iMX100-AG User Manual

Release 2.2.1

New Rock
TECHNOLOGIES

Welcome

Welcome to the iMX100-AG VoIP Gateway User manual. This document covers features, functionalities, and installation procedures for the iMX100-AG series, and provides tested configuration examples for our gateway users. After reading this book, you will learn more about the gateway, get familiar with the installation process, and feel more comfortable in using the software to perform all administrative activities.

Version:

Document Version: 2.2.1
Applicable Software Version: 1.9.3.x Series.

Copyright:

TABLE OF CONTENTS

1

PRODUCT RODUCTION

Overview

iMX100-AG VoIP gateway (iMX100-AG for short) is a multiple purpose and modular VoIP equipment based on New Rock's next generation advanced MicroXchange architecture. iMX100-AG provides an ideal solution for voice and fax transmission over the IP networks.

iMX100-AG is designed for carriers and enterprises for regular phone service, fax service and PBX service. It can be used as a part of the cost effective IP PBX solutions. iMX100-AG supports many VoIP standard protocols and voice codec. It provides effective solutions to many technical challenges that include echo cancellation, firewall/NAT traversal, and billing call record collection. Compared to other products on the market, iMX100-AG has the advantage of carrier reliability, flexible configuration, high voice quality, excellent protocol compatibility, and low cost. Its high efficient hardware and software design and powerful DSP processing power guarantee the iMX100-AG capability of full load voice and signaling processing and IP packetization. Its redundant load sharing power supplies and hot swappable modules further secures the iMX100-AG's carrier reliability.

iMX100-AG provides FXS/FXO ports and multiple 10/100M Ethernet interfaces. iMX100-AG connects to regular telephones, faxes and PBXs through the FXS/FXO analog interfaces. It connects to IP network through Ethernet interfaces. iMX100-AG provides real-time and high quality IP-based voice services.

Features

iMX100-AG has the following unique features:

- **Flexible Configuration**

  iMX100-AG uses compact modular slot chassis design. Users can configure the iMX100-AG with interface cards of different types and capacities.

- **Carrier Reliability and Easy Maintenance**

  iMX100-AG hardware is designed to reach the high MBTF (Mean Time between Failure). To satisfy the carrier reliability requirement for voice gateways, iMX100-AG has the option of load sharing power module. Should one power module fail to function, the other power module resumes the full power function. Every hardware module in the iMX100-AG is hot swappable for in-service maintenance.

- **Support of FTP file Transfer and Telnet Remote Configuration**

- **Supported Protocols and Advanced Technologies**

  iMX100-AG supports MGCP、SIP、RTP、TFTP、HTTP、SNMP、DHCP、and STUN protocols. It also supports G.711、G.729A、G.723.1, iLBC, and GSM codec; G.165 and G.168 echo cancellation; RFC2833 DTMF relay; and T.38 and T.30 IP fax relay technologies.

- **Support of Variety of End-User Devices**

  iMX100-AG supports analog telephones, faxes, and PBX devices.

- **Interoperability**

  iMX100-AG has completed the interoperability tests with soft switches and gateways from more than ten telecommunication equipment manufacturers worldwide.

Hardware Feature

Physical

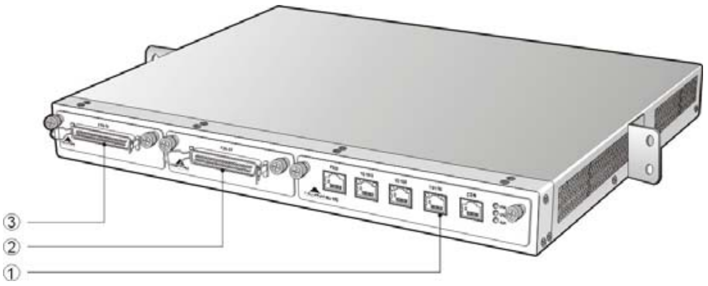


Figure 0-1 iMX100-AG Front View

①	One hot swappable main control module. The main module supports three 10/100M Ethernet ports for IP network and one console port (CON)
② & ③	Two hot swappable slots that can be configured with different interface cards

All the New Rock VOIP products offer modular, versatile, and high reliability features. iMX100-AG provides not only the pure FXS (S port) and pure FXO (O port) line interface module but also mixed FXS/FXO line interface module such as 4FXS/4FXO (4S/4) and 8FXS/8FXO (8S/8).

Both and slots can support 16S, 24S, 4FXO, 8FXO, 16FXO, 4S/4, and 8S/8 interface line module. Users can configure the iMX100-AG gateway with different configurations by selecting different line interface modules. The following table lists the most common configurations used by existing customers:

Table 0-1: iMX100 Interface Slot Configuration Options

Interface Type	Card Type	Slot②	Slot□	Life-line PSTN Fallback	DS0s
Analog	iMX100-AG 48S	FXS-24	FXS-24	No	48

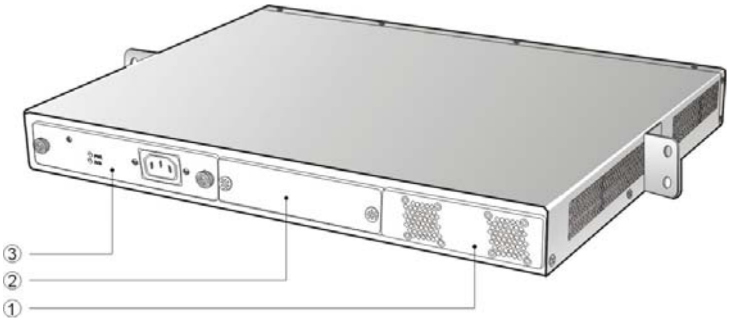


Figure 0-2 iMX100-AG Rear View

□	Two Fan Modules.
□ & □	Two hot swappable power supply modules for redundancy (optional).

Technical Specifications

Table 0-2: iMX100-AG Specification

	Specifications
Internal Memory	32MB/64MB/128MB (Standard 64MB)
Flash Memory	8MB/16MB (Standard 8MB)
Talk Battery	–24 voltage
Ringing Voltage	60V RMS
REN Equivalence	5 for short loop (300 meters), 3 for long loop (1500 meters)
Loop Current	>= 21 mA
Power Surge Protection	1000 Voltage (10/1000uS)
Max Line Length	1500 m
Off-hook Detection	Loop Start

	Specifications
Dialing	DTMF
Input Voltage	100～240 Volt
Input Current	0.7Amp (110 Volt) /0.35Amp (220 Volt)
Current Frequency	47～63 Hz
Power Consumption	75Watt (Max)
Operation Temperature	0～40°C
Non Operation Temperature	–25～70°C
Operation Humidity	5～95%(Non Condensed)
Noise	30 DB(Max)
Size (H×L×W)	4.4×44×44 cm
Net Weight	7 kg
Weight (including package)	9 kg

2

CONSOLE AND INTERFACE MODULES

iMX100-AG is designed based on modular architecture. The detailed functions of the interface modules are described in the following sections.

Main Console Module

iMX100-AG Main Console Module uses advanced framework and technology. Its main features include: high performance processors for management and signaling processing and DSP sub module for voice processing. The Main Console Module provides necessary interfaces to connect to peripheral devices and internal interface modules. It can supports up to 48 analog line/trunk ports.

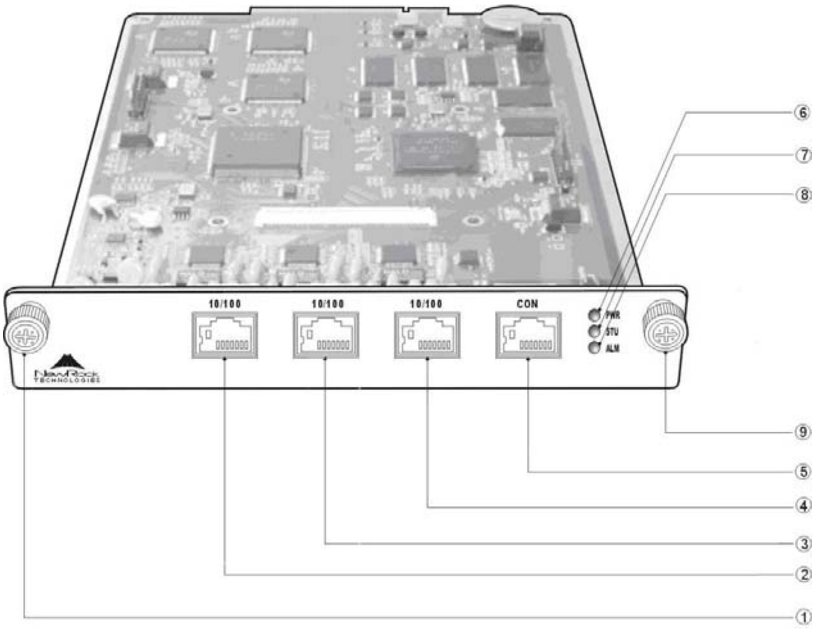


Figure 0-1 iMX100-AG Main Console Module Physical View

□ & □	Main Console Module Thumb Screw	□	Ethernet Port (0)
□	Ethernet Port (1)	□	Ethernet Port(2)
□	Console Port (CON)	□	Power LED
□	Alarm LED	□	Status LED

iMX100-AG modules are hot swappable for easy service and maintenance. For example: users can pull the main console module out for service by pulling the thumb screws on the module. The thumb screws are indicated by □ and □ on the Figure 2-1.

Note: The main console module can be secured by turning the screw clockwise. Turn screws the other way to pull the main console module out.

Ethernet Port

There are three 10/100M Ethernet ports on the iMX100-AG main console module. The connector type of the Ethernet ports is RJ45 with status LED. Table 2-2 shows the pin assignment of those Ethernet connectors and LED status specification.

Table 0-1: Ethernet Port Pin Assignment and Status LED Specification

Pin				LED	
1	2	3	6	Yellow	Green
TX+	TX-	RX+	RX-	Connected	Live

- Ethernet Port (1)： for console/management/maintenance use
- Ethernet Port (2)： reserved for future use.
- Ethernet Port (3)： Ethernet port to connect to the IP network. This port is used for all the VoIP activities that include SIP and MGCP signaling protocol and RTP packets transmission. This port can also be used for control/management/maintenance.

Note: If possible, customers should use the Ethernet port 1 for software upgrade, device configuration, and management operations and use the Ethernet port 3 for VoIP protocol and data transmissions.

Console Port

iMX100-AG supports configuration through a console port (CON) of RJ45 connector type. Table2-3 shows the connector interface scheme of RJ45 to DB9 and DB25.

Table 0-2: Console Port Pin Assignment of RJ45 to DB9 and DB25

RJ45 Connector Pin No.	1	2	3	4	5	6	7	8
Pin Description	NC	NC	TXD	GND	GND	RXD	NC	NC
DB9 Connector Pin No.			2		5	3		
DB25 Connector Pin No.			3		7	2		

The console port is used for local management and testing. Computers can be connected to iMX100-AG by linking the RS232 port to iMX100-AG console port. iMX100-AG uses three wires on the console port: one TXD (send), one RXD (receive), and one GND (ground).

iMX100-AG is shipped with a standard RJ45 to DB9 adapter.

Table 0-3: Console Port Specification

attribute	Description
Connector Type	RJ45
Port Number	1
Interface Type	RS232
Baud Rate	115200
Data Bits	8
Parity Check	No
Stop Bit	1
Flow Control	No

LED Definitions

There are three LED indicators on the front panel of the iMX100-AG main console module: power, alarm, and status.Table2-4 show the LED types and definitions.

Table 0-4 Main Console Module LED Definitions

mark	function	State	Description
PWR	Power Indicator	Green	Main power supply is on
		Off	Main power supply is off
STU	Status Indicator	Off	System is locked in a non functional state
		Flashing Green	Normal
		Red	System is in the start up mode, not ready for operation
		Flashing Red	System is in the diagnostic mode with limited operation capability
ALM	Alarm Indicator	Green	Clear of all alarms
		Flashing Red	New alarm condition from an unknown source
		Red	Alarm with identified source

FXS Line Interface Module

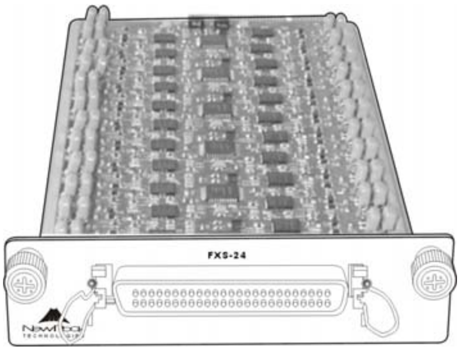


Figure 0-2 FXS Interface Module Physical View

FXS Line Interface Module Function

- iMX100-AG FXS interface module provides the interface to analog phones, faxes, modem, and PBX.
- It can be used with FXS/FXO mixed line interface module to meet the different configuration requirements. The common combinations are described in the table 1-1.

FXS Line Interface Module Pin Assignment

Each iMX100-AG FXS interface module provides up to 24 ports. Each iMX100-AG can have up to two FXS interface modules, 48 analog ports. FXS interface module provides 50 pin CHAMP connector. Table2-5 shows the scheme of the 50 pin CHAMP connector. iMX100-AG supports two configurations of the FXS interface module：16 port FXS module (16S) and 24 port FXS module (24S) .On the 16S interface module, the pins from 17 to 24 are not used.

Table 0-5: FXS Interface Module Pin Assignment

Pin	Description		Pin
1	RING1	TIP1	26
2	RING2	TIP2	27
3	RING3	TIP3	28
4	RING4	TIP4	29
5	RING5	TIP5	30
6	RING6	TIP6	31
7	RING7	TIP7	32
8	RING8	TIP8	33
9	RING9	TIP9	34
10	RING10	TIP10	35
11	RING11	TIP11	36
12	RING12	TIP12	37
13	RING13	TIP13	38
14	RING14	TIP14	39
15	RING15	TIP15	40
16	RING16	TIP16	41
17	RING17	TIP17	42
18	RING18	TIP18	43
19	RING19	TIP19	44
20	RING20	TIP20	45
21	RING21	TIP21	46
22	RING22	TIP22	47
23	RING23	TIP23	48
24	RING24	TIP24	49
25	NC	NC	50

FXO Line Interface Module

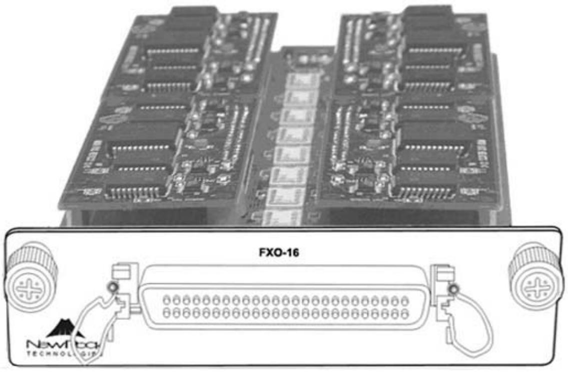


Figure 0-3 16 FXO Interface Module Physical View

FXO Line Interface Module Function

- iMX100-AG FXO interface module provides the analog relay ports. It can be connected to PBX analog POTS lines or telephony switch POTS lines.
- It can be used with FXS/FXO mixed line interface module to meet the different configuration requirements. The common combinations are described in the table 1-1.

FXO Line Interface Module Pin Assignment

Each iMX100-AG FXO interface module supports up to 16 analog relay ports. FXS interface module provides 50 pin CHAMP connector. Table2-6 shows the scheme of the 50 pin CHAMP connector. iMX100-AG supports three configurations of the FXS interface module：

- 4 port FXO module shown in table 2-6.
- 8 port FXO module shown in table 2-7
- 16 port FXO module shown in table 2-8

On the 4FXO module, the pins from 5 to 16 are not used. On the 8FXO module, the pins from 9 to 16 are not used.

Table 0-6: 4FXO Interface Module Pin Assignment

Pin	Description		Pin
1	RING1	TIP1	26
2	RING2	TIP2	27
3	RING3	TIP3	28
4	RING4	TIP4	29
5	NC	NC	30
6	NC	NC	31
7	NC	NC	32
8	NC	NC	33
9	NC	NC	34
10	NC	NC	35
11	NC	NC	36
12	NC	NC	37
13	NC	NC	38
14	NC	NC	39
15	NC	NC	40
16	NC	NC	41

Table 0-7: 8FXO Interface Module Pin Assignment

Pin	Description		Pin
1	RING1	TIP1	26
2	RING2	TIP2	27
3	RING3	TIP3	28
4	RING4	TIP4	29
5	RING5	TIP5	30
6	RING6	TIP6	31
7	RING7	TIP7	32
8	RING8	TIP8	33
9	NC	NC	34
10	NC	NC	35
11	NC	NC	36
12	NC	NC	37
13	NC	NC	38
14	NC	NC	39
15	NC	NC	40
16	NC	NC	41

Table 0-8: 16FXO Interface Module Pin Assignment

Pin	Description		Pin
1	RING1	TIP1	26
2	RING2	TIP2	27
3	RING3	TIP3	28
4	RING4	TIP4	29
5	RING5	TIP5	30
6	RING6	TIP6	31
7	RING7	TIP7	32
8	RING8	TIP8	33
9	RING9	TIP9	34
10	RING10	TIP10	35
11	RING11	TIP11	36
12	RING12	TIP12	37
13	RING13	TIP13	38
14	RING14	TIP14	39
15	RING15	TIP15	40
16	RING16	TIP16	41

FXS/FXO Mixed Line Interface Module

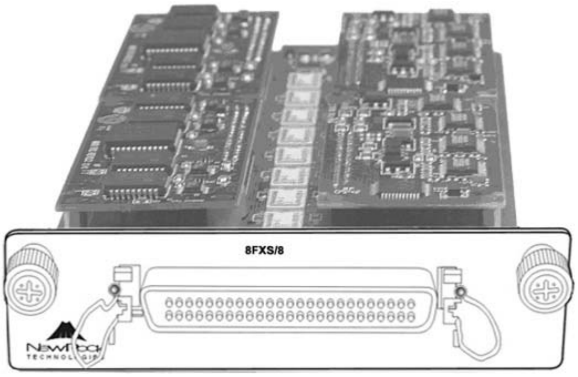


Figure 0-4 8S/8 Line Interface Module Physical View

The FXS/FXO mixed line module provides an ideal solution for enterprise and personal users to expand their existing PSTN or PBX telecommunication systems by connecting to IP network. It offers flexible configuration and routing capabilities to meet the different customer requirements.

The FXS/FXO mixed line module offers both the FXS and FXO interfaces on the same line card.

- It provides the analog interfaces to connect to telephones, faxes, modems, and PBX.

- It provides the analog relay ports. It can be connected to PBX analog POTS lines or telephony switch POTS lines.
- The FXO ports can be used for Life-line PSTN Fallback to increase the system stability and reliability.

The examples are given as follows based on the 4FXS/4FXO mixed line interface module.

- iMX100-AG with the 4S/4 has three interface types: IP, FXS, and FXO. The calls from any interface type can be routed to any of the two other interface types.
- iMX100-AG with the 4S/4 is equivalent to an IP-PBX. It offers the common PBX functions as well as the IP functions.
- iMX100-AG with the 4S/4 can be used as iMX100-AG with 4FXS or iMX100-AG with 4FXO.
- All the New Rock's VOIP gateways with the FXS/FXO line card provide the same functions and features. The gateways include iMX100_AG and MX8.
- Applicable scenarios include the connections of enterprise PBXs, the connections of PBX and VOIP, or used as IP-PBX.

Currently there are two configurations for the FXS/FXO mixed line card modules:

- 4S/4 shown in table 2-9
- 8S/8 shown in table 2-10.

The FXS/FXO mixed line card module can be used alone as used together with FXS line card module. The common combinations are listed in the table 1-1.

Table 0-9: 4FXS/FXO Interface Module Pin Assignment

Pin	Description		Pin
1	RING1 (FXO)	TIP1	26
2	RING2 (FXO)	TIP2	27
3	RING3 (FXO)	TIP3	28
4	RING4 (FXO)	TIP4	29
5	NC	NC	30
6	NC	NC	31
7	NC	NC	32
8	NC	NC	33
9	RING1 (FXS)	TIP1	34
10	RING2 (FXS)	TIP2	35
11	RING3 (FXS)	TIP3	36
12	RING4 (FXS)	TIP4	37
13	NC	NC	38
14	NC	NC	39
15	NC	NC	40
16	NC	NC	41

Table 0-10: 8FXS/FXO Interface Module Pin Assignment

Pin	Description		Pin
1	RING1 (FXO)	TIP1	26
2	RING2 (FXO)	TIP2	27
3	RING3 (FXO)	TIP3	28
4	RING4 (FXO)	TIP4	29
5	RING5 (FXO)	TIP5	30
6	RING6 (FXO)	TIP6	31
7	RING7 (FXO)	TIP7	32
8	RING8 (FXO)	TIP8	33
9	RING1 (FXS)	TIP1	34
10	RING2 (FXS)	TIP2	35
11	RING3 (FXS)	TIP3	36
12	RING4 (FXS)	TIP4	37
13	RING5 (FXS)	TIP5	38
14	RING6 (FXS)	TIP6	39
15	RING7 (FXS)	TIP7	40
16	RING8 (FXS)	TIP8	41

Switching Power Supply Module

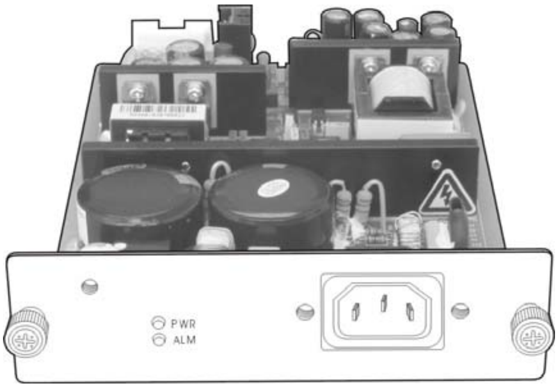


Figure 0-5 Switching Power Supply Module Physical Diagram

The iMX100-AG switching power supply module is a high performance power supply specifically designed for the New Rock's VOIP gateways. It has the common AC input and multiple DC outputs. A single module provides the ample power for a full loaded iMX100-AG system. As an option, uses can select dual redundant power supply modules. The power module supports the load sharing operation mode.

The iMX100-AG switching power supply module inputs 100v to 240 v AC voltage and output several independent DC voltages：

- -70V for ringing and off-hook
- -24V for talking battery
- +5V for ringing SLIC
- 3.3V for logic devices

iMX100-AG switch power supply module is hot swappable. iMX100-AG can maintain normal operation when a power module is added, removed, or exchanged in a live system.Table2-7 shows the pin assignments for DC outputs.

Table 0-11: Pin Assignments for DC Outputs

Pin	Description		Pin
2	-70V/0.5A	GND	1
4	-24V/1.5A	GND	3
6	5V/1A	GND	5
8	3.3V/5A	GND	7
10		GND	9

3

PREPARATION FOR INSTALLATION

To avoid any body injury and device damage, please read this chapter carefully before the installation.

Safety Check

For your safety, please follow the following items when MX 100 is installed and used. Please make sure the installation site is away from wet and heat source.

- Follow electricity safety rules
- Please let the experienced or trained operator to install and maintain iMX100-AG
- Wear static discharge wrist strap
- Ensure the proper electric ground of installed equipment
- Properly connect the power cable to iMX100-AG
- Do not unplug the power cable when in use
- UPS should be used to power iMX100-AG

📖 **Note**：Please read carefully the 💡 labeled content when installing iMX100-AG, and be strictly following the operation procedures.

Installation Environment

Temperature/Humidity

The iMX100-AG installation room must maintain normal temperature and humidity.

If the room temperature exceeds the specified maximum temperature, it will shorten the live of the electrical insulation material. If the room humidity exceeds the specified humidity, iMX100-AG may experience electrical static shock and shrinkage of electric insulation material in the metal package. It may also cause metal corrosion. All these will drastically shorten the life span of the iMX100-AG. It is strongly recommended that user control the environmental temperature between 0～40ºC and humidity between 5%～95% (none condensing).

Dust Control and Air Flow

Dust falls on the iMX100-AG might cause intermittent failure in electrical connections. It may cause long term damage to iMX100-AG. It will cause equipment failure and shorten equipment life span. Therefore, iMX100-AG needs to have ample air flow in front of the iMX100-AG air intake and outtake for proper heat exhaust.

Interference and Lighting Hazard

iMX100-AG may experience various types of EMI hazards in operation and its performance may be impacted. To reduce those hazards to the iMX100-AG, it is suggested that：

- Do not install iMX100-AG close to high power wireless equipment, RADAR transmission site, and high frequency high electric current devices.
- Ensure that power source to be electrical interference free.
- Ensure the proper grounding of the iMX100-AG and implement the lighting protection device.

Installing iMX100-AG Chassis

When installing the iMX100-AG chassis please secure the iMX100-AG with screws on a shelf with proper grounding and well air flowed environment.

Inspecting iMX100-AG and its accessories

After the installation preparation is completed, the shipping package can be opened. Please check the items in the package. The items for the iMX100-AG basic configuration are shown in Table 3-1.

Table 0-1: iMX100-AG Basic Configuration and Accessories

Model Number	Qty	Description
MX-CHS01-V02-00	1	iMX100-AG Chassis： one slot for main control module, two slots for the interface

Model Number	Qty	Description
		modules, and two fans
MX-APU70-V02-00	1	75 Watt Power Supply Module
MX-CBL00-0002	1	3 meter power cable
MX-CBL00-0003	1	3 meter console port cable
SFC00-0004	4	Screws
MX-CBL00-0012	2	Analog user line twisted cable

Note： It is suggested that the content of the shipping package are verified according to the sales contract. If there is any question or problem, please contact our customer service department (Email: support@newrocktech.com, telephone number: 011-86-21-61202700)

4

INSTALLATION

Tools Required for Installation

- Screw driver
- Static discharge wrist strip
- Ethernet and console port cables
- Power cable
- Telephone cable
- Wiring HUB, phone handset, fax or, PBX
- Terminals (a PC running terminal program can be used)
- Universal electric meter

Installing the Main Control Module

All iMX100-AG modules are hot-swappable. Installation and maintenance is very easy. Just Please follow the procedure below：

Step1： Turn the two thumb screws of the blank face plate covering the slot housing the Main Control Module counter clock-wise. Store the blank face plate away for later use.

Step2： Slide iMX100-AG Main Control Module along the guide rail into the chassis.

Step3： Snap the Main Control Module on to the backplane in the chassis.

Step4： Turn the two thumb screws clock-wise to secure the Main Control Module until they stops.

Installing the FXS Interface Module

Please follow the procedure below:

Step1： Turn the two thumb screws of the blank face plate covering the slot housing the FXS Interface Module counter clock-wise. Store the blank face plate away for later use.

Step2： Slide the FXS Interface Module along the guide rail into the chassis.

Step3： Snap the FXS Interface Module on to the backplane in the chassis.

Step4： Turn the two thumb screws clock-wise to secure the FXS Interface Module until they stops.

Installing the Power Supply Module

Please follow the procedure below to install the Power Supply Module.

Step1： Turn the two thumb screws of the blank face plate covering the slot housing Power Supply Module counter clock-wise. Store the blank face plate away for later use.

Step2： Slide the Power Supply Module along the guide rail into the chassis.

Step3： Snap the Power Supply Module on to the backplane in the chassis.

Step4： Turn the two thumb screws clock-wise to secure the Main Control Module until they stops.

Installing iMX100-AG onto a Standard Shelf

iMX100-AG is designed to fit into a standard 19 inch shelf with standard 1U form factor. Its physical dimension is 4.4cm high x 43.8cm wide x 42.5cm deep.

Installation procedure is as follows：

Step1： Place a iMX100-AG into an empty slot on a 19 inch shelf and identify the left and right hand.

Step2： Use the screws in the shipping package to secure the iMX100-AG onto the shelf, as illustrated in Figure 4-1.

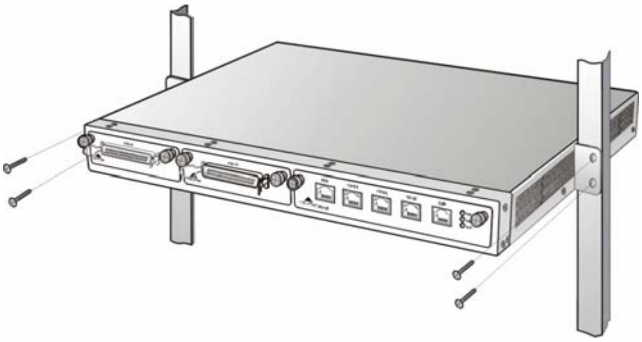


Figure 0-1 Installing iMX100-AG onto a 19 inch shelf

Step3: The shelf and the hands will hold the iMX100-AG in place.

Note:

- Ensure iMX100-AG is horizontal and stable.
- Ensure there is ample airflow space around iMX100-AG.
- Ensure enough space between two iMX100-AGs for ventilation when multiple iMX100-AGs are installed.

Installing Cables

Connecting Console Port

There is a Console Port on iMX100-AG for local configuration, management and diagnostics. iMX100-AG can be connected to a PC with the terminal simulation program through RS232 port.

The Console Port cable in the shipping package has a RJ45 connector on one end for iMX100-AG and DB9 on the other end for a PC.

Console Port cable installation procedure is as follows:

Step1: Choose a terminal (a PC for example).

Step2: Turn off the power of the terminal, and then use the console port cable to link the terminal’s RS232 port with the iMX100-AG Console Port.

Connecting Ethernet Port

There are three 10/100 BaseT Ethernet ports with RJ45 connector type on a iMX100-AG. Each Ethernet port is equipped with LED status display. Ethernet ports transmit voice packet as well as management, maintenance and control information.

The Ethernet Cable needs to be carefully made to ensure IP data and voice quality. The following is the Ethernet cable making scheme:

Step1： A user can use a proper cable peeling cutter to peel away 3cm skin of a CAT-5 cable. What is left is shown in Figure 4-2.

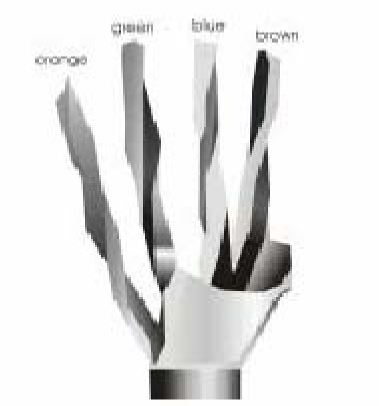


Figure 0-2

Step2： Twisted pairs. Currently the most commonly used standard wiring scheme is EIA/TIA T568B shown in Figure 4-3. In the wiring scheme, pin 1 and 2 are a pair, pin 3 and 6 are a pair, pin 4 and 5 are a pair and pin 7 and 8 are a pair. As shown in the Fig. 4-3, twisted pairs line up with colors (1: white orange，2: orange，3: white green，4:blue，5: white blue，6:green，7: white brown，8: brown). Please pay special attention that the green and white green are separated by a pair of blue wires. It is a common mistake to put green and white green close together, which will result in interference and therefore lower transmission efficiency.

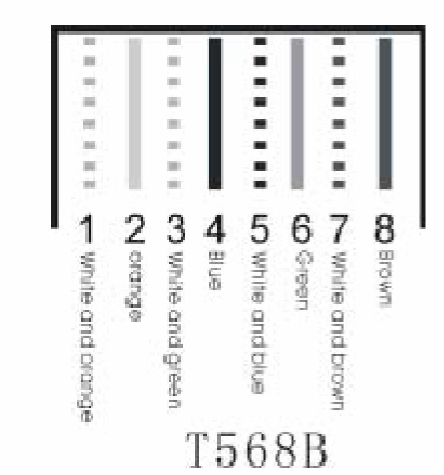


Figure 0-3 T568B Wire Pairing Scheme

Step3： After lining up wires to the correct pin positions, trim all the twisted pairs with a cable cutter, leaving 15mm leads exposed. Then follow Figure 4-4 by inserting wires to their corresponding pin position in the plastic shell of RJ45 connector. Pin 1 will house white orange wire, etc.

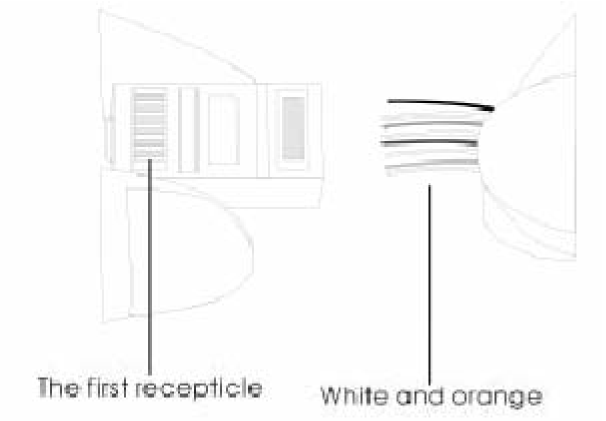


Figure 0-4: RJ 45 Wiring

Step4: After wires have been properly inserted into RJ45 connector; a cramping tool can secure the wires to the connector and make connections to the metal pins as shown in Figure 4-5.

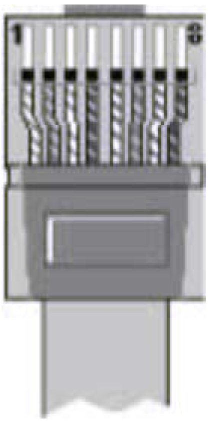


Figure 0-5: Finished RJ 45

Since straight cable is used, the connector for the other end of the cable can be made the same way using RJ45 connector.

Note: Please use shielded CAT-5 cable when option is available for better signal transmission quality.

After the Ethernet cable is ready, one end of the cable can connect to iMX100-AG and the other end connect to a HUB or IP network. Please check the Ethernet LED status: yellow means connecting in progress and green means in operation.

Connecting FXS Cable

iMX100-AG has an FXS interface that connects to analog phones.

Connect one end of the FXS cable to the iMX100-AG FXS interface, and connect the other end to phones, faxes, or PBXs, as shown in Figure 4-6.

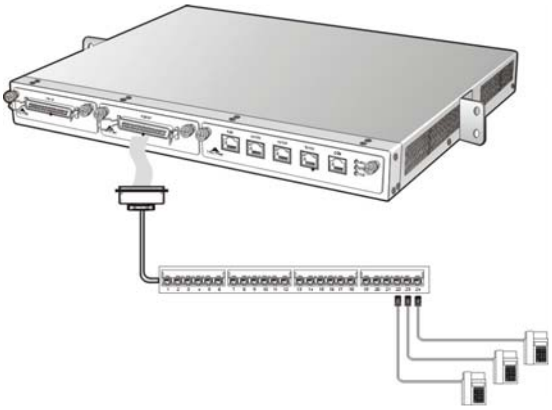


Figure 0-6: Figure 4 - 1 Connect with FXS Cable

Note: To avoid connecting to the wrong interface, please check the identity on the interface before connecting the cable.

Connecting Power Supply

iMX100-AG uses high efficient switching power supply module. Single module can power up the unit with full load. The second power supply module can also be installed to provide redundancy. The switching power supply module has the following characteristics:

Input Voltage Range: 100～240V

Output multiple independent Direct Currents: -70 for ringing and off-hook; -24V for talking battery；+5V for ringing SLIC；3.3V for logic device.

Before connecting to the power outlet, it is suggested that tri-phase power outlet be used and ground be properly connected.

Please follow the procedure when connecting to the power source：

Step1： Turn the switch for the power outlet to OFF position.

Step2： Use the power cable in the shipping package to connect power inlet on the rear end of AG100 and plug the other end to the power outlet of 110V or 220V.

Step3： Turn the switch to ON position.

Step4： Check to see if the PWR LED indicator is lit. If PWR LED is lit, everything is normal. If not, repeat Steps 1 to 3.

Note: If repeated power up fails, please contact customer support. Do not attempt to plug or unplug the power cable or open iMX100-AG while the power switch is on the ON position.

Final Checks after Installation

After installing iMX100-AG and before it is powered on, please make sure of the following:

- There is ample air space around iMX100-AG for heat exhaustion.
- The shelf and iMX100-AG is securely stable and properly grounded.
- Power cord is standard and made with safety approvals.
- Recheck all the other cables and wires and their connections.

💡 **Note:** It is very important to recheck all the installation work to ensure iMX100-AG would function properly and trouble free.

.

5

SYSTEM CONFIGURATION

Login

1. Power up the MX-AG100 and obtain the IP address.

   MX-AG100 by default uses DHCP (Dynamic Host Configuration Protocol[1]), and will automatically detect an IP address; if you cannot get the IP address (when you connect to the PC directly), use manufacturer's default IP address "192.168.2.218".

   - **If the user network uses DHCP**

     After power up (when user line LCD stops flashing), if the gateway uses MGCP protocol, it will announce repeatedly the IP address to the first off-hook user; if using SIP protocol, you can press "##" to get the IP address through any user line at any time.

   - **If the user network uses static IP address**

     When DHCP service is not on (or when iMX100 is directly connected with the PC), the MX-AG100 will use the default IP address 192.168.2.218. If you cannot login to the gateway interface, it may be because your PC is not in the same network with MX-AG100's IP address 192.168.2.218. You need to change your PC address to be in the same network as that of the gateway. If after all these effort you still cannot connect or have questions, please contact New Rock's technical support group.

2. Double click e to open IE Explorer and enter in the Address field iMX100AG IP address (for example：192.168.2.218). After you

[1] **DHCP**
DHCP (Dynamic Host Configuration Protocol) is a network protocol used to assign TCP/IP addresses to client servers. Each client server is connected to the central DHCP server, which gives the network configuration of each client, including the IP address, gateway and DNS server information.

enter username and password, you will see the web interface which is shown in Figure 5-1.

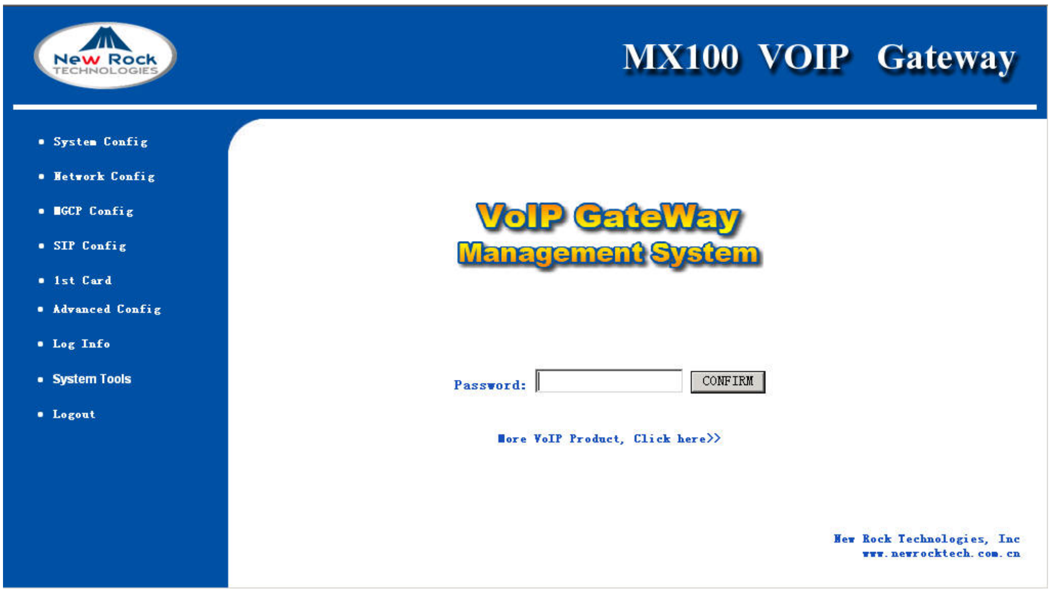


Figure 0-1: iMX100AG VoIP Gateway System Configurations Interface

iMX100AG has two levels of management：the administrator level (default password：iMX100) and the operator level (default password：operator). Administrator level has higher access privilege, and is allowed to change password for all users at all levels.

Operator level has lower access privilege, and certain options are not available including network configurations, password management and restoration of factory default settings.

iMX100AG allows multiple users of different levels to login at the same time. Users of higher privilege have the right to modify configuration; users of lower privilege can only browse.

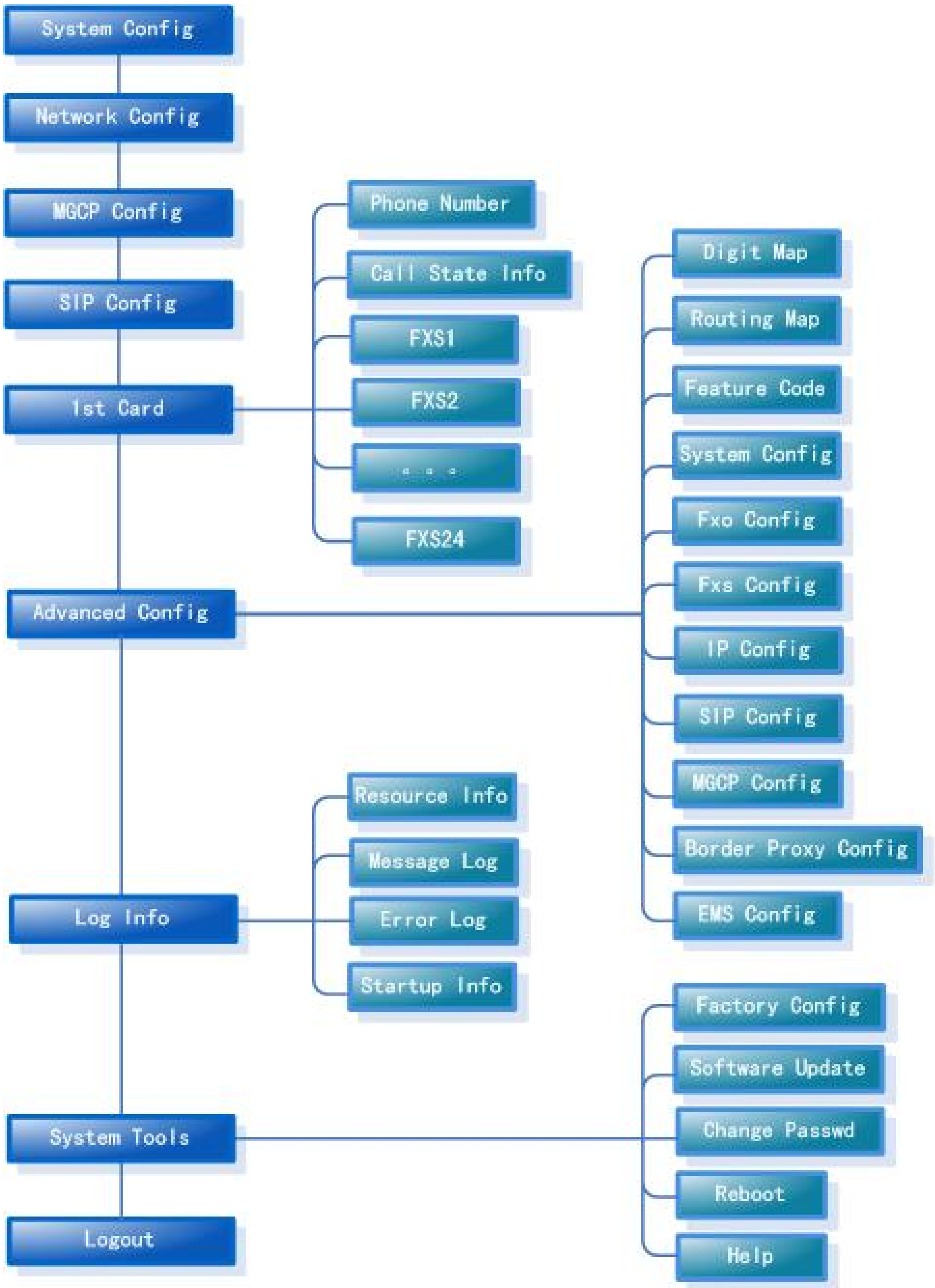
For users of the same level, only the first user to login is able to change configurations. The rest can only browse. A user can see from the log file all the current users and their access levels.

Note 1：After a user logs in, he/she will be automatically logged off if he/she is idle for more than 10 minutes. When that happens, he/she needs to log in again.

Note 2：After completing the configuration, a user must completely exit out instead of just closing the browser. This will elevate the access level of the next logged user so he/she will be able to change the configurations.

Menu Structure and Function Description of Most Used Buttons

The following is the system navigation structure:



Function Description of Most Used Buttons

At the bottom of each configuration page you will see two buttons: Submit and Default.

- **Submit**: When you are done with configuration, click this button once so that the configuration can be saved. After each submission, you will be prompted by “Submission is successful. Please restart the gateway!” You need to click OK to confirm the action.

- **Default**: Click the button once to restore the factory default setting for each parameter.

Note: Clicking this button only restore the defaults settings for the current page. It is different from System Tools -> Restore Factory Default in that the latter restore the default settings for the whole system.

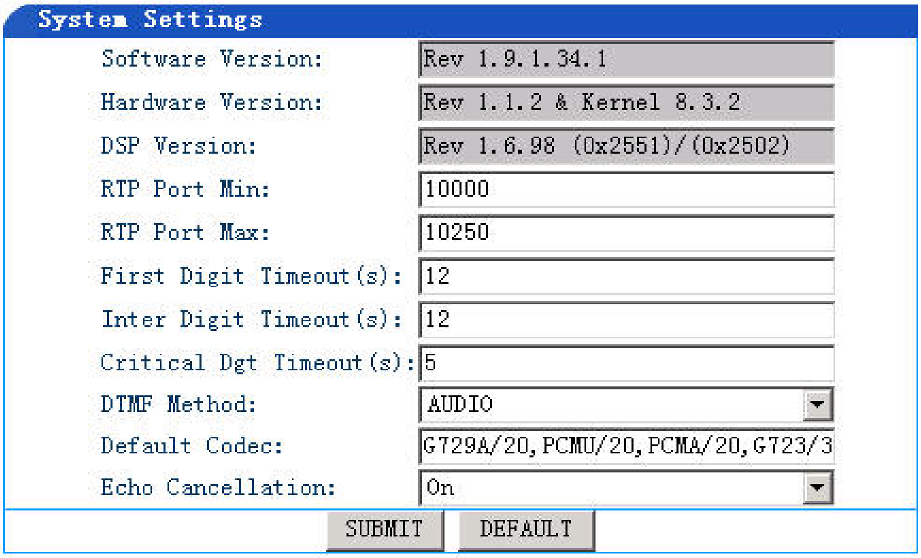
When the restoration is successful, you will be prompted by “The settings are successfully restored. Please restart the gateway!” You need to click OK to confirm the action.

System Config

In this section you input the basic information such as iMX100AG RTP port, dialing time, DTMF mode, and the default codec.

After logging in, click **System Config** link on the left of the web configuration page, and you will see the following:

Note: For information on how to use Submit and Default, see most used buttons.



System Settings

Software Version:	Rev 1.9.1.34.1
Hardware Version:	Rev 1.1.2 & Kernel 8.3.2
DSP Version:	Rev 1.6.98 (0x2551)/(0x2502)
RTP Port Min:	10000
RTP Port Max:	10250
First Digit Timeout(s):	12
Inter Digit Timeout(s):	12
Critical Dgt Timeout(s):	5
DTMF Method:	AUDIO
Default Codec:	G729A/20,PCMU/20,PCMA/20,G723/3
Echo Cancellation:	On

Figure 0-2: System Configuration Interface

Software Version

Software Version field value is automatically detected. You do not need to change this field.

Hardware Version

Hardware Version field value is automatically detected. You do not need to change this field.

DSP Version

DSP Version field value is automatically detected. You do not need to change this field.

RTP Port Min and Max

In the RTP Port Min field enter the minimum value of sending and receiving RTP port. 💡 This is a required field. It is recommended that you enter a value that is greater than 10000.

In the RTP Port Max field enter the maximum value of sending and receiving RTP port. 💡 This is a required field. It is recommended that you enter a value that equals “2 x number of lines + the minimum value”.

📖**Note:** A VoIP call uses two RTP ports: one for RTP and the other for RTCP. If iMX100AG has four lines (FXS or Trunking lines) then the RTP port is set to eight ports at least. If RTP has less than eight ports, four lines can not be used at the same time. iMX100AG supports up to 48 FXS/Trunking lines. So it is highly recommended you set RTP to 96 (48x2) ports. The default minimum value is 10010～10030. You do not need to change it.

First Digit Timeout

In the First Digit Timeout field enter the time (in second) allowed for the dialing of the first digit. When a line goes off-hook, if within the time specified here the first digit has not been dialed, iMX100AG will treat this as an abandoned called and will indicate to the caller to place the phone on hook. The default value is 12 seconds.

Inter Digit Timeout

In the Inter Digit Timeout field enter the time (in second) allowed for the dialing of the middle digits. Counting from the last digit dialed, if within the time specified here no digit has been dialed, the system will send the dialed number out. The default value is 12 second.

Critical Dgt Timeout

In the Critical Dgt Timeout field enter the time (in second) for finished dialing. 💡 This parameter is used in conjunction with x.T in the dialing rule. After the first digit in the rule has been dialed, if within the time specified here no digit follows, iMX100AG will send the dialed number out. The default value is 5 seconds.

DTMF Method

In the DTMF[2] Mode field select the transmission mode. This parameter is used to set DTMF signal transmission mode. Options are Audio mode, 2833 mode, and INFO mode. The default setting is Audio mode.

- Audio mode is a transparent transmit mode;
- INFO mode is information transmit mode;
- 2833 mode is a RTP data packet transmit mode.

In the Default codec[3] field select the codec iMX100AG supports. iMX100AG supports iLBC/30, G729A/20, G723/30, PCMU/20, PCMA/20 and GSM/20 (as shown in Table 5-1). Multiple values are demarked by commas. When multiple modes are selected, the gateway will, in a sequential order, select the mode supported by both sides.

Table 0-1: Codes supported by iMX100AG

Codec	Kbit/s	Time interval of RTP packets transmission(unit: ms)
iLBC	13.3/15.2	20/30
GSM	13	20
G729A	8	10/20/30/40
G723	5.3/6.3	30/60
PCMU/PCMA	64	10/20/30/40

[2] **DTMF（Dual Tone Multi-Frequency）**
In PSTN service, after a call is connected, user’s touch tone info is transmitted via DTMF, also known as second dial tone information. It is widely used in intelligent network and value-added services.
- Audio: Voice data transparent transmit mode.
- 2833: A special RTP packet. PT field of the header indicates this is a DTMF packet. See FTC 2833 for details.
- INFO: Optional way of DTMF transmission. As in SIP messages, use INFO to indicate a DTMF signal.

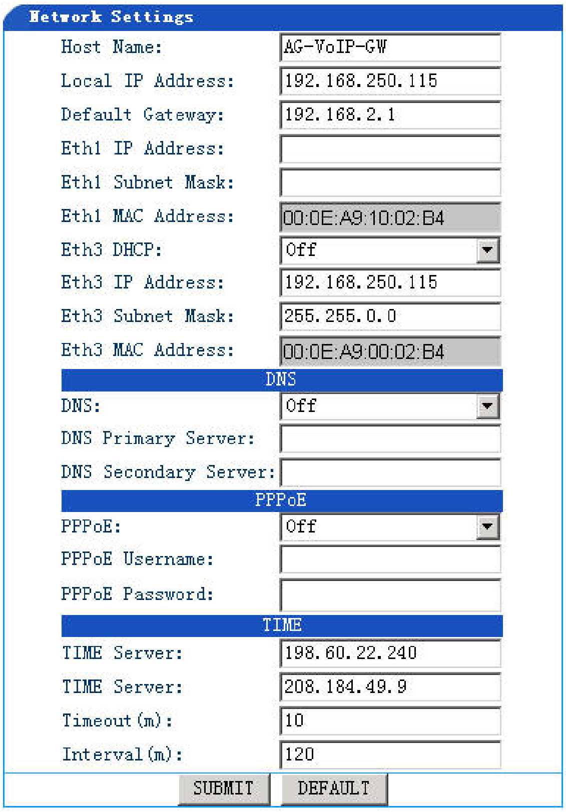
[3] **Voice CODEC**
Also called a "voice codec" or "vocoder," it is a hardware circuit that converts the spoken word into digital code and vice versa. It comprises the A/D and D/A conversion and compression technique. If music is encoded with a speech codec, it will not sound as good when decoded at the other end. A speech codec is an audio codec designed for human voice. By analyzing vocal tract sounds, a recipe for rebuilding the sound at the other end is sent rather than the soundwaves themselves. The speech codec is able to achieve a much higher compression ratio, which results in a smaller amount of digital data for transmission. When telephones were first digitized in the early 1960s, they generated digital streams of 64 Kbps. Since then, speech CODECS have reduced voice to as little as 5 Kbps and less.

In the Echo cancellation[4] select on to invoke echo cancellation and off to close echo cancellation. The manufacturer's default is on. You do not need to change it.

Network Config

After logging in, click the **Network Config** link from the left pane. You will see the following:

Note: For information on how to use Submit and Default, see most used buttons.



Network Settings

Host Name:	AG-VoIP-GW
Local IP Address:	192.168.250.115
Default Gateway:	192.168.2.1
Eth1 IP Address:	
Eth1 Subnet Mask:	
Eth1 MAC Address:	00:0E:A9:10:02:B4
Eth3 DHCP:	Off
Eth3 IP Address:	192.168.250.115
Eth3 Subnet Mask:	255.255.0.0
Eth3 MAC Address:	00:0E:A9:00:02:B4
DNS	
DNS:	Off
DNS Primary Server:	
DNS Secondary Server:	
PPPoE	
PPPoE:	Off
PPPoE Username:	
PPPoE Password:	
TIME	
TIME Server:	198.60.22.240
TIME Server:	208.184.49.9
Timeout(m):	10
Interval(m):	120

Figure 0-3 Network Settings Interface

Host Name

In the Hostname field, enter the iMX100-AG gateway name. You can use your own naming convention according to your network setup. Note: It is suggested not the use an IP address as the hostname. If you

[4] **Echo Cancellation**
The term echo cancellation is used in telephony to describe the process of removing echo from a voice communication in order to improve voice quality on a telephone call. In addition to improving quality, this process improves bandwidth savings achieved through silence suppression by preventing echo from traveling across a network.

do prefer using an IP address, use a logical IP address, i.e., the Gateway IP Address.

Local IP Address

In the Gateway IP Address field enter the iMX100-AG IP address in use.

Default Gateway

In the Ethernet Port 1 IP Address field enter the iMX100-AG Ethernet port number. If you have enabled DHCP services, this field will display the IP address that DHCP detects.

Note: iMX100-AG has three 10/100 Ethernet ports. The following lists the values to configure Ethernet port 3. However you can follow the same steps to configure Ethernet port 1 if you choose to. Ethernet port 2 is reserved for future use.

Eth1 IP Address

In the Ethernet Port 1 Subnet Mask field enter the subnet mask address you obtain from your system administrator or from your ISP if you have not enabled DHCP services.

Eth1 Subnet Mask

Leave the Ethernet Port 1 Hardware MACA Address as it is. You do not need to change it.

Eth1 MAC Address

Eth3 DHCP

Eth3 IP Address

In the Ethernet Port 3 IP Address field enter the IP address for iMX100-AG Ethernet port 3. Factory default is 192.168.2.240.

Eth3 Subnet Mask

In the Ethernet Port 3 Subnet Mask field enter the subnet mask address. Factory default is 255.255.0.0.

Eth3 MAC Address

Leave the Ethernet Port 3 Hardware Address as it is. You do not need to change it.

DNS

DNS

In the DNS[5] field select On or Off to indicate to turn on DNS services or not.

DNS Primary Server

In the DNS Primary Server field enter iMX100-AG's primary DNS server address if you have turned on DNS services. There is no factory default for this field.

DNS Secondary Server

In the DNS Secondary Server field enter alternate iMX100-AG's DNS server address if you have turned on DNS services. There is no factory default for this field.

PPPOE

TIME

Time Server

In Primary TIME Server[6] field enter the IP address of your primary Time server. There is no factory default for this field.

Time Secondary Server

[5] **DNS (Domain Name System, or Service or Server）**
DNS is a very important service of internet, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

[6] **Time Server**
Time Server provides time calibration, control, and synchronization for equipments running in the network.

In Secondary TIME Server field enter the IP address of your alternate Time server. There is no factory default for this field.

Timeout

In the Timeout field enter the time (in minute) allowed to locate the TIME server. If the server is not located within the time allowed, iMX100 will try to locate it again. There is no factory default for this field.

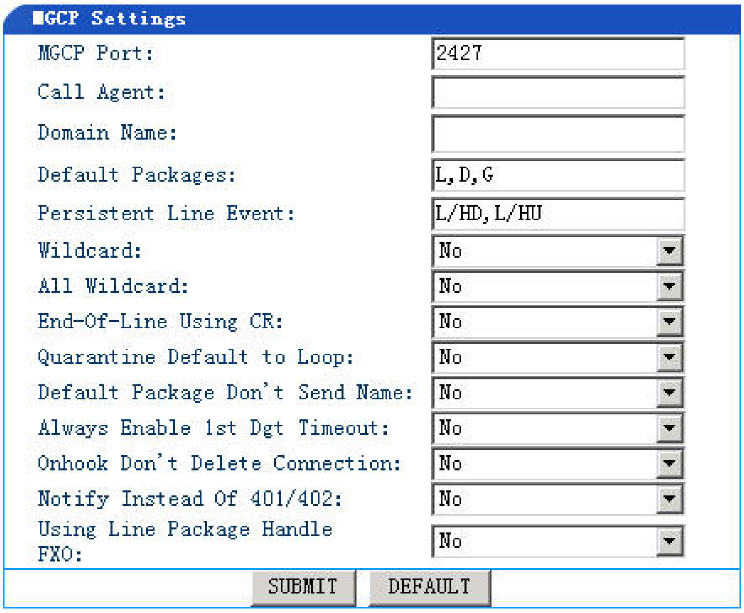
Interval

In the Interval field, enter the time interval (in minute) at which iMX100 will synchronize its time with the TIME server. There is no factory default for this field.

MGCP Config

After logging in, click the **MGCP Config** link on the left of the web configuration page, and you will see the following:

Note: For information on how to use Submit and Default, see most used buttons.



MGCP Settings

MGCP Port:	2427
Call Agent:	
Domain Name:	
Default Packages:	L,D,G
Persistent Line Event:	L/HD,L/HU
Wildcard:	No
All Wildcard:	No
End-Of-Line Using CR:	No
Quarantine Default to Loop:	No
Default Package Don't Send Name:	No
Always Enable 1st Dgt Timeout:	No
Onhook Don't Delete Connection:	No
Notify Instead Of 401/402:	No
Using Line Package Handle FXO:	No

Figure 0-4: MGCP Settings Interface

MGCP Port

In the MGCP Port field enter iMX100-AG's gateway MGCP port number. Factory default is 2427. You can use any port number as long as it does not conflict with another port number.

Call Agent

In the Call Agent[7] field enter the call agent address and port number. Address and port number should be separated by a colon. Address could be IP address or domain name. If you use domain name, you should invoke DNS service and set parameter of DNS server in the System Settings page. A complete sample configuration is like this: 202.202.2.202:2727; callagent.com:2727.

Domain Name

In the Domain Name field enter the internet address or the IP address of the gateway. Examples: test.sunshinemind.com; [192.168.2.100] (if using IP address, [ ] signs can not be omitted).

Default Packages

In the Default Packages field enter all default packages. Use comma to separate each package. The default setting is L, D, G, which means Line Package, DTMF Package, and Generic Media Package.

Persistent Line Event

[7] **Call Agent**
Call Agent, also known as Media Gateway Controller, controls the Media Gateway. In MGCP, a call agent primarily handles all the call processing by linking with the IP network through constant communications with an IP signaling device, for example an SIP Server or an H.323 gatekeeper.
Call Agent is comprised of the call control "intelligence" and a media gateway boasting the media functions, for example conversion from TDM voice to Voice over IP.

Media Gateways feature endpoints for the Call Agent to create and manage media sessions with other multimedia endpoints. Endpoints are sources and/or sinks of data that can be physical or virtual. For creating physical endpoints, hardware installation is needed while virtual endpoint can be created using available software.

Call Agents come with the capability of creating new connections, or modify an existing connection. Generally, a media gateway is a network element which provides conversion between the data packets carried over the Internet or other packet networks and the voice signals carried by telephone lines. The Call Agent provides instructions to the endpoints to check for any events and - if there is any - create signals. The endpoints are designed in such a way as to automatically communicate changes in service state to the Call Agent. The Call Agent can audit endpoints and the connections on endpoints.

In the Persistent Line Event field enter all types of persistent line event. Use comma to separate each line event. The gateway will report to call agent when it handles an event. The default setting is L/HD, L/HU, and L/HF. L/HD means off-hook; L/HU means on-hook; and L/HF means hook flash.

Wildcard

In the Wildcard field select yes or no to indicate if iMX100-AG will add the fixed prefix when it registers with the call agent (such as ： aaln/*). For example, if you select yes here, and the FXS Line 1 is setup as aaln/1, FXS Line 2 is setup ass aaln/2, FXS Line 3 as aaln/3, then the gateway will register as aaln/* with the MGCP call agent and therefore do not need to register each line separately.

All Wildcard

In the All Wildcard field select yes or no to indicate if iMX100-AG will not add the fixed prefix when it registers with the call agent (such as ： *). The default value is no; if set to yes, the gateway will deal with all wildcard.

End-Of-Line Using CR

In the End-Of-Line Using CR field select yes or no to indicate if iMX100-AG will use CR as line stop symbol when sending messages. If set to no, CRLF will be used.

Quarantine Default to Loop

In the Quarantine Default to Loop field select yes or no to indicate how iMX100-AG will response it receives a request. If set to yes, gateway will report continuously all events that are related to this request; if set to no, gateway will report only once to each request.

Default Package Don’t Send Name

In the Default Package Don’t Send Name field select yes or no. If set to yes, the gateway will respond to the default package without a package name; if set to no it will respond to the default package with a package name.

Always Enable 1st Digit Timeout

In the Always Enable 1st Digit Timeout field select yes or no to indicate how iMX100-AG will handle events when there is no timeout indication from a request. If set to yes, the gateway will timeout according to the value in system settings when the caller does not dial a phone number after going off-hook.

On-hook don't Delete Connection

In the On-hook don't Delete Connection field select yes or no. If you select yes, the gateway will disconnect automatically when the caller goes on-hook; if you select no the gateway will wait for the call agent to disconnect.

Notify Instead of 401/402

In the Notify Instead of 401/402[8] select yes or no. If you select yes, the gateway will use off-hook notification (NTFY[9])message instead of 401 message and on-hook notification message instead of 402 message; if set to no, the gateway will still send out 401 and 402 messages.

Using Line Package Handle

In the Using Line Package Handle FXO field select yes or no. If you select yes, the gateway will treat FXO using Line Package; if you select no, it will handle FXO using Handset Package.

SIP Config

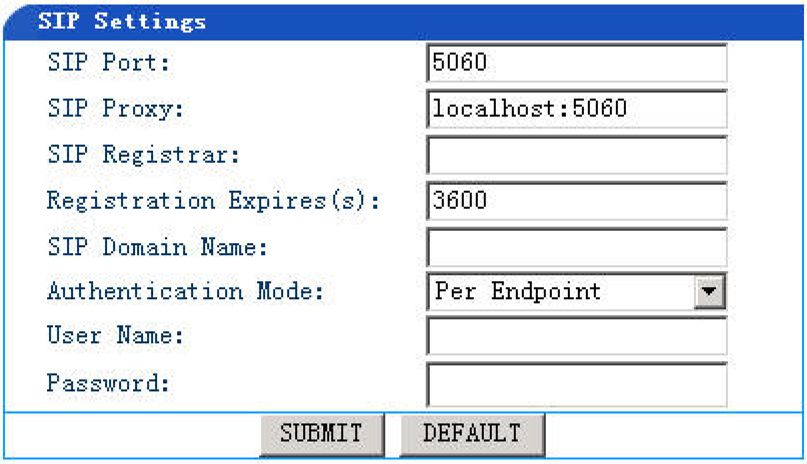
After logging in, click the **SIP[10] Config** link on the left of the web configuration page, and you will see the following:

[8] **401/402:** Response Code.

[9] **NTFY**: Notification, or Notify, a command sent from gateway to call agent.

[10] **SIP (Session Initiation Protocol)**
Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between two or more end points.

Note: For information on how to use Submit and Default, see most used buttons.



SIP Port:	5060
SIP Proxy:	localhost:5060
SIP Registrar:	
Registration Expires(s):	3600
SIP Domain Name:	
Authentication Mode:	Per Endpoint
User Name:	
Password:	

Figure 0-5: SIP Configuration Interface

SIP Port

In the SIP Port field enter the number of SIP local port. The default value is 5060. Local port number can be set to anything you like, as long as it doesn't conflict with the other port numbers in the system.

SIP Proxy

In the SIP Proxy field enter the address and port number of the Proxy server. The address and port number is separated by a colon. The address can be in either the IP address or the domain name. When using domain name, you need to invoke DNS service in the Network Setting page and set the parameters for the DNS server. The complete and valid setting should be like 201.30.170.38:5060 or softswitch.com:5060.

SIP Registrar

In the SIP Registrar[11] field enter the address and port number of the SIP Registrar. The address and port number are separated by a colon. The address can be either the IP address or the domain name. When

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

[11] **Registrar**
When a client powers on, it will tell network its IP address in order to be found. We call this procedure "register". The server that accepts this request is called "registrar".

using domain name, you need to invoke DNS service in the Network Setting page and set the parameters for the DNS server. The complete and valid setting should be like 201.30.170.38:5060 or regster.com:5060.

Registration Expires

In the Registration Expires(s)[12] field enter the time (in second) allowed for SIP re-registration. Manufacturer's default setting is 3600.

SIP Domain Name

In the SIP Domain Name field enter your SIP domain name. If the field is left empty, iMX100-AG will use the address of the Proxy server as the domain name. It is recommended that you do not use a private network IP address in this field. The valid configuration should be like 210.25.185.33 and test.sunshinemind.com.

Authentication Mode

In the Authentication Mode field use the drop down menu to make a selection. Per Endpoint means to register and authenticate according to each individual line; Per Gateway Reg means to register and authenticate according to the gateway; Per Gateway Auth means to register according to each individual line, and to authenticate according to the gateway.

User Name

Enter the User Name if registered as Per Gateway Reg or Per Gateway Auth; if registered as Per Endpoint, do not set this parameter.

Password

In the Password field enter soft-switch authentication password, which can be digits or characters. The password is case sensitive. If registered as Per Gateway Reg or Per Gateway Auth you need to set

[12] **Registration Expires**
In order to control client side, every register message has a certain stored period. If the message is modified in that period, which mean it works for user otherwise Registrar will consider the message is not useful any more, so it will be deleted.

this parameter; if registered as Per Endpoint, the password you enter here is shared by all lines; leave this field empty if you are going to use different password for each line.

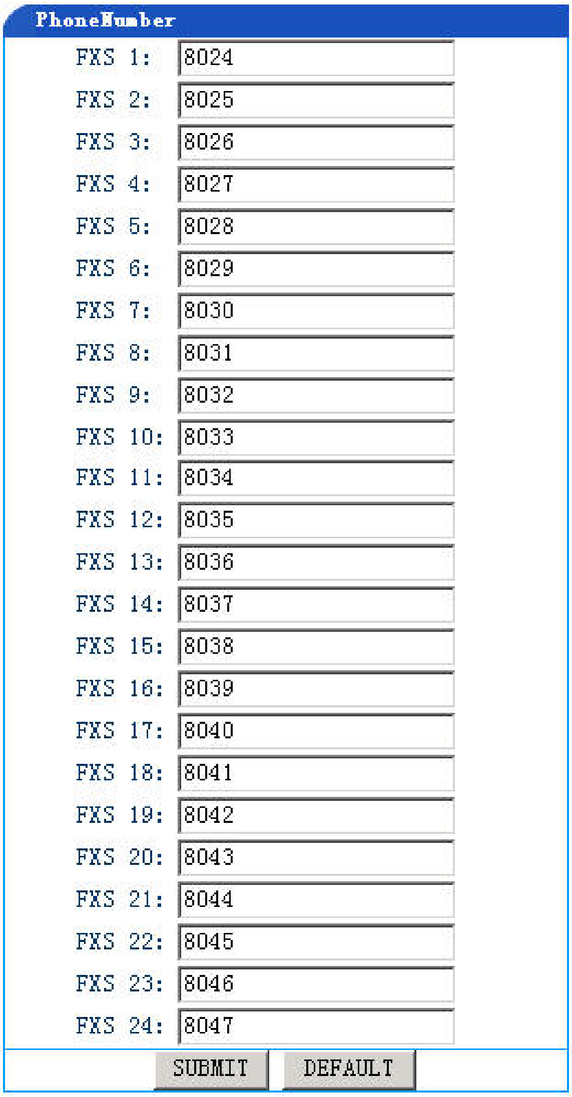
1st/2nd Card

An iMX100-AG can have up to two FXS cards, and each FXS card provides 24 phone lines. If you have two FXS cards, you will see both on the web configuration page. Both cards should be configured the same way. The following lists the steps for configuring FXS1 card.

Phone Number

After logging in, click **1st Card > Phone Number**, and you will see the following:

Note: For information on how to use Submit and Default, see most used buttons.



PhoneNumber

FXS 1:	8024
FXS 2:	8025
FXS 3:	8026
FXS 4:	8027
FXS 5:	8028
FXS 6:	8029
FXS 7:	8030
FXS 8:	8031
FXS 9:	8032
FXS 10:	8033
FXS 11:	8034
FXS 12:	8035
FXS 13:	8036
FXS 14:	8037
FXS 15:	8038
FXS 16:	8039
FXS 17:	8040
FXS 18:	8041
FXS 19:	8042
FXS 20:	8043
FXS 21:	8044
FXS 22:	8045
FXS 23:	8046
FXS 24:	8047

Figure 0-6: Phone Number Configuration Interface

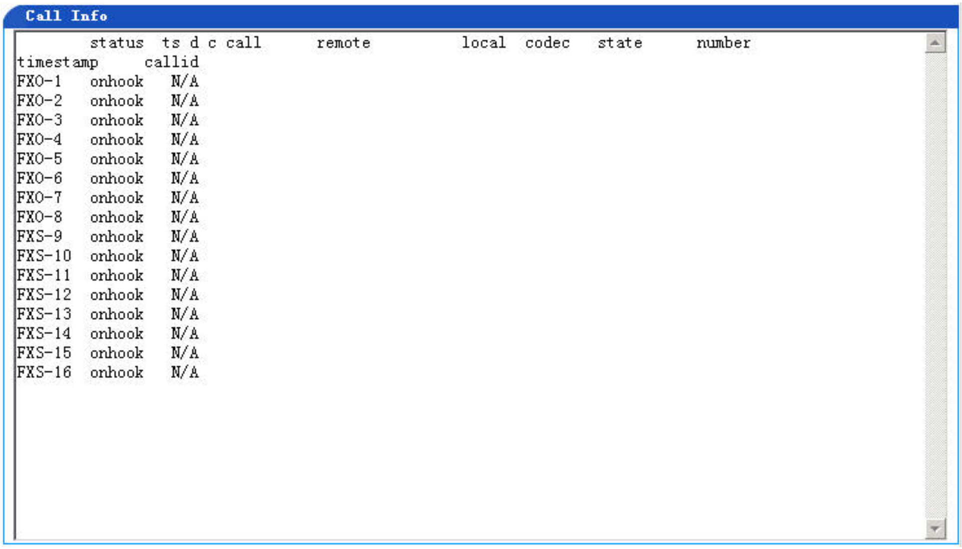
FXS1~24

Enter the phone number for each line as demonstrated in the figure above.

Call State Info

The gateway administrator is able to monitor call status.

After logging in, click **1st Card > Call State Info** link on the left of the web configuration page. The following displays:



```
       status  ts d c call      remote          local  codec   state      number
timestamp     callid
FXO-1  onhook   N/A
FXO-2  onhook   N/A
FXO-3  onhook   N/A
FXO-4  onhook   N/A
FXO-5  onhook   N/A
FXO-6  onhook   N/A
FXO-7  onhook   N/A
FXO-8  onhook   N/A
FXS-9  onhook   N/A
FXS-10 onhook   N/A
FXS-11 onhook   N/A
FXS-12 onhook   N/A
FXS-13 onhook   N/A
FXS-14 onhook   N/A
FXS-15 onhook   N/A
FXS-16 onhook   N/A
```

Figure 0-7: Call Info Interface

Table 0-2:

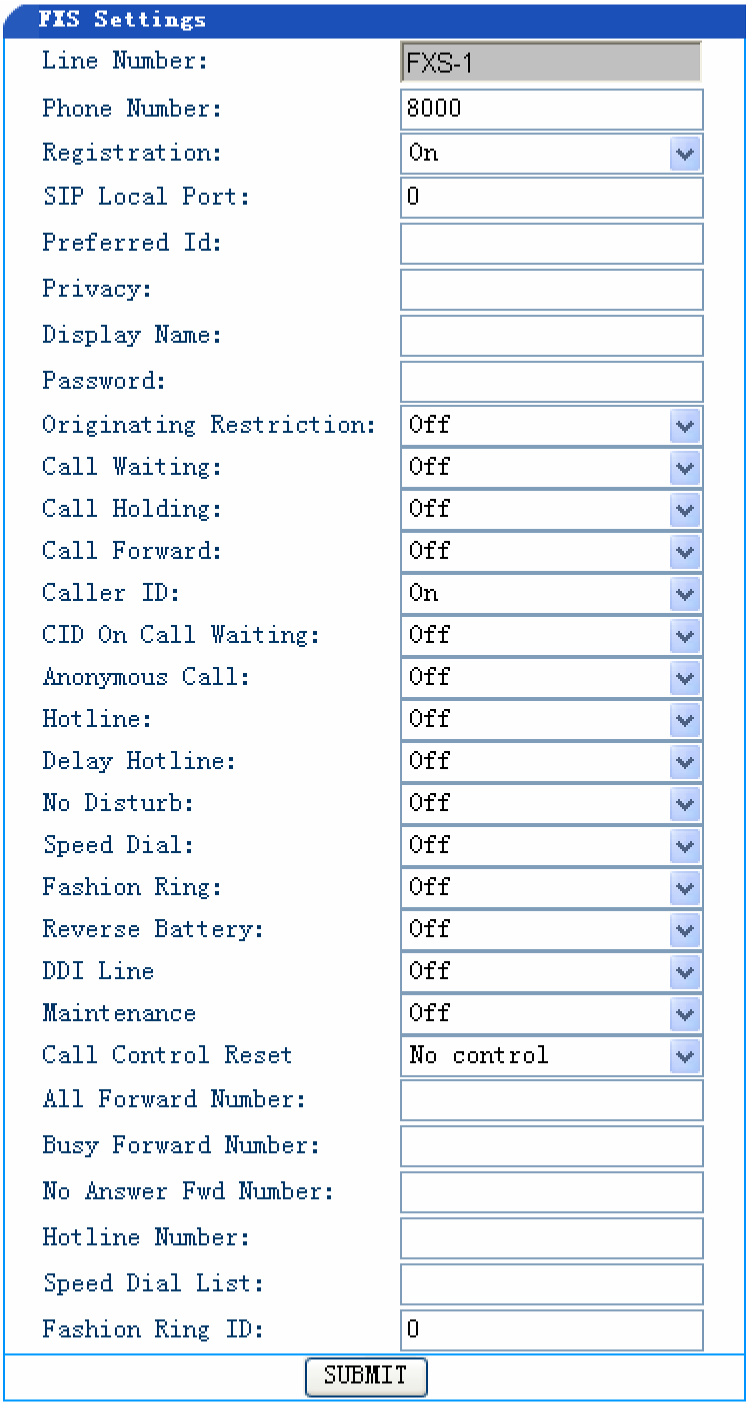
Param.	Description
status	off/on-hook and ringing status.
ts	timeslot.
d	DSP. This field shows the DSP chip used.
c	channel. This field indicates the channel of DSP.
call	call identifier which is a random number generated by the system.
remote	remote IP address followed by RTP port number.
local	the local RTP port number.
codec	encoding and decoding. iMX100-AG support the following codec: G729A/20，G723/30，PCMU/20，PCMA/20.
state	call state, which indicates the current call status. It can be DIALING; DELIVERED; PRESENT; RECEIVED; and ACTIVE.
number	phone number. (C)：calling number；(D)：called number.
timestamp	which has two types：setup time，the duration of which is 0；and connection time. In figure 5-7, the former is setup time, and the latter is connection time (in seconds).
caller id	randomly generated digit that are used to identify a call when SIP is switching information.

FXS（1～24）

iMX100-AG can have up to two FXS cards, each of which can be equipped with 24 phone lines. Each line is configured the same way. You can customize the configuration according to real life situation. The following is a sample configuration.

After logging in, click **1st Card > FXS1** link on the left of the web configuration interface. The following displays:

Note: For information on how to use Submit and Default, see most used buttons.



FXS Settings

Line Number:	FXS-1
Phone Number:	8000
Registration:	On
SIP Local Port:	0
Preferred Id:	
Privacy:	
Display Name:	
Password:	
Originating Restriction:	Off
Call Waiting:	Off
Call Holding:	Off
Call Forward:	Off
Caller ID:	On
CID On Call Waiting:	Off
Anonymous Call:	Off
Hotline:	Off
Delay Hotline:	Off
No Disturb:	Off
Speed Dial:	Off
Fashion Ring:	Off
Reverse Battery:	Off
DDI Line	Off
Maintenance	Off
Call Control Reset	No control
All Forward Number:	
Busy Forward Number:	
No Answer Fwd Number:	
Hotline Number:	
Speed Dial List:	
Fashion Ring ID:	0

Figure 0-8: FXS Configuration Interface

Line Number

This filed is read only.

Phone Number

Enter the phone number that is assigned to this line. You can enter new one or modify an existing one.

Registration

Select **on** (to register) or **off** (not to register).

Display Name

Used when the end point has display function. The maximum length in this field is 30 characters. There is no default value

Password

If you select on in Registration, then you must enter a password here.

Note: The functions beyond this point only apply to SIP protocol. When using MGCP protocol, there is no need to set them up, as the set up does not work.

Originating Restriction

Select **on** (to indicate the line can only receive calls but not initiate calls) or **off** (no restriction).

Call Waiting

Select **on** (enable) or **off** (disable).

Call Holding

Select **on** (enable) or **off** (disable).

Call Forward

Select **on** (enable) or **off** (disable).

Caller ID

Select **on** (enable) or **off** (disable).

CID On Call Waiting

Select **on** (enable) or **off** (disable).

Anonymous Call

select **on** (enable) or **off** (disable).

Hotline

Select **on** (enable) or **off** (disable).

Delay Hotline

Select **on** (enable) or **off** (disable).

No Disturb

Select **on** (enable) or **off** (disable).

Speed Dial

Select **on** (enable) or **off** (disable).

Fashion Ring

Select **on** (enable) or **off** (disable).

Reverse Battery[13]

Select **on** (enable) or **off** (disable). If set to **on**, the line will send a reverse signal upon call connection and the accounting system starts fee calculation.

DDI Line

Select **on** (enable) or **off** (disable) to use the Direct Dialing In (DDI) function. Default is **off**.

Maintenance

Select **on** or **off** to indicate to turn the power on/off for this line. Default is **off**.

Call Control Reset

All Forward Number

The forward to number set up in section Feature will display. You can also enter a different number here to overwrite the previous number. If this line subscribes to All Forward feature, enter the corresponding forward number. If left empty, it indicates All Forward feature has been disabled on this line.

Busy Forward Number

[13] **Reverse Battery Signaling**
Loop signaling in which battery and ground are reversed on the tip and ring of the loop to give an "off-hook "signal when the call receiver answers. Note: Reverse-battery signaling may be used either for a short period, or for the duration of a call, to indicate that it is a toll call.

The forward to number set up in section Feature will display. You can also enter a different number here to overwrite the previous number. If this line subscribes to Busy Forward feature, enter the corresponding forward number. If left empty, it indicates Busy Forward feature has been disabled on this line.

No Answer Fwd Number

The forward to number set up in Set up No Answer Forward will display. You can also enter a different number here to overwrite the previous number. If this line subscribes to No Answer Forward feature, enter the corresponding forward number. If left empty, it indicates No Answer Forward feature has been disabled on this line.

Hotline Number

The forward to number set up in section Feature will display. You can also enter a different number here to overwrite the previous number. If this line subscribes to Hotline Number feature, enter the corresponding hotline number here. If left empty, it indicates the Hotline Number feature has been disabled on this line.

Speed Dial List

Enter the speed dial code number (any two digits between 20 and 49) plus the actual number. There is a hyphen after the code and before the actual number. Multiple entries are separated by /. Example: 20-3221860/21-7558888/22-5552525. If the line user has already set up speed dial list, it will automatically display.

Fashion Ring ID

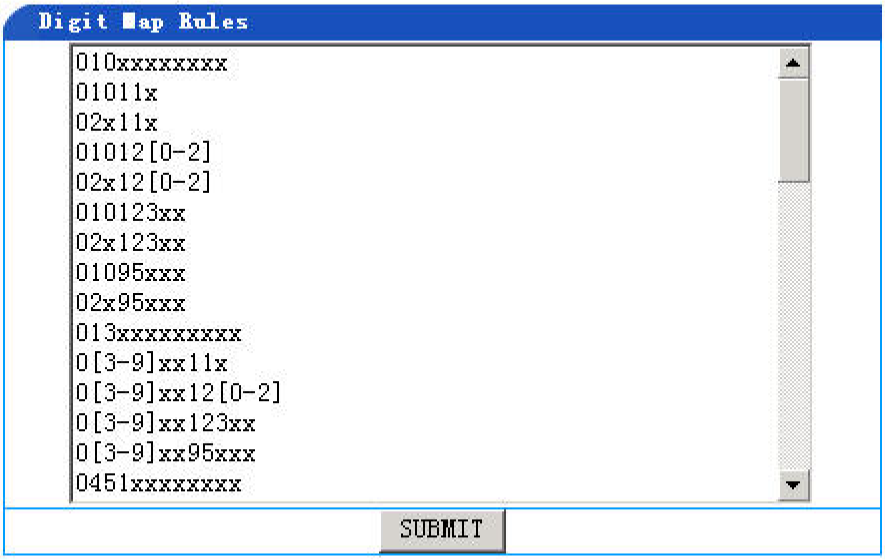
The fashion ring ID set up in section Feature will display. You can also enter a different fashion ring ID here to overwrite the previous one. If this line subscribes to Fashion Ring feature, enter the fashion ring ID here. Default is 0, meaning fashion ring function is disabled.

Advanced Config

Digit Map

After logging in, click **Advanced Config > Digit Map** on the left of the web configuration page. The following displays:

📖 **Note:** For information on how to use Submit, see most used buttons.



```
010xxxxxxxx
01011x
02x11x
01012[0-2]
02x12[0-2]
010123xx
02x123xx
01095xxx
02x95xxx
013xxxxxxxxx
0[3-9]xx11x
0[3-9]xx12[0-2]
0[3-9]xx123xx
0[3-9]xx95xxx
0451xxxxxxxx
```

Figure 0-9: Digit Map Configuration Interface

Digit Map is used to determine if the digits received are the complete numbers dialed, so that the dialing process will terminate and the digits will be sent out in a speedy way. This can shorten the connection time for calls.

iMX100-AG has in its default Digit Map most of the domestic digit map rules. You do not have to re-configure them. You can add new rules when necessary. The following is an illustration of the common rules:

Table 0-3: Common Digit Map Rules

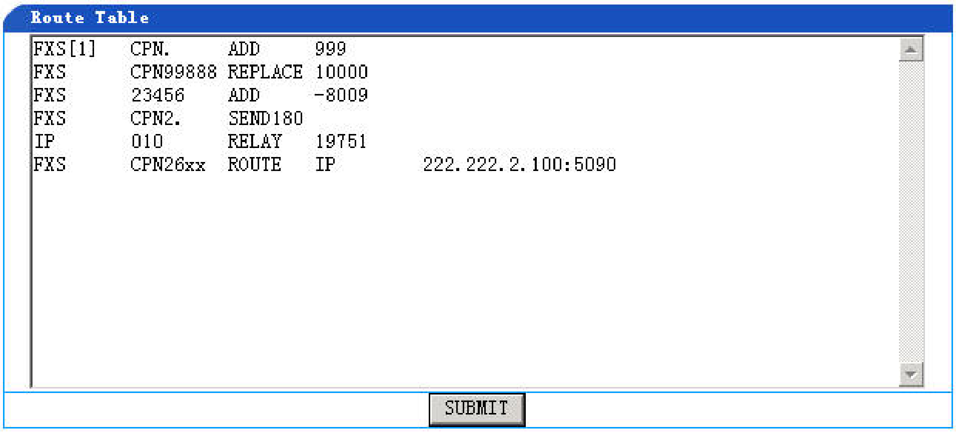
Digit Map	Description
x	Any single digit between numbers 0 to 9
.	Any multiple digits between numbers 0 to 9
##	Terminate dialing after receiving two ##. ## is iMX100AG's default function key for listening to the IP address.
X.T	The gateway will check a number of any lengths that is composed of any numbers between 0 and 9. If no new digits are received within the "dial finish" time, the gateway will send out the detected number.
X.#	A number of any lengths that starts with any number between 0 and 9. If the end user dials # right after the number, iMX100 will stop number reception and send out the number before #.
*XX	Terminate dialing after receiving * plus any two digits. *xx is mainly used to enable the supplementary features (such as Distinctive Ring, Do Not Disturb, and Call Forwarding).
#XX	Terminate dialing after receiving * plus any two digits. *xx is mainly used to enable the supplementary features (such as Distinctive Ring, Do Not Disturb, and Call Forwarding).
[2-8]XXXXXX	A seven-digit number that starts with any number between 2 and 8. This is used to terminate local call dialing.

02XXXXXXXXX	An 11-digit number that starts with 02. This is used to terminate long distance call dialing that starts with 02.
013XXXXXXXXX	A12-digit number that starts with 013. This is used to terminate long distance cellular calls that start with 013.
13XXXXXXXXX	An11-digit number that starts with 13. This is used to terminate local cellular calls that start with 13.
11X	A three-digit number that starts with 11. This is used to terminate emergency calls.
9XXXX	A five-digit number that starts with 9. This is used to terminate special service calls.
17911 (this is an example)	Send out the number right after receiving 17911. This serves as an example of terminating a special number.

Routing Map

After logging in, click **Advanced Config > Routing Map** on the left of the web configuration page. The following displays:

Note: For information on how to use Submit, see most used buttons.



```
FXS[1]   CPN.     ADD     999
FXS      CPN99888 REPLACE 10000
FXS      23456    ADD     -8009
FXS      CPN2.    SEND180
IP       010      RELAY   19751
FXS      CPN26xx  ROUTE   IP        222.222.2.100:5090
```

Figure 0-10: Route Table Configuration Interface

Routing table serves two main functions: number swapping and route exchange. The table is executed from top to bottom. Number swapping always has advantage over route exchange. A routing table can have a maximum of 50 entries.

Note: The routing table is empty by default. All the calls go to the SIP Proxy server, and are routed by this server.

1. **Number Swapping**

   One phone number consists of three sections: Origination, Number, and Action.

   - **Origination** can have the following values: IP, FXS, and FXO. IP can be any IP address, a specified IP address, and a specified IP address plus the port number. FXS and FXO can be a specific line number (for example FXS1, FXO2 or FXS 1 – 2, etc.)

- **Number** can be the calling number, or the called number. Default is the called number. If it is the calling number, add CPN before the number as the identifier. The number can use any digit between 1 to 9, *, ., #, X etc, just like the digit map. The common rules are:
    - Numbers, such as 114, 61202700
    - The beginning digits of a number, such as 61xxxx, or 612x, or 61
    - Expressions such as 268[0-1, 3-9], which indicates a number that starts with 268 and followed by any number from 0 to 1 or 3 to 9
    - The search for a matching number follows the principle of "shortest and quickest". For example, x equals all numbers; xx equals all two-digit numbers; 12x equals all three-digit numbers that start with 12
- **Action** defines the processing method and the actual information that has been processed. It can have three values:
    - **KEEP**: Keep means to keep the number. Another number goes after it. If that number is positive, it means to count the number from the front; if the number is negative, it means to count the number from the backward. For example,
      FXS 02161202700 KEEP -8.

      This means to keep the last eight digits of this called number from the FXS, that is 61202700.
    - **REMOVE**: Remove means to remove the number. Another number goes after it. If that number is positive, it means to count the number from the front; if the number is negative, it means to count the number from the backward. For example,

      FXS 021 REMOVE 3.

      This means to remove 021 if the called number from an FXS starts with 021
    - **ADD**: Add means to add digits before or after the called number. Another number goes after it. If that number is positive, it means to add before the number; if the number is negative, it means to add after the number. For example,

FXS1 CPNX ADD 021
FXS2 CPNX ADD 010

This means to add 021 to all the CNP from FXS1; to add 010 to all the CPN from FXS2.

Another example:
FXS CPN6120 ADD -8888,

meaning to add 8888 to CPN from the FXS that start with 6120

- **REPLACE:** means to replace the number, followed by the number to be replaced to. For example, FXS CPN88 REPLACE 2682000, meaning for a CPN from an FXS that starts with 88, replace it with 2682000

- **END:** means to terminate certain number processing. When performing number swapping from top to bottom, if END or ROUTE is present, then end number swapping. For example,

  FXS 12345 ADD -8001
  FXS 12345 REMOVE 4
  FXS 12345 END

  This means for the called number from an FXS that starts with 12345, first add 8001 at the end of the number; then remove the first four digits; and end the number swapping for CDN that starts with 12345.Another example,

  IP[222.34.55.1] CPNX. REPLACE 2680000
  IP[222.34.55.1] CPNX. ROUTE FXS 2

  This means for any CPN of any lengths that comes from IP address 222.34.55.1, replace it with 2680000, and then route it to the second line of the FXS.

- **SEND180**, meaning to force sending 180. For example,
  FXS CPN2 SEND180,

  meaning for CPN from the FXS that starts with 2, send 180.

- **SEND183**, meaning to force sending 183. For example,
  FXS CPN3 SEND183,

  meaning for CPN from the FXS that starts with 3, send 183.

- **CODEC** means the encoding and decoding method of the CPN/CDN, followed by the actual name of the codec. For example

  PCMU/20/16.

  PCMU is the codec method; 20 meaning every 20ms; 16 is the length of echo cancellation. If echo cancellation is not enabled, a 0 will append at the end automatically (like PCMU/20/0), indicating echo cancellation is disabled. For example,

  ```
  IP      6120    CODEC         PCMU/20/16
  ```

  This means for CDN from an IP address and starting with 6120, use codec PCMU/20. Echo cancellation length is 16ms.

- **RELAY** is one function of IP dialing. For example,

  ```
  IP      010     RELAY         17909
  ```

  This means for CDN from an IP address and starting with 010, dial 17909 first.

2. **Route Exchange**

   One route consists of five sections: Origination, Number, Action, Destination, and Destination Information. Routing table routes the number from an origination to the destination.

   - **Origination** can have the following values: IP, FXS, and FXO. IP can be any IP address, a specified IP address, and a specified IP address plus the port number. FXS and FXO can be a specific line number (for example FXS1, FXO2 or FXS 1 – 2, etc.)

   - **Number** can be the calling number, or the called number. Default is the called number. If it is the calling number, add CPN before the number as the identifier. The number can use any digit between 1 to 9, *, ., #, X etc, just like the digit map. The common rules are:

     - Numbers, such as 114, 61202700

     - The beginning digits of a number, such as 61xxxx, or 612x, or 61

     - Expressions such as 268[0-1, 3-9], which indicates a number that starts with 268 and followed by any number from 0 to 1 or 3 to 9

     - The search for a matching number follows the principle of “shortest and quickest”. For example, x equals all numbers; xx equals all two-digit numbers; 12x equals all three-digit numbers that start with 12

- **Action** should be ROUTE, meaning to route a call.
- **Destination** can have the following values: NONE, IP, FXS, and FXO.
    - Routes that have IP as the Origination usually have FXO, FXS, or NONE as Destination
    - Routes that have FXO or FXS as the Origination usually have IP or NONE as Destination
    - Routes that have FXX/FXS as Destination can use the Destination Information as the route or to hunt for an idle line
    - Routes that have IP as Destination: the Destination Information section must provide a specific gateway IP address plus its SIP port number (if no port number is defined, use the default port number 5060). For example: *192.168.2.10:5066*

      If the IP address is local, use format localhost:5060 or 127.0.0.1:5060. For example,

      ```
      IP     8621       ROUTE              FXS   1
      IP     CPN8620    ROUTE              FXS   2
      ```

      This means a call to the called number from an IP address that starts with 8621 will be routed to the first FXS line; while a call with calling number that starts with 8620 will be routed to the second FXS line.

      Another example:

      ```
      FXS    021     ROUTE               IP
             228.167.22.34:5060
      FXS    020     ROUTE               IP
             61.234.67.89:5060
      ```

      This means a call to the called number from an FXS that starts with 021 will be routed to IP address 228.167.22.34; while a call from an FXS that starts with 020 will be routed to IP address 61.234.67.89.

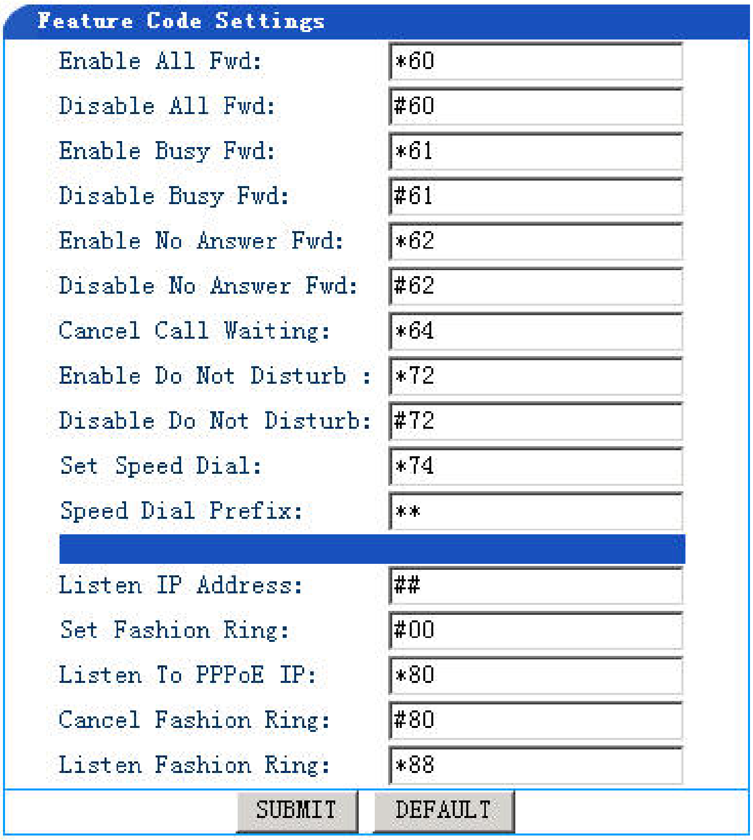
      ```
      IP     CPN[1, 3-5]    ROUTE              NONE
      ```

      This means a call from an IP address with calling number that start with 1, 3, 4, and 5 will not be routed.

Feature Code

After logging in, click **Advanced Config > Feature Code**, and you will see the following:

Note: For information on how to use Submit and Default, see most used buttons.



Feature Code Settings

Enable All Fwd:	*60
Disable All Fwd:	#60
Enable Busy Fwd:	*61
Disable Busy Fwd:	#61
Enable No Answer Fwd:	*62
Disable No Answer Fwd:	#62
Cancel Call Waiting:	*64
Enable Do Not Disturb :	*72
Disable Do Not Disturb:	#72
Set Speed Dial:	*74
Speed Dial Prefix:	**
Listen IP Address:	##
Set Fashion Ring:	#00
Listen To PPPoE IP:	*80
Cancel Fashion Ring:	#80
Listen Fashion Ring:	*88

Figure 0-11: Feature Keys Configuration Interface

This page is used to set up the supplementary feature keys. The general rule is *xx for activation (i.e. dial the * key plus any two digits that represent the feature) and #xx for de-activation (i.e. dial the # key plus any two digits that represent the feature). The screen shows all the features with their default values. The following steps use the default values for the features, and you can customize the values according to your own need.

Enable All Fwd

This allows the customer to define and enable forwarding all calls function. The default function key is *60. To use this feature the customer must first sign up for the call forwarding service.

Disable All Fwd

This feature allows the customer to disable the All Forwarding service.

To inquire the all forwarding number that was set up previously, dial *60*. The gateway will broadcast the most recent number.

For example:

To forward all calls to phone number 61202700, the enabling key is *60. The disenabling key is #60.

a) To enable:

Go off hook → Dial *60 → Upon hearing the dial tone, enter 61202700 → Dial # to end → Go on hook.

b) To verify:

Go off hook → Dial *60 → Upon hearing the forwarded number dial # to end → Go on hook.

c) To disable:

Go off hook → Dial #60 → Go on hook.

Enable Call Forwarding Busy

This allows the customer to enable the forwarding feature when the line is busy. The default function key is *61. To use this feature the customer must first sign up for the call forwarding service.

Disable Busy Forwarding

This allows the customer to disable Busy Forwarding function. The default function key is #61.

For example

To forward all the calls when the line is busy to phone number 61202700, the enabling key is *61. The disenabling key is #61.

a) To enable:

Go off hook → Dial *61 → Upon hearing the dial tone, enter 61202700 → Dial # to end → Go on hook.

b) To verify:

Go off hook → Dial *61 → Upon hearing the forwarded number dial # to end → Go on hook.

c) To disable:

Go off hook → Dial #61 → Go on hook.

Enable Call Forwarding No Answer

This allows the customer to define and enable the forwarding feature when the line is busy. To use this feature the customer must first sign up for the call forwarding service.

Disable Call Forwarding No Answer

The default function key for this feature is #62.

For example

To forward calls to 61202700 when nobody is answering the calls, the enable key is *62, and the disable key is #62.

a) To enable:

Go off hook → Dial *62 → On hearing the dial tone, dial 61202700 → Dial # to end →Go on hook

b) To verify:

Go off hook → Dial *62 → On hearing the forwarded number go on hook

c) To disable:

Go off hook → Dial #62 → Go on hook

Cancel Call Waiting

This allows the customer to disable the call waiting function when a call is in progress to avoid interruption. The default function key is *64. This feature works for only one call. To completely remove call waiting, please refer to section **FXS（1 ~ 24）**.

Enable Do Not Disturb

When this feature is enabled, the customer will not hear the ringing tone when a call comes in. The caller will hear busy tones. The default function key is *72. To use this feature, the customer needs to first sign up for the Do Not Disturb services. Please refer to section **FXS（1 ~ 24）**.

Disable Do Not Disturb

This will restore the normal call handling. The default function key is #72.

Set Speed Dial

The default function key is *74. This allows the customer to use a two-digit code (from 20 to 49) for dialing the complete digits. To use this feature the customer needs to sign up for speed dial services. . Please refer to section **1st/2nd Card > FXS（1 ~ 24）.**

Set Dial Prefix

This defines the identifiers for speed dial. The default function key is **. Before using the speed dial, the customer must first dial these two digits.

For example

The speed dial code for phone number 61202700 is 20, and the speed dial prefix is ** .

a) To enable speed dial:

Go off hook → Dial *74 → On hearing the dial tone, dial 20 plus 61202700 → Dial # to end

b) To verify:

Go off hook → Dial *74 → On hearing the dialing tone, dial 20 plus * to end → On hearing the complete digits, go on hook

c) To use the speed dialing

Go off hook → Dial ** plus 20

d) To disenable:

Go off hook → Dial *74 → On hearing the dialing tone, dial 20 plus # to end

Listen IP Address

This allows the customer to listen to the IP address of his phone line. The default function key is ##.

Enable Line Search

This allows the customer to listen to the phone number of this his phone line. The default function key is #00.

Listen to PPPoE IP

This allows the customer to listen to the gateway's PPPoE IP address. The default function key is #01.

Set Fashion Ring: This allows the customer to set the ring tones to his liking. The default function key is *80. To use this feature the customer needs to sign up for fashion ring service. Please refer to section **FXS（1 ~ 24）**.

Cancel Fashion Ring

This restores the ringing tone to normal. The default function key is #80.

For example

Use the default function key for enabling distinctive ring. Set the distinctive ring ID number from 01 (must have two digits).

a) To enable:

Go off hook → Dial *80 → On hearing the dial tone, dial 01 → Go on hook

b) To verify:

Go off hook → Dial *80 → On hearing the distinctive ringing go on hook.

c) To disenable:

Go off hook → Dial #80 → Go on hook.

Listen Fashion Ring

The default function key is *88.

To use

Go off hook → Dial *88

→ Dial fashion ring ID number 01 → Listen to the ring tones

→ Dial fashion ring ID number 02 → Listen to the ring tones

→ Dial fashion ring ID number 03 → Listen to the ring tones

→ Dial fashion ring ID number 04 → Listen to the ring tones

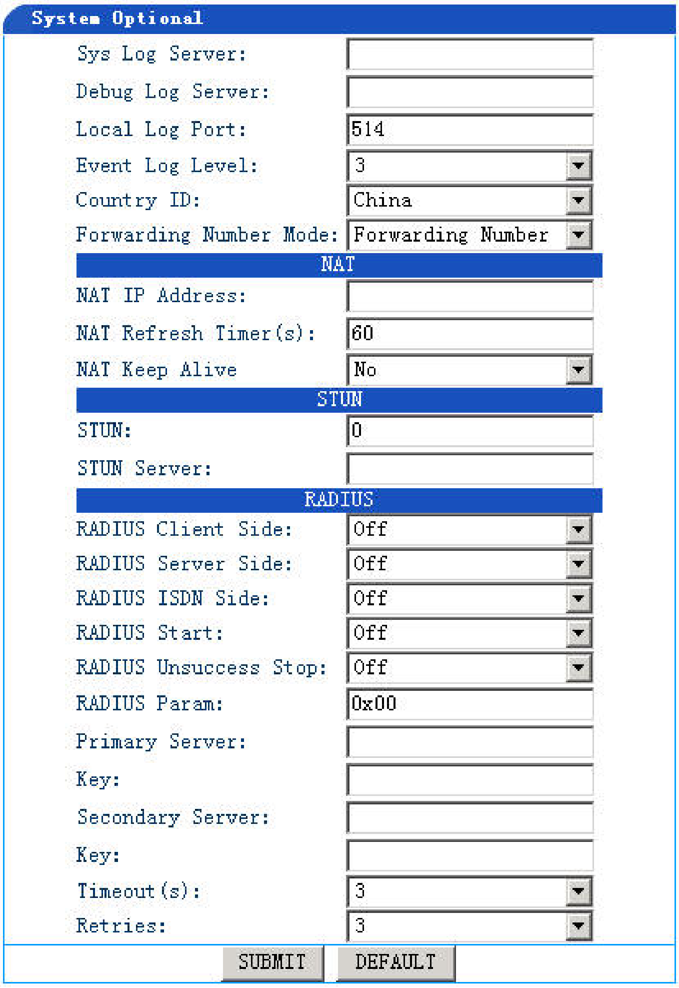
→……

→ Go on hook.

System Config

After logging in, click **Advanced Config > System Config**, and you will see the following:

📖 **Note:** For information on how to use Submit and Default, see most used buttons.



Sys Log Server:	
Debug Log Server:	
Local Log Port:	514
Event Log Level:	3
Country ID:	China
Forwarding Number Mode:	Forwarding Number
NAT	
NAT IP Address:	
NAT Refresh Timer(s):	60
NAT Keep Alive	No
STUN	
STUN:	0
STUN Server:	
RADIUS	
RADIUS Client Side:	Off
RADIUS Server Side:	Off
RADIUS ISDN Side:	Off
RADIUS Start:	Off
RADIUS Unsuccess Stop:	Off
RADIUS Param:	0x00
Primary Server:	
Key:	
Secondary Server:	
Key:	
Timeout(s):	3
Retries:	3

Figure 0-12: Advanced System Settings Configuration Interface

Sys Log Server

This is the IP address of the Event Log Server. It is used for remote debugging. You do not need to set it under normal circumstance.

Debug Log Server

This is the IP address of the Debug Log Server. It is used for remote debugging. You do not need to set it under normal circumstance.

Event Log Port

Default is 514.

Event Log Level

Select any number from 1 to 5. The higher the level, the more detailed the log. Default is set to **3**. Higher level may slow down system performance.

Country ID

Select the country in which the gateway is operate. This determines the signaling standard. Signaling includes dialing tone, ring back tone, busy tone, and ring tone. There are three options: China (Chinese standard), US (American Standard), and Hongkong (Hong Kong Standard).

Forwarding Number Mode

Select from the pull down menu to Calling Party Number or Forwarding Number. This determines if the calling party number or the forwarding number should be displayed when using call forwarding feature. For example, if Calling Party Number is selected here, when 13055553333 calls 2551111 (which has call forwarding function and the forwarded number is 3224422), line 2551111 will display 13055553333; if Forwarding Number is selected, then line 2551111will display 3224422.

NAT

NAT IP Address

If gateway is within the private network and the network outside the NAT[14] is public, you can map the IP obtained from SDP[15] message to a fixed IP. No default value

Note: You can search the IP address from the following websites: www.ipchicken.com; www.showmyip.com; www.whatismyip.com; www.myipaddress.com; and wwww.whatismyipaddress.com.

NAT Refresh Time (s)

Enter the time interval in seconds to refresh NAT status. Default is 15.

NAT Keep Alive

Select Y**es** (to enable) or **No** (to disable). When using MGCP, the gateway will send NTFY (Notify) or RSIP (Restart) message according to the set up of Nap Refresh TimeWhen using SIP, it will send empty SIP message at regular intervals. Default is No.

[14] **NAT (Network Address Translator)**
Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

[15] **SDP (Session Description Protocol)**
SDP describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

STUN

STUN[16]

Select **On** to enable STUN service or **Off** to disable STUN service. If enabled, the gateway will perform STUN operation according to the set up in **Nap Refresh Time.** Default is Off.

STUN Server

Enter the IP address of the STUN Server. If left empty, manufacturer's default STUN server will be used.

RADIUS

iMX100-AG supports RADUIS charging function, but only from the IP perspective.

RADIUS[17] Client Side

Select **On** (to invoke) or **Off** (not to invoke) to indicate to turn on or not the charging function of the called party. Default is Off.

RADIUS Server Side

Select **On** (to invoke) or **Off** (not to invoke) to indicate to turn on or not the charging function of the calling party. Default is Off.

For example:

a) If RADIUS Client is set to On and RADIUS Server is set to Off, then the line will not turn on the charging function when making phone calls; it will when it is the called party.

[16] **STUN (Simple Traversal of UDPover NATs)**
STUN（Simple Traversal of UDP over NATs）
A protocol that allows applications to detect that a network address translation (NAT) is being used. It can also detect the type of NAT and IP address assigned by it. STUN was developed to support interactive, two-way communications over the Internet such as for voice (VoIP) and videoconferencing. The STUN client sends requests to a STUN server, which is typically hosted by the service provider.
Unlike application layer gateways (ALGs) and Middlebox Communications (MIDCOM), which also support two-way communications through NATs, STUN requires no changes to the NAT.

[17] **RADIUS (Remote Authentication Dial In User Service)**
Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

b) If RADIUS Client is set to Off and RADIUS Server is set to On, then the line will turn on the charging function when making phone calls; it will not when it is the called party.

c) If RADIUS Client and RADIUS Server are both set to On, then the line will start the charging function when making or receiving phone calls.

RADIUS ISDN Side

There is no need to set this field for iMX100-AG.

RADIUS Start

Select **On** or **Off** to indicate whether or not to transmit the initial RADIUS record when the charging function of RADIUS client or server is invoked.

RADIUS Unsuccess Stop

Select **On** or **Off** to indicate whether or not to transmit RADIUS record of the unsuccessful calls when the charging function of RADIUS client or server is invoked. Default value is: Off.

RADIUS Param

There is no need to set this field for iMX100-AG.

Primary Server

Enter the IP address and the port of the primary RADIUS server. If no port is set, then use the default port number 1813.

Key

Enter the share key for the communication between primary RADIUS client and server. Make sure the settings of both sides are consistent.

Secondary Server

Enter the IP address and the port of the secondary RADIUS server. If no port is set, then use the default port number 1813.

Key

Enter the share key for the communication between secondary RADIUS client and server. Make sure the settings of both sides are consistent.

Timeout(s)

Enter the time within in which the RADIUS server will wait for a response after it starts. If no response is received within the time set here, RADIUS will re-send the message. Default setting is 3 seconds.

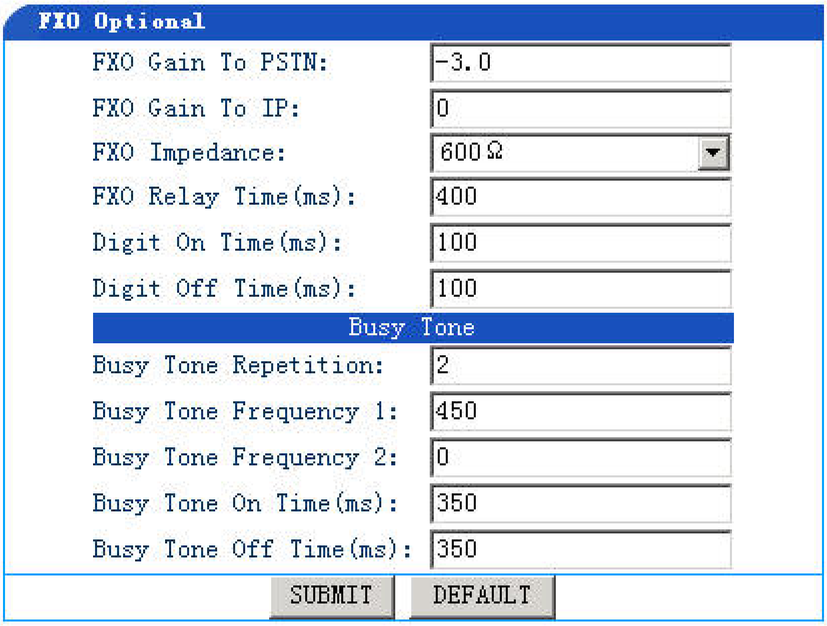
Retries

Enter the number of times to re-send the message if no response is received. Default setting is 3 seconds.

FXO Config

After logging in, click **Advanced Config > FXO Config**. The following displays:

Note: For information on how to use Submit and Default, see most used buttons.



FXO Gain To PSTN: -3.0
FXO Gain To IP: 0
FXO Impedance: 600Ω
FXO Relay Time(ms): 400
Digit On Time(ms): 100
Digit Off Time(ms): 100

Busy Tone

Busy Tone Repetition: 2
Busy Tone Frequency 1: 450
Busy Tone Frequency 2: 0
Busy Tone On Time(ms): 350
Busy Tone Off Time(ms): 350

Figure 0-13: Advanced FXO Settings Configuration Interface

FXO Gain[18] To PSTN

Enter the volume increase into the PSTN. Value range is -6 - +3dB. Default is -3.5dB.

FXO Gain To IP

Enter the volume increase into the IP. Value range is -3 - +3dB. Default is 0.

[18] **Sending Gain (or signaling gain)**
When detected signals are not strong enough over the network, we use signal gain parameter to increase the strength of the signal.

FXO Impedance[19]

Select an FXO impedance number. Options include Complex Impedance; 600Ω; and 900Ω. Default is 600Ω.

FXO Relay Time (ms)

Enter the time (in millisecond) allowed for the dialing of the first digit of the called party number to PSTN after FXO line goes off-hook. The default value is 400.

Digit On Time (ms)

Enter any number from 80 to 150. This parameter specifies the signaling mode[20]) of auto dialing from FXO to PSTN. The default is 100ms.

Digit Off Time (ms)

Enter any number from 80 to 150. This is the interval at which FXO sends out two consecutive digits. The default is 100ms.

Busy Tone

Busy Tone Repetition

Enter a number from 2 to 5. This is the number of times iMX100AG keeps checking busy tone before the FXO line goes on-hook.

Busy Tone Frequency1

Enter the first frequency of the on-hook signal. Default value is 450. There is no need for users in China and US to set up this parameter. The gateway will search for US, China, and China PBX on-hook three signal frequencies.

Busy Tone Frequency 2

Enter the second frequency of the on-hook signal. Default value is 0. There is no need for users in China and US to set up this parameter.

[19] **Line Impedance**
A measure of the total opposition to current flow in an alternating current circuit, made up of two components, ohmic resistance and reactance, and usually represented in complex notation as Z = R + iX, where R is the ohmic resistance and X is the reactance. It also refers to an analogous measure of resistance to an alternating effect, as the resistance to vibration of the medium in sound transmission.

[20] **Signaling Mode**
Signal mode refers to inserting a silence signal periodically into the voice stream. Standard used in China specifies “450 Hz, 350ms ON + 350ms OFF”, means signal cycle is 700ms; insert 350 ms signal plus a silence signal of 350 ms for each cycle.

The gateway will search for US, China, and China PBX on-hook three signal frequencies

Busy Tone On Time (ms)

Enter the time one busy tone will last. This time should be determined by the equipment the FXO is connected to. International standard is 350ms.

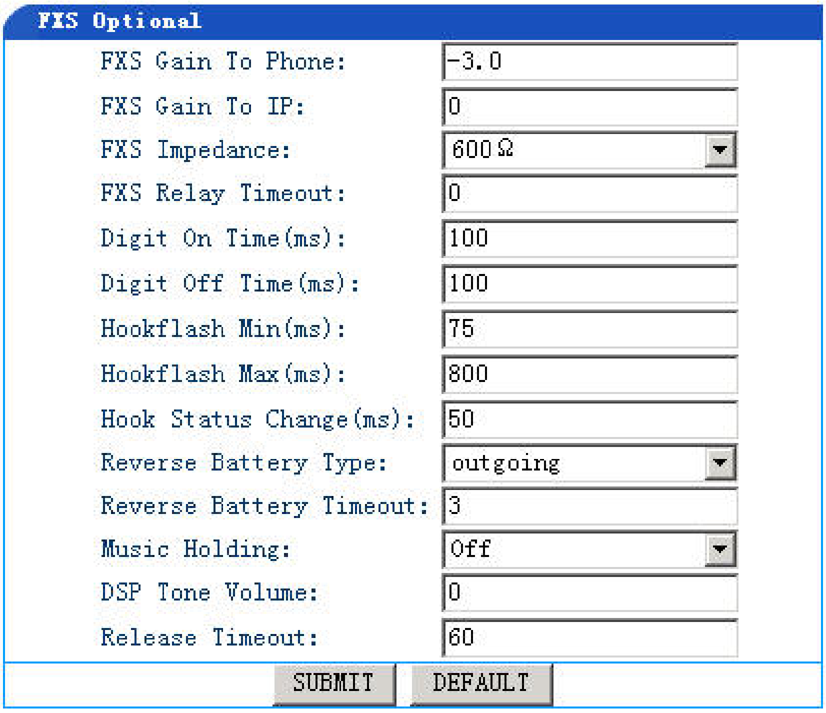
Busy Tone Off Time(ms)

Enter the time interval each busy tone is sent. This time should be determined by the equipment the FXO is connected to. International standard is 350ms.

FXS Config

After logging in, click **Advanced Config > FXS Config**. The following will display:

Note: For information on how to use Submit and Default, see most used buttons.



FXS Optional

FXS Gain To Phone:	-3.0
FXS Gain To IP:	0
FXS Impedance:	600Ω
FXS Relay Timeout:	0
Digit On Time(ms):	100
Digit Off Time(ms):	100
Hookflash Min(ms):	75
Hookflash Max(ms):	800
Hook Status Change(ms):	50
Reverse Battery Type:	outgoing
Reverse Battery Timeout:	3
Music Holding:	Off
DSP Tone Volume:	0
Release Timeout:	60

Figure 0-14: Advanced FXS Options Interface

FXS Gain To Phone

Enter the volume increase to FXS telephone. The range is -6 to +3db. Default is -3.0dB (decrease 3 decibel)

FXS Gain To IP

Enter the volume increase to IP network. The range is -3 to +3db. Default is 0dB.

FXS Impedance

Set the FXS impedance number. Options include Complex Impedance; 600Ω; and 900Ω. Default is 600Ω.

Digit Relay Timeout

Set the digit relay delay in milliseconds. Default is 0. When this parameter is set to 0, it means no digit relay on this FXS port.

Digit On Time(ms)

Set the digit duration for each DTMF digit in milliseconds. The default is 100 milliseconds.

Digit Off Time(ms)

Set the interval between two DTMF digits. The default is 100 milliseconds.

Hookflash Min(ms)

Enter the minimum time for an effective hook flash. The default is 75 ms. Only the hook flash lasts longer than this specified parameter is treated as a hook flash.

Hookflash Max(ms)

Enter the maximum time for an effective hook flash. The default is 800 ms. Hook flash that lasts shorter than the time specified here is treated as hook flash.

Hook Status Change (ms)

Sets the off-hook minimum duration. An off-hook event shorted than this value is ignored. Valid range is 20~1000 ms.

Reverse Battery Type

Default value is **Outgoing**. Two options are available for this parameter:

- **Outgoing:** starting the collect call billing after outgoing call is connected;
- **Both:** starting the collect call billing after incoming or outgoing call is connected).

Reverse Battery Call Timeout

Set the delay from the ringing to sending the collect call billing signal. The default is 3 seconds. The valid value is from 0 to 30 seconds.

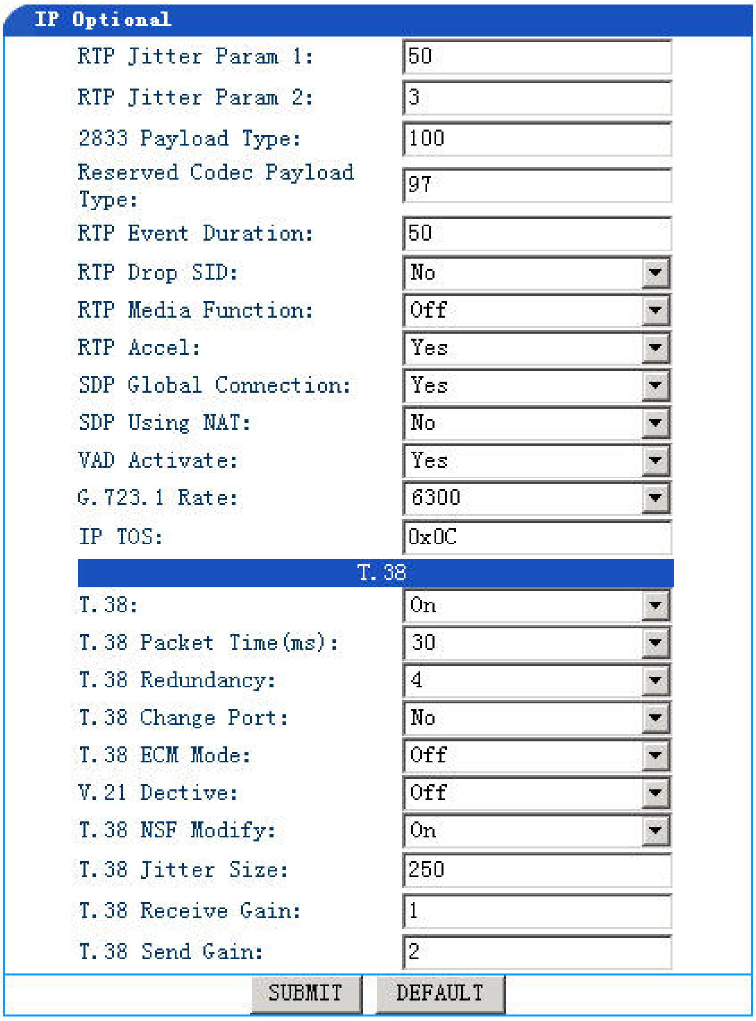
Music on Hold

Select to enable (**On**) or disable (**Off**) fashion ring when a call is put on hold. Default value is: Off.

IP Config

After logging in, click **Advanced Config > IP Config** and the following will display:

Note: For information on how to use Submit, see most used buttons.



IP Optional

RTP Jitter Param 1:	50
RTP Jitter Param 2:	3
2833 Payload Type:	100
Reserved Codec Payload Type:	97
RTP Event Duration:	50
RTP Drop SID:	No
RTP Media Function:	Off
RTP Accel:	Yes
SDP Global Connection:	Yes
SDP Using NAT:	No
VAD Activate:	Yes
G.723.1 Rate:	6300
IP TOS:	0x0C
T.38	
T.38:	On
T.38 Packet Time(ms):	30
T.38 Redundancy:	4
T.38 Change Port:	No
T.38 ECM Mode:	Off
V.21 Dective:	Off
T.38 NSF Modify:	On
T.38 Jitter Size:	250
T.38 Receive Gain:	1
T.38 Send Gain:	2

Figure 0-15: Advanced IP Options Interface

RTP Jitter Param1

Default is 50. It is recommended that you do not change this value.

RTP Jitter Param2

Default is 3. It is recommended that you do not change this value.

2833 Payload Type

Enter a value from 97 to 127. This parameter is used for transmitting 2833 packet type. Default value is: 100. This value needs to be the same with that on the platform end, i.e., the softswitch.

Reserved Codec Payload Type

Enter a value from 97 to 127. This is the RTP load type when using the iLBC codec. Default is 97.

RTP[21] Event Duration (ms)

When gateway detects DTMF events, and if RFC2833 is enabled in System Settings, it will send out the RPT event at a regular interval according to the time interval set here. Default value is: 50 ms.

RTP Drop SID[22]

Set if the gateway should ignore received RTP SID. Default value is: No.
💡 Note: This needs to be set only when irregular frames are received. RTP SID frames in Irregular lengths may cause noise or weird sound.

- **Yes:** Ignore silence packet.
- **No:** Keep silence packet.

RTP Media Function[23]

Set whether to enable Voice Proxy. Default value is: No. This is more applicable to the setting where one gateway is on the public network while the other is on the private one. Under normal situations, Voice Proxy is not needed. When symmetric RTP function is enabled, gateway checks received RTP packet and extract IP and port information from it before dynamically changing IP address and port number used for sending.

- **On:** Enable Voice Proxy.
- **Off:** Disable Voice Proxy.

RTP Accel

Set whether to apply RTP gain when sending and receiving. Default value is: No.

- **Yes:** Enable.
- **No:** Disable.

SDP[24] Global Connection

Setup whether to obtain far end IP address from SDP global connection. Default value is No.

[21] **RTP (Real-time Transport Protocol):** See Glossary.

[22] **SID:** Stands for Silence Information Description.

[23] **Voice Proxy:** See Glossary.

[24] **SDP(Session Description Protocol)**
SDP describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

- **Yes:** Get far end IP address from SDP Global Connection Information.
- **No:** Get far end IP address from Connection Information after SDP Media Description.

SDP Using NAT

Setup whether to use NAT address in out-going SDP. Default value is No.

- **Yes:** Use NAT Address in out-going SDP.
- **No:** Use Local host IP address in out-going SDP.

Notes: This parameter works only when gateway is able to get an NAT address. There are two ways to obtain NAT address:

a) When gateway is using STUN function

b) When gateway starts to register and the 200 OK it gets from the registration server contains NAT information.

VAD Activate

Setup whether to use comfort noise generation technology to simulate background noise from the origination side. Default value is: Yes.

Suggestion: Set this parameter to “Yes” in order to save network bandwidth.

- **Yes:** The speech packet will not be sent out when caller is in silence. Noise is added to the speech stream to replace the silence.
- **No:** The speech packet will be sent out even when caller is in silence.

G.723.1[25] Rate

Setup G.723.1 encoding rate. Default value is: 5300. Possible selections are:

- **5300:** 5.3kbps.
- **6300:** 6.3kbps.

IP TOS[26]

[25] **G.723.1 Speech Codec**
G.723.1 dual-rate speech coder performs compression and decompression of 8 kHz speech signals. It encodes 16-bit PCM samples into 16-bit code-words yielding 10 or 12 code-words per 240 sample frames for the 5.3 Kbps and 6.3 Kbps channels respectively. 60% of a phone call consists of silence. Silence Compression Scheme and Voice Activity Detection (VAD) reduce network bandwidth usage and save valuable speech resources.

Setup the priority for different classes of service. Default value is 0. For example, TOS=0xB8 means the priority is 5, requiring lower delay and higher throughput while concerns less about reliability.

T.38

T.38[27]

Set whether to invoke T.38 fax functionality. Default value is: Off.

- **On:** Enable
- **Off:** Disable

T.38 Packet Time (ms)

Set the packaging interval for each T.38 data frame. Default value is: 30. The valid rate range is: 10 ~ 60.

T.38 Redundancy[28]

Set the number of the redundancy frames in each T.38 data package. Default value is: 4. The valid number range is: 1 ~ 6.

T.38 Change Port

Set whether to change the UDP[29] port when gateway changes to T.38 function. The default value is No.

- **Yes:** Use new UDP port;
- **No:** Use the RTP port established during the initial connection.

T.38 ECM Mode

Select On or Off to indicate whether to invoke T.38 error detection mode. Default value is: Off.

[26] **TOS (Type of Service)**
TOS has 8 bits reserved to the service type in the IP datagram. 0-2 means precedence. 6-7 are unused. 3-5 means D (requests low delay), T (requests high throughput), R (requests high reliability), respectively.

[27] **T.38 Real time Fax Across IP networks**
T.38 is an ITU-T Recommendation. T.38 describes the technical features necessary to transfer facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. The Recommendation allows the use of either TCP or UDP depending on the service environment.

[28] **Redundancy Frame**
Redundancy frame is used to ensure more reliable fax transmissions than that of RTP voice transmission.

[29] **UDP Port**
Port has two meanings in network technology. One is the physical port, via which other equipments can be connected. The other is the logical port, interfacing with different network protocols. Logical port can be of two types as well, depending what protocols we are talking about. One is TCP port, the other is UDP port. UDP port is a protocol port for data packages. No connection between client and server is required to use this port.

- **On:** Enable error detection mode. When error occurs and is detected, gateway automatically re-sends fax.
- **Off:** Disable error detection mode.

V.21[30] Dective

Setup whether to enable V.21 fax error detection. Default value is: On.

Note: It is not necessary to enable V.21 if fax machine can send normal signals. Set this parameter to Off to reduce DSP processing load.

- **On:** Enable
- **Off:** Disabled

T.38 NSF[31] Modify

Setup whether to shield from non-standard fax transmission. Default value is: On. Recommendation:Set it to on.

- **On:** Shield from non-standard transmission.
- **Off:** Not shield from non-standard transmission.

T.38 Jitter Size[32]

Setup T.38 jitter buffer value. Default value is 250ms. Valid value range is 40 ~ 1000.

T.38 Receive Gain[33]

This sets the T.38 receiving gain value. Default value is 1. Valid range is 0 ~ 4.

- **Values 0 and 1:** mean -6dB and -3dB enhancement, respectively.

[30] **V.21**
V.21 is an ITU-T recommendation for full-duplex communication between two analogue dial-up modems using audio frequency-shift keying modulation at 300 bauds to carry digital data at 300 bit/s. If fax machine doesn't get any fax signal, the gateway can detect any fax signal throughV.21.

[31] **NSF（Non-Standard facilities）**
Non-standard fax facilities are those whose operation features are not defined by ITU. Some of those features are encoded in FIF but their encoding method was not defined.

[32] **Jitter Buffer**
Jitter is a major factor affecting the quality of IP calls. Jitter buffer is a software process that eliminates jitter caused by transmission delays in Internet telephony (VoIP) network. As the jitter buffer receives voice packets, it adds small amounts of delay to the packets so that all of the packets appear to have been received without delays. Voice signals are sequential by nature (i.e., they must be played back in the order in which they were sent) and the jitter buffer ensures that the received packets are in the correct order. Without a jitter buffer to smooth the transmission, data can be lost, resulting in choppy audio signals. There are two types of jitter buffers - dynamic and static. A static jitter buffer is hardware-based and configured by the manufacturer. A software-based jitter buffer is called a dynamic jitter buffer and can be configured by the system or network administrator.

[33] **Signal Gain**
When detected signals are not strong enough over the network, we use signal gain parameter to increase the strength of the signal.

- **Value 2:** means 0dB gain.
- **Values 3 and 4:** means 3dB and 6dB enhancements, respectively.

T.38 Send Gain

This field sets the T.38 sending gain value. Default value is 2. Valid range is 0 ~ 4.

- **Values 0 and 1:** mean -6dB and -3dB increment, respectively;
- **Value 2:** means 0dB increment.
- **Values 3:** and 4 mean 3dB and 6dB increment, respectively.

SIP Config

SIP divides the communications between the Server and the User Agent into two types: Request Line and Status Line. Both messages include a message header and a SIP payload. Header indicates the sender, the receiver, hops to route, etc., while payload describes the method to complete the session. Line feeds are used to separate commands and parameters.

Request Line

SIP message sent from agent to server to initiate the session, including INVITE, ACK, BYE, CANCEL, OPTION, and UPDATE.

- **Message header:** Call-id;
- **Parameters lines:** Via, From, To, Contact, Csq, Content-length, Max-forward, Content-type, White Space, SDP, etc.

Status Line (Response Line)

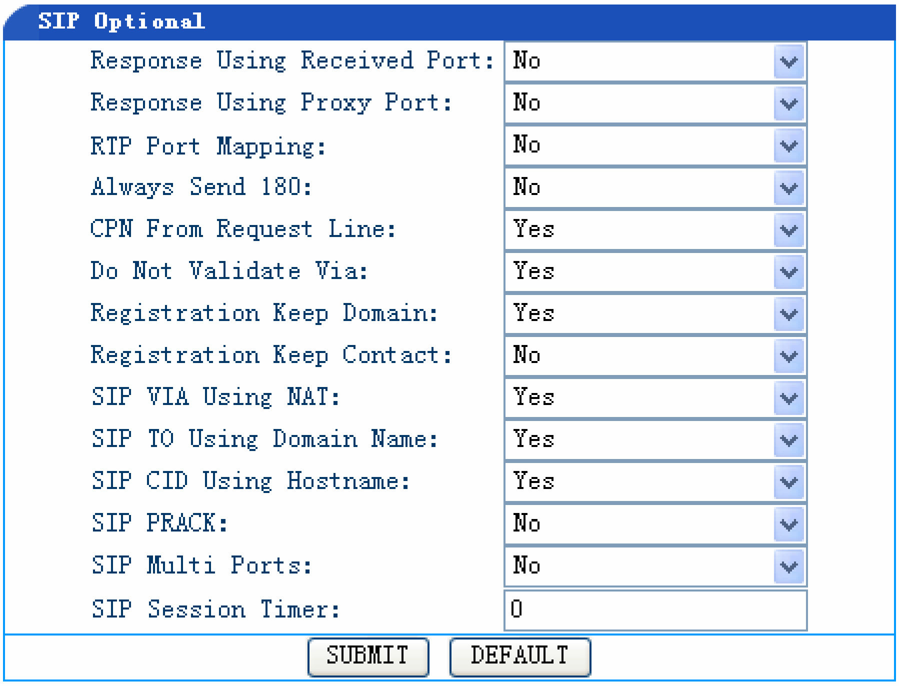
SIP messages representing the processing results to the request, including 1xx, 2xx, 3xx, 4xx, 5xx, 6xx responses.

- **Message header:** Call-id;
- **Parameters lines:** Via, From, To, Contact, Csq, Content-length, Max-forward, Content-type, White Space, SDP, etc.

The following section details server and call agent SIP communication parameters for the iMX100-AG Gateway Series.

Once logged in, click **Advanced Config > SIP Config**. The following displays:

📖 **Note:** For information on how to use Submit and Default, see most used buttons.



SIP Optional

Response Using Received Port:	No
Response Using Proxy Port:	No
RTP Port Mapping:	No
Always Send 180:	No
CPN From Request Line:	Yes
Do Not Validate Via:	Yes
Registration Keep Domain:	Yes
Registration Keep Contact:	No
SIP VIA Using NAT:	Yes
SIP TO Using Domain Name:	Yes
SIP CID Using Hostname:	Yes
SIP PRACK:	No
SIP Multi Ports:	No
SIP Session Timer:	0

Figure 0-16: Advanced SIP config

Response Using Received Port

Set whether to extract from received SIP message the received port and use it as responding port. Default value is No.

- **Yes:** Use the received port as responding port.
- **No:** Use SIP proxy port set on this gateway as responding port.

Response Using Proxy Port

Set whether to use SIP proxy port as the responding port. Default value is No.

- **Yes:** Use SIP proxy port as port for responding.
- **No:** Use default port of 5060 as responding port.

RTP Port Mapping

Set whether to enable RTP port mapping. Default value is No.

- **Yes:** Enable RTP port mapping and use local RTP port.
- **No:** Disable RTP port mapping function. Use port from STUN request.

Always Send 180

Set whether to replace 18x with 180 when gateway response to agent. Default value is No.

- **Yes:** Still sending 180 when gateway was asked to send 18x.
- **No:** Send 18x.

CPN from Request Line

Set whether to obtain CPN from Request Line. Default value is No.

- **Yes:** Obtain CPN from Request Line.
- **No:** Obtain CPN from TO field.

Do Not Validate Via

Set whether to check via[34] portion of the message when responding. Default value is: Yes.

- **Yes:** Ignore via portion when responding.
- **No:** Check via portion when responding.

Registration Keep Domain

This only applies when gateway uses a domain name string. Default value is: Yes.

- **Yes:** Use fully qualified domain for registration (FQD, i.e., 8801@registrar.newrock.com)
- **No:** Use only common portion of the domain name to register, i.e., 8801@newrock.com.

Registration Keep Contact

This only applies when the gateway is used to register through private networks. Default value is No.

- **Yes:** Keep original contact info when registering.
- **No:** Use NAT[35] info turned from registration server.

SIP VIA Using NAT

Set to use public or private network info obtained from NAT in SIP VIA53 message. Default value is Yes.

- **Yes:** SIP VIA uses NAT53 address.
- **No:** Use gateway local address.

[34] **Via**
Via indicates path of route request. Via portion explains origin, route request time, route destination, and port. For example, R 128.200.10.0/24 [120/1] via 128.200.1.1, 00:00:17, ethernet0/0.

[35] **NAT（Network Address Translator or Translation）**
Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

SIP TO Using Domain Name

Set whether to use the value from SIP config > SIP Proxy in the TO field of SIP message, or use the value from SIP config **> Domain Name.** Default value is Yes.

- **Yes:** SIP TO use domain name specified in SIP config **> Domain Name.**
- **No:** Use the address specified in SIP Proxy, or use address specified in SIP config **> Proxy.**

SIP CID Using Hostname

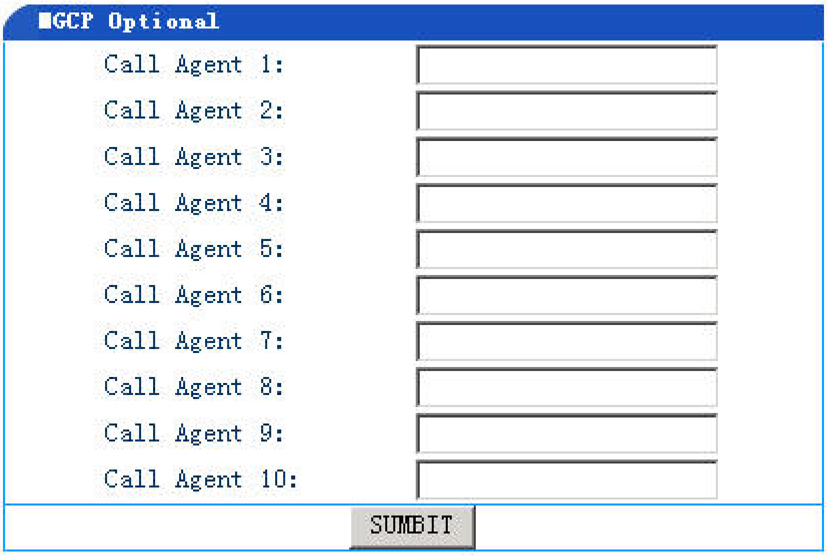
Set whether Call ID in SIP message to use server host name or to use IP address. Default value is No.

- **Yes:** Use host name.
- **No:** Use an IP address.

MGCP Config

Click **Advanced Config > MGCP Config** from the left pane. The following displays:

Note: For information on how to use Submit and Default, see most used buttons.



MGCP Optional

Call Agent 1:	
Call Agent 2:	
Call Agent 3:	
Call Agent 4:	
Call Agent 5:	
Call Agent 6:	
Call Agent 7:	
Call Agent 8:	
Call Agent 9:	
Call Agent 10:	

Figure 0-17: Advanced MGCP Settings

Call Agent 1~10

Set call agent IP address and port number of MGCP. No default value.

- Use “:” between IP address and port number.

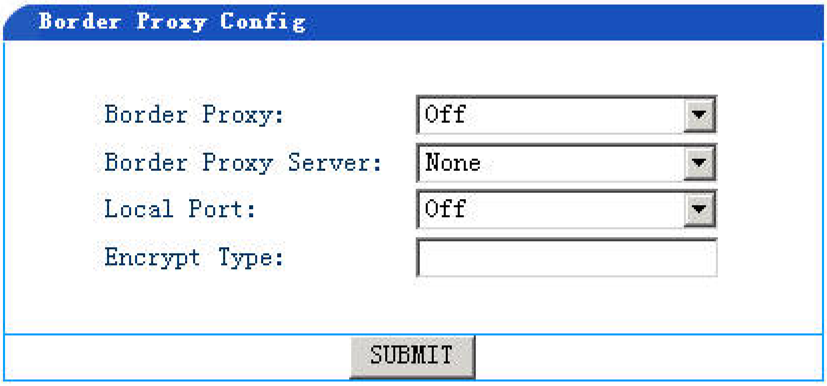
- Address can be either IP address or domain name. If using domain name, the user must set DNS server parameters in Network Settings page and enable the DNS service.
- Sample format of fully qualified addresses: 202.202.2.202:2727; callagent.com:2727.

Border Proxy Config

To connect to user agents, we also need to gather information about border agent, registration server, and local network domain name and IP address. Customer can be in different locations, and settings are all depending on their locations and local networks.

Click Advanced **Options > Border Proxy Config** from the left pane. The following displays:

Note: For information on how to use Submit, see most used buttons.



Border Proxy Config

Border Proxy: Off

Border Proxy Server: None

Local Port: Off

Encrypt Type:

Figure 0-18: Border Agent Settings

Border Proxy[36]

Set whether signaling and RTP are using a border agent. Default value is None. Possible settings are: None, Signaling, Signaling and RTP.

- **None:** Do not use border agent.
- **Signaling:** Only Signaling is going to use border agent.
- **Signaling and RTP:** Both Signaling and RTP stream are using border agent.

Border Proxy Server

[36] **Border Agent:** Also known as Border Controller, which normally includes Sign Proxy and Media Proxy function modules.

Set IP address and port number for border agent. No default value. Separate IP address and port number with a ":".

Local Port

Local port number for border agent. Default value is: 4660. Local port number can be anything, as long as it does not conflict with port numbers for other equipments.

Encrypt type

Set encryption method. Default value is: None.

Note: Encryption setting must be the same with what the border agent is using. Possible options are:

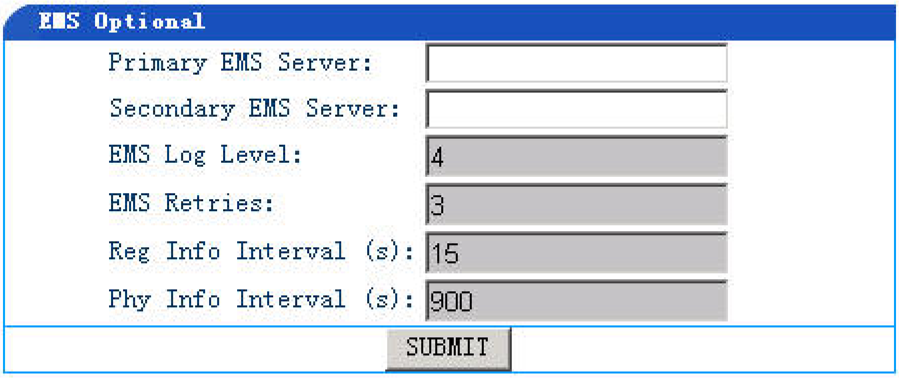
- **None:** TCP encryption, HTTPU mode. No encryption algorithm is used.
- **Encrypted:** TCP encryption, HTTPU mode. Encryption algorithm is used.
- **TCP Encrypted:** Encrypt signaling and RTP over TCP. Also use encryption algorithm.
- **TCP Not Encrypted:** Encrypt signaling and RTP over TCP, but no encryption algorithm is used.
- **UDP Not Encrypted:** Encrypt signaling and RTP over UDP, but no encryption algorithm is used.
- **UDP Encrypted:** UDP encryption. Also use encryption algorithm.
- **Using Keyword:** UDP encryption using backward keyword encryption algorithm
- **Using Keyword2:** UDP encryption using forward keyword encryption algorithm.
- **RC4**[37]: Using RC4 encryption algorithm.

EMS Config

After log in, click **Advanced Config > EMS Config** from the left pane. The following displays:

Note: For information on how to use Submit, see most used buttons.

[37] **RC4**
The RC4 encryption algorithm is stream cipher, which can use variable length keys. The algorithm was developed by Ron Rivest, for RSA Data security. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10^{100}. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure.



EMS Optional

Primary EMS Server:	
Secondary EMS Server:	
EMS Log Level:	4
EMS Retries:	3
Reg Info Interval (s):	15
Phy Info Interval (s):	900

Figure 0-19: Advanced EMS Settings

Primary EMS Server

Enter primary EMS Server IP address if you want to use EMS service.

Secondary EMS Server

Enter secondary EMS server IP address.

EMS Log Level

EMS Retries

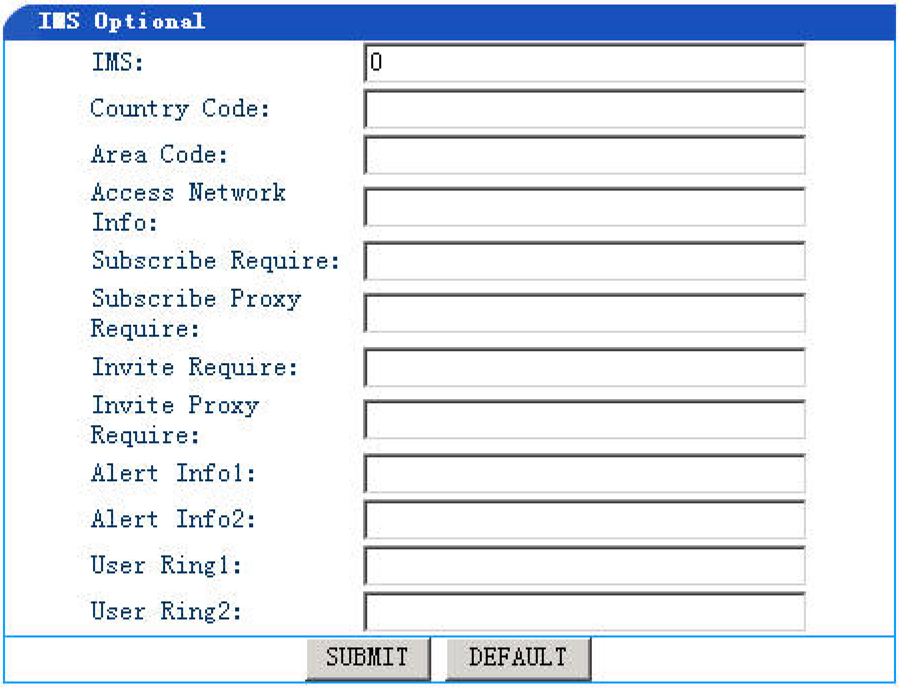
Reg Info Interval(s)

Phy Info Interval(s)

IMS Options

Especially Declare: This Option just is suitable to iMX100-AG 1.9.3 Series.

Click the Advance Config link on the left side of Figure 0-1. Then click IMS Config. The IMS Optional screen displays:



IMS Optional

IMS:	0
Country Code:	
Area Code:	
Access Network Info:	
Subscribe Require:	
Subscribe Proxy Require:	
Invite Require:	
Invite Proxy Require:	
Alert Info1:	
Alert Info2:	
User Ring1:	
User Ring2:	

Figure 0-24 IMSOptional screen

IMS

Set number **1** (enable) or number **0** (disable). When IMS is disabled, SIP messages flows and formats are compliant with RFC 3261; when IMS is enabled SIP message flows and formats are compliant with IMS/TISPAN.

Country Code

In **Country Code** field, if the Country Code and the Area Code are entered, the From and Contact info in INVITE will display “Country Code + Area Code +xxxx”(for example：enter 86 in Country Code field and enter 021 in Area Code field, then the From and Contact info will show: +8621xxxx).

Area Code

In **Area Code** field, if just the Area Code is entered, the From and Contact info in INVITE will display “Area Code +xxxx” (for example：enter 021, then the From and Contact info: 021xxxx).

Access Network Info

In **Access Network Info** field, enter access network information. It will be carried into REGISTER/INVITE message’s P-Access-network-info header.

Subscribe Require

In **Subscribe Require** field, enter the Require info, the value will be carried into the head info of SUBSCRIBE message.

Subscribe Proxy Require

In **Subscribe Proxy Require** field, enter the Proxy Require info, the value will be carried into the head info of SUBSCRIBE message.

Invite Require

In **Invite Require** field, enter Require info, the value will be carried into the head info of IINVITE message.

Invite Proxy Require

In **Invite Proxy Require** field, enter Proxy Require info, the value will be carried into the head info of INVITE message.

Alert Info1

In **Alert Info1** field, enter Alert-info value1 into INVITE message. This field is used for “Distinctive Ringing” service. Two ringing patterns are supported by iMX100. When the string in Alert-info of received INVITE matches this parameter, the ringing pattern defined in User Ring1 (See below) will be applied to the line.

Alert Info2

In **Alert Info2** field, enter Alert-info value2 into INVITE message. This parameter corresponds to **User Ring2** field. When the string in Alert-info of received INVITE matches this parameter, the ringing pattern defined in User Ring2 (See below) will be applied to the line.

User Ring1

Set the ringing mode1. Note: this parameter corresponds to **Alert Info1** field. For example:

- USER_RING1 = 2,500,500,1000,3000
  Definition:
  2 periods,0.5s ringing,0.5s stop,1s ringing, 3s stop.
- USER_RING2 = 1, 2000,4000
  Definition: 1 period, 2s ringing, 4s stop.

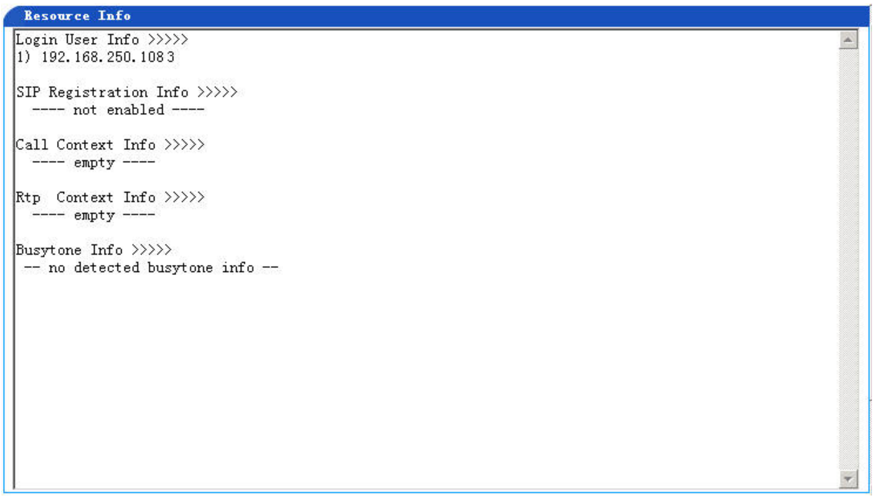
User Ring2

Set the ringing mode2. Note: this parameter corresponds to **Alert Info2** field.

Log Info

Resource Info

After login, click **Log Info > Resources Info** from left pane. The following displays:



Resource Info

```
Login User Info >>>>>
1) 192.168.250.108 3

SIP Registration Info >>>>>
  ---- not enabled ----

Call Context Info >>>>>
  ---- empty ----

Rtp  Context Info >>>>>
  ---- empty ----

Busytone Info >>>>>
 -- no detected busytone info --
```

*Figure 0-20: **Resource Information***

All information can be viewed on this page. User Info shows user IP address and login level, SIP registration information, calling information, and related RTP information.

Login User Info

This information indicates login user's status:

- It shows multiple IP addresses if more than one IP addresses are logged in. The number right after the IP can be either 1 or 3, with 1 being the administrator.
- When more than one IP log in, the first one will be 1, and rest will all be 3.
- Operator login will be level 3. Level 3 users can only view, but not to change, system settings.

For Example:

```
Login User Info >>>>>
1） 192.168.2.247    1
```

SIP Registration Information

This information provides registration status on the system.

- Not enabled: No FXS or FXO registered.
- Latest response: The latest registration response. 200 is the typical response of OK.
- No response: Check if the registration server is on or if it is reachable, etc.

For Example:

```
SIP Registration Info >>>>>
 ---- Not enabled ----
SIP Registration Info >>>>>
Contact: <sip:2681403@220.248.27.70:1003;user=phone>
       latest response: 200 （timeout-555）
Contact: <sip:2681402@220.248.27.70:1003;user=phone>
       latest response: 200 （timeout-555）
```

Call Context Info

This information shows the current calling status of the system.

RTP Context Info

This information indicates the voice channel of the RTP stream.

For Example:

```
RTP Context Info >>>>>
3） created,   call =e011
```

If this is an iMX100-AG with FXO ports, information will also show if the FXO port is busy or not.

Busytone Info

This information indicates the FXO busytone status of the gateway,

From Advanced Config **> Advanced FXO Settings,** click the **Busy Tone** button, you will see as the following:

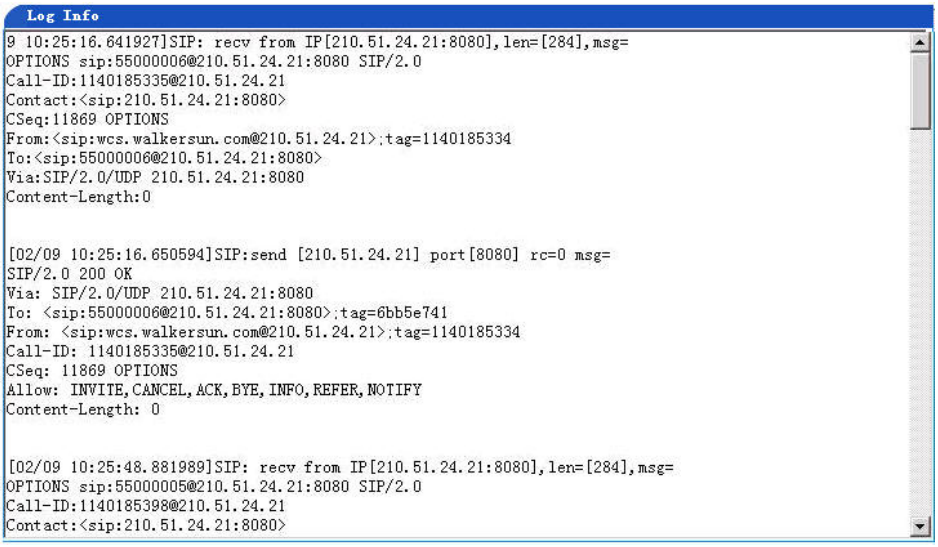
For Example:

```
Busytone Info >>>>>
-- Detect busytone in progress --
```

Now if you call from an FXO, resource log (Figure 5-23) will show Detect busytone in progress. When you hang up, it will show detected busy tone, single channel or dual channel, as well as the on/off time.

Message Log

After login, click **System Tools > Message Log** from the left pane. The following displays. It displays signaling messages from this gateway. Please see RFC documentation for standard SIP message definitions.

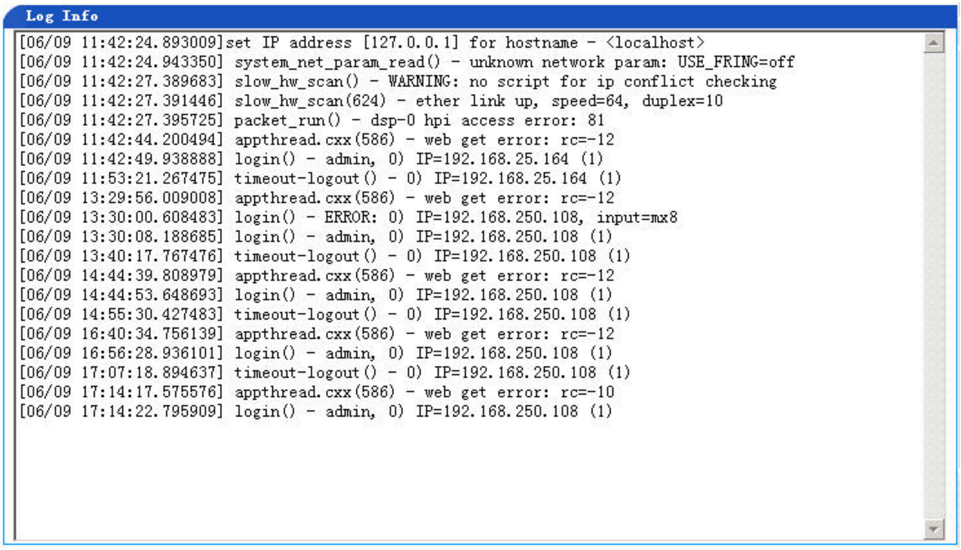


```
9 10:25:16.641927]SIP: recv from IP[210.51.24.21:8080],len=[284],msg=
OPTIONS sip:55000006@210.51.24.21:8080 SIP/2.0
Call-ID:1140185335@210.51.24.21
Contact:<sip:210.51.24.21:8080>
CSeq:11869 OPTIONS
From:<sip:wcs.walkersun.com@210.51.24.21>;tag=1140185334
To:<sip:55000006@210.51.24.21:8080>
Via:SIP/2.0/UDP 210.51.24.21:8080
Content-Length:0


[02/09 10:25:16.650594]SIP:send [210.51.24.21] port[8080] rc=0 msg=
SIP/2.0 200 OK
Via: SIP/2.0/UDP 210.51.24.21:8080
To: <sip:55000006@210.51.24.21:8080>;tag=6bb5e741
From: <sip:wcs.walkersun.com@210.51.24.21>;tag=1140185334
Call-ID: 1140185335@210.51.24.21
CSeq: 11869 OPTIONS
Allow: INVITE,CANCEL,ACK,BYE,INFO,REFER,NOTIFY
Content-Length: 0


[02/09 10:25:48.881989]SIP: recv from IP[210.51.24.21:8080],len=[284],msg=
OPTIONS sip:55000005@210.51.24.21:8080 SIP/2.0
Call-ID:1140185398@210.51.24.21
Contact:<sip:210.51.24.21:8080>
```

Figure 0-21: Viewing Calling Log

Error Info Log

After login, click **System Tools > Error Logs** from left pane. The following displays:



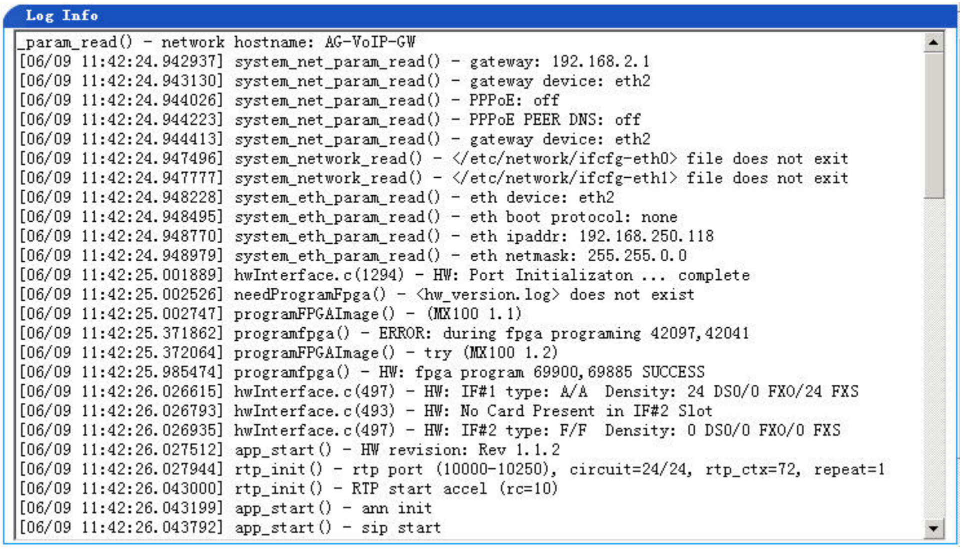
```
[06/09 11:42:24.893009]set IP address [127.0.0.1] for hostname - <localhost>
[06/09 11:42:24.943350] system_net_param_read() - unknown network param: USE_FRING=off
[06/09 11:42:27.389683] slow_hw_scan() - WARNING: no script for ip conflict checking
[06/09 11:42:27.391446] slow_hw_scan(624) - ether link up, speed=64, duplex=10
[06/09 11:42:27.395725] packet_run() - dsp-0 hpi access error: 81
[06/09 11:42:44.200494] appthread.cxx(586) - web get error: rc=-12
[06/09 11:42:49.938888] login() - admin, 0) IP=192.168.25.164 (1)
[06/09 11:53:21.267475] timeout-logout() - 0) IP=192.168.25.164 (1)
[06/09 13:29:56.009008] appthread.cxx(586) - web get error: rc=-12
[06/09 13:30:00.608483] login() - ERROR: 0) IP=192.168.250.108, input=mx8
[06/09 13:30:08.188685] login() - admin, 0) IP=192.168.250.108 (1)
[06/09 13:40:17.767476] timeout-logout() - 0) IP=192.168.250.108 (1)
[06/09 14:44:39.808979] appthread.cxx(586) - web get error: rc=-12
[06/09 14:44:53.648693] login() - admin, 0) IP=192.168.250.108 (1)
[06/09 14:55:30.427483] timeout-logout() - 0) IP=192.168.250.108 (1)
[06/09 16:40:34.756139] appthread.cxx(586) - web get error: rc=-12
[06/09 16:56:28.936101] login() - admin, 0) IP=192.168.250.108 (1)
[06/09 17:07:18.894637] timeout-logout() - 0) IP=192.168.250.108 (1)
[06/09 17:14:17.575576] appthread.cxx(586) - web get error: rc=-10
[06/09 17:14:22.795909] login() - admin, 0) IP=192.168.250.108 (1)
```

Figure 0-22: View Error Log Window

This log shows all errors, as well as login, logout, and timeout info about the users.

Startup Info

After login, click **System Tools > Startup Info** from the left pane. The following displays:



```
_param_read() - network hostname: AG-VoIP-GW
[06/09 11:42:24.942937] system_net_param_read() - gateway: 192.168.2.1
[06/09 11:42:24.943130] system_net_param_read() - gateway device: eth2
[06/09 11:42:24.944026] system_net_param_read() - PPPoE: off
[06/09 11:42:24.944223] system_net_param_read() - PPPoE PEER DNS: off
[06/09 11:42:24.944413] system_net_param_read() - gateway device: eth2
[06/09 11:42:24.947496] system_network_read() - </etc/network/ifcfg-eth0> file does not exit
[06/09 11:42:24.947777] system_network_read() - </etc/network/ifcfg-eth1> file does not exit
[06/09 11:42:24.948228] system_eth_param_read() - eth device: eth2
[06/09 11:42:24.948495] system_eth_param_read() - eth boot protocol: none
[06/09 11:42:24.948770] system_eth_param_read() - eth ipaddr: 192.168.250.118
[06/09 11:42:24.948979] system_eth_param_read() - eth netmask: 255.255.0.0
[06/09 11:42:25.001889] hwInterface.c(1294) - HW: Port Initializaton ... complete
[06/09 11:42:25.002526] needProgramFpga() - <hw_version.log> does not exist
[06/09 11:42:25.002747] programFPGAImage() - (MX100 1.1)
[06/09 11:42:25.371862] programfpga() - ERROR: during fpga programing 42097,42041
[06/09 11:42:25.372064] programFPGAImage() - try (MX100 1.2)
[06/09 11:42:25.985474] programfpga() - HW: fpga program 69900,69885 SUCCESS
[06/09 11:42:26.026615] hwInterface.c(497) - HW: IF#1 type: A/A  Density: 24 DS0/0 FXO/24 FXS
[06/09 11:42:26.026793] hwInterface.c(493) - HW: No Card Present in IF#2 Slot
[06/09 11:42:26.026935] hwInterface.c(497) - HW: IF#2 type: F/F  Density: 0 DS0/0 FXO/0 FXS
[06/09 11:42:26.027512] app_start() - HW revision: Rev 1.1.2
[06/09 11:42:26.027944] rtp_init() - rtp port (10000-10250), circuit=24/24, rtp_ctx=72, repeat=1
[06/09 11:42:26.043000] rtp_init() - RTP start accel (rc=10)
[06/09 11:42:26.043199] app_start() - ann init
[06/09 11:42:26.043792] app_start() - sip start
```

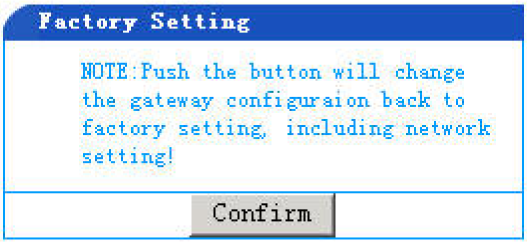
Figure 0-23: Startup info

All startup info and settings for the gateway are listed here.

System Tools

Factory Config

After login, click **System Tools > Factory Config** from the left pane. The following displays:



NOTE:Push the button will change the gateway configuraion back to factory setting, including network setting!

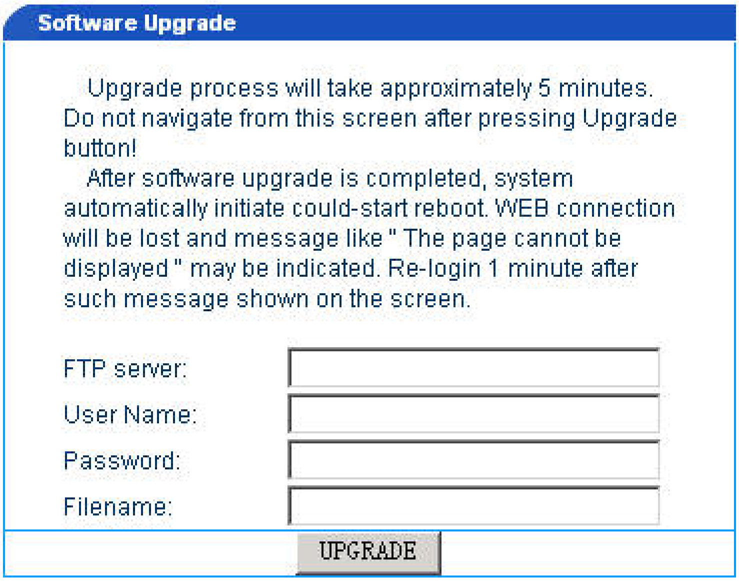
Figure 0-24: Restore Factory Default

Click the Confirm button to restore default factory settings.

iMX100-AG Gateway has most parameters set to commonly used default value. In most cases, customers do not have to set the parameters for themselves. See Index for details about factory default settings.

Software Update

After login, click **System Tools > Software Update** from the left pane. The following displays:



Software Upgrade

Upgrade process will take approximately 5 minutes. Do not navigate from this screen after pressing Upgrade button!

After software upgrade is completed, system automatically initiate could-start reboot. WEB connection will be lost and message like " The page cannot be displayed " may be indicated. Re-login 1 minute after such message shown on the screen.

FTP server:	
User Name:	
Password:	
Filename:	

Figure 0-25: Software Upgrade

FTP Server

IP address of FTP server from which you get the new software. No default value is shown.

User Name

Username to logon to the FTP server

Password

Password to logon to the FTP server

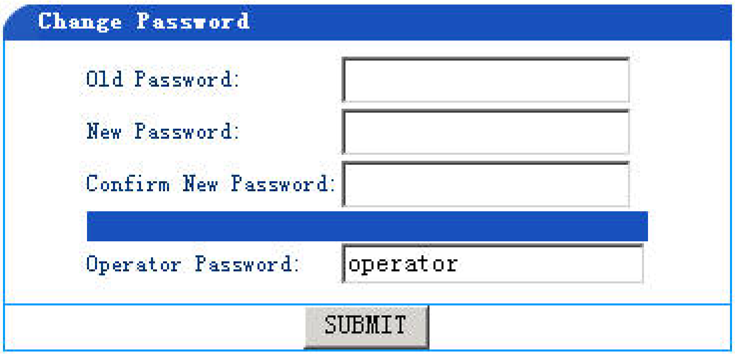
Filename

Enter absolute file path on the FTP server and the file name. No default Value is shown. The file extension must be .tar.

Note: No operation is permitted during software upgrade! The Reboot window will pop up when update is successful. Click the OK button and you will see a Reboot page. After clicking the Reboot button, please recycle the power manually to restart the gateway.

Change Passwd

After login, click **System Tools > Change Passwd** from the left pane. The following displays:



Change Password

Old Password:

New Password:

Confirm New Password:

Operator Password: operator

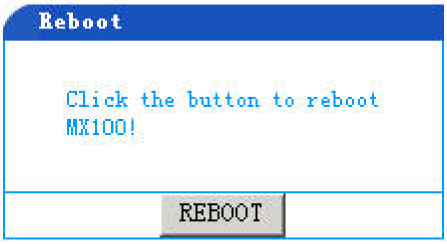
Figure 0-26: Change Password

Only an administrator has the authority to change password. The first three fields are used to change administrator password. Enter old password in the Old password field. Enter new password in the New password field. Enter the new password again in Confirm new password field. Click the Submit button to finish.

Operator's password is shown as clear text. Administrator can change it at any time. It is not necessary to enter administrator's password to change operator's password. Enter new password in the operator password field and click submit button to finish.

Reboot the Gateway

After login, click **System Tools > Reboot** from left pane. The following displays:



Reboot

Click the button to reboot MX100!

Figure 0-27: Reboot the Gateway

Click Reboot button to reboot the gateway.

Help

After login, click **System Tools > Help** from left pane. The following displays:

MX100 User Guide

http://www.newrocktech.com.cn

Figure 0-28: ***Help Info***

Launch the website as shown to get more help.

Exit

When logged in, click Logout link from left pane to exit the Web interface. You will return to the login screen.

6

APPENDIX

Factory Default Settings

System Settings

Item	Factory Setting	Default Value
Software Version	*	
Hardware Version	*	
DSP Version	*	
RTP Port Min	10000	No default value, must be set
RTP Port Max	10250	No default value, must be set
First Digit Timeout (s)	12	12
Inter Digit Timeout (s)	12	12
Critical Digit Timeout (s)	5	5
DTMF Method	Audio	Audio
Default Codec	iLBC/30, G729A/20 , G723/30, PCMU/20, PCMA/20, GSM/20	iLBC/30, G729A/20, G723/30, PCMU/20, PCMA/20, GSM/20
Echo Cancellation	On	On

Note: * indicates a craft read-only, system recognizable parameter.

Network Settings

Item	Factory Setting	Default Value
Host Name	iMX100-AG-VoIP-AG	iMX100-AG-VoIP-AG
Logical IP address	*	
Gateway IP address	192.168.2.1	No default value, must be set
Ethernet 1 IP address	No	No
Ethernet 1 Subnet Mask	No	No
Ethernet 1 Hardware adds.	*	
Ethernet 3 IP address	192.168.2.240	192.168.2.240
Ethernet 3 Subnet Mask	255.255.0.0	255.255.0.0
Ethernet 3 Hardware adds.	*	
DNS		
DNS	host: files	No default value, must be set
Primary DNS Server	No	If start DNS service, must be set

Item	Factory Setting	Default Value
Secondary DNS Server	No	If start DNS service, must be set
TIME		
Primary TIME Server	192.43.244.18	No default value, must be set
Secondary TIME Server	192.43.22.240	No default value, must be set
Overtime (min.)	10	No default value, must be set
Request Interval (min)	10	No default value, must be set

Note: * indicates a craft read-only, system recognizable parameter.

MGCP Settings

Item	Factory Settings	Default Value
MGCP Port	2427	2427
Call Agent	No	No
Domain Name	No	No
Default Packages	L,D,G	No default value, must be set
Persistent Line Event	L/HD,L/HU	No default value, must be set
Partial Wildcard	No	No
All Wildcard	No	No
End-of-Line Using CR	No	No
Quarantine Default to Loop	No	No
Default Package Don't Send Name	No	No
Always Enable 1st Digit Timeout	No	No
On-hook Delete Connection	No	No
Notify Instead of 401/402	No	No
Using L Package Handle FXO	No	No

SIP config

Item	Factory Settings	Default Value
Local Port	5060	5060
Proxy Server	No	No
Registration Server	No	No
Registration Expires	3600	No default value, must be setup
Domain Name	No	No
Registration	0	0
Registration ID	No	No
Registration Password	No	No

1st/2nd Card

Phone Number Settings

Item	Factory Settings	Default Value
Hardware Settings	*	
Start Number	8000	No default value, must be setup
FXS 1	8000	If no start number, must be setup
FXS 2	8000	If no start number
FXS 3	8000	If no start number
FXS 4	8000	If no start number

Note: * indicates a craft read-only, system recognizable parameter.

Call Status Information

None.

FXS（1 ~ 24）

Item	Factory Settings	Default Value
Line Number	*	
Phone Number	8000	None
Registration	On	On
Display Name	None	None
Password	None	None
Originating Restriction	Off	Off
Call Waiting	Off	Off
Call Holding	Off	Off
Call Forwarding	Off	Off
Caller ID	Off	Off
CID On Call Waiting	Off	Off
Anonymous Call	Off	Off
Hotline	Off	Off
Delay Hotline	Off	Off
Do No Disturb	Off	Off
Speed Dial	Off	Off
Fashion Ring	Off	Off
Collect Call Billing	Off	Off
To FXO	Off	Off
Maintenance Status	Off	Off
All Forward Number	None	None
Busy Forward Number	None	None
None Answer Forward Number	None	None
Hotline Number	None	None
Speed Dial List	None	None
Fashion Ring ID	0	0

Note: * indicates a craft read-only, system recognizable parameter.

Advanced Config

Dialing Plan Settings

None

Digit Map

None

Service Code

Item	Factory Settings	Default Value
Enable All Forward	*60	*60

Item	Factory Settings	Default Value
Disable All Forward	＃60	＃60
Enable Busy Forward	*61	*61
Disable Busy Forward	#61	#61
Enable No Answer Forward	*62	*62
Disable No Answer Forward	#62	#62
Cancel Call Waiting	*64	*64
Enable Do Not Disturb	*72	*72
Disable Do Not Disturb	#72	#72
Set Speed Dial	*74	*74
Speed Dial Prefix	**	**
Listen to IP Address Announcement	##	##
Listen to FXS number	#00	#00
Set Fashion Ring	*80	*80
Cancel Fashion Ring	#80	#80
Listen to Fashion Ring	*88	*88

Advanced System Settings

Item	Factory Settings	Default Value
System Log Server IP Address	None	None
Error Log Server IP Address	None	None
System Log local Port	None	None
Event Log Level	3	3
Country ID	0	0
Forwarding Number Mode	1	1
NAT		
NAT IP Address	None	None
NAT Refresh Timer	15	15
NAT Keep Alive	Yes	No
STUN		
STUN	Off	Off
STUN Server	Off	Off
RADIUS		
RADIUS Client Side	Off	Off
RADIUS Server Side	Off	Off
RADIUS ISDN Side	iMX100-AG does not need this parameter.	
RADIUS Start	Off	Off
RADIUS Unsuccessful Stop	Off	Off
RADIUS Parameter（1）	iMX100-AGneed not this parameter	
Primary RADIUS Server	None	None
Shared Password	None	None
Secondary RADIUS Server	None	None
Shared Password	None	None
Timeout	3	3
Number of Retries	3	3

Advanced FXO Settings

Item	Factory Settings	Default Value
Signal Enhancement to PSTN	-3.0	-3.0
Signal Enhancement to IP	0	0
Line Impedance Parameter	1	1
FXO Dial Delay	400	400
Signal Keep Alive	100	100
Signal Interval	100	100
Number of Retries	2	2
Signal Tone Frequency parameter 1	450	450
Signal Tone Frequency parameter 2	0	0
Signal Tone Alive	350	350
Signal Tone Interval	350	350

Advanced FXS Settings

Item	Factory Settings	Default Value
Signal Enhancement to Endpoint	-3.0	-3.0
Signal Enhancement to IP	0	0
Line Impedance Parameter	1	1
Forward Number Delay	0	0
Outpulsing Alive	100	100
Outpulsing Interval	100	100
Min. Hook Flash	75	75
Max Hook Flash	800	800
Off-Hook Jitter Free	50	50
Collect Call Billing Method	0	0
Reverse Signal Delay	3	3
Music on hold	Off	Off

Advanced IP Settings

Item	Factory Settings	Default Value
Jitter Buffer Max Value	50	50
Jitter Buffer Min Valeu	3	3
2833 Package Type	100	100
iLBC Capacity	97	97
RTP Event Duration	50	50
RTP Drop SID	No	No
Voice Proxy	No	No
RTP Media Function	No	No
SDP Global Connection	Yes	Yes
SDP Using NAT	No	No
VAD Activate (Silence Compression and Comfort Noise Generation)	Yes	Yes
G.723.1 Rate	5300	5300
IP TOS	0x0C	0x0C
	T.38	
T.38 Enabled	On	Off
Packet Time (Data Frame Length)	30	30

Item	Factory Settings	Default Value
Number of Redundancy Frames	4	4
Change UDP Port	No	No
ECM Mode	Off	Off
V.21 Detect	On	On
Shield NSF	On	On
Jitter Size	250	250
Receive Gain	1	1
Send Gain	2	2

Optional SIP config

Item	Factory Settings	Default Value
Response Using Received port	No	No
Response Using Proxy Port	No	No
RTP Port Mapping	No	No
Always Send 180	No	No
Always Send 183	iMX100-AG does not need this parameter.	
Using Local CODEC Configuration List	iMX100-AG does not need this parameter.	
180 with SDP	iMX100-AG does not need this parameter.	
Registration Keep Original Contact	No	No
SIP VIA Using NAT	Yes	Yes
SIP TO Using Domain Name	Yes	Yes
SIP Call ID Using Hostname	No	No

MGCP Advanced Config

None

Border Agent Settings

Item	Factory Settings	Default Value
Border Agent	None	None
Border Agent Server	None	None
Local Port	460	460
Encryption	None	None
Encryption Keyword	None	None

Advanced EMS Settings

Item	Factory Settings	Default Value
Primary EMS Server	None	None
Secondary EMS Server	None	None

Auto Provisioning Software Upgrade

None

Log Information

None

System Tools

None

Glossary

DHCP（Dynamic Host Configuration Protocol）

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to assign TCP/IP addresses to client servers. Each client server is connected to the central DHCP server, which gives the network configuration of each client, including the IP address, gateway and DNS server information.

DSP（Digital Signal Processing）

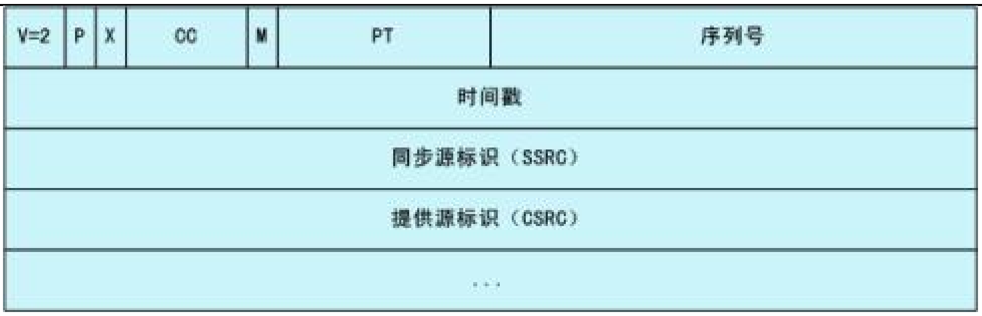
Adjust, and filtrate digital frequency.

RTP（Real-Time Transport Protocol）

RTP is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. RTP is defined as working one to one or one to more, which can provide real time. RTP usually using UDP (User Datagram Protocol) to transfer data, but RTP also works for TCP (Transmission Control Protocol) or ATM (Asynchronous Transfer Mode).There are 2 ports when a program starts a RTP communication: one for RTP and one for RTCP. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

RTP port refers to sending and receiving port.

RTP provides support for media data packetization and real time transmission. Every RTP packet consists of a Header and a Payload. The first 12 bits are RTP Fixed Header Fields. Payload can be either video or audio. Figure 0-1 shows the RTP header format.



V=2	P	X	CC	M	PT	序列号
时间戳						
同步源标识（SSRC）						
提供源标识（CSRC）						
...						

Figure 0-1: RTP Header Format

Key header fields and their meanings:

- **CSRC Count (CC)**: 4 bits. The CSRC count contains the number of CSRC identifiers that follow the fixed header. For example, one CSRC list can represent a audio conference. This call uses a RTP mixer to combine audios of all callers into an RTP data stream.
- **Payload Type (PT):** 7 bits. Indicates payload format, including codec, clock rate, channel, etc. For example, type 2 indicates payload in this packet is using ITU G721 codec, sample rate is 8000Hz and using single channel.
- **Sequence Number:** 16 bits. The sequence number is mainly used to detect losses. RTP does not try to re-transmit for detected losses. It's up the application to handle lost packets.
- **Time Stamp:** 32 bits. The timestamp is used to place the incoming audio and video packets in the correct timing order (playout delay compensation). The sequence number is mainly used to detect losses. Sequence numbers increase by one for each RTP packet transmitted, timestamps increase by the time "covered" by a packet. For video formats where a video frame is split across several RTP packets, several packets may have the same timestamp. In some cases such as carrying DTMF (touch tone) data (RFC 2833), RTP timestamps may not be monotonic.

DTMF（Dual Tone Multi-Frequency）

In PSTN service, after a call is connected, user's touch tone info is transmitted via DTMF, also known as second dial tone information. It is widely used in intelligent network and value-added services.

- Audio: Voice data transparent transmit mode.
- 2833: A special RTP packet. PT field of the header indicates this is a DTMF packet. See FTC 2833 for details.
- INFO: Information transmission mode. Optional way of DTMF transmission. As in SIP messages, use INFO to indicate a DTMF signal.

Speech CODEC

Also called a "voice codec" or "vocoder," it is a hardware circuit that converts the spoken word into digital code and vice versa. It comprises the A/D and D/A conversion and compression technique. If music is encoded with a speech codec, it will not sound as good when decoded at the other end. A speech codec is an audio codec designed for human voice. By analyzing vocal tract sounds, a recipe for rebuilding the sound at the other end is sent rather than the soundwaves themselves. The speech codec is able to achieve a much higher compression ratio, which results in a smaller amount of digital data for transmission. When telephones were first digitized in the early 1960s, they generated digital streams of 64 Kbps. Since then, speech CODECS have reduced voice to as little as 5 Kbps and less.

Echo Cancellation

The term echo cancellation is used in telephony to describe the process of removing echo from a voice communication in order to improve voice quality on a telephone call. In addition to improving quality, this process improves bandwidth savings achieved through silence suppression by preventing echo from traveling across a network.

There are two types of echo of relevance in telephony: acoustic echo and hybrid echo. Speech compression techniques and digital processing delay often contribute to echo generation in telephone networks. Echo cancellation involves first recognizing the originally transmitted signal that re-appears, with some delay, in the transmitted or received signal. Once the echo is recognized, it can be removed by 'subtracting' it from the transmitted or received signal.

This technique is generally implemented using a digital signal processor (DSP), but can also be implemented in software. Echo cancellation is done using either echo suppressors or echo cancellers.

MGCP (Media Gateway Control Protocol)

Media Gateway Control Protocol (MGCP) is used for controlling telephony gateways from external call control elements called media gateway controllers or call agents. A telephony gateway is a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks.

MGCP assumes a call control architecture where the call control intelligence is outside the gateways and handled by external call control elements. The MGCP assumes that these call control elements, or Call Agents, will synchronize with each other to send coherent commands to the gateways under their control. MGCP is, in essence, a master/slave protocol, where the gateways are expected to execute commands sent by the Call Agents.

The MGCP implements the media gateway control interface as a set of transactions. The transactions are composed of a command and a mandatory response. There are nine types of commands:

MGCP Commands (MGC=Media Gateway Controller; MG=Media Gateway)

MGC --> MG CreateConnection: Creates a connection between two endpoints; uses SDP to define the receive capabilities of the participating endpoints.

MGC --> MG ModifyConnection: Modifies the properties of a connection; has nearly the same parameters as the CreateConnection command.

MGC <--> MG DeleteConnection: Terminates a connection and collects statistics on the execution of the connection.

MGC --> MG NotificationRequest: Requests the media gateway to send notifications on the occurrence of specified events in an endpoint.

MGC <-- MG Notify: Informs the media gateway controller when observed events occur.

MGC --> MG AuditEndpoint: Determines the status of an endpoint.

MGC --> MG AuditConnection: Retrieves the parameters related to a connection.

MGC <-- MG RestartInProgress: Signals that an endpoint or group of endpoints is taking in or out of service.

MGC --> MG: Endpoint Configuration

The first four commands are sent by the Call Agent to a gateway. The Notify command is sent by the gateway to the Call Agent. The gateway may also send a DeleteConnection. The Call Agent may send either of the Audit commands to the gateway. The Gateway may send a RestartInProgress command to the Call Agent.

All commands are composed of a command header, optionally followed by a session description. All responses are composed of a response header, optionally followed by a session description. Headers and session descriptions are encoded as a set of text lines, separated by a carriage return and line feed character (or, optionally, a single line-feed character). The headers are separated from the session description by an empty line.

MGCP uses a transaction identifier to correlate commands and responses. Transaction identifiers have values between 1 and 999999999. An MGCP entity cannot reuse a transaction identifier sooner than 3 minutes after completion of the previous command in which the identifier was used.

The command header is composed of:

- A command line, identifying the requested action or verb, the transaction identifier, the endpoint towards which the action is requested, and the MGCP protocol version,
- A set of parameter lines, composed of a parameter name followed by a parameter value.

The command line is composed of:

- Name of the requested verb.
- Transaction identifier correlates commands and responses. Values may be between 1 and 999999999. An MGCP entity cannot reuse a transaction identifier sooner than 3 minutes after completion of the previous command in which the identifier was used.
- Name of the endpoint that should execute the command (in notifications, the name of the endpoint that is issuing the notification).
- Protocol version.

These four items are encoded as strings of printable ASCII characters, separated by white spaces, i.e., the ASCII space (0x20) or tabulation (0x09) characters. It is recommended to use exactly one ASCII space separator.

MGCP Call Agent

Call Agent, also known as Media Gateway Controller, controls the Media Gateway. In MGCP, a call agent primarily handles all the call processing by linking with the IP network through constant communications with an IP signaling device, for example an SIP Server or an H.323 gatekeeper.

Call Agent is comprised of the call control "intelligence" and a media gateway boasting the media functions, for example conversion from TDM voice to Voice over IP.

Media Gateways feature endpoints for the Call Agent to create and manage media sessions with other multimedia endpoints. Endpoints are sources and/or sinks of data that can be physical or virtual. For creating physical endpoints, hardware installation is needed while virtual endpoint can be created using available software.

Call Agents come with the capability of creating new connections, or modify an existing connection. Generally, a media gateway is a network element which provides conversion between the data packets carried over the Internet or other packet networks and the voice signals carried by telephone lines. The Call Agent provides instructions to the endpoints to check for any events and - if there is any - create signals. The endpoints are designed in such a way as to automatically communicate changes in service state to the Call Agent. The Call Agent can audit endpoints and the connections on endpoints.

401/402 Response Code

Response Code is a 3-digit response to the request, indicating the processing results for requests. For example, 401 and 402 represent responses to the on-hook and off-hook operations.

NTFY

Notification, or Notify, a command sent from gateway to call agent.

SIP (Session Initiation Protocol)

Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between two or more end points.

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides the capabilities to:

- Determine the location of the target end point—SIP supports address resolution, name mapping, and call redirection.

- Determine the media capabilities of the target end point—Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between the end points. Conferences are established using only the media capabilities that can be supported by all end points.

- Determine the availability of the target end point—If a call cannot be completed because the target end point is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target end point was unavailable.

- Establish a session between the originating and target end point—If the call can be completed, SIP establishes a session between the end points. SIP also supports mid-call changes, such as the addition of another end point to the conference or the changing of a media characteristic or codec.

- Handle the transfer and termination of calls—SIP supports the transfer of calls from one end point to another. During a call transfer, SIP simply establishes a session between the transferee and a new end point (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

Components of SIP

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:

- User agent client (UAC)—A client application that initiates the SIP request.
- User agent server (UAS)—A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.
- Typically, a SIP end point is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.
- From an architecture standpoint, the physical components of a SIP network can be grouped into two categories: clients and servers. Figure 1-1 illustrates the architecture of a SIP network.
- SIP Clients
- SIP clients include:
    - Phones - Can act as either a UAS or UAC. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
    - Gateways - Provide call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side.

- SIP Servers

SIP servers include:

- Proxy server - The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

- Redirect server - Provides the client with information about the next hop or hops that a message should take and then the client contacts the next hop server or UAS directly.

- Registrar server - Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

How SIP Works

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more end points.

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:userID@gateway.com. The user ID can be either a user name or an E.164 address.

Users register with a registrar server using their assigned SIP addresses. The registrar server provides this information to the location server upon request.

When a user initiates a call, a SIP request is sent to a SIP server (either a proxy or a redirect server). The request includes the address of the caller (in the From header field) and the address of the intended callee (in the To header field). The following sections provide simple examples of successful, point-to-point calls established using a proxy and a redirect server.

Over time, a SIP end user might move between end systems. The location of the end user can be dynamically registered with the SIP server. The location server can use one or more protocols (including finger, rwhois, and LDAP) to locate the end user. Because the end user can be logged in at more than one station and because the location server can sometimes have inaccurate information, it might return more than one address for the end user. If the request is coming through a SIP proxy server, the proxy server will try each of the returned addresses until it locates the end user. If the request is coming through a SIP redirect server, the redirect server forwards all the addresses to the caller in the Contact header field of the invitation response.

For more information, see RFC 2543—SIP: Session Initiation Protocol, which can be found at http://www.faqs.org/rfcs/.

Using a Proxy Server

If a proxy server is used, the caller UA sends an INVITE request to the proxy server, the proxy server determines the path, and then forwards the request to the callee.

The callee responds to the proxy server, which in turn, forwards the response to the caller.

The proxy server forwards the acknowledgments of both parties. A session is then established between the caller and callee. Real-time Transfer Protocol (RTP) is used for the communication between the caller and the callee.

Using a Redirect Server

If a redirect server is used, the caller UA sends an INVITE request to the redirect server, the redirect server contacts the location server to determine the path to the callee, and then the redirect server sends that information back to the caller. The caller then acknowledges receipt of the information.

The caller then sends a request to the device indicated in the redirection information (which could be the callee or another server that will forward the request). Once the request reaches the callee, it sends back a response and the caller acknowledges the response. RTP is used for the communication between the caller and the callee.

SIP Versus H.323

In addition to SIP, there are other protocols that facilitate voice transmission over IP. One such protocol is H.323. H.323 originated as an International Telecommunications Union (ITU) multimedia standard and is used for both packet telephony and video streaming. The H.323 standard incorporates multiple protocols, including Q.931 for signaling, H.245 for negotiation, and Registration Admission and Status (RAS) for session control. H.323 was the first standard for call control for VoIP and is supported on all Cisco Systems' voice gateways.

SIP and H.323 were designed to address session control and signaling functions in distributed call control architecture. Although SIP and H.323 can also be used to communicate to limited intelligence end points, they are especially well-suited for communication with intelligent end points.

Although SIP messages are not directly compatible with H.323, both protocols can coexist in the same packet telephony network if a device that supports the interoperability is available.

For example, a call agent could use H.323 to communicate with gateways and use SIP for inter-call agent signaling. Then, after the bearer connection is set up, the bearer information flows between the different gateways as an RTP stream..

Proxy

Proxy is the kernel of SIP, implementing message transfer functions.

Registrar

When a client powers on, it will tell network its IP address in order to be found. We call this procedure “register”. The server that accepts this request is called “registrar”.

Registration Expire(s)

In order to control client side, every register message has a certain stored period. If the message is modified in that period, which mean it works for user otherwise Registrar will consider the message is not useful any more, so it will be deleted.

DNS (Domain Name System, or Service or Server）

DNS is a very important service of internet, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

PPPoE（Point-to-Point Protocol Over Ethernet）

PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. The feature of PPPoE:

- All the users over the Ethernet share a common connection
- Allow single user P2P to different network
- Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

Time Server

Time Server provides time calibration, control, and synchronization for equipments running in the network.

Caller ID Detecting

Using FXO to detect caller ID from the PSTN and use this number as the originating number for the IP call.

SNMP (Simple Network Management Protocol)

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Two versions of SNMP exist: SNMP version 1 (SNMPv1) and SNMP version 2 (SNMPv2). Both versions have a number of features in common, but SNMPv2 offers enhancements, such as additional protocol operations.

Standardization of yet another version of SNMP—SNMP Version 3 (SNMPv3) - is pending.

SNMP basic components:

SHORT NAME	DESCRIPTION
MIB	MANAGEMENT INFORMATION BASES
SMI	STRUCTURE OF MANAGEMENT INFORMATION
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL

There are two ways to get data from managed network equipment, one is polling-only, which engages the workstation all the time; the other is interrupt-based method, which gets data periodically. Both methods have their disadvantages. The result is the combined method, called trap-directed polling. This is probably the most effective way to gather managed network data.

UDP Port

Port has two meanings in network technology. One is the physical port, via which other equipments can be connected. The other is the logical port, interfacing with different network protocols. Logical port can be of two types as well, depending what protocols we are talking about. One is TCP port, the other is UDP port. UDP port is a protocol port for data packages. No connection between client and server is required to use this port.

SNMP Trap

Trap is part of SNMP. A trap is a one-way message from a network element, such as a router, switch or server, to the NMS. The messages are sent via UDP, which means they are not guaranteed to arrive.

NAT（Network Address Translator or Translation）

Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations.

SDP (Session Description Protocol)

SDP describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

STUN（Simple Traversal of UDP over NATs）

A protocol that allows applications to detect that a network address translation (NAT) is being used. It can also detect the type of NAT and IP address assigned by it. STUN was developed to support interactive, two-way communications over the Internet such as for voice (VoIP) and videoconferencing. The STUN client sends requests to a STUN server, which is typically hosted by the service provider.

Unlike application layer gateways (ALGs) and Middlebox Communications (MIDCOM), which also support two-way communications through NATs, STUN requires no changes to the NAT.

RADIUS（Remote Authentication Dial In User Service）

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

RADIUS Server

RADIUS Server authenticates clients and returns corresponding settings.

Signal Gain

When detected signals are not strong enough over the network, we use signal gain parameter to increase the strength of the signal.

Line Impedance

A measure of the total opposition to current flow in an alternating current circuit, made up of two components, ohmic resistance and reactance, and usually represented in complex notation as Z = R + iX, where R is the ohmic resistance and X is the reactance. It also refers to an analogous measure of resistance to an alternating effect, as the resistance to vibration of the medium in sound transmission.

Signal Mode

Signal mode refers to inserting a silence signal periodically into the voice stream. Standard used in China specifies “450 Hz, 350ms ON + 350ms OFF”, means signal cycle is 700ms; insert 350 ms signal plus a silence signal of 350 ms for each cycle.

Jitter Buffer

Jitter is a major factor affecting the quality of IP calls. Jitter buffer is a software process that eliminates jitter caused by transmission delays in Internet telephony (VoIP) network. As the jitter buffer receives voice packets, it adds small amounts of delay to the packets so that all of the packets appear to have been received without delays. Voice signals are sequential by nature (i.e., they must be played back in the order in which they were sent) and the jitter buffer ensures that the received packets are in the correct order. Without a jitter buffer to smooth the transmission, data can be lost, resulting in choppy audio signals. There are two types of jitter buffers - dynamic and static. A static jitter buffer is hardware-based and configured by the manufacturer. A software-based jitter buffer is called a dynamic jitter buffer and can be configured by the system or network administrator.

RTP Payload Type

RTP Payload type indicates payload format, including codec, clock rate, channel, etc. For example, type 2 indicates payload in this packet is using ITU G721 codec, sample rate is 8000Hz and using single channel.

SID (Silence Information Description)

SID describes parameters to apply silence compression and comfort noise generation.

Voice Proxy

This is primarily used to resolve problems of accessing networks (for example, ADSL, Cable Modem, Ethernet, Proxy, etc.) using a faux/hidden IP or internal IP. It enables endpoints to access the network without having to change network settings. For IAD using public network and real IP address, voice proxy is not needed.

Symmetric RTP

RTP receiving end and sending end are using the same port.

Kernel

Kernel refers to the Linux Operating System. New Rock gateway uses Linux OS.

SDP（Session Description Protocol）

SDP describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation.

G.723.1 Voice CODEC

G.723.1 dual rate speech coder performs compression and decompression of 8 kHz speech signals. It encodes 16-bit PCM samples into 16-bit code-words yielding 10 or 12 code-words per 240 sample frames for the 5.3 Kbps and 6.3 Kbps channels respectively. GAO's G.723.1 software has switchable transmission rates over 5.3 or 6.3 Kbps channels providing 4 kHz of quality speech bandwidth in conformance with the ITU-T standard. The higher bit rate has greater quality. The lower bit rate gives good quality and provides system designers with additional flexibility.

The ITU-T G.723.1 standard specifies a coded representation that can be used for compressing the speech or other audio signal component of multimedia services at a very low bit rate as part of the overall H.324 family of standards. This coder was optimized to represent high quality speech at the above rates using a limited amount of complexity. It encodes speech or other audio signals in frames using linear predictive analysis-by-synthesis coding. The excitation signal for the high rate coder is Multipulse Maximum Likelihood Quantization (MP-MLQ) and for the low rate coder is Algebraic-Code-Excited Linear-Prediction (ACELP).

TOS (Type of Service)

TOS has 8 bits reserved to the service type in the IP datagram. 0-2 means precedence. 6-7 are unused. 3-5 means D (requests low delay), T (requests high throughput), R (requests high reliability), respectively.

T.38 Standard Fax Protocol

T.38 is an ITU-T Recommendation. T.38 describes the technical features necessary to transfer facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. The Recommendation allows the use of either TCP or UDP depending on the service environment.

Redundancy Frame

Redundancy frame is used to ensure more reliable fax transmissions than that of RTP voice transmission.

V.21

V.21 is an ITU-T recommendation for full-duplex communication between two analogue dial-up modems using audio frequency-shift keying modulation at 300 bauds to carry digital data at 300 bit/s. If fax machine doesn’t get any fax signal, the gateway can detect any fax signal throughV.21.

NSF（Nonstandard facilities）

Non-standard fax facilities are those whose operation features are not defined by ITU. Some of those features are encoded in FIF but their encoding method was not defined.

Request Line

Request Line and Status Line are one of the RFC 822[9] defined information formats to carry out real time transmission task. Request line uses a method field right after the URI and protocol version fields to indicate request type, and ends with CRLF (Carriage Return or Line Feed). The request can be divided by spaces, but not Carriage Returns or Line Feeds can be used unless when reaching the end of the request.

Via

Via indicates path of route request. Via portion explains origin, route request time, route destination, and port. For example, R 128.200.10.0/24 [120/1] via 128.200.1.1, 00:00:17, ethernet0/0.

Border Agent

Border Agent includes Sign Proxy and Media Proxy.

RC4 Algorithm

The RC4 encryption algorithm is stream cipher, which can use variable length keys. The algorithm was developed by Ron Rivest, for RSA Data security. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure.

Editor	**Wang Hongyu**
Technical Details	**Yu Zhigang & Xia Jingyong**
Last Modified	**2006-03-09**
English Translator	**Sunshinmind, Inc., New Rock Tech U.S. Office June 6, 2006**

This document contains proprietary trade secrets of New Rock Technologies, Inc. and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture, use, or sell anything that it may describe. Reproduction (including photo-copying, translating into other languages, burning on CD/DVD), disclosure (including putting on the Internet or BBS), or use without specific written authorization of New Rock Technologies, Inc. is strictly forbidden.