

New Rock Technologies, Inc.

LS20

Administrator Manual

<http://www.newrocktech.com>

Document Version: 202001



Amendment Records

Document Rev. 01 (January, 2020)

Copyright © 2020 New Rock Technologies, Inc. All Rights Reserved.

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

Manual Description

This manual is applicable to LS20.

Contents

Amendment Records	2
Manual Description	3
Contents	4
Contents of Figures.....	7
Contents of Tables	9
1 Overview.....	11
1.1 Introduction.....	11
1.2 Equipment Structure.....	11
1.3 Accessing the Device	14
1.3.1 Connection.....	14
1.3.2 Log in to the Web GUI	14
1.4 Web GUI Overview.....	16
1.5 Network Configuration.....	18
1.5.1 Network Settings.....	18
1.5.2 DNS	19
1.5.3 STUN (RFC3489)	20
1.5.4 802.1X.....	21
1.5.5 4G	22
1.5.6 VPN.....	23
2 Features.....	26
2.1 Auto Attendant.....	26
2.1.1 Configuring Auto Attendant	26
2.1.2 Creating new audio files.....	27
2.1.3 Creating Multi-level IVR	29
2.2 Operators/Receptionists	34
2.3 Trunk	36
2.3.1 Analog trunks	36
2.3.2 IP Trunk	38
2.3.3 Backup SIP Proxy Server Settings	45
2.3.4 IMS.....	46
2.4 Configuring Extensions	47
2.4.1 Analog extensions.....	47
2.4.2 IP Extensions	50
2.4.3 IP Trusted Authentication.....	51
2.4.4 Sharing extension	51
2.5 Extension Features	52
2.5.1 Basic Functions.....	52
2.5.2 Making Outbound Calls.....	55
2.5.3 IP table.....	57
2.5.4 Hunt Group	59
2.5.5 LS20Group Call Pickup.....	60

2.5.6 Call Pickup	62
2.5.7 Three-way Calling	62
2.5.8 Call Parking.....	62
2.5.9 DID.....	62
2.5.10 Feature Access Codes.....	63
2.6 Local Survival (LS)	63
2.7 Recording and Voicemail	65
2.7.1 Recording.....	65
2.7.2 Voicemail	68
2.8 FoIP	71
2.9 System Settings	72
2.9.1 Built-in Storage Management	72
2.9.2 Work schedule	73
2.9.3 CRBT	74
2.9.4 Music on Hold	75
2.9.5 Time	76
2.9.6 Routing Table.....	77
2.9.7 Dialed Number Detection and Digit Map.....	83
2.9.8 Call Progress Tone	84
2.9.9 SIP Advanced Configuration.....	86
2.9.10 DTMF	88
2.9.11 Media	88
2.9.12 Call Detail Record (CDR).....	90
2.9.13 SIP Transmission Mode.....	90
2.9.14 Auto Provisioning	91
2.9.15 TR069	93
2.9.16 Ping Diagnosis.....	94
2.9.17 Voice prompt packages (system voice prompt files).....	94
2.10 Security management	97
2.10.1 Access list	97
2.10.2 Brute Force Login Prevention	98
2.10.3 ACL-based Traffic Filtering	100
2.10.4 Packet Rate Limiting Based Dynamic Blacklisting	101
2.10.5 Change Password.....	103
2.10.6 SSH.....	103
2.10.7 Ping Blocking	104
2.10.8 Web Management.....	104
2.10.9 Voice Security	105
2.11 Maintenance.....	106
2.11.1 Upgrading	106
2.11.2 Configuration Maintenance	107
2.11.3 Rebooting.....	108
2.11.4 Port Capture.....	108
2.11.5 Ethereal Capture.....	109
2.11.6 Log Management	109
2.11.7 Runtime log.....	111
2.12 View Runtime Information	112
2.12.1 Running Status	112
2.12.2 Alarm.....	112

2.12.3 Product Information.....	113
2.12.4 Call Messages	114
3 FAQs	114
3.1 Incoming Call Number is Not Displayed.....	114
3.2 IP Trunk Registration Fails	115
3.3 IP Network Connection Fails	115
3.4 Analog Extension Does Not Ring	116
3.5 Incorrect Date is Displayed on the Phone	116
3.6 Low Volume on an Extension.....	116
3.7 Crosstalk on an Analog Extension	117
3.8 Can I Press the R Key on an Analog Extension?.....	117
3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?.....	117
3.10 What to Do When the Analog Trunk is Abnormal.....	118
4 Making an OpenVPN Client Certification	119
Appendix A: Registering a SIP Terminal to LS20	122
SIP Phone	122
Softphone	123
Appendix B:	126

Contents of Figures

Figure 1-1 LS20 front panel.....	12
Figure 1-2 LS20 back panel	13
Figure 1-3 RJ45 to RS232 serial cable	14
Figure 1-4 USB to RS232 converter cable	14
Figure 1-5 Diagram for proper connection	14
Figure 1-6 Login interface	15
Figure 1-7 Web GUI layout.....	17
Figure 1-8 Network configuration interface	18
Figure 1-9 DNS server configuration interface	19
Figure 1-10 STUN configuration interface.....	20
Figure 1-11 802.1X configuration interface	22
Figure 1-12 VPN configuration interface	23
Figure 1-13 VPN configuration interface	24
Figure 2-1 Auto attendance interface	27
Figure 2-2 Text-to-greeting conversion interface	28
Figure 2-3 Audio file interface	28
Figure 2-4 Interface to upload greetings	29
Figure 2-5 IVR interface	30
Figure 2-6 IVR1 screenshot	31
Figure 2-7 IVR2-1screenshot	32
Figure 2-8 IVR2-2screenshot	34
Figure 2-9 Auto attendant configuration interface	35
Figure 2-10 Analog trunk configuration interface	36
Figure 2-11 Analog trunk advanced configuration interface	37
Figure 2-12 IP trunk configuration interface	39
Figure 2-13 IP trunk configuration interface	42
Figure 2-14 IP trunk registrar interface.....	43
Figure 2-15 Secondary SIP proxy server interface	45
Figure 2-16 IMS configuration interface	47
Figure 2-17 Analog extension configuration interface	48
Figure 2-18 Analog extension advanced configuration interface	49
Figure 2-19 IP extension configuration interface	50
Figure 2-20 IP authentication interface	51
Figure 2-21 Interface of extension features.....	52
Figure 2-22 Outbound dialing rule interface	56
Figure 2-23 IP table configuration interface	58
Figure 2-24 Hunt group configuration interface	59
Figure 2-25 Group configuration interface.....	61
Figure 2-26 Group interface	61
Figure 2-27 DID configuration interface	62
Figure 2-28 Feature access codes interface	63
Figure 2-29 Remote recording configuration interface	65
Figure 2-30 Extension recording configuration interface	66
Figure 2-31 USB recording configuration interface	67
Figure 2-32 Extension recording interface	67
Figure 2-33 Voicemail configuration interface	69

Figure 2-34 FAX configuration interface.....	71
Figure 2-35 Storage interface.....	73
Figure 2-36 Work schedule interface	73
Figure 2-37 Time plan details.....	74
Figure 2-38 CRBT file uploading interface	75
Figure 2-39 Music on hold configuration interface	76
Figure 2-40 System time configuration interface.....	76
Figure 2-41 Routing table configuration interface (number transformation).....	77
Figure 2-42 Routing table configuration interface- Limit the call duration	79
Figure 2-43 Dialing interface	83
Figure 2-44 Call progress tone interface	85
Figure 2-45 SIP related configuration interface.....	86
Figure 2-46 DTMF interface	88
Figure 2-47 Media configuration interface.....	89
Figure 2-48 CDR server configuration interface.....	90
Figure 2-49 SIP transmission mode configuration interface.....	91
Figure 2-50 Auto provision interface	92
Figure 2-51 TR069 interface	93
Figure 2-52 Ping diagnosis interface.....	94
Figure 2-53 Voice prompt packages interface.....	94
Figure 2-54 Audio file configuration interface.....	95
Figure 2-55 Whitelist interface.....	98
Figure 2-56 Brute Force Login Prevention (Login Retry Lockout) Configuration Interface	99
Figure 2-57 Brute Force Login Prevention (Lockout IP Addresses) Interface.....	99
Figure 2-58 Static Defense Configuration Interface	100
Figure 2-59 Dynamic Defense Configuration Interface	101
Figure 2-60 Dynamic Defense (Blocked IP Addresses) Interface	102
Figure 2-61 Password interface	103
Figure 2-62 SSH configuration interface	104
Figure 2-63 Ping blocking/unblocking interface.....	104
Figure 2-64 Web management interface.....	105
Figure 2-65 Voice security interface	105
Figure 2-66 Data importing interface.....	107
Figure 2-67 Data exporting interface.....	108
Figure 2-68 Restore factory settings interface	108
Figure 2-69 Rebooting interface.....	108
Figure 2-70 Port-capture interface	109
Figure 2-71 Ethereal interface	109
Figure 2-72 Running log interface.....	111
Figure 2-73 Running status interface	112
Figure 2-74 Alarm interface.....	112
Figure 2-75 Product information interface	113
Figure 2-76 Call message interface	114
Figure 4-1 SIP Phone registration interface	122
Figure 4-2 X-Lite login interface	124
Figure 4-3 X-Lite registration interface	125
Figure 4-4 Schematic diagram of the subscriber line connection.....	126

Contents of Tables

Table 1-1 LS20 product models	11
Table 1-2 LS20 indicator status	12
Table 1-3 LS20 port description	13
Table 1-4 Login parameters	16
Table 1-5 Web management interface layout	17
Table 1-6 Network parameters	18
Table 1-7 DNS server parameters	20
Table 1-8 STUN parameters	20
Table 1-9 802.1X parameter description	22
Table 1-10 4G parameter description	23
Table 1-11 VPN parameter description	24
Table 2-1 Auto attendant parameters	27
Table 2-2 Default greeting files	28
Table 2-3 Auto attendant parameters	35
Table 2-4 Analog trunk parameters	36
Table 2-5 Analog trunk advanced parameters	38
Table 2-6 IP trunk registration parameters	39
Table 2-7 IP trunk parameters	42
Table 2-8 IP trunk registration parameters	44
Table 2-9 Secondary SIP proxy server parameters	45
Table 2-10 IMS parameters	47
Table 2-11 Analog extension parameters	48
Table 2-12 Analog extension advanced parameters	49
Table 2-13 IP extension parameters	50
Table 2-14 Extension basic features	52
Table 2-15 Outbound dialing rule parameters	56
Table 2-16 IP table parameters	58
Table 2-17 Hunt group parameters	59
Table 2-18 Managing recorded files	67
Table 2-19 Voice mailbox sending server parameters	70
Table 2-20 Managing message files	70
Table 2-21 FAX parameters	71
Table 2-22 Work schedule parameter description	73
Table 2-23 System time parameters	76
Table 2-24 Description of a digit map	84
Table 2-25 Call progress tone parameters	85
Table 2-26 Examples of customized tone	85
Table 2-27 SIP related parameters	86
Table 2-28 DTMF parameters	88
Table 2-29 Media parameters	89
Table 2-30 SIP transmission mode parameters	91
Table 2-31 Auto provision parameters	92
Table 2-32 TR069 parameters	93
Table 2-33 System voice prompt files	95
Table 2-34 Access list parameters	98
Table 2-35 Login Retry Lockout Parameters	99

Table 2-36 Brute Force Login Prevention (Lockout IP Addresses) Information	99
Table 2-37 Static Defense Configuration Parameters	100
Table 2-38 Dynamic Defense (Rule Configuration) Parameters	101
Table 2-39 Dynamic Defense (Blocked IP Addresses) Information	102
Table 2-40 Subsequent choices for moving the Blocked IP Addresses to static defense.....	103
Table 2-41 Access list parameters	104
Table 2-42 Web management parameters.....	105
Table 2-43 Voice security parameters.....	106
Table 2-44 System-reboot interface	108
Table 2-45 Log-management parameters.....	110
Table 2-46 Runtime log parameters.....	111
Table 2-47 Classification of alarm messages.....	113
Table 3-1 Solutions to IP trunk registration failures.....	115
Table 3-2 Solutions to low voice volume on an extension.....	117
Table 4-1 SIP Phone registration parameters	122
Table 4-2 SIP Phone registration parameters	125
Table 4-3 Pin specifications for the RJ45 socket port	126

1 Overview

1.1 Introduction

With VoIP and cloud communications being fast developed and widely used, enterprises are able to deploy the telephone solution based on distributed PBX communications or cloud/hosted communications networks at a lower cost. To prevent the interruption of calling and call-related services when headquarters server or cloud/hosted server disconnects, New Rock LS20 border appliance is designed to be deployed at local offices or branches to handle the calls instead of the disconnected server. After connection recovers, the calling services will be switched to the headquarters server or cloud/hosted server again.

Advantages

- ☐ Connection to PSTN by FXO ports, or connection to IP trunk by 4G/5G
- ☐ PSTN failover upon network or network failure
- ☐ Rich local voice features: call recording, high speed fax, video call, 3-way calling
- ☐ Enhanced security: TLS/SRTP encryption, white/black list, brute force login prevention etc.
- ☐ Configuration and management with Web GUI or network management system

1.2 Equipment Structure

Table 1-1 LS20 product models

Models	Interface Card	Number of Interface Card	Number of FXO Ports	Number of FXS Ports
LS20-4S	401A-4S	1	0	4
LS20-4FXO	401A-4FXO	1	4	0
LS20-2S/2	401A-4S	1	2	2

Figure 1-1 LS20 front panel



Table 1-2 LS20 indicator status

Indicator	Status	Description
PWR (green)	Blinking green	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.
	Blinking red	The device is starting or the Kupdate is upgrading.
	Steady green	An IP address is obtained by WAN interface and the registration of SIP trunk is successful.
	Blinking alternatively between red and green	An IP address is obtained by WAN interface and the registration of SIP trunk is failed.
	Blinking green	An IP address is obtained by WAN interface and no SIP trunk is registered.
USB (green)	Steady green	A USB storage device is inserted properly
	Blinking green	The Internet access via 3G/4G USB dongle is successful**
	Off	The USB device is not detected or the Internet access via 3G/4G USB dongle is failed or not performed**
WAN (green)	Steady green	A WAN connection is established without any service flow.
	Blinking green	A WAN connection is established with service flows.
	Off	WAN interface is disconnected.
PC (green)	Steady green	A link is connected without any service flow.
	Blinking green	A service flow is being transmitted.
	Off	A link is not connected.
VOICE (Green-FXS, yellow-FXO)	Indicates line type and device status:	
	Blinking yellow	The device is starting and the port is an FXO port.
	Blinking green	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.
	Blinking yellow	Ringling of calling in for an analog trunk.
	Steady green	Picking up an analog extension or calling on.
	Blinking green	Ringling of a call coming for an analog extension.
	off	Idle
	Note: The device starts up for approximate 30 s to indicate line type, then indicates running status.	
Button	RST	To restore the device to factory default, press the RST for 3 to 5 seconds and release it when STU turn blinking red. This setting will be valid after rebooting the device.

Figure 1-2 LS20 back panel



Table 1-3 LS20 port description

Ports	Description
FXS	The FXS ports (RJ11) are used for connecting analog phones, fax machines or POS machines.
FXO	The FXO ports (RJ11) are used for connecting to the PSTN or another PBX.
PC/WAN	The PC port is used to connect a computer. The WAN port is used to connect the uplink network. Both are 10/100 Mbps Ethernet ports (RJ45). They share one IP address, which, by default, is obtained through DHCP. If no IP address is obtained, 192.168.2.218 is used by default, and you can change it on Basic > Network page.
USB	The USB port is used for connecting the USB device. Note: The device has 16 GB internal flash storage.
CON	The console port is used for local management and testing. Note: The console port is used for local management and testing. A PC 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 port, please use the cable together with a USB to an RS232 converter cable. Cables are shown below in Figure 1-3 and Figure 1-4. Generally, the console port is not used.
RST	The reset button restores factory default settings.
PWR	The power interface is used for connecting the power supply. Note: Please use the power adapter provided with the device.
Grounding terminal	The grounding terminal is used to connect the grounding cable.

Figure 1-3 RJ45 to RS232 serial cable



Figure 1-4 USB to RS232 converter cable

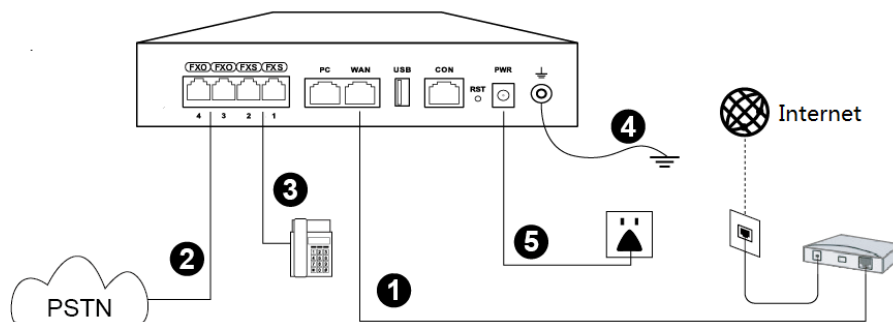


1.3 Accessing the Device

1.3.1 Connection

Place the device on an even surface, or secure it in a rack, and then follow these steps to connect:

Figure 1-5 Diagram for proper connection



Step 1 Connect the WAN port of the device to the Internet.

Step 2 Connect the FXO port of the device to the telephone line provided by a telecom operator or an extension line from another PBX.

Step 3 Connect the FXS port to an analog phone or a fax machine.

Step 4 Connect the grounding cable: connect the end with a smaller diameter to the device, and connect the other end to a ground bar.

Step 5 Connect the power supply.

1.3.2 Log in to the Web GUI

Step 1 Use a CAT5 cable to connect the PC port to a PC.

Step 2 Obtain the IP address of the device.

By default, the IP address of LS20 is automatically obtained by DHCP.

The IP address can be obtained by using these methods:

- FXS device and FXS + FXO device: dial "###" to obtain device IP address by an analog telephone connected to the FXS port after the equipment is powered on.
- FXO device: obtain device IP address via New Rock's Finder software.
You can get the "Finder" software by visiting: <http://en.newrocktech.com/show/594.html>

Additional information:

- (1) To assign a static IP address for your device, dial *90 and configure your network parameters as the following example on an analog phone:

192*168*2*218#255*255*0*0#192*168*2*1#0#

IP address	Subnet mask	Default gateway

- (2) To obtain an IP address via DHCP, dial *90###1# and reboot the device after you hear "The feature is now activated".

Step 3 Make sure that the PC and the device are on the same network segment.

Step 4 Enter the device IP address in the browser address bar (e.g. 192.168.2.240);

Step 5 You can enter the login interface for device configuration by selecting your role and entering a password on the login interface. The default administrator password is **admin**.



Note

- The device is only allowed to access using HTTPS. Since the factory default certificate is used, a prompt like "There is a problem with this website's security certificate" may occur. Click **Continue to this website** to access the login page.
- To log out, please click the **Logout** button on the upper right corner instead of closing the browser tab.

Figure 1-6 Login interface

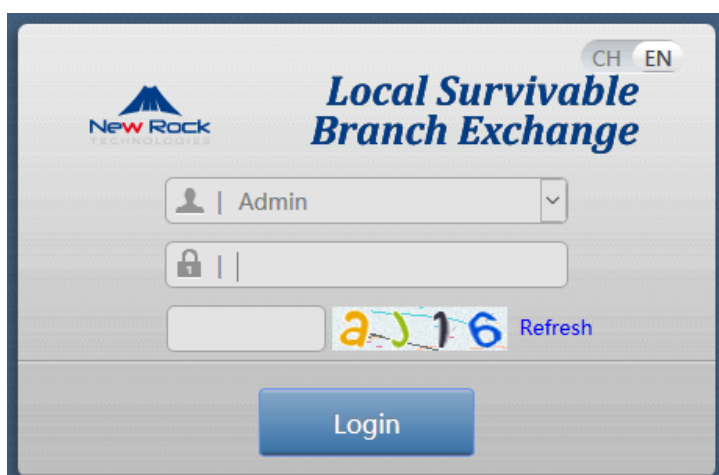


Table 1-4 Login parameters

Item	Description
Language	Select a language.
Role	The Web utility provides two authority levels: □ An administrator is allowed to make changes to any configuration, such as login passwords. After login, "Admin" is displayed on the upper left corner. □ An operator is allowed to browse configuration pages. After login, "Operator" is displayed on the upper left side of the interface. The device allows multiple terminals to log in, if multiple terminals log in with the account Admin at the same time, only one succeeds and others turn to "Viewer" automatically. If there is a logged-in Admin, and you log in by another terminal with the account Admin, you may log out the logged-in Admin forcedly, or not, in which case, you will log in as a Viewer. Note: In the "Viewer" and "Operator" mode, you can only browse certain pages. The pages that cannot be browsed include: Advanced> Security, System tool >Change password, System tool>Software upgrade, System tool >Import data, System tool>Export data. The passwords of SIP trunks, passwords and PINs of extensions also cannot be queried.
Password	The default administrator password is "admin". The default operator password is operator. Please change the default password after the first time logging in to the Web utility to keep it secure. For details, see 2.10.5 Change Password.
CAPTCHA	It is composed by 4 digits and letters. You can click Refresh to change a picture.

1.4 Web GUI Overview

The web GUI includes three areas: System button area, Menu bar, and Configuration area.

Figure 1-7 Web GUI layout

The screenshot displays the LS20 Web GUI. At the top, the header shows 'LS20 Admin' and links for 'Info', 'Feedback', 'Reboot', and 'Logout'. Below this is a main menu bar with tabs: 'Status', 'Basic' (highlighted), 'Extension', 'Trunk', 'LS', 'Application', 'Advanced', 'Security', 'System tool', and 'Log'. Under the 'Basic' tab, there is a sub-menu bar with 'Network' (highlighted), 'Dialing rule', 'Auto attendant', 'IVR', and 'Audio files'. The main content area is titled 'Basic' and contains configuration options for 'Ethernet (WAN)', 'PPPoE', and 'VPN'. The 'Ethernet (WAN)' section includes a 'Host name' field with 'LS20' and radio buttons for 'Obtain an IP address automatically' (selected) and 'Static IP address'. Below this are fields for 'IP address' (192.168.140.38), 'Subnet mask' (255.255.252.0), and 'Default gateway' (192.168.140.1). The 'PPPoE' section has radio buttons for 'Obtain an IP address automatically' (selected) and 'Specified manually'. The 'VPN' section has radio buttons for 'Enable' and 'Disable' (selected). A 'Save' button is located at the bottom right of the configuration area.

Table 1-5 Web management interface layout

Item	Description
1 System button area	Contains buttons such as Reboot, Logout, and Product information; and displays the identity of the current login user.
2 Menu bar	Displays submenus for your selection when the mouse pointer is moved onto a menu. The selection result is displayed in the configuration area.
3 Configuration area	View or modify or view configuration.

1.5 Network Configuration

1.5.1 Network Settings

Go to **Basic > Network** to set IP address according to the installed network environment.

By default, network ports PC and WAN are switch ports that share the same IP address configured for WAN on the **Basic>Network** page. By default the WAN IP address is obtained through DHCP. If no IP address is obtained, 192.168.2.218 is used by default..

The PC port has two work modes, for details, see Figure 1-8.

Figure 1-8 Network configuration interface

The screenshot shows the 'Network' configuration page under the 'Basic' tab. The page has a top navigation bar with tabs: Status, Basic, Extension, Trunk, LS, Application, Advanced, Security, System tool, and Log. Below this is a sub-navigation bar with links: Network, Dialing rule, Auto attendant, IVR, and Audio files. The main content area is divided into sections: Default gateway (192.168.120.1, Specified manually), Primary DNS server (114.114.114.114), Secondary DNS server (114.114.115.115), PPPoE (Disable), VPN (Disable), PC (Disable), and STUN (Switching port). A 'Save' button is at the bottom right.

Table 1-6 Network parameters

Item	Description
WAN	
	Methods for obtaining an IP address. - Static IP address: static IP address is used. - Obtain an IP address automatically: use the dynamic host configuration protocol (DHCP) to obtain IP addresses and other network parameters. - PPPoE: use PPPoE to obtain IP addresses and other network parameters.
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.

Item	Description
Subnet mask	The subnet mask is used with an IP address. When the gateway 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 the LAN gateway. When the gateway obtains an IP address through DHCP, the system will display the LAN gateway address automatically obtained through DHCP. It has no default value.
PC	
Mode	You can set to either of the following two modes: ☐ Switching port (default mode): The PC port and WAN port are switching ports and share the IP address configured for the WAN. ☐ Specialized port for SIP trunks (IP address configurable): This mode is generally used to connect an optical network unit (ONU) and is connected to the dedicated voice network of the carrier. If the dedicated voice network also includes cloud services, automatic management, call detail record (CDR) servers, API applications, and recording servers, corresponding options should be selected to use this network port.
IP address	Enter the IP address of the PC port.
Subnet mask	Enter the subnet mask of the PC port.
Default gateway	Enter the gateway IP address of the LAN in which the PC port is located.

1.5.2 DNS

When the device accesses a domain name, the device first requests the DNS server to translate the domain name to an IP address. The DNS server needs to be configured.

Step 1 Go to the **Basic>Network** to configure DNS server.

Figure 1-9 DNS server configuration interface

The screenshot displays the 'Basic' configuration tab for the 'Network' section. The 'Ethernet (WAN)' settings are configured with 'Static IP address' selected. The IP address field contains '192 . 168 . 2 . 218', the Subnet mask is '255 . 255 . 0 . 0', the Default gateway is '192 . 168 . 2 . 1', the Primary DNS server is '192 . 168 . 2 . 1', and the Secondary DNS server is '. . .'. The 'PPPoE' section has 'Disable' selected, and the 'VPN' section also has 'Disable' selected. A 'Save' button is located at the bottom right of the configuration area.

Table 1-7 DNS server parameters

Item	Description
Obtained automatically	The device automatically obtains the DNS server address by using DHCP or PPPoE. This option can be selected only when the network connection mode is set to DHCP or PPPoE .
Specified manually	Use the DNS server addresses specified manually. It is the default value.
Primary DNS Server	If Specified manually is selected, the network IP address of the Primary DNS server must be entered, and there is no default value. For It is 114.114.114.114 by default.
Secondary DNS Server	If Specified manually is selected, the network IP address of the Secondary DNS server can be entered, and there is no default value. It is 114.114.115.115 by default.

1.5.3 STUN (RFC3489)

Go to **Basic > Network**, and set related parameters to obtain the public IP address of the front-end router by using the STUN function.

Figure 1-10 STUN configuration interface

The screenshot displays the STUN configuration interface. At the top, there are tabs for 'Status', 'Basic', 'Extension', 'Trunk', 'LS', 'Application', 'Advanced', 'Security', 'System tool', and 'Log'. Under the 'Basic' tab, there are sub-tabs for 'Network', 'Dialing rule', 'Auto attendant', 'IVR', and 'Audio files'. The 'Network' sub-tab is active. Below the sub-tabs, there are sections for 'PC', 'STUN', and '802.1X'. The 'STUN' section is expanded, showing the following configuration options:

- STUN**: A radio button selection between 'Enable' (selected) and 'Disable'.
- Server IP address / Name**: A text input field containing 'stun.newrocktech.com'.
- Server port**: A text input field containing '3478'.
- Session interval**: A text input field containing '60', followed by 's (Range: 30 - 65535)'.
- Operations**: Two radio buttons, 'SIP re-registration' (selected) and 'SIP re-registration & NAT address updating'.

A 'Save' button is located at the bottom right of the configuration area.

Table 1-8 STUN parameters

Item	Description
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 enabled by default.
Server IP address / Name	Set the IP address or domain name of the STUN server. The default STUN server is the New Rock STUN server at stun.newrocktech.com.
Server port	Set the port of STUN server. It is 3478 by default.

Item	Description
Session interval	The interval at which the device sends a STUN request ranges from 30 to 65535 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 with the 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.

1.5.4 802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Go to **Basic > Network**, and check the box of 802.1X to enable it.

Figure 1-11 802.1X configuration interface

Server IP address / Name:

Server port:

Session interval: s (Range: 30 - 65535)

Operations: ☒ SIP re-registration ☐ SIP re-registration & NAT address updating

802.1X

Enable: ☒

Identity:

Username:

Password:

4G

☐ Enable ☒ Disable (When enabled, Please reboot the device)

Save

Table 1-9 802.1X parameter description

Item	Description
Enable	Enable 802.1X. By default, it is disabled.
Identity	Input the identity provided by authentication server.
Username	Input the username provided by authentication server.
Password	Input the password provided by authentication server.

1.5.5 4G

LS20 supports to connect with 4G wireless network.

Go to **Basic > Network** and enable 4G.

Figure 1-12 VPN configuration interface

4G status

enable Disable (when enabled, please reboot the device)

4G
0K/s

Current connection

Status 已连接

Received/Sent 0KB/0KB

APN settings

APN

Username

Password

Save

Table 1-10 4G parameter description

Parameter	Description
APN	Enter the access point name.
Username	Enter the username.
Password	Enter the password.

1.5.6 VPN

With a built-in OpenVPN client, the LS20 is ready to be directly connected to the VPN server to avoid the firewall issues and NAT issues of SIP.

Note: The VPN function is only applicable when the SIP trunks of LS20 register to a SIP server in a VPN network.

After login, go to **Basic > Network**, enable VPN function.

Figure 1-13 VPN configuration interface

VPN

☒ Enable ☐ Disable

Accurate device time is necessary for OpenVPN, please verify the current device time or calibrate on [System time](#) page.

OpenVPN client certificate No certificate exists. [Choose File](#) No file chosen [Upload](#)

PC

Mode Switching port

STUN

STUN ☒ Enable ☐ Disable

Server IP address / Name

Server port

Session interval s (Range: 30 - 65535)

[Save](#)

Table 1-11 VPN parameter description

Parameter	Description
VPN	Choose On and click Save to enable VPN function Note: Accurate device time is necessary for OpenVPN, please verify the device time on System tool>System time page.
OpenVPN certificate client	1. Prepare a certificate file whose name should be “client.ovpn”. Please see 4 Making an OpenVPN Client Certification on how to make a certificate file. 2. Choose the certification file “client.ovpn” and click Upload. The certificate information will be listed on Advanced > Cert. page. 3. Restart the device. 4. After the device is restarted, click Basic > Status to view the VPN connection status.

2 Features

2.1 Auto Attendant

2.1.1 Configuring Auto Attendant

Auto Attendant allows callers of inbound calls to be automatically transferred to an extension without the intervention of an operator/receptionist.

LS20 provides two types of auto attendant:

- ☐ An audio file, only allows the callers to reach a live operator by dialing a number, usually “0”, or other extensions by dialing the extension number.

For example:

Thank you for calling. If you know your party's extension, please dial it now. Or, to transfer to an operator, press zero.

- ☐ A multi-level IVR, provides a hierarchical menu structure.

For example:

Thank you for callings, for English, press one, for Chinese, press two. (level-1)

After you press one, you will hear: For sales, press 1, for technical support, press 2. (level-2)

Note: The device allow up to 30 trunks to play greetings at the same time.

Configuring auto-attendant greetings (Global)

By default, every trunk uses auto attendant greetings which can be different for business and non-business hours. If you want to configure the auto attendant for a single trunk, please modify the **Greeting** on **Trunk > Analog trunk** or **Trunk > IP trunk**.

Follow this procedure to configure the auto attendant for all trunks.

Step 1 Go to **Basic > Auto attendant**.

Step 2 Assign time schedule. The default is business hours all.

Step 3 Select desired audio file or IVR for **Business hours** or **Non-business hours** respectively.

Figure 2-1 Auto attendant interface

Table 2-1 Auto attendant parameters

Item	Description
Time schedule	Customize: Set the range of business hours in a week. The hours outside of business hours are non-business hours. Click + to divide one day into up to three business-hour segments. The device will play corresponding greetings to callers of incoming calls according to the preset business hours or non-business hours.
Business hours IVR	Choose an audio file or an IVR name for business hours. By default, the factory default audio file is “welcome” To change it to another audio file, you should prepare the audio file first and upload it, for details, see 2.1.2 Creating new audio files. To change it to a multi-level IVR, please click Add IVR, for details, see 2.1.3 Creating Multi-level IVR . To determine if you have chosen the correct file, click Audit.
Non-business hours IVR	Choose an audio file or an IVR name for non-business hours. By default, the factory default audio file is “offhour”. To change it to another audio file, you should prepare the audio file first and upload it, for details, see 2.1.2 Creating new audio files. To change it to a multi-level IVR, please click Add IVR, for details, see 2.1.3 Creating Multi-level IVR . To determine if you have chosen the correct file, click Audit.

Step 4 Click **Save**.

2.1.2 Creating new audio files

There are two factory default audio files used as the **Auto attendant** greetings:

Table 2-2 Default greeting files

Type	File name	Content
Business hours	welcome	Thank you for calling. If you know your party's extension, please dial it now. Or, to transfer to an operator, press zero.
Non-business hours	offhour	Thank you for calling. Our office is closed. If you know the extension, please dial it now.

To create new audio files, there are three methods can be selected:

- ☐ Text-to-greeting conversion
- ☐ Recording the greeting file on a phone
- ☐ Upload greetings

1) Text-to-greeting conversion

This is a simple way to customize the greetings in Chinese or English with high voice quality. This method is recommended when the device is connected to the Internet.

Follow this procedure:

Step 1 Go to **Basic >Network** page to configure DNS server. For details, see 1.5.2 DNS.

Step 2 Go to **Basic >Audio files >Text-to-greeting conversion** page. Enter the greeting content in English and click **Start**.

Figure 2-2 Text-to-greeting conversion interface

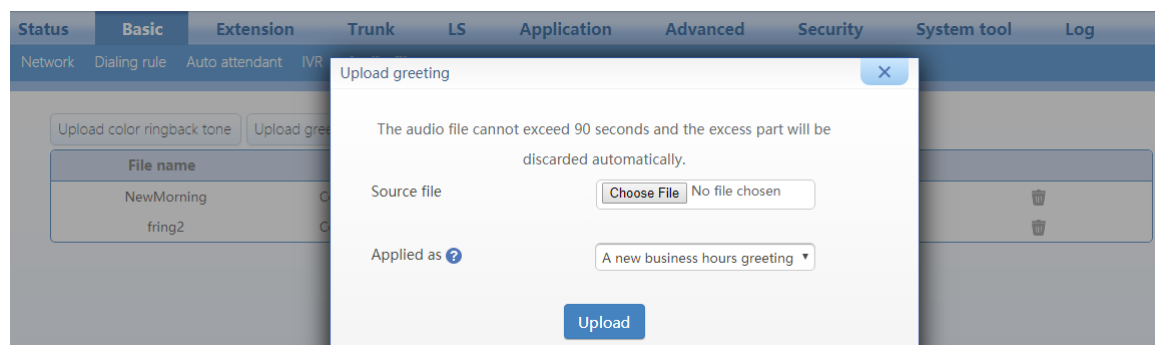
Step 3 You can also audit or delete the saved greetings for business hours or non-business hours.

Figure 2-3 Audio file interface

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
Network	Dialing rule	Auto attendant	IVR	Audio files					
Upload color ringback tone Upload greeting Text-to-greeting conversion									
File name	Type	Music on hold	Audit						
NewMorning	Color ringback tone	☒	Play Delete						
fring2	Color ringback tone	☐	Play Delete						

2) Upload greetings

Step 1 Go to **Basic > Audio files > Uploading greeting**.

Figure 2-4 Interface to upload greetings

Step 2 Click **Choose File** to select the audio files for uploading.

Step 3 Click **Upload**.



Note

- The name of the audio file to be uploaded should begin with "user", and can contain letters, digits or underscores only. You must use a .wav file format.
- The sampling rate of the .wav file can only be 22.050 kHz or 8.000 kHz.

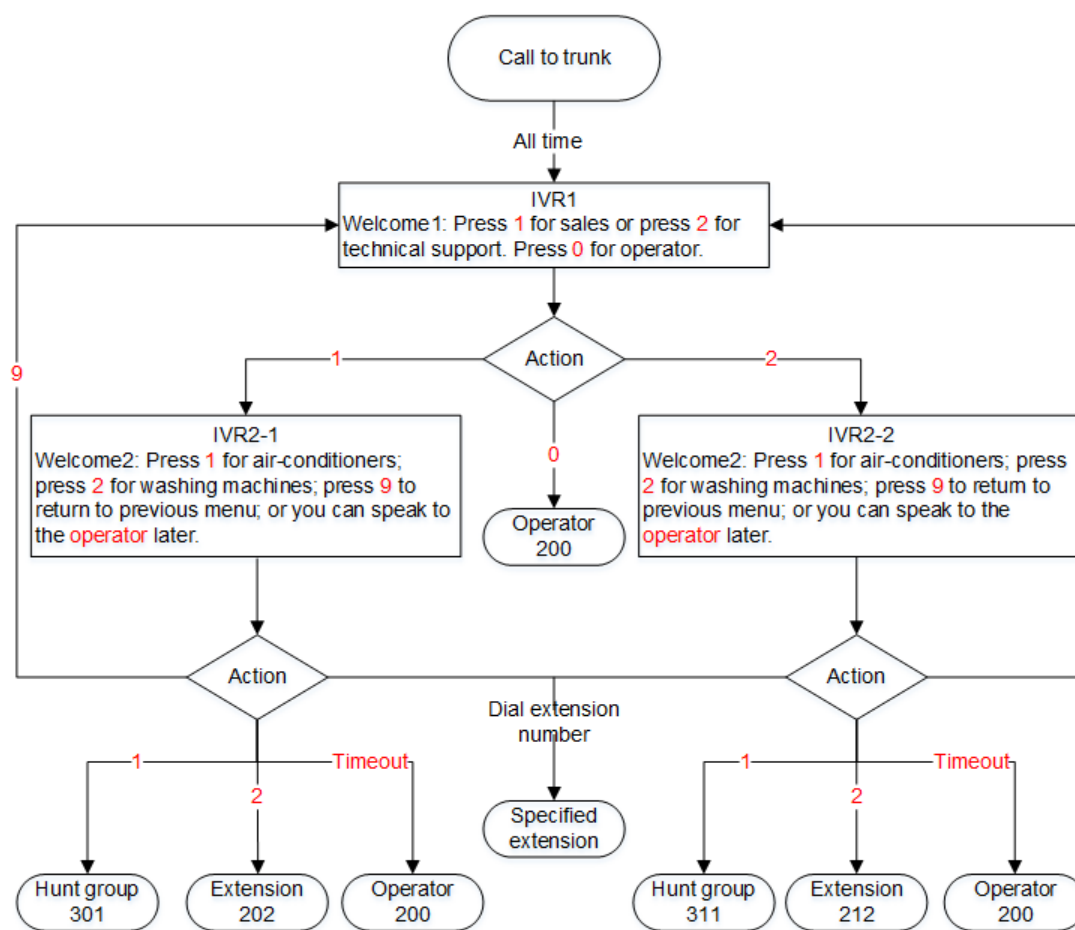
2.1.3 Creating Multi-level IVR

With the multilingual IVR function, caller of incoming call can press a button to choose a language based on the navigation menu.

The following is an example to show how to configure multi-level IVR.

A shopping hotline needs to be able to answer calls 7x24 from customers and its IVR consists of a two-level menu. When users call in, level 1 will guide them to select "sales" or "technical support" and level 2 will guide them to select more specifically from the "sales" and "technical support" menu. Users can also choose to return to the previous menu, transfer to the operator and directly dial an extension number.

Detailed IVR processes are:



Step 1 Prepare audio files "welcome1" and "welcome2". Refer to Creating new audio files.

Step 2 Go to **Basic>Multi-level IVR** page and click **Add** to create IVR1 (level 1), IVR2-1 (level 2) and IVR2-2 (level 2).

Figure 2-5 IVR interface

Status Basic Extension Trunk LS Application Advanced Security System tool Log

Network Dialing rule Auto attendant IVR Audio files

Gray indicates the IVR uses an invalid audio file or voice prompt package, please modify.

Add IVR

Name	Note	Prompt	Language	Prompt repeat count	Dial extension	Dial timeout(s)	Edit	Remove
IVR1	Level1	---	Default	1	☐	3		

 NewMorning
 fring2
 offhour
 welcome

Save

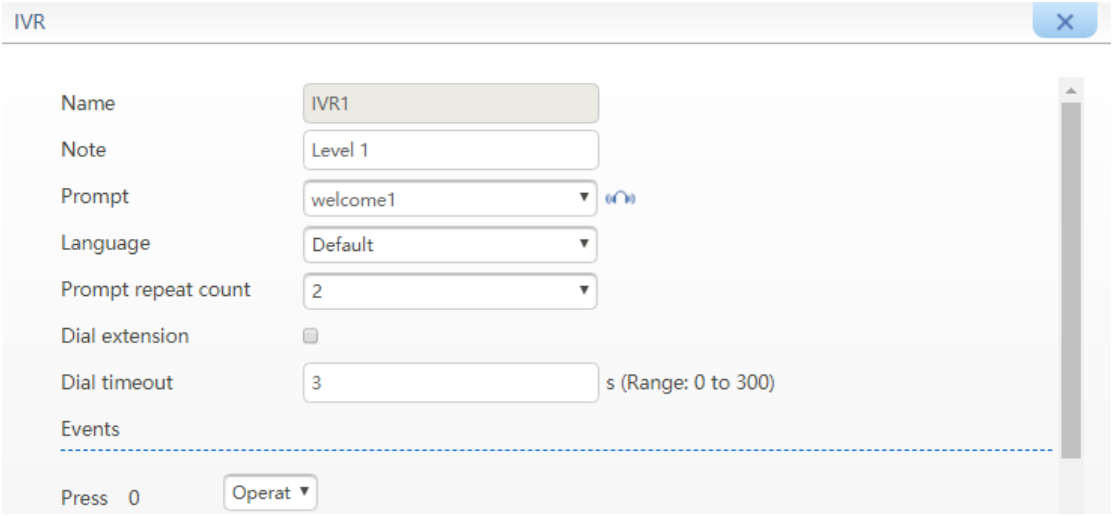
Configuration items	Description
Name	Menu name. English letters, digits, hyphens and underlines are allowed. The length is no more than 20 characters.
Note	Menu description.
Prompt	Choose an audio file. Refer to Creating new audio files if you need prepared audio files.

Configuration items	Description
Language	This applies to multilingual IVR. When it is single language, it remains blank. The default voice prompt package works.
Prompt repeat count	Number of times to play audio files without dialing
Dial extension	Check it to allow callers dial extensions when the current audio files are playing.
Dial timeout	After playing the prompts in the IVR, the LS200G will wait for the DTMF entry within the timeout (in seconds). If no DTMF entry is detected within the timeout, a timeout response defined in the menu tree will be took.
IVR tree	Key options: ☐ 0 to 9,*, #: actions after users press 0 to 9,*or # ☐ No digit timeout: action for no DTMF entry within the timeout after voice prompt are played. ☐ Invalid: action on wrong dialing Actions for key option ☐ Transfer to extensions: Transfer to an extension. Select the extension number from the dropdown list or input a number. Note: If you want to transfer to a target extension of another device in multisite-network scenario, you have to input the extension number. ☐ Transfer to hunt groups: Transfer to a hunt group. Select the group number from the dropdown list. Note that you need to pre-configure hunt groups on Basic>Dialing rule page. ☐ IVR: Transfer to another menu. Select menu name from the dropdown list. ☐ Operator: Transfer to an operator. The operator should be pre-configured on Basic<Auto attendant page.

Step 3 Click **Save**.

Step 4 Click  and set IVR1 according to the screenshot then click **OK**.

Figure 2-6 IVR1 screenshot



IVR

Name: IVR1

Note: Level 1

Prompt: welcome1 

Language: Default

Prompt repeat count: 2

Dial extension: ☐

Dial timeout: 3 s (Range: 0 to 300)

Events: -----

Press 0 Operat ▼

Press 1: IVR (dropdown) IVR2-1 (dropdown) >>

Press 2: IVR (dropdown) IVR2-2 (dropdown) >>

Press 3: -- (dropdown)

Press 4: -- (dropdown)

Press 5: -- (dropdown)

Press 6: -- (dropdown)

Press 7: -- (dropdown)

Press 8: -- (dropdown)

Press 9: -- (dropdown)

Press *: -- (dropdown)

Press #: -- (dropdown)

Press any key: IVR (dropdown) IVR1 (dropdown) >>

Time out: Operat (dropdown)

Ok Cancel

Step 5 Click  and set IVR2-1 according to the screenshot then click **OK**.

Figure 2-7 IVR2-1screenshot

IVR

Name: IVR2-1

Note: Level 2-purchase

Prompt: welcome2 (dropdown) 

Language: Default (dropdown)

Prompt repeat count: 2 (dropdown)

Dial extension: ☒

Dial timeout: 3 s (Range: 0 to 300)

Events

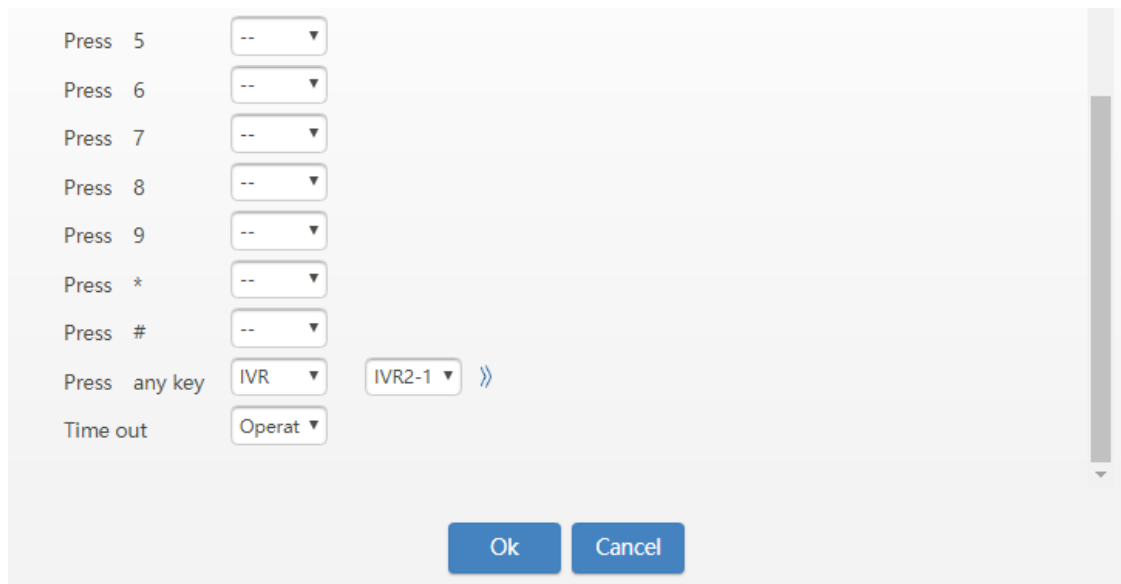
Press 0: -- (dropdown)

Press 1: Extensi (dropdown) 301 (dropdown)

Press 2: Extensi (dropdown) 202 (dropdown)

Press 3: -- (dropdown)

Press 4: -- (dropdown)



Press 5	-- ▾
Press 6	-- ▾
Press 7	-- ▾
Press 8	-- ▾
Press 9	-- ▾
Press *	-- ▾
Press #	-- ▾
Press any key	IVR ▾
Time out	Operat ▾

IVR2-1 ▾ »

Ok Cancel

Step 6 Click  and set IVR2-2 according to the screenshot then click **OK**.

Figure 2-8 IVR2-2screenshot

The screenshot shows the 'IVR2-2' configuration window. The fields are as follows:

- Name:** IVR2-2
- Note:** Level2-support
- Prompt:** welcome2
- Language:** Default
- Prompt repeat count:** 2
- Dial extension:** ☒
- Dial timeout:** 3 s (Range: 0 to 300)

The **Events** section contains the following settings:

Press	Action	Value
Press 0	--	
Press 1	Extensi	311
Press 2	Extensi	212
Press 3	--	
Press 4	--	
Press 5	--	
Press 6	--	
Press 7	--	
Press 8	--	
Press 9	IVR	IVR1
Press *	--	
Press #	--	
Press any key	IVR	IVR2-2
Time out	Operat	

At the bottom of the window are 'Ok' and 'Cancel' buttons.

2.2 Operators/Receptionists

By default, when the caller dials 0, the call is transferred to an operator. By default, the first FXS port is reserved for the operator. If the first port is an FXS port, the operator uses the extension number 200. For devices without an FXS port (such as LS20-4FXO), no default operator is available.

But to add an operator or modify other related information, follow these procedures:

Step 1 Go to **Basic > Auto Attendant** to configure **Operator** settings.

Figure 2-9 Auto attendant configuration interface

Table 2-3 Auto attendant parameters

Item	Description
Extension number for the operator	The default extension number is 200. You can fill in up to five extension numbers, separated by a comma ",". Call waiting, call forwarding and DND are disabled by default. Note: No default extension number for an operator exists on a non-FXS device.
Call Distribution	Select a call distribution scheme below when there is more than one operator: □ Sequential: Terminate the incoming call to the first available extension on the operator list starting from the first one. □ Circular: Terminate the incoming call to extension in Round-robin order; □ Simultaneous: Terminate incoming calls to all available extensions on the operator list simultaneously and the first one to pick up is connected. Note: If all extensions are busy, the device supports a call queue of up to 10 calls.
Press (number) to reach the operator	The number to reach the operator. The default value is 0. Note: If the default value is changed, you must modify related greetings, such as "To transfer to an operator, press zero".
Number of rings before voice prompt	The device will play prompts when the number of rings reaches the value set here. The default value is 10.
First digit timeout	The device plays a greeting to incoming callers. The call will be transferred to the operator within the preset time after the greeting is played. After playing the greeting the first time, transfer it to the operator after 24 seconds if there is no caller dialing.

Step 2 Click **Save** to save the configuration.

2.3 Trunk

2.3.1 Analog trunks

Follow this procedure:

Step 1 Go to **Trunk > Analog trunk** to configure the analog trunk settings.

Figure 2-10 Analog trunk configuration interface

Connection status	Port	Enable	Number *	Polarity reversal detection	Inbound route	Greeting	DID number	Outbound call	Recording	Caller ID detection	Gain
Unconnected	3	☒	202	☐	Attendant	Greeting ☒	--	Allowed	☒	Priority	☒
Unconnected	4	☒	203	☐	Attendant	Greeting ☒	--	Allowed	☒	Priority	☒

Table 2-4 Analog trunk parameters

Item	Description
Connection status	Displays whether the current port is connected to an analog trunk.
Port	FXO port number on the device.
Enable	Select to enable the line. By default, the trunk line is enabled.
Number	The trunk number will be displayed as the calling number when the incoming call number is not displayed or the caller ID is disabled, so it is recommended to use an actual trunk number. The number is 2xx by default.
Polarity Reversal Detection	Calls will be processed in the loop-start signaling mode if no polarity reversal signal is detected after the polarity reversal detection function is enabled.
Inbound route	Select the destination for an external number calling into device through an inbound route: ☐ Attendant: Direct the received calls to auto attendant. ☐ DID: Direct the received calls to the extension specified in DID number without passing through the auto attendant.
Greetings	Select the greeting for the trunk. It is available when the Inbound route is configured as Attendant . ☐ Greeting: the trunk use the auto attendant configured on Basic > Auto attendant page. It is the default value. ☐ Voice: choose an audio file to be the auto attendant of this trunk. Note that the audio file chose here only applicable for business hours. ☐ IVR: choose a multi-level IVR for this trunk. This is available after you configure a multi-level IVR on Basic>IVR page first. Note: The device allow up to 30 trunks to play greetings at the same time.

Item	Description
DID number	Enter the number of extension or hunting group that is bound to the trunk. Note: When the Inbound route is set to DID , this item needs to be configured.
Outbound call	When the Inbound route is configured as Attendant , there are two choice : ☐ Allowed: Allowed to make outbound calls; ☐ Pickup prohibit: Not allowed to make outbound calls. When the Inbound route is configured as DID , there are two choice : ☐ Share: Other extensions are allowed to make outbound calls. ☐ DID only: Only the extension or hunt group specified in DID number is allowed to make outbound calls through this trunk. And the bound extensions can only use this trunk to make outbound calls.
Recording	Enable recording for the trunk. Note: To enable the trunk recording, you need to enable the recording function on the Application > Recording page at first. For details, see 2.7.1 Recording.
Caller ID detection	Allow the extension to display the caller ID detected from a received call over the trunk. If no caller ID is detected or the caller ID is disabled, the trunk number will be displayed. Note: You need to enable the caller ID delivery for the extension.
Gain to IP	Adjust the call volume received on the FXO port. Increase the value when the volume received by internal party is low. Range: -3.0 to +9.0 dB
Gain to PSTN	Adjust the call volume sent from the FXO port. Increase the value when the volume received by external party is low. Range: -6.0 to +3.0 dB
Advanced	Configure advanced properties of an analog trunk.

Step 2 Click **Advanced** to enter the advanced settings of an analog trunk. The parameters relate to the volume, the caller ID detection, and busy tone detection of a trunk. There is no need to make changes to the default values, unless there is an issue with one of the functions.

Figure 2-11 Analog trunk advanced configuration interface

The screenshot displays the 'Analog trunk' configuration page. The top navigation bar includes tabs for Status, Basic, Extension, Trunk (active), LS, Application, Advanced, Security, System tool, and Log. Below the navigation bar, the page title is 'Analog trunk' with a sub-tab for 'IP trunk'. The main content area is divided into two sections: 'Analog trunk' and 'Busy detection'. The 'Analog trunk' section includes sliders for 'Gain to IP' (set to 0.0 dB) and 'Gain to PSTN' (set to -3.0 dB), radio buttons for 'Impedance' (Complex is selected, with 600 Ω and 900 Ω as options), a text input for 'Outpulsing delay' (1000 ms), and a dropdown for 'Call ID detection' (After ring priority). The 'Busy detection' section includes text inputs for 'Busy tone count' (3), 'Tone-on duration' (350 ms), and 'Tone-off duration' (350 ms), and a checkbox for 'Detect dual-frequency busy tone' (unchecked). A 'Save' button is located at the bottom right of the page.

Table 2-5 Analog trunk advanced parameters

Item	Description
Gain to IP	Adjust the call volume received on the FXO port. Increase the value when the volume received by internal party is low. Range: -3.0 to +9.0 dB
Gain to PSTN	Adjust the call volume sent from the FXO port. Increase the value when the volume received by external party is low. Range: -6.0 to +3.0 dB
Impedance	If there is echo on the PSTN side, this parameter can be adjusted. Otherwise, accept the default value.
Outpulsing delay	The interval between FXO off-hook to sending the DTMF called number. If the value is too small, the peer device could miss a number; too large, it might increase the call connection time. Otherwise, accept the default value 1000 for LS20.
Caller ID detection	Select the caller ID detection mode according to the features of the peer switch. In this mode, the caller ID display mode is automatically identified, and caller ID display after ringing is detected with priority. If the caller ID cannot be detected at the first call after the telephone line is plugged out and re-inserted or device reboot, the parameter can be set to Before ring or Before ring priority .
Busy tone count	Compares the count of busy tones with the detection threshold. If the count is less than the detection threshold, the device will ignore the received signals. Range: 2 to 5.
Tone-on duration	The tone on period for the cadence on-off cycle of busy tone. The value is varied depending on the standard for your country/area. By default, the value is 350ms. For details, please see 2.9.8 Call Progress Tone.
Tone-off duration	The tone off period for the cadence on-off cycle of busy tone. The value is varied depending on your country or area. By default, the value is 350ms. For details, please see 2.9.8 Call Progress Tone.

2.3.2 IP Trunk

The LS20 supports standard SIP specifications and Skype Connect. Before setting the IP trunk, you need to obtain an account from your ITSP.

Follow this procedure:

Step 1 Go to **Trunk > IP trunk**.

Step 2 Click **Add**, enter the registration information.

Note: To register trunks to different SIP servers (including Skype Connect), go to **Trunk > IP trunk > Register OPTIONS** and enable **Permit to use multiple ITSPs** first.

Figure 2-12 IP trunk configuration interface

The screenshot shows the 'Add' dialog for IP trunk configuration. The 'Trunk type' section has three radio buttons: 'Peer trunk', 'Register(client)' (selected), and 'Register(server)'. The 'Account type' section has two radio buttons: 'SIP trunk' (selected) and 'Skype Connect'. Below these are input fields for 'SIP server', 'UA domain name', 'Number', 'Username', and 'Password'. The 'Concurrent calls' field is a text input with '1' entered. The 'Inbound route' and 'Greeting' are dropdown menus with 'Attendant' and 'Greeting' selected respectively. 'Ok' and 'Cancel' buttons are at the bottom.

Table 2-6 IP trunk registration parameters

Account type	Item	Description
IP trunk	SIP server	Enter the server IP address and port provided by the ITSP.
	UA domain name	Provided by your ITSP, for example, salesdepart.abccompany.com.
	Number	Provided by your ITSP.
	Username	Provided by your ITSP. It is used for authentication when registering an IP trunk. If no username is entered, the trunk ID will be used for authentication.
	Password	Provided by your ITSP. The password is encrypted by default. Please contact your service provider if you forgot the password. The registration password can contain up to 16 characters if encryption is enabled (The password can contain up to 30 characters if encryption is disabled).
	Concurrent calls	The number of concurrent calls supported by the single trunk. Note: each trunk supports a maximum of 120 concurrent calls. But the total concurrent calls for all trunks should not exceed the maximum number for the SIP trunks, which is 24.
	Trunk type	□ Peer trunk: This is applicable when the LS20 and the peer device both have an fixed IP address. In this mode, enter the IP address of the peer device. □ Register (client): This mode is applicable when the LS20 register to a SIP server. □ Register (server): This mode is applicable when remote FXO gateways register to the LS20 so that the LS20 can utilize the FXO ports as LS20's trunks. You need to configure the username and password and so on, then fill this information on the FXO gateway to register to the LS20.

Account type	Item	Description
	Inbound route	Select the destination for an external number calling into device through an inbound route: ▫ Attendant: Handles the incoming calls from this trunk using the auto attendant. ▫ DID: Binds the trunk to an extension. When a call is received, the device directs the call to the specified extension without passing through the auto attendant.
	Greeting	Select the greeting for the trunk. It is available when the Inbound route is configured as Attendant. ▫ Greeting: the trunk use the auto attendant configured on Basic > Auto attendant page. It is the default value. ▫ Voice: choose an audio file to be the auto attendant of this trunk. Note that the audio file chose here only applicable for business hours. ▫ IVR: choose a multi-level IVR for this trunk. This is available after you configure a multi-level IVR on Basic>IVR page first. Note: The device allow up to 30 trunks to play greetings at the same time.
	DID number	Enter the number of extension or hunt group that is bound to the trunk. Note: When the Inbound route is set to DID, this item needs to be configured.
	Outbound call	When the Inbound route is configured as Attendant, there are two choice : ▫ Allowed: Allowed to make outbound calls; ▫ Pickup prohibit: Not allowed to make outbound calls. When the Inbound route is configured as DID, there are two choice : ▫ Share: Other extensions can make outbound calls over the trunk. ▫ DID only: Only the extension specified in DID number can make outbound calls over the trunk.

Account type	Item	Description
Skype Note: Please go to Trunk>IP trunk>Register OPTIONS and enable Permit to use multiple ITSPs first.	SIP User	Input the SIP user of the SIP profile created in Skype Manager. To obtain SIP profile's registration details, see the Skype Connect User Guide .
	Password	Input the password of the SIP profile created in Skype Manager. The password is displayed as cypher text. Click  to display the password in plain text.
	Skype Connect address	Generally, it is sip.skype.com . It should be identical to the Skype Connect address of the SIP profile created in Skype Manager.
	UDP port	It is 5060 by default. It should be identical to the UDP port of the SIP profile created in Skype Manager.
	Registration	Select this to enable registration.
	Inbound route	Select the destination for an external number calling into device through an inbound route: ▫ Attendant: Handles the incoming calls from this trunk using the auto attendant. ▫ DID: Binds the trunk to an extension. When a call is received, the device directs the call to the bundled extension without passing through the auto attendant.
	Greeting	Select the greeting for the trunk. It is available when the Inbound route is configured as Attendant . ▫ Greeting: the trunk use the auto attendant configured on Basic > Auto attendant page. It is the default value. ▫ Voice: choose an audio file to be the auto attendant of this trunk. Note that the audio file chose here only applicable for business hours. ▫ IVR: choose a multi-level IVR for this trunk. This is available after you configure a multi-level IVR on Basic>IVR page first. Note: The device allow up to 30 trunks to play greetings at the same time.
	DID number	Enter the number of extension or hunting group that is bound to the trunk. Note: When the Inbound route is set to DID , this item needs to be configured.
	Outbound call	When the Inbound route is configured as Attendant , there are two choice : ▫ Allowed: Allowed to make outbound calls; ▫ Pickup prohibit: Not allowed to make outbound calls. When the Inbound route is configured as DID , there are two choice : ▫ Share: Other extensions can make outbound calls over the trunk. ▫ DID only: Only the extension specified in DID number can make outbound calls over the trunk.

Account type	Item	Description
	Add Skype Number	Skype number bound to the SIP account on the Skype website. For example: 13152880961.

Step 3 Click **OK** to return to the IP trunk setting interface, and view the registration status for the configured IP trunk.

Figure 2-13 IP trunk configuration interface

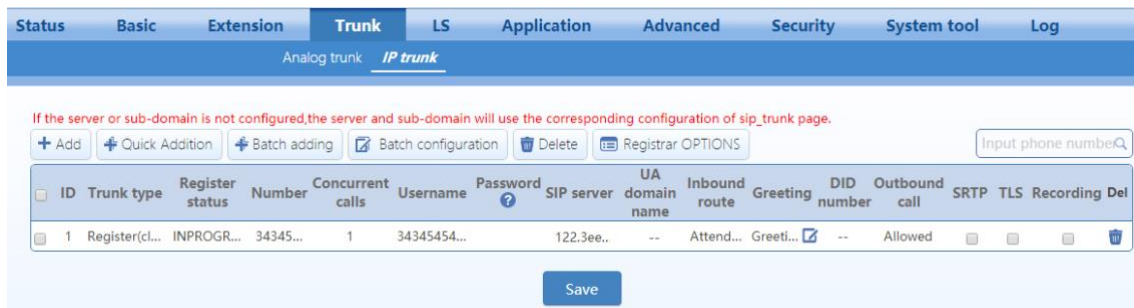


Table 2-7 IP trunk parameters

Item	Description
ID	Line number
Register status	Indicate the status of registration: □ Register success: The IP trunk can be used. □ Register failure: An error occurs during IP trunk registration and the IP trunk cannot be used. The issue can be determined according to the returned error code. □ Unregistered: The registration option is not selected. □ Timeout: The registration fails during the specified registration period and the IP trunk cannot be used. You need to check whether the account of the IP trunk is being used. □ DNS failure: The registration of the IP trunk fails due to a failure in domain name resolution. You should go to the Basic > Network page to check whether the DNS server is correctly configured.
Trunk ID	See Table 2-6.
Concurrent calls	
Username	
Password	
SIP server	
UA domain name	
Registration	
Inbound route	
Greeting	
DID number	
Outbound calls	

Item	Description
Recording	Enable recording for the trunk. Note: To enable the trunk recording, you need to enable the recording function on the Application > Recording page at first. For details, see 2.7.1 Recording.
Delete	Deletes the current IP trunk.

Step 4 Click **Registrar OPTIONS**. You can modify information such as local signaling port and registration expiration. It is recommended to change the **Local signaling port** to prevent SIP attacks.

Figure 2-14 IP trunk registrar interface

The screenshot displays the 'IP trunk' configuration page. At the top, there's a navigation bar with tabs: Status, Basic, Extension, Trunk (selected), LS, Application, Advanced, Security, System tool, and Log. Below the navigation bar, there's a sub-tab for 'IP trunk' (selected over 'Analog trunk').

The main content area is divided into several sections:

- SIP server:** Contains fields for 'Default registrar' (122.3eed@ccc.com), 'Local signaling port' (5060), 'Registration expiration' (600), 'Proxy server' (122.3eed@ccc.com), and 'Increments of port number' (0). Each field has a help icon (?) and a note: 'e.g. 168.33.134.51:5000 or www.sipproxy.com:5000'.
- Register to multiple ITSPs:** Includes an 'Enable' checkbox.
- Other:** Includes 'UA domain name' and 'Sub domain' fields, each with a help icon (?) and a note: 'e.g. 168.33.134.51:5000'.
- PSTN failover:** Includes 'IP address in SIP **Contact** header' and 'IP address in SDP **c** header' fields, each with radio buttons for 'Local address' (selected) and 'NAT address'. Below these are checkboxes for 'Upon outgoing timeout' (checked) and 'Upon outgoing failure' (unchecked).
- Second server:** Includes 'Backup method' (Fixed) and 'Backup SIP proxy' (168.33.134.53:5060) fields, each with a help icon (?) and a note: 'e.g. 168.33.134.53:5000'.
- IMS:** Includes an 'IMS' checkbox.
- Limit the concurrent calls of SIP trunks:** Includes a 'Limit the concurrent calls of SIP trunks' field.

A 'Save' button is located at the bottom right of the form.

Table 2-8 IP trunk registration parameters

Item	Description
Default registrar	The address and port number of the default SIP registration server. The address and port number is separated by ":". It has no default value. The 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, DNS service must be activated and DNS server parameters configured on the Basic > Network page.
Local signaling port	The local SIP port used by the device to send SIP messages to the registrar server. It is 5060 by default and can be changed. It is recommended to change this port to prevent SIP attacks.
Registration expiration	Period for the device to register to the server. Range: 15 to 86400; default value: 600. It needs to be entered as required by the ITSP.
Proxy server	Generally, ensures that it is identical to the register server. If the ITSP provides a separate proxy server, it needs to be entered as required by the ITSP. When a domain name is used, a secondary IP address can be entered in 2.3.3 Backup SIP Proxy Server Settings. This enables the device to switch to this IP address when the domain name resolution service fails.
Increments of port number	The local signaling port number is automatically added by 1 when the value is configured as non-zero under the conditions of failed calls or registration. A new incremental cycle is started when the configured value is reached. The times for Upon call or registration failure,
Permit to use multiple ITSPs	To register trunks to different SIP servers, enable this function first. If disabled, the configured Default registrar will be used for the registration of each IP trunk.
UA domain name	A domain name assigned by the SIP service provider. For example: abccompany.com.
Sub domain	A sub domain name assigned by the SIP service provider. It works with the SIP UA domain name. If the domain name is set to abccompany.com and the sub domain name is set to ims, the full domain name is ims.abccompany.com.
IP address in SIP Contact Header	Set the IP address in the SIP Contact header field. If the device is used in an intranet (behind NAT) and one-way audio condition occurs during the outgoing call, you can try to rectify the one-way audio by adjusting this parameter. □ LAN IP address: The LAN IP address configured by the device is used. □ NAT IP address: The detected NAT IP address is used.
IP address in SDP c Header	Set the IP address in the Connect of SDP. If the device is used in an intranet (behind NAT) and one-way audio condition occurs during the outgoing call, you can try to rectify the one-way audio by adjusting this parameter. It is suggested to set as the same as the one for Contact header. □ LAN IP address: The LAN IP address configured by the device is used. □ NAT IP address: The detected NAT IP address is used.
PSTN Failover	Upon outgoing timeout: The outgoing call timeout caused by the failure of router, Internet or SIP server, etc. Upon outgoing failure: The current outgoing call fails and the device receives failure response codes including 4xx, 5xx or 6xx from SIP server, except 401/404/407/422. Note: This function can be used only when the device has analog trunk port.
Limit the concurrent calls of SIP trunks	Set the maximum number for the total concurrent calls for all SIP trunks. By default, it is 24

2.3.3 Backup SIP Proxy Server Settings

The second server is automatically used when the primary server of the IP trunk is unavailable.

Note: The primary server indicates the proxy server that is set in the **Trunk > IP trunk > Registrar OPTIONS** interface. If multi-platform is enabled, other SIP servers configured for SIP trunks do not support the backup mode.

Follow this procedure:

Step 1 Click **Trunk > IP trunk > Registrar OPTIONS**, and locate the **Second server**.

Figure 2-15 Secondary SIP proxy server interface

The screenshot displays the 'Registrar OPTIONS' interface for an 'IP trunk'. The 'Second server' section is active, showing the following configuration options:

- Backup method:** A dropdown menu set to 'DNS SRV'.
- SRV refresh interval:** Two radio buttons: 'Use TTL (Time To Live) in SRV response' (selected) and 'Use configured value'.
- Local port:** A text input field with the value '1026'.
- Server port:** A text input field with the value '53'.
- Retransmission count:** A text input field with the value '3'.
- Fallback interval:** A text input field with the value '300', followed by the text 's Interval to transmit REGISTER request to primary server'.
- Send NAPTR query before SRV query:** A checkbox that is unchecked.
- Send DNS A type query after receiving SRV record:** Two radio buttons: 'Always' and 'Only when there is no IP address in SRV response' (selected).
- DNS server:** A text input field with the placeholder text 'Resolve SIP server only.'

Below the 'Second server' section, there are two checkboxes: 'IMS' and 'Multi port', both of which are unchecked. At the bottom, there is a section titled 'Limit the concurrent calls of SIP trunks' with a text input field and a 'Save' button.

Table 2-9 Secondary SIP proxy server parameters

Parameters	Description
Backup methods	□ No backup: Disable the second server configuration. When the primary server is unavailable, the secondary server will not be used for registration. □ Fixed: Enable the second server configuration. The server IP address can be preset in the Backup SIP proxy. The IP address of the second server is provided by VoIP service provider. □ DNS SRV: Enable the second server configuration. Multiple IP addresses can be obtained via DNS. The first IP address indicates the primary server, while the second indicates the second server.
SRV refresh interval	□ Use TTL (Time To Live) in SRV response: Default configuration: □ Use configured value: Customize the refreshing interval. The range is 1–65535s.
Local port	Used for sending DNS query requests. The default value is 1026.
Server port	The receiving port of the DNS server. The default value is 53.

Parameters	Description
Retransmission count	The times for the device to retransmit a DNS SRV query request to the DNS server when there is no response from DNS server. The default value is 3.
Failback interval	When the second server is used, the interval for the device to send a registration request to the primary server for failing back to the primary server can be set. The default value is 300 s.
Send NAPTR query before SRV query	Configure whether to send a NAPTR query before a SRV query.
Send the DNS an A type query after receiving the SRV record	Set the conditions for sending an A type query, after a response to the SRV query request is returned. □ Always: The A query request is always sent, regardless of the data type returned for the SRV query request. □ Only when there is no IP address in SRV response: A query request is sent only when a domain name is returned for the SRV query request. This option is selected by default.
DNS server	It is only user to resolve SIP server.

Step 2 Choose **Backup method**.

Step 3 Click **Save** to save the configuration.

2.3.4 IMS

The LS20 can interwork with an IP Multimedia Subsystem (IMS) service network.

In addition to the configuration on the **Trunk>IP trunk> Add** interface, you must configure IMS information.

Follow this procedure to configure IMS information:

Step 1 Click **Trunk > IP trunk > Registrar OPTIONS**, and locate **IMS configuration**.

Figure 2-16 IMS configuration interface

Table 2-10 IMS parameters

Item	Description
IMS	Enable interworking with IMS.
Obtain caller ID info from	For a received call of a SIP trunk, you can set to get the Caller ID from P-Asserted-Identity header or From header in the SIP message.
Access network info	The IP address and port number of the access network. For example: 192.168.100.200:5060. It is optional, input only when the IMS service provider requires.

Step 2 Check **IMS** and enter the **access network info**.

Step 3 Click **Save** to save the configuration.

2.4 Configuring Extensions

The LS20 supports analog and IP extensions, which are separately described below.

2.4.1 Analog extensions

Each FXS port corresponds to one analog extension. To configure an analog extension, follow this procedure:

Step 1 Go to **Extension > Analog** to configure analog extensions.

Figure 2-17 Analog extension configuration interface

Do not use the same extension number as hunt group number, the number to reach the operator, feature access code, IP extension number or another analog extension number. It is only applicable to feeding registration under No.1 dual phone, but not to all IP phone registration.

Port	Enable	WeWei	Number *	Password *	PIN *	Display as	Group	Call restriction	Email ?	Mobile phone ?	Call transfer to outside	Setting
1	☒	☐	200					Domestic			☐	
2	☒	☐	201					Domestic			☐	

[Advanced](#)

Table 2-11 Analog extension parameters

Item	Description
Batch configuration	Configure extensions in batch mode. Batch mode allows the configuration of multiple parameters for multiple extensions at once.
Batch renumbering	Modify extension numbers in batch.
Port	Analog extension port (FXS port) on the device.
Enable	Select to use this line. By default, the line is enabled.
Number	Number of the analog extension. The allocated numbers start from 200 by default.
Display as	Set the display name of the analog or IP extension. This feature is only limited to calls between extensions, and it requires that the name display feature be supported at the called terminal. If display names are configured on both the LS20 and the IP extension, the display name configured on the LS20 prevails.
Group	Select a department for the extension. The extensions within the same department can use group call pickup. For details, see 2.5.5 Group Call Pickup.
Call restriction	Each extension has an assigned privilege for making outbound calls. When a user makes a call beyond its restriction, the device rejects the call with a voice announcement. If extension A is allowed only to make internal calls, when it tries to make outgoing call, the following announcement is heard, "Sorry, you are not authorized to make outgoing call, please contact the administrator." By default, the extension is allowed to make long distance calls. Internal: Internal calls are allowed. Local: Internal calls and local calls are allowed. Long distance: Internal calls, local calls, and long distance calls are allowed. International: Internal calls, local calls, long distance calls, and international calls are allowed. Prohibited: The extension is only allowed to receive calls.
Email	Enter e-mail address to forward the call recording file or voicemail file to the user via email. For information on settings for voice mail, see 2.7.2 Voicemail.
Call transfer to outside	An incoming call is allowed to be transferred to an external party. Note 1: Before using this function, the extension must have corresponding outbound rights. Note 2: During an outbound transfer, two lines are used.

Item	Description
Setting	Set multiple functions for the extension such as Authorization with PIN, Speed dialing, Call forking, Blocked numbers, Assistant, Block from being picked up, Call waiting, DND, Call hold, Call transfer, Call transfer to outside, and so on. For details, see 2.5.1 Basic Functions.
Advanced	Set advanced parameters of the analog extension.

Step 2 Click **Save** to save the configuration.

Step 3 Click **Advanced**, and set advanced properties of the extension such as Gain and Impedance. There is no need to make changes to the default values, unless there are issues when using the extension.

Figure 2-18 Analog extension advanced configuration interface

The screenshot displays the 'Advanced' configuration page for an analog extension. The top navigation bar includes tabs for Status, Basic, Extension (selected), Trunk, LS, Application, Advanced, Security, System tool, and Log. Below this, there are sub-tabs for Analog, IP, IP table, and Group. The main content area contains the following settings:

- Gain to IP:** A slider set to 0.0 dB. Description: Adjust the voice volume from the analog extension.
- Gain to terminal:** A slider set to -3.0 dB. Description: Adjust the voice volume to the analog extension.
- Impedance:** Radio buttons for Complex (selected), 600 Ω, and 900 Ω.
- Hook flash timer min:** A text input set to 75 ms. Range: 25 - 780, Default: 75.
- Hook flash timer max:** A text input set to 800 ms. Range: 800 - 1400, Default: 800.
- Hook debouncing timer:** A text input set to 150 ms. Range: 10 - 1000, Default: 150.
- Ring frequency:** A text input set to 25 Hz. Range: 20 - 50, Default: 25.
- Caller ID transmission mode:** Four dropdown menus: FSK, SDMF, After ringing, and With parity.
- Hotline dialing delay:** A text input set to 5 s. Range: 2-20, Default: 5.

A 'Save' button is located at the bottom right of the configuration area.

Table 2-12 Analog extension advanced parameters

Item	Description
Gain to IP	Adjust the call volume received on the FXS port. Increasing the value gives the internal party a louder voice. Range: -3.0 to +9.0 dB.
Gain to terminal	Adjust the call volume sent from the FXO port. Increasing the value gives the external party a louder voice. Range: -6.0 to +3.0 dB.
Impedance	Select the impedance of the FXS port. You can select Complex, 600 ohms, and 900 ohms. Complex is selected by default.
Hook flash time min	Used to detect hook flash, the default is 75 ms. The device will ignore any flash that shorter than the Min.hook flash . Generally, this value should not be less than 75 ms. You should adjust the parameter when the phone rings after an on-hook but no voice is heard after the off-hook.
Hook flash time max	Used to detect hook flash, the default is 800 ms. The device will regard the flash duration between Min.hook flash and Max.hook flash as effective flash. Any flash lasting over the longest time will be considered by the gateway as hang up. Generally, this value should not be less than 800 ms.

Item	Description
Hook debouncing timer	Used to avoid a phone status glitch. When the duration of on-hook/off-hook status changed is less than the value configured here, the device will consider the status to have not changed. The range is 10-to-1000 ms and the default value is 150 ms.
Ring frequency	The default is 25 Hz and the pattern is 1 second on, 4 seconds off. Generally, there's no need to change it. The range is 15 to 50 Hz.
Caller ID transmission mode	You need to adjust the parameter when the caller ID is displayed abnormally. Generally, there's no need to change it.
Hotline dialing relay	This parameter specifies the delay time before the preset hotline number is automatically dialed after hook-off. The default value is 5 seconds, and the value range is 2 to 20 seconds. This parameter works only if the delay mode is set for hotline function on Extension>Analog page. See Table 2-14.

2.4.2 IP Extensions

The IP phone or SIP softphone registered to the LS20 successfully can be used as an IP extension.

Before using an IP extension, you need to set the extension number and registration password on the LS20. Follow this procedure:

Step 1 Go to **Extension > IP**.

Step 2 Click **Add**, and enter the IP extension number (for example, 208) and password (for example, 187986).

Figure 2-19 IP extension configuration interface

The screenshot displays the LS20 web interface. At the top, there are tabs: Status, Basic, Extension, Trunk, LS, Application, Advanced, Security, System tool, and Log. Under the 'Extension' tab, there are sub-tabs: Analog, IP, IP table, and Group. The 'IP' sub-tab is active. A red warning message is visible: 'Do not use the same extension number as hunt group number, the number to reach the operator, feature access code, analog extension number or another IP extension number.' Below this, a modal window titled 'Add/Modify IP extension' is open. It contains the following fields: 'Number' (text input), 'Registrar password' (text input), 'PIN' (text input), 'Display as' (text input), 'Call restriction' (dropdown menu showing 'Domestic'), 'Group' (dropdown menu showing '-'), and 'IP address for IP trusted authentication' (text input). At the bottom of the modal are 'Ok' and 'Cancel' buttons. In the background, there is a search bar labeled 'Input Ext. number' and a table with columns: Group, Call restriction, Delete, and Setting.

Table 2-13 IP extension parameters

Item	Description
Enable	Select to use this line. By default, the line is enabled.
Online status	Displays the current status of the IP extension.
Number	Phone number
Password	The password used for extension registration. The password is the same as PIN by default. After the password is changed, the PIN does not change.

Item	Description
PIN, Group, display as, Call restriction, Settings	See Table 2-11. Note: all IP extensions only can make an internal call by default. You can change the call restriction for them only after you change the PIN and password.

Step 3 Click **Save** to save the configuration.

For details about registering an IP phone or SIP softphone to LS20, see 4 Making an OpenVPN Client Certification .

2.4.3 IP Trusted Authentication

To simplify the establishment of SIP sessions between LS20 and SIP terminals, you can define a trusted SIP terminal by entering its IP address here. For the trusted SIP terminal, there's no need to perform registration.

Go to **Extension > IP**, click **Setting**, and enter the IP address of the SIP terminal works with the LS20.

Note: On the voice gateway, you need to enter the IP address of the LS20 on the **Proxy server**. For details, see the *MX User Manual*.

Figure 2-20 IP authentication interface

The screenshot displays the LS20 web interface for configuring an extension. The top navigation bar includes tabs: Status, Basic, Extension (selected), Trunk, LS, Application, Advanced, Security, System tool, and Log. Below this, the 'Extension' section has sub-tabs: Analog, IP (selected), IP table, and Group. The main content area shows the configuration for extension 453454353. Fields include: Number (453454353), Group (highlighted with a red box), Authorization with PIN (checkbox), Email, Display as, Call restriction (Domestic), Color ringback tone, Call forward (Disable), Speed dial groups, Call forking, Blocked numbers, Assistant, IP address for IP trusted authentication (highlighted with a red box), Silent monitoring (Disable), Barge (Disable), and SRTP (checkbox). At the bottom, there are checkboxes for Caller ID delivery, Caller ID with call waiting, Block from being picked up, and Call waiting. A blue 'Save' button is located at the bottom right.

2.4.4 Sharing extension

Each extension number can be allocated to an analog phone or IP phone, and a WeWei extension. Calling to this extension number will ring these two terminals – a WeWei extension and a phone, which allow you

to receive this call by either.



Note

When the IP phone and WeWei both are in public network but the LS20 is in a private network, these two terminals can register to LS20 by using the fixed IP address or dynamic domain name of LS20, rather than the P2P traversal domain name of LS20.

2.5 Extension Features

2.5.1 Basic Functions

Go to **Extension > Analog/IP > Setting**, and set the basic functions for the extension.

Figure 2-21 Interface of extension features

Table 2-14 Extension basic features

Item	Description
Gain to IP	Adjust the call volume received on the FXS port. Increasing the value gives the internal party a louder voice. Range: -3.0 to +9.0 dB

Item	Description
Gain to terminal	Adjust the call volume sent from the FXO port. Increasing the value gives the external party a louder voice. Range: -6.0 to +3.0 dB
Group	See Table 2-11.
Display as	
Call restriction	
Email	
Authorization with PIN	Select it to lock the extension. The locked extension can only make an internal call. If an outbound call needs to be made, a PIN is required for authorization.
Call forward	Forward incoming calls to the specified phone or voicemail. This function is disabled by default. □ CFA (phone): Forward all incoming calls to the specified phone. Note: This function cannot be enabled for an operator extension. □ CFB/CFNA (phone): Forward incoming calls to the specified phone when the extension is busy or does not answer. □ CFB (phone): Forward incoming calls to the specified phone when the extension is busy. □ CFNA (phone): Forward incoming calls to the specified phone when the extension does not answer. □ CFA (voicemail): Forward all incoming calls to voicemail For details on voicemail, see 2.7.2 Voicemail. □ CFB/CFNA (voicemail): Forward incoming calls to voicemail when the extension is busy or does not answer. Note: To set the ring duration before CFNA, go to Advanced>System>Forward no answer ring counts.
Different CFB / CFNA target number	If the call forwarding mode is CFB/CFNA (phone) , you can set a target phone number for CFB and a target number separately for CFNA.
Target number	Set the target phone number for call forwarding . The number can include extension number and external number (a mobile phone number or an external phone number). For external numbers, the extension should be allowed to make outgoing call. An outgoing call prefix and a comma are required to be input before you input the external number if the dialing prefix is required to make an outgoing call.
Color ringback tone	Select a CRBT file for the extension. For details on uploading and managing CRBT files, see 2.9.3 CRBT.
Speed dial groups	Allow users to dial the destination with a two-digit speed dial code preceded by **. The format for each group is "Speed dial code - Phone number". Up to 30 speed dial groups are allowed, separated by comma ",". The speed dial code must be in the range of 20–49. For example, speed dial group 20–13823218765 indicates 20 as the speed dial code for 13823218765.
Hot line	Outgoing calls are automatically routed to the preprogrammed telephone number when the user takes the telephone off-hook. □ Disable: Disable hot line feature. □ Immediate: Automatically dials out the preset number after off-hook. □ Delay mode: Automatically dials out the preset number if the user does not dial any digit after off-hook for a certain period of time. The default value is 5s. This parameter is only applicable to analog extensions. For IP extensions, hot line configuration is set on the IP phones.

Item	Description
Number	Enter the hot line number.
Call forking	The device forwards the call to both your extension and another receiving terminal (for example, a mobile phone) simultaneously. Enter the number you want to fork to. Notes: □ The function does not work when DND or CFA is enabled. □ Call forking will be inactive when the incoming call is waiting. □ When the call is forked to external terminal via analog trunk, the incoming call is routed to the external terminal when the ringing exceeds the No. of rings before voice prompt configured on Auto-attendant page.
Blocked numbers	Enter the incoming numbers you want to block for the extension. For an incoming call with a blocked number, the device will play busy tone. Up to 20 blocked numbers are allowed, separated by comma ",". Note 1: An outbound call to the blocked numbers is allowed. Note 2: The blocked numbers configured here are applicable to an extension. To configure blocked numbers for all extensions, go to Extension>IP table.
Silent monitoring	□ Disable: Forbid the extension to monitor a call of another extension. □ Any: Allow the extension to monitor a call of any other extensions. □ Within a group: Allow the extension to monitor a call of other extensions within the same group. Note: If either of the two parties of the monitored call enables the Block from being silently monitored, the silent monitoring function does not work.
Barge	□ Disable: Forbid the extension to barge into a call of another extension. □ Any: Allow the extension to barge into a call of any other extensions. □ Within a group: Allow the extension to barge into a call of another extension within the same group. Note: If either of the two parties of the barged call enables the Block from being barged-in, the barging function will not work.
Caller ID delivery	If enabled, the caller ID is delivered to the extension.
Caller ID with call waiting	If call waiting is enable and a new call arrives while a call is in progress, the caller number of the new call is be displayed.
Block from being picked up	The incoming calls cannot be picked up by other extensions. Note: The local extension can pick up the calls of other extensions by default.
Call waiting	When a new incoming call arrives while a call is in progress, the user will hear beeps and has three choices: □ Ignore a new call: No operation is required, and the current conversation continues. The beeps stop after the specified time. □ Answer a new call: The user can press ** to suspend the current call and switch to the new incoming call. Meanwhile the suspended party hears call waiting music. □ Switch call: The user can press ** to suspend the current call and switch back to the original call. Note: Before using this function, ensure that call hold is enabled.
Call hold	The user can suspend a current call and make a new call. Meanwhile the suspended party hears call waiting music.

Item	Description
Call transfer by called party	Transfers received calls to an external phone or other extension. To transfer to an external phone, the extension should be allowed to transfer calls to outside. □ Blind transfer: Transfers a call without consulting with the intended recipient (another internal extension). The number of the original caller is displayed on the recipient's phone. □ Consultation transfer: Transfers a call after consulting with the intended recipient (an internal extension or an external phone). The number of the person who transfers the call is displayed on the recipient's phone. Note: Before using the call transfer function, ensure that Call Hold is enabled.
Call transfer by calling party	Transfers the current call to another extension or an external phone when the extension serves as the calling party. Transferring to an external requires the allowance to transfer calls to outside. □ Blind transfer: Same as above. □ Consultation transfer: Same as above. Note: Before using the call transfer function, ensure that Call hold and Call forward are enabled.
Call transfer to outside	See Table 2-11.
Recording	Record the whole conversation for each call. Note: To enable the total recording by the extension, you need to enable the recording on Recording page. For details, see 2.7.1 Recording.
Distinctive Ringing	The extension rings with different ringing pattern according to the type of the incoming call. □ Internal call: "beep - beep - beep – beep - beep" □ External call: "beep beep - beep beep beep" □ Speed dial call: "beep beep beep beep beep - beep - beep"
Polarity reversal signal sending	In the events of answers and disconnect at the remote end, the device sends polarity reversal signals to the local terminal as indication. Polarity reversal signals can be used on a phone with billing function. Note: This function is applicable only to analog extensions.
Block from being silently monitored	All the conversation with the extension cannot be monitored.
Block from being barged-in	The conversation with the extension cannot be barged-in.
On-demand recording	Allow the user to start on-demand recording on phone set with either of the following methods: □ Dial *# during the call □ Dial *# before dialing phone number. For details on recording, see 2.7.1 Recording.
Do not disturb	Allow the user to set Do not disturb (DND) on phone set to ensure the extension does not ring when incoming calls are received. The user can dial *72(or*99) to enable or disable DND. Note: After the device reboots, DND of the phone set is still valid.

2.5.2 Making Outbound Calls

Go to **Basic > Dialing rule > Outbound** to configure outbound dialing rule.

Figure 2-22 Outbound dialing rule interface

International call limitation

Prefix: 00 Allowed call duration per day: [] hr. [] min.

Outbound

Do not use the same outbound prefix as hunt group number, the number to reach the operator, feature access code, analog/IP extension number or another outbound prefix.

Automatic insertion of long distance dialing prefix: [] e.g. 17909

Long distance call prefix: 0 ☒ The outbound calls dialed with this prefix are identified as long distance call.

Dialing method for outbound calls: ☒ Dialing without a prefix ☐ A prefix is required for analog extensions but optional for IP extensions

☐ Dialing with a prefix

Least cost routing Select the ITSP for long distance call.

Hunt group

Do not use the same hunt group number as the number to reach the operator, feature access code, analog/IP extension number or another hunt group number.

Ring the next available extension in the group after: 15 seconds of ringing

Number	Hunting	Extensions
[]	Sequential	Directly enter or click the icon to select the extensions

Save

Table 2-15 Outbound dialing rule parameters

Item	Description
International call limitation	The outbound calls dialed with the prefix configured here are identified as international call. You can limit the international call time for every day. Note: If the Call restriction of the extension is configured as Prohibited , Internal , local or long distance , the number with the prefix configured here cannot be dialed.
Automatic insertion of long distance dialing prefix	When the user makes a long distance call using the analog trunk, the prefix set will be automatically added.
Long distance call prefix	The outbound call to a number started with the prefix configured here is identified as long distance calls. The default prefix value is 0. The system can identify home locations of mobile numbers in Mainland China, and automatically adds 0 when a long-distance mobile phone number is called. Note: If the Call restriction of the extension is configured as Prohibited , Internal or local , no long distance outbound call will be allowed.
Dialing method for outbound calls	☐ Dialing without prefix: Directly dial internal extension or external numbers. ☐ Intercom dialing with specified prefix*: Dial external numbers directly while dial internal numbers by adding prefix *. ☐ Outbound dialing with prefix: Dial internal extension numbers directly while dial internal numbers with prefix.
Routing	When the device is configured with multiple trunks, a corresponding outbound call hunting method can be selected as required. The device provides six routes of outbound call for users to select. ☐ Sequential hunting for analog trunk: Make the outgoing call through the first available analog trunk on the analog trunk list starting from the first one. ☐ Round-robin hunting for analog trunk: Make the outgoing call through the analog trunk in Round-robin order. ☐ Sequential hunting for IP trunk: Make the outgoing call through the first available IP trunk on the IP trunk list starting from the first one. ☐ Round-robin hunting for IP trunk: Make the outgoing call through the IP trunk in Round-

Item	Description
	robin order. □ Least cost routing: Analog trunks are selected for local calls, and IP trunks are selected for long distance/international calls. The device determines the long distance/international calls based on the prefix. For example: If the long distance call prefix is 0 and the international call prefix is 00, an IP trunk is selected for the calls made with the numbers starting with "0" or "00". An analog trunk is selected for local calls. If the IP trunk is not activated or a network failure occurs, an analog trunk is also selected for calls made with the numbers starting with "0" or "00". Note: If a long distance/international call is made with all IP trunks occupied, the following announcement will be played: All circuits are busy. Please try your call again later. □ Route: The routing table rules are used to make the call to the PSTN. For details, see 2.9 System Settings. Note: When the routing mode is sequential or round-robin, for a single prefix, you can set trunks for LS20.
Prefix	The user can make an outbound call with a routing method identified by the prefix configured here. For example, if the prefix for Sequential hunting for IP trunk is 9, the device will make sequential hunting over IP trunk when dialing the number starting with 9. Note: □ The parameter can be configured only when the Dialing method for outbound calls is Outbound dialing with prefix. □ To avoid collision, the prefix must be different from extension number, hunting group number, number to reach the operator, feature access code, and other outbound call prefixes.
Secondary dial tone	After the extension user dials the prefix, the device prompts the user to dial the called number with secondary dial tone. Note: Applicable only when the Dialing method for outbound calls is Outbound dialing with prefix.
Trunk	Specify the corresponding trunk numbers for the outbound group of analog trunks and IP trunks. Select the trunk numbers directly or enter them manually. The trunk numbers must be separated by ",".

2.5.3 IP table

Go to **Extension > IP Table**, and set rules for filtering inbound and outbound call numbers. For example: If 12345678 is set in **Blocked number**, the device will play a busy tone when a call dialed with this number arrives.

Figure 2-23 IP table configuration interface

Disallow outbound calls for certain prefixes

Unrestricted numbers for outbound call

ID	Blocked numbers	ID	Blocked numbers
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	
21		22	
23		24	
25		26	
27		28	
29		30	

Save

Table 2-16 IP table parameters

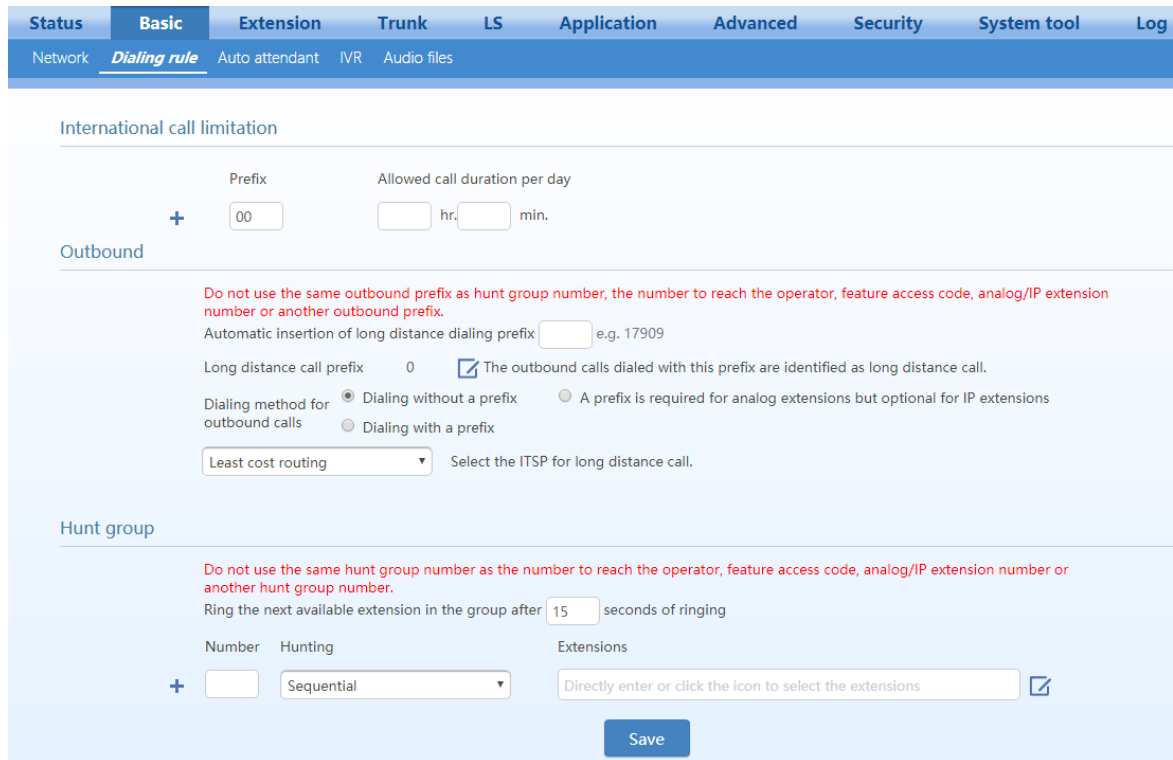
Item	Description
Disallow outbound calls for certain prefixes	The device prohibits the user from dialing numbers with the prefix configured here. When the number is dialed, the device plays a busy tone. You can fill in up to 20 prefixes, separated by comma ",". Note: The user can dial Unrestricted numbers for outbound call even if it is started with the prefix configured here.
Unrestricted numbers for outbound calls	The user can dial the number regardless of Call restriction and Disallow outbound calls for certain prefixes.
Blocked numbers	A table listed with up to 30 phone numbers, which are prohibited from calling in and busy tone will be played to reject the calls. Note: □ Caller ID detection feature must be enabled for this feature to take effect. □ The blocked numbers can be called from the device. □ The blocked numbers configured here is applicable for all extensions. To configure blocked numbers for individual extension, see 2.5.1 Basic Functions.

2.5.4 Hunt Group

You can allocate multiple extensions to a hunt group of extensions. When a caller dials the hunt group number, the device will ring an idle extension in the group according to the preset allocation.

Go to **Basic > Dialing rule**, and set the hunting group. You can click  to add new groups.

Figure 2-24 Hunt group configuration interface



The screenshot displays the 'Basic' configuration tab for a 'Dialing rule'. The 'Hunt group' section is active, showing a warning: 'Do not use the same hunt group number as the number to reach the operator, feature access code, analog/IP extension number or another hunt group number.' Below this, there is a field for 'Ring the next available extension in the group after' set to 15 seconds. The 'Number' field is empty, and the 'Hunting' method is set to 'Sequential'. The 'Extensions' field is empty with a warning icon. A 'Save' button is at the bottom right.

Table 2-17 Hunt group parameters

Item	Description
Ring the next available extension in the group after XX seconds of ringing	Ring timeout to select the next available extension in the group.
Numbers	Add extension numbers to the hunt group. Note: The numbers must be different from an outbound call prefix, a number forwarded to the auto attendant, an extension number, or a feature access code.

Item	Description
Hunting	Select a hunt group method: ▢ Sequential: Terminate the incoming call to the first available extension on the extension list starting from the first one; ▢ Circular: Terminate the incoming call to extension in Round-robin order ▢ Simultaneous: Terminate incoming calls to all available extensions on the operator list simultaneously and the first one to pick up is connected. In this mode, you may add at most 40 extensions for LS20. Note: ▢ If an extension configured with call forward is included in a sequential or circular hunt group, the incoming call will never re-route to the extension in the group after being forwarded to the call forward target number. ▢ If all extensions are busy, the device supports a call queue of up to 20 calls.
Extensions	Enter extension numbers included in a hunting group.

2.5.5 LS20Group Call Pickup

The group call pickup function allows users in the same group to pick up incoming calls for each other. To enable this function, you need to define groups and add member extensions to the groups.

To configure a department, follow this procedure:

Step 1 Go to **Extension >Group** to enter or change the group name. You can define up to 32 groups

Step 2 Click **Save** to save the configuration.

Figure 2-25 Group configuration interface

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log																																																																				
Analog IP IP table Group																																																																													
Group call pickup is available in the same group. A group name can include alphabetic or numeric characters. <table> <thead> <tr> <th>ID</th> <th>Group name</th> <th>ID</th> <th>Group name</th> </tr> </thead> <tbody> <tr><td>1</td><td> </td><td>2</td><td> </td></tr> <tr><td>3</td><td> </td><td>4</td><td> </td></tr> <tr><td>5</td><td> </td><td>6</td><td> </td></tr> <tr><td>7</td><td> </td><td>8</td><td> </td></tr> <tr><td>9</td><td> </td><td>10</td><td> </td></tr> <tr><td>11</td><td> </td><td>12</td><td> </td></tr> <tr><td>13</td><td> </td><td>14</td><td> </td></tr> <tr><td>15</td><td> </td><td>16</td><td> </td></tr> <tr><td>17</td><td> </td><td>18</td><td> </td></tr> <tr><td>19</td><td> </td><td>20</td><td> </td></tr> <tr><td>21</td><td> </td><td>22</td><td> </td></tr> <tr><td>23</td><td> </td><td>24</td><td> </td></tr> <tr><td>25</td><td> </td><td>26</td><td> </td></tr> <tr><td>27</td><td> </td><td>28</td><td> </td></tr> <tr><td>29</td><td> </td><td>30</td><td> </td></tr> <tr><td>31</td><td> </td><td>32</td><td> </td></tr> </tbody> </table> Save										ID	Group name	ID	Group name	1		2		3		4		5		6		7		8		9		10		11		12		13		14		15		16		17		18		19		20		21		22		23		24		25		26		27		28		29		30		31		32	
ID	Group name	ID	Group name																																																																										
1		2																																																																											
3		4																																																																											
5		6																																																																											
7		8																																																																											
9		10																																																																											
11		12																																																																											
13		14																																																																											
15		16																																																																											
17		18																																																																											
19		20																																																																											
21		22																																																																											
23		24																																																																											
25		26																																																																											
27		28																																																																											
29		30																																																																											
31		32																																																																											

To distribute extensions to a specific group, follow this procedure:

Step 3 Go to **Extension > Analog/IP > Setting**, and enter the extension function configuration interface.

Step 4 Select the group you want to distribute the extension to from the **Group** drop-down list, and **save** the configuration.

Figure 2-26 Group interface

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log																																																																																										
Analog IP IP table Group																																																																																																			
Go back <table> <tbody> <tr> <td>Gain to IP</td> <td> 0.0 </td> <td>dB</td> <td colspan="7">Adjust the voice volume from the analog extension.</td> </tr> <tr> <td>Gain to terminal</td> <td> -3.0 </td> <td>dB</td> <td colspan="7">Adjust the voice volume to the analog extension.</td> </tr> <tr> <td>Impedance</td> <td colspan="9"> ☒ Complex ☐ 600 Ω ☐ 900 Ω </td> </tr> <tr> <td>Hook flash timer min</td> <td> 75 </td> <td>ms</td> <td colspan="7">(Range: 25 - 780 , Default: 75)</td> </tr> <tr> <td>Hook flash timer max</td> <td> 800 </td> <td>ms</td> <td colspan="7">(Range: 800 - 1400, Default: 800)</td> </tr> <tr> <td>Hook debouncing timer</td> <td> 150 </td> <td>ms</td> <td colspan="7">(Range: 10 - 1000, Default: 150)</td> </tr> <tr> <td>Ring frequency</td> <td> 25 </td> <td>Hz</td> <td colspan="7">(Range: 20 - 50, Default: 25)</td> </tr> <tr> <td>Caller ID transmission mode</td> <td>FSK</td> <td>SDMF</td> <td>After ringing</td> <td>With parity</td> <td colspan="5"></td> </tr> <tr> <td>Hotline dialing delay</td> <td> 5 </td> <td>s</td> <td colspan="7">(Range: 2-20, Default: 5)</td> </tr> </tbody> </table> Save										Gain to IP	0.0	dB	Adjust the voice volume from the analog extension.							Gain to terminal	-3.0	dB	Adjust the voice volume to the analog extension.							Impedance	☒ Complex ☐ 600 Ω ☐ 900 Ω									Hook flash timer min	75	ms	(Range: 25 - 780 , Default: 75)							Hook flash timer max	800	ms	(Range: 800 - 1400, Default: 800)							Hook debouncing timer	150	ms	(Range: 10 - 1000, Default: 150)							Ring frequency	25	Hz	(Range: 20 - 50, Default: 25)							Caller ID transmission mode	FSK	SDMF	After ringing	With parity						Hotline dialing delay	5	s	(Range: 2-20, Default: 5)						
Gain to IP	0.0	dB	Adjust the voice volume from the analog extension.																																																																																																
Gain to terminal	-3.0	dB	Adjust the voice volume to the analog extension.																																																																																																
Impedance	☒ Complex ☐ 600 Ω ☐ 900 Ω																																																																																																		
Hook flash timer min	75	ms	(Range: 25 - 780 , Default: 75)																																																																																																
Hook flash timer max	800	ms	(Range: 800 - 1400, Default: 800)																																																																																																
Hook debouncing timer	150	ms	(Range: 10 - 1000, Default: 150)																																																																																																
Ring frequency	25	Hz	(Range: 20 - 50, Default: 25)																																																																																																
Caller ID transmission mode	FSK	SDMF	After ringing	With parity																																																																																															
Hotline dialing delay	5	s	(Range: 2-20, Default: 5)																																																																																																

2.5.6 Call Pickup

The call pickup function allows another extension user to pick up an incoming call if the call is not answered. By default, the call pickup function is enabled.

2.5.7 Three-way Calling

The three-way calling function allows the extension user to invite a third party to attend the conversation for three-way calls. It also allows the extension user to communicate with one party while having the other party listening to the background music, and to switch between the parties. The drop of either of the other two parties from the three-way call will not affect the conversation. The extension user can hang up the phone to end the three-way calling.

Note: When **Call hold** is enabled, three-way calling is enabled by default. For details, see [Call hold](#).

2.5.8 Call Parking

Call parking allows a user to put a call on hold at one extension and continue the conversation from any other extension.

Note: When **Call hold** is enabled, call parking is enabled by default. For details, see [Call hold](#).

2.5.9 DID

With DID enabled, an incoming call can be directly routed to a specified extension or hunt group without passing through the auto attendant. The trunk can be used either by the specified extension/hunt group or other extensions/hunt groups depended on configuration.

Follow this procedure:

Step 1 Go to **Trunk > Analog trunk/IP trunk** to select bundled trunk for extension/hunting group, and select **DID** for **Inbound route**.

Figure 2-27 DID configuration interface

When the cloud PBX is connected, the device only handles the incoming calls from analog trunks and outgoing calls from analog extensions.
When the cloud PBX is disconnected, the device handles all calls taking place of the cloud PBX.

Batch configuration

Connection status	Port	Enable	Number *	Polarity reversal detection	Inbound route	Greeting	DID number	Outbound call	Recording	Caller ID detection	Gain
Unconnected	3	☒	202	☐	Attendant	☒	--	☒ Allowed ☐ Pickup prohibit	☒	Priority	☐
Unconnected	4	☒	203	☐	Attendant	☒	--	Allowed	☒	Priority	☐

[Advanced](#) ➔

Step 2 Select drop-down list In the **DID number** field, enter and select the extension number or hunting group number that needs to be bundled.

Step 3 Select the **Outbound call** mode.

- ☐ **Share:** The trunk can be used by all extensions or hunt groups.
- ☐ **DID only:** The trunk can be used only by the specified extension or hunt group.

Step 4 Click **Save** to save the configuration.

2.5.10 Feature Access Codes

Go to **Advanced**> **Feature access code** to query or customize feature access codes Click to view details about the feature access codes.

Figure 2-28 Feature access codes interface

System	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
System Cert. <u>Feature access codes</u> Routing Dialing Tone SIP DTMF Call record									
Do not use the same number as hunt group number, the number to reach the operator, analog/IP extension number or another feature access code.									
System ?									
Obtain IP address		##		Set up IP address		*90			
Set up extension number		*96		Obtain extension number		#00			
Voice prompt recording ?									
Record		*81		Audit		*82			
Save		*83							
Operation ?									
Call park		*30		Call park retrieval		#30			
Any call pickup		*51		Attendant call pickup		*50			
Directed call pickup		*55		Group call pickup		*56			
Calling with PIN		*33		Blind transfer		*38			
Three-way calling		*79		Silent monitoring		*34			
Speed dial		**		On-demand recording		*#			
Automatic callback busy		*31		Barge		*39			
General feature voice menu ?		*99		Listen to voice messages		*98			
Bind incoming call		*66		Unbind incoming call		*67			
Save Default									



Note

To avoid collision, the feature access code must be different from any extension number, hunt group number, number to reach the operator, outbound call prefix, and other feature access codes.

2.6 Local Survival (LS)

Go to **LS** page to set a cloud PBX address. LS20 will accept IP extensions to register and will handle the calls from the IP extensions when cloud PBX is disconnected with LS20. After connection recovers, the calling services will be switched to the cloud PBX again.

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
Username Password Cloud PBX localhost:5060 Backup cloud PBX Local signaling port 5060 OPTIONS request interval 0 s Emergency call numbers Supplemental authentication ☒ Allow call from IP range(s) IP address range 1 IP address range 2 TLS ☐ SRTP mode SRTP only (fallback to RTP for i Handle PSTN incoming in standby mode Send to the cloud PBX Save									

Item	Description
Username	Enter the username which the cloud PBX provides.
Password	Enter the password which the cloud PBX provides.
Cloud PBX	Enter the IP address of the cloud PBX.
Backup cloud PBX	Enter the backup address of the cloud PBX.
Local signaling port	Enter the local signaling port.
OPTIONS request interval	Enter the interval in which the LS20 sends OPTIONS request to the cloud PBX. LS20 uses OPTIONS requests to check if the connection with the cloud PBX is good.
Emergency call numbers	Enter emergency call numbers. When extensions make calls to these numbers, LS20 assures these calls to have trunks to use even when the trunks are occupied by other calls.
Supplemental authentication	In local survival mode, LS20 handles calling from trusted extensions, which are authenticated by setting trusted IP address segments.
IP address range 1	Specify an IP address segment of trusted IP extensions.
IP address range 2	Specify another IP address segment of trusted IP extensions.
TLS	Tick the check box to enable TLS.
SRTP mode	☐ SRTP only (fallback to RTP for incoming calls): only SRTP negotiation is used for outgoing calls, but RTP negotiation is preferred for incoming calls. ☐ Disable: Disable SRTP, support only RTP
Handle PSTN incoming calls in standby mode	When cloud PBX is connected with LS20, LS20 handles PSTN incoming calls in any of the following ways: ☐ Send to the cloud PBX: LS20 just sends these calls to the cloud PBX. ☐ Send to the bonding FXS port: LS20 handles these calls itself and establishes a call between the FXO port and its bonding FXS port. ☐ Reject: LS20 rejects these calls.

2.7 Recording and Voicemail

2.7.1 Recording

The LS20 supports remote recording and USB-device recordings, both for G.711 and G.729.

Remote recording

All the recorded files generated by the device are stored in the external recording server in real time. Before recording, an external recording server installed with New Rock Recording Agent is required. You can download the recording agent from <http://en.newrocktech.com/show/593.html>.

Tick the check box of **Locally save recordings upon server disconnected**, the device can store the recordings generated when the network between the device and the recording server is disconnected, and the recording server will get these recordings after the network is connected.

Follow this procedure:

Step 1 Go to **Application > Recording**, and select **Remote recording**.

Figure 2-29 Remote recording configuration interface

The screenshot displays the 'Recording' configuration page. At the top, there is a navigation bar with tabs: Status, Basic, Extension, Trunk, LS, Application (selected), Advanced, Security, System tool, and Log. Below this is a sub-menu bar with options: Casting rule, Fax, Media, Recording (selected), Storage, Duty schedule, Alarm notification, and Remote support. The main content area is titled 'Recording' and contains the following settings:

- Recording:** Three radio buttons are present: 'Disable', 'Remote recording' (selected), and 'Internal USB flash drive'.
- Recording server:** A text input field.
- Locally save recordings upon server disconnected:** A checkbox that is currently unchecked.
- Secure code to copy recordings:** A text input field containing the value '259243'.
- Voicemail email settings:**
 - Outgoing email server:** A text input field with a hint 'e.g. 192.168.45.32 or smtp.sohu.com'.
 - Sender:** A text input field with a hint 'It is recommended to use a public email address'.
 - Password:** A text input field.

At the bottom of the page, there is a note: 'Note: Change the email address of receiving recording in [Analog extension](#) [IP extension](#)'. A 'Save' button is located at the bottom right of the configuration area.

Step 2 Enter the IP address and port number of the recording server. The default port number is 1311.

Step 3 Click **Save** to save the configuration.

Step 4 Go to **Extension > Analog/IP**, select the desired extension, and click **Setting**.

Step 5 Select **Recording**.

Figure 2-30 Extension recording configuration interface

The screenshot shows the 'Extension' configuration tab in the LS20 Administrator. The 'Recording' checkbox is checked and highlighted with a red box. Other settings include 'Call forward' set to 'Disable', 'Color ringback tone' set to '--', 'Speed dial groups' set to an empty field, 'Hot line' set to 'Disable', 'Call forking' set to an empty field, 'Blocked numbers' set to an empty field, 'Assistant' set to an empty field, 'Silent monitoring' set to 'Disable', and 'Barge' set to 'Disable'. There are also checkboxes for 'Caller ID delivery', 'Call hold', 'Recording', 'Block from being silently monitored', 'Block from being barged-in', 'Caller ID with call waiting', 'Call transfer by called party', 'Distinctive ringing', 'Block from being picked up', 'Call waiting', 'Call transfer by calling party', 'Call transfer to outside', 'Call blocking/restriction', 'Polarity reversal signal sending', 'Satisfaction survey', 'On-demand recording', 'Do not disturb', 'Call forwarding', and 'Call forking'. A 'Save' button is at the bottom right.

Step 6 Click **Save** to save the configuration.

For details about managing recording files on the recording server, please refer to [OM Recording Agent User Guide](#).

USB device recording

All the recording files are stored in local storages of the device, which include the internal USB flash drive or external USB device. The storage space allocated for the internal USB flash drive is 10240 MB by default. You can modify it on **Application>Storage** page.

Note: The recording files stored in the USB device can be backed up to the remote recording server, in which case the **Back up to recording server** should be enabled. For details about how to back up recording files to the remote recording server, see *OM Recording Agent User Guide*.

Step 1 Go to **System tools> System time** to check that the current time of the device is correct. For details of time setting, see 2.9.5 Time.

Note: Please make sure the system time is correct because the recording files are named using the system time.

Step 2 Go to **Application > Recording**, and select the storage mode. Before selecting **Recording through external USB device**, you need to connect the external USB device.

Step 3 Tick the check box of **Keep the original files**, if the SIP server or IP phones enable silence suppression.

Step 4 Choose the operation when the available space is insufficient.

Recording priority: The new recording will overwrite the existing recording. When the available storage space is less than 500MB, recording files for the earliest day or the earliest 100 recording files are overwritten.

Retention priority: The new recording will be stopped.

Figure 2-31 USB recording configuration interface

Step 5 Click **Save** to save the configuration.

Step 6 Go to **Extension > Analog/IP**, select the desired extension, and click **Set**.

Step 7 Select **Recording**.

Figure 2-32 Extension recording interface

Step 8 Click **Save** to save the configuration.

Managing recorded files

Table 2-18 Managing recorded files

Format	Calling party_Called party_Date_Time_Random code_cg.wav Calling party_Called party_Date_Time_Random code_cd.wav cg.wav indicates a recorded file that is generated when the extension serves as the calling party. cd.wav indicates a recorded file that is generated when the extension serves as the called party.
---------------	--

	For example: 200_80001_20121130_180028_a00a_cg.wav indicates that the recorded file is generated at 18:00:28 on November 30, 2012 when the extension 200 calls 80001.
View recorded files	□ Go to Application > Storage to get the access path and view the recorded files in the browser. Click builtin to view the files recorded through internal USB flash drive, and usb to view the files recorded through external USB device. The typical example of the storage path is: sda1/Recorder/20140930. □ If recorded files are stored in an external USB device, you can remove the USB device from the LS20 and connect it to your PC, then view the recorded files. The typical example of the storage path is: G:/Recorder/20140930.
Listen to recorded files	You can listen to the recorded files with either of the following methods: □ Locate and download the recorded files, and play it; □ Play the recordings on the Call log page of NeeHau Business Phone Assistant.
Backup and clear recorded files	□ Internal USB flash drive: Go to Application > Storage, click Backup to store the Recorder folder to the root directory of the external USB device. When the backup is completed, click clear to delete the remaining recorded files from the internal USB flash drive. □ External USB device: Remove the USB storage device and connect it to your PC, and then back up or clear the recorded files.

2.7.2 Voicemail

When the extension user cannot receive the incoming call, the calling party can leave a message after the prompt.

Step 1 Go to **Application > Recording**, and enable the recording. For details, see 2.7.1 Recording.

The storage path of recorded files is varied depending on the recording mode, for example, if **Internal USB flash drive** is selected, the voicemail messages will be stored in the internal USB flash drive.

Step 2 Go to **Extension > Analog/IP > Setting**, and set the **Call Forward to CFA (voicemail)** or **CFB/CFNA (voicemail)**.

Figure 2-33 Voicemail configuration interface

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
Analog IP IP table Group									
Email									
Mobile phone ?									
Authorization with *33 ?	☐								
Call forward	Disable Disable CFA (phone) CFB/CFNA (phone) CFB(phone) CFNA(phone) CFA (voicemail) CFB/CFNA (voicemail)								
Color ringback tone									
Speed dial groups ?									
Hot line									
Call forking									
Blocked numbers	You can fill in up to 20 blocked numbers, separated by comma "," .								
Assistant									
Silent monitoring	Disable								
Barge	Disable								
☒ Caller ID delivery	☒ Caller ID with call waiting	☐ Block from being picked up		☐ Call waiting					
☒ Call hold	☒ Call transfer by called party	☒ Call transfer by calling party		☐ Call transfer to outside					
☒ Recording	☐ Distinctive ringing	☐ Call blocking/restriction		☐ Polarity reversal signal sending					
☐ Block from being silently monitored	☐ Block from being barged-in	☐ Satisfaction survey							
Allow extension to configure ☐ On-demand recording ☐ Do not disturb ☒ Call forwarding ☒ Call forking									
View the feature access codes Save									

Step 3 Click **Save** to save the configuration.

When the recording mode is **Remote recording**, the voicemail messages can be sent to the mailbox of the extension user. To configure it, follow this procedure:

Step 1 Select **Remote recording** on the **Recording** page and configure the **Recording server** and **Outgoing email server**.

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
Casting rule Fax Media Recording Storage Duty schedule Alarm notification Remote support									
Recording									
Recording ?	☐ Disable ☒ Remote recording ☐ Internal USB flash drive								
Recording server ?									
Locally save recordings upon server disconnected	☐								
Secure code to copy recordings	259243								
Voicemail email settings									
Outgoing email server	e.g. 192.168.45.32 or smtp.sohu.com								
Sender	It is recommended to use a public email address								
Password									
Note: Change the email address of receiving recording in Analog extension IP extension Save									

Table 2-19 Voice mailbox sending server parameters

Item	Description
Outgoing email server	Enter the IP address or domain name of the mail server. The device supports Sina mailbox and Sohu mailbox.
Sender	Enter the mailbox address of the sender.
Password	Enter the mailbox password of the sender.

Step 2 Click **Save**.

Step 3 Go to **Extension > Analog/IP > Setting**, and configure **Email**. The mailbox will serve as the mailbox for receiving voicemail messages.

Step 4 Click **Save**.

Managing voicemail message files

Table 2-20 Managing message files

Format	The name of a voicemail message file is in this format: vm_Called party-Calling party-Random code.pcm. For example: vm_200-6033432345-946685192.pcm. If the user presses Replay or Next when listening to a voicemail message or the voicemail message is played, the message will be identified with the file name become oldvm_200-6033432345-946685192.pcm. Note: The filename extensions are varied depending on the codec of the voicemail message: □ G.711μ: The file extension is .pcm. □ G.711a: The file extension is .pcma. □ G.729: The file extension is .dat. □ G.722: The file extension is .g722. □ G.722.2: The file extension is .g722B.
View the voicemail message files	□ Go to Application > Storage to get the access path and view the voicemail message files in the browser. Click builtin to view the files recorded through internal USB flash drive, and usb to view the files recorded through external USB device. The typical example of the storage path is: Recorder/voicemail. □ If recorded files are stored in an external USB device, you can remove the USB device from the LS20 and connect it to your PC, then view the recorded files. The typical example of the storage path is: G:\Recorder\ voicemail.
Listen to the voicemail message files	□ Analog phone: Press *98 and listen to the voicemail messages. You may hear: "You have no voicemail messages". "You have n new/saved voicemail messages" After the voicemail message is played, you may hear: "To repeat the message, press one. To delete, press two. To listen to the next message, press three". □ IP phone: Configure the feature access code for listening to the voice messages by MWI function key and memory key. For details about the configuration on New Rock's IP phone, see NRP User Manual.
Backup and clear voicemail message files	Same as Table 2-18.

2.8 FoIP

A fax machine can be connected to either FXS port on the LS20 or the FXS port of the gateway registered to LS20. To send a fax message, dial the fax number just like making an outbound call. For details, see 2.5.2 Making Outbound Calls.

Go to **Application > Fax**, and set the fax parameters.

Figure 2-34 FAX configuration interface

Table 2-21 FAX parameters

Item	Description
Initial offer	To configure codecs in the range of RTP ports for fax transmission, click Modify to go to Media page for modification. For details, see Table 2-29. Note: For G.711 pass-through mode, be sure to select G.711U/20 or G.711A/20 as initial codecs to ensure a successful fax relay.
Transport mode	The device supports two fax transport modes: T.38 relay and G.711 pass-through . The fax transport modes should be selected based on the service provider's requirement. □ Transport via analog trunk: Select G.711 pass-through □ Transport via SIP trunk: Select the fax transport mode based on the service provider's capabilities. If the SIP trunk provider supports both T.38 relay and G.711 pass-through, it is recommended to select T.38 relay for more reliable transport.
Max. fax rate	Select the fax maximum transmission rate. The fax messages can be sent at either the higher speed of 33,600 bps or the lower speed of 14,400 bps. Note: the service provider's gateways must support T.38 version 3 with V.34 for the fax to actually be sent at 33,600bps, otherwise, it will fall back to V.17 speeds (14,400bps).
Port for fax transmission	Set whether to use a new RTP port when the gateway switches to the T.38 mode. The default value is Use original RTP port .
ECM mode	The error correction mode (ECM) for the fax feature. The default setting is varied depending on the fax transport mode. □ When the maximum transmission rate is 14400 bps, this mode is disabled by default. When the maximum transmission rate is 33600 bps, this mode is enabled by default.

Item	Description
Output gain control	Set the output gain for T.38 fax. The value ranges from -6 dB to 6 dB with the default value 0 dB.
Packet size	Set the T.38 data packet interval for T.38. The options include 30 ms and 40 ms. The default value is 30 ms.
Signaling redundancy level	Set the number of signaling redundant frames in T.38 data packets. The range is 0 to 6 frames, and the default value is 4 frames.
Image Data Redundancy level	Set the number of image data frames in T.38 data packets. The range is 0 to 2 frames, and the default value is 1 frames.
Allow opposite terminal to switch to T.38	When the device serves as a fax sending terminal with G.711 pass-through , the fax transport mode will automatically switch to T.38 relay if the T.38 negotiation request is sent from the opposite terminal.



Note

It is recommended to assign a DID trunk for the extension used for fax transmission. For details, see 2.5.9 DID.

2.9 System Settings

2.9.1 Built-in Storage Management

The LS20 has an internal storage device of 16 GB.

The internal USB flash drive of the LS20 is used for storing recording files, comments, logs, audio files, etc.

The data in the internal storage is not lost after the device reboots.

Go to **Application > Storage** to manage the internal storage for LS20. Storage space is allocated by default as follows:

Item	Space
Recording	10,240MB
Log	3072MB
Audio file	1024MB
Others	800MB

To expand the storage space for LS20, connect an external storage device to the USB port on the device. You can click **Backup** to back up recording files to the external storage device, and then click **Clear** to delete files from the internal USB flash drive. Before backing up files, ensure that sufficient free space is available in the external storage device.

Figure 2-35 Storage interface

2.9.2 Work schedule

Work schedule allows you to set detailed time ranges for work hour and off hour.

Note: if you configure a work schedule, the time schedule configured on **Basic > Auto attendant** page will be invalid.

Step1 Go to **Application > Work schedule**, click  to add a rule.

Figure 2-36 Work schedule interface

Table 2-22 Work schedule parameter description

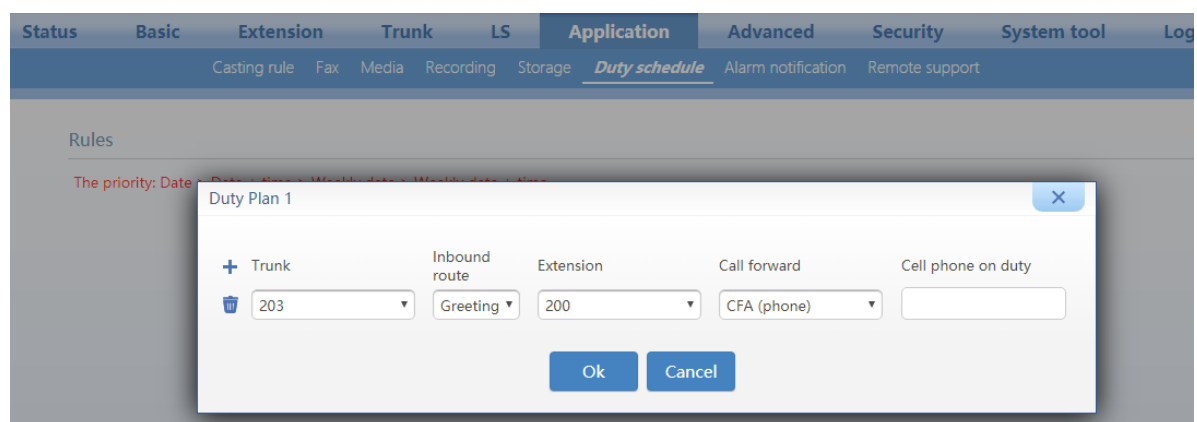
Item	Description
Period	A cycle by which a rule runs periodically. Each rule runs periodically by week or by month.

Item	Description
Date	Choose the dates when the rule takes effect. If you choose Week for period, you need to tick the dates within a week. If you choose Month, you need to input the specified dates in the format of “month.day”, for example, 10.1, 10.2 means October 1 st and October 2 nd . Commas are needed to separate multiple dates.
Validate at time	Set the time at which the rule begins to take effect. Note: Keeping the time empty indicates the rule takes effect for the whole day. If multiple rules cover the same time, for example, four rules are supposedly cover the time of 10:00 on March 1 st , from the highest priority to the lowest priority, the rules are ordered as follows: The rule whose Date (Month) is specified The rule whose Date (Month) and Validate time are specified The rule whose Date (Week) is specified The rule whose Date (Week) and Validate time are specified
Time plan	Choose the name of a time plan from the drop-down list. Here you only choose a name of a time plan, the details of the time plan should be configured by clicking  .
Details	Configure the details for the time plan.

Step2 Click  to configure the details for the time plan.

Attention: Only Duty Plan 1 can specify the trunks whose incoming calls need to be transferred to a mobile phone. You cannot add or delete trunks for the other duty plans , but can modify the mobile phone number.

Figure 2-37 Time plan details

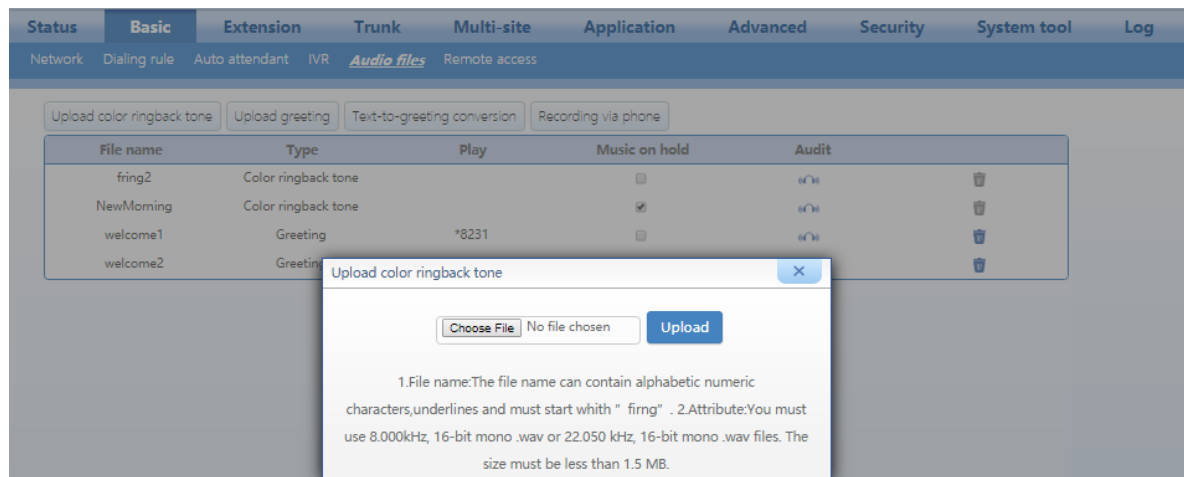


2.9.3 CRBT

Step 1 Go to **Basic > IVR**, click **Upload color ringback tone**, and locate and then upload a CRBT file. If the name of the uploaded CRBT file is the same as that of an existing CRBT file, the existing RBT file will be overwritten.

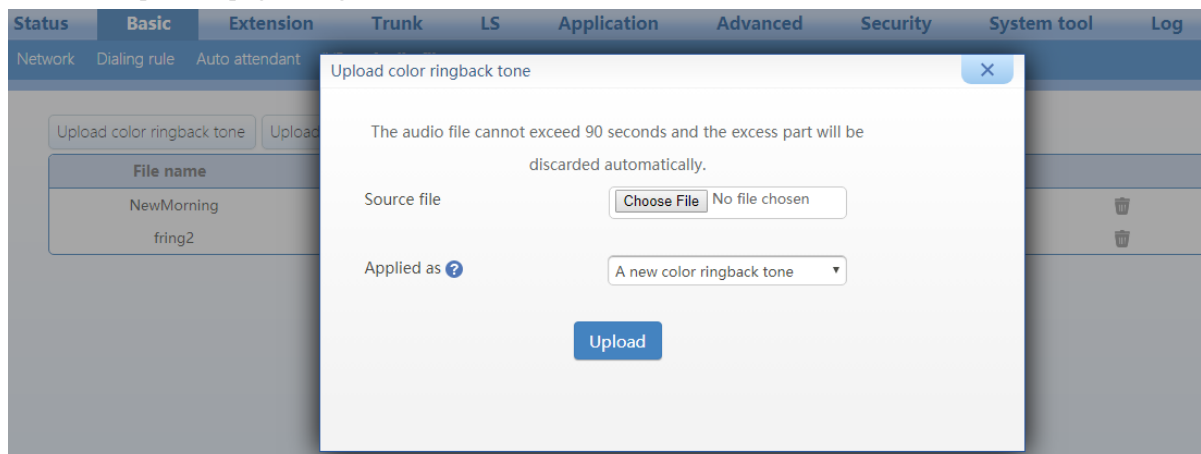
The name of the uploaded audio file must be "fring+number", for example, fring1; the format must be .wav; and the size must not exceed 1.5 MB. The uploaded file is stored in the built-in storage unit (the path is /media/sda1/ann). The number of audio files is only limited by the amount of space available on the built-in storage unit.

Figure 2-38 CRBT file uploading interface



The audio file conversion tool of New Rock Technologies Inc. can be used to convert a customized audio file into a CRBT file supported by the LS20. For details on how to use the tool, see the [User Guide for Telegreeting](#).

The method referred earlier has a strict limit to the audio files. So, you are recommended to follow the instruction on the Web GUI to download and install the Telegreeting software. After that, reopen the page to upload audio files, then all audio files with the following file extensions are allowed to be uploaded: MP3, WAV, M4A, WMA, AAC, OGG, AMR, 3GPP. Make sure to reopen the page using Firefox or Chrome browser.



Step 2 Click on the **Extension>Analog/IP ext.** page to set the sequence number of the CRBT file to be used for your extension.

Click  to play the CRBT file.

Step 3 Click **Save** to save the configuration.

CRBT files can be used to set background music. For details, see 2.9.4 Music on Hold.

2.9.4 Music on Hold

Background music will be played for the party that is placed on hold. Two background music files are available by default: fring2 and New Morning. You can customize and upload audio files.

CRBT audio files and background music audio files can be shared by the device. For information about uploading a customized audio file, see 2.9.3 CRBT.

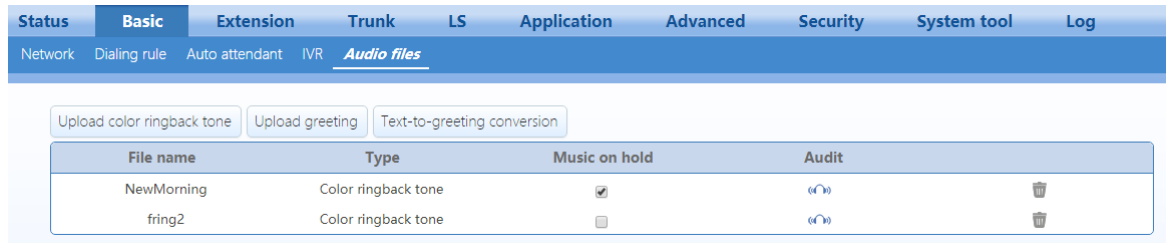
After uploading an audio file, follow this procedure to set background music:

Step 1 Go to **Basic > Audio files**, select the check box of the desired audio file below **Music on hold**, and then click **OK**.

To play the audio file, click .

To delete an audio file, click .

Figure 2-39 Music on hold configuration interface



File name	Type	Music on hold	Audit	
NewMorning	Color ringback tone	☒		
fring2	Color ringback tone	☐		

2.9.5 Time

The device gets its time from a time server in the network. The device provides a cell for the clock system to ensure normal running of the system in case of a power failure.

Click **System tools > System time**, and configure the time server.

Figure 2-40 System time configuration interface

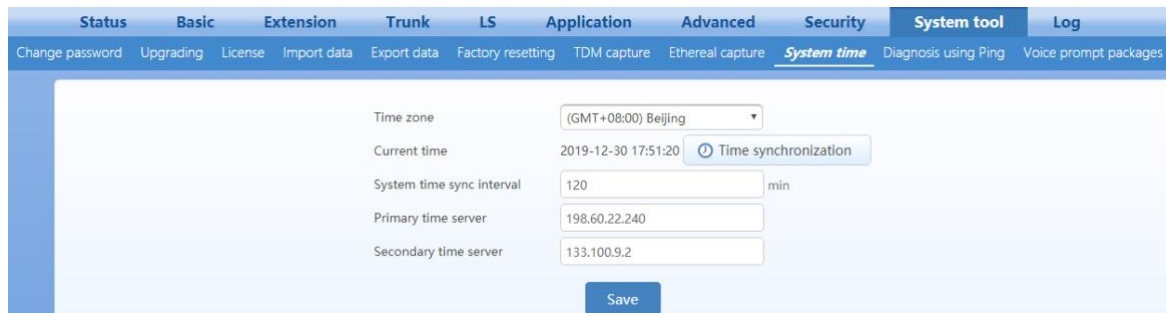


Table 2-23 System time parameters

Item	Description
Time Zone	Select the time zone according to the region where the device is located.
Current time	Displays the current time of the device. You can click Time synchronization to calibrate the time.
System time sync interval	Interval for the device to synchronize with the time server. The default value is 120 minutes.
Primary time server	Enter the IP address of primary 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.



Note

If the device cannot synchronize with a time server, you can click **Time synchronization** to set the time of your PC as the system time of the device.

2.9.6 Routing Table

A routing table is used to implement number replacement and route allocation. A routing table can contain up to 500 routing rules, which are applied in the order they appear in the table.

Go to **Advanced > Routing table**, and add routing rules. The routing rules are described below.

Number Transformation

Figure 2-41 Routing table configuration interface (number transformation)

1. Format of rules

You can add a rule either configuring through the configuration area or you can directly input a rule manually into the text box of the routing table.

Trunk type *called number prefix* **ADD** *added prefix*

This rule is used to add the *added prefix* to a called number matching the *called number prefix* for an outbound call.

Note: Trunk types include FXS and FXO. FXS indicates that the IP trunk is used to make outbound calls; FXO indicates that the analog trunk is used to make inbound calls

Examples:

- ☐ When an analog trunk is used to make an outbound call, the prefix 17909 is added to the number of the called party:

FXO *x* **ADD** 17909

- ☐ When an analog trunk is used to make a national toll call(for example: begins with 0), the prefix

17909 is added to the number of the called party:

FXO 0 ADD 17909

- When an analog trunk is used to make an international toll call(for example: begins with 00), the prefix 17909 is added to the number of the called party:

FXO 00 ADD 17909

- When a specified analog trunk is used to call a specified called party (for example, analog trunk 1, 2, 3, 4, or 6 is used to call a called number starting with 9), the prefix 17909 is added to the number of the called party:

FXO[1-4,6] 9 ADD 17909

- When an IP trunk is used to make an outbound call, the prefix 17909 is added to the number of the called party:

FXS x ADD 17909

- When an IP trunk is used to call a called number starting with 10, the prefix 17909 is added to the number of the called party:

FXS 10 ADD 17909

2. Description of configuration fields

Items	Description
Outbound call by	Choose a trunk type (analog trunk or IP trunk) from the drop-down list. If needed, click + to select specific trunk numbers or input trunk numbers in the text box, use a comma “,” to separate them if there are multiple numbers.
Called number matched	Choose Any or Specified . If you choose Specified , input the prefix of the called number to be matched. For example, input 0, then all outbound calls to a called number starting with 0 will be matched.
Add prefix	Input a prefix to be added to the called number. For example, input 9, then when you dial a called number (given it is 22222222) which is matched this rule, the LS20 will place a call to 92222222.

Example: configure a routing rule to add a prefix 17909 to all outbound calls via analog trunks.

Do as follows:

1. Choose **Analog trunk** from the drop-down list.
2. Choose **Any** for called number to be matched.
3. Input 17909 for added prefix.
4. Click **Add to routing table**.
5. Then you can see the rule is added to the routing table:

FXO X ADD 17909

StatusBasicExtensionTrunkLSApplicationAdvancedSecuritySystem toolLog

SystemCert.Feature access codesRoutingDialingToneSIPDTMFCall record

Number transformationLimit the call durationRouteItems marked with * are required

Outbound call by

Called number matched

Add prefix

* Analog trunk

☒ Any ☐ Specified

* 17909

Select or input port numbers, separated by a comma *.*+

Add to routing table

Routing table [Change the display mode](#)

FXO X ADD 17909

SaveRefresh

Call Duration Restriction

Figure 2-42 Routing table configuration interface- Limit the call duration

StatusBasicExtensionTrunkLSApplicationAdvancedSecuritySystem toolLog

SystemCert.Feature access codesRoutingDialingToneSIPDTMFCall record

Number transformationLimit the call durationRouteItems marked with * are required

Prefix of called number

Time duration (Min)

* Input prefix or number of called party

* Input the time duration

Add to routing table

Routing table [Change the display mode](#)

FXO X ADD 17909

SaveRefresh

1. **Format of rules**
You can add a rule either configuring through the configuration area or you can directly input a rule manually into the text box of the routing table.

FXS *Called number prefix* **TIME** *Duration-limit-of-a-single-call/total-duration-limit/type/remaining-duration*

Note:

- ❑ The *remaining-duration* do not need to be configured, for it is calculated automatically by the system.
- ❑ The call duration restriction rule starts with "FXS" no matter the outbound call is made by an analog extension or an IP extension.

This rule restricts the call duration of an outbound call whose called number matches the *called number prefix*.

Type: there are two options, D indicates per day, M indicates per month.

Examples:

When a call is made to a specified called number (for example, a called number starting with 00), the call duration is restricted to 100 minutes per day, and there is no limit for a single call:

You should configure the rule as **FXS 00 TIME 0/100/D**, the rule will be displayed as **FXS 00 TIME 0/100/D/100**

2. Description of configuration fields

Items	Description
Prefix of called number	Input a prefix of the called number. This rule restricts the call duration of an outbound call whose called number matches the <i>called number prefix</i> .
Time duration (Min.)	Input a total duration for all matched calls. For example, input 100, indicates that the total call duration for all outbound calls which match the rules are restricted to 100 minutes.

Example: Configure a rule to restrict the call duration for all outbound international calls (given the international call prefix is 00).

Do as follows:

1. Input "00" in the text box of **Prefix of called number**.
2. Input "100" for **Time duration**.
3. Click **Add to routing table**.
4. Then you can see the rule is added to the routing table:

FXS 00 TIME 0/100/D

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
System Cert. Feature access codes Routing Dialing Tone SIP DTMF Call record									

Number transformation
Limit the call duration
Route
Items marked with * are required

Prefix of called number	Time duration (Min)
* 00	* 100

Add to routing table

Routing table [Change the display mode](#)

FXS 00 TIME 0/100/D

Save Refresh

Directional Route

Status	Basic	Extension	Trunk	LS	Application	Advanced	Security	System tool	Log
System Cert. Feature access codes Routing Dialing Tone SIP DTMF Call record									

Number transformation
Limit the call duration
Route
Items marked with * are required

Call from	Number matched	To
* Analog extension	* ☐ Caller ☒ Callee	* Analog trunk
Select or input port numbers, separated by a comma "*,*"	☐ Any ☒ Specified	Select line
* Input the prefix or number to be match		

Add to routing table

Routing table [Change the display mode](#)

FXS 00 TIME 0/100/D

Save Refresh

1. Format of rules

You can add a rule either configuring through the configuration area or you can directly input a rule manually into the text box of the routing table.

FXS *called number prefix* **ROUTE** *destination*

This rule is used to direct an outbound call whose called number matches the *called number prefix* to a

specified destination. And this rule requires the dialing rule is set to “Routing” on **Basic > Dialing rule** page.

Note: No matter the outbound call is made by an analog extension or an IP extension, the directional routing rule starts with "FXS". The destination can be FXO (analog trunk), IPT (IP trunk), or IP (IP address).

Examples:

- Called-party-number-based routing to an outbound analog trunk. In this example, calls to destination numbers starting with 6120 are routed to FXO port 1 or port 2 in sequential fashion

FXS 6120 ROUTE FXO 1-2

- Called-party-number based routing to an outbound SIP trunk. In this example, calls to destination numbers starting with 6120 are routed to SIP trunk with ID 1 to 6 in sequential fashion:

FXS 6120 ROUTE IPT 1-6

- Called party number based routing to an IP address. **FXS 6120 ROUTE IP
192.168.2.218**

2. Description of configuration fields

Items	Description
Call from	Choose a trunk type (analog trunk or IP trunk) from the drop-down list. If needed, click + to select specific extension numbers or input extension numbers in the text box, use a comma “,” to separate them if there are multiple numbers.
Number matched	Choose Caller or Callee , then choose Any or Specified . If you choose Specified , input the prefix of the number to be matched. For example, if you choose Caller and Specified and input 2, then all calls made by the extension whose number begins with 2 will match this rule.
To	Choose a destination for the outgoing call matched the rule.

- **Example:** Calls made by analog extensions to destination numbers starting with 6120 are routed to SIP trunk in sequential fashion

Do as follows:

1. Choose **Analog extension** for **Call from**.
2. Choose **Callee** and **Specified**, then input 6120 for **Number matched**.
3. Choose **SIP trunk** for **To**.

4. Then you can see the rule is added to the routing table:

FXS 6120 ROUTE IPT

The screenshot shows the 'Advanced' configuration page with the 'Routing' sub-tab selected. Under the 'Route' tab, a rule is being configured. The 'Call from' field is set to 'Analog extension'. The 'Number matched' field contains '6120'. The 'To' field is set to 'SIP trunk'. Below these fields is an 'Add to routing table' button. Underneath, the 'Routing table' is displayed, showing the rule 'FXS 6120 ROUTE IPT'. At the bottom are 'Save' and 'Refresh' buttons.

2.9.7 Dialed Number Detection and Digit Map

During the process of collecting DTMF digits, the device matches the receiving digit string with the rules in the digit map. The receiving process is completed when a matching pattern is encountered. A well-defined digit map helps to speed up the time it takes to dial a number.

Click **Advanced>Dialing**, and set digit map rules.

Figure 2-43 Dialing interface

The screenshot shows the 'Advanced' configuration page with the 'Dialing' sub-tab selected. Under the 'Dialing timers' section, there are three fields: 'Off-hook timer' set to 15s, 'Interdigit timer' set to 5s, and 'Complete entry timer' set to 2s. Below this is the 'Digit map' section, which contains a list of rules for digit matching. The rules are: 01[3-5,7,8]xxxxxxxx, 010xxxxxxxx, 02xxxxxxxx, 0[3-9]xxxxxxxx, 120, 11[0,2-9], 111xx, 123xx, 95105xxx, 95xxx, 100xx, 1[3-5,7,8]xxxxxxxx, and [2-3,5-7]xxxxxx. At the bottom are 'Save' and 'Refresh' buttons.

A digit map in the device is composed of up to 100 rules, each with up to 50 digits. The total length of a digit map is limited to 4,500 digits. 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 2-24 Description of a digit map

Character	Description
Off-hook timer	If an analog phone hasn't dialed any number within a specified time by this parameter after being offhook, the device will consider that the analog phone has given up the call and prompt them to hang up with a busy tone. The default value is 15s.
Interdigit timer	If an analog phone hasn't dialed the next number key from the time of dialing the last number key to the time set by this parameter, the device will consider that the dialed number is complete and outdial the dialed number. The default value is 5s.
Complete entry timer	It works with the "XXXXXXXXXX.T" rule in the digit map. The default value is 2s.
0-9, *, #	Matches a specific a DTMF digit.
x	Matches any single digit. For example, x can match 1 or 2 or 3...
.	Matches any string of DTMF digits. For example: "1." can match any DTMF numbers starting with "1".
T	End of collecting DTMF digits after the timeout waiting for the next digit. For example, x.T means matching a string (a DTMF string) with any length. The ending is triggered by the timeout for waiting for the next digit.
[]	Matches to a set of DTMF digits. For example: [1-3,5,7-9] means the set of 1, 2, 3, 5, 7, 8 and 9.
xxxxxxxxxx.T	For a number with 10 digits, or less than 10 digits, the device terminates receiving digits and sends detected numbers if the duration of no dialing period exceeded the value of the Interdigit timer parameter. For a number with more than 10 digits, the device terminates receiving digits and sends detected numbers if the duration of no dialing period exceeded the value of the Complete entry timer parameter.
x.#	If "#" is received after any digit is received, the device terminates receiving digits.
[2-8]xxxxxxx	The device terminates receiving digits after receiving eight digits starting with any digits between 2 and 8.
02xxxxxxxxx	The device terminates receiving digits after receiving 11 digits starting with 02.
013xxxxxxxxx	The device terminates receiving digits after receiving 12 digits starting with 013.
13xxxxxxxxx	The device terminates receiving digits after receiving 11 digits starting with 13.
11x	The device terminates receiving digits after receiving three digits starting with 11.
9xxxx	The device terminates receiving digits after receiving five digits starting with 9.

2.9.8 Call Progress Tone

Go to **Advanced> tone**, and set or customize prompt tones according to the country or region, such as set dial tone, busy tone, and ring back tone.

Figure 2-44 Call progress tone interface

Table 2-25 Call progress tone parameters

Item	Description
Tones	Customized: you can customize the following call prompt tones.
Country/Region	There are call progress tone plans for several countries and regions that are pre-programmed in the device. Users can also specify the tone plan according to the national standard. The device provides tone plans for the following countries and regions: China, the United States, Singapore, Israel, Malaysia, Indonesia, United Arab Emirates, Australia, Republic of Zimbabwe, France, Italy, Germany, Mexico, Chile, Russia, Japan, Korea, Hong Kong, Taiwan, India, Sudan, Iran, Algeria, Pakistan, Philippines, Kazakhstan, Turkey, and Argentina.
Dial tone	Prompt tone for off-hook dial tone.
Second dial tone	Used for the second stage dial tone.
Stutter dial tone	Used to notify the following conditions: 1. DND or unconditional call forwarding is activated, or there is new voice message arrived.
Busy tone	Used to notify the caller of a busy line condition.
Congestion tone/reorder 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 to notify the off-hook and no dial activity status of the analog phone.
Call waiting tone	Used to notify the subscriber who is engaged on a call that another caller is attempting to call.
Confirmation tone	Used to confirm feature access codes being entered.

Table 2-26 Examples of customized tone

Examples	Description
350+440 (dial tone)	Indicates the dual-frequency tone consisting of 350 and 440 Hz

Examples	Description
480+620/500,0/500 (busy)	Indicates the dual-frequency tone consisting of 480 and 620 Hz, repeated playing with 500 ms on and 500 ms off. Note: 0/500 indicates 500 ms mute.
440/300,0/10000,440/30 0,0/10000	Indicates 440 Hz single frequency tone, repeated twice, with 300 ms on and 10s off.
950/333,1400/333,1800/ 333,0/1000	Indicates repeated playing of 333 ms of 950 Hz, 333 ms of 1400 Hz, 333 ms of 1800 Hz, and mute of 1 second.

2.9.9 SIP Advanced Configuration

Go to **Advanced> SIP**, and set SIP compatibility information.

Figure 2-45 SIP related configuration interface

Table 2-27 SIP related parameters

Item	Description
PRACK	Determine whether to activate Provisional Response ACKnowledgement (PRACK). (RFC 3262) It is not selected by default.
Early media	Enable RFC5009. It is not enabled by default.
Media direction attribute	Set parameter values of the P-Early-Media header field: ☐ Supported ☐ Sendrecv ☐ Sendonly ☐ recvonly ☐ Inactive The fields vary according to the type of SIP message. They should be set as required by the peer end. Note: This parameter can be configured after Early media is selected.

Item	Description
Session timer	UAs send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The interval for the session refresh requests is determined through negotiation between UAs. If a session refresh request is not received before the interval passes, the session is considered terminated. Both UAs are supposed to send a BYE, and call stateful proxies can remove any state for the call. The refresher and refresh interval are determined based on the negotiation among related parties in the session (including the two parties in the session and the traversing proxies). The refresh interval (carried by the header field of Session-Expires) cannot be less than the Minimum timer (carried by the header field of Min-SE). The session refresh function is disabled by default. It is advisable to enable it if the resource release mechanism is incomplete for session-related parties (for example, if there is no RTP stream detection or BYE request timeout detection). After session refresh is enabled: If the device is the calling party, it sends INVITE requests that contain session refresh header field. If the device is the called party, it inserts the final session refresh interval and recommended refresher into the 200 OK message to finish the negotiation.
Session interval	The session refresh interval is the value contained in the Session-Expires header field of INVITE or UPDATE requests. The value range is 30s to 65535s, and the default value is 1800s.
Minimum timer	The minimum session refresh interval allowed by the device. The value range is 30s to 65535s, and the default value is 1800s. The final session refresh interval cannot be less than this value.
Selecting the receiving port for response	Use the receiving port of proxy or use the sending port of proxy. Using received port to send response as default. Use the proxy receiving port or the proxy sending port. The received port is used to send a response as default.
To header field	Choose whether to apply a Sub domain name or an 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 the Host name or Local IP address. The default is Local IP address .
Called party number	Choose whether the gateway acquires the called number from Request Line header field or the "To" header field. The default is From Request line field .
Target number in Contact Header of 302 message	In case of call forwarding, this parameter is used to specify whether the prefix added in the routing rules is included in the target number in the Contact header field of the 302 message sent by the device. This parameter works only when all the following conditions are met: □ FT_FAT_X=on is set for the IP trunk. □ DID to an extension is set for the IP trunk. □ Call forwarding to an external target number (e.g. 13812345678) is set for the corresponding DID extension. □ A routing rule is configured in which a prefix is added for outbound calls to the target number through an IP trunk (e.g. for routing rule FXS 138 ADD 9). □ If this parameter is selected, the target number in the Contact header field of the 302 message sent by the device includes the prefix 9 set in the routing rule, for example 913812345678. Otherwise, the target number in the Contact will be 13812345678.

2.9.10 DTMF

Go to **Advanced > DTMF**, and configure DTMF information.

Figure 2-46 DTMF interface

Table 2-28 DTMF parameters

Item	Description
Transmission method	Transmission modes for the DTMF signal supported by the device include RFC 2833, Audio and SIP INFO. The default value is RFC 2833. □ RFC2833: Separate the DTMF signal from the media stream and transmit it to the platform through an RTP data package in the format of RFC2833. □ Audio: The DTMF signal is transmitted to the platform in-band. □ SIP INFO: Separate the DTMF signal from the media stream and transmit it to the platform in the SIP INFO message format.
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 is 96 - 127. This parameter should match the setting of a far-end device (e.g. a platform).
DTMF Tone duration	This parameter sets the on time (in ms) of the DTMF signal sent from the FXO port. The default value is 100 ms. The duration time range is 50 - 150 ms.
DTMF Inderdigit pause	This parameter sets the off time (ms) of the DTMF signal sent from the FXO 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. The valid value ranges from 32 to 96 ms in multiples of 16 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	The valid values should be multiples of 16. Increasing the value can prevent false detection of DTMF signal.

2.9.11 Media

Go to **Application > Media**, and set IP media parameters.

Figure 2-47 Media configuration interface

The screenshot displays the 'Media' configuration page within the LS20 Administrator interface. The top navigation bar includes tabs for Status, Basic, Extension, Trunk, LS, Application (selected), Advanced, Security, System tool, and Log. Below this, a sub-navigation bar shows options like Casting rule, Fax, Media (selected), Recording, Storage, Duty schedule, Alarm notification, and Remote support.

The main configuration area includes the following settings:

- Codec:** A list of codecs with 'Disabled codecs' and 'Enabled codecs' sections. Enabled codecs include G.711U/20, G.711A/20, and G.729A/20.
- RTP port min.:** Set to 10010 (Range: 3000 - 65535).
- RTP port max.:** Set to 10266 (Range: 3020 - 65535).
- TOS/DSCP:** Set to 0x0C.
- Min. jitter buffer:** Set to 2 frame (Range: 0 - 30, Default: 3). Higher value results in long delay.
- Max. jitter buffer:** Set to 50 frame (Range: 10 - 250, Default: 50).
- RTP drop SID:** Checked.
- Obtain Media Address From:** Radio buttons for 'SDP Global Address' (selected) and 'SDP Media Address'.
- Echo cancellation:** Checked.
- Echo suppression:** Checked.
- Time threshold for echo:** Set to 150 ms (Range: 0 - 300).

A 'Save' button is located at the bottom right of the configuration area.

Table 2-29 Media parameters

Item	Description
Codec	Support G729A/20, PCMU/20, PCMA/20, G.722.2/20, and G.722/20. Multiple codec types can be set separated by a comma, and in this case the device will sequentially negotiate a codec with the peer SIP device.
RTP port Min.	The lower boundary of RTP transmission and the receiving port. The value range is 3000 to 65535 and the default value is 10010. It is recommended that the value be greater than or equal to 10000. Note: Each phone call will occupy RTP and RTCP ports. If the device is equipped with 4 subscriber lines (or trunk line), then 8 UDP ports are needed.
RTP port Max.	The upper boundary of RTP transmission and the receiving port. The value range is 3020 to 65535, and the default value is 10266. The configured value must be greater than or equal to "2 X number of lines + min. RPT port".
TOS/DSCP	Set the service level quality as a guarantee for different priorities. The default value is 0x0c. This parameter specifies the priorities of media streaming.
Max. Jitter buffer	The RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This parameter specifies the maximum number of RTP packets that can be stored in the buffer area. The value range is 0 to 30 frames, and the default value is 2 frames.
Min. Jitter buffer	RTP Jitter Buffer is constructed to reduce the influence brought by network jitter. This parameter specifies the minimum number of RTP packets that need to be stored in the buffer area. The value range is 10 to 250 frames, and the default value is 50 frames.
RTP drop SID	If it is selected, the received RTP SID voice packets will be discarded. By default, this is not selected. Note: RTP SID packets should be dropped only when they do not conform to the specifications. Nonstandard RTP SID data could generate noise in calls.
Obtain Media Address From	SDP global address: obtain the media destination IP address from the global connection entry in received SDPs; SDP media address: Obtain the media destination IP address from the first media description in received SDPs. If the first media descriptor in a received SDP does not contain an IP address, the global connection address is used.

Item	Description
Echo cancellation	By default, it is enabled.
Echo suppression	By default, it is enabled.
Time threshold for echo suppression	Its value ranges from 0 to 300 ms, the default value is 150 ms.

2.9.12 Call Detail Record (CDR)

The device is capable of outputting a detailed record for each call to an external storage server. The information of a CDR includes (among many details), the calling party number, called party number, and the starting and ending timestamps of a call.

The detailed call records are output to a storage server after the completion of a call, and they can be read, searched, saved and deleted through a pre-installed software "CDR software". For details about using the CDR software, see the *CDR Software User Guide*.

Go to **Advanced > Call record**, and set the IP address and port number of the CDR server. The default port number is 1809.

Figure 2-48 CDR server configuration interface

2.9.13 SIP Transmission Mode

Go to **Advanced > System**, and set SIP transmission mode.

Figure 2-49 SIP transmission mode configuration interface

Table 2-30 SIP transmission mode parameters

Item	Description
SIP transport type	Select either UDP&TCP or UDP for SIP messages, and the default is UDP. Both sides must select the same transmission protocol.
SIP TCP local port	Local SIP port used when TCP is used.

2.9.14 Auto Provisioning

The auto provision function allows you to centrally manage software and configuration files for the device by using an auto provisioning server (ACS).

Go to **Advanced > System**, choose Auto provision for management type.

Figure 2-50 Auto provision interface

Table 2-31 Auto provision parameters

Item	Description
Obtain ACS address via DHCP option 66	ACS (TFTP/HTTP/HTTPS) address is obtained by using option 66 of the DHCP
ACS URL	Manually configure the ACS address, which can be a TFTP, FTP, or HTTP server. ☐ tftp://ACS address ☐ ftp:// ACS address ☐ http:// ACS address ☐ https://ACS address
User name	Input a user name for accessing the ACS. Note: If the ACS is a TFTP server, the username and the password are not displayed.
Password	Input a password for accessing the ACS.
Firmware upgrade	Download the firmware upgrade package from the firmware upgrade package address set in the configuration file. The device will automatically upgrade the firmware. Note: For the LS20, the firmware can be a tar.gz file or an img file.
Update mode	☐ Power on: The device detects whether there are configurations and firmware to be updated when the device is powered on. ☐ Power on + Periodic: 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 + Period is set, this parameter specifies the interval for periodic automatic upgrades. The default is 3600s. The value range is 5 to 86400 second.

2.9.15 TR069

Go to **Advanced > System**.

Figure 2-51 TR069 interface

The screenshot displays the TR069 configuration page within the LS20 Administrator interface. The top navigation bar includes tabs for Status, Basic, Extension, Trunk, LS, Application, **Advanced**, Security, System tool, and Log. Under the 'Advanced' tab, the 'System' sub-tab is selected, showing options like Cert., Feature access codes, Routing, Dialing, Tone, SIP, DTMF, and Call record. The main configuration area includes:

- forward no answer ring counts**: A dropdown menu.
- Area/country code**: A section header.
- Local area code**: A text input field.
- Data transmit**: A section header.
- SIP transport type**: Radio buttons for UDP&TCP and **UDP**.
- Management system type**: A section header.
- Type**: A dropdown menu set to TR069.
- ACS-URL**: A text input field with a help icon.
- Username**: A text input field.
- Password**: A text input field.
- Serial number**: A text input field.
- Periodic inform enable**: Radio buttons for **On** and **Off**.
- Periodic inform interval**: A text input field set to 900, with a range of 60 - 7200 seconds.
- Connection request URL**: A text input field.
- Connection request username**: A text input field.
- Connection request password**: A text input field.
- Save**: A blue button at the bottom right.

Table 2-32 TR069 parameters

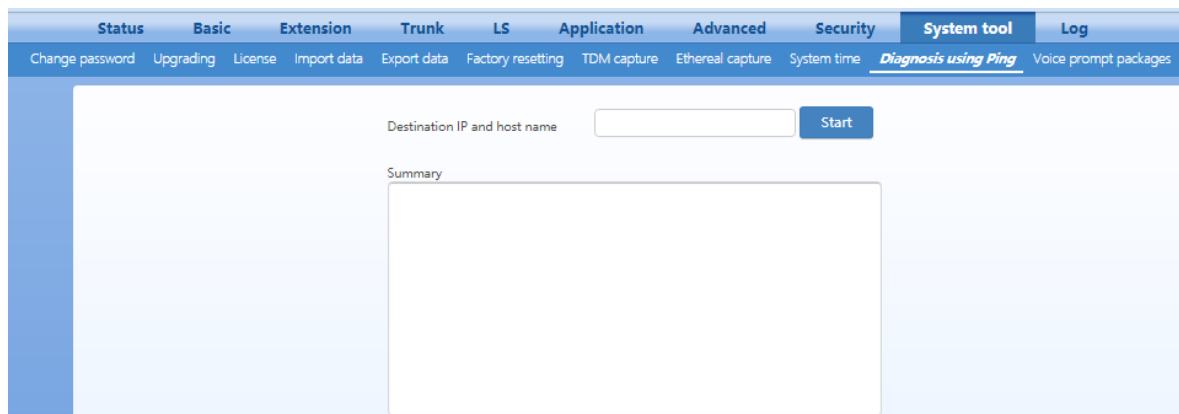
Item	Description
ACS-URL	Specify the URL of the ACS.
User name	Specify the user name to be used by the device to authenticate with the ACS.
Password	Specify the password to be used by the device to authenticate with the file server
Serial number	Serial number of the product. By default, it is the MAC address provided by New Rock. When the device is connected to the operator's network management server, the serial number provided by the operator can be entered.
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. Generally, it is automatically generated. You can also enter the address of the device manually.
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.

2.9.16 Ping Diagnosis

This tool is used to check the connectivity of the network.

Go to **System tools>Diagnosis using ping**, enter the IP address or host name, and start diagnosis. The diagnosis details can be seen in the **Summary** box.

Figure 2-52 Ping diagnosis interface



2.9.17 Voice prompt packages (system voice prompt files)

A voice prompt package contains all system voice prompt files for a language. For details of the system voice files, see Table 2-33.

To upload a voice prompt package, follow this procedure:

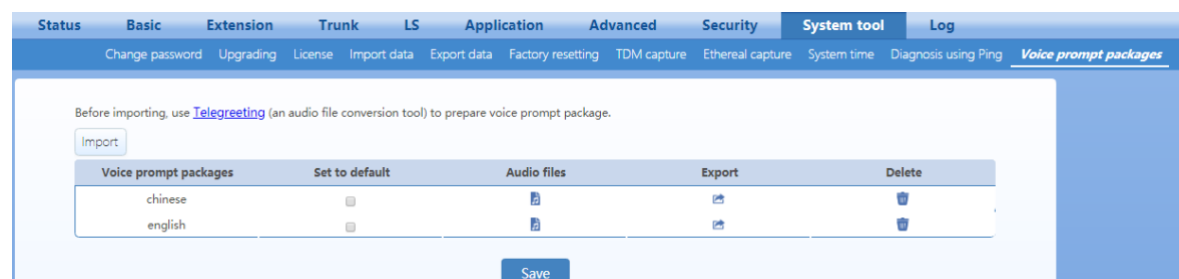
Step 1 Go to **System tool>Voice prompt packages**.

Step 2 Click **Import** to import the prepared voice prompt package.

Please use *Telegreeting*, an audio file conversion tool developed by New Rock Technologies, Inc., to prepare voice prompt package. For details, see *User Guide for Telegreeting*.

Step 3 Enable the **Set to default** checkbox to set a default language for system voice prompt.

Figure 2-53 Voice prompt packages interface



Step 4 If required, click and then upload an audio file to replace the existing file.

Figure 2-54 Audio file configuration interface

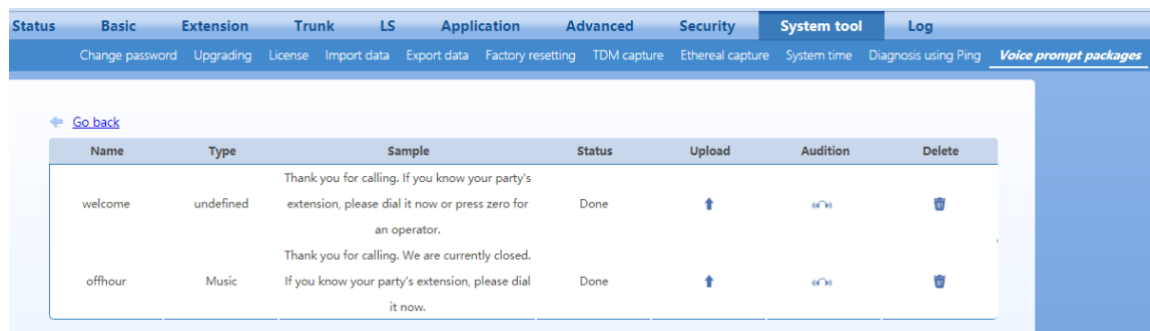


Table 2-33 System voice prompt files

File	Content
0_tip	Zero
1_tip	One
2_tip	Two
3_tip	Three
4_tip	Four
5_tip	Five
6_tip	Six
7_tip	Seven
8_tip	Eight
9_tip	Nine
account	Please enter the extension number, followed by the PIN.
block	You are not authorized to make this call. Please contact the administrator.
busy	That line is busy. Enter another number now, or hold for an operator.
call waiting	Please hold. That line is busy, but your party has been notified of your call.
cancel	The feature is now deactivated.
confirm	The feature is now activated.
connect	Please hold while your call is transferred.
disable	Disable.
dnd	The extension you are trying to reach has do-not-disturb activated. Please hang up.
dot_tip	Dot.
enable	Enable.
gateway	Gateway.
group busy	Please hold. All lines are busy.
hang-up	Your call is being disconnected. Thank you for calling.
hangup2	This call will be disconnected in one minute.
ip_tip	IP address.
IVR1	For call forward, press one. For voicemail, press two. Do not disturb: three. Call forking: four. Call waiting: five. Color ringback tone: six. For other extensions, press seven. To repeat this message, press nine.
IVR2	Enter the extension number, followed by the PIN then pound.

File	Content
IVR3	Sorry, the feature cannot be activated.
IVR4	To obtain the current settings, press star; To return to the previous menu, press pound.
IVR5	The feature is now activated.
IVR6	Sorry, the feature cannot be activated.
wrong	Sorry, the feature cannot be activated.
IVR7	The feature is now deactivated.
IVR8	This is an invalid PIN, please enter a new PIN.
reenter	This is an invalid PIN, please enter a new PIN.
IVR9	The current setting is ____
setting	The current setting is ____
IVR10	To activate do not disturb, press one. To deactivate, press zero.
IVR11	To disable voicemail, press zero. To forward all calls to voicemail, press one. To forward busy or no-answer calls to voicemail, press two.
IVR12	To listen to the color ringback tone, press star. To change, press two, To disable, press zero. To return to the previous menu, press pound.
IVR14	To set the target number, press one.
IVR14A	To disable call forking, press zero. To enable and set destination number, press one.
IVR15	Enter the extension number, followed by the PIN. When done, press pound.
IVR16	To disable call forward, press zero. To set the target number, press nine. To forward all calls, press one. To enable call forward busy or no answer, press two. To obtain the current settings, press star; To return to the previous menu, press pound.
IVR18	This is an invalid PIN, please enter a new PIN.
netmask	Netmask.
noanswer	There is no answer. Please enter another number, or hang up.
nocircuit	All circuits are busy. Please try your call again later.
nonumber	The number you have entered is not valid. Please check the number and enter again, or press zero for an operator.
offhour	Thank you for calling. We are currently closed. If you know your party's extension, enter it now.
operator	Please hold while your call is transferred to an operator.
operbusy	All operators are busy. Please enter another number or press star to hold.
port	Port.
record	Please record your message at the tone, and hang up when done.
tryagain	Your call cannot be completed, please try again later
version	Firmware version.
vm_all	Your call will be forwarded to voicemail. Leave your message at the tone and hang up when done.
vm_busy	That line is busy. Leave your message at the tone and hang up when done.
vm_fail	Your call cannot be completed, Leave your message at the tone and hang up when done.
vm_noans	Your party did not answer. Leave your message at the tone and hang up when done.
webport	Web access port

File	Content
welcome	Thank you for calling. If you know your party's extension, enter it now, or press zero for an operator.
vm_new	___ new voicemail messages.
vm_no	You have no voicemail messages.
vm_old	___ saved voicemail messages.
vm_pre	You have ___
vm_prompt	To repeat the message, press one. To delete, press two. To listen to the next message, press three.
wakeup	Hello, this is your scheduled notification.
btime	Sorry, you are not authorized to make calls at this time, please contact the administrator.
binternal	Sorry, you are not authorized to make outgoing call, please contact the administrator.
lock	Sorry, your extension is locked. Please unlock it.
bres	Sorry, you are not allowed to call this number.
bdomestic	Sorry, you are not authorized to make international calls, please contact the administrator.
bloclal	Sorry, you are not authorized to make long distance calls, please contact the administrator.

2.10 Security management

2.10.1 Access list

Go to the **Security>Access list** page to enter the IP addresses that are allowed to access the web or SSH service on the device.

After the Whitelist function is enabled, only IP addresses in the Whitelist are allowed to access the web or SSH service on the LS20. The LS20 also provides an embedded white-listed address 192.168.2.100 upon factory delivery, in addition to the customized Whitelist.

Follow this procedure:

Step1 Go to **Security > Firewall**, click **Add**, and enter an address. A maximum of 20 addresses can be added.

Figure 2-55 Whitelist interface

Table 2-34 Access list parameters

Item	Description
Authorized IP addresses	Click Add , enter the IP address allowed to access the LS20.
Service	Select services that can be accessed, such as SSH, HTTP and HTTPS.
Delete	Delete the current entry from the Whitelist.

Step2 Click **Save** to save the configuration.

Step3 Click **Enable**.



Note

- To access the device by using a SSH session, you also need to enable the SSH service on the **Security > Security** page.
- If you forgot the white-listed address previously set and cannot access the device it can be recovered. For details, see 3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?

2.10.2 Brute Force Login Prevention

A brute force login attack makes multiple login attempts within a short time period, trying to guess the password to login. To prevent brute force login attacks, the LS20 provides several methods including CAPTCHA for logging into Web GUI, limiting the number of login attempts, and access whitelist of trusted IP addresses.

Login Retry Lockout Configuration

After a specified number of login attempts within a specified time, the source IP address of the accessor

will be blocked.

After login, go to **Security > Brute force login prevention** page to configure.

Figure 2-56 Brute Force Login Prevention (Login Retry Lockout) Configuration Interface

Table 2-35 Login Retry Lockout Parameters

Name	Description
Max. login failure	Specify the maximum number of login failures allowed for a source IP address from which login attempts are made to the Web GUI or SSH in a day. The IP addresses whose login attempts exceeding the specified limit will be added to the locked list. Value range: 1 to 6 times/day Default value: 3 times/day
Lock time	Specify the IP address lock time. An IP address will be unlocked after the lock time and is allowed to access the device again. Default value: 10 minutes

Locked IP addresses

You may view or delete the IP address from the locked list.

Figure 2-57 Brute Force Login Prevention (Lockout IP Addresses) Interface

Table 2-36 Brute Force Login Prevention (Lockout IP Addresses) Information

Name	Description
IP address	Indicates a locked IP address.
Date	Indicates the date when an IP address is locked.
Services	Indicates the login method of the locked IP address (Web or SSH).

2.10.3 ACL-based Traffic Filtering

Access Control List (ACL) based filtering provides predictable traffic filtering. You can configure filtering rules to allow or deny receiving packets from specified IP addresses to certain ports on the device. For example, if a remote host (with the IP address x.x.x.x) is allowed to connect to a certain service using port X, create an ACCEPT rule to allow traffic from IP address x.x.x.x destined to port X on the device.

After login, go to **Security > Firewall > Static defense** to go to the configure interface.

Figure 2-58 Static Defense Configuration Interface

Table 2-37 Static Defense Configuration Parameters

Name	Description
Accept/Block	Specify whether to receive or block data packets when the specified conditions are matched (source IP address, local port, protocol).
Local port	Specify the local port range of the device for receiving data packets. Range is 0 to 65535.
Source IP address	Specify the source IP address range. Note: This parameter does not support domain names.
Protocol	Specify the protocol type. The value can be set to TCP , UDP , ICMP , or any .

You may do the following operations:

- ☐ **Add:** Add a new rule
- ☐ **Copy** : Duplicate the selected rule to a new rule
- ☐ **Delete** : Delete the selected rule
- ☐ **Batch delete:** Delete all selected rules in batch


Note

The static defense rules take effect from top to bottom.

Examples

Explanations of the rules listed in Figure 2-58 are as follows:

- ☐ **Rule 1:** Port 80 of the device is allowed to receive TCP data packets from the source IP address 192.168.120.54.
- ☐ **Rule 2:** Port 22 of the device is prohibited from receiving TCP data packets from the source IP address 192.168.120.54.
- ☐ **Rule 3:** Ports 5060 and 5061 of the device are prohibited from receiving data packets (of any protocol type) from the source IP address 192.168.120.54.

2.10.4 Packet Rate Limiting Based Dynamic Blacklisting

Packet rate limiting based dynamic blacklisting enables the device to defend against DoS/DDoS attacks which involve multiple computers all over the world and amounts of traffic.

You can set multiple defense rules. When the rate at which the data packets received by the device exceeds the threshold preset in the rules, the received data packets are discarded, and moreover the IP address of the attack source is added to the blocked list. Data packets from this address will no longer be received.

Rule configuration

After login, go to **Security > Dynamic defense** to configure.

Figure 2-59 Dynamic Defense Configuration Interface

Table 2-38 Dynamic Defense (Rule Configuration) Parameters

Name	Description
Local port	Specifies the local port range of the device for receiving data packets. The supported port range is 0 to 65535.
Protocol	Specifies the protocol type. The value can be set to TCP , UDP , or any .
Packets per second	Specifies the maximum data packet rate allowed for a local port. If the data packet receiving rate exceeds this value, the IP address of the attack source is added to the blocked IP addresses.

You may do the following operations:

- ☐ **Add:** Add a new rule
- ☐ **Copy** : Duplicate the selected rule to a new rule
- ☐ **Delete** : Delete the selected rule
- ☐ **Batch delete:** Batch Delete all selected rules

Blocked IP addresses

The blocked IP addresses of dynamic defense will be deleted after the device reboots.

Figure 2-60 Dynamic Defense (Blocked IP Addresses) Interface

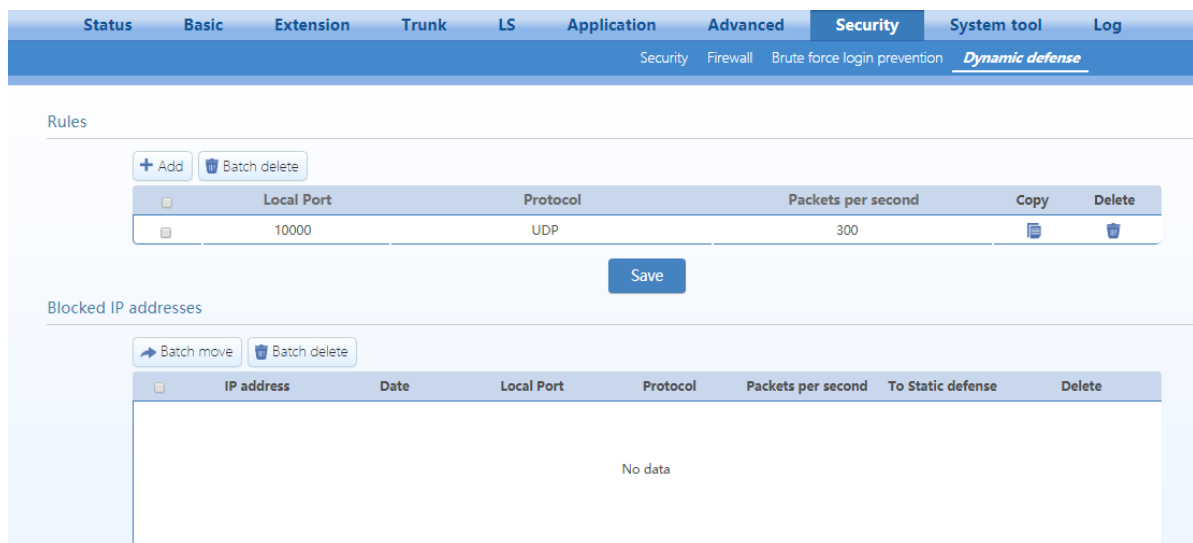


Table 2-39 Dynamic Defense (Blocked IP Addresses) Information

Name	Description
IP address	The IP address of the attacker detected by the device.
Date	The time when the device detects the attacker and initiates defense.
Local port	The port through which the data packet from the attacker is received.
Protocol	The protocol type.
Packets per second	The data packet receiving rate threshold.

You can perform the following operations:

- ☐ **Block:** Add the entry to the static defense list and block the matched packets.
- ☐ **Accept:** Add the entry to the static defense list and accept the matched packets.
- ☐ **Cancel:** Cancel to add the entry to the static defense list.
- ☐ **Batch move:** Move the selected entries in batch to the static defense rules, and provides three subsequent choices:

Table 2-40 Subsequent choices for moving the Blocked IP Addresses to static defense

Handling Method	Description	Applicable Scenario
Block	Add the entry to the static defense list and block the matched packets.	These entries are confirmed to be an attack sources.
Accept	Add the entry to the static defense list and accept the matched packets.	These entries are confirmed to be valid sources (applicable to heavy traffic scenarios such as call centers).
Cancel	Cancel to add the entry to the static defense list.	/

For details about static defense, see 2.10.3 ACL-based Traffic Filtering.

- ☐ **Batch delete:** Delete selected entries in a batch.

Example

Explanations of the rules listed in Figure 2-59 are as follows:

- ☐ **Rule 1:** Port 5060 is allowed to receive at most 20 UDP packets per second.
- ☐ **Rule 2:** Port 5060 is allowed to receive at most 50 TCP packets per second.

2.10.5 Change Password

Go to **System tools > Change password**, change administrator password or operator password, and set a login timer. Only an administrator is allowed to change passwords.

Figure 2-61 Password interface

The screenshot displays the 'System tool' menu with 'Change password' selected. The interface is divided into three main sections:

- Change administrator password:** Includes fields for 'Old password', 'New password', and 'Confirm new password', each with a toggle for visibility. A 'Save' button is located below these fields.
- Change operator password:** Includes fields for 'New password' and 'Confirm new password', each with a toggle for visibility. A 'Save' button is located below these fields.
- Login timeout value:** Includes a 'Timeout' field with the value '600' and a range indicator 's(Range: 60 - 7200)'. A 'Save' button is located below the field.

2.10.6 SSH

By default, SSH is disabled on the device. Generally, it is recommended that the Telnet/SSH be disabled. To enable SSH, go to **Security > Security**.

Figure 2-62 SSH configuration interface

Table 2-41 Access list parameters

Name	Description
Enable SSH	If this parameter is selected, terminals are allowed to access the device through SSH. It is not selected by default. It is recommended to disable SSH access after a successful connection is finished.
Access level	Either root or operator. When accessing the device with root , you should login with user operator first (password is Operator@021 by default), and use su root command to switch to user root (password is voipgateway by default).
Change Telnet/SSH password	Set password of user root or operator . Password must meet the following requirements: ☐ 6 to 20 characters ☐ At least the two of following: English letters, numbers, and symbols ☐ Excluding &, =, and “

2.10.7 Ping Blocking

If **Block** is chosen, the device will not respond to any Ping requests, which helps prevent malicious attacks.

Go to **Security > Security** to block or unblock the Ping requests.

Figure 2-63 Ping blocking/unblocking interface

2.10.8 Web Management

The device supports access to the Web GUI by using HTTP or HTTPS.

Go to **Security > Security**, and configure an HTTPS or HTTP port. The settings take effect after the

LS20 is restarted.

Figure 2-64 Web management interface

The screenshot shows the 'Web management' section of the LS20 web interface. At the top, there are tabs for 'Status', 'Basic', 'Extension', 'Trunk', 'LS', 'Application', 'Advanced', 'Security', 'System tool', and 'Log'. The 'Security' tab is selected, and within it, the 'Security' sub-tab is active. The 'Inbound Ping request' section has 'Unblock' selected. Below this, the 'Web management' section is expanded, showing 'HTTPS port' set to 443 and 'HTTP port' set to 80. A 'Save' button is located at the bottom of this section.

Table 2-42 Web management parameters

Item	Description
HTTPS port	Set the port used to access the device with HTTPS. The value range is 1 to 9999, and the default value is 443.
HTTP port	Set the port used to access the device with HTTP. The value range is 1 to 9999, and the default value is 80.

2.10.9 Voice Security

Go to **Security > Security**, and configure voice security related functions.

Figure 2-65 Voice security interface

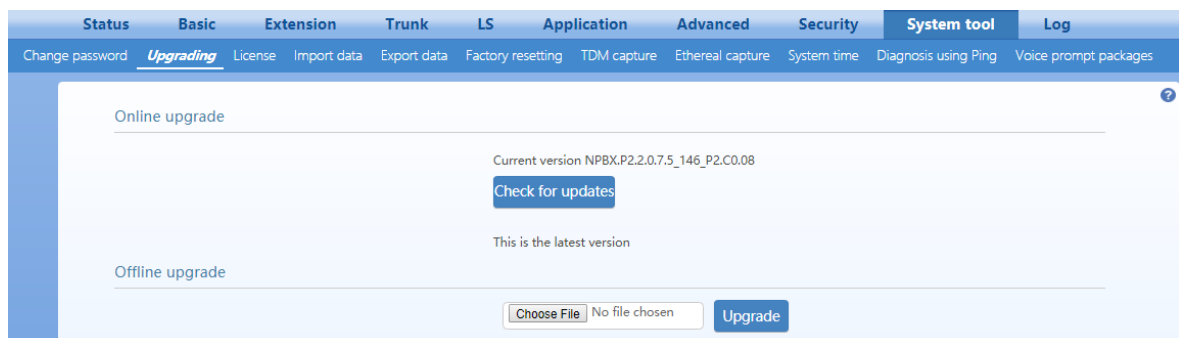
The screenshot shows the 'Voice security' section of the LS20 web interface. At the top, there are tabs for 'Status', 'Basic', 'Extension', 'Trunk', 'LS', 'Application', 'Advanced', 'Security', 'System tool', and 'Log'. The 'Security' tab is selected, and within it, the 'Security' sub-tab is active. The 'Inbound Ping request' section has 'Unblock' selected. Below this, the 'Voice security' section is expanded, showing 'Level' set to 'Middle'. A 'Save' button is located at the bottom of this section.

Table 2-43 Voice security parameters

Item	Description
Level	The security levels are described as follows: ▫ High security level: For an IP extension in an internal network, if the SIP signaling port is greater than 10000 and if the registration password and number are the same, registration is not allowed. For an IP extension in an external network, if the registration password and number are the same, registration is not allowed. A terminal in an external network is not allowed to access the Web GUI. ▫ Medium security level: Similar to the above restrictions, except that a terminal in an external network is allowed to access the Web GUI. ▫ Low security level: The preceding restrictions are not imposed.
Prohibit the outgoing dialing by IP extensions on public network	An IP extension in an external network is only allowed to call extensions.
User-Agent header fields	Input the User-Agent header field of the clients that are allowed to register with the device. If there are multiples of client fields, each of them must be separated by ",". If this parameter is set when registering with the device, the IP extension must carry the same User-Agent header field, otherwise registration fails.
Limit the number of authentication failures	When the number of authentication failures of the IP extension exceeds the specified threshold, the device will reject the registration request by the IP extension. The IP extension is allowed to register with the device only after the IP address of the extension is changed or the LS20 is restarted.

2.11 Maintenance

2.11.1 Upgrading



Online upgrading

Step 1 Go to **System tool > Upgrading**.

Step 2 Click **Check for updates**.

Step 3 If there is a newer version, click **Upgrade**. If there is no newer version, the system will display:
This is the latest version.

Offline upgrading

An upgrading will not clear configurations, but you are recommended to export the current configuration

on **System tool** > **Export data** page for backup.

Step 1 Go to **System tool** > **Upgrading**.

Step 2 Choose the intermediate version whose name is “*version-number.advanced_spe.tar.gz*”.

Note: if it prompts you to select the upgrade package whose file extension is **.img.tar.gz**, it means the intermediate version is already the latest version and you do not need to upgrade it. Then you should perform step 4 directly.

Step 3 Click **Upgrade** to upgrade the intermediate version.

Step 4 Upload the target version upgrade package

After completing the upgrade of intermediate version, you are directed to a page for uploading the target version (If the page displays incorrectly, input the device IP address in the address bar of the browser and refresh the page). Just Click **Choose File** to select the target upgrade package, and click **Next** to upload the package.

Step 5 Click **Next** to upgrade the target version.



Note

- The online upgrading takes about 15 minutes and the offline upgrading takes a few minutes. It is not advisable to upgrade software when network traffic is heavy.
- During the upgrade, do not power off, restart the device, or disconnect the device from the Internet, otherwise the system will be corrupted, and the device cannot be started. When the upgrade succeeds, the device will restart automatically.

2.11.2 Configuration Maintenance

Go to **System tool** > **Import data/ Export data/Factory resetting** to import/export configuration files for the device or restore the device to factory settings.

Figure 2-66 Data importing interface

Figure 2-67 Data exporting interface

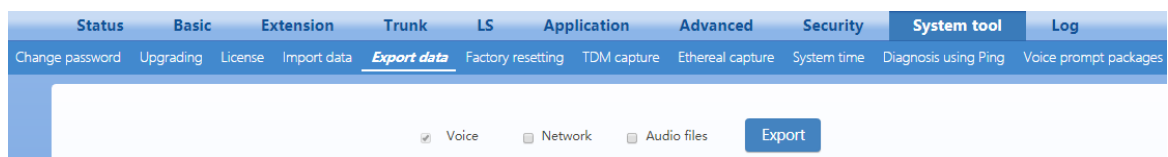


Figure 2-68 Restore factory settings interface



Note

- Don't operate the device during this period. When the configuration is imported successfully, the device will restart automatically.
- The speed at which configuration files are imported or exported is affected by the network. Please be patient.

2.11.3 Rebooting

To restart the device on the Web interface, click **Reboot** in the top right corner of the page.

Figure 2-69 Rebooting interface

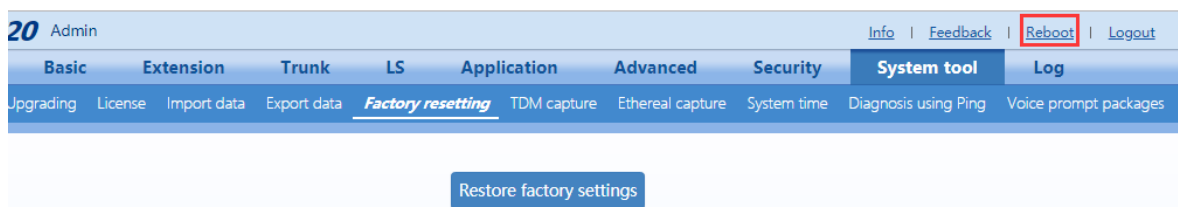


Table 2-44 System-reboot interface

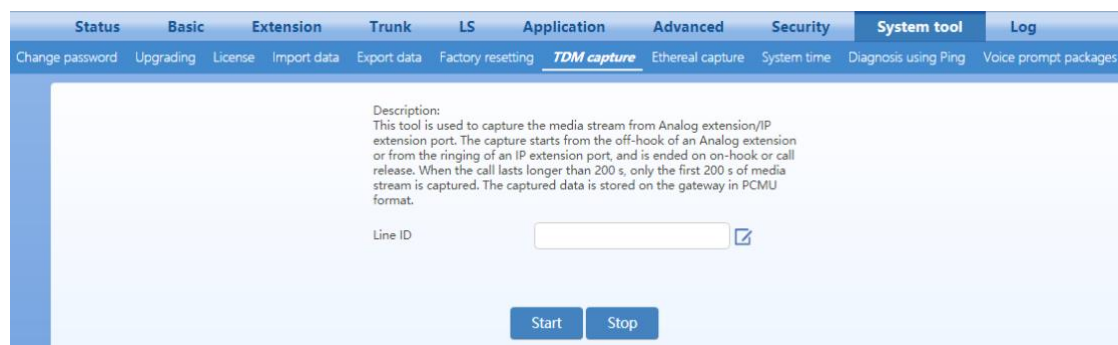
Item	Description
Reboot	Reboot system (both hardware and software).

2.11.4 Port Capture

This feature is used for troubleshooting media-related issues, such as CID detection failure or busy tone detection failure. Port capture records the media stream from the analog line. The capturing starts from the off-hook of a phone interface or from the ringing of a line interface, and it is ended upon on-hook. Only the first 200 seconds of a media stream is captured and data captured afterwards will be discarded. The captured data will be saved on LS20 as PCMU format file.

Step 1 Go to **System tool > TDM capture**, select the desired port, and then click **OK**.

To ensure the capture of an entire call, it must be completed in 200 seconds.

Figure 2-70 Port-capture interface

Step 2 Click **Start** to initiate the capture procedure.

Step 3 Make the test call (Outbound call for FXS port, inbound call for FXO port).

Step 4 Click **Stop** to finish the capture procedure. A download-request window will pop up to allow you to download the captured data to your PC.

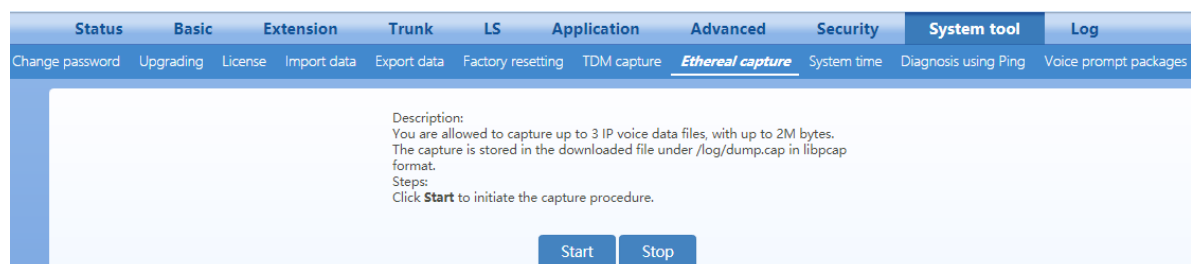
Send the captured file or related issue description to gs@newrocktech.com. Our technicians will help you to analyze and solve the issue.

2.11.5 Ethereal Capture

This feature is used for troubleshooting IP-packet-related issues, such as one-way voice, noise or echo.

Up to three files each with max. 2MB in size can be captured. Files will be saved as dump.cap in LS20 and click STOP to finish the capturing and download these files. The file will not be stored in LS20 after downloading.

Step 1 Go to **System>Ethereal capture**, and click Start.

Figure 2-71 Ethereal interface

Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Stop** to finish the capture procedure. A download request window will pop up to allow you to download the captured packets to your PC.

Step 4 If you need help with problem analysis, you can send the captured file to gs@newrocktech.com. You can open the file by using Wireshark.

2.11.6 Log Management

Log files contain the status change information of the device, which are helpful for troubleshooting and understanding the network conditions.

Log files are stored in RAM by default, and can be backed up to the internal storage device (by default, there is 3GB space for backup log file, the log storage space can also be changed on the **Application>Storage** page).

RAM only stores the latest log files which will be cleared after a reboot. While the backup log files in the internal storage device will not be affected by a reboot.

In addition, you can download the log files stored in RAM. Do as follows:

Step 1 Go to **Log > Log download**, select a log level, and click **Save**.

Step 2 Make the problem recur, for example, establish a call.

Step 3 Click **Download**. When the device instructs you to download the log file and select a path, create or choose a folder to save the log file.

Step 4 If you need help with problem analysis, you can send the captured file to gs@newrocktech.com.

If you want to collect all logs, select a log level and configure the log server. For details of log level and log server, see Table 2-45 Log-management parameters.

Table 2-45 Log-management parameters

Item	Description
Log level	By default, the log level is 4. Select a log level as required. Note: Whenever the device restarts, the default log level is restored.
System log server	- Enter the IP address or domain name of the log server (Syslog). If a port number is required, separate it from the IP address by using ":". For example: 192.168.1.100:518. - After this parameter is set, log files of the system will be sent to the log server instead of the local device.
Call Message server	- It is used for interworking with the Syslog server. Enter the IP address or domain name of the Syslog server. If a port number is required, separate it from the IP address with a ":". For example: 192.168.1.100:518. - After this parameter is set, call messages for the system will be sent to the log server instead of the local device.
Local port for sending logs	Local port for sending log files. It is used for interworking with the Syslog server. The default value is 514. Generally, this value does not need to be changed.

Item	Description
Back up logs to internal storage	Enable it, the log files in RAM will be backed up to the internal storage device automatically. The log files in the internal storage will not be cleared after a reboot. By default, it is not enabled.

2.11.7 Runtime log

The runtime log provides device's runtime status and events.

Go to **Log > Running log**, and then click **Refresh** to view the currently running information of the system.

Figure 2-72 Running log interface

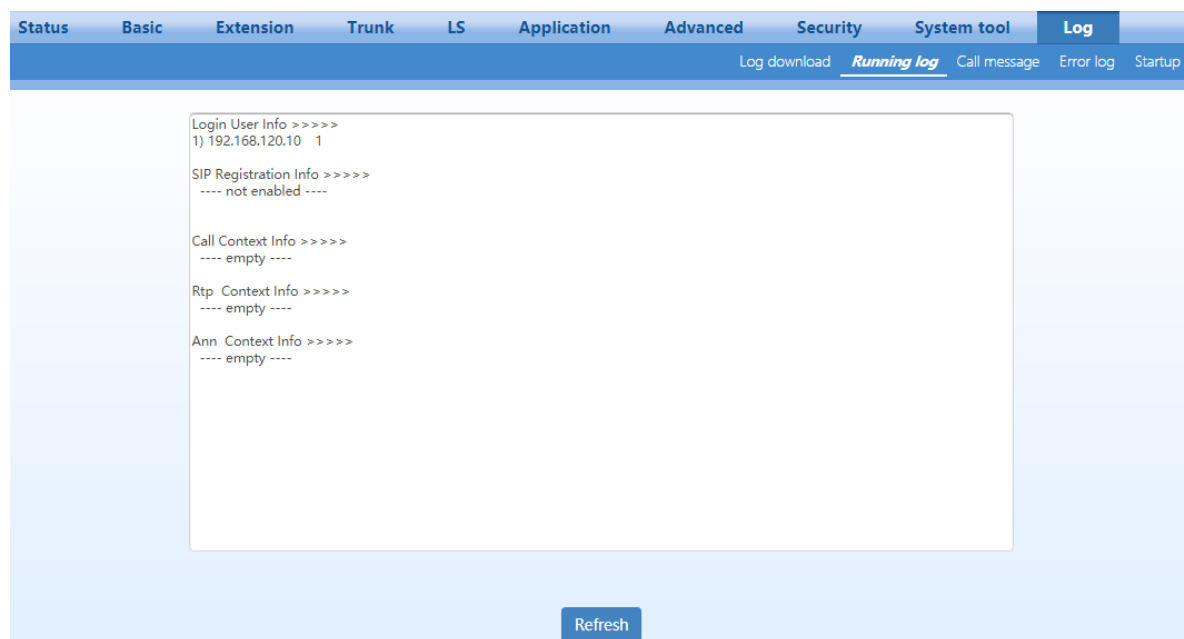


Table 2-46 Runtime log parameters

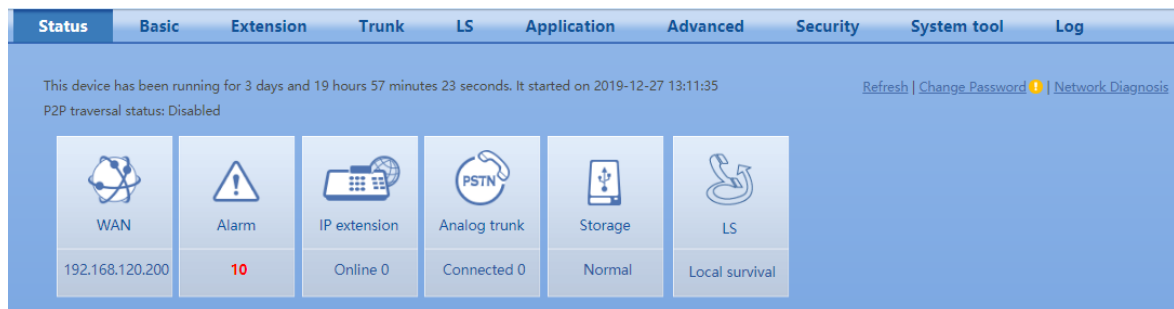
Item	Description
Login User Info	Displays the IP address that currently accesses the Web GUI and its operation privilege: 1: administrator 2: operator 3: Read only
SIP Registration Info	Displays registration information of the device. Not enabled: The registration server's address is not entered yet. Latest response: The latest response message for the registration. 200 means registered successfully. No response: No response from the registration server. The IP network fails, or the registration server is unreachable.
Call Context Info	Shows the call status.
RTP Context Info	Shows the voice channel related to the calls.
Ann Context Info	Displays IVR file resources.

2.12 View Runtime Information

2.12.1 Running Status

Open the **Status** interface. Device information such as network parameters, alarms, extension and trunk statuses, storage usage, tie trunk (for multi-site application), and the dynamic domain name is displayed.

Figure 2-73 Running status interface



2.12.2 Alarm

After opening the **Status** interface, move the mouse pointer to the **Alarm** icon to view alarm messages of the device.

In terms of severity level, the alarm messages are classified respectively into security alerts, orange alarms, and red alarms.

Figure 2-74 Alarm interface

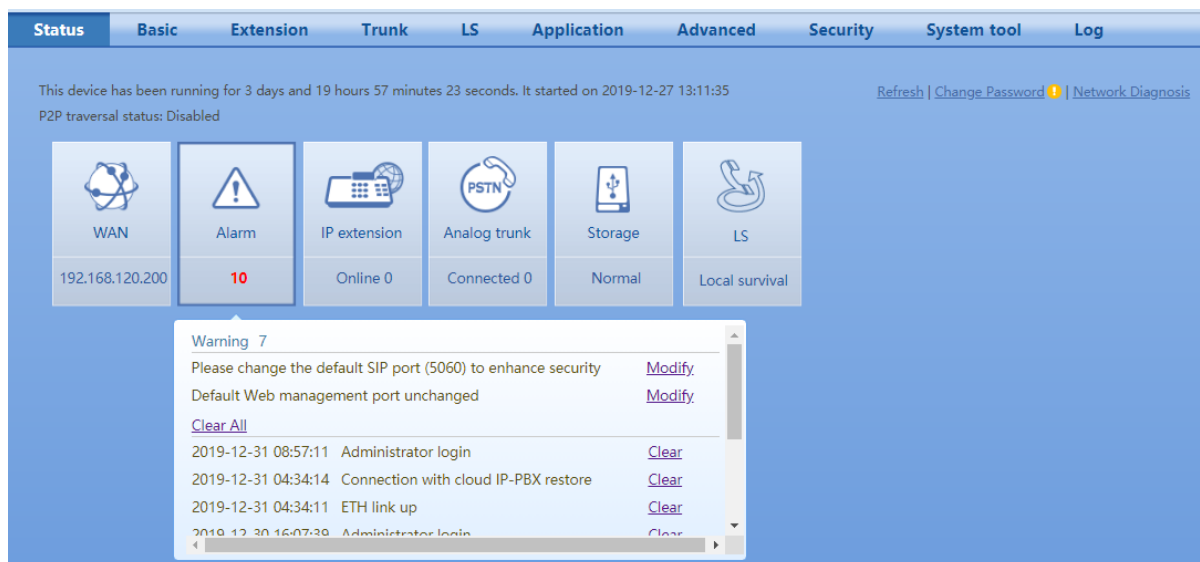


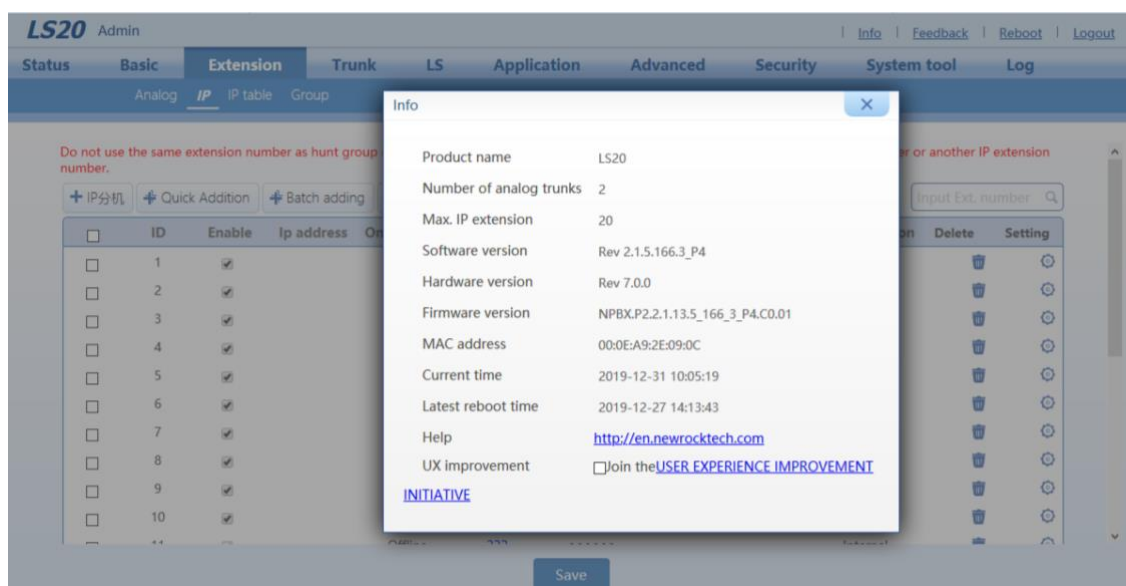
Table 2-47 Classification of alarm messages

Type	Description
Security alerts	Registration of IP trunk succeeded.
	Please modify the local SIP port.
	The WAN is connected.
	The operator has logged on.
	The administrator has logged on.
	The IP address has changed.
	The FXO port is connected.
	The FXO port is not connected.
	Connection with cloud PBX restore
Orange alarms	The administrator password was changed.
	A logon password was incorrect.
	The operator password was changed.
Red alarms	The device restarts.
	Software reboot
	Disconnected with cloud PBX
	An IP extension registration failed.
	A DNS resolution failed.
	The network port connection is malfunctioning.
	SIP attack has or is occurring.

2.12.3 Product Information

Click **Info** in the right upper part to view information such as device model, version, number of extensions, and MAC address.

Figure 2-75 Product information interface

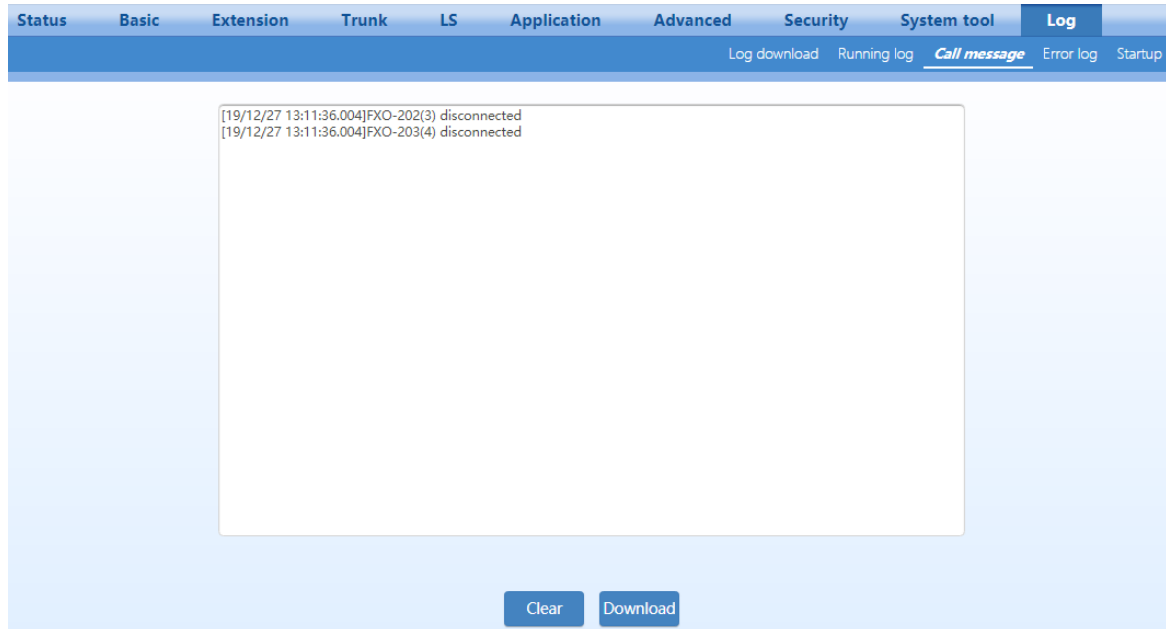


2.12.4 Call Messages

You can use call messages to locate a call problem.

Step 1 Go to **Log > Call message**, and click **Clear** to delete the current call messages.

Figure 2-76 Call message interface



Step 2 Make the problem recur. For example: establish a call.

Step 3 Click **Download** to save the call message file.

Step 4 Send the captured file to gs@newrocktech.com to get help with problem analysis.

3 FAQs

3.1 Incoming Call Number is Not Displayed

Symptom: For an incoming call from the analog trunk (FXO), the Line port number instead of the calling number is displayed on the phone.

Solution:

1. Check the line

Connect the phone to the telephone line directly to check whether the Calling Number Identification Presentation (CLIP) function is enabled on the line by the provider. If the phone does not show the correct calling number, contact the provider. If the correct calling number is displayed, check whether the calling number is displayed before the first ring or displayed after one or two rings.

2. Check the device configuration

Go to the **System > Analog trunk** page to check whether the CLIP function is enabled and whether the value of Call ID detection mode (before ringing or after ringing) matches the line.

3.2 IP Trunk Registration Fails

Symptom: When an outbound call is made with the IP trunk, there is a dial tone, but the call cannot be connected.

Solution:

Go to the **Logs > System Status** page to check the IP trunk registration status. See the table below for details.

Table 3-1 Solutions to IP trunk registration failures

Displayed Content	Registration Status	Solution
SIP Registration Info >>>>> Contact:<sip:61208000@192.168.250.5:5060> response: 200	Registration is successful.	Check the network configuration and wiring, and analyze call SIP signaling.
SIP Registration Info >>>>> Contact: <sip:61208000@192.168.250.5:5060> No Response	There is no response to the registration request.	Contact the VoIP service provider to confirm whether the address of the IP trunk registration server is correct, and test whether the network communications from the device to the registration platform are normal.
SIP Registration Info >>>>> Contact: <sip:61202000@192.168.250.5:5060> response: 404	IP trunk registration number is incorrect.	Contact the VoIP service provider to confirm whether the IP trunk registration number is correct.
SIP Registration Info >>>>> Contact: <sip:61208000@192.168.250.5:5060> response: 403	Registration password is incorrect.	Contact the VoIP service provider to confirm whether the IP trunk registration password is correct.

3.3 IP Network Connection Fails

Symptom: Unable to log on to the web administrator's interface.

Solution:

1. Connect your phone to the FXS port on the device, pick up the phone, and press ## to listen and check whether the network parameters of the device are correct.
2. Check the LAN where the device is located.

3. Check the connection between the LAN and the device.

3.4 Analog Extension Does Not Ring

Symptom: The analog extension does not ring for an incoming call.

Solution:

1. Replace the phone to determine whether the ringing function of the original phone is normal.
2. Go to **Extension > Analog > Advanced**, change Caller ID transmission mode, and dial the extension until the caller ID display modes supported by the device and the phone are the same and the ringing function becomes normal.
3. Go to **Extension > Analog > Advanced**, and change the ring frequency to different values to test whether the extension rings. Recommended test values include 15, 20, 30, 40, and 50.

3.5 Incorrect Date is Displayed on the Phone

Symptom: The date and time displayed with the calling number on the phone is inconsistent with those on the device.

Solution:

1. Check whether time information can be obtained from a time server on the Internet.
2. If the device cannot access the time server on the Internet, select a PC in the LAN to serve as the time server. If the operating system is Windows Vista, Windows 7, or Windows server 2008, manually start the Windows time service.
3. Check whether the firewall of the Windows operating system is enabled on the PC. If the firewall is enabled, perform the following steps to enable the port through which the device accesses the time server on the firewall.
 - a) Open the firewall window, and choose **Exceptions > Add Port**.
 - b) Add port 1 Name the port ntp-tcp, specify the port number as 123, and select the TCP mode.
 - c) Add port 2 Name the port ntp-udp, specify the port number as 123, and select the UDP mode.
 - d) Go to the **Control Panel > Administrative Tools > Services page**, and confirm that the Windows time service has been enabled.
4. Call extension B from any extension A. Extension B shows the same time information as that on the device.

3.6 Low Volume on an Extension

Symptom: The other party's voice is too low on a call.

Solution:

Table 3-2 Solutions to low voice volume on an extension

Extension Type	Solution
Volume is too low on an analog extension	Go to Extension > Analog > Advanced , and increase the value of Gain to terminal .
Volume is too low on an IP extension called by an analog extension	Go to Extension > Analog > Advanced , and increase the value of Gain to IP .

3.7 Crosstalk on an Analog Extension

Symptom: Conversation on another extension is heard during a call.

Solution:

Generally, crosstalk is caused by telephone line short-circuits. Check the connection line of the FXS port and remove the line fault.

3.8 Can I Press the R Key on an Analog Extension?

Pressing the R key after off-hook is equivalent to hook-flash. However, because R keys on different phones may follow different design specifications, pressing the R key on an extension is not always reliable. It is recommended that you press ** for functions such as three-way calling, call transfer, and call parking.

3.9 What if I Cannot Log On to the Device Because I Forgot the Preset Whitelist IP Address?

The LS20 provides the embedded white-listed address of 192.168.2.100 upon factory delivery. When the Whitelist function is enabled, if you forget the whitelisted IP address previously set, the following steps can be performed for recovery.

- Step 1** Connect a PC directly to the LS20 through a network cable.
- Step 2** Press *90 to set the IP address of the LS20 to one that is located in the same network segment as the embedded white-listed address, such as 192.168.2.101. To do so, continuously dial *90192*168*2*101#255*255*255*0#192*168*2*1#0# after off-hook, and then hook on after hearing the successful service registration announcement.
- Step 3** Restart the LS20.
- Step 4** Set the IP address of the PC to 192.168.2.100.
- Step 5** Enter the new IP address of the LS20 on the Internet Explorer or the Telnet client of the PC to access the LS20.

3.10 What to Do When the Analog Trunk is Abnormal

Symptom: The analog trunk is connected, but the incoming or outgoing call is abnormal. For example, incoming and outgoing calls cannot be made or are disconnected after ringing once.

Solution:

Check the analog trunk on the status page and check whether error information on cable exceptions is generated. If yes, the external line cannot provide sufficient voltage (the standard voltage is 48 V); lay out new lines or seek assistance from the carrier.

4 Making an OpenVPN Client Certification

When the device serves as the OpenVPN client, a certificate needs to be uploaded. To make a certificate, follow this procedure:

Step 1 Obtain the .ovpn file, or the “ca.crt”, “client.crt”, “client.key” and “ta.key files, and other information from the OpenVPN server.

Step 2 Create a text file client.ovpn.

Step 3 Client.ovpn contains following contents:

```
# Claim it is a OpenVPN client
client
# Could be tap or tun as required by the VPN server
dev tap
persist-tun
persist-key
# Encryption type as required by the VPN server
cipher AES-128-CBC
tls-client
tls-auth ta.key 1
# The address and the port of the VPN server
remote 192.168.143.235 1194
# Could be udp or tcp as required by the VPN server
proto udp
tls-remote yfadmin
comp-lzo
passtos
ns-cert-type server
<ca>
# Copy the content beginning with “-----BEGIN ...” and ending with “-----END ...” from ca.crt to
# replace the following content.
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
</ca>
<cert>
# Copy the content beginning with “-----BEGIN ...” and ending with “-----END ...” rom client.crt to
# replace the following content.
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

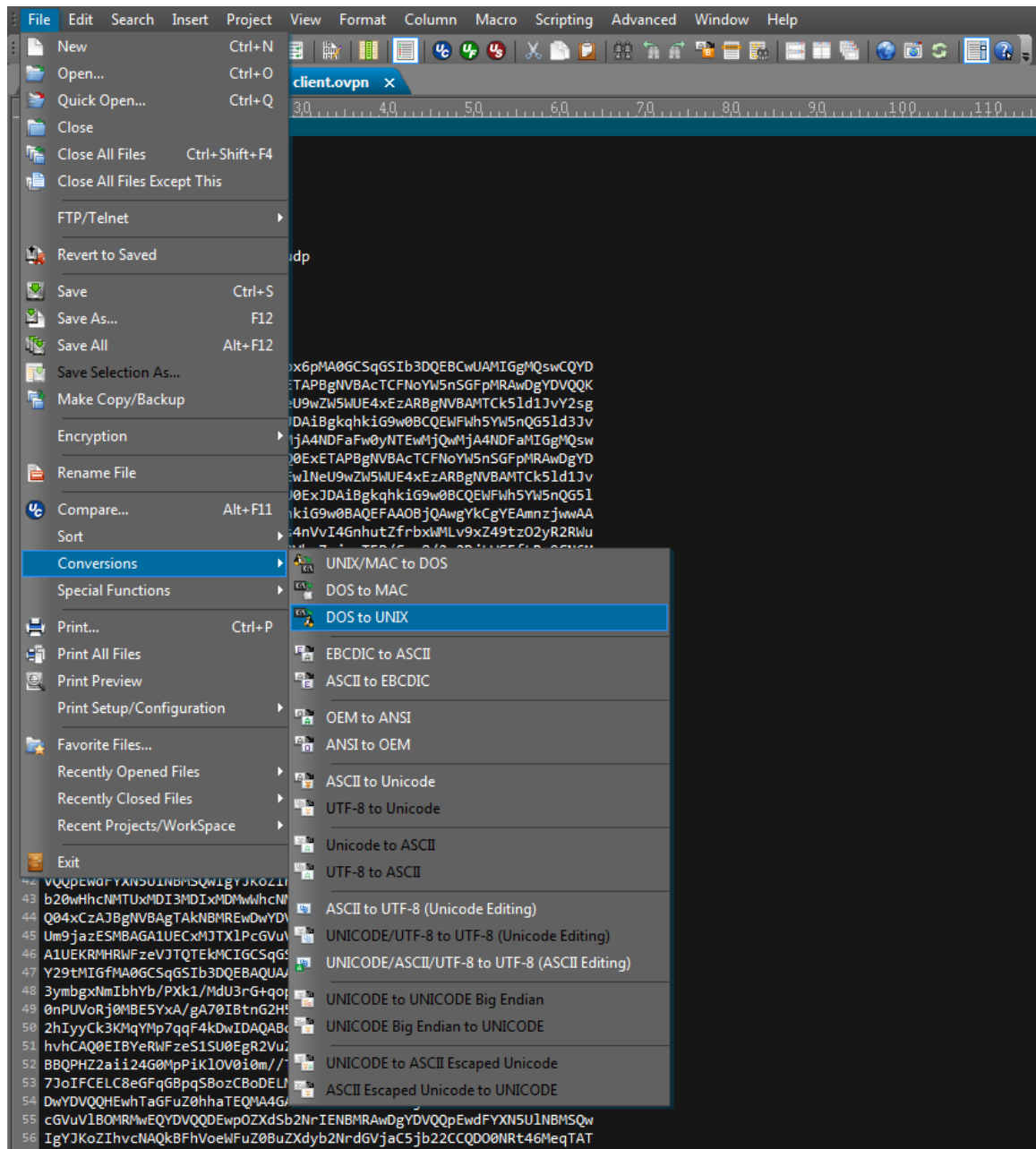
```
</cert>
<key>
# Copy the content beginning with "-----BEGIN ..." and ending with "-----END ..." from client.key to
# replace the following content.
-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----
</key>
<tls-auth>
# Copy the content beginning with "-----BEGIN ..." and ending with "-----END ..." from ta.key to
# replace the following content.
-----BEGIN OpenVPN Static key V1-----

-----END OpenVPN Static key V1-----
</tls-auth>
```

Step 4 Save the file as the name of client.ovpn.

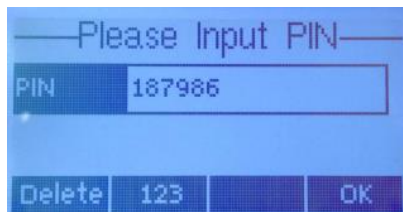
Step 5 Transform the format to UNIX. Take the Ultra Edit as an example to describe the transform procedure, shown as the figure below.
After transformation, save the file.



Appendix A: Registering a SIP Terminal to LS20

SIP Phone

- If a New Rock NRP phone is used, it can be registered with the device as follows: Connect the phone to the network where the device is located, and enter the corresponding PIN of the IP extension on the device.



- For a phone that is not a New Rock NRP phone, registration information must be entered. The following describes the registration information using the NRP1000 as an example.

Step 1 Open the Web management interface of the IP phone, click **VOIP > SIP**, select the desired SIP line, and then enter the registration information in **Basic setting**.

Figure 4-1 SIP Phone registration interface

Table 4-1 SIP Phone registration parameters

Item	Description
Server Address	Enter the IP address or dynamic domain name of the LS20.
Server port	Enter the SIP listening port of the LS20. The default port is 5060. Note: By default, the SIP listening port of the device and the SIP trunk share a port, that is, port 5060. You can set a different registration port on the

Item	Description
	Extension > IP> Registrar OPTIONS.
Authentication User	Enter the number of the IP extension that is set in the LS20. For example: 208.
Authentication Password	Enter the password corresponding to the number of the extension. For example: the password corresponding to the number 208 is 187986.
SIP user	Enter the number of the IP extension that is set on the LS20. For example: 208.
Display name	The name to be displayed on the other party's phone. The name of the extension user can be set. If it is not set, the Authentication User will be displayed on the other party's phone. For example: 208.

Step 2 Select **Enable registration**, and click **Apply**.

Step 3 On the web interface of the LS20, go to **Extension > IP** to view the registration status of the IP extension.



Note

For an IP phone, it is recommended that G.729 codec standard be selected, and that the DTMF processing mode be the same as that on the device.

Softphone

- If the New Rock WeWei softphone is used, it can be registered with the device as follows:

Use your smartphone to scan the QR code to download the WeWei installation package.



After installing is completed, open the WeWei and input username, password and domain, then click Register. Username is the IP extension number and password is the one for IP extension, both number and password can be modified on **Extension > IP** page of LS20 Web GUI.

中国移动 16:43 56%

209

10.126.10.140:5070

Register

Skip>>

- If another softphone is used, registration information must be entered. The following describes the specific registration information using the X-Lite as an example.

Step 1 Register X-Lite: Enter the SIP configuration page. Click the button "Add" which pops up the interface for Properties of Account.

Figure 4-2 X-Lite login interface

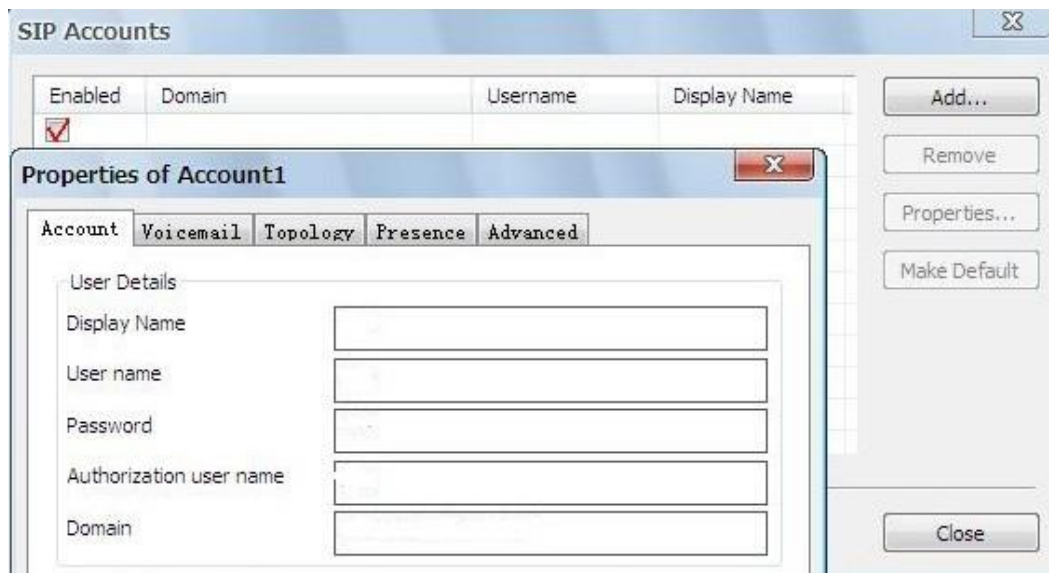
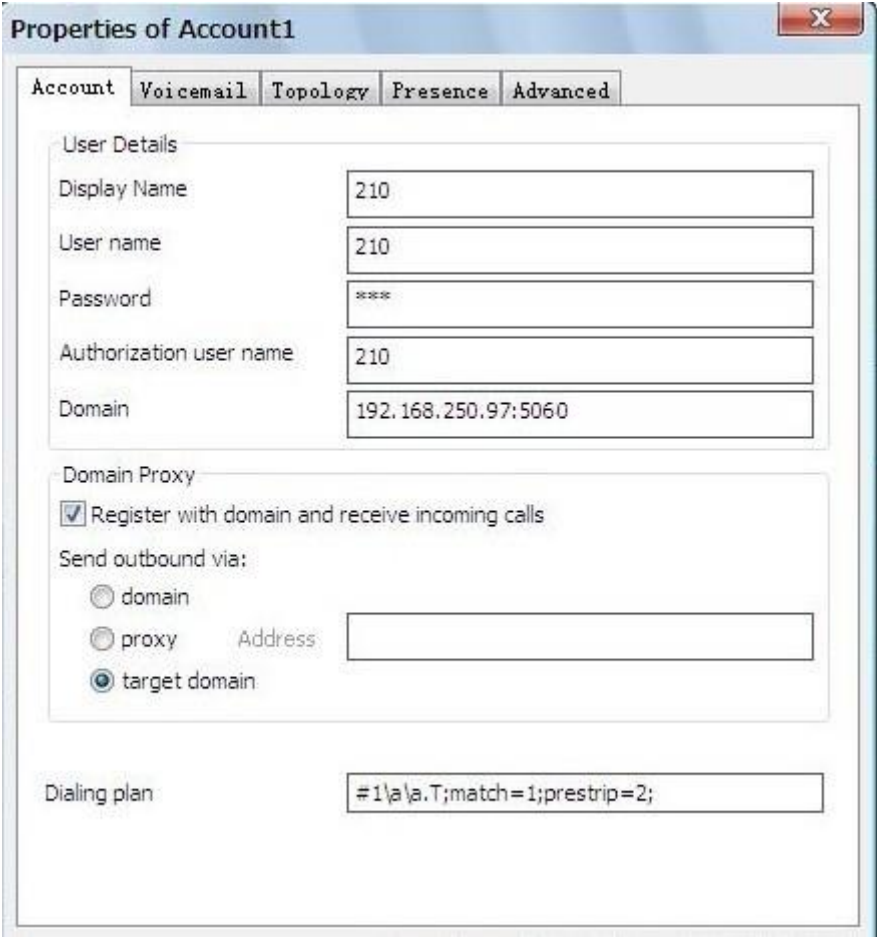


Figure 4-3 X-Lite registration interface



Properties of Account1

Account Voicemail Topology Presence Advanced

User Details

Display Name: 210

User name: 210

Password: [masked]

Authorization user name: 210

Domain: 192.168.250.97:5060

Domain Proxy

☒ Register with domain and receive incoming calls

Send outbound via:

☐ domain

☐ proxy Address: [empty]

☒ target domain

Dialing plan: #1\|a\|a.T;match=1;prestrip=2;

Table 4-2 SIP Phone registration parameters

Item	Description
Display name	The name to be displayed on the other party's phone. The name of the extension user can be set. If it is not set, the User Name will be displayed on the other party's phone. For example: 208.
User name	Enter the number of the IP extension that is set on the LS20. For example: 208.
Password	Enter the password corresponding to the number of the extension. For example: the password corresponding to the number 208 is 187986.
Authorization user name	Enter the number of the IP extension that is set on the LS20. For example: 208.
Domain	Enter the IP address or dynamic domain name of the LS20. When the extension needs to register with the LS20 from an external network, the external access address of the device needs to be entered. Go to Basic > Remote access to view the IP address of the device.

Appendix B:

Each RJ45 socket has 8 pins leading out to 4 pairs of analog telephone lines/trunk lines in agreement with the pair specifications for Ethernet interfaces. The correspondence is listed in the table below. The correspondence between RJ45 and RJ11 is listed in Table 4-3. Standard RJ11 telephone lines can also be plugged in RJ45 sockets. In this case, the telephone/trunk lines are connected to the 3rd pair of pins for simple call tests.

Table 4-3 Pin specifications for the RJ45 socket port

RJ45 Pin Number	1	2	3	4	5	6	7	8
Analog line pair	1 st Pair		2 nd Pair	3 rd Pair		2 nd Pair	4 th Pair	
	TIP1	RING1	TIP2	TIP3	RING3	RING2	TIP4	RING4
Reference color	White Orange	Orange	White Green	Blue	White Blue	Green	White Brown	Brown

Figure 4-4 Schematic diagram of the subscriber line connection

