Activate CFU	The function key for activating unconditional call forwarding, with a default of *60. Dialing this key will activate unconditional call forward of the line and set the destination number for call forwarding. User operation: off hook → press *60 →enter the destination number. Users can determine the latest destination number set by dialing *60*. Note: It's required to enable call forwarding service before using this function (please see the instructions on the relevant configuration of **subscriber line**).
Deactivate CFU	The function key for deactivating unconditional call forwarding, with default of #60. User operation: off hook → press #60 → hang up.
Activate CFB	The function key for activating call forwarding on busy, with default of *61. Dialing this key may activate CFB, and specify the destination number. It's required to enable call forwarding on busy service before using this function (please see the instructions on relevant configuration of **subscriber line**).
Deactivate CFB	The function key for deactivating call forwarding on busy, with default of #61. User operation: off hook → press #61 → hang up. User operation: off hook → press #61 → hang up.
Activate CFNR	The function key for activating call forwarding on no answer, with default of *62. Dialing the function key should activate call forwarding on no answer and specify destination number. Note: It's required to enable call forwarding on no answer service before using this function (please see the instructions on relevant configuration of **subscriber line**).
Deactivate CFNR	The function key for deactivating call forwarding on no answer, with default of #62.
Activate CRBT	The function key for activating color ringback tone, with default of *80. Subscribers may select their favorite color RB tone by using this key. Note: It's required to start color ring service before using this function (please see **Phone** for how to assign the feature to the phone). User operation: upon off hook, the subscriber may press the function key (e.g. *80), then, input the two-digit index numbers of color ring; *80* is used for hearing and inquiring the color ring that has been previously set.
Deactivate CRBT	The function key for deactivating the color ring, with default of #80. The subscriber may use such key to recover the normal ring of phone. User operation: off hook → press #80 → hang up.
Call Forking	The function key for activating the double-ring/forking feature, with default of *75.
Deactivate forking	The function key for deactivating the feature, with default of #75.

Name	Description
Do not disturb	Activate “Don't Disturb”, with default of *72. With DND selected, the gateway will reject all coming calls by sending busy tone to the caller. Note: It’s required to start “Don't Disturb” prior to using this function (please see the instructions on relevant configuration of **subscriber line**).
Deactivate DND	The function key to cancel “Don't Disturb”, with default of #72. Dialing the function key may recover normal ringing upon the arrival of incoming calls.
Speed dial	Define the function key of dial, with default of *74. This key allows the user to build a table of 2-digits (20~49) speed-dial numbers. Note: It’s necessary to get the dial-up service under way before applying this function (please see **Phone** for how to assign the feature to the phone). User operation: upon dialing the function key (*74), dial the two-digit speed dial followed by the expanded number terminated with #. To cancel the relationship, see the following descriptions.
Speed dial prefix	The prefix number for applying abbreviated dialing, with default of **. The said prefix should be added ahead of abbreviated dialing numbers when using abbreviated dialing. User operation: off hook → dial the prefix number of abbreviated dialing (**) and dial abbreviated dialing number (20).
Suspend call waiting	The function key for cancelling the call waiting feature for next call, with default of *64. Dialing this function key will temporarily shield the user from a call-waiting distraction for next call, avoiding the possible intervention. Note: The function key works only for single cancel, if to cancel the call waiting completely, please refer to the instructions on relevant configuration of **subscriber line**. “FXS-n” corresponds to the “Line > FXS phone Number ID n”.
Blind call transfer	Function key of blind call transfer, with default of *38. User operation: during the call, tap the phone hook switch or press R button→ dial *38→ dial the called number and then hang up.
Audit CRBT	The function key for listening to the color ring, with default of *88. User operation: off hook → press *88 → input color ring number. During listening, you can press a two-digit CRBT index to change to another CRBT file.
Three-way calling	The default value is *79.

2.7.13 Clock Service

After login, click the label of **Advanced > System time** to open this interface.

Figure 2-40 Clock Service Interface

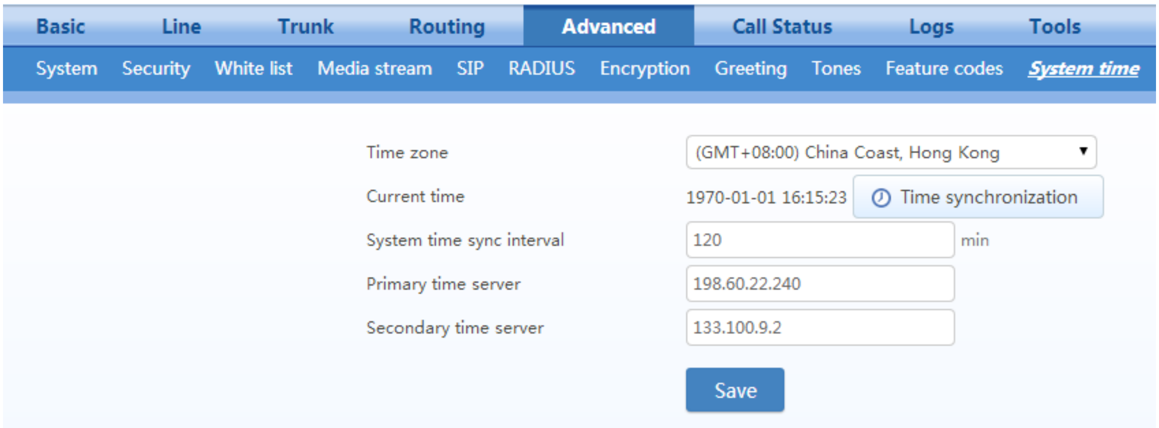


Table 2-33 Clock Service Parameters

Name	Description
Time Zone	Select a time zone, and the parameter values include: • (GMT-11:00) Midway Island • (GMT-10:00) Honolulu. Hawaii • (GMT-09:00) Anchorage, Alaska • (GMT-08:00) Tijuana • (GMT-06:00) Denver • (GMT-06:00) Mexico City • (GMT-05:00) Indianapolis • (GMT-04:00) Glace_Bay • (GMT-04:00) South Georgia • (GMT-03:30) Newfoundland • (GMT-03:00) Buenos Aires • (GMT-02:00) Cape_Verde • (GMT) London • (GMT+01:00) Amsterdam • (GMT+02:00) Cairo • (GMT+02:00) Israel • (GMT+02:00) Zimbabwe • (GMT+03:00) Moscow • (GMT+03:30) Teheran • (GMT+04:00) Muscat • (GMT+04:00) United Arab Emirates • (GMT+04:30) Kabul • (GMT+05:30) Calcutta • (GMT+05:00) Karachi • (GMT+06:00) Almaty • (GMT+07:00) Bangkok • (GMT+07:00) Indonesia • (GMT+08:00) Beijing • (GMT+08:00) Taipei • (GMT+08:00) Singapore • (GMT+08:00) Malaysia • (GMT+09:00) Tokyo • (GMT+10:00) Canberra • (GMT+10:00) Adelaide • (GMT+11:00) Magadan • (GMT+12:00) Auckland
Current time	Display current time for the device. Click **Clock calibration** to calibrate the time.
System time sync interval	Set the synchronization period of the time. It is 120 minutes by default.

Name	Description
Primary time server	Enter the IP address of preferred time server here. It has no default value.
Secondary time server	Enter the IP address of Secondary time server here. It has no default value.

2.8 Status

2.8.1 Call Status

After login, click **Call Status** > **Call Status** to open this interface.

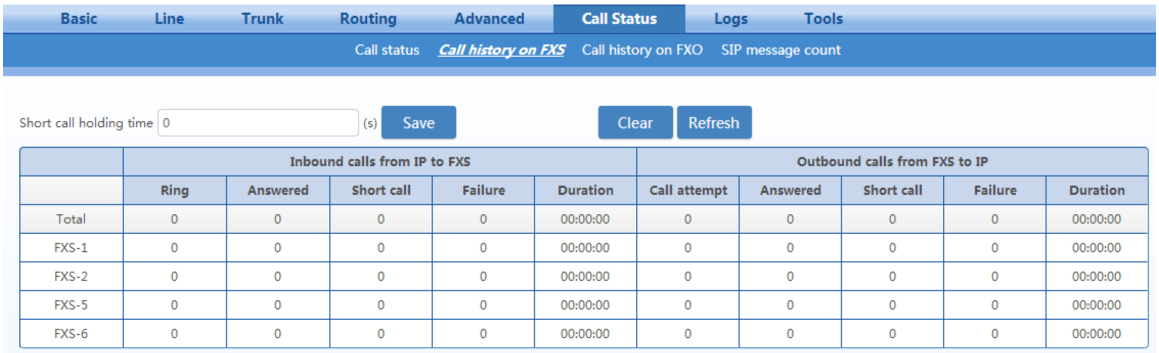
Figure 2-41 Call Status Interface

Line ID	Number	Register status	Line Status	Call Status	Phone No. (Other End)	Duration	In	Out	Answered	Operation
FXS-1	8000	Server not response	Idle	Idle			0	0		-
FXS-2	8001	Server not response	Idle	Idle			0	0		-
FXO-3	8002	Server not response	Disconnected	Idle			0	0		-
FXO-4	8003	Server not response	Disconnected	Idle			0	0		-
FXS-5	8004	Server not response	Idle	Idle			0	0		-
FXS-6	8005	Server not response	Idle	Idle			0	0		-
FXO-7	8006	Server not response	Disconnected	Idle			0	0		-
FXO-8	8007	Server not response	Disconnected	Idle			0	0		-

2.8.2 Call History on FXS

After login, click Call **Status** > **Call history on FXS** to open this interface.

Figure 2-42 Interface of Call history on FXS

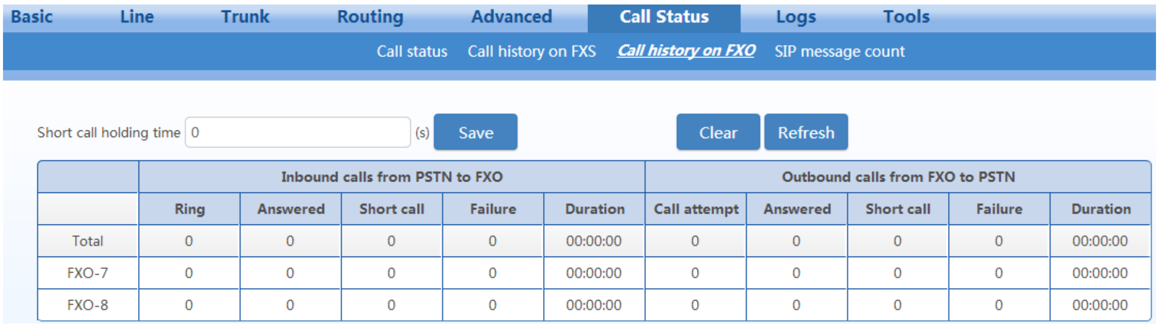


	Inbound calls from IP to FXS					Outbound calls from FXS to IP				
	Ring	Answered	Short call	Failure	Duration	Call attempt	Answered	Short call	Failure	Duration
Total	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXS-1	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXS-2	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXS-5	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXS-6	0	0	0	0	00:00:00	0	0	0	0	00:00:00

2.8.3 Call History on FXO

After login, click the label of **Call Status** > **Call history on FXO** to open this interface.

Figure 2-43 Interface of Call on FXO

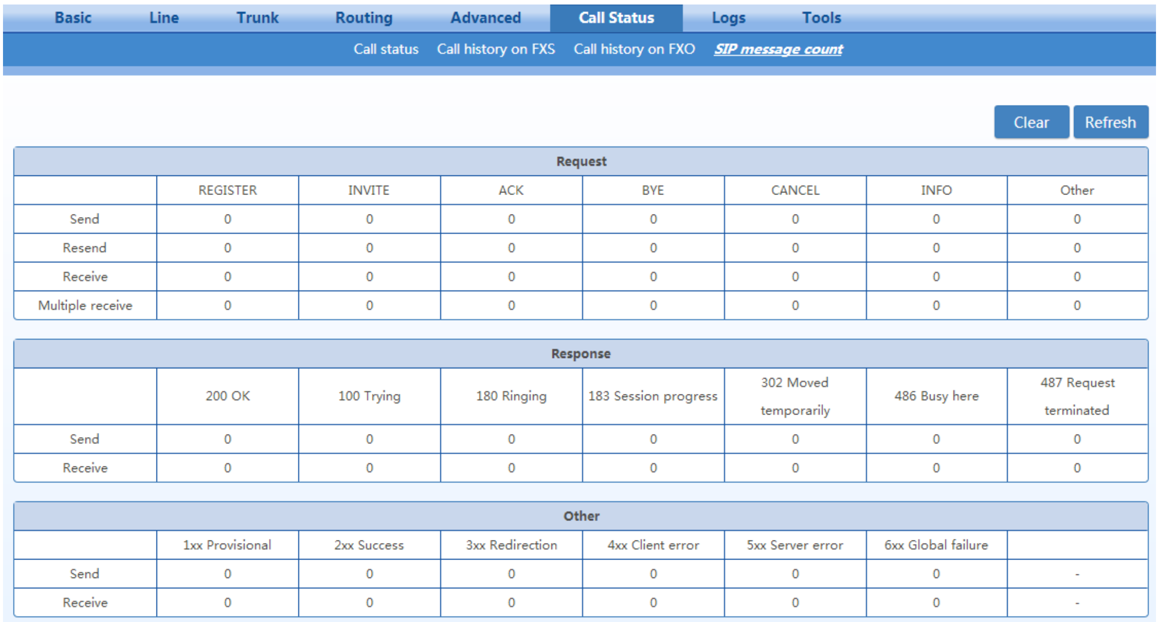


	Inbound calls from PSTN to FXO					Outbound calls from FXO to PSTN				
	Ring	Answered	Short call	Failure	Duration	Call attempt	Answered	Short call	Failure	Duration
Total	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXO-7	0	0	0	0	00:00:00	0	0	0	0	00:00:00
FXO-8	0	0	0	0	00:00:00	0	0	0	0	00:00:00

2.8.4 SIP Message Count

After login, click **Call Status** > **SIP message count** to open this interface.

Figure 2-44 SIP Message Count Interface



Request							
	REGISTER	INVITE	ACK	BYE	CANCEL	INFO	Other
Send	0	0	0	0	0	0	0
Resend	0	0	0	0	0	0	0
Receive	0	0	0	0	0	0	0
Multiple receive	0	0	0	0	0	0	0

Response							
	200 OK	100 Trying	180 Ringing	183 Session progress	302 Moved temporarily	486 Busy here	487 Request terminated
Send	0	0	0	0	0	0	0
Receive	0	0	0	0	0	0	0

Other							
	1xx Provisional	2xx Success	3xx Redirection	4xx Client error	5xx Server error	6xx Global failure	
Send	0	0	0	0	0	0	-
Receive	0	0	0	0	0	0	-

2.9 Logs

2.9.1 System Status

Critical runtime information of gateways can be obtained in this interface, including:

- The information about login interface (including IP address and permissions of the user)
- SIP registration status
- Call-related signaling and media (RTP) information

After login, click the label of **Logs** > **System Status** to open this interface.

Figure 2-45 System Status Interface

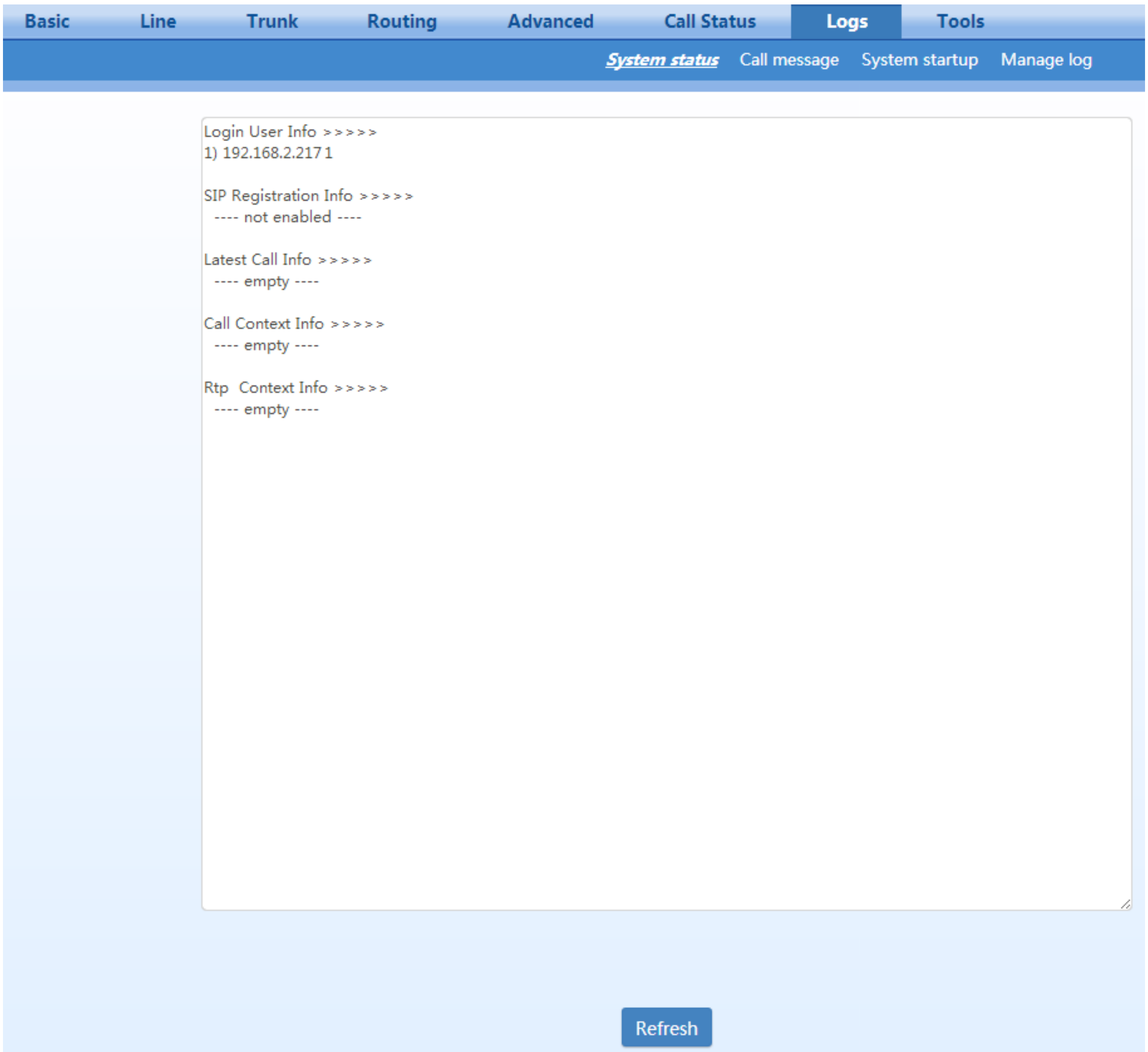


Table 2-34 System Status Parameters

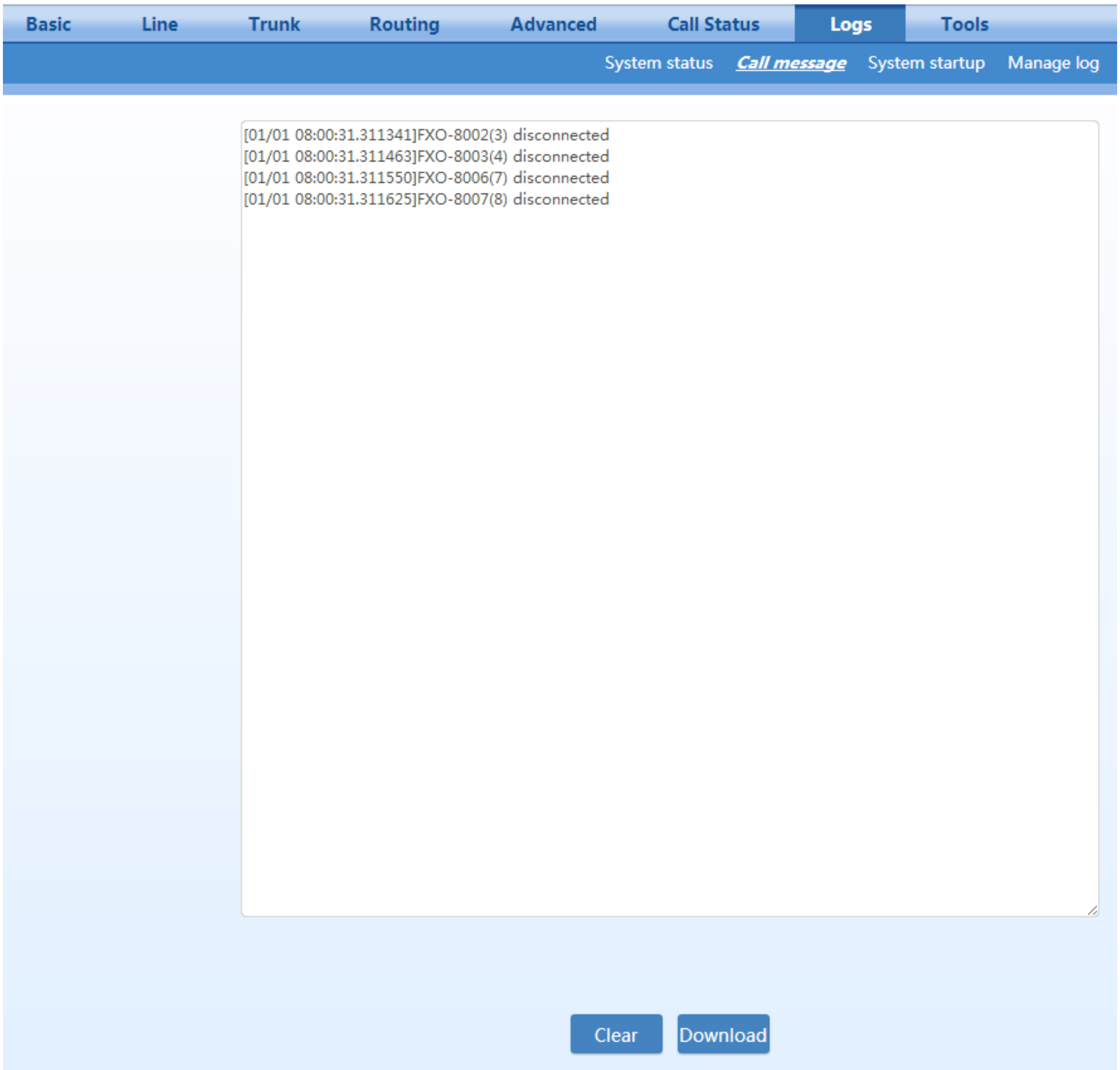
Name	Description
Login User Info	Show the IP address and permissions of the login user. The numbers following the IP address show the online permission level of the user: 1- administrator; 2 - operator; 3 – viewer. The viewer can only read the configuration. When more than one administrator logs in at the same time, the first login’s permission level is 1; others are 3; also, when more than one operator logs in at the same time, the first one’s permission is 2, others are 3.
SIP Registration Info	Show registration status: Not enabled: the registration server’s address is not entered yet; Latest response: the latest response message for the registration. 200 means registered successfully; No response: no response from registration server. The cause may contribute to 1) incorrect address for the registration server; 2) IP network fault; or, 3) the registration server is not reachable.
Latest Call Info	Show the latest call.

Name	Description
Call Context Info (Call Context Info)	Show the call status.
Rtp Context Info	Show the voice channel related to the calls.

2.9.2 Call Message

After login, click **Logs** > **Call Message** to open this interface.

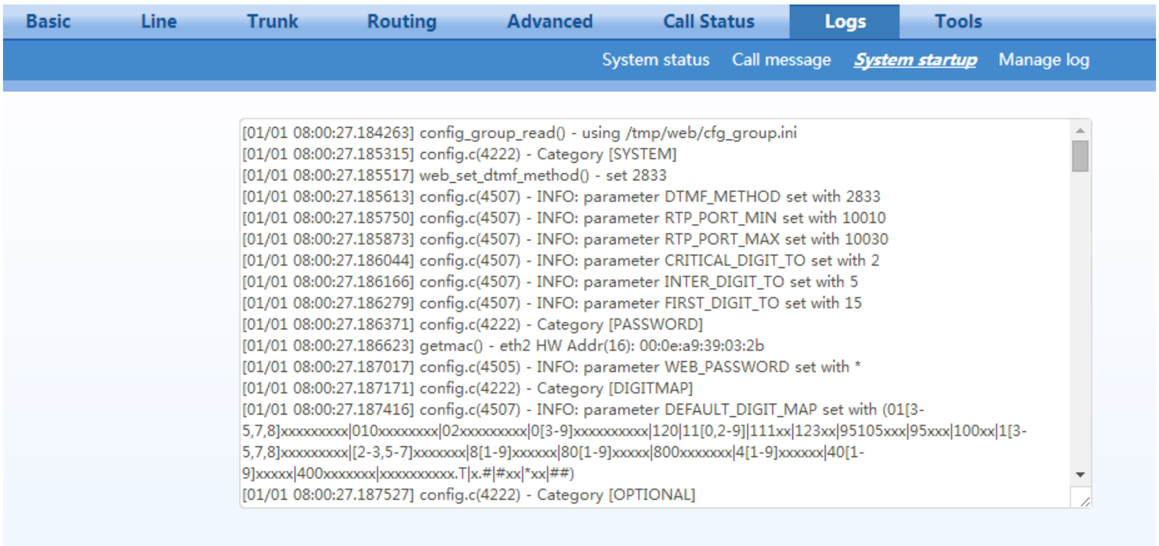
Figure 2-46 Call Message Interface



2.9.3 System Startup

After login, click **Logs** > **System Startup** to open this interface. Log files can be downloaded through this interface.

Figure 2-47 Interface of System Startup



2.9.4 Manage Log

After login, click **Logs** > **Manage Log** to open this interface. Log files can be downloaded through this interface.

Figure 2-48 Manage Log Interface

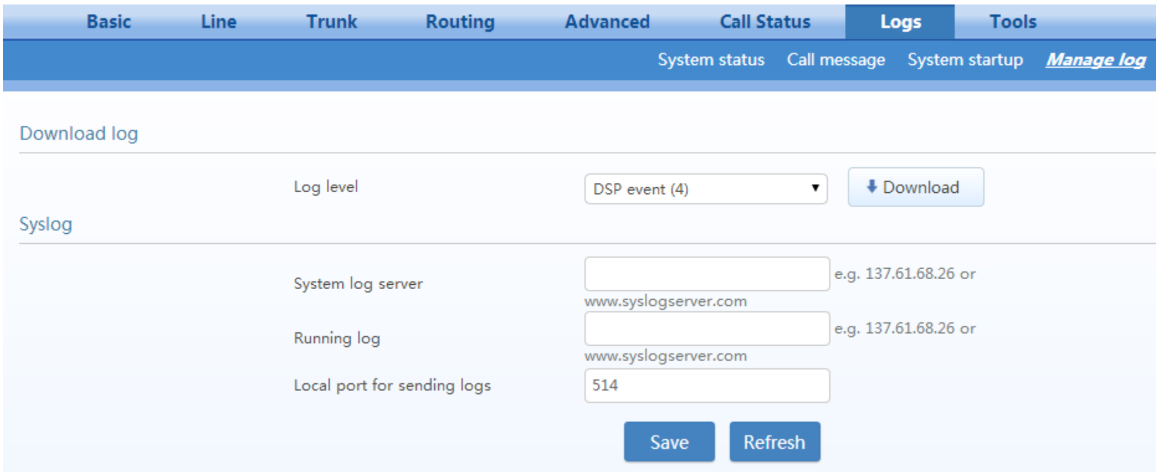


Table 2-35 Log Management Configuration Parameters

Name	Description
Download log	
Log level	Select the log file level of gateway, default is 4. The higher the level the more details the log file will be. Note: Log level should be set to 4 or lower when gateway is used in normal operation, avoiding reducing the system performance.
Syslog	
System log server	The syslog server receives the logs that are recorded in debug.log, message.log and boot.log otherwise.
Running server	The syslog server receives the logs that are recorded in message.log otherwise.

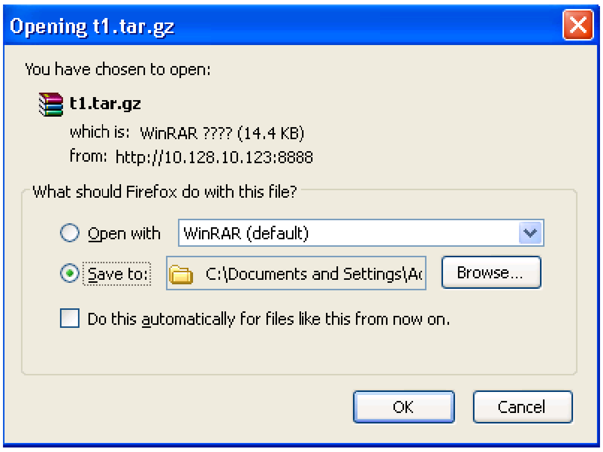
Name	Description
Local port for sending logs	The port used to send logs.

Procedure for downloading the log:

Step 1 Click **Download**, the gateway begins to assemble the logs.

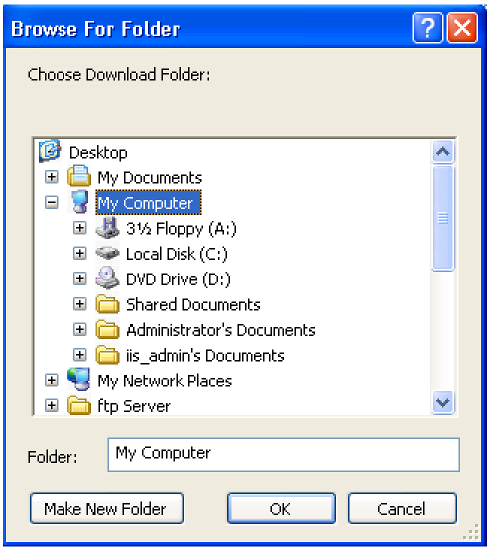
Step 2 After a few seconds, the interface of log saving will appear.

Figure 2-49 Log Saving Interface



Step 3 Click **Save**, and select path to save.

Figure 2-50 Path Saving Interface



Step 4 The user may review the log from the server.

2.10 Tools

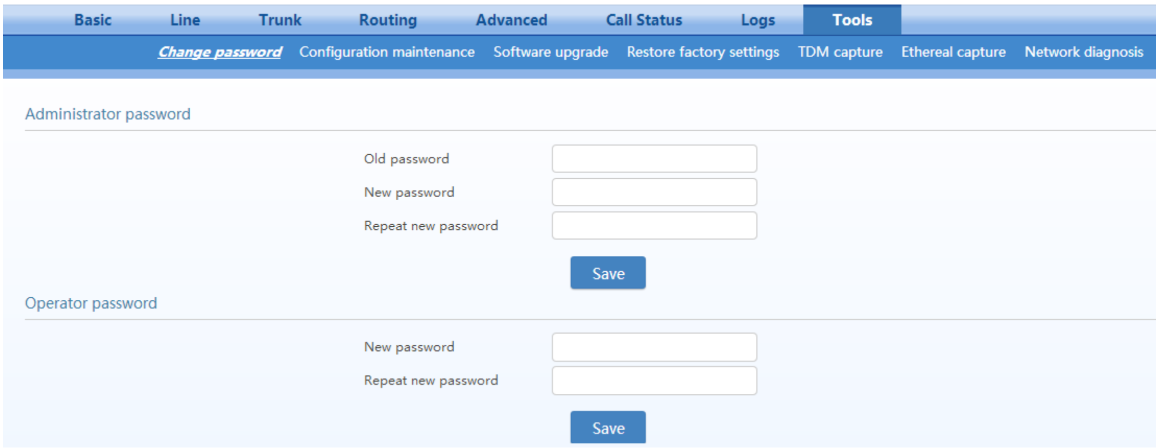
2.10.1 Change Password

After login, click **Tools** to open this interface. Only administrator is entitled to change the password of login.

For changing administrator password, it's required to enter new password into Old password, **New password** field and **Repeat new password** field, and then click **Save**.

The password being used by the operator will not be displayed, which could be changed by the administrator at any time. The administrator is allowed to change the operator's password by entering the new password into **Operator password** > **New password**.

Figure 2-51 Password Change Interface

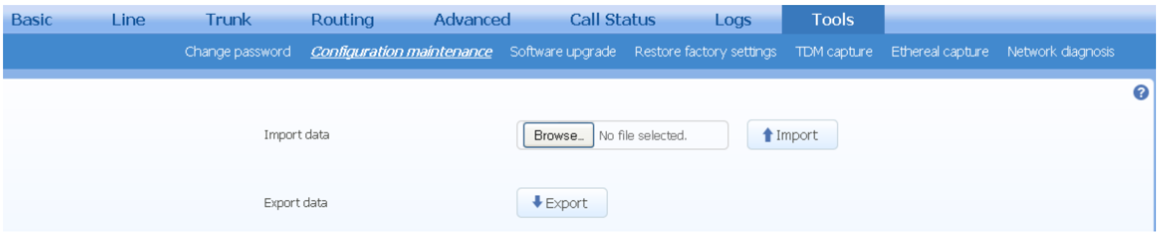


2.10.2 Configuration Management

After login, click **Tools**>**Import data** to open this interface.

The download procedure is similar to the download procedure of log files.
The steps for importing configuration files are the same as the Upgrade. The steps for exporting configuration files are the same as the steps for **Log Download**.

Figure 2-52 Configuration Management Interface



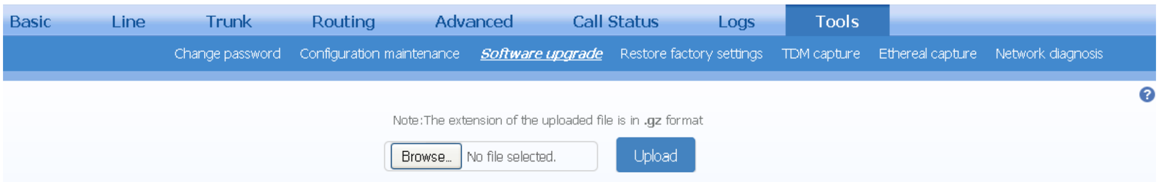
2.10.3 Upgrade

After login, click **Tools** > **Software upgrade** to open this interface. The software upgrade procedure is presented as below:

Step 1 Obtain the upgrade files (tar.gz file), and save the file onto a local computer.

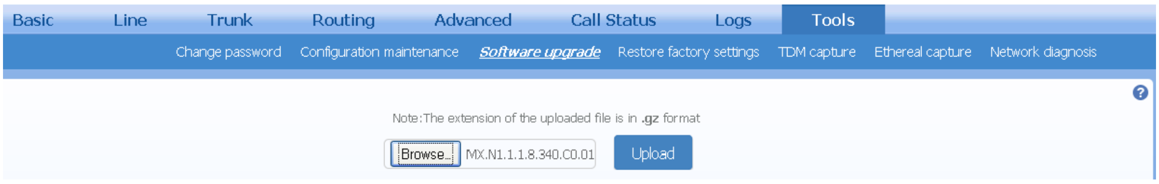
Step 2 Click **Tools** > **Software upgrade** to access to the page of software upgrade.

Figure 2-53 Upgrade Interface



Step 3 Click **Browse** to select the upgrade files.

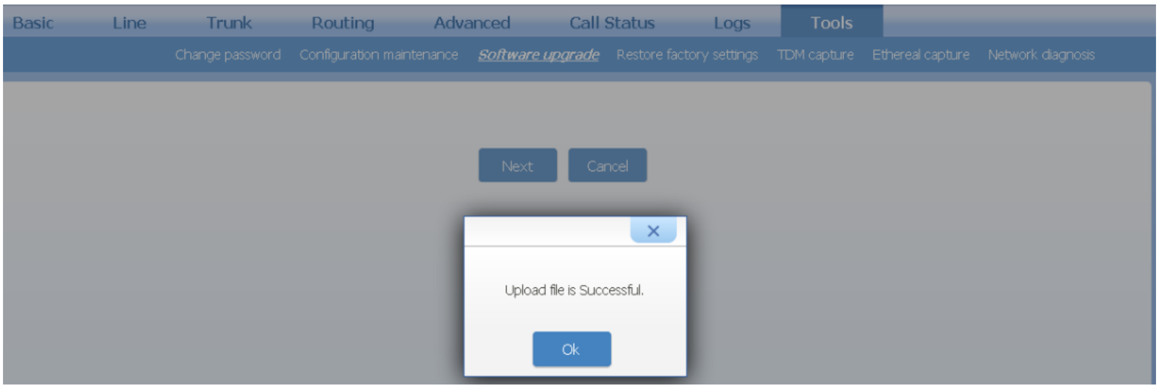
Figure 2-54 File Upload Interface



Step 4 Click **Upload**.

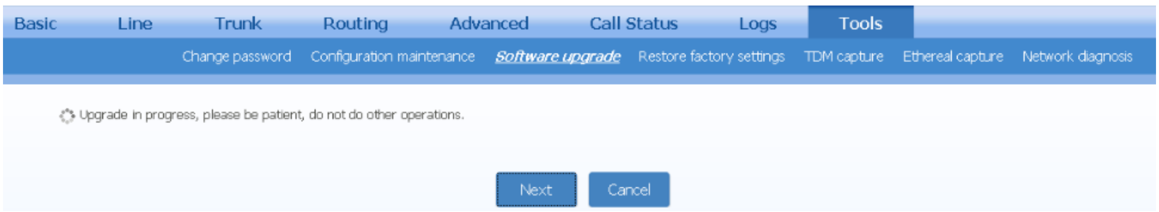
Step 5 Uploading will be completed in about 30 seconds, then click **Next**.

Figure 2-55 Upgrade Interface



Step 6 The following prompt appears during the upgrade.

Figure 2-56 Upgrade Process Screen

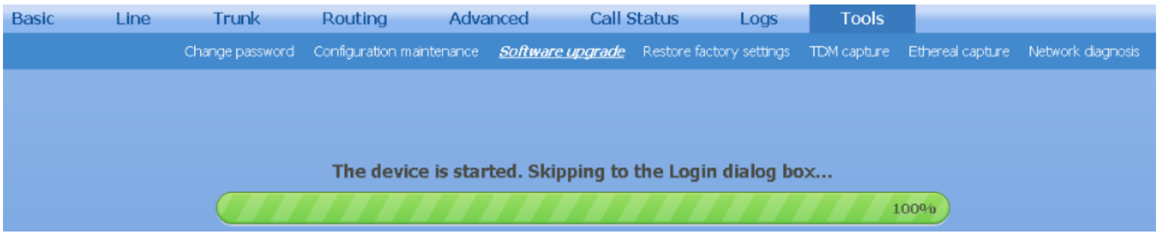


Note

A few minutes are needed to upgrade the gateway. Don't operate the gateway during this period.

Step 7 The device automatically restarts after upgrade is successful.

Figure 2-57 Interface for Completing Device Restart after Upgrade



The gateway is on the progress of reboot when the interface cannot be displayed.

Wait for about two minutes, and access the interface of gateway management system, click **Info** and check the software version.

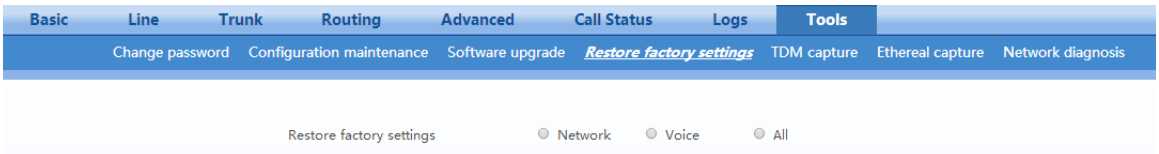
2.10.4 Restore Factory Settings

After login, click **Tools** > **Restore factory settings** to restore the factory settings.

The factory settings are designed based on common applications, and therefore, no need to modify them in many deployment situations.

You can choose to restore network or telephony related factory settings, or both.
Restoration takes effect after the system is restarted.

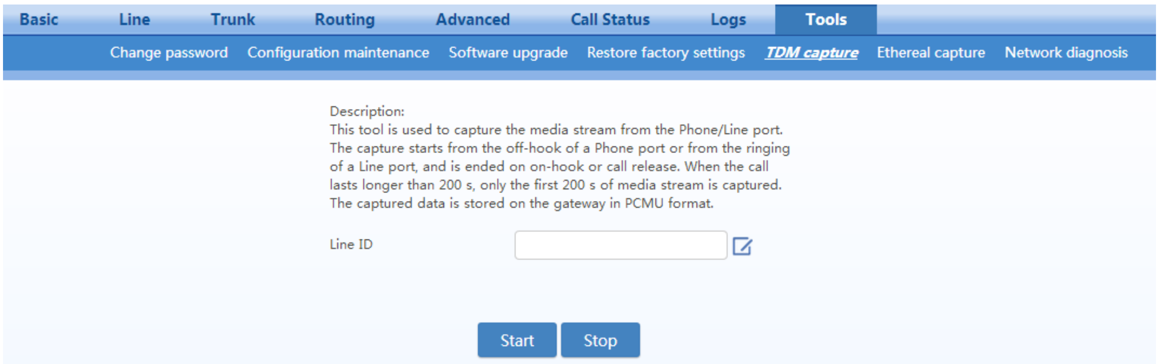
Figure 2-58 Restore Factory Settings Interface



2.10.5 Capture Recordings on the Port

After login, click **Tools > TDM capture** to open this interface. This tool can be used to capture the voice stream from the Phone or Line interface. When the call lasts longer than 200 seconds, only the first 200 seconds of voice stream will be captured. The voice file is stored on the gateway in PCMU format.

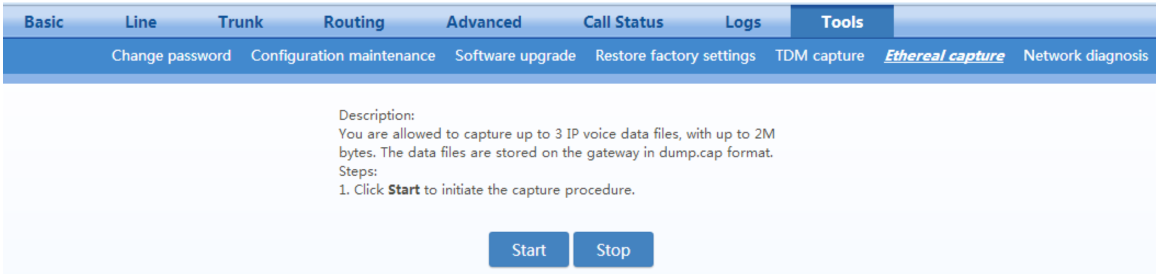
Figure 2-59 Interface for capturing Port Recordings



2.10.6 Ethereal Capture

After login, click **Tools** > **Ethereal capture** to open this interface. You are allowed to capture up to three IP voice data files, each with up to 2M bytes. The data files are stored on the gateway in dump.cap format under catalog /var/log.

Figure 2-60 Ethereal Capture Interface



2.10.7 Network Diagnosis

After login, click **Tools** > **Network diagnosis** to open this interface.

If the Internet is unavailable, you can use this tool to diagnose whether the network is connected.

Figure 2-61 Automatic Diagnosis Interface

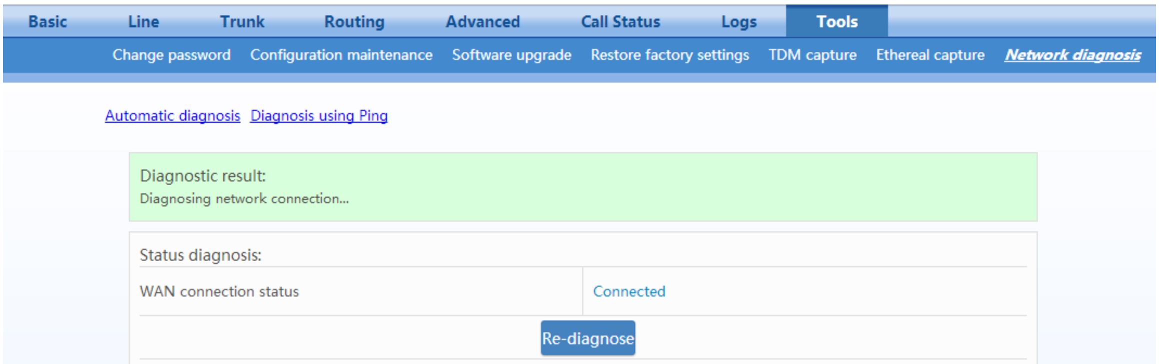
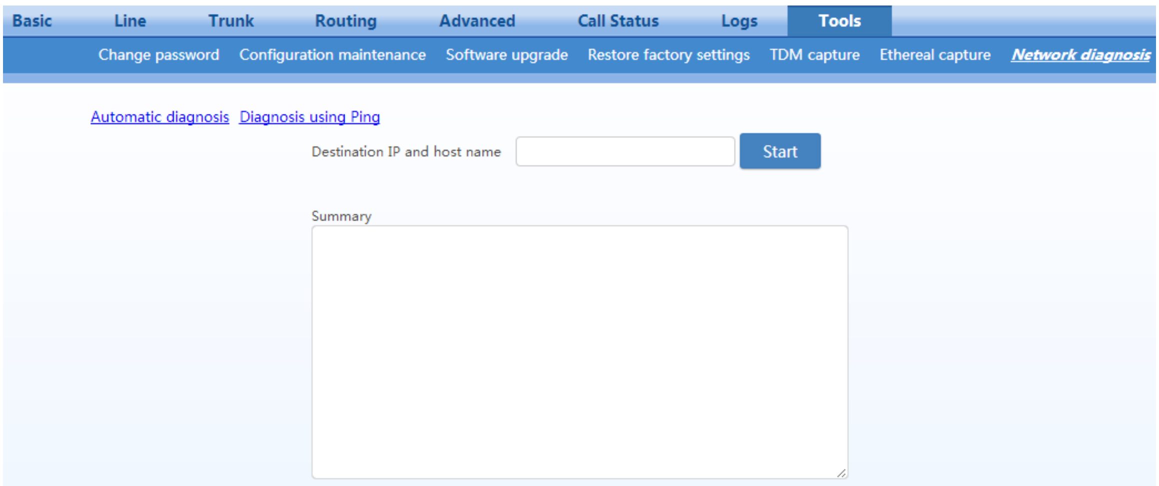


Figure 2-62 Ping Diagnosis Interface



2.11 Product Information

After login, click **Version info** to view the gateway hardware and software version information.

2.12 Reboot

To restart the gateway, click **Reboot** in the top right corner.
As this is a system wide reset, it takes longer time.

2.13 Logout

After login, click the **Logout** at top right to exit the gateway management system and return to the login interface.

3 Appendix: VLAN Configuration

Virtual Local Area Network (VLAN) virtually divides a physical LAN into multiple broadcast domains. Only hosts in the same VLAN can directly communicate without a router, so broadcast packets are restricted to the same VLAN, improving network security (e.g, a data-only VLAN or voice-only VLAN). VLAN technology identifies the VLAN information of a data packet by adding the VLAN tag field in the Ethernet frame header.

When a gateway accesses a VLAN, configurations such as VLAN tags and priorities are required for the gateway.

The following methods are used for configuring VLANs:

- Manual configuration: Via a web-based GUI, and restart is required after the configuration.
- Automatic configuration: With Link Layer Discovery Protocol (LLDP) enabled, during startup the device automatically obtains VLAN configuration information via an LLDAP message, adds VLAN tag in packets it sends, and obtains network information such as IP address using the DHCP mode by default.

New Rock gateways support two VLAN modes: single VLANs and multi-service VLANs (including voice and management VLANs). Manual mode is used to configure single and multi-service VLANs. Automatic mode can configure only single VLANs.

3.1 Manual Configuration

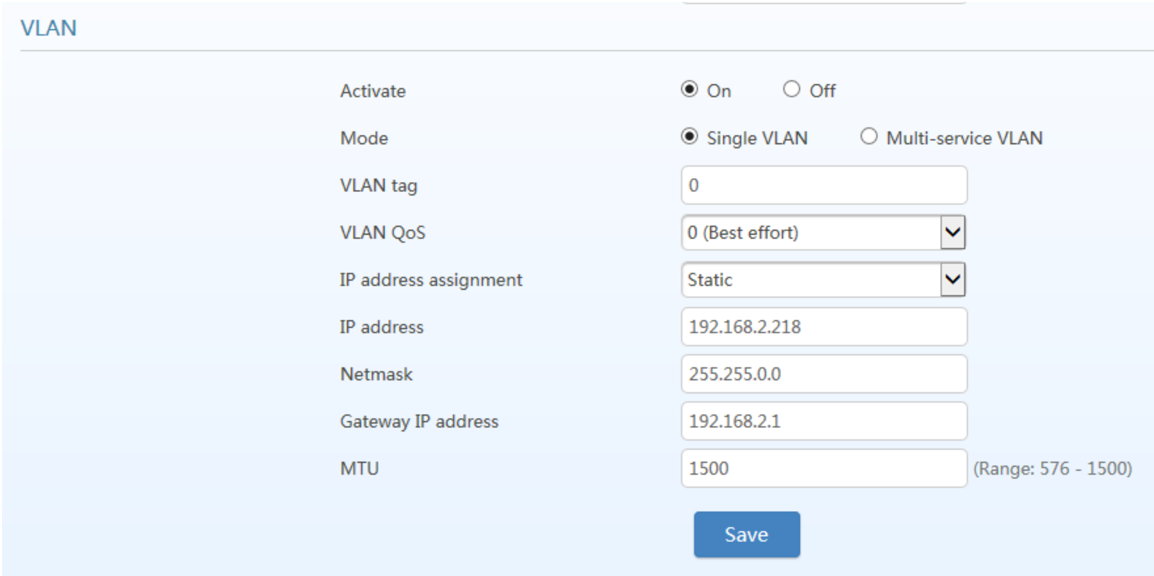
3.1.1 Single VLAN

All services of the device are on the same VLAN, and the device receives only data packets carrying the VLAN and includes the VLAN tag in all sent data packets. In the single VLAN mode, all device services belong to the same VLAN. The device receives only data packets that carry the VLAN tag and includes the VLAN tag in all sent data packets. In this mode, the physical network port of the device has no separate address and shares the IP address of the VLAN interface.

Configuration

On the web interface, click **Network**, set the VLAN function to **On**, set **Mode** to **Single VLAN**, enter the VLAN tag, and specify network information such as IP address or select **DHCP**. As shown in Figure 3-63.

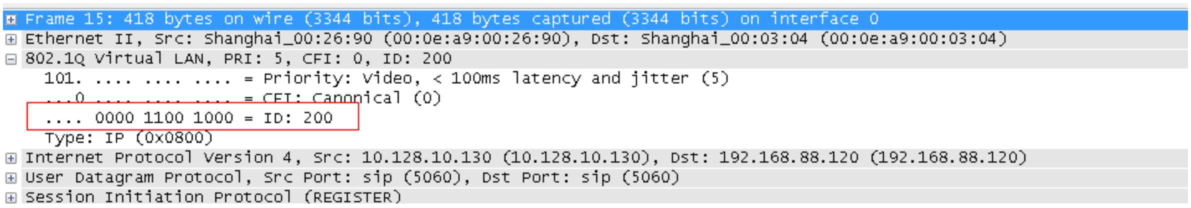
Figure 3-63 Configuring the single VLAN



Example of Single VLAN

Configure the device to work in single VLAN mode with a corresponding VLAN tag of 200, and restart the device. Check that all data packets sent by the device carry a VLAN ID 200, as shown in Figure 3-64.

Figure 3-64 A Data Packet Carrying a Corresponding VLAN Tag in the Single VLAN Mode



3.1.2 Multi-service VLAN

In the multi-service VLAN mode, the device can configure a VLAN tag; a priority for the voice service (SIP signaling and RTP/T.38 media stream); and a management service (HTTP, Telnet, TR069, and SNMP). The device carries a different VLAN tag in data packets for different services. In this mode, the physical network port of the device can have a separate address or obtain an address from a non-VLAN network.

Configuring Voice VLAN

The device includes a VLAN tag configured in the voice VLAN in SIP, RTP and T.38 data packets.

The voice VLAN of the device has the following two modes: Mode 1 and Mode 2.

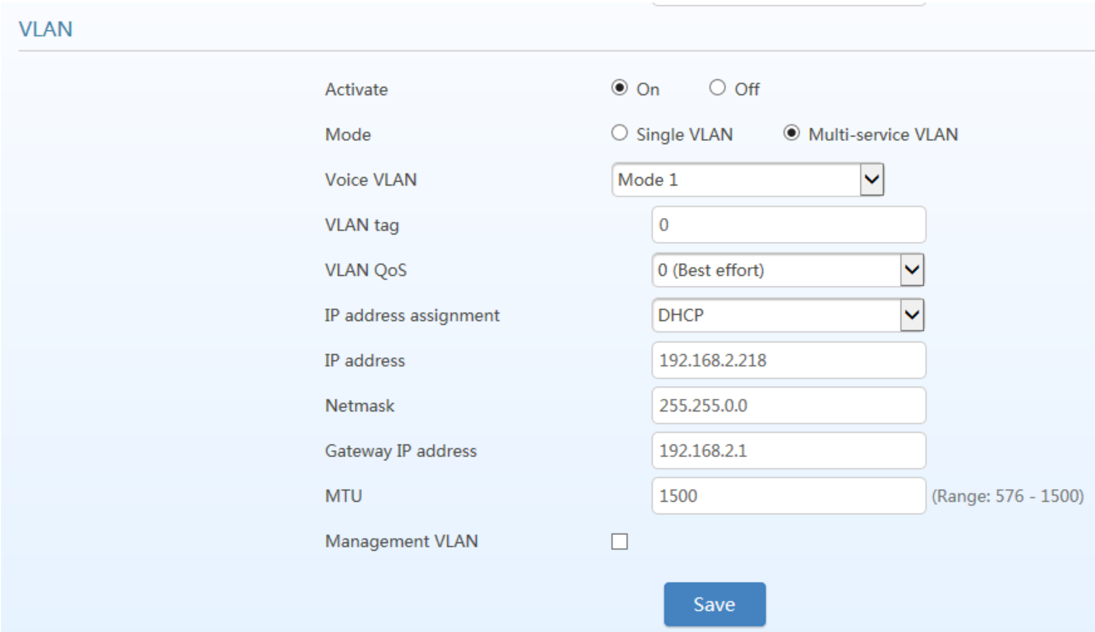
- **Mode1 - Signaling (SIP) and media stream (RTP/T.38) are on the same VLAN**

Note

In this mode, the voice VLAN can be configured with a separate IP address.

On the web interface, click **Network**, and ensure that the VLAN function is set to **On** and **Mode** is set to **Multi-service VLAN**. Select **Mode 1** for **Voice VLAN**, enter the VLAN tag, and specify network information such as IP address.

Figure 3-65 Configuring Voice VLAN to Work in Mode 1



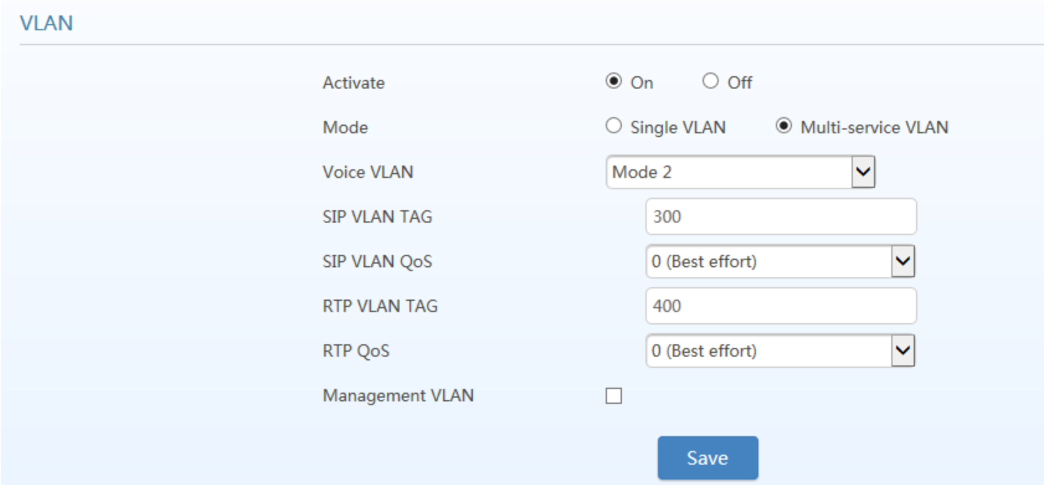
- **Mode2 - Signaling (SIP) and media stream (RTP/T.38) are divided into different VLANs**

Note

In this mode, the voice VLAN cannot be configured with a separate address but shares the IP address of the VLAN interface of the device.

On the web interface, click **Basic** > **VLAN**, and ensure that the VLAN function is set to **On**, and **Mode** is set to **Multi-service VLAN.** Select **Mode 2** for **Voice VLAN**, and specify VLAN tags for SIP and RTP/T.38.

Figure 3-66 **Configuring Voice VLAN to Work in Mode 2**

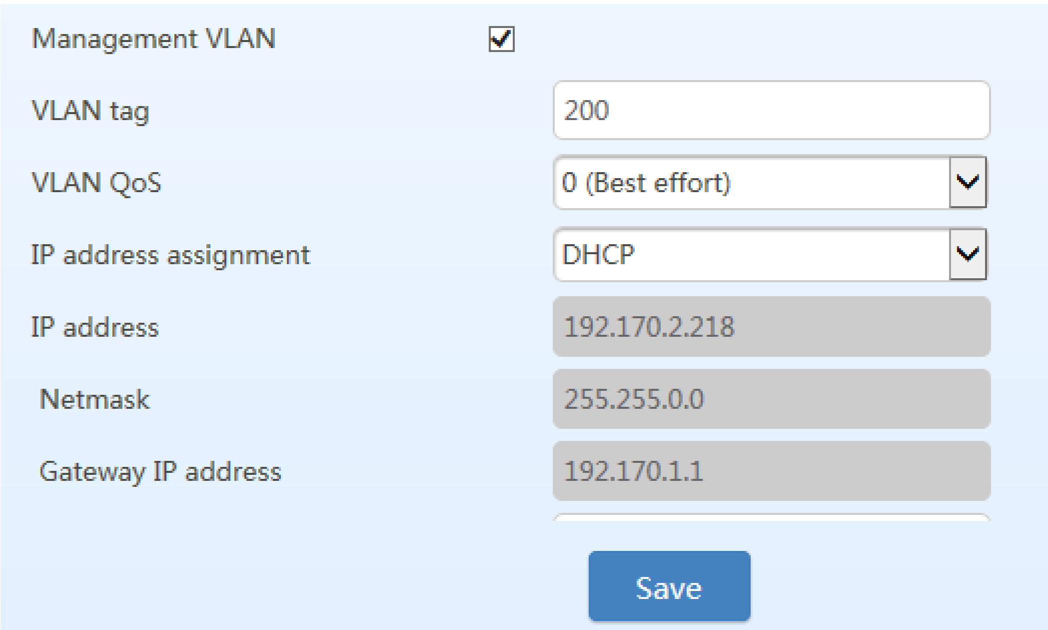


Configuring Management VLAN

The device includes, VLAN tags configured in the management VLAN: HTTP, Telnet, TR069, and SNMP, in data packets of the four service types.

On the web interface, click **Basic** > **VLAN**, and ensure that the VLAN function is set to **On** and **Mode** is set to **Multi-service VLAN**. Select **Management VLAN**, set the VLAN tag of the management service, and specify network information such as **IP address**.

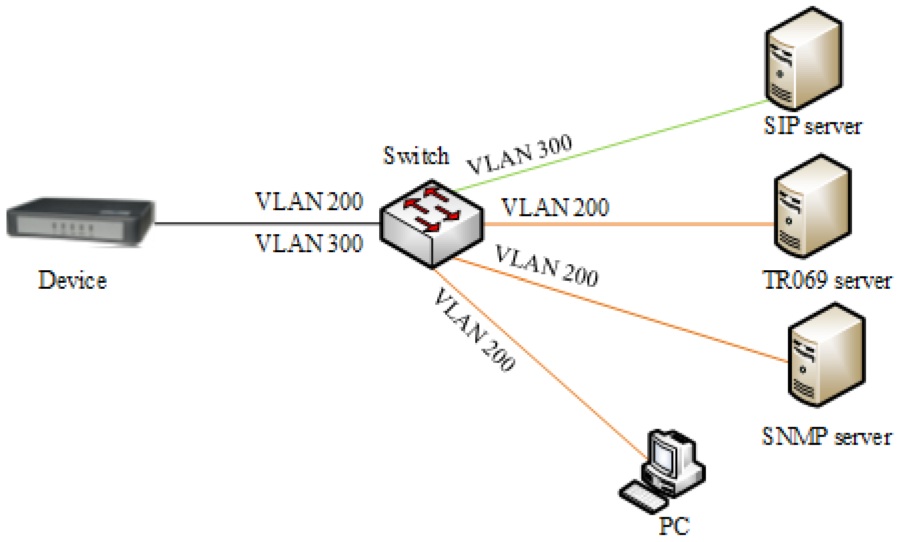
Figure 3-67 **Configuring Management VLAN**



Example of Multi-service VLAN

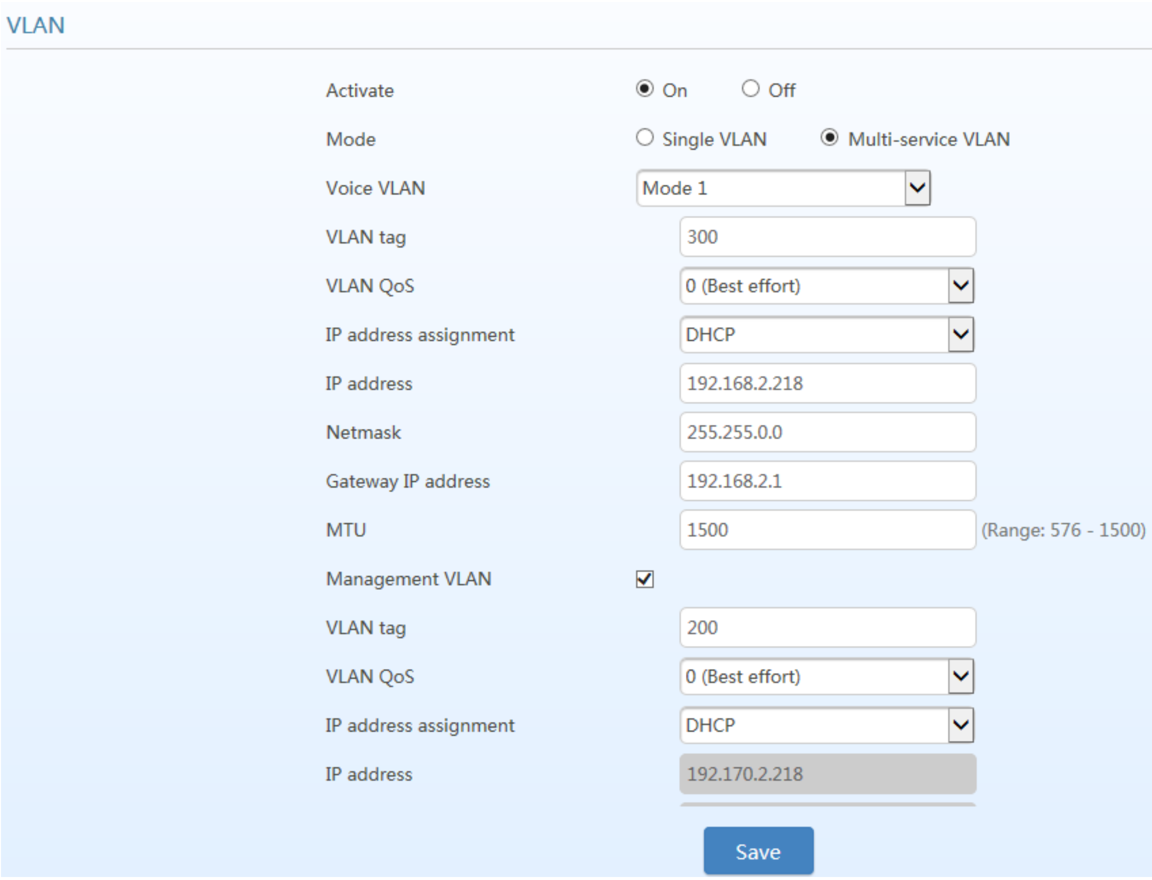
Figure 3-68 shows the network environment. The ports for connecting the switch and HX4 are added to VLAN 200 and VLAN 300. The port for connecting the switch and SIP server is added to VLAN 300. The ports for connecting the switch to the PC (used for managing HX4), TR069 server, and SNMP server are added to VLAN 200.

Figure 3-68 Network environment



1. Configure multi-service VLAN on the HX4 device: the voice VLAN uses mode 1, the VLAN tag is 300, the VLAN tag of the management VLAN is 200, and the IP address is obtained from the corresponding VLAN network using DHCP. As shown in Figure 3-69.

Figure 3-69 Configuring Multi-service VLAN



2. Restart the device for the VLAN to take effect.
3. Use the PC belonging to VLAN 200 to log in to the web page. On the Basic > Status page, the IP address of each interface of the device can be viewed. As shown in Figure 3-70. From top to bottom: IP address of the device physical network port, IP address of the management VLAN, and IP address of the voice VLAN.

Figure 3-70 IP Addresses of the Device in Multi-service VLAN

4. Enable the device to register with the SIP server and call an extension number on the SIP server.

Check that VLAN tag 300 configured in the voice VLAN is carried in the SIP packet and RTP packet.

Figure 3-71 SIP Data Packet Carrying VLAN Tag of the Voice VLAN in the Multi-service VLAN Mode

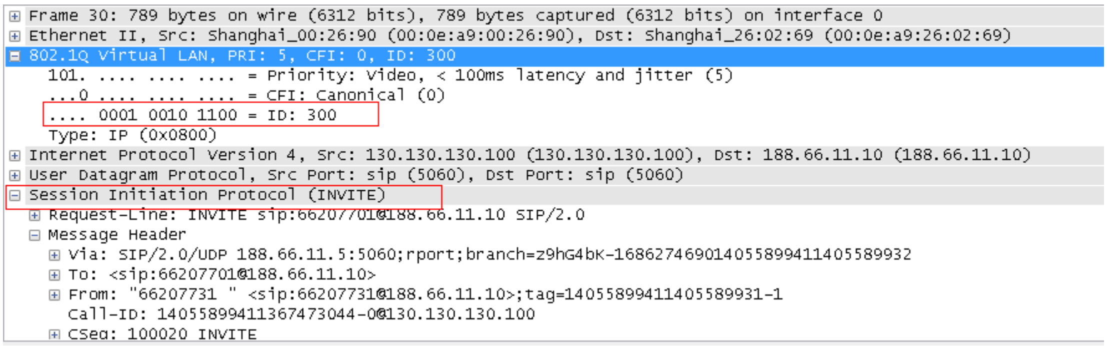
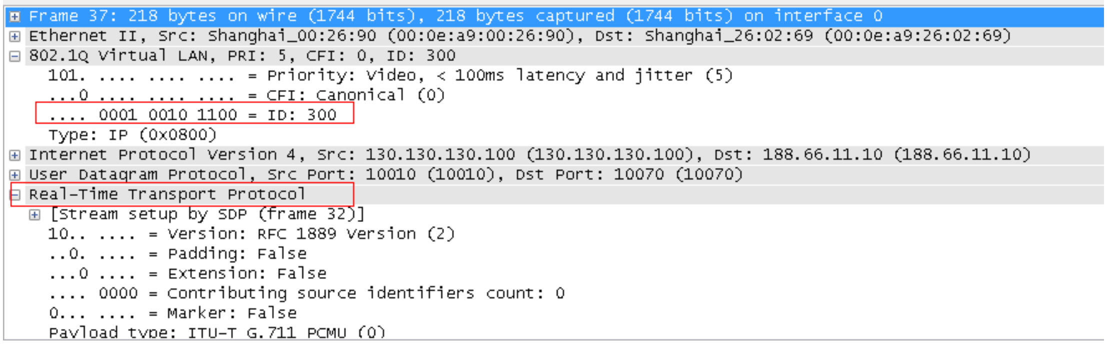
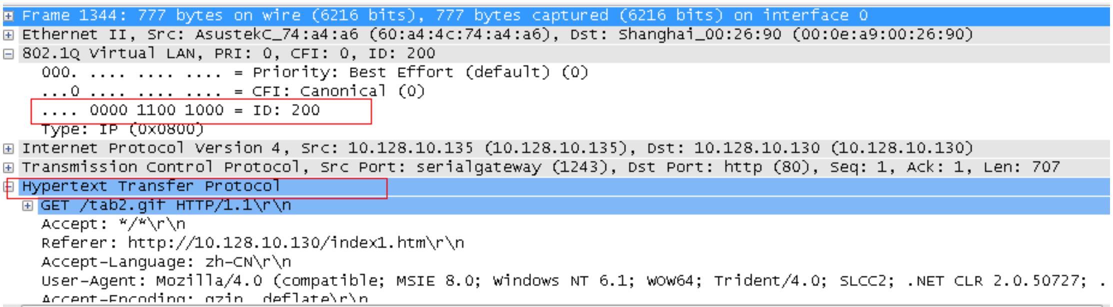


Figure 3-72 RTP Data Packet Carrying VLAN Tag of the Voice VLAN in the Multi-service VLAN Mode



5. Check that tag 200 of the management VLAN is carried in the HTTP packet in the PC management HX4E/MX8A Web GUI.

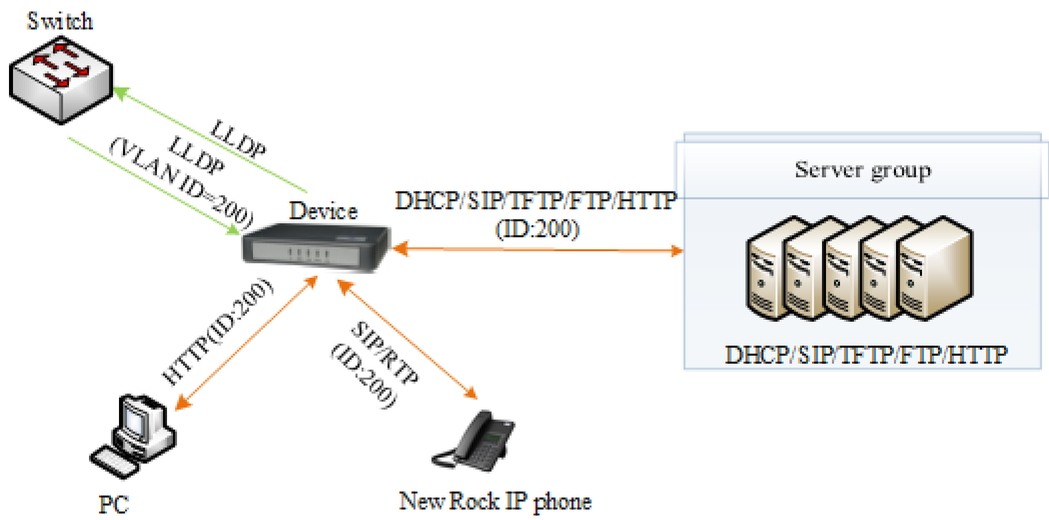
Figure 3-73 RTP Data Packet Carrying VLAN Tag of the Management VLAN in the Multi-service VLAN Mode



3.2 Automatic Configuration

3.2.1 Handling Process for Automatically Enabling VLAN

Figure 3-74 System Composition



The process consists of the following steps:

The device periodically sends an LLDP message to notify the switch the device information. The sending interval is modifiable on the GUI interface. See Table 2-4.

At the same time, the device receives an LLDP message from the switch, and parses VLAN ID, Priority, and DSCP fields.

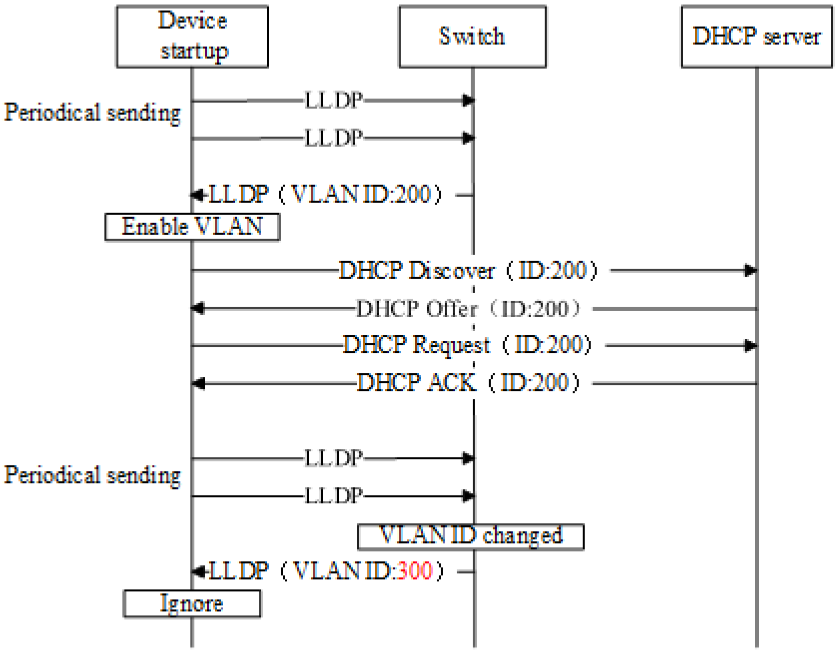
- If the message carries a VLAN ID, the device enables the VLAN, adds VLAN information to the next messages to be sent, and obtains network information such as an IP address via DHCP.

  If the VLAN is also manually enabled on the GUI interface, its VLAN information will be replaced by the information that the device has obtained from the LLDP message.
- If the message does not carry a VLAN ID, the device checks whether the VLAN is manually enabled. If the VLAN is manually enabled, the device uses the VLAN information configured manually; otherwise, the device enters the non-VLAN communication status.

- **Handling Procedure When the LLDP Message Carries a VLAN ID**

The device detects whether the LLDP message carries a VLAN ID upon startup only. Once a VLAN ID is detected, the device enables the VLAN, adds VLAN information to the next messages to be sent, and obtains network information such as an IP address via DHCP. The device ignores any subsequent LLDP message with different VLAN ID. Figure 3-75 shows the handling procedure.

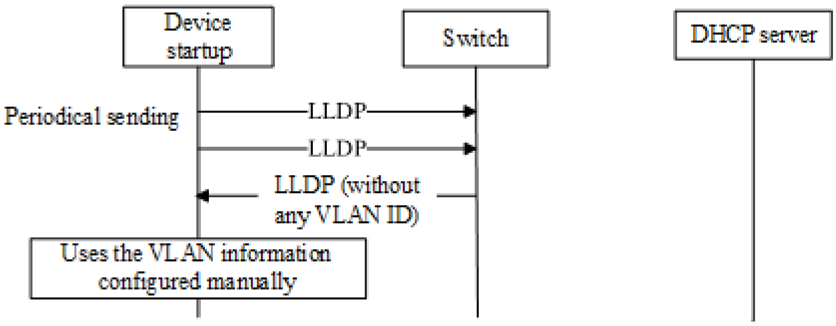
Figure 3-75 Procedure of handling LLDP message carrying a VLAN ID



- Procedure of Handling the LLDP Message with no VLAN ID

During startup period, if the device receives LLDP messages with no VLAN ID, it uses the VLAN information configured manually. Figure 3-76 shows the handling procedure.

Figure 3-76 Procedure of handling the LLDP message with no VLAN ID



3.2.2 Messages

- LLDP Message

Upon receipt of an LLDP message, the device will check if the VLAN ID, Priority, and DSCP fields are included.

Figure 3-77 shows the LLDP message.

Figure 3-77 LLDP Message

```
Link Layer Discovery Protocol
  Chassis Subtype = MAC address, Id: 00:0e:a9:20:33:66
  Port Subtype = MAC address
  Time To Live = 120 sec
  System Name = VoIP-AG
  System Description = VoIP Gateway
  Capabilities
  Management Address
  Port Description = eth0
  IEEE 802.1 - VLAN Name
  IEEE 802.3 - Link Aggregation
  IEEE 802.3 - MAC/PHY Configuration/Status
  TIA TR-41 Committee - Media Capabilities
  TIA TR-41 Committee - Inventory - Software Revision
  TIA TR-41 Committee - Network Policy
    1111 111. .... .... = TLV Type: Organization Specific (127)
    .... ...0 0000 1000 = TLV Length: 8
    Organization Unique Code: 0x0012bb
    Media Subtype: Network Policy (0x02)
    Application Type: Voice (1)
    0... .... .... .... = Policy: Defined
    .1.. .... .... .... = Tagged: Yes
    ...0 0001 1001 000. = VLAN Id: 200
    .... ...1 01.. .... = L2 Priority: 5
    ..10 1110 = DSCP Value: 46
  End of LLDPDU
```

- **Sent Message with a VLAN ID**

After obtaining a VLAN ID from the LLDP message, the device adds the VLAN information to the Ethernet frame headers of all messages to be sent. In addition, the device adds a DSCP value to the RTP message. Figure 3-78 shows the sent message with a VLAN ID.

Figure 3-78 Adding a VLAN ID to the message to be sent

```
Frame 41: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
Ethernet II, Src: Shanghai_00:26:90 (00:0e:a9:00:26:90), Dst: Shanghai_05:14:07 (00:0e:a9:05:14:07)
802.1Q Virtual LAN, PRI: 5, CFI: 0, ID: 200
  101. .... .... .... = Priority: Video, < 100ms latency and jitter (5)
  ...0 .... .... .... = CFI: Canonical (0)
  .... 0000 1100 1000 = ID: 200
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.128.10.173 (10.128.10.173), Dst: 10.128.88.120 (10.128.88.120)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (0x2e)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 200
  Identification: 0x0000 (0)
  Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
```

4 Appendix: High availability configuration

For configuration details, see: http://www.newrocktech.com/Files/MX Gateway High Reliability Configuration Manual.pdf.

Note: If the link is unavailable, for to New Rock's official website: http://newrocktech.com to obtain the file from **support** > **support**.

5 Appendix: Auto provisioning configuration

MX8A/HX4E series voice gateways support auto provisioning, which allows users to remote and central management of gateway configuration and firmware upgrades.

In this mode, users manage and store firmware upgrade packages and gateway configuration files on an automatic configuration server (ACS), and the gateway accesses the ACS when the gateway is powered on, or accesses the ACS periodically according to configuration; then automatically downloads the latest firmware package or configuration files.

The auto provisioning of the gateway supports the following functions:

- Configuring all gateways or upgrading the firmware of all gateways, or selectively upgrading certain gateways
- Automatically updating all gateway parameters
- Supporting TFTP, FTP, or HTTP mode
- Supporting auto provisioning and local management through web services
- Obtaining the address of the ACS from DHCP option 66 or by manual configuration

Auto provisioning features the following advantages:

- Supports highly-efficient and low-cost deployment, management, and maintenance of gateways on a large scale
- Provides configuration file backup
- Enables centralized management of configuration files to enhance account information security

For configuration details, see: http://newrocktech.com/Files/MX%20Gateway%20Auto%20Provisioning%20Configuration%20Manual.pdf.

Note: If the link is unavailable, go to New Rock's official website: http://newrocktech.com to obtain the file from **Support** > **Download**.