InnoMedia MTA8000 Series Administrative Guide

V13, November 2022

Table of Contents

1 Introduction 8

1.1 Product Overview 8
1.2 Package Contents 8
1.2.1 Residential models: MTA8328-1N, MTA8328-1W, MTA8328-1NP, MTA8328-1WP, MTA8338-1N 8
1.2.2 Business Models MTA8328-MP: MTA8328-4, MTA8328-8, MTA8328-24 9
1.3 Residential Models: Out of the Box Setup 9
1.3.1 MTA8328-1W WiFi Connection Optimizer (WCO) Test 10
1.4 Business Models: Out of the Box Setup 12
1.5 Terminology and Usage 12
2 Home -- Device States 13

3 Network 16

3.1 IP Address Configuration for MTA 16
3.1.1 Network Operation Mode 16
3.1.2 DHCP Server Setting 16
3.1.3 Ethernet IP Address Setting – WAN Interface 17
3.1.4 Ethernet IP Address Setting – LAN Interface 18
3.1.5 WiFi Configuration and IP Address Setting 19
3.1.6 Host and DNS Servers 20
3.1.7 Master DNS 20
3.1.8 TOS Setting 21
3.1.9 VLAN Settings 21
3.1.10 Port Forwarding 22
4 Telephony 23

4.1 Profile Config 23
4.1.1 SIP Server Setting 23
4.1.2 Security Setting 26
4.1.3 Codec Setting 27
4.1.4 SIP Timer Setting 28
4.1.5 DigitMap Setting 30
4.1.6 Emergency Service Setting 34
4.1.7 Feature and Service Code Setting (MTA8328-MP only) 37
4.1.8 Feature and Service Code Setting (MTA8328-1N/W and MTA8338-1N only) 38
4.1.9 Fax Setting 40
4.1.10 Call Report Setting 41
4.2 Port Config 42
4.2.1 SIP Account Setting 42
4.2.2 Features Setting 43
4.2.3 Line Setting 44
4.2.4 Speed Dial 45
4.2.5 IMS related SIP settings 45
4.3 Telephony Region and Misc Setting 46
4.3.1 Media Port Setting 46
4.3.2 Regional Setting 46

4.3.3 Tone Cadence Setting 47
4.3.4 Ring Cadence Setting 48
4.4 Line Diagnostics 49
4.4.1 GR909 Tests: triggered from the WEB Administrative Console 49
4.4.2 GR909 Tests: triggered from SIP NOTIFY Message 50
5 System 51
5.1 Account Settings 51
5.1.1 Administrator Account Setting 51
5.1.2 End User Account Setting 51
5.2 Page Permission 51
5.3 Firmware Upload 52
5.4 Reboot 53
5.5 Restore To Factory 53
5.6 Provisioning Setting 54
5.6.1 Provisioning Parameters 54
5.6.2 Provisioning Factory Default Settings to Devices Deployed in the Field 56
5.7 EMS Setting 57
5.7.1 EMS Server 57
5.8 Trace Log 59
5.8.1 Trace Log Setting 59
5.9 System Time 60
5.9.1 Time Setting 60
5.10 Language 62
5.11 Uplink Connection 62
5.12 Certificate & Key 63
5.13 Config File 63
5.14 SNMP Setting 63
5.15 Remote Access 65
5.15.1 Remote Access Setting 65
6 CLI Command references 65
Appendix A LED States 67
Model MTA8328-1W 67
Model MTA8328-1N / MTA8338-1N 68
Model MTA8328-4, MTA8328-8, MTA8328-24 69
Appendix B The use of encryption key methods 70
Inno rc4_102 70
Openssl command example 70
Appendix C: WiFi Connection Setup through Captive Portal 71
Appendix D – Provisioning through DHCP Options 73
Method 2 – Use both DHCP Option 66 and DHCP Option 67 together 73
Important Note: 73

Table of Figures

Figure 1. Residential MTA Package....8
Figure 2. MTA8328-1N Front and back panel (Example)....8
Figure 3. MTA8328-MP business models (4, 8, and 24 FXS port models)....9
Figure 4. Setup the Residential MTA device to connect to the router or network switch....9
Figure 5. WCO test result....11
Figure 6. Setup the MTA in a business environment....12
Figure 7. Login Screen - Input Username and Password. MTA8328-1N login screen example.....13
Figure 8. Current status of MTA8328-1N (as an example)....14
Figure 9. Configure the Operation Mode....16
Figure 10. Configure the DHCP Server....17
Figure 11. Configure the IP Address on the WAN Interface (MTA8328-1N, MTA8338-1N)....18
Figure 12. Configure the IP Address on the WAN Interface (MTA8328-MP)....18
Figure 13. Configure the IP Address on the LAN Interface of MTA8328-MP....19
Figure 14. WiFi Configuration and IP Address Setting....19
Figure 15. Configuring the host information on the device....20
Figure 16. Configuring the Master DNS Information....20
Figure 17. TOS Setting....21
Figure 18. VLAN settings....21
Figure 19. Port Forwarding Settings....22
Figure 20 Configuring Telephony options....23
Figure 21. SIP Server Setting—SIP Proxy Server....23
Figure 22. SIP Server Settings – SIP Option....24
Figure 23. MTA Security Settings....26
Figure 24. Codec Setting....27
Figure 25. SIP Timer Setting....28
Figure 26. Digitmap Setting....30
Figure 27**.** FXS Setting....33
Figure 28. Overall Message Flow for Geolocation Services....34
Figure 29. Emergency Service Setting....36
Figure 30. Feature and Service Code Setting....37
Figure 31. Feature and Service Code Setting....39
Figure 32. Fax Setting....40
Figure 33 Call report settings....41

Figure 34. Phone port status overview....42

Figure 35. SIP Account Setting....42

Figure 36. Call Feature Setting....43

Figure 37. Line Setting....44

Figure 38. Speed Dial....45

Figure 39. IMS Settings....45

Figure 40. Media Port Setting....46

Figure 41. Regional settings for power and analog line specifications....46

Figure 42. Tone Cadence Setting....47

Figure 43. Ring Cadence Setting....49

Figure 44. GR909 Line Test (illustrative example showing a four port MTA)....49

Figure 45. Administrator account setting....51

Figure 46. User Account Setting....51

Figure 47. User Page Permission Setting....52

Figure 48. Firmware Upload....52

Figure 49. Reboot Dialog....53

Figure 50. Restore To Factory Dialog....53

Figure 51. Provisioning Server Setting....54

Figure 52. Configuring EMS Server Information....57

Figure 53. Trace Log Setting....59

Figure 54. Time Setting....61

Figure 55. Language Selection for IVR system....62

Figure 56. Uplink Detection Settings....62

Figure 57. Certification & Key....63

Figure 58. System Config....63

Figure 59. SNMP Setting....64

Figure 60. Protocol and Port Settings for Remote Access....65

Figure 61. Captive Portal - Welcome....71

Figure 62. Captive Portal – SSID selection....71

Figure 63. Captive Portal – SSID password input....72

Figure 64. Captive Portal – Confirm settings....72

About This Document

This document provides details of the features available on the InnoMedia MTA8000 series as well as feature descriptions and the configurations required.

Revision History

Date	Version	Notes
2016/10/25	V1.0	Based on firmware V1.0.0.19
2016/11/08	V1.1	Based on firmware V1.0.0.23
2016/11/23	V1.1	Based on firmware V1.0.0.27
2017/03/25	V5	Based on firmware V1.0.5.1
2017/04/07	V6	Based on firmware V1.0.5.3
2018/06/25	V7	Add high density port models
2019/04/08	V8	Add Router/Switch mode features
2022/02/03	V9	Add MTA8338-1N model
2022/05/31	V10	Based on firmware V1.0.22.66/1.0.0.7
2022/06/20	V11	Add features for (1) Port forwarding, (2) Bidirectional VQM
2022/08/02	V12	Add VLAN feature
2022/11/21	V13	Add Geolocation Services (MTA8328-MP only)

Federal Communication Commission Interference Statement

The MTA8000 series of products have been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference using one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of **20cm** between the radiator & your body.

1 INTRODUCTION

1.1 Product Overview

The InnoMedia MTA8000 series is an integrated device providing telephony service over a broadband network.

It allows the connection of your device to a Router/Firewall through either a wired Ethernet connection or through WiFi[1]. This guide will help you to quickly install and configure your unit so that you can start placing calls right away.

1.2 Package Contents

1.2.1 Residential models: MTA8328-1N, MTA8328-1W, MTA8328-1NP, MTA8328-1WP, MTA8338-1N

- MTA8328-1W(P): Supports WiFi and Ethernet interfaces
- MTA8328-1N(P): Supports Ethernet interfaces only
- MTA8338-1N(P): Supports Ethernet interfaces only

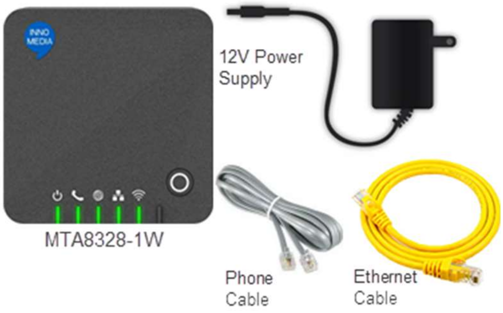


Figure 1. Residential MTA Package

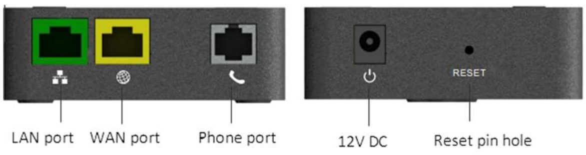


Figure 2. MTA8328-1N Front and back panel (Example)

[1] WiFi functionality is supported on certain models only.

1.2.2 Business Models MTA8328-MP: MTA8328-4, MTA8328-8, MTA8328-24

The MTA 8328-MP high density port models (4, 8, 24 FXS ports) allow the use of an Ethernet interface to connect to the office Router/Firewall.

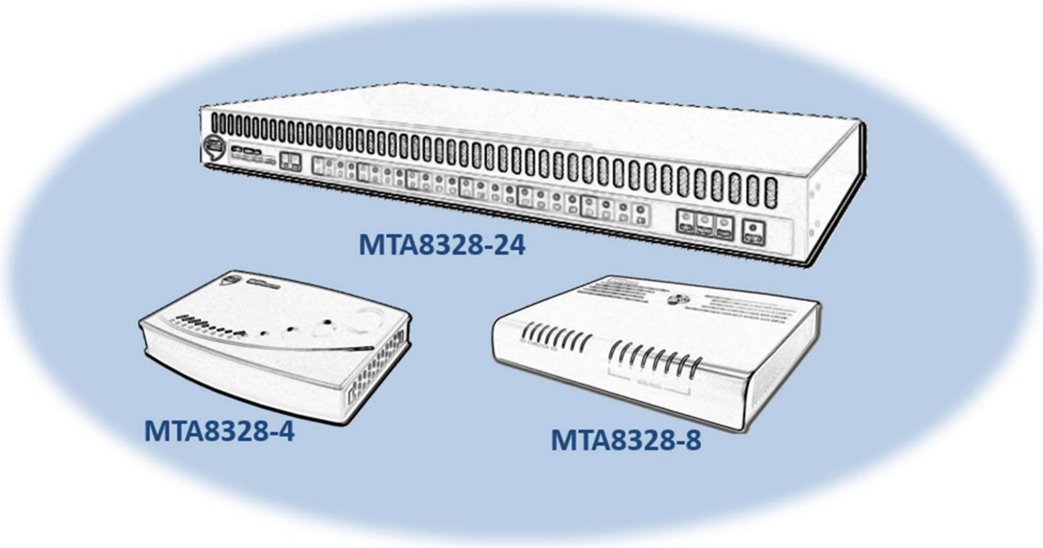


Figure 3. MTA8328-MP business models (4, 8, and 24 FXS port models)

1.3 Residential Models: Out of the Box Setup

This section provides a step-by-step guide to install the MTA and setup the system for connecting to a broadband network. Before starting the Installation, make sure your broadband Internet access device is powered on and your connection is up. (Check your Internet service provider's documentation).

Note that the Ethernet connection setup applies to MTA8338-1N, MTA8328-1N and MTA8328-1W models; whereas the WiFi connection setup applies to MTA8328-1W only.

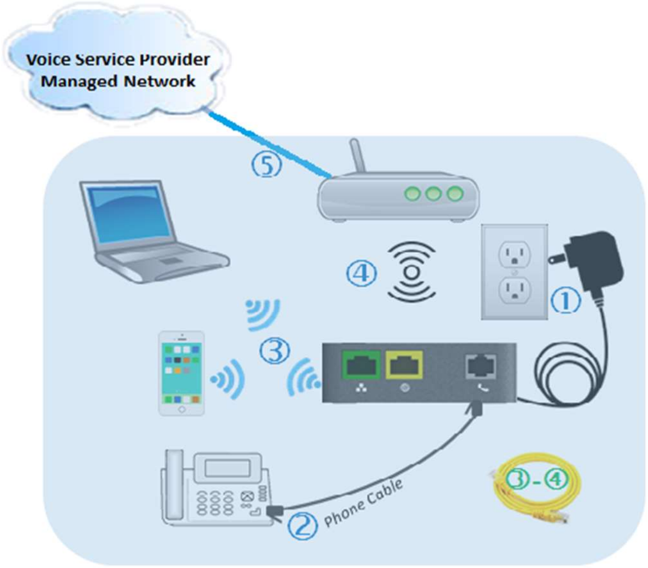


Figure 4. Setup the Residential MTA device to connect to the router or network switch

① Plug the supplied power adapter into the MTA. The power LED will show steady green.

② Connect your phone into the PHONE port on the MTA using the supplied Phone Cable.

③ Setup the MTA to connect to your Home Router.

- **For Ethernet Connection.** If your MTA is located close to your Home Router, connect the yellow Ethernet cable (supplied) into the WAN port on the MTA and connect the other end into an available Ethernet port on your router or LAN network. Then proceed to step ④ directly.
- **For WiFi Connection.** Alternatively, connect the MTA to the Home Router through a WiFi connection. You will connect the MTA to a WiFi Access Point using your smartphone, tablet or PC. Press the round button on the top of the unit for about 5 seconds, the MTA will switch to "Setup Mode" and the WiFi LED will change to solid yellow. Connect your smartphone or PC to the MTA's preset SSID shown on the back of the unit, i.e., MTA8328-xxxxxx, product name followed by the last 6 digits of MAC address. The MTA welcome portal web page will show up on your smartphone/PC. If this page does not popup, open a web browser and type in the following address: **http://192.168.199.1/wifisetup/** During setup, follow the instructions on the welcome portal. You will need to select the WiFi SSID of your WiFi Access Point and input the WiFi passphrase. For detailed instructions, please see **Appendix C: WiFi Connection Setup through Captive Portal.**

④ Confirm that the MTA is successfully connected to the Home Router and acquires an IP address as follows:

For Ethernet Connection. The WAN LED shows green for 100BT connection, or shows amber for 10BT.
For WiFi Connection. The WiFi LED shows green. If it is not green, repeat step ③**.**

⑤ Once the MTA connects to the voice service provider network, and completes the registration and service provision process, you should see a solid green PHONE LED light displayed.

1.3.1 MTA8328-1W WiFi Connection Optimizer (WCO) Test

This feature applies to the MTA8328-1W only. The WCO test is designed to determine an ideal location for the MTA by performing voice quality validation thru a WiFi connection[2]. One of the following results will be displayed/announced after the WCO test is completed:

Your device location is **Excellent|Good|Not Good**

If the test result is "Not Good", one or more of the following steps are recommended before running the WCO test again until the result is "Good" or "Excellent":

- Change the location of the MTA. Decrease the distance between the MTA and the WiFi router and/or avoid any large obstructions between the MTA and WiFi router.
- Switch to another WiFi channel.
- Change WiFi frequency between 2.4GHz and 5 GHz to improve reception.

Note:

- The WCO test can only be invoked when the WAN Ethernet is not connected.
- Run the WCO test only when the WiFi LED displays solid green as its initial state.
- The WCO test will run for 30 seconds. During a test period, the WiFi LED changes its state to "blinking yellow" (0.5 sec ON | 0.5 sec OFF).

Execute the WCO test using any of the following three approaches:

[2] Note that some WiFi routers may drop WCO packets for strict security configurations.

Method 1: Dial ***8 from the phone connected to the MTA.

Off hook the phone, dial ***8, and the MTA Interactive Voice Response (IVR) will play “Wireless connection optimizer test is in progress, please wait…” After the test is complete, the IVR will then announce the test result, as well as displaying it through its respective LED state, as shown in **LED State**

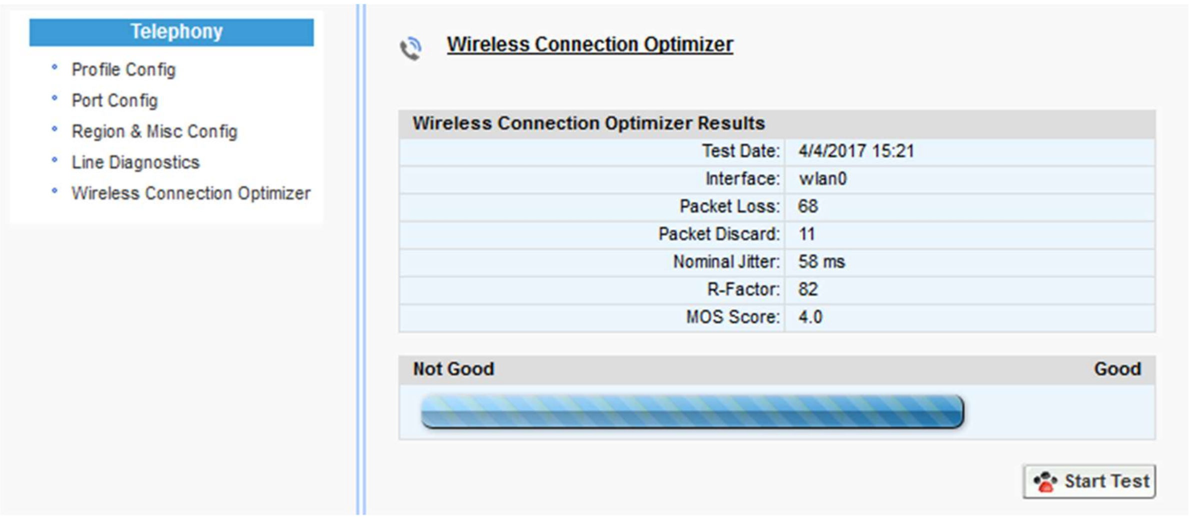
Method 2: Double click the round button on the top of the MTA box

Double click the round button on the top of the unit. After the WCO test is complete, the result is displayed through its respective LED state, as shown in **LED State**

Method 3: Device administrative WEB console

Login to the MTA administrative web console (Figure 7). Navigate to Telephony > Wireless Connection Optimizer page, and click the <Start Test> Button. The test result will be displayed on the WEB GUI page (Figure 5) as well as through its respective LED state, as shown in

Table 1: WCO Result-LED State.



Wireless Connection Optimizer Results

Test Date:	4/4/2017 15:21
Interface:	wlan0
Packet Loss:	68
Packet Discard:	11
Nominal Jitter:	58 ms
R-Factor:	82
MOS Score:	4.0

Figure 5. WCO test result

Table 1: WCO Result-LED State. The WCO test result represented through its LED status will stay active for 20 seconds.

Test State	WiFi LED Representation
WCO Initial State	Solid Green
WCO Result State	
• Excellent	Solid Green
• Good	Alternates between solid yellow and solid green.
• Not Good	Solid yellow

1.4 Business Models: Out of the Box Setup

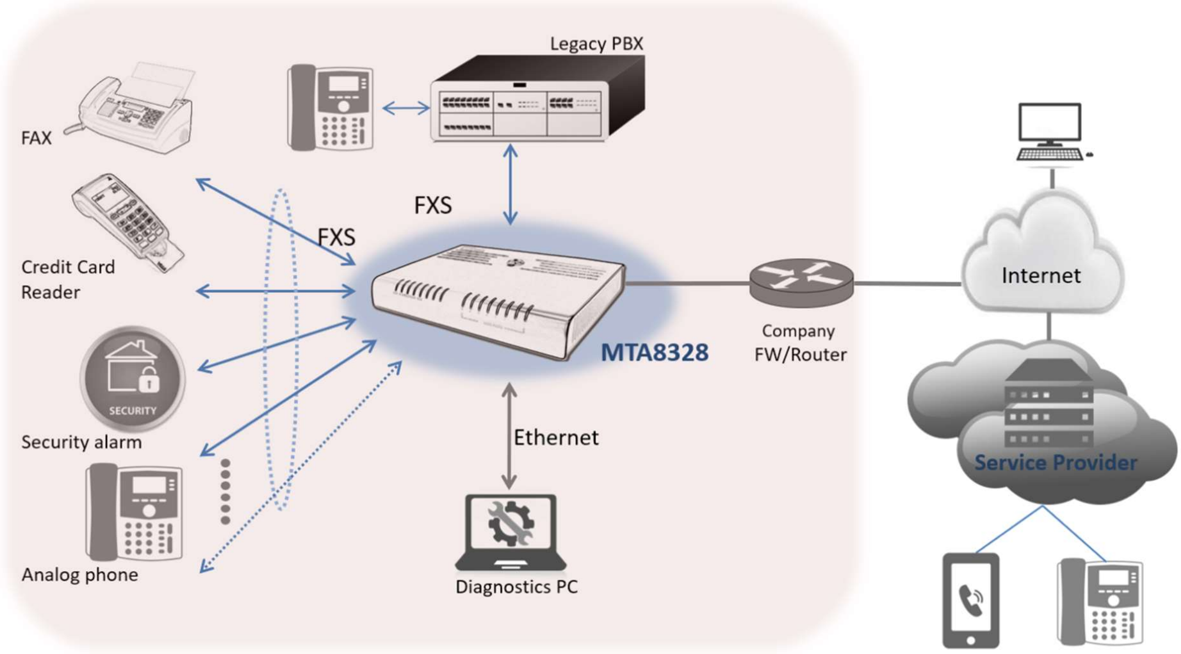


Figure 6. Setup the MTA in a business environment

① Plug the supplied power adapter into the MTA. The power LED will show steady green.

② Connect phones or other analog devices into the PHONE X port on the MTA.

③ Setup the MTA to connect to the Internet. Connect the yellow Ethernet cable (supplied) into the WAN port on the MTA and connect the other end into an available Ethernet port on your router or LAN network switch.

④ Confirm that the MTA is successfully connected to the Router and acquires an IP address. If the WAN LED shows steady green, it is connected.

- The MTA WAN interface is configured as DHCP client by factory default so that it can obtain an IP address from the corporate DHCP server.
- When a static IP address is needed, refer to section 2 to login to the MTA web console and configure the WAN interface accordingly.

⑤ Once the MTA connects to the voice service provider network, and completes the registration and service provision process, you should see a solid green PHONE LED light displayed.

1.5 Terminology and Usage

1. The supported character set of the device text input box: 7 bit ASCII.

2 HOME -- DEVICE STATES

The MTA can be managed via a Web Browser interface. Once the MTA is connected to the network, connect a device with a browser to the same router as the MTA WAN interface, or directly connect the device to the MTA LAN interface. Access and configure the MTA via a Web Browser.

The IP address of the Ethernet LAN interface is 192.168.99.1.

Press ***1 on a phone connected to the MTA and the IP address of the MTA WAN interface will be played through the telephone handset.

When the Ethernet WAN interface is connected to the Router, the IP address played is always the Ethernet WAN IP; otherwise, the WiFi WAN IP address will be played if a WiFi connection has been setup.

The default Admin Username is: ***admin***
The default Password is: ***password***

The default end user Username is: ***user***
The default Password is: ***welcome***

Note: The username and password could be different if changed by the service provider. They also could be changed through service provisioning process, Please refer to the user's guide of provisioning system provided by specific vendors..

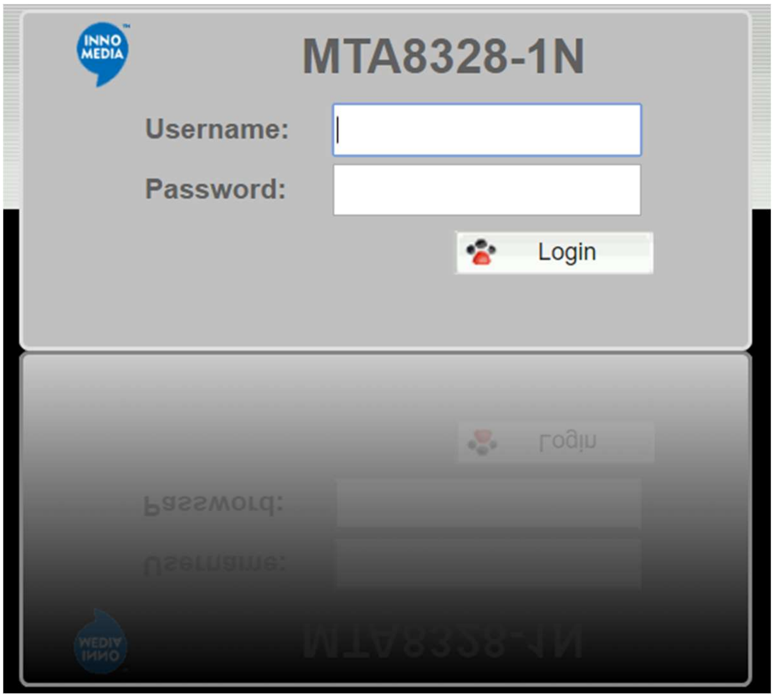
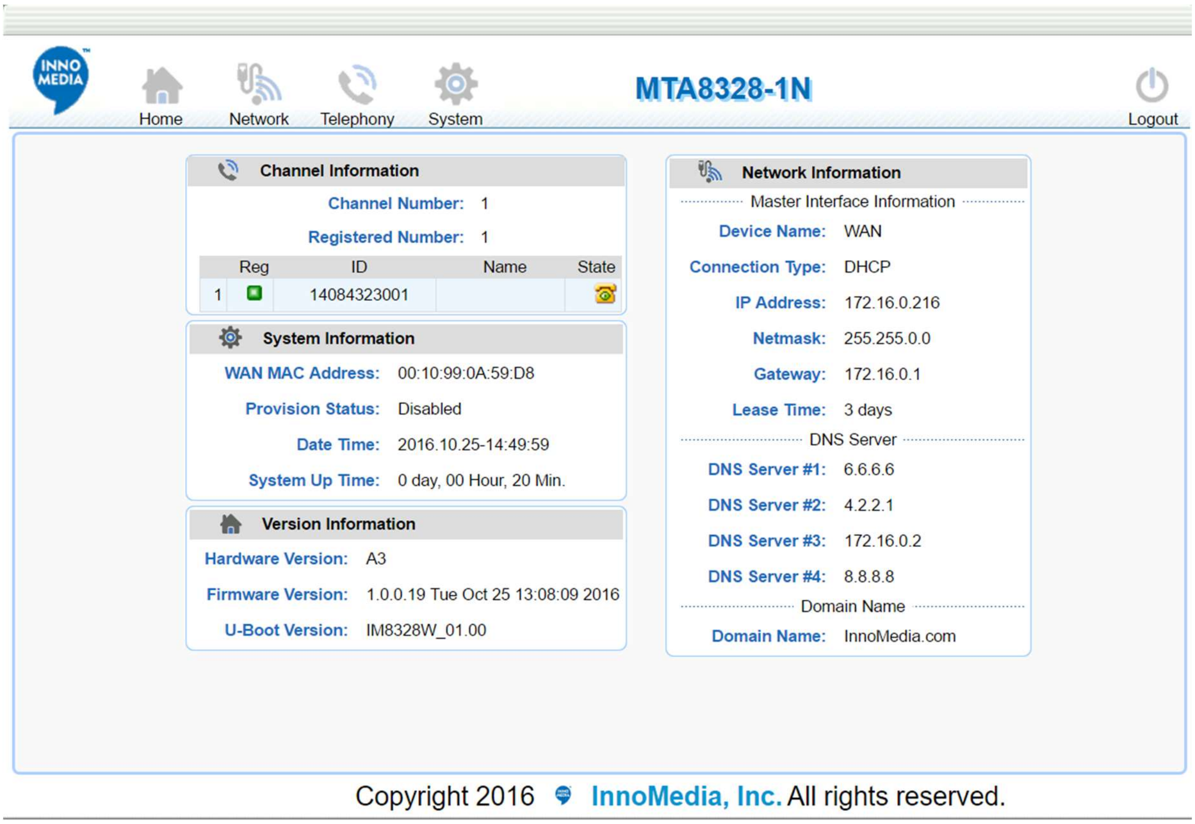


Figure 7. Login Screen - Input Username and Password. MTA8328-1N login screen example.

The Home page displays the MTA current status.



Channel Information

Channel Number: 1

Registered Number: 1

	Reg	ID	Name	State
1	🟩	14084323001		☎

System Information

WAN MAC Address: 00:10:99:0A:59:D8

Provision Status: Disabled

Date Time: 2016.10.25-14:49:59

System Up Time: 0 day, 00 Hour, 20 Min.

Version Information

Hardware Version: A3

Firmware Version: 1.0.0.19 Tue Oct 25 13:08:09 2016

U-Boot Version: IM8328W_01.00

Network Information

Master Interface Information

Device Name: WAN

Connection Type: DHCP

IP Address: 172.16.0.216

Netmask: 255.255.0.0

Gateway: 172.16.0.1

Lease Time: 3 days

DNS Server

DNS Server #1: 6.6.6.6

DNS Server #2: 4.2.2.1

DNS Server #3: 172.16.0.2

DNS Server #4: 8.8.8.8

Domain Name

Domain Name: InnoMedia.com

Copyright 2016 InnoMedia, Inc. All rights reserved.

Figure 8. Current status of MTA8328-1N (as an example)

Field Name	Description
Channel Information	Number of phone lines provisioned Number of SIP accounts provisioned
Reg Status	🟩 Successfully REGISTERED with SIP proxy 🟥 Not REGISTERED with SIP proxy ■ Account disabled
State	☎ Phone on hook ☎ Phone off hook
System Information	• MAC address of Ethernet WAN • Provision Status: last provisioning date-time and status • Date Time: current date and time • System Up Time: up time since last power up.
Version Information	• Hardware Version • Firmware Version • Boot Loader Version
Network Information	• Master Interface Information: Current active (in use) network. • DNS Server: all DNS server IP addresses configured on the MTA devices. The

	priority order of DNS servers (in order of decreasing priority) used is: Master DNS server(s) > those obtained from the DHCP server > user configured DNS server(s). See section 3.1.7 for details on Master DNS. • Domain Name: the domain name obtained from DHCP Option 15 or the configured value described in section 3.1.6. The value obtained from DHCP has higher priority than any manually configured domain name.

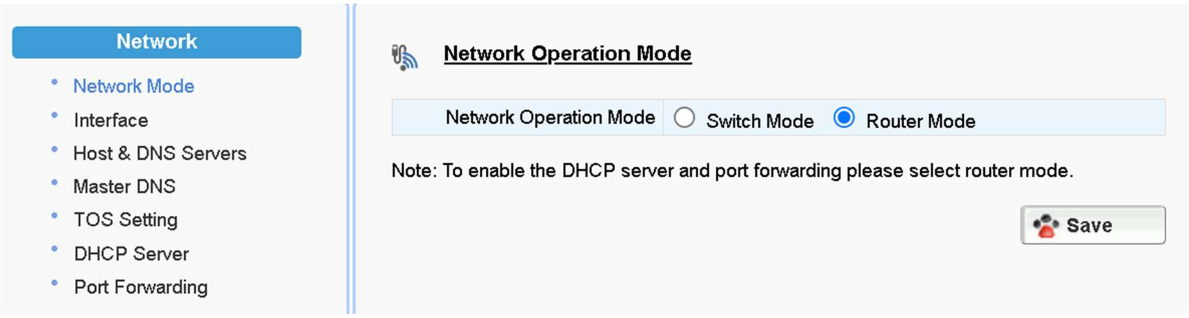
3 NETWORK

The Network pages allow the configuration of the MTA network parameters.

3.1 IP Address Configuration for MTA

3.1.1 Network Operation Mode

This setting is applicable to MTA8328-MP series models only.



Network Operation Mode ○ Switch Mode ● Router Mode

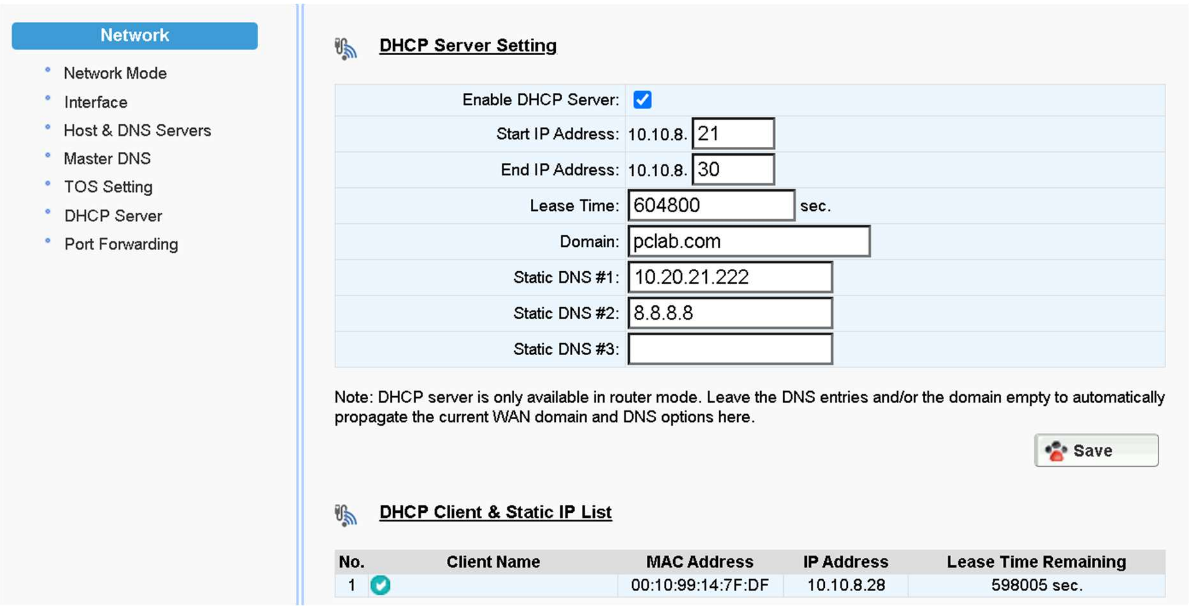
Note: To enable the DHCP server and port forwarding please select router mode.

Figure 9. Configure the Operation Mode

Field Name	Description
Network Operation Mode	• Switch Mode, the factory default setting. The MTA LAN ports are switch ports. Hosts connect to the LAN ports have the same IP network as the MTA WAN interface. • Router Mode. The MTA provides NAT and DHCP Server services to hosts which connect to its LAN ports.

3.1.2 DHCP Server Setting

This setting is only applicable to the MTA8328-MP series model, and when the Network Operation Mode is configured as “Router Mode.”



DHCP Server Setting

Enable DHCP Server:	☑
Start IP Address:	10.10.8. 21
End IP Address:	10.10.8. 30
Lease Time:	604800 sec.
Domain:	pclab.com
Static DNS #1:	10.20.21.222
Static DNS #2:	8.8.8.8
Static DNS #3:	

Note: DHCP server is only available in router mode. Leave the DNS entries and/or the domain empty to automatically propagate the current WAN domain and DNS options here.

DHCP Client & Static IP List

No.	Client Name	MAC Address	IP Address	Lease Time Remaining
1 ✓		00:10:99:14:7F:DF	10.10.8.28	598005 sec.

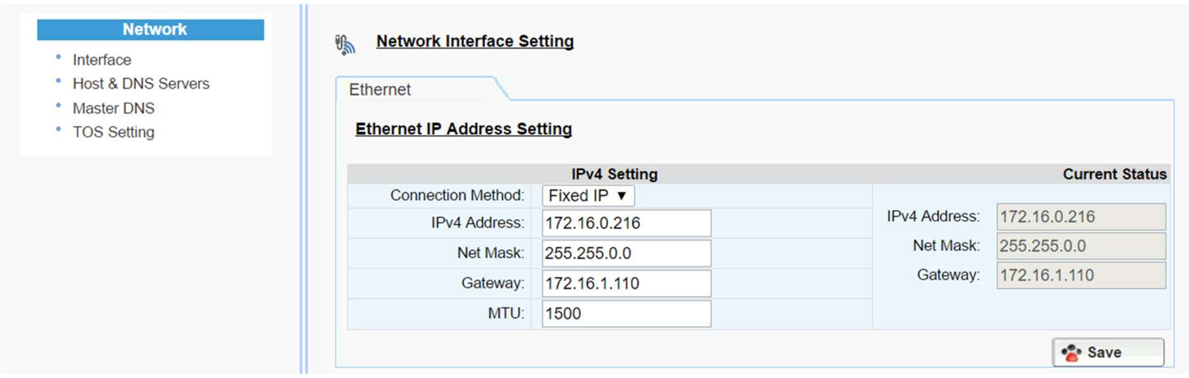
Figure 10. Configure the DHCP Server

Field Name	Description
Enable DHCP Server	Select to allow the MTA to offer IP addresses to hosts connect to its LAN port(s)
Start IP Address End IP Address	Input the start/end IP addresses which the MTA to offer to its LAN hosts. The IP network is limited to the subnet with netmask 255.255.255.0. The network address is the same as that of its LAN interface. The IP range of DHCP clients should not overlap with the MTA LAN IP address.
Lease Time	Input the IP address lease time offered to the LAN hosts.
Static DNS #1, #2, #3	Input the DNS server(s) that the MTA offers to its LAN hosts.

Note: The “DHCP Client & Static IP List” will be cleared if the device is restored to factory default.

3.1.3 Ethernet IP Address Setting – WAN Interface

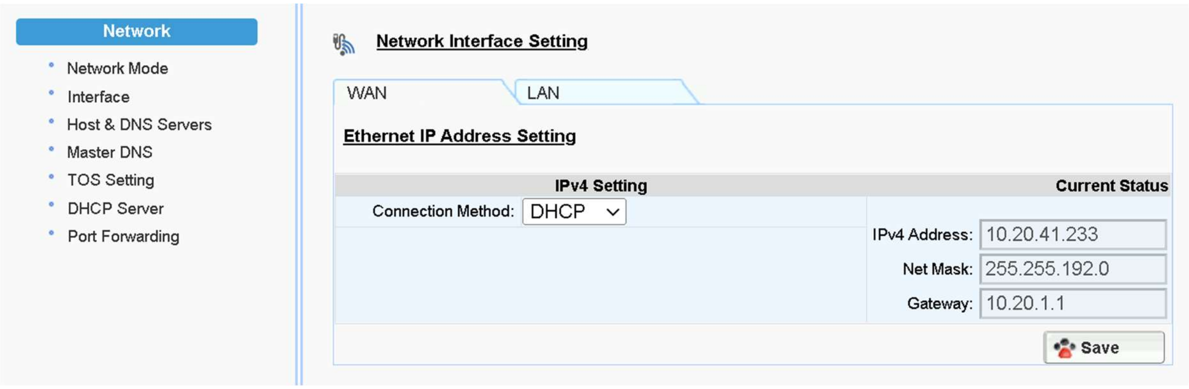
Configure the IPv4 IP address for the device WAN interface. Click the “Interface” menu from the left panel.



Connection Method: Fixed IP
IPv4 Address: 172.16.0.216
Net Mask: 255.255.0.0
Gateway: 172.16.1.110
MTU: 1500

Current Status:
IPv4 Address: 172.16.0.216
Net Mask: 255.255.0.0
Gateway: 172.16.1.110

Figure 11. Configure the IP Address on the WAN Interface (MTA8328-1N, MTA8338-1N)



Connection Method: DHCP

Current Status:
IPv4 Address: 10.20.41.233
Net Mask: 255.255.192.0
Gateway: 10.20.1.1

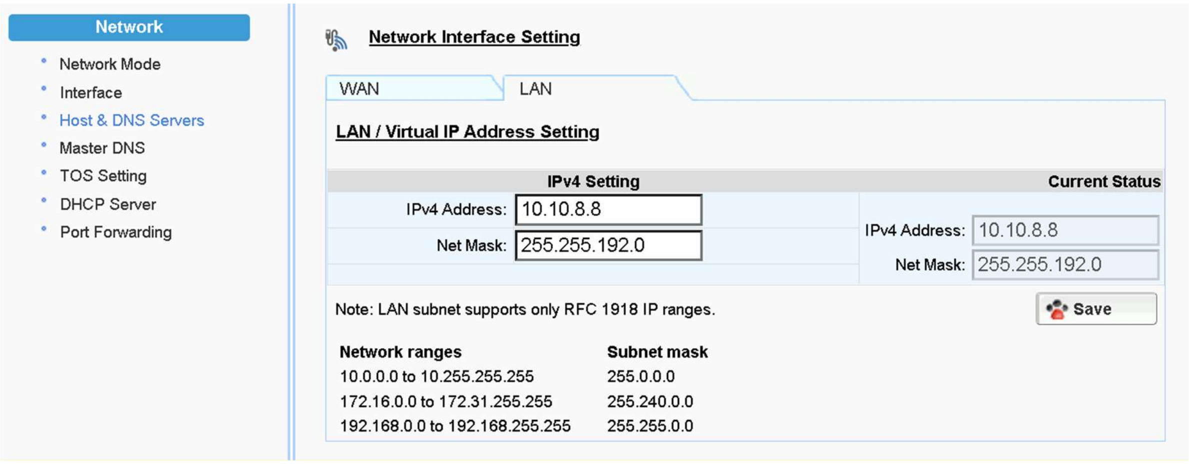
Figure 12. Configure the IP Address on the WAN Interface (MTA8328-MP)

Field Name	Description
Connection Method	• DHCP: Automatically acquires WAN IP address from the Router. • Fixed IP: Need to configure the following parameters according to the Router network settings. IPv4 IP address | Net Mask | Gateway | MTU (maximum size of an IP packet, in bytes). Note that default value of MTU is 1500, and its valid value ranges from 150 to 1500. Do not change the MTU value unless necessary.

3.1.4 Ethernet IP Address Setting – LAN Interface

This setting is only applicable to the MTA8328-MP series.

All LAN port(s) share the same IP address. For maintaining optimum voice quality, the device should not exceed a total (WAN and LAN) throughput of 40 Mbit/sec.



LAN / Virtual IP Address Setting

IPv4 Setting		Current Status	
IPv4 Address:	10.10.8.8	IPv4 Address:	10.10.8.8
Net Mask:	255.255.192.0	Net Mask:	255.255.192.0

Note: LAN subnet supports only RFC 1918 IP ranges.

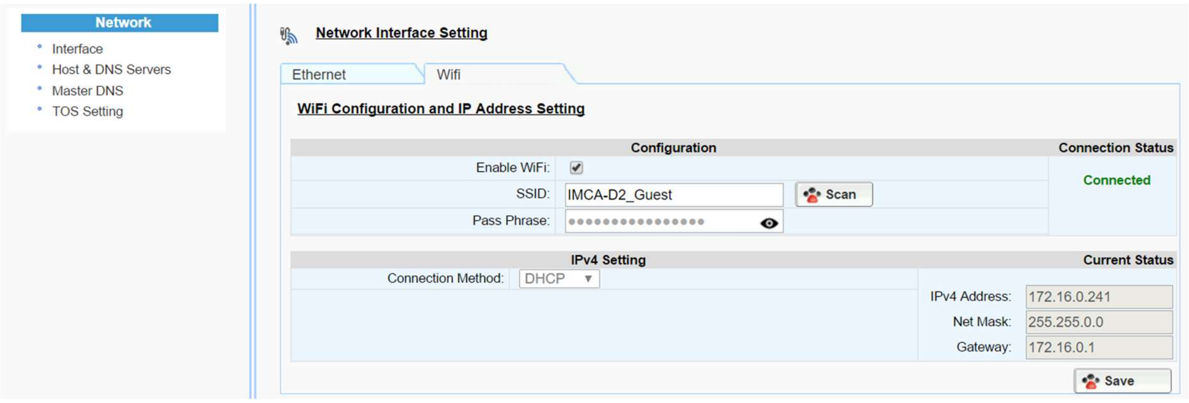
Network ranges	Subnet mask
10.0.0.0 to 10.255.255.255	255.0.0.0
172.16.0.0 to 172.31.255.255	255.240.0.0
192.168.0.0 to 192.168.255.255	255.255.0.0

Figure 13. Configure the IP Address on the LAN Interface of MTA8328-MP

Field Name	Description
IPv4 IP Address Net Mask	• Default IPv4 Address & Net Mask: 192.168.99.1 / 255.255.255.0. Change to the desired IP address to match the LAN network. • IP address ranges: Only RFC1918 defined private networks are supported as follows. Network ranges / Subnet mask : 10.0.0.0 to 10.255.255.255 /255.0.0.0 172.16.0.0 to 172.31.255.255/255.240.0.0 192.168.0.0 to 192.168.255.255/255.255.0.0 • Net Mask: LAN network netmask can be equal to, or a subnet of the RFC1918 subnet masks.

3.1.5 WiFi Configuration and IP Address Setting

This page is applicable to the MTA8328-1W model only.



WiFi Configuration and IP Address Setting

Configuration		Connection Status
Enable WiFi:	☑	Connected
SSID:	IMCA-D2_Guest	
Pass Phrase:	●●●●●●●●●●●●●●●●	

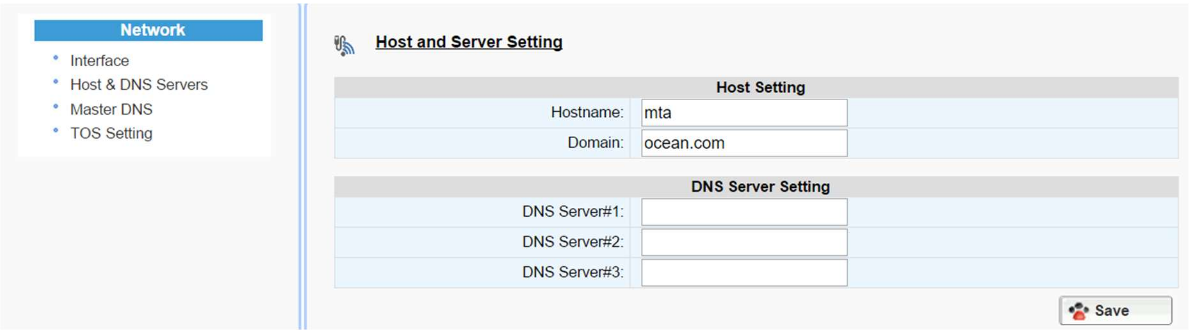
IPv4 Setting		Current Status	
Connection Method:	DHCP	IPv4 Address:	172.16.0.241
		Net Mask:	255.255.0.0
		Gateway:	172.16.0.1

Figure 14. WiFi Configuration and IP Address Setting

Select a WiFi SSID and input the password (Pass Phrase) for WiFi Access Point. Note that the WiFi password cannot be retrieved from this page by the administrator if it is entered through the Captive Portal page.

3.1.6 Host and DNS Servers

Configure the host and the DNS server information provided by your network operator.



Host and Server Setting

Host Setting	
Hostname:	mta
Domain:	ocean.com

DNS Server Setting	
DNS Server#1:	
DNS Server#2:	
DNS Server#3:	

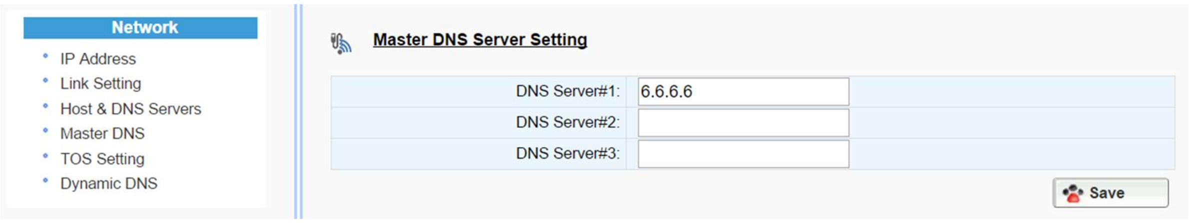
Figure 15. Configuring the host information on the device

Field Name	Description
Host Name	Configure the host name for the device.
Domain	Configure the domain name for the device.
DNS Server Setting	Allows configuration of up to three DNS servers.

3.1.7 Master DNS

"Master DNS" is the IP address of the domain name server specified by the telephony service provider rather than the internet service provider. If "Master DNS" is configured, the MTA gets related DNS services from this configured server to perform voice communication functions. The MTA acquires DNS information from the following servers in the priority shown (in order of decreasing priority):

1. Master DNS
2. DHCP Option
3. Manually configured DNS (see section 3.1.6)



Master DNS Server Setting

DNS Server#1:	6.6.6.6
DNS Server#2:	
DNS Server#3:	

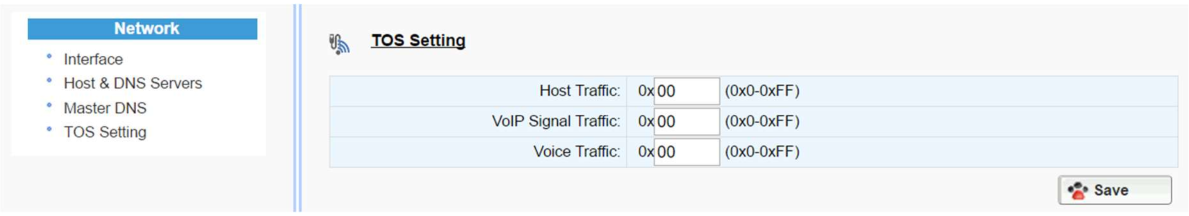
Figure 16. Configuring the Master DNS Information

Field Name	Description

DNS Server	Configure the DNS server information specified by the VoIP service provider for up to 3 DNS servers.

3.1.8 TOS Setting

TOS (Type of Service) is a part of the IPv4 header which is used for precedence, or in other words categorizing traffic classes. The higher the value of the IP Precedence field, the higher the priority of the IP packet.



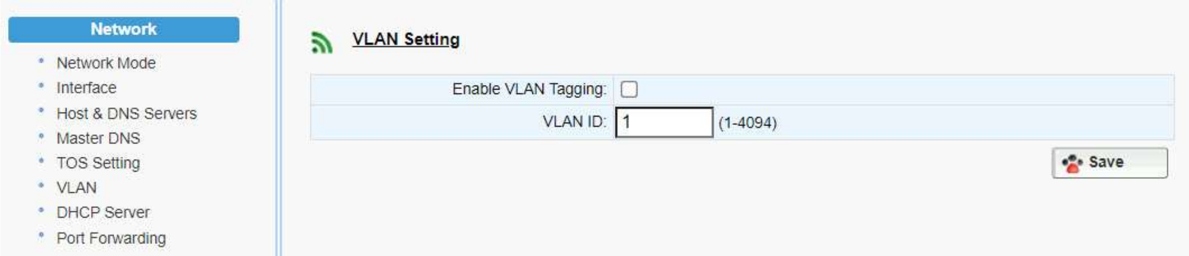
Host Traffic: 0x 00 (0x0-0xFF)
VoIP Signal Traffic: 0x 00 (0x0-0xFF)
Voice Traffic: 0x 00 (0x0-0xFF)

Figure 17. TOS Setting

Field Name	Description
TOS Setting	Host Traffic: Use the configured TOS value to tag data traffic other than SIP or RTP packets.
	VoIP Signal Traffic: Use the configured TOS value to tag SIP signaling packets.
	Voice Traffic: Use the configured TOS value to tag voice RTP packets.

3.1.9 VLAN Settings

This VLAN setting is only applicable to the MTA8328-MP series.



Enable VLAN Tagging: □
VLAN ID: 1 (1-4094)

Figure 18. VLAN settings

Field Name	Description
Enable VLAN Tagging	Check this box to enable VLAN tagging on the MTA WAN Ethernet interface.
VLAN ID	Configure the VLAN ID which matches the ID of the connected VLAN network.

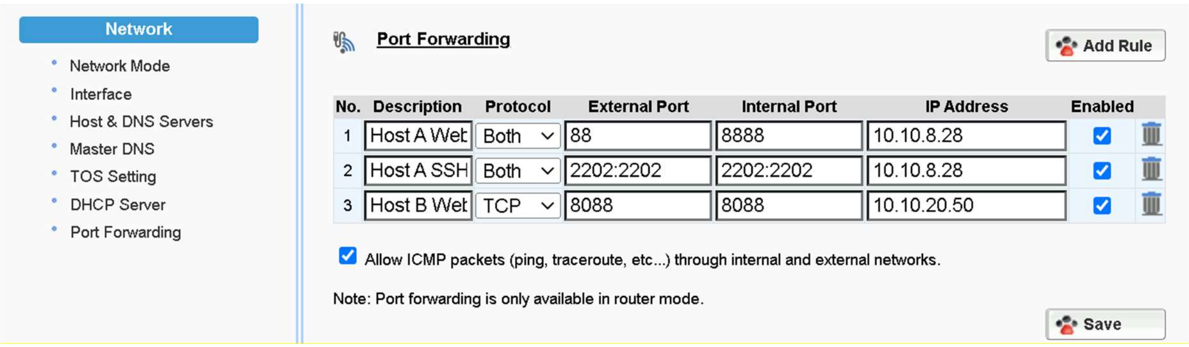
Note: When VLAN is enabled, ALL traffic sent by the device will be tagged with the configured VLAN ID, i.e. it is not possible to tag different types of traffic with different VLAN IDs.

3.1.10 Port Forwarding

This setting is only applicable to the MTA8328-MP series, and only when the Network Operation Mode is configured as “Router Mode.”

The target hosts can be either of the following:

- DHCP clients of the MTA8328-MP acting as a DHCP server
- Fixed IP addresses which meet the following requirements:
  (1) IP address within the LAN netmask configured (see description in section 3.1.4), and
  (2) Default gateway of target host points to the MTA8328-MP LAN IP address.



Port Forwarding

No.	Description	Protocol	External Port	Internal Port	IP Address	Enabled	
1	Host A Wet	Both	88	8888	10.10.8.28	☑	
2	Host A SSH	Both	2202:2202	2202:2202	10.10.8.28	☑	
3	Host B Wet	TCP	8088	8088	10.10.20.50	☑	

☑ Allow ICMP packets (ping, traceroute, etc...) through internal and external networks.

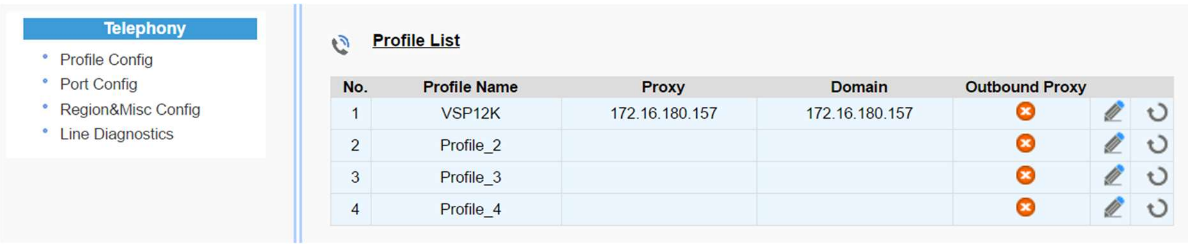
Note: Port forwarding is only available in router mode.

Figure 19. Port Forwarding Settings

Field Name	Description
Description	Brief text description of this rule.
Protocol	Protocol subject to port forwarding. Options: TCP|UDP|Both (TCP&UDP)
External port	The listening port of the MTA8328-MP WAN interface.
Internal port	The listening port of the LAN host. Note: The format is “Starting port [: ending port]”, where ending port is optional (single port assumed if no ending port provided).
IP Address	The IP address of the LAN host that is to be accessible to the WAN domain.
Enabled	Check this box to enable this port forwarding rule.
Delete	Delete this rule.
Allow ICMP packets through internal and external networks	Check this box to allow LAN hosts to send ICMP packets through port forwarding.

4 TELEPHONY

The Telephony section is used to configure SIP Parameters, telephony settings (including regional settings) and line diagnostics.



Telephony

- Profile Config
- Port Config
- Region&Misc Config
- Line Diagnostics

Profile List

No.	Profile Name	Proxy	Domain	Outbound Proxy		
1	VSP12K	172.16.180.157	172.16.180.157	✖	✎	↻
2	Profile_2			✖	✎	↻
3	Profile_3			✖	✎	↻
4	Profile_4			✖	✎	↻

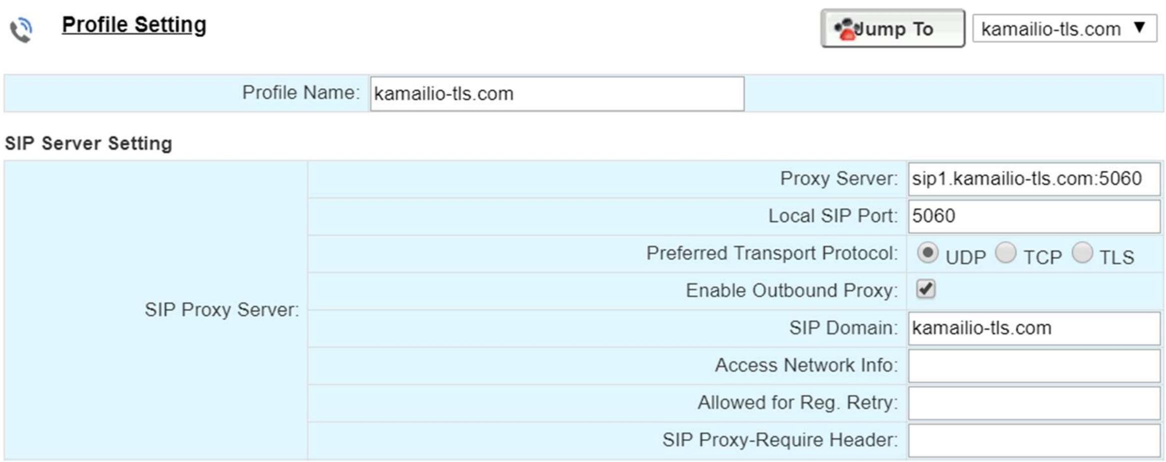
Figure 20 Configuring Telephony options

4.1 Profile Config

Profiles include SIP Server/Proxy Settings, Security Settings, Codec Settings, SIP Timer Settings, Digitmap Settings, FXS Settings, Feature and Service Code Settings, Fax Settings and Call Report Settings which are described in the following sections.

Click on the Edit icon ✎ of a particular profile to display the profile setting screen.

4.1.1 SIP Server Setting



Profile Setting

Jump To: kamailio-tls.com ▼

Profile Name: kamailio-tls.com

SIP Server Setting

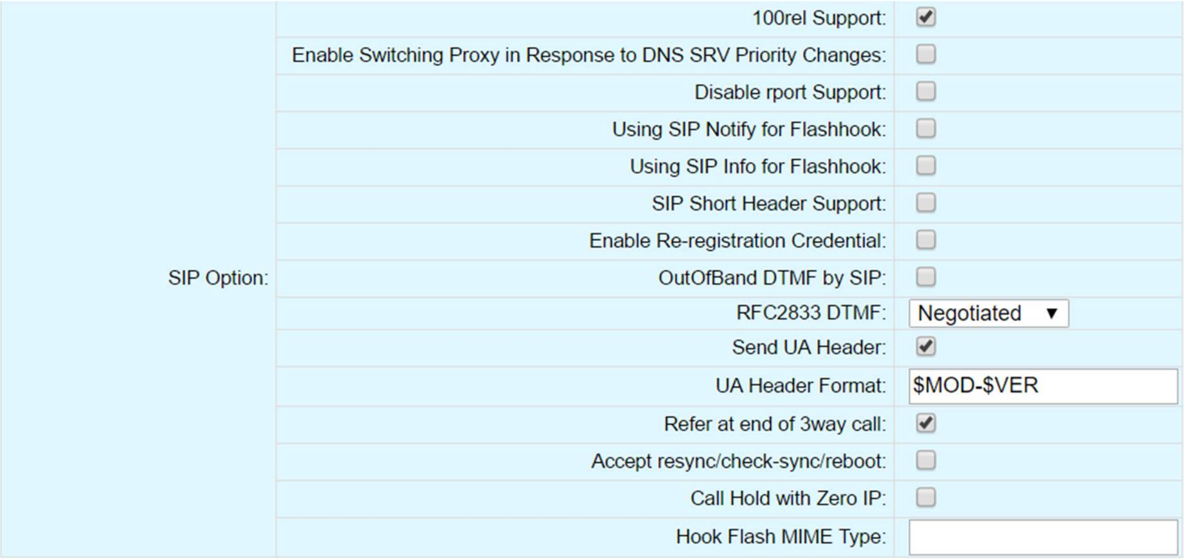
SIP Proxy Server:

Proxy Server:	sip1.kamailio-tls.com:5060
Local SIP Port:	5060
Preferred Transport Protocol:	● UDP ○ TCP ○ TLS
Enable Outbound Proxy:	☑
SIP Domain:	kamailio-tls.com
Access Network Info:	
Allowed for Reg. Retry:	
SIP Proxy-Require Header:	

Figure 21. SIP Server Setting—SIP Proxy Server

Field Name	Description
Profile Name	Up to 4 profiles can be created. (The profile ID corresponds to the No. in the Profile List.)
Proxy Server	The FQDN or IP address of the SIP proxy server
Local SIP Port	The SIP port used on the MTA
Preferred Transport Protocol	If there are no queried NAPTR records specifying the transport protocols to be used, the MTA uses this configured setting to set up VoIP calls with the SIP server.

	UDP | TCP | TLS
Enable Outbound Proxy	If enabled, the MTA uses the value configured in “Proxy Server” as the outbound proxy server setting.
SIP Domain	The MTA uses this setting to (1) compose the host part of SIP request URI strings and (2) perform NAPTR/SRV queries.
Access Network Info	This header is useful in SIP-based networks that also provide layer 2/layer 3 connectivity through different access technologies. SIP User Agents may use this header to relay information about the access technology to proxies that are providing services.
Allowed for Reg. Retry	Upon registration failure, the configured registration response SIP error codes can be used to trigger re-registration. If multiple error codes are to be used, use a comma (,) to separate them. No entry indicates registration is always retried if registration fails.
SIP Proxy-Require Header	The Proxy-Require header field is used to list features and extensions that a UA requires a proxy to support in order to process the request.



SIP Option:

100rel Support:	☑
Enable Switching Proxy in Response to DNS SRV Priority Changes:	☐
Disable rport Support:	☐
Using SIP Notify for Flashhook:	☐
Using SIP Info for Flashhook:	☐
SIP Short Header Support:	☐
Enable Re-registration Credential:	☐
OutOfBand DTMF by SIP:	☐
RFC2833 DTMF:	Negotiated ▼
Send UA Header:	☑
UA Header Format:	$MOD-$VER
Refer at end of 3way call:	☑
Accept resync/check-sync/reboot:	☐
Call Hold with Zero IP:	☐
Hook Flash MIME Type:	

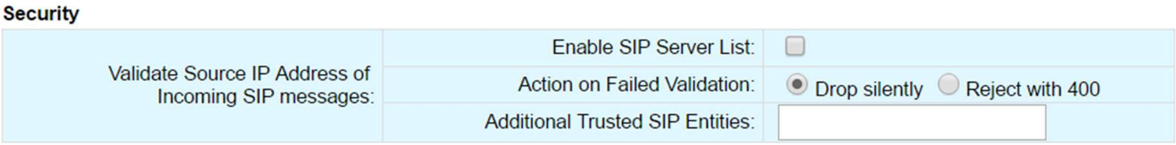
Figure 22. SIP Server Settings – SIP Option

Field Name	Description

100rel Support	Enable 100rel response support.
Enable Switching Proxy in Response to DNS SRV Priority Change	When this item is enabled, whenever the MTA is ready to send a REGISTER request and the SRV TTL has expired, it performs an SRV query and the MTA will switch to the most preferred SIP server (lowest priority) in the SRV query response. If this item is disabled, the MTA stays with the currently registered SIP proxy and only saves the SRV query results. However, if the current SIP proxy is unreachable, or the MTA reboots and starts a new DNS query process, the MTA will then register to the most preferred SIP server (lowest priority) in the SRV query response.
Disable rport Support	Do not append rport (response port number) in the Via header.
Using SIP Notify for Flashhook Support	Send a SIP NOTIFY hook flash event message during the call when a hook flash is detected.
Using SIP Info for Flashhook Support	Send a SIP INFO hook-flash event message during the call when a hook flash is detected.
SIP Short Header Support	Send SIP Headers in short format (compact form) to reduce message packet size.
Enable Re-registration Credential	Enable Re-registrations to carry the previous successful authentication credentials.
OutOfBand DTMF by SIP	Use SIP INFO to send DTMF.
RFC2833 DTMF	Use RFC2833 for sending DTMF digits. Available options: • Negotiated – MTA and SIP Server negotiate if RFC2833 is enabled or not. • Always off – RFC2833 is never used. • Always on – RFC2833 is always used.
Send UA Header	Allow MTA to send User-Agent Header in SIP message.
UA Header Format	User-Agent Header sent out is modifiable. (Note: If “SIP Short Header Support” is enabled, there will be no UA Header in SIP messages.) Available parameters:

	• Model name ($MOD) • MAC ($MAC) • Version ($VER) Example Syntax: $MOD $MAC $VER. Output: SIP User-Agent: MTA-8328-1N 001099112233 V1.0.0.0
Refer at End of 3way Call	Send REFER when mixer (local MTA) hangs up, so the other two parties can continue the conversation.
Accept resync/check-sync/reboot	When enabled, the MTA device supports events triggered by SIP NOTIFY messages sent to the MTA from the SIP server. Event types are: (1) check-sync. MTA reboots itself and starts provisioning process. (2) reboot. MTA reboots itself (and starts provisioning process). (3) resync. MTA starts provisioning process only.
Call Hold with Zero IP	Use 0.0.0.0 in SDP for call hold.
Hook Flash MIME Type	Input the MIME type string for Flash hook events.

4.1.2 Security Setting



Security

Validate Source IP Address of Incoming SIP messages:

Enable SIP Server List: □

Action on Failed Validation: ● Drop silently ○ Reject with 400

Additional Trusted SIP Entities:

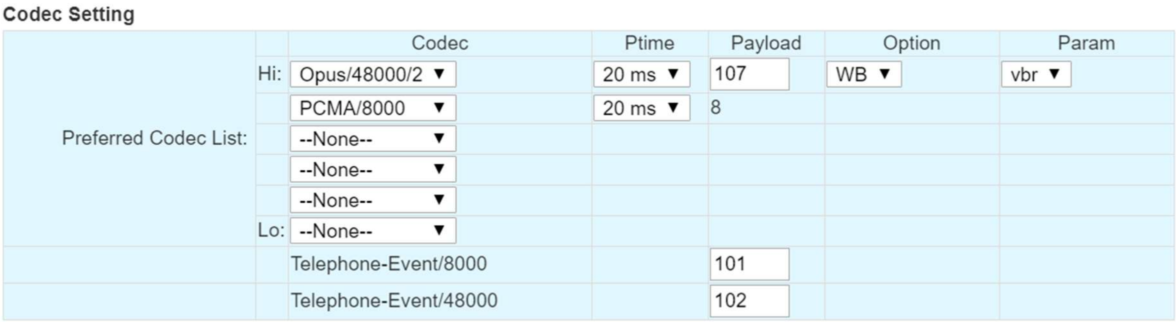
Figure 23. MTA Security Settings

Field Name	Description
Enable SIP Server List	When this feature is enabled, the MTA checks all incoming out-of-dialog SIP request messages for their source IP addresses. If the source IP is not in the "SIP Server list", the MTA rejects or drops this message. The MTA initially creates a "SIP Server list" which contains the IP addresses resolved from the settings of "Proxy Server", "SIP Domain" and the "EMS Server". See also below for adding additional Trusted SIP entities.

Action on Failed Validation	Drop silently. The MTA simply drops the incoming out-of-dialog SIP request messages. Reject with 400. The MTA replies with an error SIP response code of 400 to the sender.
Additional Trusted SIP Entities	Input one or more addresses (IP or FQDN) for additional servers from which the MTA will accept incoming SIP messages. These servers are in addition to those in the "SIP Server List" which the MTA automatically creates (see above).

4.1.3 Codec Setting

Configure voice codecs allowed by service providers for telephony services.



Codec Setting

		Codec	Ptime	Payload	Option	Param
Preferred Codec List:	Hi:	Opus/48000/2 ▼	20 ms ▼	107	WB ▼	vbr ▼
		PCMA/8000 ▼	20 ms ▼	8		
		--None-- ▼				
		--None-- ▼				
		--None-- ▼				
	Lo:	--None-- ▼				
		Telephone-Event/8000		101		
		Telephone-Event/48000		102		

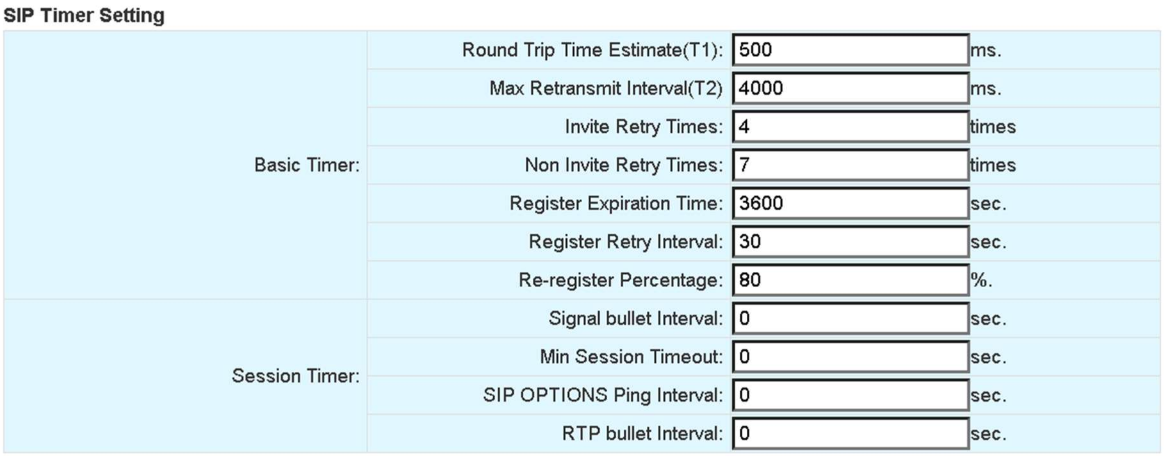
Figure 24. Codec Setting

Field Name	Description
Preferred Codec List	List the Codecs to be enabled for this profile and their order of importance. Available Codecs: • PCMU/8000 – Set Ptime • PCMA/8000 – Set Ptime • G729/8000 – Set Ptime and annexb on or off • G722/8000 – Set Ptime • iLBC/8000 – Set Ptime, dynamic payload type, and mode (codec frame size, 20ms or 30ms) • Opus/48000/2 - Set Ptime, dynamic payload type, wideband|narrowband mode, and vbr (variable bit rate)|cbr (constant bit rate).

Telephone-Event	Configure payload type for Telephony Events. Two options available. • Telephone-Event/8000: for use with codecs operating at a 8000Hz RTP timestamp clock rate • Telephone-Event/48000: for use with codecs operating at a 48000Hz RTP timestamp clock rate

4.1.4 SIP Timer Setting

SIP timers define transaction expiration timers, retransmission intervals when UDP is used as a transport, and the lifetime of dynamic TCP connections. The retransmission and expiration timers correspond to the timers defined in RFC 3261.



SIP Timer Setting

Basic Timer:	Round Trip Time Estimate(T1):	500	ms.
	Max Retransmit Interval(T2)	4000	ms.
	Invite Retry Times:	4	times
	Non Invite Retry Times:	7	times
	Register Expiration Time:	3600	sec.
	Register Retry Interval:	30	sec.
	Re-register Percentage:	80	%.
Session Timer:	Signal bullet Interval:	0	sec.
	Min Session Timeout:	0	sec.
	SIP OPTIONS Ping Interval:	0	sec.
	RTP bullet Interval:	0	sec.

Figure 25. SIP Timer Setting

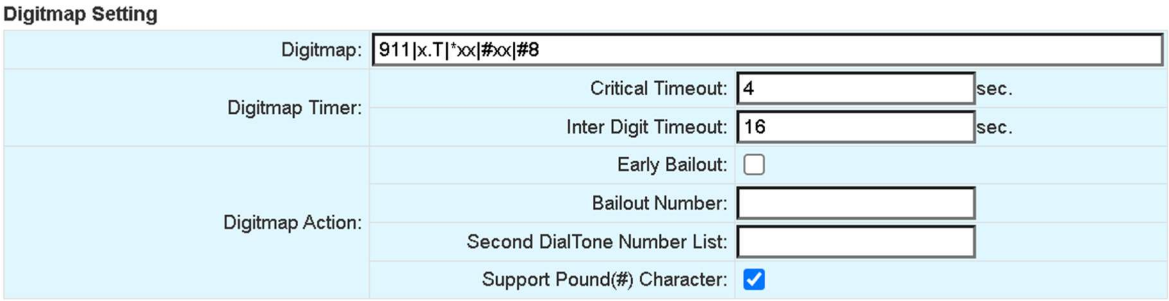
Basic Timer	Description
Round Trip Time Estimate (T1)	Estimated time it takes for a packet to make a round trip from the device to the far end and back.
Max Retransmit Interval (T2)	The maximum retransmit interval for non-INVITE requests and INVITE responses.
Invite Retry Times	The maximum number of times that a SIP INVITE is retransmitted if no response is received. According to RFC3261, INVITE requests are retransmitted at an interval which starts at T1 and doubles until it hits T2, and then repeats at interval T2. The MTA stops retries when a 32 second cap is reached, or the max number of INVITE retries has been attempted.
Non Invite Retry Times	The maximum number of times that a SIP message other than an INVITE request is retransmitted if no response is received.

	According to RFC3261, Non-INVITE requests are retransmitted at an interval which starts at T1 and doubles until it hits T2, and then repeats at interval T2. The MTA stops retries when a 32 second cap is reached, or the max number of non-INVITE retries has been attempted.
Register Expiration Time	Time to wait after a registration before it expires. • Generic SIP version: If the timer is set to be x seconds, the MTA re-registers at $ReregisterPercentage% of the expiration time (e.g., x*90% seconds). • IMS version: If value is greater than 1200 sec, the MTA will re-register 600 seconds before registration time expires. If less than or equal to 1200 seconds, it will re-register when half of the expiration time expires.
Register Retry Interval	The time interval in seconds in which the SIP Device will retry registration when the retry interval expires, after a SIP Registration failure, as long as the “retry-after” SIP header field is non-zero. This behavior is also dependent on the “Allowed for Reg. Retry” (in section 4.1.1) configuration as this determines if the MTA will retry registration.
Re-register Percentage	Configure the time for the MTA to Re-register based on the percentage of the value of Registration Expiry Time.
Session Timer	**Description**
Signal bullet Interval	Time between sending dummy keep-alive UDP packets. Set to 0 to disable sending out signaling bullet packets
Min Session Timeout	Enable session Audit.
SIP OPTIONS Ping Interval	Time interval between sending SIP OPTIONS ping messages.
RTP bullet Interval	Time between sending an empty keep-alive RTP packet to keep a port open. Set to 0 to disable sending out RTP bullet packets.

4.1.5 DigitMap Setting

Digitmaps are templates that match different sequences of digits that users dial as part of their interaction with their phone system. After the user dials, when there is a match between the digits dialed and the digitmap, the MTA device sends the digits to the server to initiate the call. If there is no match, the system waits for the user to enter more digits or press the send key to indicate dialing is complete.

Load the SIP device with the digitmap pattern which corresponds to the dial plan selected by the service operator. The digitmap is expressed in a format derived from the UNIX system command, "egrep." You must build the digit map based on the dialing plan which you wish to support.



Digitmap Setting

Digitmap: 911|x.T|*xx|#xx|#8

Digitmap Timer:
Critical Timeout: 4 sec.
Inter Digit Timeout: 16 sec.

Digitmap Action:
Early Bailout: □
Bailout Number:
Second DialTone Number List:
Support Pound(#) Character: ☑

Figure 26. Digitmap Setting

Digitmap	Description
Digitmap	Define patterns of dial strings that the MTA can send to the SIP server when the pattern has been met, and not have to wait for the InterDigit Time out or the Critical Timeout. This helps improve call completion times.
Digitmap Timer	Inter Digit Timeout value should be greater than that of Critical Timeout value
Critical Timeout	Short timeout if match digitmap T pattern.
Inter Digit Timeout	Time to wait between digits being dialed before assuming no more entries are to be made. This is required to ensure a pause in dialing does not trigger an incomplete number to be sent to the SIP server.
Digitmap Action	
Early Bailout	If a dialed number does not match any digitmap pattern, call a predefined bailout number. This number may be configured as an announcement to inform the user that this is an invalid number.
Bailout Number	The outgoing number when early bailout is enabled.
Second DialTone Number List	Once the Secondary Dial Tone (SDT) prefix is matched, the user hears a secondary dial

	tone. Digits dialed after this point will be collected and sent out, prepended with the SDT prefix if the dialed digits match a digitmap pattern.
Support Pound (#) Char	This feature only controls the "#" at the end of a dialed string. If this feature is enabled, pressing pound (#) after dialing numbers will cause the MTA to dial out immediately without waiting for the expirations of associated timers, e.g., "Critical Timeout" and "Inter Digit Timeout". If this feature is disabled, and there are associated digitmap rules ended with a "#" sign, the MTA sends out "%23", which is equivalent to "#".

4.1.5.1 A Digitmap Example

0	Local operator
00	Long distance operator
[1-7]xxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
[0-9*].#	Any dialed numbers followed by a “#” sign
*xx	Star services
91xxxxxxxxxx	Long distance number
9011 + up to 15 digits	International number

The dial plan described above results in the following digit map:

(0| 00|[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxx|9011x.T|[0-9*].#)

4.1.5.2 Digitmap syntax

A DigitMap, according to this syntax, is defined either by a (case insensitive) “String” or by a “list of strings” over which the SIP Device will attempt to find a shortest possible match. Regardless of the above syntax, a timer is currently only allowed if it appears in the last position in a string. Each string in the list is an alternate numbering scheme.

The formal syntax of the digit map is described by the following notation:

Digit ::= “0” | “1” | “2” | “3” | “4” | “5” | “6” | “7” | “8” | “9”

Timer ::= “T” | “t” -- matches the detection of a timer

Letter ::= Digit | Timer | “#” | “*” | “A” | “a” | “B” | “b” | “C” | “c” | “D” | “d”

Range ::= “X” | “x” -- matches any single digit

| “[“ Letters “]” -- matches any of the specified letters

Letters ::= Subrange | Subrange Letters

Subrange ::= Letter -- matches the specified letter

| Digit “-” Digit -- matches any digit between first and last

Position ::= Letter | Range

StringElement ::= Position -- matches an occurrence of the position

| Position “.” -- matches an arbitrary number of occurrences of the position, including 0

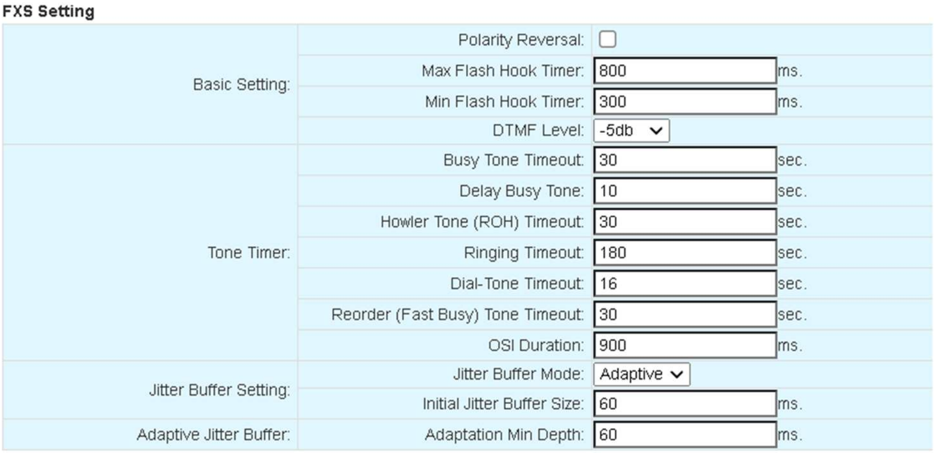
String ::= StringElement | StringElement String

StringList ::= String | String “|” StringList

DigitMap ::= String | “(“ StringList “)"

4.1.5.3 FXS Setting

FXS port configuration allows you to set parameters based on the requirements of the telephony connection. You can alter the default settings and fine-tune the parameters for specific needs. For example, you might need to configure the ring timeout duration dependent on your needs. You can set the following configuration parameters for an FXS port:



FXS Setting

Basic Setting:	Polarity Reversal:	□	
	Max Flash Hook Timer:	800	ms.
	Min Flash Hook Timer:	300	ms.
	DTMF Level:	-5db	
Tone Timer:	Busy Tone Timeout:	30	sec.
	Delay Busy Tone:	10	sec.
	Howler Tone (ROH) Timeout:	30	sec.
	Ringing Timeout:	180	sec.
	Dial-Tone Timeout:	16	sec.
	Reorder (Fast Busy) Tone Timeout:	30	sec.
	OSI Duration:	900	ms.
Jitter Buffer Setting:	Jitter Buffer Mode:	Adaptive	
	Initial Jitter Buffer Size:	60	ms.
Adaptive Jitter Buffer:	Adaptation Min Depth:	60	ms.

Figure 27. FXS Setting

Field Name	Description
Basic Setting	
Polarity Reversal	Enable Polarity Reversal – Tip and Ring are reversed when a call is answered.
Max Flash Hook Timer	The maximum flash hook cannot last more than X ms for the MTA to treat it as a Flash Hook.
Min Flash Hook Timer	The minimum flash hook needs to last at least X ms before MTA treats it as a Flash Hook.
DTMF Level	The level of Dual Tone Multi Frequency tones.
Tone Timer	
Busy Tone Timeout	Busy Tone will play for xx seconds and then drop the call.
Delay Busy Tone	If the phone is in an off hook state, the time duration that the MTA waits before playing busy tone.
Howler Tone (ROH) Time out	Will play Howler tone for this period of time and then become silent.
Ringing Timeout	Will ring a line for this period of time and then cancel the call.
Dial-Tone Timeout	Will play Dial Tone for this period of time and then play fast busy.

Reorder (Fast Busy) Tone Time Out	Will play fast busy tone for this period of time and then play Howler tone.
OSI Duration	When a call is terminated, place line in open circuit for X ms. A value of 0 disables OSI.
Jitter Buffer Setting	
Jitter Buffer Mode	• Adaptive – Jitter Buffer Size changes during the call in response to network conditions. • Fixed – Jitter Buffer Size stays at the programmed value. • NetEQ–when NetEQ is selected, the 'Initial Jitter buffer size,' and 'adaptation Min Depth' values are not used.
Initial jitter buffer size	The initial jitter buffer size in ms.
Adaptation Min Depth	If network conditions are good, and no late packets are detected, the jitter buffer will continue to decrease until it meets the configured size.

4.1.6 Emergency Service Setting

This section is specific to the MTA8328-MP series. For emergency calling on the MTA8328-1N/W or MTA8338-1N, see section 4.1.8.

The MTA8328-MP series supports Geolocation Services for Emergency Calling. A general, high-level outline of the overall flow for Geolocation Services is provided in the following diagram:

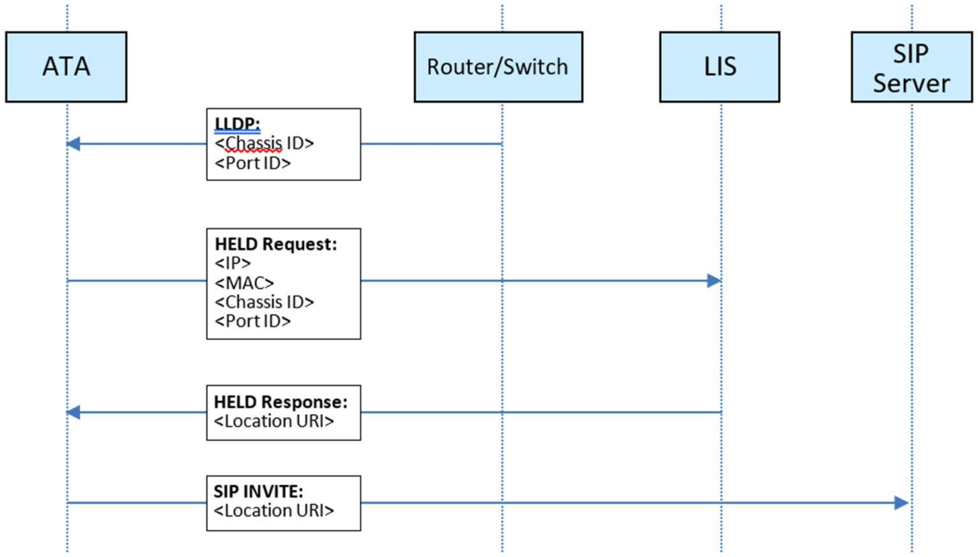


Figure 28. Overall Message Flow for Geolocation Services

Phase 1: LLDP

- The MTA8328-MP listens to LLDP packets from the switches and routers in the network and, from these packets, it determines the router/switch's Chassis ID and Port ID.

Phase 2: HELD

- The MTA then initiates a HELD request to the Location Information Server (LIS) and provides its own IP address, MAC address and the Chassis ID/Port ID from the LLDP step above.
- Based on these parameters, the LIS responds and provides the MTA with the Location URI (this is "location-by-reference" in terms of the Geolocation RFC's).

Phase 3: SIP INVITE

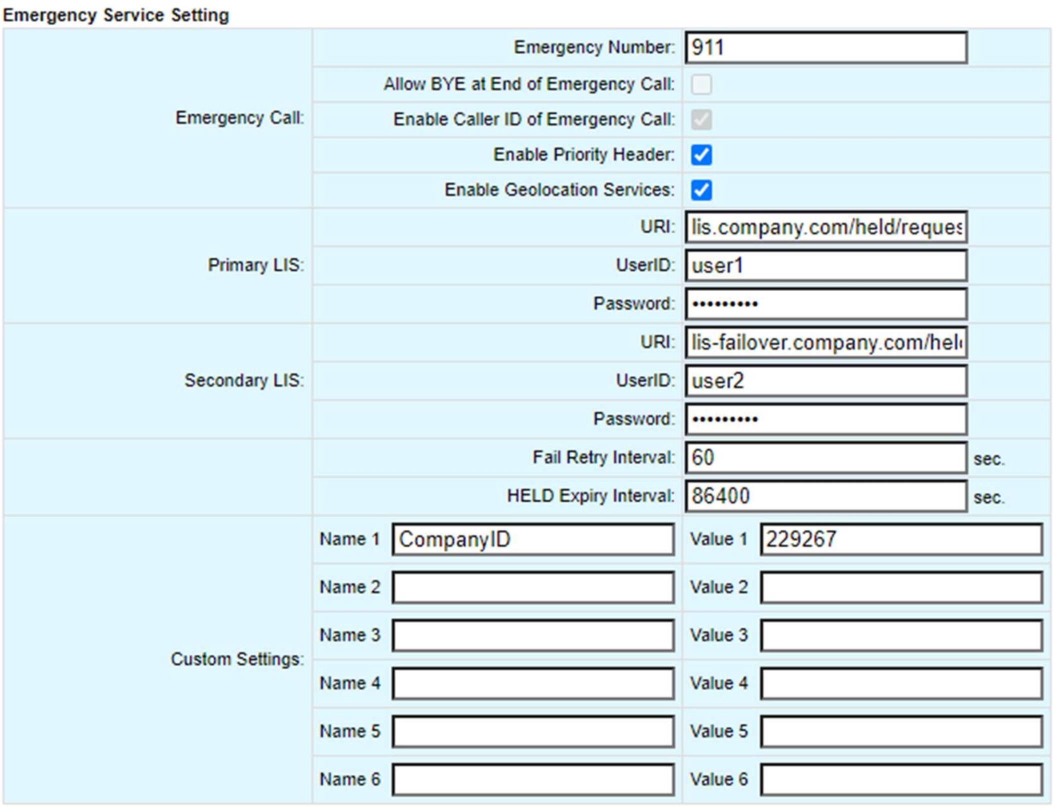
- For each outgoing SIP INVITE to an emergency number, the MTA includes the Location URI and sends it to the SIP server.

Phase 4: Location Dereferencing

- The SIP server passes the Location URI to the remote SIP UA which, acting as the Location Recipient (LR), uses the Location URI to dereference the location of the Target (MTA in this case) and obtain a Location Object (PIDF-LO).
- As described in RFC6442, this dereferencing may be done either using a SIP SUBSCRIBE to the Location URI and the resulting NOTIFY should contain the PIDF-LO, or through an HTTP GET to the Location URI and the resulting 200 message contains the PIDF-LO.
- It is important to note that the MTA is not involved in this phase at all, and so this phase does not constitute part of the Geolocation Services functionality provided by the MTA.

It should also be noted that Phases 1 and 2 are performed by the MTA at boot-up (and then at regular intervals thereafter), while Phase 3 is performed for each outgoing emergency call.

As mentioned earlier, the above outline of Geolocation Services is highly simplified. For a more detailed description of the functionality, please refer to the App Note: "Geolocation Services for Emergency Calling on the InnoMedia ATA".



Emergency Service Setting

Emergency Call:	Emergency Number:	911
	Allow BYE at End of Emergency Call:	☐
	Enable Caller ID of Emergency Call:	☑
	Enable Priority Header:	☑
	Enable Geolocation Services:	☑
Primary LIS:	URI:	lis.company.com/held/reques
	UserID:	user1
	Password:	•••••••••
Secondary LIS:	URI:	lis-failover.company.com/hel
	UserID:	user2
	Password:	•••••••••
	Fail Retry Interval:	60 sec.
	HELD Expiry Interval:	86400 sec.

Custom Settings:	Name 1	CompanyID	Value 1	229267
	Name 2		Value 2	
	Name 3		Value 3	
	Name 4		Value 4	
	Name 5		Value 5	
	Name 6		Value 6	

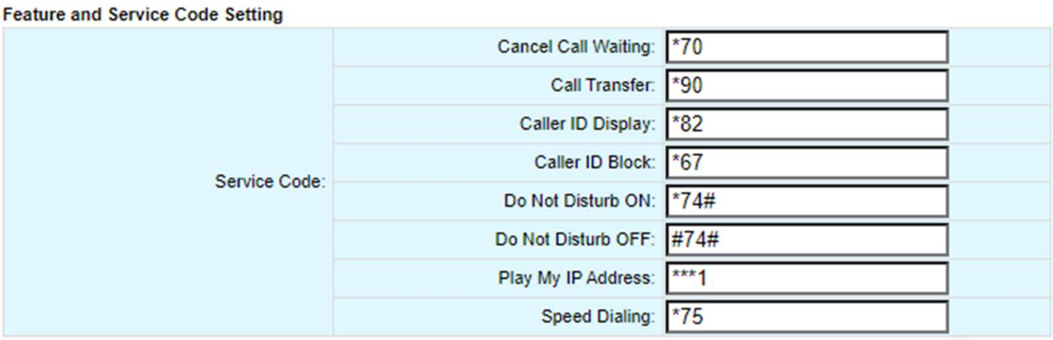
Figure 29. Emergency Service Setting

Field Name	Description
Emergency Number	If the entered number is dialed, all call features are disabled. (Call Waiting, Call Transfer, etc…)
Allow BYE at End of Emergency Call.	If enabled, when you hang up a call to an emergency number, treat this as a normal call hang-up. If it is disabled, the MTA will ring the phone when you hang up instead of terminating the call.
Enable Caller ID of Emergency Call	If Caller ID is enabled, on an outbound call to the Emergency Number, Caller ID will be sent.
Enable Priority Header	Enable/Disable use of SIP Priority header. When enabled, Priority header is set to “emergency” for calls to the emergency number.
Enable Geolocation Services	Enable/Disable use of Geolocation Services. If this box is unchecked, the remaining entries below it are not visible.

Primary/Secondary LIS URI	URI for the primary/secondary LIS. Use of 'HTTP' or 'HTTPS' in the URI determines the protocol used.
Primary/Secondary LIS Username	Username for use with the primary/secondary LIS.
Primary/Secondary LIS Password	Password for use with the primary/secondary LIS.
Fail Retry Interval	Interval in secs to wait before retrying the current LIS under a 'retry failure' scenario. Range: 60 secs to 3600 secs.
HELD Expiry Interval	Value in secs to use instead of "expires" in a HELD response if: (a) duration to "expires" received is out-of-range (less than 30 mins or more than 24 hours) OR (b) HELD Expiry Interval is less than the duration to the "expires" received. Range: 1800 secs to 86400 secs.
Custom Settings	Up to 6 custom names and values that are included in the HELD request. See the figure above for an example with the name "CompanyID" set to a custom value.

4.1.7 Feature and Service Code Setting (MTA8328-MP only)

This section is specific to the MTA8328-MP series. For feature and service code settings on the MTA8328-1N/W or the MTA8338-1N, see section 4.1.8.



Feature and Service Code Setting

Service Code:	Cancel Call Waiting:	*70
	Call Transfer:	*90
	Caller ID Display:	*82
	Caller ID Block:	*67
	Do Not Disturb ON:	*74#
	Do Not Disturb OFF:	#74#
	Play My IP Address:	***1
	Speed Dialing:	*75

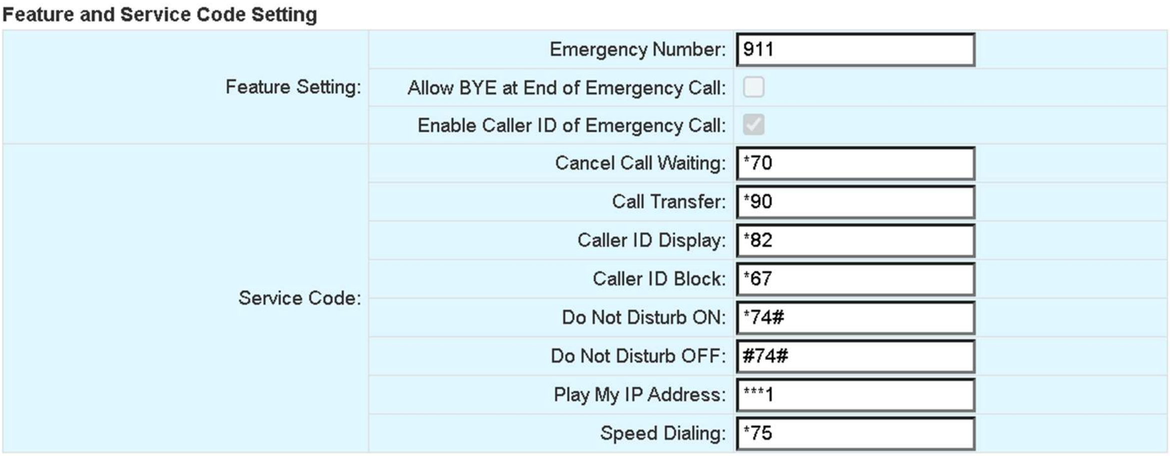
Figure 30. Feature and Service Code Setting

Field Name	Description
Service Code	The following settings are applicable to device based call features.

Cancel Call Waiting	The service code to cancel/resume receiving and answering an incoming call when this line is engaged on a call.
Call Transfer	The service code to transfer the current call to another destination.
Caller ID Display	The service code to display the incoming caller phone number and its display name.
Caller ID Block	The service code to hide the outbound caller phone number and its display name.
Do Not Disturb ON	The service code for "Do Not Disturb-On", prevents incoming calls from ringing the phone.
Do Not Disturb OFF	The service code for "Do Not Disturb-Off", allows incoming calls to ring the phone.
Play My IP Address	When a phone is connected to the MTA, and this service code is dialed, the current MTA IP address will be played out to the phone handset.
Speed Dialing	Enter a prefix to use with the Speed Dialing Settings under the Port Config section. For example, if you configure a #9 in this setting, to dial the phone number for Speed Dialing Settings 0, simply dial a #90. Ensure the Prefix and Speed Dialing Settings don't cause a dialing conflict with other features such as Call Transfer and Caller ID Display.

4.1.8 Feature and Service Code Setting (MTA8328-1N/W and MTA8338-1N only)

This section is specific to the MTA8328-1N/W and MTA8338-1N series. For emergency calling on the MTA8328-MP, see section 4.1.6. For feature and service code settings on the MTA8328-MP, see section 4.1.7.



Feature and Service Code Setting

Feature Setting:	Emergency Number:	911
	Allow BYE at End of Emergency Call:	□
	Enable Caller ID of Emergency Call:	☑
Service Code:	Cancel Call Waiting:	*70
	Call Transfer:	*90
	Caller ID Display:	*82
	Caller ID Block:	*67
	Do Not Disturb ON:	*74#
	Do Not Disturb OFF:	#74#
	Play My IP Address:	***1
	Speed Dialing:	*75

Figure 31. Feature and Service Code Setting

Field Name	Description
Feature Setting	
Emergency Number	If the entered number is dialed, all call features are disabled. (Call Waiting, Call Transfer, etc…)
Allow BYE at End of Emergency Call.	If enabled, when you hang up a call to an emergency number, treat this as a normal call hang-up. If it is disabled, the MTA will ring the phone when you hang up instead of terminating the call.
Enable Caller ID of Emergency Call	If Caller ID is enabled, on an outbound call to the Emergency Number, Caller ID will be sent.
Service Code	The following settings are applicable to device based call features.
Cancel Call Waiting	The service code to cancel/resume receiving and answering an incoming call when this line is engaged on a call.
Call Transfer	The service code to transfer the current call to another destination.
Caller ID Display	The service code to display the incoming caller phone number and its display name.
Caller ID Block	The service code to hide the outbound caller phone number and its display name.
Do Not Disturb ON	The service code for "Do Not Disturb-On", prevents incoming calls from ringing the phone.

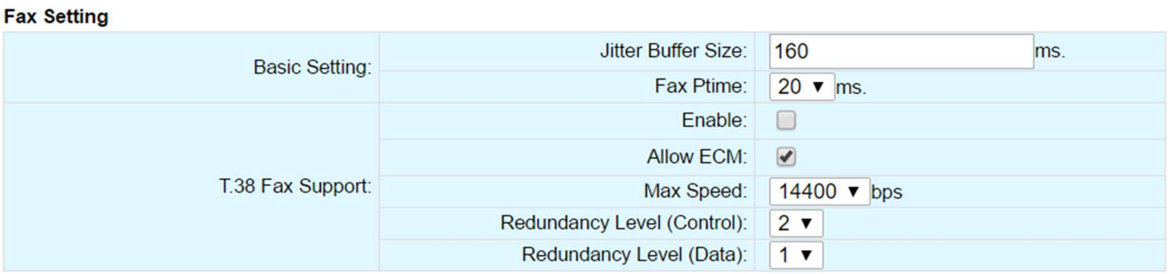
Do Not Disturb OFF	The service code for "Do Not Disturb-Off", allows incoming calls to ring the phone.
Play My IP Address	When a phone is connected to the MTA, and this service code is dialed, the current MTA IP address will be played out to the phone handset.
Speed Dialing	Enter a prefix to use with the Speed Dialing Settings under the Port Config section. For example, if you configure a #9 in this setting, to dial the phone number for Speed Dialing Settings 0, simply dial a #90. Ensure the Prefix and Speed Dialing Settings don't cause a dialing conflict with other features such as Call Transfer and Caller ID Display.

4.1.9 Fax Setting

Configure the parameters for sending and receiving a fax over the VoIP channel. Two major approaches can be used for fax over IP.

- G.711, sending fax signals in-band using the coding method used in regular voice transmissions, or
- T.38, a protocol that sends fax image data over the IP network. T38 is designed for more efficient and robust transmission compared to using the same method as voice communications.

There are pros and cons of both approaches described above. Consult your service provider for the appropriate configuration when needed.



Fax Setting

Basic Setting:	Jitter Buffer Size:	160 ms.
	Fax Ptime:	20 ▾ ms.
T.38 Fax Support:	Enable:	□
	Allow ECM:	☑
	Max Speed:	14400 ▾ bps
	Redundancy Level (Control):	2 ▾
	Redundancy Level (Data):	1 ▾

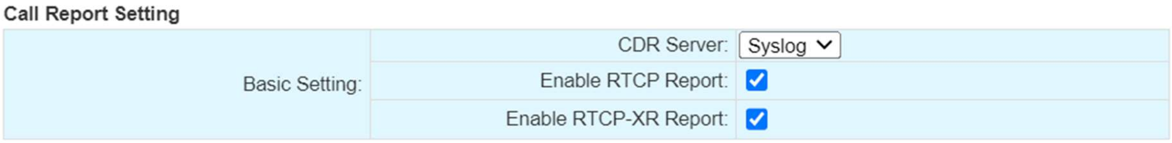
Figure 32. Fax Setting

Field Name	Description
Basic Setting	
Jitter Buffer Size	A jitter buffer temporarily stores arriving packets in order to minimize the impact of delay variations. If the jitter buffer size is too small, then an excessive number of fax packets may be discarded when network jitter occurs. If a

	jitter buffer is too large, then it introduces additional delay.
Fax PTime	Available Options: 10, 20, 30, 40, 50, 60 (ms).
T38 Setting	
Enable T38	Enable/Disable T.38 Fax feature.
Allow ECM	Enable Error Correction Mode (ECM) for fax transmission.
Max Speed	Bit Rate. Choose a maximum fax transmission speed to be attempted: 2400, 4800, 9600, or 14400.
Redundancy Level (Control)	Low Speed Redundancy. Number of redundant T.38 fax packets to be sent for the low speed V.21-based T.30 fax machine protocol. Default value is 2. Do not change the default value unless necessary.
Redundancy Level (Data)	High Speed Redundancy. Number of redundant T.38 fax packets to be sent for high-speed V.17, V.27ter and V.29 fax machine image data. Default value is 1. Do not change the default value unless necessary.

4.1.10 Call Report Setting

Configure Call Detail report setting. When a call terminates, the MTA will generate and send the CDR details of the terminated phone call to a CDR server. In addition, the MTA can send RTCP-XR reports within the call.


Call Report Setting

Basic Setting:

CDR Server: Syslog

Enable RTCP Report: ☑

Enable RTCP-XR Report: ☑

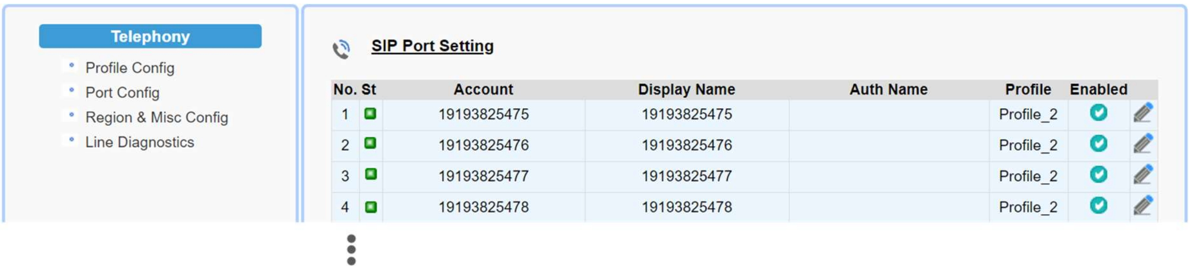
Figure 33 Call report settings

Field Name	Description
CDR Server	Send call detail records to (1) syslog server or (2) EMS server or (3) none.
Enable RTCP Report	Enable this item for the MTA to send out mid-call RTCP reports.
Enable RTCP-XR Report	Enable this item to allow the MTA to send out mid-call RTCP-XR sender reports (VoIP

	Metrics Block only) as well as end-of-call quality statistics.

4.2 Port Config

SIP Port Setting – List of current SIP user accounts. You may configure each user account from this page.



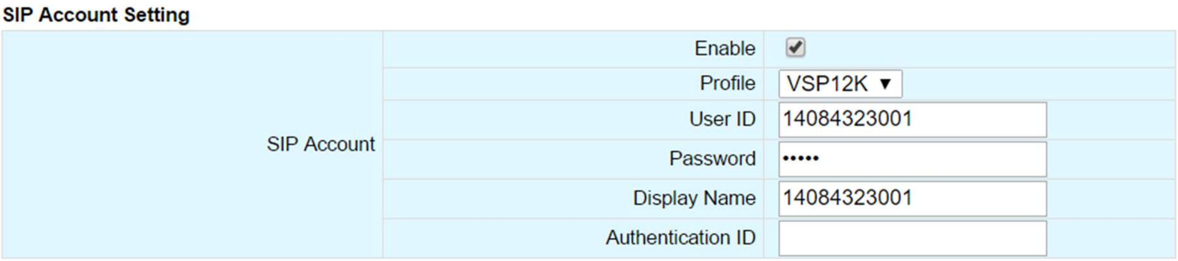
SIP Port Setting

No.	St	Account	Display Name	Auth Name	Profile	Enabled	
1	🟩	19193825475	19193825475		Profile_2	✓	✎
2	🟩	19193825476	19193825476		Profile_2	✓	✎
3	🟩	19193825477	19193825477		Profile_2	✓	✎
4	🟩	19193825478	19193825478		Profile_2	✓	✎

Figure 34. Phone port status overview

Click on the Edit icon ✎ of a particular user account to display the account setting screen.

4.2.1 SIP Account Setting



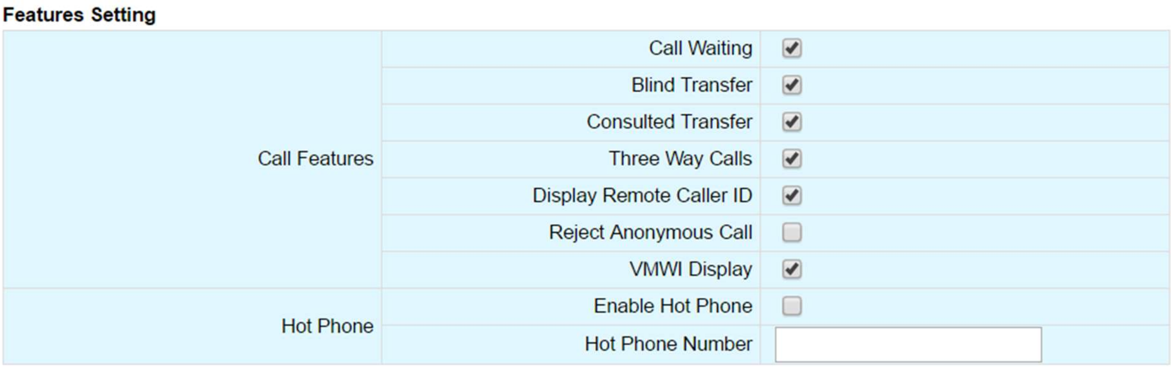
SIP Account Setting

SIP Account	Enable	☑
	Profile	VSP12K ▼
	User ID	14084323001
	Password	•••••
	Display Name	14084323001
	Authentication ID	

Figure 35. SIP Account Setting

Field Name	Description
Enable	Enable/Disable SIP User Account.
Profile	Choose which Profile Name created under Profile Config should be used for this account.
User ID	Account User ID/Name.
Password	Account Password.
Display Name	Name to be displayed for Caller ID.
Authentication ID	Authentication ID if needed.

4.2.2 Features Setting



Features Setting

Call Features	Call Waiting	☑
	Blind Transfer	☑
	Consulted Transfer	☑
	Three Way Calls	☑
	Display Remote Caller ID	☑
	Reject Anonymous Call	□
	VMWI Display	☑
Hot Phone	Enable Hot Phone	□
	Hot Phone Number	

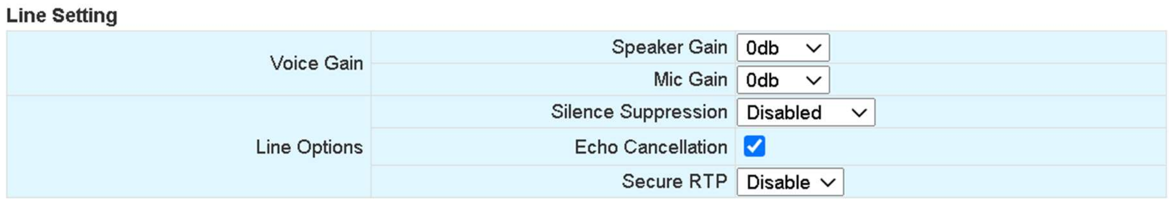
Figure 36. Call Feature Setting

Field Name	Description The following call features use “Service Codes” for device based call features defined in the “Profile Setting” page section.
Call Features	
Call Waiting	To receive and answer an incoming call when this line is engaged in an active call.
Blind Transfer	Blind transfer is when a call is routed to a third party and the original call is transferred without any check being made to determine whether the transferred call is answered or if the number is busy.
Consulted Transfer	Consulted Call Transfer is used for transferring a call to another destination without releasing the call from the voice platform until after the call is successfully transferred.
Three Way Calls	3-Way Calling connects a third person to the current two-way conversation.
Display Remote Caller ID	Display of Caller ID (the caller phone number and display name) for inbound calls from a remote party.
Reject Anonymous Call	Rejection of Anonymous inbound calls.
VMWI Display	To enable/disable MTA to display a voice mail waiting indicator.
Hot Phone	
Enable Hot Phone	Hot Phone feature that automatically dials the Hot Phone Number when the phone is taken off hook.

Hot Phone Number	Enter the phone number that the MTA dials automatically when the phone is taken off hook.

4.2.3 Line Setting

Line setting page includes input-MIC/output-speaker volume controls (gain controls) and the way silence suppression is performed.



Line Setting

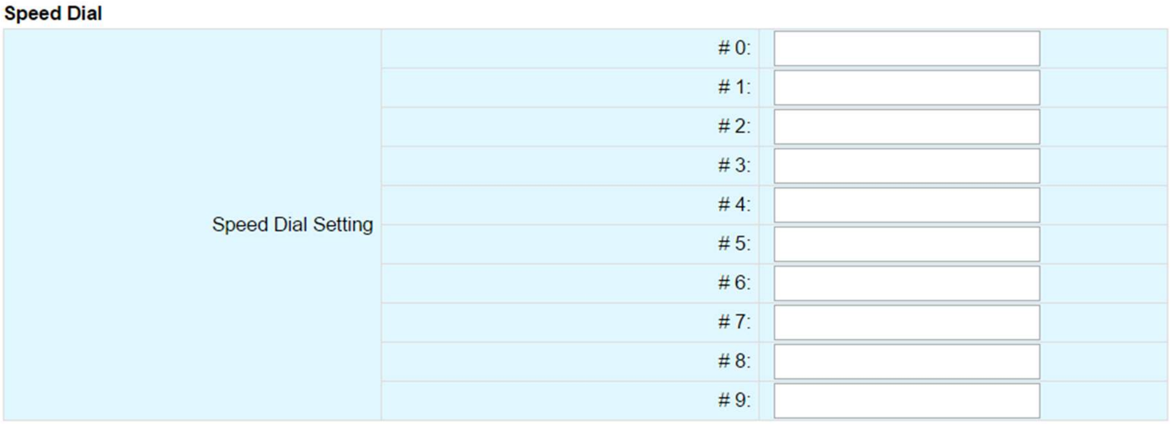
Voice Gain	Speaker Gain	0db
	Mic Gain	0db
Line Options	Silence Suppression	Disabled
	Echo Cancellation	☑
	Secure RTP	Disable

Figure 37. Line Setting

Field Name	Description
Voice Gain	
Speaker Gain	Downstream volume control in the direction from the network to the MTA's analog output.
Mic Gain	Upstream volume control in the direction from the MTA's analog input to the network.
Line Options	
Silence Suppression	Silence Suppression involves not transmitting voice packets when one of the parties involved in a call is not speaking. Available options: • Negotiated • Disabled
Echo Cancellation	Enable or disable line echo cancellation.
Secure RTP	Two options are supported: • Disabled • SRTP with SDES key management (this setting requires "TLS" to be selected as the SIP transport protocol)

4.2.4 Speed Dial

Speed dial is a function to place a call by pressing a reduced number of keys. This function is particularly useful for phone users who dial certain numbers on a regular basis. Please refer to section **Error! Reference source not found.** for more details on using speed dials.



Speed Dial

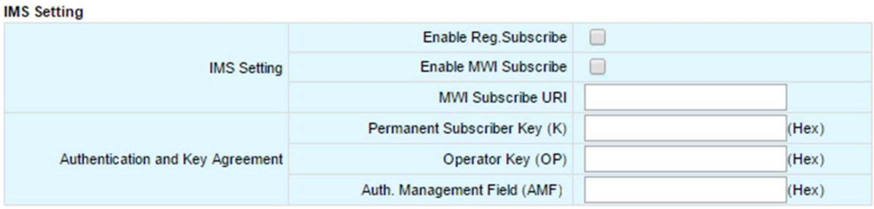
Speed Dial Setting	# 0:	
	# 1:	
	# 2:	
	# 3:	
	# 4:	
	# 5:	
	# 6:	
	# 7:	
	# 8:	
	# 9:	

Figure 38. Speed Dial

Field Name	Description
Speed Dial Testing	0-9

4.2.5 IMS related SIP settings

Only available on IMS firmware versions.



IMS Setting

IMS Setting	Enable Reg.Subscribe	□
	Enable MWI Subscribe	□
	MWI Subscribe URI	
Authentication and Key Agreement	Permanent Subscriber Key (K)	(Hex)
	Operator Key (OP)	(Hex)
	Auth. Management Field (AMF)	(Hex)

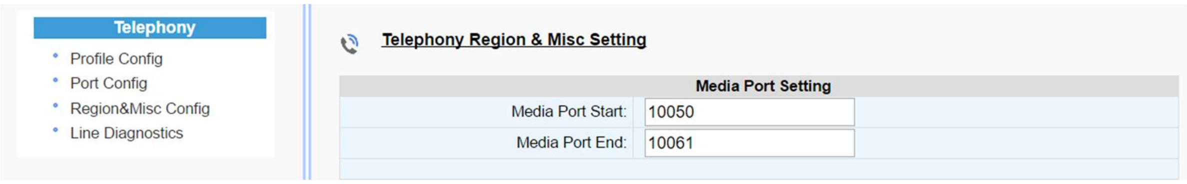
Figure 39. IMS Settings

IMS Setting	Description
IMS Setting	
Enable Reg Subscribe	The MTA subscribes to the registration event, and responds to IMS server NOTIFY messages which include AOR related information in XML format.
Enable MWI Subscribe	The MTA subscribes to the “Message Waiting Indicator” event package, as defined by 3GPP.
MWI Subscribe URI	Specify the URI of the message waiting indicator subscription server.

Authentication and Key Agreement	
Permanent Subscriber Key (K)	ISIM specific service.
Operator Key (OP)	ISIM specific service
Auth. Management Field (AMF)	ISIM specific service

4.3 Telephony Region and Misc Setting

4.3.1 Media Port Setting



Telephony Region & Misc Setting

Media Port Setting

Media Port Start: 10050

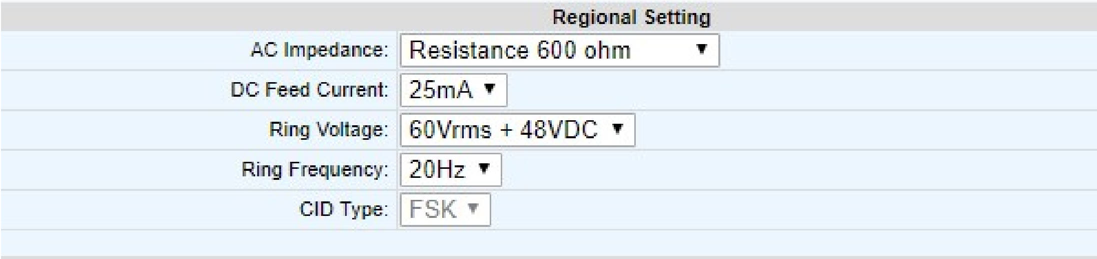
Media Port End: 10061

Figure 40. Media Port Setting

Media port starting value should fall within the range 10 to 65535 and should be an even number. Care should be taken as these settings can significantly impact voice performance or result in no voice path if configured incorrectly. Consult your telephony service provider for configuration guidelines.

Field Name	Description
Media Port Start	The lowest RTP port number to be used when sending RTP/RTCP traffic – It must be an even number.
Media Port End	The highest RTP port number to be used when sending RTP/RTCP traffic – It must be an odd number.

4.3.2 Regional Setting



Regional Setting

AC Impedance: Resistance 600 ohm ▼

DC Feed Current: 25mA ▼

Ring Voltage: 60Vrms + 48VDC ▼

Ring Frequency: 20Hz ▼

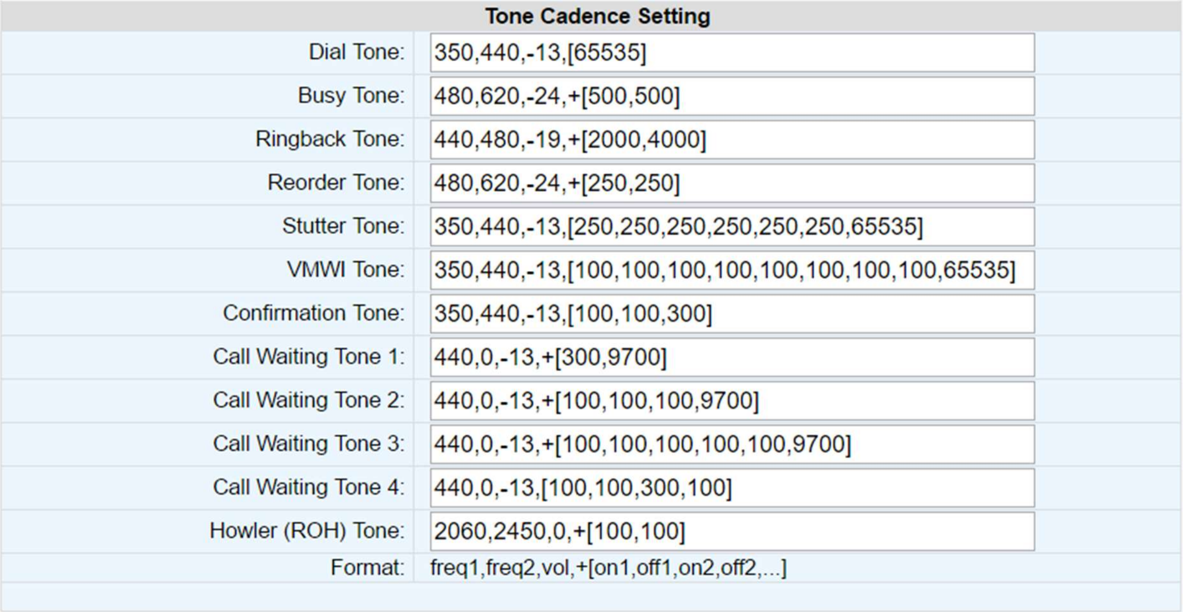
CID Type: FSK ▼

Figure 41. Regional settings for power and analog line specifications

Field Name	Description (options available)
AC Impedance	• Resistance 600 ohm • GR-57 900R+2.16uF • ETSI 270R+750R/150nF
DC Current Feed	• 25mA • 40mA
Ring Voltage	• 60Vrms +48VDC • 90Vrms Balanced
Ring Frequency	• 20Hz • 25 Hz
CID Type	Support for FSK only

4.3.3 Tone Cadence Setting

Configures the tone cadence for an FXS port. When shipped from the factory, the MTA tone cadences are set to match country requirements. You can manually set the tone cadence if you wish to override the default country values.



Tone Cadence Setting

Dial Tone:	350,440,-13,[65535]
Busy Tone:	480,620,-24,+[500,500]
Ringback Tone:	440,480,-19,+[2000,4000]
Reorder Tone:	480,620,-24,+[250,250]
Stutter Tone:	350,440,-13,[250,250,250,250,250,250,65535]
VMWI Tone:	350,440,-13,[100,100,100,100,100,100,100,100,65535]
Confirmation Tone:	350,440,-13,[100,100,300]
Call Waiting Tone 1:	440,0,-13,+[300,9700]
Call Waiting Tone 2:	440,0,-13,+[100,100,100,9700]
Call Waiting Tone 3:	440,0,-13,+[100,100,100,100,100,9700]
Call Waiting Tone 4:	440,0,-13,[100,100,300,100]
Howler (ROH) Tone:	2060,2450,0,+[100,100]
Format:	freq1,freq2,vol,+[on1,off1,on2,off2,...]

Figure 42. Tone Cadence Setting

Tone Cadence Setting

Format – freq1, freq2,vol,+[on1,off1,on2,off2,…]

- frequency 1, frequency 2, volume level in dBm
- + : loop the tone(s) forever
- [on1 duration in ms, off1 duration in ms…]. If the duration value is 65535, keep playing the last tone.

Field Name	Description
Dial Tone	A dial tone indicates that the MTA is ready to accept calls.

Busy Tone	A busy signal indicates a failure to complete the requested call. Reasons could be: • The called number is occupied, or • The other party has hung up at the end of a call.
Ringback Tone	A ring back tone (or ringing tone) is heard by the caller while the phone they are calling is being rung.
Reorder Tone	Reorder tone, also known as fast busy tone, is the congestion tone or all trunks busy tone of a PSTN network. It varies from country to country.
Stutter Tone	A "stuttered" or interrupted dial tone is often used to indicate a Calling feature such as Call forwarding has been activated. (The voice mail waiting tone is represented by VMWI Tone below.)
VMWI Tone	Voice Mail Waiting Indication, indicating that voice mail is waiting.
Confirmation Tone	Confirmation Tone is used to acknowledge receipt for special services, such as: • Speed dialing, dial number has been recorded. • Call forwarding activation and de-activation, etc.
Call Waiting Tone 1-4	Call waiting tones are used for call waiting conditions.
Howler (ROH) Tone	Receiver off hook tone

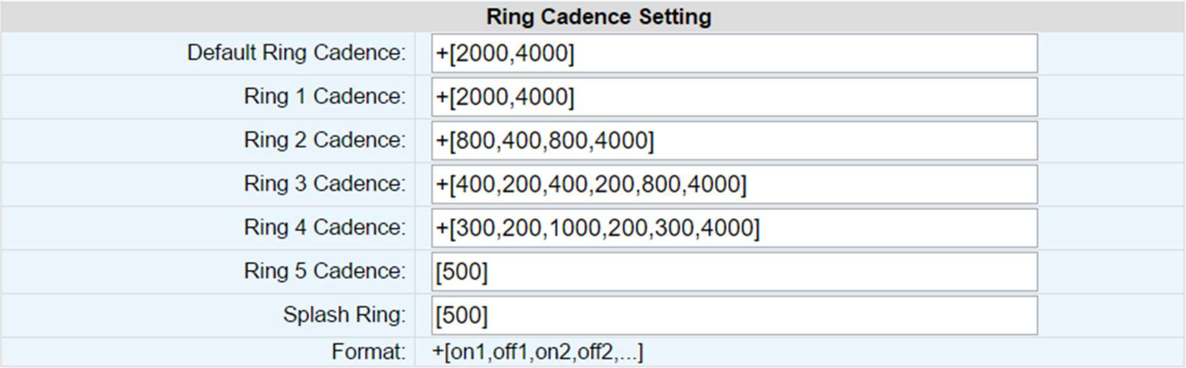
4.3.4 Ring Cadence Setting

For a telephone receiving an incoming call, ring cadence settings control the timing of the incoming ring-signal. This varies from country to country and may consist, for instance, of the ring voltage being applied for two seconds, followed by four seconds off, then back on for two seconds, and so on, until the phone is answered or the calling party hangs up, or a maximum number of rings is reached. Note that MTA supports multiple ring cadence profiles for different countries.

When shipped from the factory, the MTA’s ring cadence is set to match country requirements. You can manually set the ring cadence if you wish to override the default country values.

Ring Cadence Setting (Format +[on1,off1,on2,off2,…])

- + : loop the tone(s) forever
- [on1 duration in ms, off1 duration in ms…]. If the duration value is 65535, keep playing the last tone.



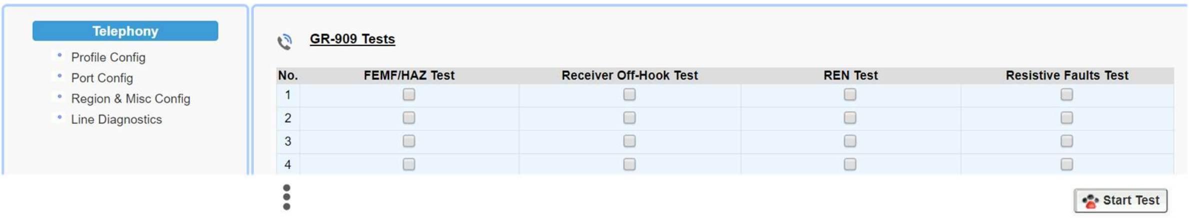
Ring Cadence Setting	
Default Ring Cadence:	+[2000,4000]
Ring 1 Cadence:	+[2000,4000]
Ring 2 Cadence:	+[800,400,800,4000]
Ring 3 Cadence:	+[400,200,400,200,800,4000]
Ring 4 Cadence:	+[300,200,1000,200,300,4000]
Ring 5 Cadence:	[500]
Splash Ring:	[500]
Format:	+[on1,off1,on2,off2,...]

Figure 43. Ring Cadence Setting

Field Name	Description
Default Ring Cadence	For a telephone receiving an incoming call, the default timing pattern of the incoming ring-signal.
Ring Cadence, 1-5	Different Ring Cadence settings for distinctive rings.
Splash Ring	A short ring to notify that some specified call features are processed. For instance, a short ring (splash tone) can be used to notify each time a call is forwarded.

4.4 Line Diagnostics

4.4.1 GR909 Tests: triggered from the WEB Administrative Console



No.	FEMF/HAZ Test	Receiver Off-Hook Test	REN Test	Resistive Faults Test
1	□	□	□	□
2	□	□	□	□
3	□	□	□	□
4	□	□	□	□

Figure 44. GR909 Line Test (illustrative example showing a four port MTA)

MTA supports GR-909 test items which use a suite of standards-based electrical tests. Click all the checkboxes for which GR909 confirmation is required. Then Click the <Start Test> button.

NOTE: If the Receiver is Off-hook, the REN Test and the Resistive Faults Test will show failures.

Field Name	Description
GR909 Line Diagnostic Test	A suite of standards-based electrical tests which detect physical problems with the phone line.
FEMF/HAZ Test	This procedure tests for hazardous electromotive force (HEMF) and foreign electromotive force (FEMF) between the

	TIP-GROUND and RING-GROUND leads. It reports a failure if the following limits are exceeded: – Foreign DC HEMF limit = 135V. – Foreign AC HEMF limit = 50Vrms. – Foreign DC EMF limit = 6V. – Foreign AC EMF limit = 10Vrms. NOTE: Once this test is initiated and if a failure is detected, the test will automatically run periodically, e.g., every 30 sec till the foreign voltage is removed.
Receiver Off-Hook Test	This procedure discriminates between resistive fault and a receiver off-hook condition by checking for a non-linear DC resistance.
REN Test	This procedure measures REN (Ringer Equivalence Number) loading by measuring the load impedance at 20 Hz. An REN loading of less than 0.175 REN or greater than 5 REN is reported as a failure.
Resistive Faults Test	This procedure measures TIP to RING on-hook DC resistance. A DC resistance less than 150 kΩ is reported as a failure.

4.4.2 GR909 Tests: triggered from SIP NOTIFY Message

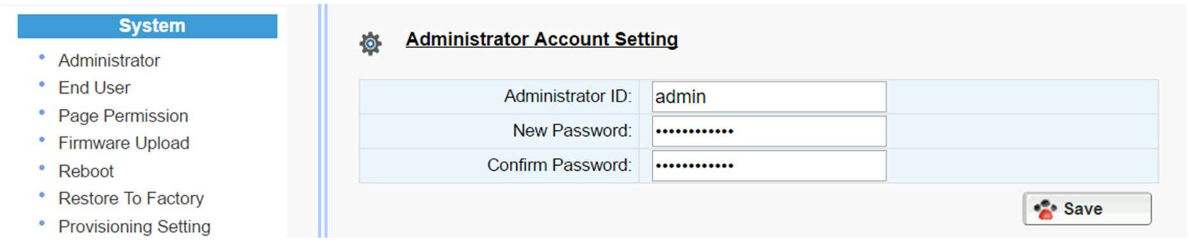
The MTA supports server-initiated GR909 tests triggered by an incoming SIP NOTIFY Message with “**Event: gr909**”. Example trace as follows:

```
NOTIFY sip:2148298788@172.16.0.119;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.16.200.212:5060;branch=z9hG4bKac101ead5060-
76517495;rport
From: <sip:GR909@172.16.200.212>;tag=rebootapp_tag
To: <sip:2148298788@172.16.0.119;user=phone>
Event: gr909
Call-ID: 3-75ff0490-4bdccd8@ac101ead
CSeq: 1401 NOTIFY
Max-Forwards: 70
Contact: <sip:GR909@172.16.200.212>
Content-Length: 0
```

5 SYSTEM

5.1 Account Settings

5.1.1 Administrator Account Setting



Administrator Account Setting

Administrator ID: admin

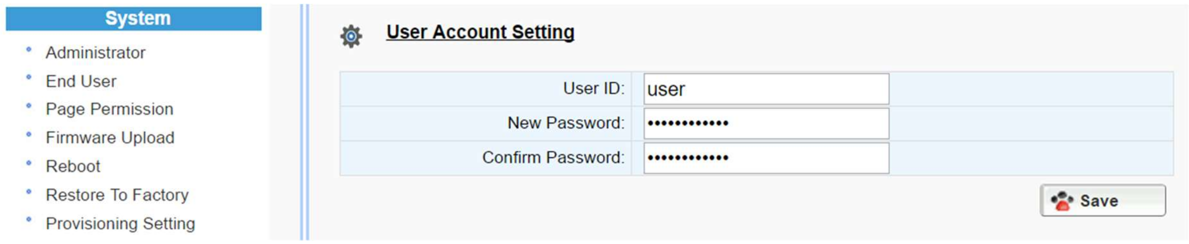
New Password: ••••••••••••

Confirm Password: ••••••••••••

Figure 45. Administrator account setting

Field Name	Description
Administrator Account Setting	This allows you to configure an Administrator ID and Password. Default ID is ‘admin’. Default Password is ‘password’. However, the default values are service provider dependent.

5.1.2 End User Account Setting



User Account Setting

User ID: user

New Password: ••••••••••••

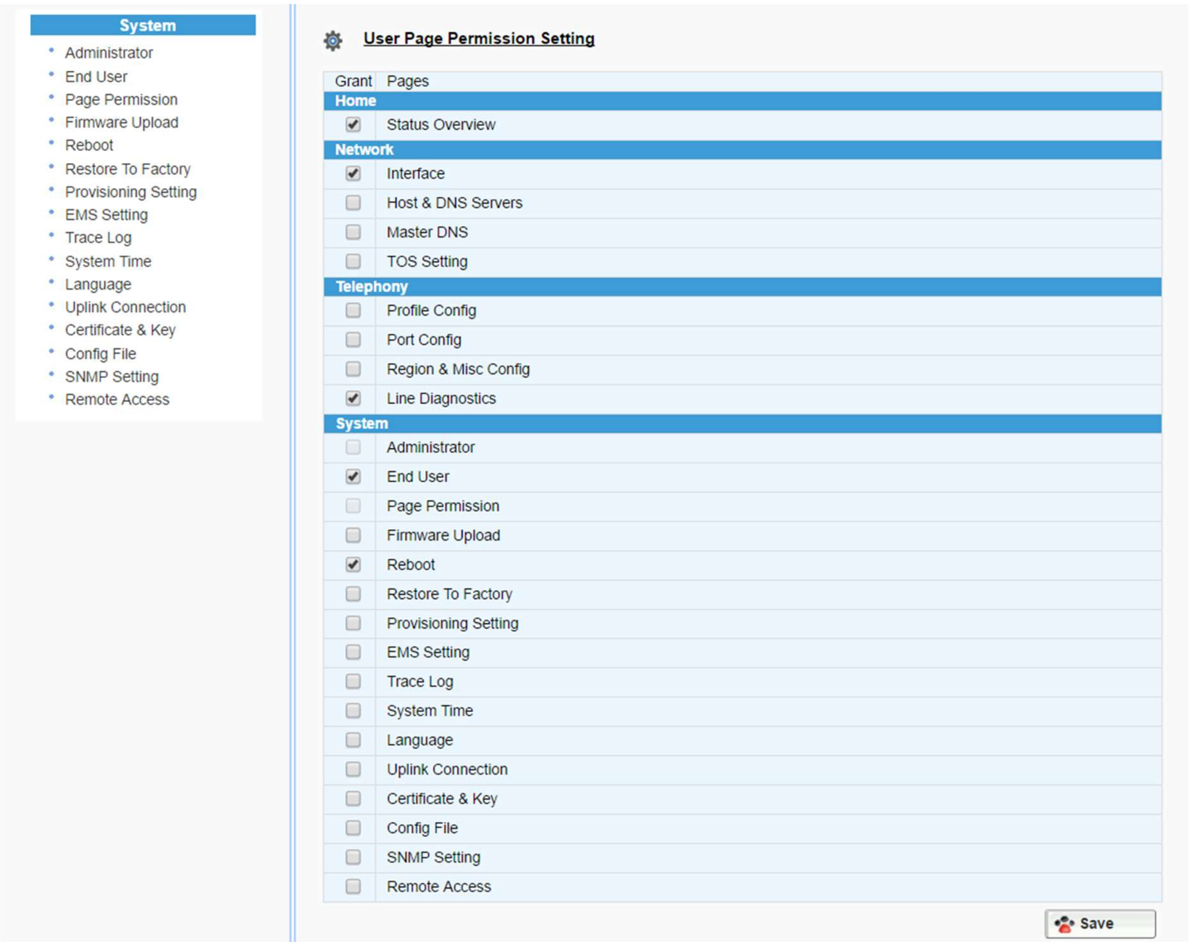
Confirm Password: ••••••••••••

Figure 46. User Account Setting

Field Name	Description
User Account Setting	This allows you to configure a user’s user ID and password. Default ID is ‘user’. Default Password is ‘welcome’. However, the default values are service provider dependent.

5.2 Page Permission

The administrator may specify which features are available for subscribers (ie users) to configure.



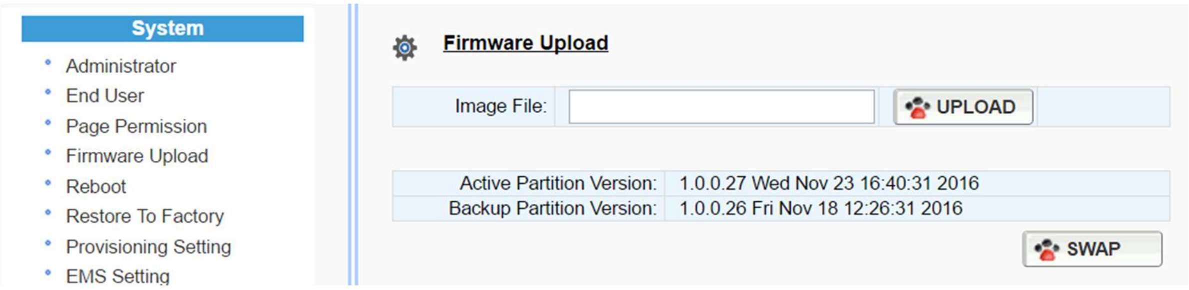
User Page Permission Setting

Grant	Pages
Home	
☑	Status Overview
Network	
☑	Interface
□	Host & DNS Servers
□	Master DNS
□	TOS Setting
Telephony	
□	Profile Config
□	Port Config
□	Region & Misc Config
☑	Line Diagnostics
System	
□	Administrator
☑	End User
□	Page Permission
□	Firmware Upload
☑	Reboot
□	Restore To Factory
□	Provisioning Setting
□	EMS Setting
□	Trace Log
□	System Time
□	Language
□	Uplink Connection
□	Certificate & Key
□	Config File
□	SNMP Setting
□	Remote Access

Figure 47. User Page Permission Setting

Field Name	Description
User Page Permission Setting	Configure which pages the User Login account can access.

5.3 Firmware Upload



Firmware Upload

Image File:

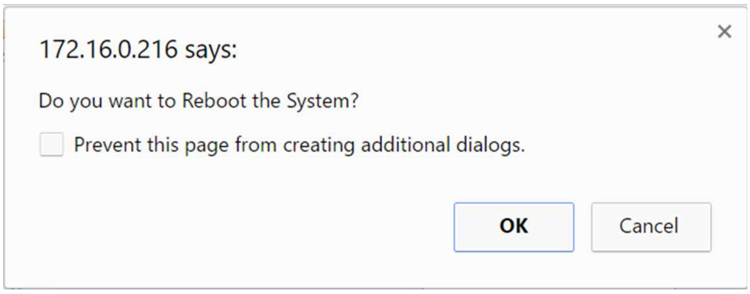
Active Partition Version: 1.0.0.27 Wed Nov 23 16:40:31 2016
Backup Partition Version: 1.0.0.26 Fri Nov 18 12:26:31 2016

Figure 48. Firmware Upload

Field Name	Description
Firmware Upload	Browse to a new firmware image file to upload to the unit.

SWAP	Click “SWAP” to switch the backup system firmware to be active.

5.4 Reboot



172.16.0.216 says:

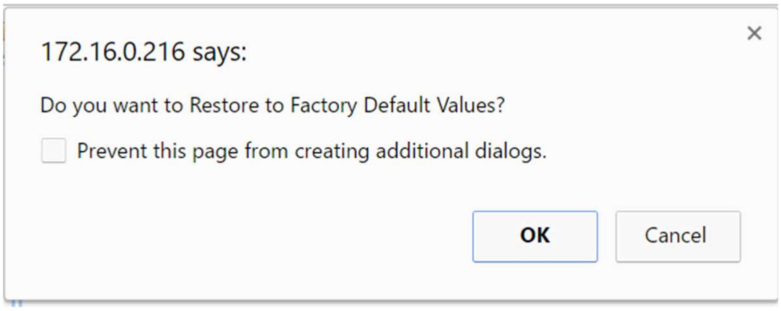
Do you want to Reboot the System?

□ Prevent this page from creating additional dialogs.

Figure 49. Reboot Dialog

Field Name	Description
Reboot	Reboot opens a dialog box, and asks for a confirmation to “Reboot the System”.

5.5 Restore To Factory



172.16.0.216 says:

Do you want to Restore to Factory Default Values?

□ Prevent this page from creating additional dialogs.

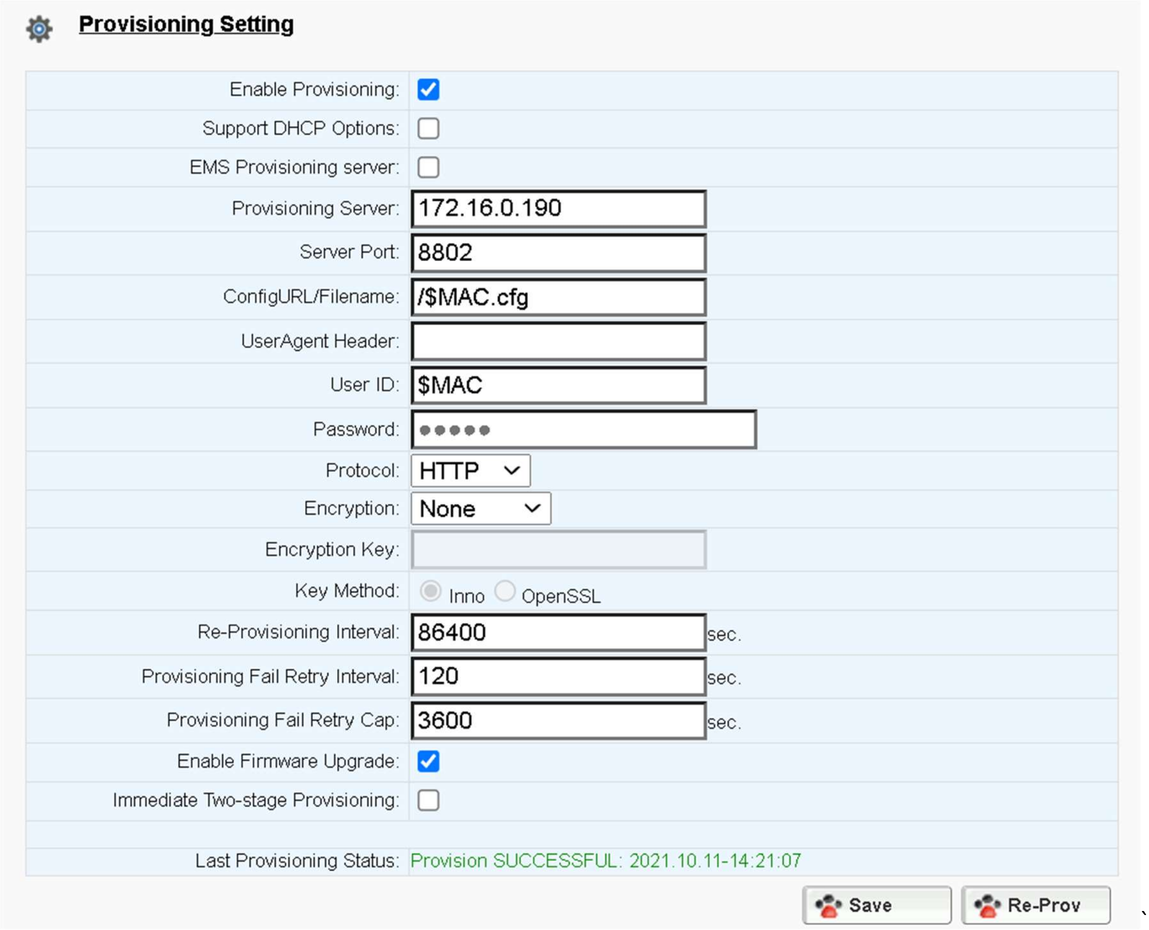
Figure 50. Restore To Factory Dialog

Field Name	Description
Restore To Factory	Opens a dialog box, and asks for a confirmation to “Restore to Factory Default Values”. The factory default values are service provider dependent.

5.6 Provisioning Setting

Provisioning Setting – Configure provisioning server and associated settings for this MTA device. Provisioning is a powerful feature that allows you to automatically configure the unit with all of its parameters. Therefore, if the unit is configured from the Factory with the desired Provisioning information, you will not need to manually configure the MTA with its SIP Profile and User Information, since the desired information can be entered into the Configuration File for that unit. Subsequently, when the device is powered on and obtains its IP address, it will go to the provisioning server and be configured.

5.6.1 Provisioning Parameters



Provisioning Setting

Enable Provisioning:	☑
Support DHCP Options:	□
EMS Provisioning server:	□
Provisioning Server:	172.16.0.190
Server Port:	8802
ConfigURL/Filename:	/$MAC.cfg
UserAgent Header:	
User ID:	$MAC
Password:	●●●●●
Protocol:	HTTP
Encryption:	None
Encryption Key:	
Key Method:	○ Inno ○ OpenSSL
Re-Provisioning Interval:	86400 sec.
Provisioning Fail Retry Interval:	120 sec.
Provisioning Fail Retry Cap:	3600 sec.
Enable Firmware Upgrade:	☑
Immediate Two-stage Provisioning:	□
Last Provisioning Status:	Provision SUCCESSFUL: 2021.10.11-14:21:07

Figure 51. Provisioning Server Setting

Field Name	Description
Enable Provisioning	Turns provisioning on/off.
Support DHCP Options	If enabled, the device will use the string (including the provisioning server FQDN and config file path) obtained from DHCP options 66 and 67 to compose the request URI for provisioning.

	See “Appendix D – Provisioning through DHCP Options” for details.
Provisioning Server	IP or FQDN of the Provisioning Server.
Server Port	Port to be used to connect to the Provisioning Server.
ConfigURL/Filename	Specify the complete path and the config file name to download.
UserAgent Header	The UserAgent header sent out is modifiable. Available parameters: • Model name ($MOD) • MAC ($MAC). The Ethernet WAN MAC address is chosen as the device ID. • Version ($VER) • Config file last loaded ($CFG) Example Syntax: $MOD $MAC $VER $CFG. Output: MTA-8328-1N 001099112233 V1.0.0.0 /Provisioning/Config/xyz.cfg
User ID	The User ID used for HTTP, FTP, and HTTPS authentication purposes
Password	The Password used for HTTP, FTP, and HTTPS authentication purposes.
Protocol	The Protocol to connect to the server. Supported protocols are: HTTP, HTTPS, FTP, and TFTP.
Encryption	The Encryption Format of the config file to be sent to the MTA. Supported formats are: None, RC4, and AES-256.
Encryption Key	The passphrase to be used for encryption.
Key Method	The following utilities (or approaches) can be used to encrypt the provisioning config file: Inno and Openssl. **Inno** – InnoMedia proprietary hash key encryption utility. This method can only be applied when “RC4” is selected from the Encryption menu. Provisioning config file should be encrypted using the utility – rc4_102 See “Appendix B The use of encryption key methods”. **Openssl** – the open source toolkit. This method can be applied when either RC4 or AES256 is selected from the Encryption

	menu. Provisioning file should be encrypted using Openssl.
Re-Provisioning Interval	Time to next Re-Provision after a successful Provision.
Provisioning Fail Retry Interval Provisioning Fail Retry Cap	There are 2 associated timers: Provisioning Fail Retry Interval : T1 Provisioning Fail Retry Cap: T2 If provisioning fails, the MTA initially retries at T1 interval, and then doubles T1 each time until it reaches T2, and then continues at this interval until the system reboots or there is a successful provisioning.
Enable Firmware Upgrade	When enabled, firmware will be downloaded when a new version is available. When disabled, firmware will not download even if a new version is available.
Immediate Two-stage provisioning	Behavior to follow when the provisioning server and/or config file path change. Enable: The MTA triggers its next provisioning immediately to the new server and/or config file (if present). This setting can be used, for instance, to set up a provisioning server re-direct whereby an initial provisioning server is configured, which then provides a config file including details of a second provisioning server that the device is re-directed towards. Disable: After a successful provisioning, the device will only re-provision after the “Re-Provisioning Interval” expires.

5.6.2 Provisioning Factory Default Settings to Devices Deployed in the Field

This section provides details of a method to provisioning factory default config files to devices.

1. Upload the factory default files to a server location where they can be accessed by devices with the appropriate protocol. There are three files (please use the exact filenames below):

• netcfg.xml.default	(settings for “Network” configuration category)
• syscfg.xml.default	(settings for “System” configuration category)
• sipcfg.xml.default	(settings for “Telephony” configuration category)

2. Configure the URL where the above config xml files can be found along with the correct access protocol in the provisioning config file.
   - Provisioning tag: System.Prov.DefaultCfgUrl (Partial url for default config xml files)
   - Syntax: *Protocol://FQDNofProvisioningServer:Port/Path*

Example:

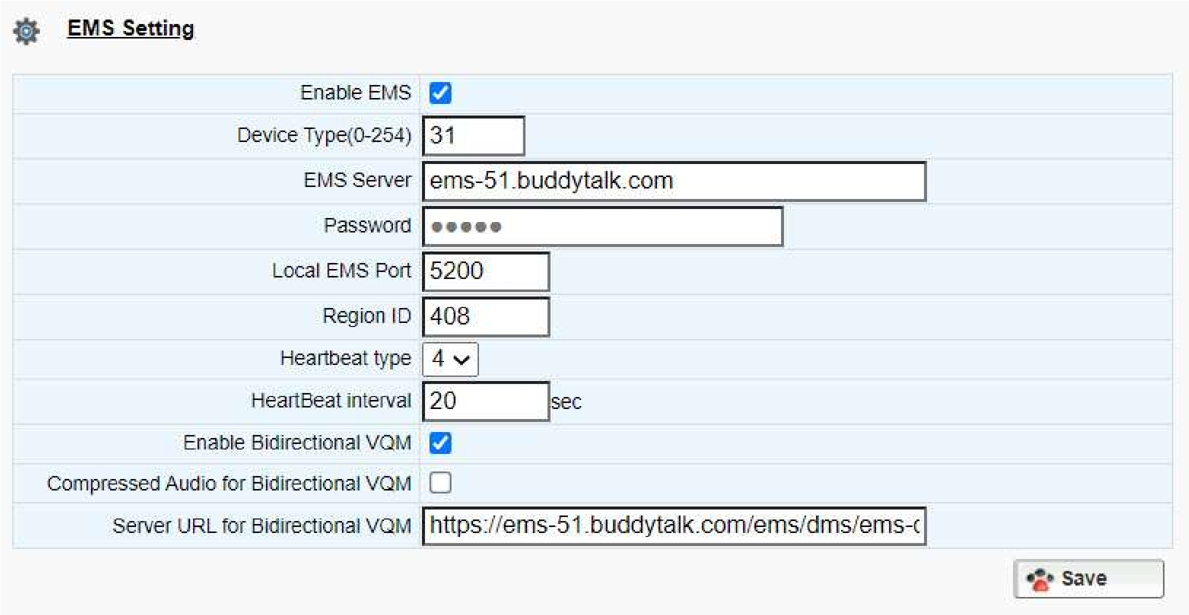
```
System.Prov.DefaultCfgUrl=”http://prov.example.com:8802/MTAFactoryDe
faultFilePath”
```

3. Optional: Trigger the restore-to-factory-default (RSTD) on the MTA right after the new factory default files have been downloaded.
   Provisioning tag: System.Prov.Restore2Default (1 : enable; 0: disable).
   Example: `System.Prov.Restore2Default=”1”`
   Note: RSTD event will only be triggered when the following two conditions are met:
   - This System.Prov.Restore2Default tag value transitions 0 to 1 (further provisioning events will not trigger an RSTD event even if this tag is left as “1”)
   - A set of factory default files has been downloaded

5.7 EMS Setting

5.7.1 EMS Server

The InnoMedia EMS server is a powerful provisioning and management platform for service providers to perform device configuration/firmware management, to be able to see Call Statistics, Voice Quality information, and to provide the ability to connect to devices behind NAT routers for diagnostics purposes.



EMS Setting

Enable EMS	☑
Device Type(0-254)	31
EMS Server	ems-51.buddytalk.com
Password	●●●●●
Local EMS Port	5200
Region ID	408
Heartbeat type	4
HeartBeat interval	20 sec
Enable Bidirectional VQM	☑
Compressed Audio for Bidirectional VQM	□
Server URL for Bidirectional VQM	https://ems-51.buddytalk.com/ems/dms/ems-(

Figure 52. Configuring EMS Server Information

Field Name	Description
Enable EMS	This enables the EMS feature.
Device Type (0-254)	This is the device type configured on the EMS Server, so that a user of the EMS server will see the device by name in the device list. The type is also important for what

	options/features will be seen when a device is queried by the EMS.
EMS Server	The IP or FQDN address of the EMS Server and port. Default is to use port 5200 for connection to the EMS server.
Password	The authentication password to connect to the EMS server.
Local EMS Port	The port number used at the MTA device in order to connect to EMS server.
Region ID	The Region to which the device is assigned. This is a number value that has to be entered, so an example of region configuration might be based on Area Codes. Another example might be time zones. When the EMS Server is set up, careful consideration should be given to how the regions are defined.
Heartbeat type	The MTA will send a heartbeat to the EMS Server to let it know it is up and running. A Data Tunnel between the EMS and MTA is used, and this can be encrypted or not, depending on the Option type chosen. Below are the current Heartbeat types: 2 = Plain text tunnel formatted. 3 = Encrypted text using a shared secret key 4 = Plain text and carrying SIP registration status 5= Encrypted text and carrying SIP registration status
Heartbeat interval	The interval at which to send heartbeat packets to the EMS server, in seconds. The MTA uses this HB interval unless instructed by EMS for a new HB interval
Enable Bidirectional VQM	Enable this feature to allow the device to store and upload a media stream to the EMS server for its decoded output stream during a test-agent-based media loopback test. This allows voice quality monitoring (VQM) to be performed by the EMS for both the EMS-to-ATA and ATA-to-EMS directions during the loopback call.
Compress Audio for Bidirectional VQM	Enable this feature to compress the uploaded media stream to the EMS server during Bidirectional VQM.

Server URL for Bidirectional VQM	When ‘Bidirectional VQM’ is enabled, the URL to which the MTA’s decoded output media stream will be uploaded must be configured here.. Replace the <FQDNofEMSServer> in the URL string below with the details of the EMS server to be used for Bidirectional VQM: **https://<*FQDNofEMSServer*>/ems/dms/ems-device-mlb-upload.php**

5.8 Trace Log

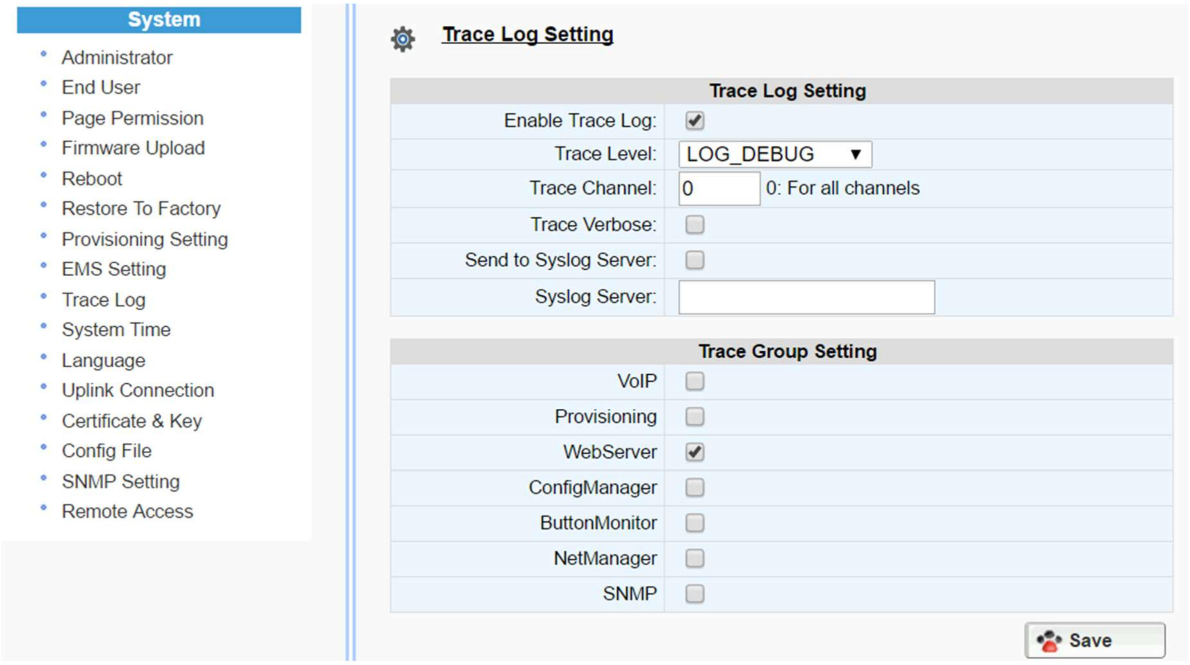
5.8.1 Trace Log Setting

Configure the MTA device to display debugging messages according to the trace level parameters. Note: Trace Level “LOG_DEBUG” will have a significant performance impact on the MTA device. It is recommended to use this feature only when debugging is needed.

An example is described as follows.

On WEB GUI:

1. Check “Enable Trace Log”
2. Trace Level menu, choose “LOG_DEBUG”
3. Check “Trace Verbose”
4. Configure “Trace Channel” to be “0” to monitor all ports of the system.
5. Check whatever items to be monitored from the “Trace Group Setting” table.



Trace Log Setting

Trace Log Setting	
Enable Trace Log:	☑
Trace Level:	LOG_DEBUG ▼
Trace Channel:	0 0: For all channels
Trace Verbose:	☐
Send to Syslog Server:	☐
Syslog Server:	

Trace Group Setting	
VoIP	☐
Provisioning	☐
WebServer	☑
ConfigManager	☐
ButtonMonitor	☐
NetManager	☐
SNMP	☐

Figure 53. Trace Log Setting

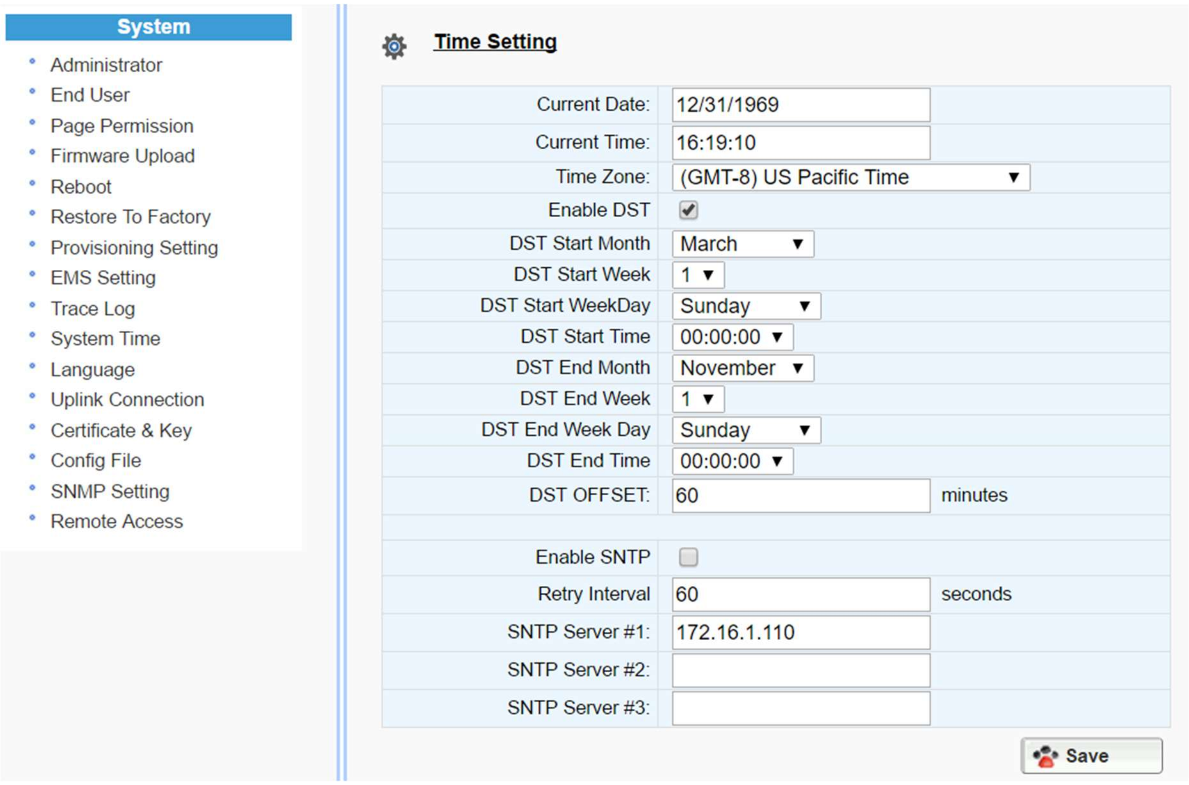
Trace Log Setting	Description
Enable Trace Log	Enables the trace log.
Trace Level	Follows RFC5424 syslog message severities. 1 Alert: Action must be taken immediately 2 Critical: Critical conditions. 3 Error: Error conditions. 4 Warning: Warning conditions. 5 Notice: Normal but significant condition. 6 Informational: Informational messages. 7 Debug: Debug-level messages. Additional Messages available: LOG_STACK -- Network protocol related messages. LOG_DSP -- RTP traffic related messages.
Trace Channel	The ports (lines) you wish to monitor/debug. 0 covers all ports.
Trace Verbose	Enable Trace logs to be displayed in a Telnet session.
Send to Syslog Server	When checked, will send out messages to a configured Syslog Server.
Syslog Server	Syslog server IP address or FQDN.

Trace Group Setting	Description
Item list	Select items to monitor and display associated messages. These messages can be displayed on the CLI console or the specified syslog server. Note that some particular items will only be displayed on the GUI when they are enabled.

5.9 System Time

5.9.1 Time Setting

Configure the SNTP time server IP/FQDN and time zone with which the MTA device synchronizes. Accurate time information is important for ensuring reliable telephony services.



Time Setting

Current Date:	12/31/1969	
Current Time:	16:19:10	
Time Zone:	(GMT-8) US Pacific Time ▼	
Enable DST	☑	
DST Start Month	March ▼	
DST Start Week	1 ▼	
DST Start WeekDay	Sunday ▼	
DST Start Time	00:00:00 ▼	
DST End Month	November ▼	
DST End Week	1 ▼	
DST End Week Day	Sunday ▼	
DST End Time	00:00:00 ▼	
DST OFFSET:	60	minutes
Enable SNTP	□	
Retry Interval	60	seconds
SNTP Server #1:	172.16.1.110	
SNTP Server #2:		
SNTP Server #3:		

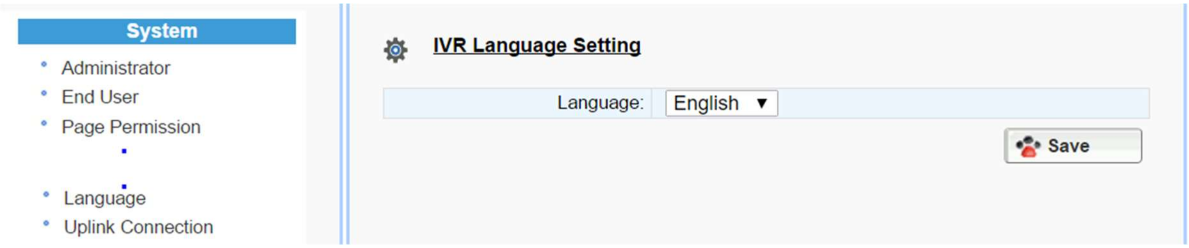
Figure 54. Time Setting

Field Name	Description
Current Date	The current date, which can be modified.
Current Time	The current time, which can be modified.
Time Zone	The current Time Zone configured, which can be modified through the pull down list. Note a reboot is needed for this setting to become effective.
Enable DST	Enable or disable daylight saving time.
DST Start Month | Week | WeekDay |Time	Configure the DST starting date/time each year.
DST End Month | Week | WeekDay |Time	Configure the DST ending date/time each year.
DST Offset	Most of the regions where DST is deployed have an offset of 60 minutes; however, a few regions have an offset of 30 minutes. Check the MTA deployment region for this requirement.
Enable SNTP	Enable the SNTP service.

Retry Interval	The time interval at which to synchronize with the time server, in seconds.
SNTP Server #1, #2, and #3	FQDN or IP of SNTP time servers to synchronize with. (Note: MTA tries all the configured servers, and bases its calculation on RFC 2030 and the delay. It then uses the lowest delay as the peer updates and sets the local time.)

5.10 Language

The MTA device supports English, Spanish for Interactive Voice Response (IVR) services. Select the desired language for your needs.

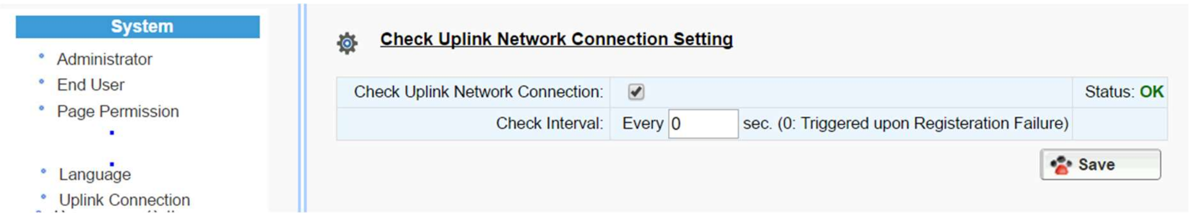


Language: English ▼

Figure 55. Language Selection for IVR system

Field Name	Description
IVR Language Setting	The language of IVR announcements.

5.11 Uplink Connection



Check Uplink Network Connection: ☑ Status: OK

Check Interval: Every 0 sec. (0: Triggered upon Registeration Failure)

Figure 56. Uplink Detection Settings

Field Name	Description
Check Uplink Network Connection	Enable or disable the MTA to probe the internet connection status.
Check Interval	How often device will send a 'probe' message out to determine whether the Internet connection is active. Set value to 0 to trigger 'probe' message being sent when SIP registration fails.

5.12 Certificate & Key

This page allows you to upload the encrypted keys or certificate for transporting signaling data through a secured TLS tunnel.

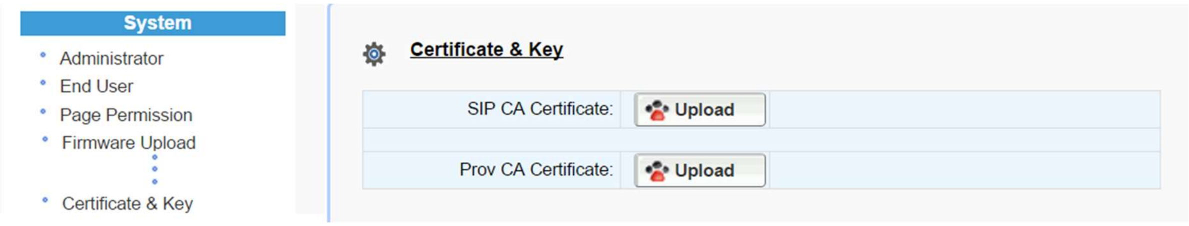
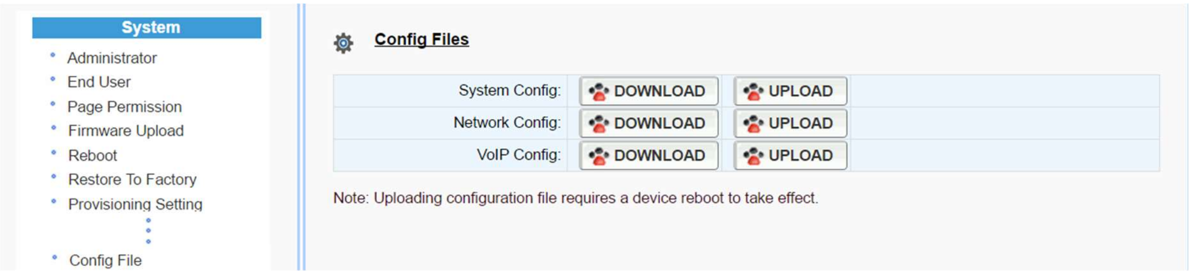


Figure 57. Certification & Key

Field Name	Description
SIP CA Certificate	Root certificate for verifying the SIP server TLS Certificate.
Prov CA Certificate	Root certificate for verifying the Provisioning server Certificate.

5.13 Config File



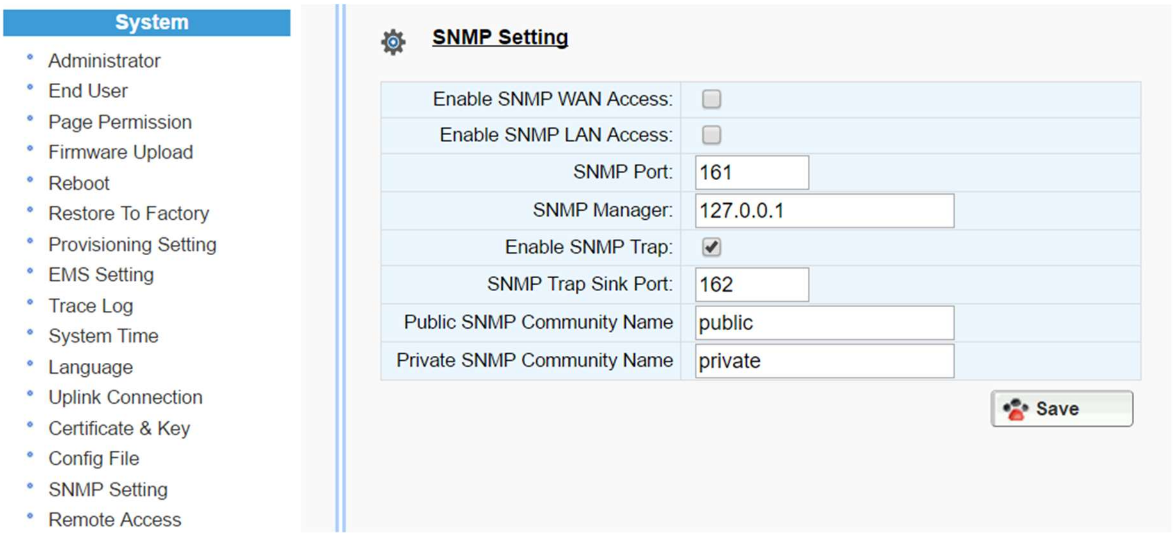
Note: Uploading configuration file requires a device reboot to take effect.

Figure 58. System Config

Field Name	Description
Config File	Upload: upload a config file to the MTA. Download: Store the config file from the MTA to a local drive. System Config: settings from the “System” category. Network Config: settings from the “Network” category. VoIP Config: settings from the “Telephony” category.

5.14 SNMP Setting

Configure the SNMP server information for the MTA to send traps to or to get commands from the SNMP server.



SNMP Setting

Enable SNMP WAN Access:	□
Enable SNMP LAN Access:	□
SNMP Port:	161
SNMP Manager:	127.0.0.1
Enable SNMP Trap:	☑
SNMP Trap Sink Port:	162
Public SNMP Community Name	public
Private SNMP Community Name	private

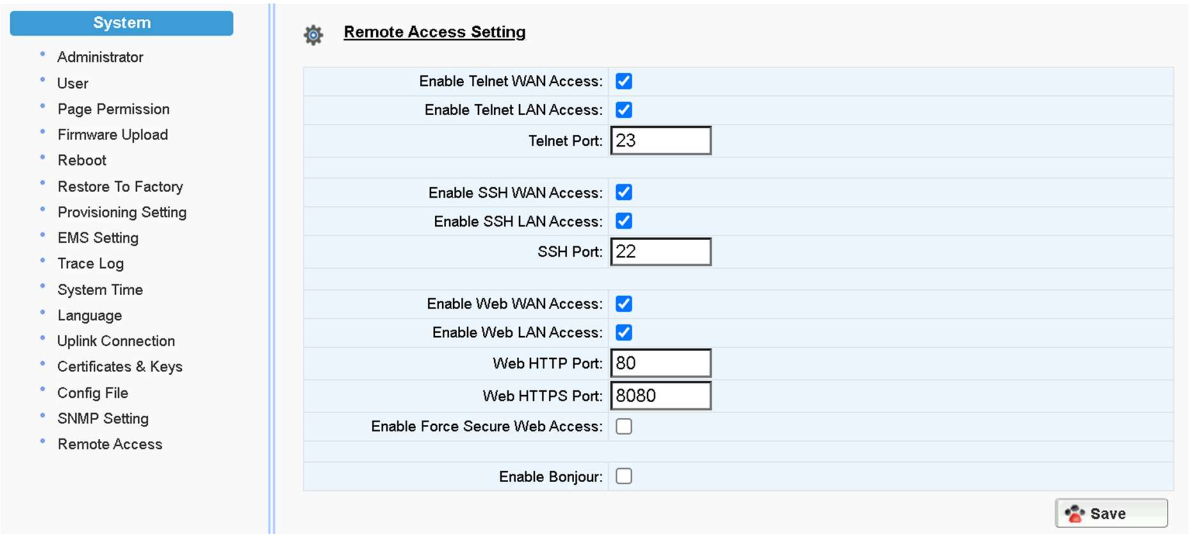
Figure 59. SNMP Setting

Field Name	Description
Enable SNMP WAN Access Enable SNMP LAN Access	Enable|Disable SNMP access from LAN or WAN interface(s).
SNMP Port	The port for SNMP communications.
SNMP Manager	IP address or FQDN of the SNMP Manager system.
Enable SNMP Trap	Enable|Disable sending traps to the SNMP server. Refer to the associated MTA MIB file for the list of supported traps.
SNMP Trap Sink Port	Define an SNMP trap receiver.
Public SNMP Community Name	Read only community string. This string is used with an SNMP GET to access the MTA.
Private SNMP Community Name	Read-write community string. This string is used with an SNMP SET to set a certain SNMP MIB variable (OID) to a specified value.

5.15 Remote Access

5.15.1 Remote Access Setting

Configure the designated protocols and ports for a system to access the MTA device remotely.



Remote Access Setting

Enable Telnet WAN Access: ☑
Enable Telnet LAN Access: ☑
Telnet Port: 23

Enable SSH WAN Access: ☑
Enable SSH LAN Access: ☑
SSH Port: 22

Enable Web WAN Access: ☑
Enable Web LAN Access: ☑
Web HTTP Port: 80
Web HTTPS Port: 8080
Enable Force Secure Web Access: ☐

Enable Bonjour: ☐

Figure 60. Protocol and Port Settings for Remote Access

Field Name	Description
Telnet WAN|LAN Access	Enable/Disable WAN/LAN access via Telnet and configure what port Telnet will be allowed to use.
SSH WAN|LAN Access	Enable/Disable WAN/LAN access via SSH and configure what port SSH will be allowed to use.
WEB WAN|LAN Access	Enable/Disable WAN/LAN access via HTTP or HTTPS and configure what ports will be used for each.
Enable Force Secure Web Access	If this option is enabled, any attempt to use HTTP for web console access will trigger a redirect to use HTTPS.
Bonjour	Enable Bonjour – allows Apple devices to discover the MTA on the network.

6 CLI COMMAND REFERENCES

Only the Administrator user is allowed to access the MTA CLI console. The login ID and password are identical to those for WEB console login. The CLI command hierarchy is designed similarly to that of the WEB console.

- Once logged in successfully, the command menu is displayed.

```
[v]voip                 VoIP Configuration
[n]net                  Network Configuration
```

```
   [s]system                 System
   [f]factory                Factory
   [d]restore                Restore to Default Setting
```

- Type the char enclosed in the square bracket [] to enter that particular section.
- Type question mark "?" at any level to display available commands.
- Type "`cd ..`" to go back to the upper level.
- [f] factory sub-menu is password protected.
- Type command "save" or "write" whenever the MTA configurations being updated through CLI commands.

Under any level, to show debug messages on the CLI console, type "debug on"; to stop debug messages being displayed, simply type "debug off".

APPENDIX A LED STATES

Model MTA8328-1W

LEDs	Blinking State	MTA State
PWR ⏻	Steady Green	Powered ON.
	Off	Powered OFF.
WAN 🌐	Solid or Blinking Green	WAN Ethernet 100BT link is active, blinks with activity.
	Solid or Blinking Yellow	WAN Ethernet 10BT link is active, blinks with activity.
	Off	WAN Ethernet link is not connected.
	Fast Blinking Green (0.25 secs on, 0.25 secs off)	WAN Ethernet 100BT link is active but is unable to reach the Internet.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	WAN Ethernet 10BT link is active but is unable to reach the Internet.
	Medium-Slow Blinking Green (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with the WAN LED.
LAN 🖧	Solid Green	LAN Ethernet 100BT link is active.
	Solid Yellow	LAN Ethernet 10BT link is active.
	Off	LAN Ethernet link is not connected.
WiFi 📶	Solid or Blinking Green	WiFi is connected successfully and link is active. Blinks with activity.
	Solid Yellow	WiFi has failed the setup, or it is disconnected after a successful connection.
	Medium-Slow Blinking Yellow (1 sec on, 1 sec off)	WiFi is in the process of being setup via the welcome portal.
	Off	WiFi is disabled
	Fast Blinking Green (0.25 secs on, 0.25sec off)	WiFi link is active but device is unable to get an IP address, OR is unable to reach a public IP address. This is the same condition in which the "no Internet connection" IVR is played.
PHONE 📞	Off	- No power, OR - Device is initializing, OR - Failed to register for voice services, OR - This line is disabled.
	Steady Green	The device is ready to make calls.
	Slow Blinking Green (3 secs on, 1 sec off)	There are new voicemail messages.
	Medium-Fast Blinking Green (0.5 secs on, 0.5 secs off)	The device is registered and ready to make calls, and the line is in use.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	The device has failed the FEM/HAZ online diagnostic (GR909) test. The LED will return to its previous state after the fault has been removed.
	Medium-Slow Blinking Green (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with the WAN or WiFi LED.

WCO Test State	WCO WiFi LED Representation
WCO Initial State	Solid Green
WCO Result State (last for 20 secs)	
• Excellent	Solid Green

• Good	Alternates between solid yellow and solid green.
• Not Good	Solid yellow

Model MTA8328-1N / MTA8338-1N

LEDs	Blinking State	MTA State
PWR ⏻	Steady Green	Powered ON.
	Off	Powered OFF.
WAN 🌐	Solid or Blinking Green	WAN Ethernet 100BT link is active, blinks with activities.
	Solid or Blinking Yellow	WAN Ethernet 10BT link is active, blinks with activities.
	Off	WAN Ethernet link is not connected.
	Fast Blinking Green (0.25 secs on, 0.25 secs off)	WAN Ethernet 100BT link is active but is unable to reach the Internet.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	WAN Ethernet 10BT link is active but is unable to reach the Internet.
	Medium-Slow Blinking Green (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with the WAN LED.
LAN 🖧	Solid Green	LAN Ethernet 100BT link is active, blink with activities.
	Solid Yellow	LAN Ethernet 10BT link is active, blinks with activities
	Off	LAN Ethernet link is not connected.
PHONE 📞	Off	- No power, OR - Device is initializing, OR - Failed to register for voice services, OR - Line is disabled.
	Steady Green	The device is ready to make calls.
	Slow Blinking Green (3 secs on, 1 sec off)	There are new voicemail messages.
	Medium-Fast Blinking Green (0.5 secs on, 0.5 secs off)	The device is registered and ready to make calls, and the line is in use.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	The device has failed the FEM/HAZ online diagnostic (GR909) test. The LED will return to its previous state after the fault has been removed.
	Medium-Slow Blinking Green (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with the WAN LED.

Model MTA8328-4, MTA8328-8, MTA8328-24

LEDs	Blinking State	MTA State
PWR	Steady Green	Powered ON.
	Off	Powered OFF.
WAN	Solid or Blinking Green	WAN Ethernet 1000BT link is active, blinks with activity.
	Solid or Blinking Yellow	WAN Ethernet 10/100BT link is active, blinks with activity.
	Off	WAN Ethernet link is not connected.
	Fast Blinking Green (0.25 secs on, 0.25 secs off)	WAN Ethernet 1000BT link is active but is unable to reach the Internet.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	WAN Ethernet 10/100BT link is active but is unable to reach the Internet.
	Medium-Slow Blinking Yellow (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with all other LEDs (except PWR LED)
LAN	Solid Green	LAN Ethernet 1000BT link is active, blinks with activity
	Solid Yellow	LAN Ethernet 10/100BT link is active, blinks with activity
	Medium-Slow Blinking Yellow (1 sec on, 1 sec off)	Device firmware is being upgraded. The PHONE LED blinks in unison with all other LEDs (except PWR LED)
	Off	LAN Ethernet link is not connected.
RUN	Fast Blinking Green (0.25 secs on, 0.25 secs off)	Device is being provisioned or firmware is being upgraded.
	Fast Blinking Red (0.25 secs on, 0.25 secs off)	Device provisioning or firmware upgrade has failed.
	Solid Green	Device has been provisioned or firmware upgraded has been successful.
	Off	Device has provisioning disabled.
PHONE 1 through 24 (depending on Model)	Off	- No power, OR - Device is initializing, OR - Failed to register for voice services, OR - Line is disabled.
	Steady Green	The device is ready to make calls.
	Slow Blinking Green (3 secs on, 1 sec off)	There are new voicemail messages.
	Medium-Fast Blinking Green (0.5 secs on, 0.5 secs off)	The device is registered and ready to make calls, and the line is in use.
	Fast Blinking Yellow (0.25 secs on, 0.25 secs off)	One or more lines have failed the FEM/HAZ online diagnostic (GR909) test. The LED will return to its previous state after the fault has been removed.

APPENDIX B THE USE OF ENCRYPTION KEY METHODS

Inno rc4_102

Use utility “rc4_102” to encrypt the plaintext config file (e.g., MTA6328_$MAC.cfg) with a 32-char-long key.

Syntax:

```
rc4_102 mac key input-file ['out-prefix'] [logfile]
```

Example:

```
rc4_102 001099001122 1234567890qwertyuiop1234567890as
MTA_sample_config.txt MTA
```

Output:

Encrypted config file: ***MTA001099001122.cfg*** is created.

Openssl command example

Provisioning config file should be encrypted using the following command at the provisioning server when AES-256 or RC4 is selected from the encryption menu.

```
 $ openssl enc -aes-256-cbc -k password -in infile -out outfile
```

AES-256

```
openssl aes-256-cbc -k password -in infile -out outfile
openssl aes-256-cbc -kfile keyfile -in infile -out outfile
```

RC4

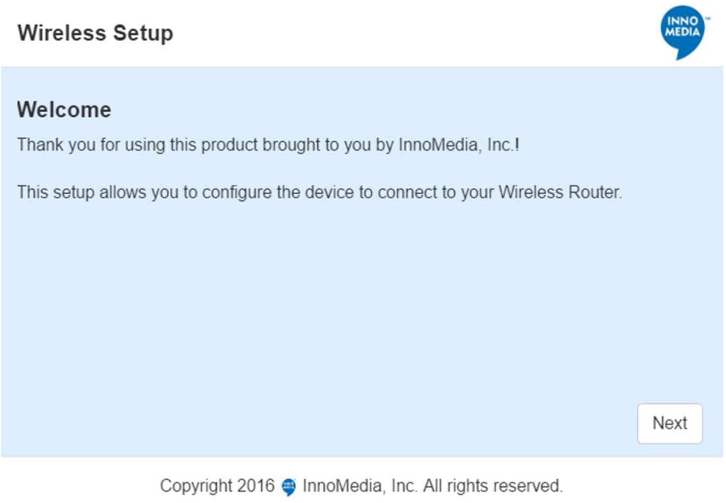
```
openssl rc4 -e -k password -md md5 -salt -p -in infile -out outfile
openssl rc4 -e -kfile keyfile -md md5 -salt -p -in infile -out outfile
```

APPENDIX C: WIFI CONNECTION SETUP THROUGH CAPTIVE PORTAL

Connect the MTA to the Home Router through a WiFi connection. You will connect the MTA to a WiFi Access Point using your smartphone, tablet or PC. Press the round button on the top of the unit for about 5 seconds, the MTA will switch to "Setup Mode" and the WiFi LED will change to solid yellow. Connect your smartphone or PC to the MTA's preset SSID shown on the back of the unit, i.e., MTA8328-xxxxxx, product name followed by the last 6 digits of MAC address. The MTA welcome portal web page will show up on your smartphone/PC. If this page does not popup, open a web browser and type in the following address:
http://192.168.199.1/wifisetup/

WiFi setup steps are as on the following screens:

(1) Welcome page



Wireless Setup

Welcome

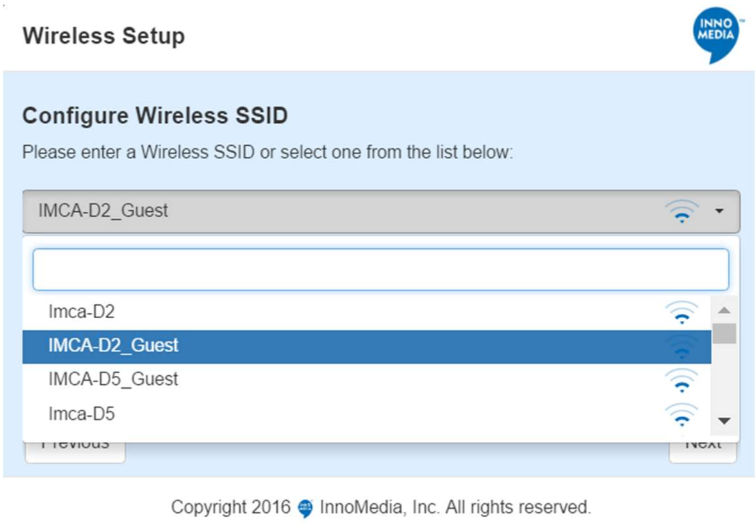
Thank you for using this product brought to you by InnoMedia, Inc.!

This setup allows you to configure the device to connect to your Wireless Router.

Copyright 2016 InnoMedia, Inc. All rights reserved.

Figure 61. Captive Portal - Welcome

(2) Select a Wireless SSID from the list, or just type the SSID name in the input box if the SSID name is hidden.



Wireless Setup

Configure Wireless SSID

Please enter a Wireless SSID or select one from the list below:

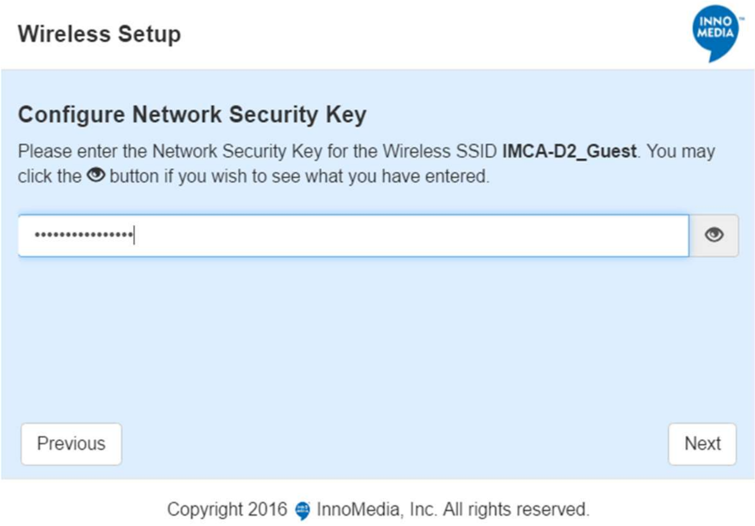
IMCA-D2_Guest

Imca-D2
IMCA-D2_Guest
IMCA-D5_Guest
Imca-D5

Copyright 2016 InnoMedia, Inc. All rights reserved.

Figure 62. Captive Portal – SSID selection

(3) Input the password for the selected SSID.



Wireless Setup

Configure Network Security Key

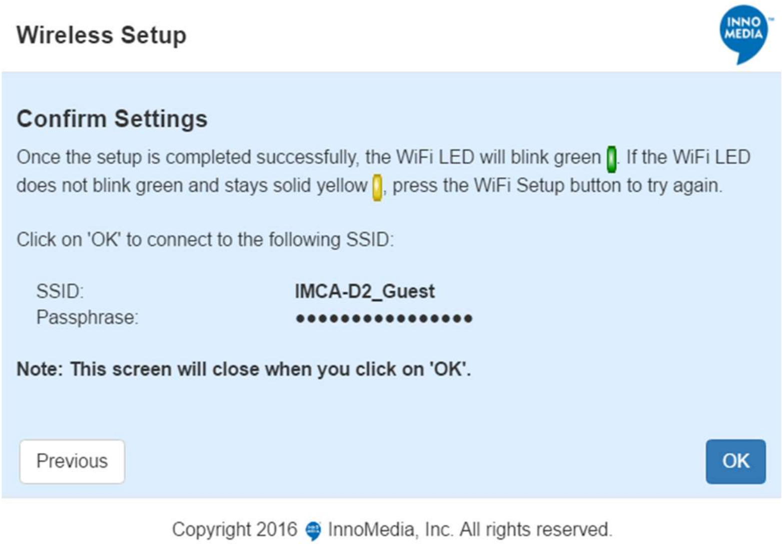
Please enter the Network Security Key for the Wireless SSID **IMCA-D2_Guest**. You may click the 👁 button if you wish to see what you have entered.

••••••••••••••••

Copyright 2016 InnoMedia, Inc. All rights reserved.

Figure 63. Captive Portal – SSID password input

(4) Complete the WiFi setup, and start the voice quality validation test.



Wireless Setup

Confirm Settings

Once the setup is completed successfully, the WiFi LED will blink green 🟩. If the WiFi LED does not blink green and stays solid yellow 🟨, press the WiFi Setup button to try again.

Click on 'OK' to connect to the following SSID:

SSID: **IMCA-D2_Guest**
Passphrase: ••••••••••••••••

Note: This screen will close when you click on 'OK'.

Copyright 2016 InnoMedia, Inc. All rights reserved.

Figure 64. Captive Portal – Confirm settings

APPENDIX D – PROVISIONING THROUGH DHCP OPTIONS

Method 1 – Use DHCP Option 66 only

Configure DHCP Option 66 string on the DHCP server with the complete provisioning URL of the config file.

Syntax of the provisioning URL string –

```
Protocol://FQDNofProvsisionServer:Port/Path/ConfigFileName
```

Port information is required, even it is the default port of the selected protocol. (If port information is absent from the URL string, then get the port from the MTA flash.)

Examples –

http://prov.example.com:80/MTA/config.cfg

http://prov.example.com:8802/MTA/config.cfg

ftp://ftp.example.com:**21**/MTA/config.cfg

tftp://OfficeVoiceServer:**69**/MTA/config.cfg

https://sprov.example.com:**443**/MTA/config.cfg

The network connection method chosen for the MTA device must be DHCP. When a device powers up, it will obtain the provisioning URL from the Option 66 string in DHCP Offer messages from the network DHCP server. This then triggers the provisioning process.

Method 2 – Use both DHCP Option 66 and DHCP Option 67 together

1. This method requires the user to configure the MTA provisioning protocol and server port settings.
   - Protocol. Choose among options: [HTTP|HTTPS|TFTP|FTP].
   - Server Port. The provisioning server port.
2. Configure DHCP Option 66 and 67 strings on the DHCP server.
   - Option 66: the provisioning server IP address or FQDN.
     Examples: 192.168.1.1 or prov.example.com.
   - Option 67: the path and filename of the config file on the provisioning server.
     Example: /MTA/config.cfg

The network connection method chosen for the MTA device must be DHCP. When the device powers up, it will obtain the provisioning server information from Option 66, and provisioning path and filename from Option 67, in addition to the other settings (protocol and server port) configured on the web console . This then triggers the provisioning process.

Important Note:

When two-stage provisioning is implemented (with a change in the provisioning server in the 2nd stage), “DHCP Provisioning” must be disabled in the config file for the MTA to reach the updated server.

Example: `System.Prov.Dhcp-opt=”0”`

<End of Document>