

InnoMedia MGCP Device Administrator's Guide

May 2008



Table of Contents

About This Document.....	5
Chapter 1.....	6
MGCP Device Internal Port Setup.....	6
Overview.....	6
Hardware Installation Steps.....	6
Setting up Your Computer.....	7
Configuring the Internal Port.....	7
Chapter 2.....	9
MGCP Device Configuration.....	9
Overview.....	9
Configuring MGCP Device via Web User Interface.....	9
Logging In.....	9
IP Network Settings.....	11
Configuring Interface Settings.....	11
Configuring Provisioning Settings.....	11
Configuring SNMP Settings.....	12
Configuring NAT Port Mapping (for Router Device Only).....	13
Configuring QoS Settings.....	14
Configuring Access Filtering options (for Router Device Only).....	16
IP Filtering.....	17
Domain Filtering.....	17
URL Filtering.....	18
MAC Filtering.....	19
Configuring PPPoE Settings.....	20
PPPoE Status.....	21
Management.....	21
Configuring DMS Settings.....	21
Changing Administrator ID and Password.....	22
Changing End User ID and Password.....	23
Time Zone Settings.....	23
Rebooting MGCP Device.....	24
Restoring Default Values.....	25
VoIP Settings.....	25
Configuring Call Agent Settings.....	25
Configuring Endpoint Names.....	27
Configuring Fax.....	27
Advanced Settings.....	28
Configuring MGCP Device via Telnet/ HyperTerminal Interface.....	30
Overview.....	30
Before You Begin.....	30
Logging In.....	31



Help (h)	31
Show System Information (I).....	32
Show Hardware Information (Ih).....	32
Use the "Ih" command to view the hardware information	32
Displaying DMS parameters (Ik).....	32
Configuration of IP Information (C).....	33
Viewing the Current IP Information (Cf)	33
Configuring IP Information (Ci).....	33
Ci configuration description	34
Configuring MAC Cloning (Co).....	34
Configuring VLAN Setting (Cv)	35
Change Password (Cw).....	36
Configuring DMS (Cx).....	37
Miscellaneous Settings (M)	37
Viewing MTA SNTP time (M0).....	37
Configuring NTP server (M1)	38
Configuring SysLog Server (M2).....	38
Displaying Syslog Message (M3).....	39
Configuring Default Timeout Parameters (M4)	39
Configuring RFC3389 (Comfort Noise) Setting (M6)	40
Configuring Global Call Agent Access (M7)	40
RFC2833 control (Ma).....	41
System Alive Time (Mb)	41
Call Agent ID and Port (Mc)	41
Configuring Dynamic Payload Type Setting (Md).....	42
Configuring Control Parameters (Me)	42
Configuring Flash Hook timer (Mf)	44
Voice Service Control (Mg).....	44
Jitter Buffer Settings (Mj).....	44
Local Signaling Port (Mk)	45
Viewing Line Parameter Settings (Ml).....	45
Ml configuration description.....	45
Mm Command (Mm).....	46
IP Information (Mn).....	46
Line Configuration (Mp).....	47
Echo Timer Setting (Mq)	47
Configuring the Voice Volume (Mr)	47
Configure the IP ToS Settings	48
Information of VLAN Setting (Mv)	48
Setting endpoint start index (Mu)	49
Configuring the Endpoint Name (Mx).....	49
Pinging a Remote IP Address (P)	49
Manually Forcing Security Provisioning (Qr)	50
VSP Security Provisioning Shell (Qv).....	50
Configuring Router Functions (N).....	53
PPPoE Setting configuration (N,1).....	53



Configuring DHCP Server (N, 2) (for Router Device Only).....	54
Configuring NAT (Port map) (N, 3) (for Router Device Only)	55
Showing DHCP Server Leasing Information (N, 4) (for Router Device Only) ...	56
Accessing Filtering options (N, 5) (for Router Device Only)	56
IP Filtering (N, 5, 1):.....	57
Domain Filtering (N, 5, 2):	58
URL Filtering (N, 5, 3):	59
MAC Filtering (N, 5, 4):.....	59
Configuring MAC Cloning (N, 6) (for Router Device Only).....	60
Configuring NAT Bandwidth (N, 7).....	61
Configuring the Networking Mode (N, c)	62
Debug Information (D)	63
Enable Debug Mode (D1) & (D0)	63
Setting Project Variant (D1,Th, 1).....	63
Setting Line Reverse mode (D1, Th, 3)	63
G726 Configuration (D1, Th, 6)	64
Setting T.38 Fax (D1, Th, 18).....	65
Cisco T38 Support (D1, Th, 19)	67
Pinging Gateway (D1, Th, 20).....	68
Enabling/Disabling Detect FAX CNG Tone (D1, Th, 30)	68
Configuring Provison 301 Redirect Server (D1, Th, 31).....	68
Trace Settings (Dl).....	69
Displaying List of All Configured Values (Dc).....	71
Showing the State of Connections for All Endpoints (Dn).....	75
Showing Notification Information for All Endpoints (Ds).....	75
Showing DHCP Lease Information (Dt).....	76
Showing RTP Statistics (Du)	76
MGCP Device Version Information (V).....	76
Restoring System Default	77
Chapter 3.....	78
MGCP Device Firmware Updates	78
Overview.....	78
Manually Uploading MGCP Device Firmware via Web Interface	78
Auto-upgrading MGCP Device Software Code from Server Side	79
APPENDIX A: MGCP Device LED Indicators	80
APPENDIX B - HTTP Provisioning for MGCP Device	82



About This Document

Welcome to the InnoMedia MGCP Device Administrator's Guide. The purpose of this manual is to give system integrators and service operators detailed reference information on configuring and administering InnoMedia's MTA line of products running the MGCP protocol.

The commands necessary for unit's configuration and provisioning are covered in this document for InnoMedia's MGCP-based voice CPE. For conciseness, all examples reference configuration of a 2-port device, but are applicable to the rest of InnoMedia's MGCP-based voice CPE as well.

Any device-specific variances can be found within the appendices of this document. Therefore, it is advisable to refer to the appendix if the information you require is not found within the general documentation.

This document has the following chapters:

Chapter 1, MGCP device Internal Port Setup, provides step-by-step instructions for installing the MGCP device system and setting up the IP addresses of your computer.

Chapter 2, MGCP device Configuration, describes how to configure MGCP device via a web interface and a command line interface.

Chapter 3, MGCP device Firmware Updates, describes the procedure for uploading MGCP device firmware through a web interface, an external TFTP server or HTTP server to the unit.



Chapter 1

MGCP Device Internal Port Setup

Overview

This chapter provides step-by-step instructions for setting up MGCP device.

Hardware Installation Steps

Do the following steps to connect your MGCP Device with a PC:

NOTE: You will need to use a PC that has an Internet browser and a network interface card (NIC) properly installed.

Table 1. Hardware Installation Steps

<i>Step</i>	<i>Action</i>
<i>1</i>	Using a network cable, connect your PC's NIC to the MGCP Device's LAN port
<i>2</i>	Connect the included power adapter to the port marked 12V DC/1A on the MGCP Device.

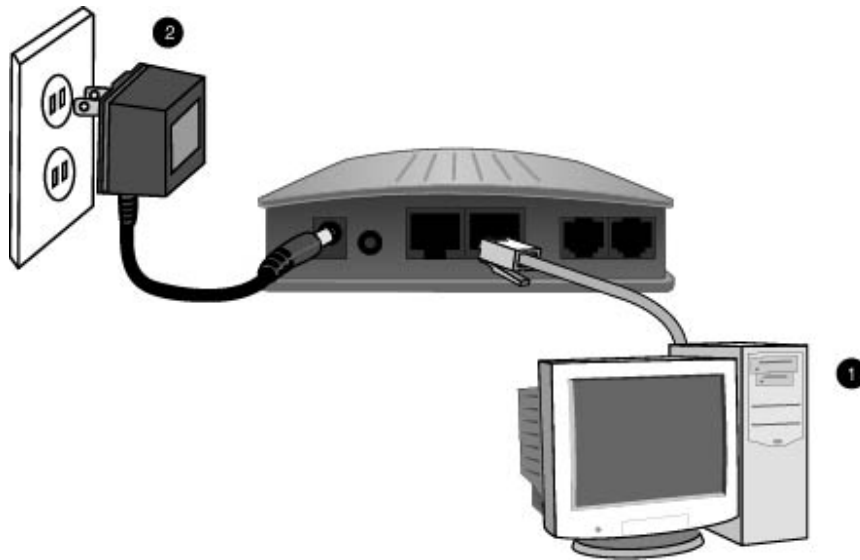


Figure 1. Hardware Installation Steps

NOTE: If you want to connect more than one computer to the MGCP Device, please use an Ethernet hub or a switch and make sure the 'uplink' port of your hub is connected to the 'LAN' port of MGCP device.

Setting up Your Computer

Configuring the Internal Port

Your MGCP device's LAN side is factory set to a static IP address of 192.168.99.1. Hook up a PC to your MGCP device and follow these steps to configure the IP settings. This will configure the internal port which communicates to your PC through a network cable.

We recommend that you refer to your Operating System manual to do this. An example of how to do this with Windows XP appears below:

NOTE: The procedure may be different because of your computer settings.

Table 2. Procedure for Setting up Your Computer

<i>Step</i>	<i>Action</i>
1	Click Start on your Taskbar.
2	Click Control panel.
3	Click Network Connections.
4	Right mouse click on Local Area Connection (See Figure 2. Setting up Your Computer – Local Area Connections).
5	Choose Properties.

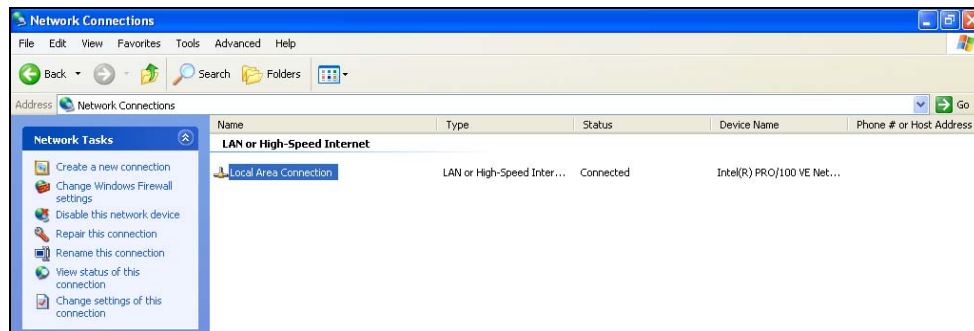


Figure 2. Setting up Your Computer – Local Area Connections

Table 3. Setting up Your Computer

<i>Step</i>	<i>Action</i>
6	Double Click on Internet Protocol (TCP/IP) (See Figure 3 Setting up Your Computer - Local Area Connection Properties).
7	Write down the current settings before making any changes in case you need to restore your original settings.
8	Enter an IP address that is within the same subnet as your MGCP device. The MGCP device has a default of 192.168.99.1 so if you enter 192.168.99.5, you should have no problem connecting to the MGCP DEVICE (See Figure 4 Setting up Your Computer - Using the Static IP Address).
9	Enter 255.255.255.0 as your subnet mask.
10	Enter 192.168.99.1 as your default gateway IP.
12	Leave the DNS information as is.
13	Click OK.
14	Verify this by typing "ipconfig" at the command prompt. Your PC should have an IP address 192.168.99.5.



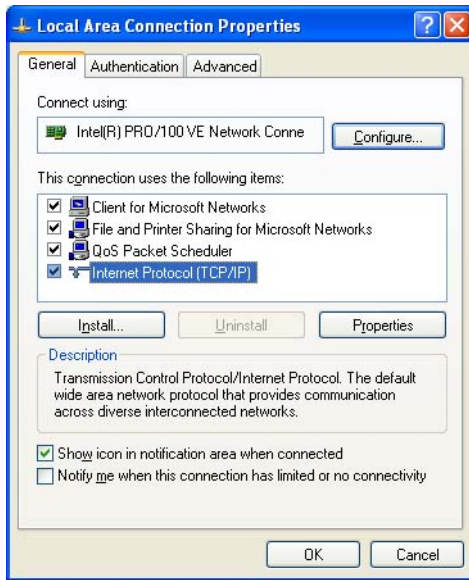


Figure 3 Setting up Your Computer - Local Area Connection Properties

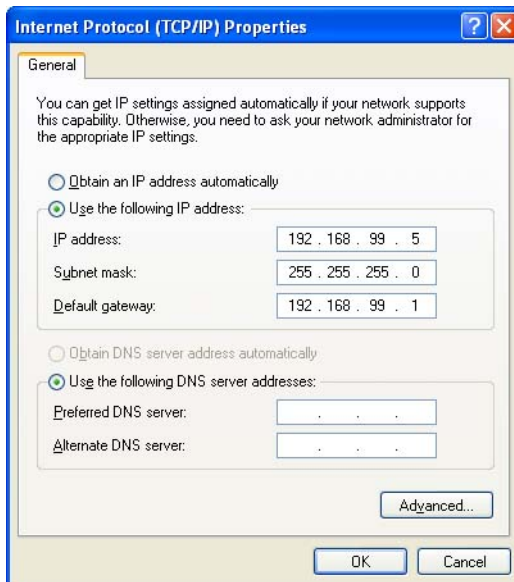


Figure 4 Setting up Your Computer - Using the Static IP Address



Chapter 2

MGCP Device Configuration

Overview

Setup and configuration of the MGCP Device can be managed via a Web Browser interface and a command line interface. In order to access these interfaces, your PC must be configured properly as outlined previously in Chapter 1. If you have not completed the steps outlined in Chapter 1, please do so before proceeding to the following.

- The MGCP Device needs two IP addresses, one is for WAN (External Port) and one is for LAN (Internal Port). The internal port has already been configured. The IP address used by the "WAN" is the IP assigned by your ISP. This address can be either a dynamic or a static IP.

At this point you need to know which method is used for your connection. You will need to know this before you can proceed with configuring the MGCP Device.

Configuring MGCP Device via Web User Interface

Logging In

To login the Web User Main page, follow these steps:

NOTE: The following instruction is assuming you have LAN connection (that is connecting MGCP Device via the LAN port).

Table 4. Web User Interface - Logging in

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and enter the IP address of the MGCP Device. 192.168.99.1 is the default address. The Login Dialogue Box as shown in Figure 5 appears.
<i>2</i>	Enter your Username and Password. NOTE: The default Username is "Admin" and Password is "adminpass". For security reason, it is recommended to change the default Administrator ID and Password after initial login. See 13 for details.





Figure 5. MGCP Device Login Dialogue Box

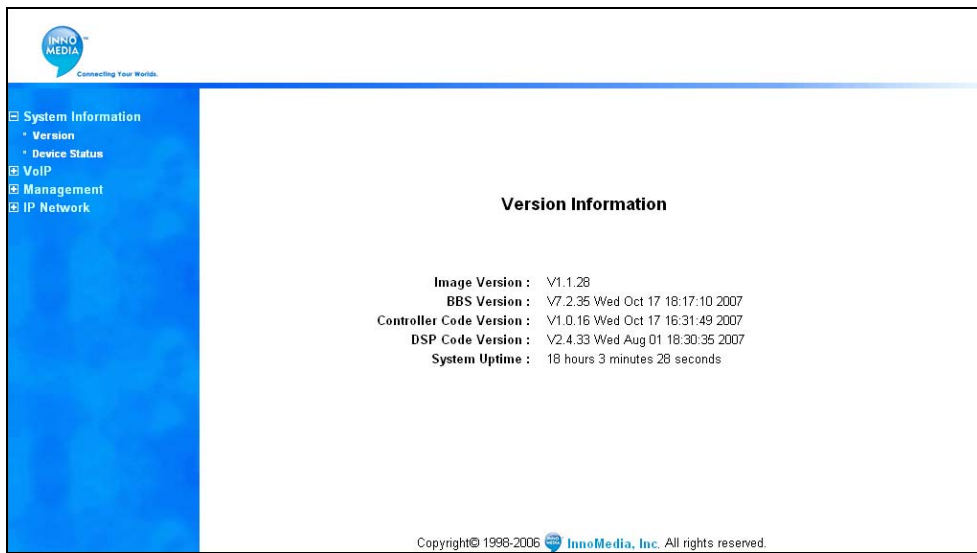


Figure 6. MGCP Device Web User Interface - Main Page



IP Network Settings

Configuring Interface Settings

The IP address used by the "WAN" is the IP assigned by your ISP, MGCP Device can either use a static assigned IP or get an IP dynamically by using DHCP. The default setting is DHCP.

To configure the interface settings, follow these steps:

Table 5. Configuring Interface Settings

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MGCP Device at http://192.168.99.1 .
<i>2</i>	Click on IP Network, then Interface Setting.
<i>3</i>	If you choose to use DHCP, then click the check box, otherwise, enter your IP address, Subnet Mask, Default Gateway, DNS (if available), and FQDN (Fully Qualified Domain Name). This information should be supplied by your ISP or network administrator.
<i>4</i>	Click Save & Reboot to save your changes, or click the Reset button to undo your changes.

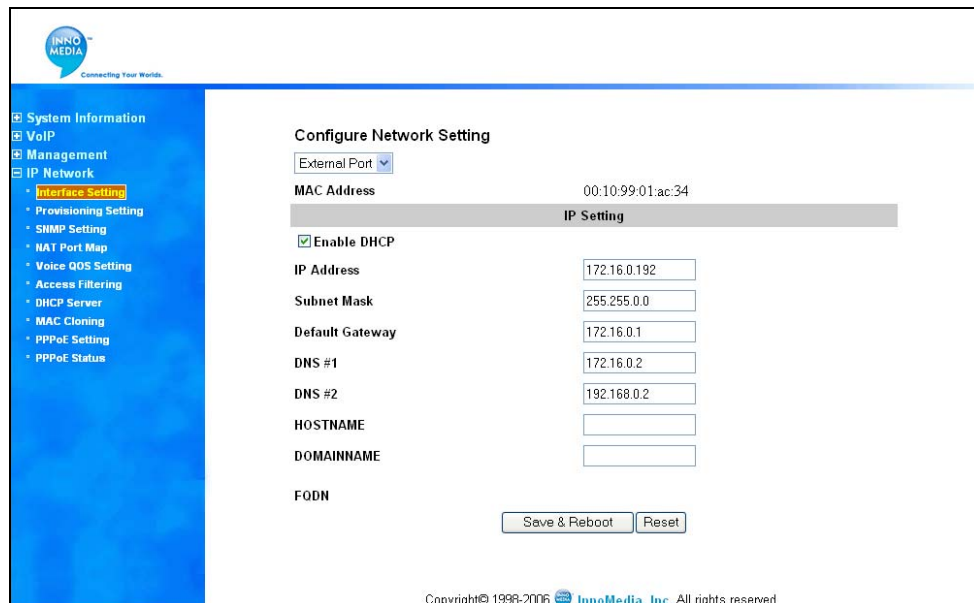


Figure 7. Configuring Network Settings

Configuring Provisioning Settings

If you would like to use a provisioning server to provision your MGCP device, you will need to configure the provisioning settings on your MGCP device. To configure the provisioning settings, follow these steps:



NOTE: Web interface only allows you to configure some basic provisioning settings. Please refer to the Telnet interface section to finish configuring the provisioning settings for your MGCP device.

Table 6. Configuring Provisioning Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then Provisioning Setting.
3	Check the option box to enable the provisioning function.
4	Enter the DNS or the IP address of your provisioning server.
5	Enter the port number of your provisioning server.
6	Click Save & Reboot to save your changes, or click the Reset button to undo your changes.

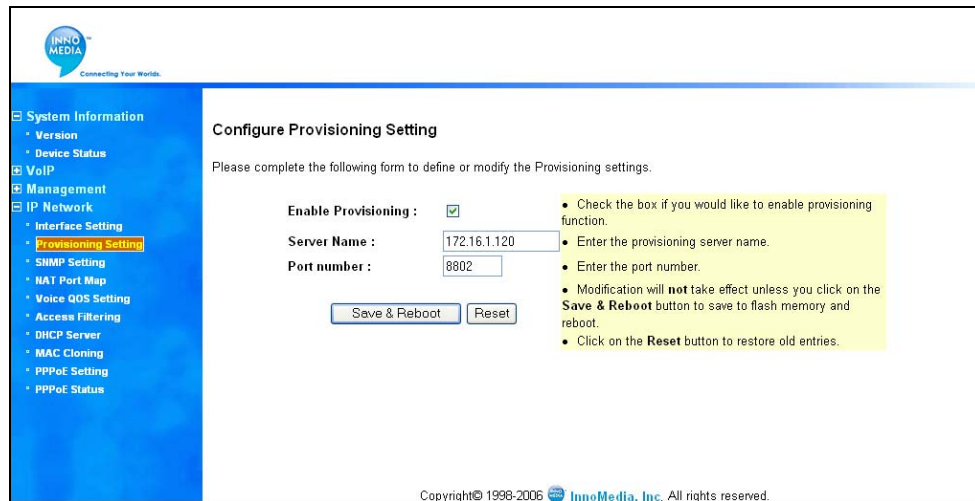


Figure 8. Configuring Provision Settings

Configuring SNMP Settings

If you want to use a SNMP Manager to monitor your MGCP Device, you must configure the MGCP Device SNMP settings. To configure SNMP settings, follow these steps:

Table 7. Configuring SNMP Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then SNMP Setting.
3	Enter the SNMP Manager Address where the SNMP software is installed.
4	Enter the SNMP Community Name #1. It must match the string configured on your SNMP server. By default, SNMP community #1 is a read-only community string for SNMP Get-request.
5	Enter in the SNMP Community Name #2. It must match the string configured on your SNMP server. By default, SNMP community #2 is a read-write community string for SNMP Set-request.
6	Click Save & Reboot to save your changes, or click the Reset button to undo your changes.



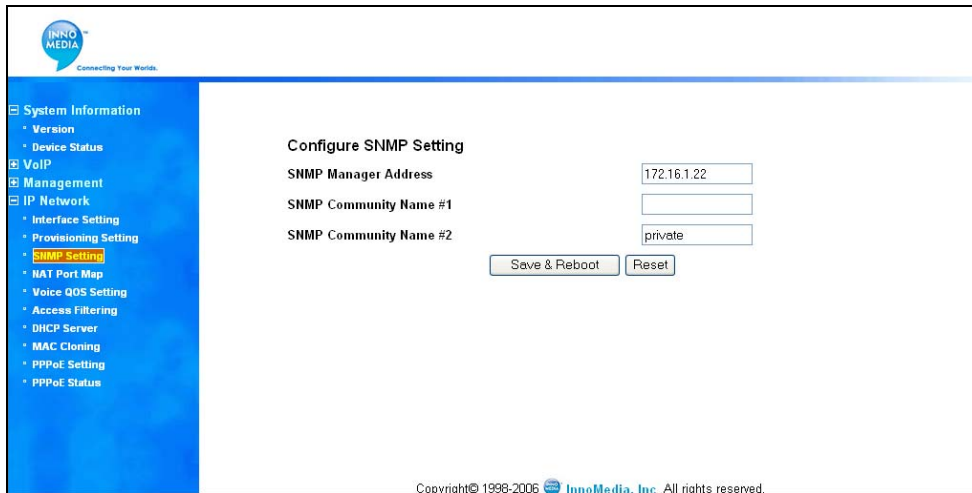


Figure 9. Configuring SNMP Setting

Configuring NAT Port Mapping (for Router Device Only)

Port mapping is an advanced configuration in which the router forwards incoming protocols to computers on your local network. You will need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. To configure the NAT Port Mapping, follow these steps:

NOTE: For best results, a port should only be mapped to an Internal Source IP that is static. Therefore, you should assign a static IP address to the PC or PCs that will be forwarded any traffic by the port maps above.

Table 8. Configuring NAT Port Mapping

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP Device.
2	Click on IP Network, then NAT PortMap.
3	Enter External Source Port number that you want to redirect to another unit.
4	Choose either TCP/IP or UDP protocol.
5	Enter the IP address of the PC that is running the application or game that uses this source port and protocol.
6	Enter the Internal Source Port you want to send it to. If the application or service only uses one port, then the Internal Source Port will be the same as the External Source Port.
7	Click the Save button to save your changes, or click the Reset button to undo your changes.



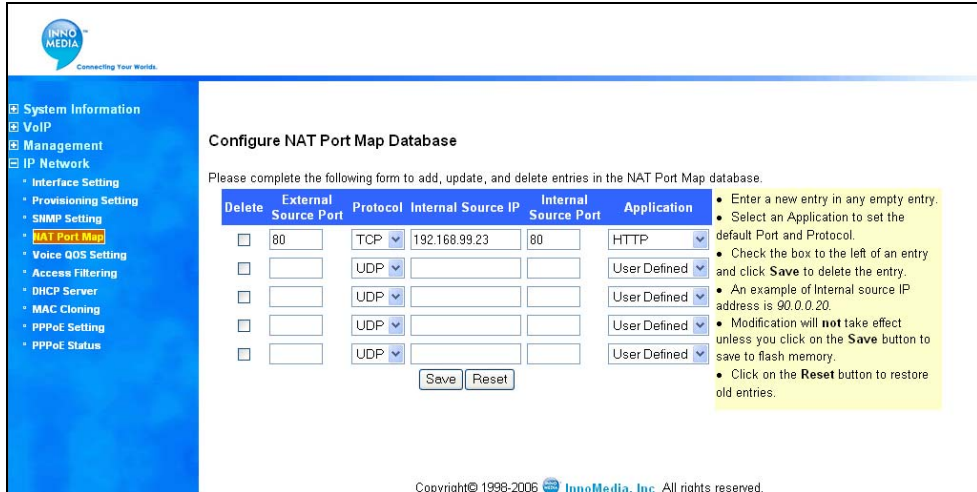


Figure 10. Configuring NAT Port Mapping

EXAMPLE:

Figure 11. Port Mapping diagram is a sample illustration of the NAT Port Mapping.

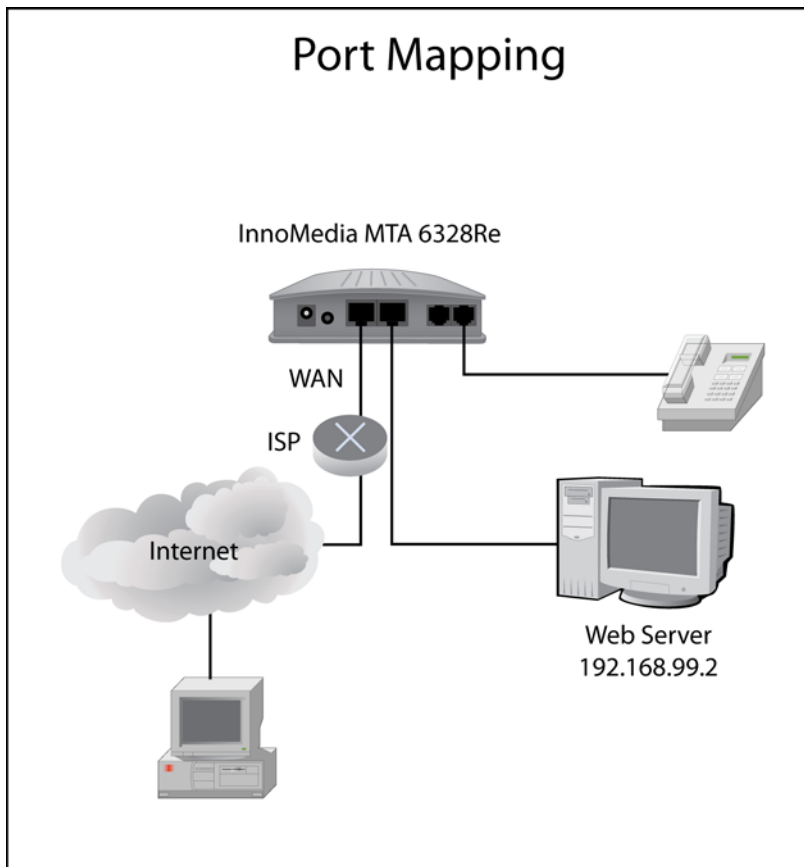


Figure 11. Port Mapping diagram

Configuring QoS Settings

QoS Settings allow the user to designate the amount of bandwidth available on the uplink ports of the MGCP device. When the QoS is enabled, the voice packets have higher



priority over data packets. In addition, by enabling the ToS (Type of Service) control, you can change the LAN, and CPE ToS values to allow packets that pass through network devices have their relative priorities differentiated from one another. The Type Of Service (TOS) bits are a set of four-bit flags in the IP header, and each of the four bits has a different purpose. One of the TOS bits may be set at any time, so combinations are not allowed. Set the bit flags to tell the network the type of network service an application requires.

This screen also allows you to set the parameters for VLAN tagging on the MGCP device. This advanced feature is only recommended if your network consists of VLAN-enabled servers and components. If you are unsure whether your network is using VLAN, leave it disabled on your MGCP device.

To configure the QoS Settings, follow these steps:

Table 9. Configuring QoS Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP Device.
2	Click on IP Network, then QoS Settings.
3	Check the option box to enable Data Bandwidth Control.
4	Enter the maximum WAN uplink speed in the field. The maximum bandwidth can accept values up to 100000.
5	Check the option box and enter the values in the fields if you want to enable LAN1 and ToS control. NOTE The value field is not case sensitive and uses hex notation. You can enter any two-digit value between 00 to ff in the field.
6	Check the option box and enter the values in the fields if you want to enable Voice ToS control for each channel. NOTE It is recommended to set a higher value for Voice because it involves RTP packets. The precedence bit = 7.
7	Click the option box to enable WAN port VLAN setting
8	Click the option box to enable the WAN port Priority Mapping feature.
9	Enter the WAN port Traffic VLAN ID and Priority values in the fields.
10	Enter the MTA Voice Traffic VLAN ID and priority values in the fields.
11	Enter the MTA Voice Signaling VLAN ID and priority values in the fields.
12	Enter the MTA other Data VLAN ID and priority values in the fields.
13	Check the option box if you want to enable the LAN port VLAN Setting.
14	Check the option box if you want to enable the LAN port priority Mapping feature.
15	Enter the LAN port traffic VLAN ID in the field.
16	Enter the LAN port Traffic Priority value in the field.
17	Click Save to save your changes, or click the Reset button to undo your changes.

The screenshot displays the InnoMedia web interface for configuring QoS and VLAN settings. The left sidebar shows a navigation menu with 'Voice QoS Setting' highlighted. The main content area is divided into two sections:

Configure Voice QoS Settings

- Enable Data Bandwidth Control
 - Max. WAN Uplink Speed (kbps):
- Enable LAN1 ToS Control
 - LAN1 ToS Byte Value (hex): 0x
- Enable ToS Control for Voice
 - Voice ToS Byte Value for Channel 0 (hex): 0x
 - Voice ToS Byte Value for Channel 1 (hex): 0x
 - Signaling ToS Byte Value (hex): 0x

Configure VLAN setting
(IP TOS must be set to a non-zero value)

- Enable WAN port VLAN setting
 - Enable IP ToS to 802.1p Priority Mapping for WAN port
 - WAN port Traffic VLAN ID (hex): 0x
 - WAN port Traffic Priority (hex): 0x (0-7)
 - MTA Voice Data VLAN ID (hex): 0x
 - MTA Voice Data Priority (hex): 0x
 - MTA Voice Signaling VLAN ID (hex): 0x
 - MTA Voice Signaling Priority (hex): 0x
 - MTA other Data VLAN ID (hex): 0x
 - MTA other Data Priority (hex): 0x
- Enable LAN-port-1 VLAN setting
 - Enable IP ToS to 802.1p Priority Mapping for LAN-port-1
 - LAN-port-1 Traffic VLAN ID (hex): 0x
 - LAN-port-1 Traffic Priority (hex): 0x

Buttons: Save, Reset

Copyright © 1998-2006 InnoMedia, Inc. All rights reserved.

Figure 12. Configuring QoS Settings.

Configuring Access Filtering options (for Router Device Only)

Access filtering is a feature designed to help you regulate the access of internal PCs to the outside network. It is useful when you wish to block access to certain websites or addresses for individual PCs that are connected to the MGCP device.

The MGCP device offers four ways to control the access available to your internal PCs:

- 1 IP Filtering – Allows you to control what IP, port, and protocol traffic to allow or disallow going out of MGCP device.
- 2 Domain Filtering – Allows you to block access to specific domains and websites. This is useful for controlling access to certain web addresses. This filtering is a global setting that applies to all PCs connected to your SIP Device.
- 3 URL Filtering – Allows you to block access to specific URLs. This is useful for controlling access to certain URLs. This filtering is a global setting that applies to all PCs connected to your MGCP device.
- 4 MAC Filtering –allows you to prevent certain MAC addresses from accessing the Internet. It will also allow certain MAC Addresses to access the Internet and deny all others. This filtering is assigned per MAC address.



IP Filtering

To configure the IP Filtering, follow these steps:

Table 10. Configuring IP Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then Access Filtering
3	Select IP Filtering from the pull-down menu
4	Check the box to enable IP Filtering
5	In the 'Restricted IP Addresses' field, enter the IP addresses or an IP range.
6	In the 'Ports' field, specify the port or a range of ports you wish to block.
7	In the 'Protocol' field, specify the protocol. If you are unsure, choose Any.
8	In 'Schedule' fields, select "Always" to always block the restricted internal IP addresses to access outside Internet, or select "From Time" and enter a blocking time range.
9	Click the Save button to save your changes, or click the Reset button if you want to undo your changes.

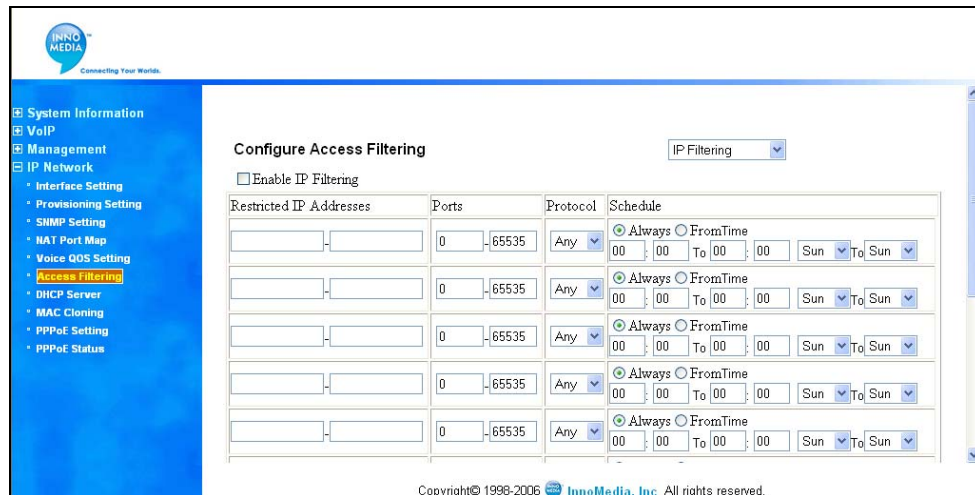


Figure 13. Configuring Access Filtering – IP Filtering

Domain Filtering

To configure the Domain Filtering, follow these steps:

Table 11. Configuring Domain Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then Access Filtering
3	Select Domain Filtering from the pull-down menu
4	Check the box to Enable Domain Filtering



5	Select Restricted to block access to specific domains/websites, or select Allowed only to allow access to specific domains/websites.
6	Enter the domain names in the fields. You can enter up to 10 domains.
7	Click the Save button to save your changes, or click the Reset button if you want to undo your changes.

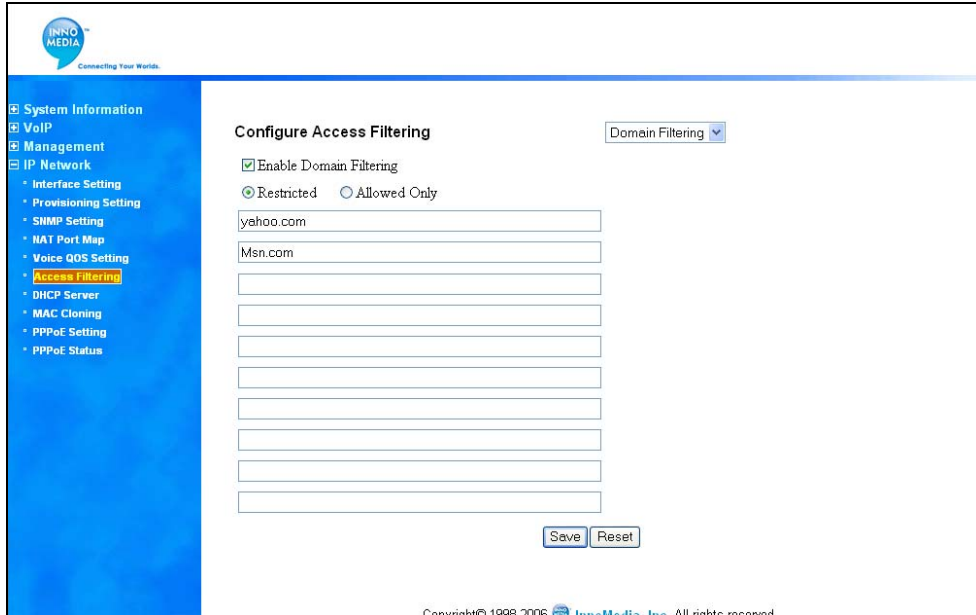


Figure 14. Configuring Access Filtering – Domain Filtering

URL Filtering

To configure the URL Filtering, follow these steps:

Table 12. Configuring URL Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then Access Filtering
3	Select URL Filtering from the pull-down menu
4	Check the box to Enable URL Filtering
5	Select “Restricted” to block accessing to specific URLs entered in the fields, or select “Allowed only” to allow access to specific URLs.
6	Enter the URLs in the fields. You can enter up to 10 URLs.
7	Click the Save button to save your changes, or click the Reset button if you want to undo your changes.



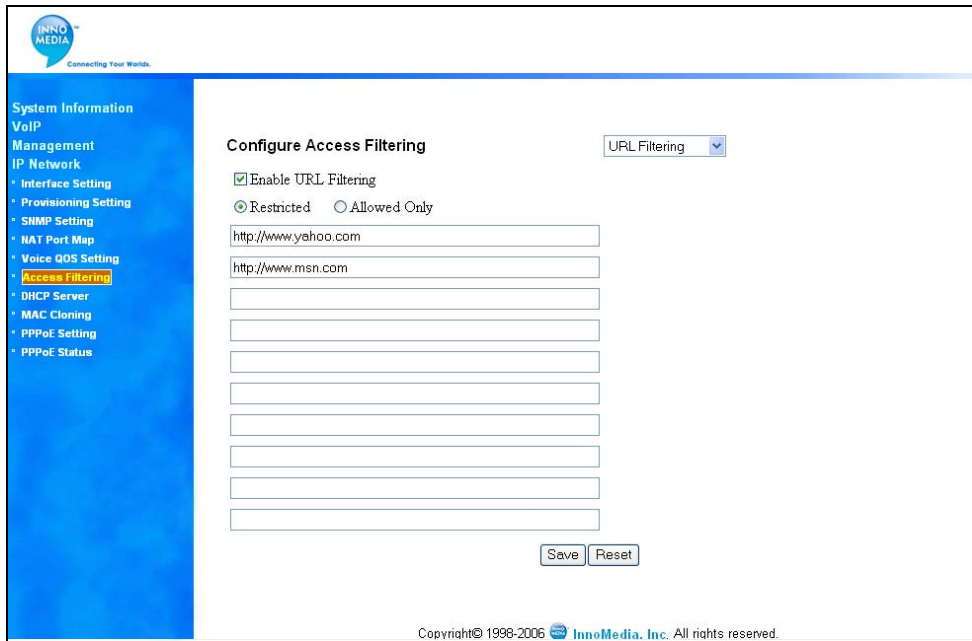


Figure 15. Configuring Access Filtering – URL Filtering

MAC Filtering

To configure the MAC Filtering, follow these steps:

Table 13. Configuring MAC Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then Access Filtering
3	Select MAC Filtering from the pull-down menu
4	Check the box to Enable MAC Filtering
5	Select “Restricted” to restrict the MAC addresses entered in the fields from accessing outside Internet, or select “Allowed only” to allow only those MAC addresses to access the outside Internet.
6	Enter the MAC addresses in the fields. You can enter up to 10 MAC addresses.
7	Click the Save button to save your changes, or click the Reset button if you want to undo your changes.



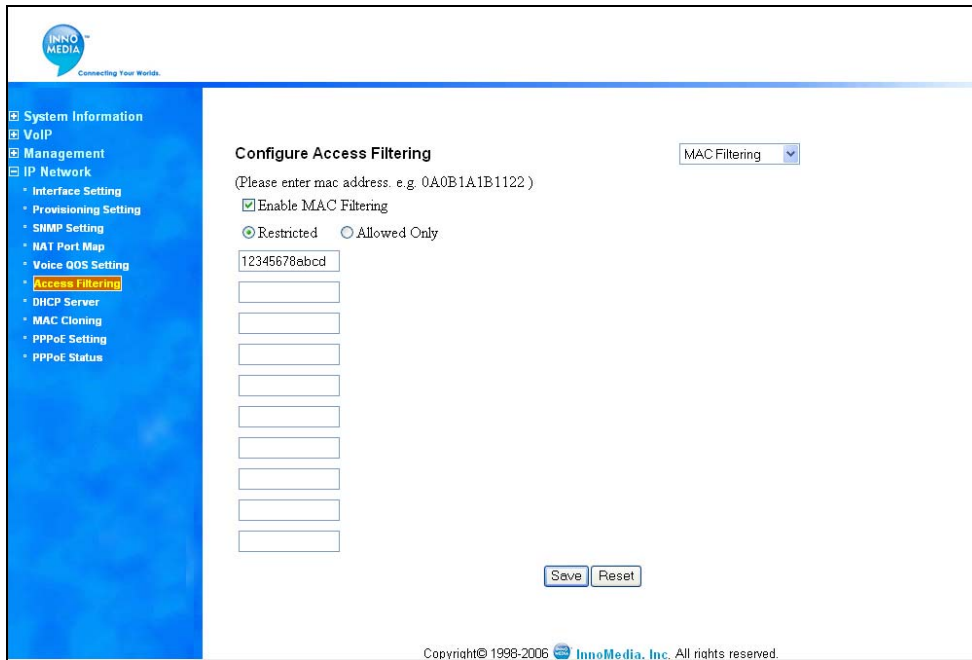


Figure 16. Access Filtering – MAC Filtering

Configuring PPPoE Settings

If your ISP provides your external IP address using PPPoE, then you will need to configure your MGCP device so that it will be able to establish a PPPoE connection. To configure PPPoE settings, follow these steps:

Table 14. Configuring PPPoE settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on IP Network, then PPPoE Settings.
3	Click Enable PPPoE to enable the service.
4	Check Auto Connect When System Boots up if you would like to connect to PPPoE server automatically when the system boots up.
5	Enter your Service ID if provided by your ISP. Otherwise, leave this field blank.
6	Enter your User ID, sometimes referred to as Username.
7	Enter your Password.
8	Select PAP or CHAP for the Authentication Protocol depending on your ISP.
9	Enter the idle time out in minutes. Entering 0 means the link is connected all the time.
10	Click Save & Reboot to save your changes, or click the Reset button to undo your changes.

NOTE: If you are using a static IP, refer to IP Network Settings on page 11 to disable DHCP and configure your IP information. Your ISP will supply you with your IP information, User ID, Password, and Authentication Protocol.



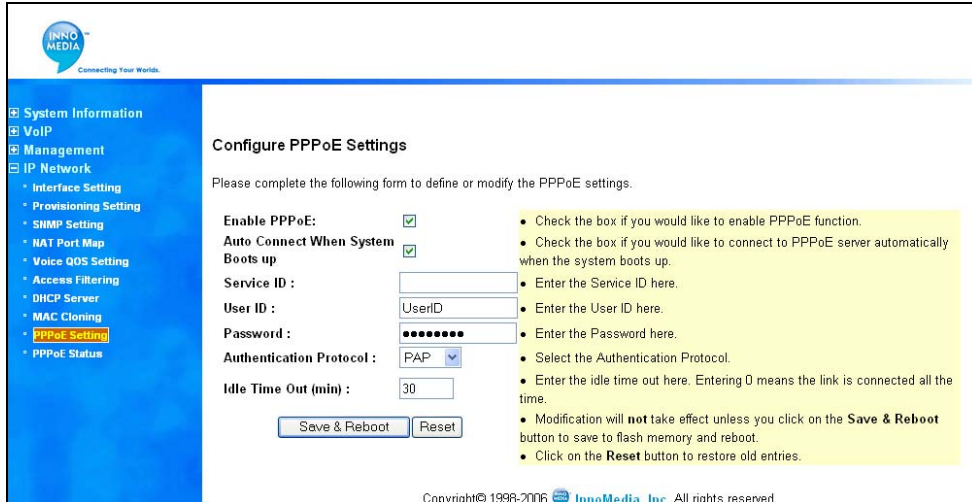


Figure 17. Configuring PPPoE settings

PPPoE Status

The PPPoE Status link allows you to manage your connection with your broadband service provider. When you power on your MGCP device, it normally will auto-connect to your broadband service provider using PPPoE. If you ever wish to manually disconnect and/or reconnect to your Internet connection, simply click the appropriate button on the PPPoE Status page.

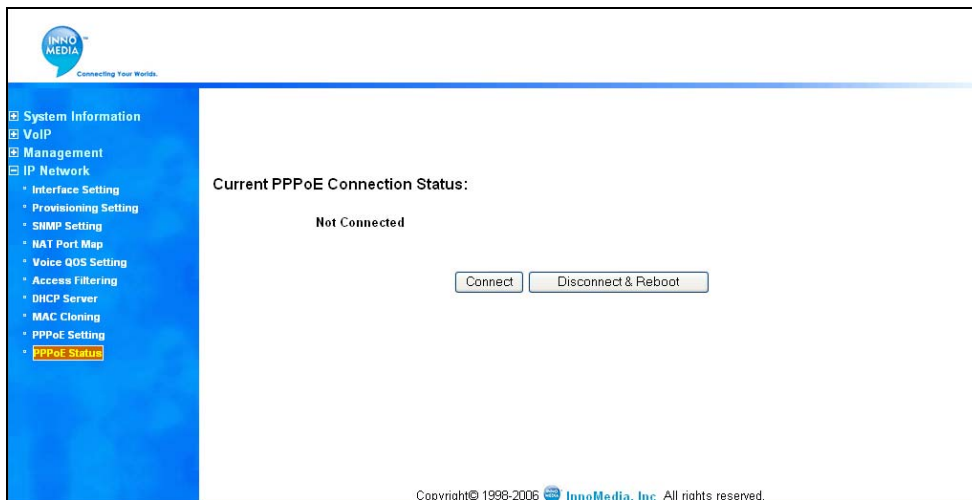


Figure 18. Current PPPoE Connection Status

Management

Configuring DMS Settings

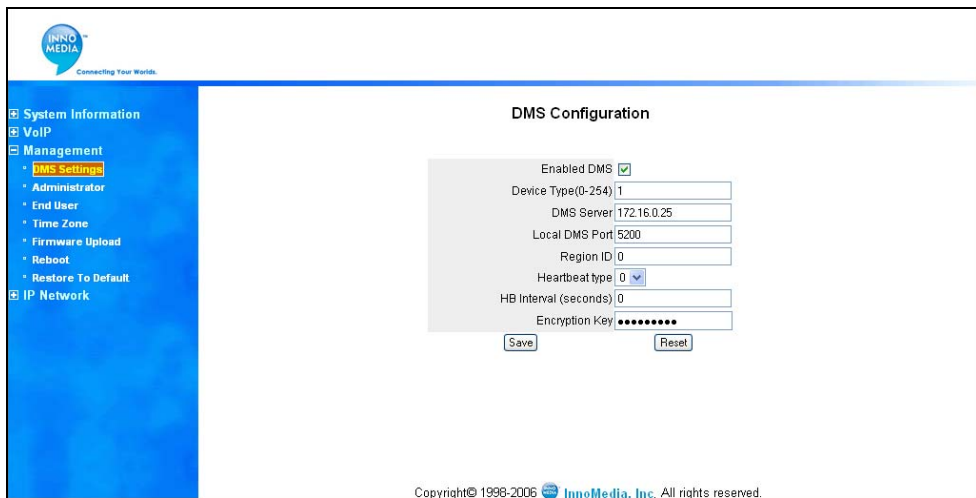
To configure InnoMedia Device Management System (DMS) setting, follow these steps:

NOTE: Please refer to your DMS server settings to configure the DMS parameters on your MTA.



Table 15. Configuring DMS Setting

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your SIP Device at http://192.168.99.1.
<i>2</i>	Click on IP Network, then DMS Setting.
<i>3</i>	Check the option box to enable DMS.
<i>4</i>	Enter the device type, DMS server IP, local port, Region ID, Heartbeat type, HB Interval, and Encryption Key.
<i>5</i>	Click Save to save the DMS setting, or click the Reset button if you want to undo your changes.

**Figure 19. Configuring DMS Setting**

Changing Administrator ID and Password

To change your Administrator ID and Password, follow these steps:

Table 16. Changing Administrator ID and Password

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MGCP Device.
<i>2</i>	Click on Management, then Administrator.
<i>3</i>	Enter the new Administrator ID you wish to use.
<i>4</i>	Enter the new password in New Password field
<i>5</i>	Reenter your new password in Confirm Password field.
<i>6</i>	Click Update to save your new ID and Password or click the Restore button to undo your changes.

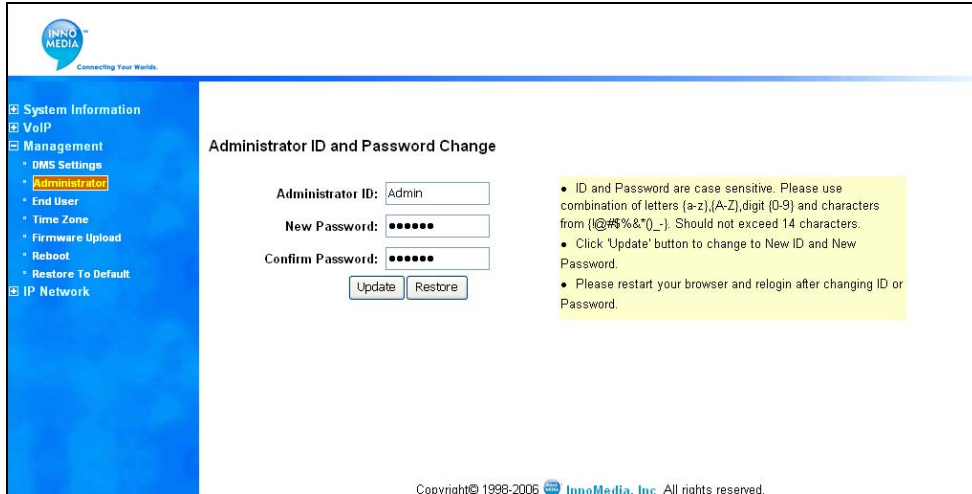


Figure 20. Changing Administrator ID and Password

Changing End User ID and Password

To change the end user ID and Password, follow these steps:

Table 17. Changing End User ID and Password

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click on Management, then End User.
3	Enter the New End User ID for user to access the MGCP device.
4	Enter the new password in New Password field
5	Reenter your new password in Confirm Password field.
6	Click Update to save your new ID and Password or click the Restore button to undo your changes.

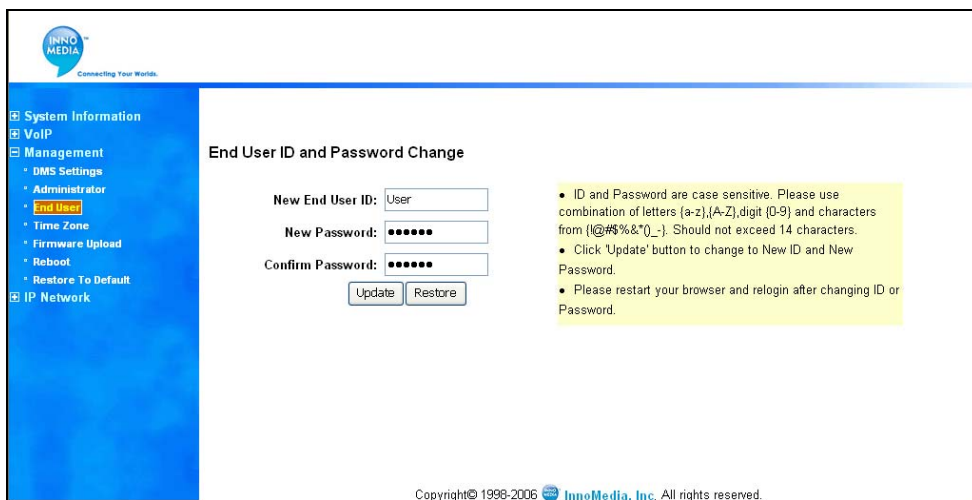


Figure 21. Changing End User ID and Password

Time Zone Settings



This page displays the current MGCP device time. Also, it allows you to configure the time zone and NTP server. To configure the time zone settings, follow these steps:

Table 18. Time Zone Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device (See Logging In on page 9 for more details).
2	Click on Management, then TimeZone Settings.
3	Select the time zone from the drop down list
4	Enter the NTP server IP in the field. If you are entering more than one NTP server IPs, separate them with a comma.
5	Click Save to save your changes, or click the Reset button to undo your changes.



Figure 22. Configuring Time Zone Settings

Rebooting MGCP Device

To reboot your MGCP device, follow these steps:

Table 19. Rebooting MGCP DEVICE

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP Device.
2	Click on Management, then Reboot.
3	Click OK to reboot the MGCP Device, or Cancel if you do not want to Reboot at this time.



Figure 23. Rebooting MGCP DEVICE



Restoring Default Values

To restore default settings, follow these steps:

CAUTION: All Web-based management settings and parameters will be restored to their default values. This includes the administrator password; a user-specified password will no longer be valid. The default User Name and Password are "Admin" and "adminpass" respectively for the administrator account; "User" and "userpass" for the end user account.

Table 20. Restoring Default Values

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP Device (See Logging In on page 9 for more details).
2	Click on Management, then Restore Default.
3	Click OK to restore factory default or Cancel if you do not want to do it at this time.



Figure 24. Restoring MGCP Device 6328-Re to Factory Default

VoIP Settings

Configuring Call Agent Settings

To configure the Call Agent Settings, follow these steps:

Table 21. Configuring Call Agent Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP Device.
2	Click VoIP, and then Call Agent.
3	Enter the IP address of your Primary and Secondary Call Agent.
4	Enter the Call Agent UDP port number. The default is 2727.
5	Enter MGCP device Signaling UDP port number. The default is 2427.
6	Enter MGCP device RTP port number. The default is 6024. RTP port number has to be an even number with a range of 1024 to 65535 and not equal to the MGCP signaling port.
7	Enter the MTA Fax Port number. The default is 40000.
8	Click Save to save the settings to the MGCP device, or click the Reset button to restore the old entries.

The screenshot shows a web-based configuration interface for InnoMedia. On the left is a blue sidebar with a navigation menu containing: System Information, VoIP (with sub-items: Call Agent, Endpoint Settings, Fax, Advanced Settings), Management, and IP Network. The 'Call Agent' item is highlighted. The main content area is titled 'Configure Call Agent Settings' and contains the following fields:

- port 1 Primary Call Agent: port 1 Secondary Call Agent:
- port 2 Primary Call Agent: port 2 Secondary Call Agent:
- Call Agent 1 - UDP Port No.:
- Call Agent 2 - UDP Port No.:
- MTA Signaling UDP Port No.:
- MTA RTP Port No.:
- MTA Fax Port No.:

At the bottom of the form are 'Save' and 'Reset' buttons. A copyright notice at the bottom right of the interface reads: 'Copyright© 1998-2006 InnoMedia, Inc. All rights reserved.'

Figure 25. Configuring Call Agent Settings



Configuring Endpoint Names

The endpoint names can be either configured explicitly or automatically created by the MGCP device. To configure endpoint names follow these steps:

Table 22. Configuring Endpoint Names

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click VoIP, and then Endpoint Names.
3	Select Automatic if you want the MGCP device using the IP address or FQDN to create the endpoint names (format: aaln/0 or aaln/1@[ip or FQDN]). Otherwise, select Explicit and type the endpoint names in the fields. NOTE: Explicit supports up to 128 alphanumeric characters. If end point is explicitly configured, it must match with the ones defined in the call agent configuration. Otherwise, the call agent will reject the unknown end points.
4	Click Save to save the settings to the MGCP device, or click the Reset button to restore the old entries.

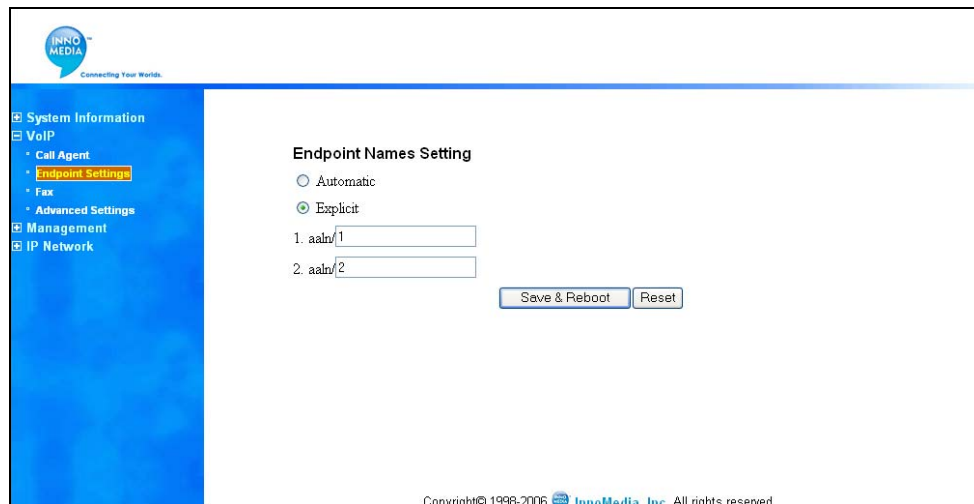


Figure 26. Configuring Endpoint Name Setting

Configuring Fax

To configure the Fax settings, follow these steps.

Table 23. Configuring Fax

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MGCP device.
2	Click VoIP, and then Fax

3	Check the option boxes to enable or disable fax feature for Line 1 and Line 2
4	Enter the values in the fields. See the description below.
5	Click Save to save the settings to the MGCP device, or click the Reset button to restore the old entries.

T.38 Fax configuration description

Jitter Buffer = Enter the jitter buffer size (0-240 ms)
 T2 = Timer for awaiting packets (0-800ms)
 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. Range varies by platform from 0 (no redundancy) to 4
 High speed redundancy = Number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. The value range varies by platform from 0 (no redundancy) to 4.

NOTE: Setting the High Speed redundancy parameter greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Bit rate = Enter the fax transmission speed to be attempted: 2400, 4800, 9600, 4800, or 14400
 ECM = Error Correction Mode (ECM) for the gateway. By default ECM is not enabled.
 Fax Max Buffer = Maximum buffer size (200)
 Fax Max Datagram = Maximum datagram size

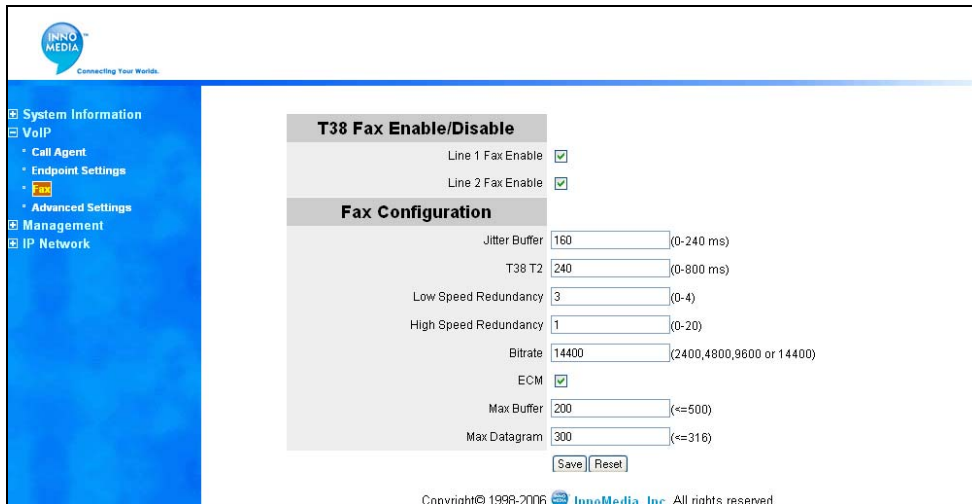


Figure 27. Configuring Endpoint Name Setting

Advanced Settings

This page allows you to configure the FXS Settings.

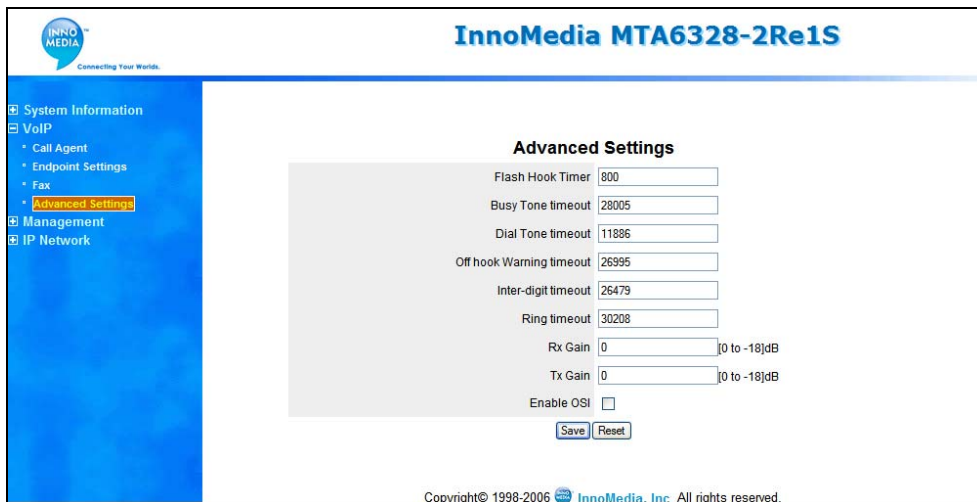
Table 24. Configuring Advanced settings

<i>Step</i>	<i>Action</i>
-------------	---------------



1	Open your web browser and connect to your MGCP device.
2	Click VoIP, and then Advanced Settings.
3	Enter the values in the fields. See the description below.
4	(1) Enable OSI if your Call agent does not support it. Therefore, even without Call Agent's command, MTA will automatically do OSI (900ms open loop), when the remote hangs up the phone. (2) Disable OSI if your call agent supports it to prevent confliction.
5	Click Save to save the settings to the MGCP device, or click the Reset button to restore the old entries.

- Busy tone timeout = the duration of busy tone played in seconds before it times out.
- Dial tone timeout = the duration of dial tone played in seconds before it times out.
- Off hook warning tone timeout = the duration of offhook warning tone played in seconds before it times out.
- Interdigit timeout = the length of time in seconds between dialed digitals. If the timer expires while a user is dialing, the MTA will send NTFY with the current partial phone number.
- Ring timeout = the duration in seconds of ringing tone played before it times out.
- Rx Gain = Rx (Receive) Gain. Range: 0 ~ -18 (default=0). To optimize the voice quality, enter 0 db in the field.
- Tx Gain = Tx (transmit) Gain. Range: 0 ~ -18 (default=0). To optimize the voice quality, enter 0 db in the field.



Configuring MGCP Device via Telnet/ HyperTerminal Interface

Overview

MGCP device can also be configured via a TCP/IP interface, such as Telnet or a terminal emulation program. The following instructions are for use with a terminal emulation program.

Before You Begin

1. Make sure you have performed the steps outlined in the "Setting up your computer" section in Chapter 1.
2. Connect your PC to MGCP device's internal port (LAN port).
3. Telnet to MGCP device

If you are using MS-DOS Prompt window

1. From a windows machine open a Dos command prompt.
2. Type in Telnet 192.168.99.1 (or the IP address of your MGCP device), then press enter.

If you are using HyperTerminal:

1. Open the HyperTerminal application on your PC.
2. Select TCP/IP from the Connect using field's drop-down menu.
3. Enter the IP address 192.168.99.1 and port number '23' in the fields.
4. Click OK.

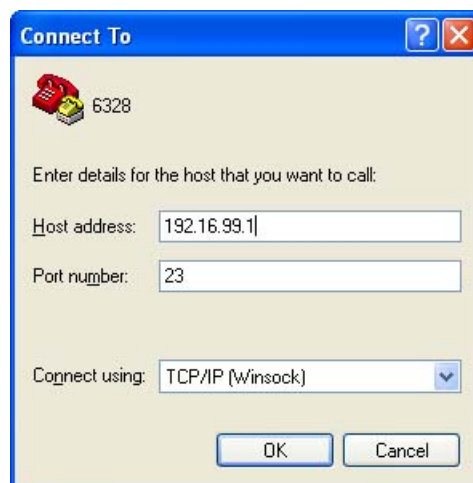


Figure 28. Configuring Your MGCP Device via HyperTerminal-Properties

Logging In

Help (h)

Command "H" prompts for Username and Password for users to login and also displays a list of the MGCP device commands.

NOTE: Type the commands in bold face and match case as shown.

SAMPLE:

```

H
Enter Username:           Admin
Enter Password:          adminpass
H
Help
I:  Show System Information
    Ih: Show Hardware Information
    Ik: Display DMS parameters
C:  Configuration of IP Information
    Cf: Get the current IP Information
    Ch: Configure Hwardware ID information
    Ci: Re-Configure the IP Information
    Co: MAC CLONE          configure
    Cv: Configure VLAN Setting
    Cw: Change Password
    Cx: Configuring EMS
        CX: EMS shell

D:  Debug Information
    D0: Disable Debugging
    D1: Enable Debugging
    D1: Trace Settings
        Dc: Display list of all configured values
    Dn: Show the state of connections for all endpoints
    Ds: Show notification information for all endpoints
    Dt: Show DHCP lease information
    Du: Show RTP statistics

M:  Miscellaneous Settings
    M0: Show MTA SNTP time
    M1: Configure NTP server
    M2: Configure log server
    M3: Show syslog
    M4: Signal default timeout configure
    M6: Configure RFC3389 (Comfort Noise) setting
    M7: Configure global call agent access for MTA
    Ma: RFC2833 control
    Mb: System alive time
    Mc: Information of Call agent ID and port
    Md: Dynamic playtype setting
    Me: Information of control parameters

```



```

Mf: Flash_Hook_timer_Setting
Mg: Voice_Service_Control
Mj: Information of Jitter Buffer Size, Bandwidth Params
Mk: MGCP local ports configuration
Ml: Information of Line parameters
Mm: Authentication for CNC
Mn: Information of IP Information
Mq: Dummy packet timer setting
Mp: Configure phone lines
Mr: Configure the voice volume
Ms: Configure the IP ToS Settings
Mv: Information of VLAN Setting
Mu: Setting endpoint start index
Mx: Configure the endpointname
N: Configure router function
P: Ping
Qr: Manually Vsp security provisioning
Qv: Vsp security provisioning shell
R: Reset system
E: Exiting and Logout
#: Entry to New CLI

```

Show System Information (I)

Show Hardware Information (Ih)

Use the "Ih" command to view the hardware information.

SAMPLE:

```

Ih

Hardware version = 10.0.0.0
Layout Version = A3-0

```

Displaying DMS parameters (Ik)

Use the "Ik" command to view the InnoMedia DMS parameters. If you wish to modify the DMS settings, use the web interface (see page 21) or Cx command (see page 36.)

NOTE: The Ik command will not work if debug is enabled. See page 63 "Enable Debug Mode (D1) & (D0)" for how to enable and disable debug mode.

SAMPLE:

```

Ik

InnoMedia DMS is Enabled
DMS Server is:172.16.0.25:5200
DMS Local port:6880
DMS device type is 63
DMS regionID:1408
DMS Heartbeat type is 1

```



Configuration of IP Information (C)

Viewing the Current IP Information (Cf)

Use the "Cf" command to view your MTA's current IP settings.

SAMPLE:

```
Cf

Your current configuration:
Your WAN port setting:
Ether Address      = 00:10:99:01:ac:34;
You are using DHCP.
Local IP           = 172.16.0.203;
Local IP Mask      = 255.255.0.0;
Local Default GW IP = 172.16.0.1;
Local Default GW Mask = 255.255.0.0;
Primary DNS Server IP = 172.16.0.2;
Your MTA's FQDN    =
System Enable Provisioning Process = FALSE;

Virtual device :
IP address       = 192.168.99.1
Subnet mask      = 255.255.255.0
Gateway IP address = 192.168.99.1
```

Configuring IP Information (Ci)

The "Ci" command is used to configure the IP information such as IP address, default Gateway IP address, DNS server IP address or call agent IP address. In addition, you may modify other host settings as described later in this document. Reboot the MTA when you finish the configuration.

Using DHCP

SAMPLE:

```
Ci

Do you use DHCP to get dynamic IP address and IP mask? [y/n]
Y
Use DHCP to get dynamic IP address, subnet mask and default
gateway's IP.

Do you want to store the changes permanently?[y/n]y
```

Using a Static IP

SAMPLE:

```
Ci
```



```

Do you use DHCP to get dynamic IP address and IP mask? [y/n]
n
Please enter the Gateway FQDN :

Input name is :
Please enter your IP address...
Example: 192.45.6.4
192.168.0.122
IP address entered: 192.168.0.122
Please enter your IP Mask...
255.255.255.0
IP Mask entered: 255.255.255.0
Please enter your Default Gateway IP addr...
192.168.0.1
Gateway IP address entered: 192.168.0.1
Please enter the Primary DNS Server IP Address...
192.168.0.142
Primary DNS Server IP Address Entered: 192.168.0.142
Please enter the Second DNS Server IP Address...
192.168.0.143
Second DNS Server IP Address Entered: 192.168.0.143
Do you want to store the changes permanently? [y/n]y
Please wait for flash update...
Please reboot the system
    
```

Ci configuration description

- DHCP = Answer Y if you use a DHCP server to assign IP addresses. Otherwise, answer N
- Gateway FQDN = You may assign an FQDN (Fully Qualified Domain Name) for this MTA. This step is optional and may be left blank.
- IP Address = Enter the static IP you wish to assign to the MTA
- IP Mask = Enter the Subnet Mask used on your network
- Default Gateway = Enter the IP of the Default Gateway used on your network
- DNS Sever = Enter the primary and secondary DNS server IPs

Configuring MAC Cloning (Co)

A MAC address is the numeric code that identifies a device on a network, such as your external cable/DSL modem or a PC network card. Your service provider may ask you to supply the MAC address of your PC, external modem, or both. To simplify the installation process, MTA automatically grabs the MAC address of your PC's Ethernet card. So you do not need to delay the setup process by informing your service provider of newly installed equipment.

NOTE: If there are more than one PCs connected, MTA will grab the MAC address of the PC that first received the IP address from the DHCP server. If you do not want to use this one, just manually input the MAC address of your other PC in the field.

Use the "Co" command to configure the MAC cloning.

SAMPLE:

```

Co

=====
MAC Clone Configuration
=====
    
```



```

MAC CLONING : DISABLED
CLONED MAC ADDRESS : ff.ff.ff.ff.ff.ff

ENABLE MAC CLONING (y/n): y
Please enter the cloned MAC Address (xx.xx.xx.xx.xx.xx) :
01.00.10.20.00.ff

The cloned Ethernet MAC Address = 01.00.10.20.00.ff
Do you want to store the changes permanently?[y/n]

```

Configuring VLAN Setting (Cv)

The "Cv" command is used to set the parameters for VLAN tagging on the MTA. This advanced feature is only recommended if your network consists of VLAN-enabled servers and components. If you are unsure whether your network is using VLAN, leave it disabled on your MTA. To enable VLAN tagging on the WAN port, select interface "0". To enable VLAN tagging on the LAN port, select interface "1".

SAMPLE:

```

Cv
=====
VLAN CONFIGURATION
=====
c -- change interface VLAN settings
w -- save and quit
p -- print VLAN settings
h -- help
q -- quit without saving
VLAN> p
=====
VLAN CONFIGURATION
=====
CURRENT PHYSICAL INTERFACE No. : 0
VLAN OUTPUT TAGGING : Disabled
IP TOS TO 802.1p PRIORITY MAPPING : Disabled
VLAN Strict mode Disabled
VLAN PVID apply to untagged packet is Disabled
VLAN ID : 0x000
802.1p PRIORITY : 0
VLAN ID for voice RTP data: 0x000
802.1p PRIORITY for voice RTP data: 0
VLAN ID for voice signalling: 0x000
802.1p PRIORITY for voice signalling: 0
VLAN ID for voip data: 0x000
802.1p PRIORITY for voip data: 0

CURRENT PHYSICAL INTERFACE No. : 1
VLAN OUTPUT TAGGING : Disabled
IP TOS TO 802.1p PRIORITY MAPPING : Disabled
VLAN Strict mode Disabled
VLAN PVID apply to untagged packet is Disabled
VLAN ID : 0x000
802.1p PRIORITY : 0

```



```

VLAN> c
MTA global VLAN control is Disable
Do you enable it(y/n)
Y
SELECT PHYSICAL INTERFACE [0-1]
0 is wan AP port
1 is lan AP port 1
1
0: help
1: Vlan Egress tag setting
2: Vlan Ingress strict mode setting
3: pvid apply on ingress untagged packet
4: Pvid setting
5: Priority maping setting
e: Exit

input your choice[0-5 & E]
1

AP 1 ENABLE VLAN Egress TAGGING (y/n): y enable

input your choice[0-5 & E]
2
AP 1 ENABLE VLAN STRICT mode (y/n): y
input your choice[0-5 & E]
3
AP 1 ENABLE PVID to untagged packet(y/n): y
input your choice[0-5 & E]
4
AP 1 PLEASE INPUT VLAN ID [0x000-0xFFFF]: 0x000
AP 1 PLEASE INPUT VLAN PRIORITY [0-7]: 0
input your choice[0-5 & E]
5
AP 1 ENABLE IP TOS TO 802.1p PRIORITY MAPPING (y/n): y
input your choice[0-5 & E]
e
VLAN>w

```

Change Password (Cw)

Use the "Cw" command to change your User Name and Password. The default User Name is **Admin** and Password is **password**.

SAMPLE:

```

Cw
Please input your OLD Password:*****
Please input your NEW Username:innomedia
Please input your NEW Password: *****
Please REENTER your NEW Password: *****

```



```
INFO: read from NVS_PRIMARY (0x9fb)
INFO: write to NVS_SECONDARY (0x9fc)
INFO: write to NVS_PRIMARY (0x9fc)
FS write: OK.
```

Configuring DMS (Cx)

Use the "Cx" command to configure the InnoMedia Device Management System (DMS) settings if you are using one.

NOTE: Please refer to your DMS server settings to configure the DMS parameters on your MTA 6328-2Re.

SAMPLE

```
Cx
InnoMedia DMS feature is available,Disabled
DMS device type is 1
DMS Heartbeat type is 0
DMS Proxy=0.0.0.0:5200
DMS Local port:5200
DMS regionID:1
Do you want to configure it? [y/n] y

InnoMedia DMS feature is disable
Do you want InnoMedia DMS feature? [y/n] y

Do you want to configure UDP DMS Proxy address and port?
[y/n] 172.16.0.123

You current local DMS port is 5200,Do you want to configure
it? [y/n]
y
Please input new local DMS port(UDP):
5202
You current deviceType(1 to 254) is 1,Do you want to
configure it? [y/n]
n
You current regionID(4 bytes integer) is 1,Do you want to
configure it? [y/n]
n
You current HB type is 0,Do you want to configure it? [y/n]
y
Please input new HB type (0 to 1):
1
You new HB type is 1

Do you want to store the changes permanently?[y/n]y
```

Miscellaneous Settings (M)

Viewing MTA SNTP time (M0)

The "M0" command is used to show the SNTP time from the NTP server.



SAMPLE:

M0

```
Currently Date&Time= Wed Apr 23 23:03:40 2008
clock offset is 1259 msec
```

Configuring NTP server (M1)

The "M1" command is used to configure the IP address of the SNTP server. This allows the MTA to synchronize its system time with the NTP server.

SAMPLE:

M1

```
Currently SNTP Server = time.nist.org;
Please enter SNTP servr(FQDN/IPaddress)
Example: 192.45.6.4 or pool.ntp.org
time.nist.org
ntp server is: time.nist.org
current ntp timer zone offset is 0
Do you want to change it?[y/n]
y
input your offset[-12,..13]
-6

Do you want to store the changes permanently?[y/n]y
Y
input your offset[-12,..13]
-8
Do you want to store the changes permanently?[y/n]y
```

Configuring SysLog Server (M2)

The "M2" command is used to configure the IP address of the Syslog server. This will allow the MTA to dump log messages to the remote server for analysis.

SAMPLE:

M2

```
Currently SysLOG Server = [0.0.0.0];
1: system log feature control, currently is disabled
2: system log server configuration
1
Please input your choice. 0:disable;1:enable
1
Do you want to store the changes permanently?[y/n]y
Please wait for flash update...

INFO: read from NVS_PRIMARY (0x59c)
INFO: write to NVS_SECONDARY (0x59d)
INFO: write to NVS_PRIMARY (0x59d) Please reboot the system
```



```

M2
1: system log feature control, currently is enabled
2: system log server configuration
2Currently SysLOG Server = [172.16.0.184];
Please enter SysLOG servr IP address...
Example: 192.45.6.4
10.0.0.202
IP address entered: 10.0.0.202

Do you want to store the changes permanently?[y/n]y
Please wait for flash update...

INFO: read from NVS_PRIMARY (0x59d)
INFO: write to NVS_SECONDARY (0x59e)
INFO: write to NVS_PRIMARY (0x59e)Please reboot the system
R
Are you sure you want to RESET system? [y/n]y

```

Displaying Syslog Message (M3)

The "M3" command is used to allow operators to read log messages from the local log storage. You can choose how many messages to retrieve and the starting point of the first message for viewing.

SAMPLE:

```

M3
How many records you want see?
10
Input start point?
1
IM_display_syslog:index = 1
Do you need see more record ? Y/N
n

```

Configuring Default Timeout Parameters (M4)

The "M4" command is used to configure the default timeout values for dialing features such as dial tone timeout, interdigit timeout, etc.

SAMPLE:

```

M4
Currently timeout setting:
busy tone timeout is 180 seconds
dial tone timeout is 360 seconds
off hook warning tone timeout is 360 seconds
inter_digit_timeout is 16 seconds
ring timeout is 180
do you want change the configuration(y/n):

```



```

y
input busy tone timeout value[0 is infinite]: 120

input dial tone timeout value[0 is infinite]: 180

input offhook warning tone timeout value[0 is infinite]: 360

input inter digit timeout value[0 is infinite]: 10

input ring timeout value[0 is infinite]: 180

do you want save the configuration's change(y/n)do you want
change the configuration(y/n):y

```

M4 configuration description

Busy tone timeout	= the duration of busy tone played in seconds before it times out.
Dial tone timeout	= the duration of dial tone played in seconds before it times out.
Off hook warning tone timeout	= the duration of offhook warning tone played in seconds before it times out.
Inter_digit_timeout	= the length of time in seconds between dialed digitals. If the timer expires while a user is dialing, the MTA will send NTFY with the current partial phone number.
Ring timeout	= the duration in seconds of ringing tone played before it times out.

Configuring RFC3389 (Comfort Noise) Setting (M6)

"M6" command allows you to enable/disable use of RFC3389.

SAMPLE:

```

M6
RFC 3389 (Comfort Noise) is disabled
Do you want enable it?(y/n):
y
do you want save the configuration's change(y/n):y

```

Configuring Global Call Agent Access (M7)

"M7" command allows you to enable/disable use of Global Access. By enabling the Global Call Agent Access, any third party call agent can access the MTA.

SAMPLE:

```

M7
Currently, global access is Disabled

Please input your choice. 0:disable; 1:enable

```

```

1
Do you want to store the changes permanently? [y/n]y
Configurations aren't changed.

```

RFC2833 control (Ma)

"Ma" command allows you to enable/disable use of RFC2833.

SAMPLE:

```

Ma

2833 feature is enabled
Signaling control MTA DTMF 2833 feature
Do you want to change current setting? [y/n]
Y
Please input your choice. 0:By signaling; 1:Force
1
Do you want enable/disable 2833 redundance packet format.
0:disable;1:enable
1
Do you want to store the changes permanently?[y/n]y
Please wait for flash update...

```

System Alive Time (Mb)

For diagnostic purposes, the "Mb" command simply informs you how long your MTA has been running since the last time it was booted up.

SAMPLE:

```

Mb

This system already running 5 days 0 hours 4 minutes 54
seconds

```

Call Agent ID and Port (Mc)

The "Mc" command allows you to view and/or change the current settings for the call agent that your MTA will register to.

SAMPLE:

```

Mc

ch 1 's call agent are:
Primary Call agent ID is      :      ;
Secondary Call agent ID is    :      ;
call agent listen port is     :      2727;
ch 2 's call agent are:
Primary Call agent ID is      :      ;
Secondary Call agent ID is    :      ;
call agent listen port is     :      2727;

```

```
Select line [1-2]('F' to finish)1

Enter Primary Call Agent Name: 172.16.1.120

Enter Secondary Call Agent Name:
Enter call agent signaling port:
2727

Select line [1-2]('F' to finish)F
```

Configuring Dynamic Payload Type Setting (Md)

The "Md" command allows the user to manually set payload types for supported codecs. It is recommended that the automatic settings to be used.

```
Md

Current Dynamic payload types are
CODEC:G729E, payloadtype:96
CODEC:G726-16, payloadtype:97
CODEC:G726-24, payloadtype:98
CODEC:G726-40, payloadtype:99
CODEC:TELEPHONE-EVENT, payloadtype:100
CODEC:TEL-EVE-BLK, payloadtype:101
CODEC:ILBC, payloadtype:102
CODEC:G729B, payloadtype:103
CODEC:G729D, payloadtype:104
Do you want to change the configuration? [y/n]
y
input q for exit

Do you want automatic setting payload type? [y/n]
Y
Do you want to change the configuration? [y/n]
Y
flash writing is done.
Do you want to exit? [y/n]y
```

Configuring Control Parameters (Me)

Use the "Me" command to view or change the current control parameters for Provisioning, DHCP, DHCP Options and Software Upgrade via the provisioning server. The SW_UPGRADE is in effect only when you have provisioning enabled. Otherwise this parameter is ignored. When it is enabled, the MTA will always check if there is a newer software version to download. When it is disabled, MTA will ignore the parameter.

NOTE: After each change, type "Me" again to go back to the Me menu.

SAMPLE:

```
Me

1. DHCP enable
```



```

2. SW_UPGRADE enable
3. NO Provisioning, For Nuera_ORCAV52_NCS; NO SNMP mibs
4. DHCP Check Option 43 disable
5. MTA does not take DHCP option 12 and 15
7. Currently provisioned maximum waiting delay is 3 seconds
8. HTTP Provisioning Server
9. disable endpoint bullet packet
a: setting "x-fresh" bullet packet format
b. TFTP Provisioning Server

Do you want to change [1-9,a-c/N]
    
```

Me configuration description

- | | |
|--------------------------------------|--|
| 1. DHCP | = select this option to enable/disable DHCP. |
| 2. SW_UPGRADE | = select this option to enable/disable software upgrade with the provisioning server. This option is only valid if provisioning is enabled |
| 3. For TFTP Provisioning | |
| • 11: sec_tftp (762) | - secure or non-secure |
| For HTTP Provisioning | |
| • 13: Secure-VSP (9768) | - secure and encryption type RC4. Need InnoMedia utility programs to encrypt configuration file. |
| 4. DHCP Options 43 enable/disable | = enable or disable Option 43 |
| 5. DHCP Option 12 and 15 | = select 1 to take DHCP Option 12 (Host Name) and 15 (Domain Name) |
| 7. Provisioned Maximum Waiting Delay | = enter provisioned maximum waiting delay in seconds. |
| 8. HTTP Provisioning Server | = follow the prompts to enter the Domain Name/IP address and the port number of the HTTP server.
NOTE: Also, can use Qv to configure provisioning parameters. |
| 9. Endpoint bullet packet | = enter the bullet timer in seconds (enter 0 to disable it). |
| a. "x-fresh" bullet packet format | = select either "0:use x-fresh" or "1:use x-keepalive" depending on your network device implementation. |
| b. TFTP Provisioning Server | = follow the prompts to configure the TFTP provisioning server name, default directory, provisioning interval, and encryption key.
NOTE: Also Qv use to configure provisioning parameters. |
| • TFTP Provisioning Server Name | = Enter the TFTP provisioning server name or IP address. |
| • TFTP Provisioning Default | = the directory location of the configuration |



- Directory
- TFTP Provisioning Interval = the time interval in seconds before consecutive provisioning interval
- TFTP Encryption Key = Enter the encryption key if one is used.

Configuring Flash Hook timer (Mf)

Use the "**Mf**" command to change the default timer for sending a flashhook to the MTA. The default setting is 800ms, and you may specify it to be as short as 10ms and as long as 1270ms (step side 10 ms). For most applications, the default setting should be fine. You must reboot in order for changes to take effect.

SAMPLE:

```
Mf
Flash_Hook_timer = 800 ms, range is [10-1270 ms, this value depends on your telephone]

Please enter Flash hook timer setting (ms): 400
Do you want to store the changes permanently? [y/n] y
Writing to Flash, please wait...
Writing to Flash is done successfully.

Reboot system to make new setting effective!
```

Voice Service Control (Mg)

Use "**Mg**" to enable or disable the MTA's ability to make phone calls for all the FXS ports at once.

```
Mg
Current Voice service is enable

Please enter Variant (0:disable; non zero:enable):
```

Jitter Buffer Settings (Mj)

For advanced users, the "**Mj**" command allows you to change the parameters of the MTA's jitter buffer. It is recommended not to change these settings from their defaults. (Default Settings: Frames per Packet=1, and Jitter Buffer Size=60, Adaptive)

SAMPLE:

```
Mj
Jitter Buffer Size (ms) = 60, Adaptive

Do you want to re-configure Jitter buffer size?
Please enter 'y' to configure it or 'q' to exit.
y
```



```

Please enter Jitter Buffer Size (0-400(ms), 0 disable
it)[60]: 50

Jitter Buffer Size Entered: 50
Do you want to fix jitter buffer delay? [y/n] n
Do you want to store the changes permanently? [y/n]y
Writing to Flash, please wait...
Writing to Flash is done successfully.

```

Local Signaling Port (Mk)

The "**Mk**" command is used to set the local signaling port, the RTP port, and T38 fax port for the MTA. The default value for local signaling port is 2427, for RTP port is 6024, and for T38 Fax port is 40000. If an RTP port is blocked by an ISP, you can change that value to any even number between the range of 1024 to 65535.

```

Mk

The Local signaling port is 2427
The Local voice port start at 6024
The Local T38 fax port start at 40000
which port will be changed(1:signal port;2: voice/fax
port;others: exit)
2

Please input the start voice port
2020

Please input the start T38 fax port
40000
Do you want to save it to Flash? (Y/N)y

```

Viewing Line Parameter Settings (Ml)

Use the "**Ml**" command to view the various settings for the FXS port(s) on the MTA. As some MTAs have more than one port, you will need to specify which port settings you want to view.

SAMPLE:

```

Ml

Please input the channel number n/No(1-2) ?1

Channel No =: 0;
1.Line Status is:                2;
2.Line Codec is:                  -1;
3.Line receiveVoiceGain is:      0db;
4.Line transmitVoiceGain is:     0db;
5.Line phone Number is:         aaln/0;
6.Endpoint Name is:              aaln/0;
7.Line silenceDetectionStatus is: 2;
8.Line echoCancellationStatus is: 1;

```

Ml configuration description

Line Status = 1: Not Available
 2: Onhook

3: Offhook
 4: Ringing
 5: Active
 Line Codec = 1: Other
 2: Unknown
 3: G729
 4: G729A
 5: G729E
 6: G711 U-law
 7: G711 A-law
 8: G726
 9: G729
 10: G723
 20: Fax
 Line Receive Voice Gain = Not used
 Line Transmit Voice Gain = Not used
 Line Phone Number = The phone number assigned to this MTA by the server
 Endpoint Name = The MGCP endpoint name of this line
 Silence Detect Status = 1: On
 2: Off
 Echo Cancel Status = 1: On
 2: Off

NOTE: The line codec used is determined by the Call Agent. Therefore, the codec parameters cannot be changed.

Mm Command (Mm)

This command is used only with certain MGCP variants. Please contact InnoMedia if you need to use this feature.

IP Information (Mn)

The “**Mn**” command allows you to individually set the parameters that were specified in the Ci command. Reboot your MTA if you have done any changes.

SAMPLE:

```

Mn
SystemStatus is :          0
Box Mac Address is :      00:10:99:01:ac:34;
0. Local IP is :          172. 16.  0.203;
1. Local Default GW IP is : 172. 16.  0.  1;
2. Local IP Mask is :     255.255.  0.  0;
3. Current HOSTNAME is:
   Current DOMAINNAME is:
   Current FQDN is:
4. Box Server Dns1 is :    172. 16.  0.  2;
5. Box Server Dns2 is :    192.168.  0.  2;
6. Local Default GW Mask is: 255.255.  0.  0;
7. Snmp manager IP is:     0.  0.  0.  0;
8. Snmp community 1 is:    ;
9. Snmp community 2 is:    ;

Which item do you want to change or n/No ?2
    
```



```

Please input Local IP Mask: 255.255.255.0

INFO: read from NVS_PRIMARY (0xb58)
INFO: write to NVS_SECONDARY (0xb59)
INFO: write to NVS_PRIMARY (0xb59)Local IP Mask is :
255.255.255.0

If any change is made, Please reboot the system !

```

Line Configuration (Mp)

Use the "**Mp**" command to enable or disable the FXS ports individually on the MTA.

SAMPLE:

```

Mp

Currently line (1) is enabled

Currently line (2) is enabled
 1. Enable all endpoints
 2. Disable all endpoints
 3. Manually configure each endpoint
3
Do you want to enable line 1 ?[y/n] y
Line 1 enabled.
Do you want to enable line 2 ?[y/n] y
Line 2 enabled.
Do you want to store the changes permanently?[y/n]y

```

Echo Timer Setting (Mq)

Use the "**Mq**" command to set the echo timer when your MTA is installed behind a firewall.

SAMPLE:

```

Mq

The timer is disabled

Please input echo timer (seconds, 0 is disable)
30

Do you want to store the changes permanently?[y/n]y
Please wait for flash update...

```

Configuring the Voice Volume (Mr)

Use the "**Mr**" command to change your MTA's voice volume. You may adjust the volume downwards by entering the negative dB values between 0db to -18db. The default value is 0 dB.

SAMPLE:

```

Mr

```



```

Current RX Gain level is 0
Current TX Gain level is 0
Do you want to change these configuration?[y/n] y
Please enter RX gain Variant (0_-18)db:-1

Please enter TX gain Variant (0_-18)db:-1
Do you want to store the changes permanently? [y/n]y

```

Configure the IP ToS Settings

The Type Of Service (TOS) bits are a set of four-bit flags in the IP header, and each of the four bits has a different purpose. One of the TOS bits may be set at any time, so combinations are not allowed. Set the bit flags to tell the network the type of network service an application requires.

Use the "**Ms**" command to configure the ToS settings.

SAMPLE:

```

Ms

The current TOS settings are:
TOS control for voice Packet is disabled!
TOS control for port 1 is disabled
TOS for MTA Siganling: 0
Do you want to change it [y/n] y
Do you want to enable TOS control for voice packet?[y/n] y
Do you want all channel share same TOS byte? [y/n] y
Please input TOS byte value for MTA's RTP packet (hex)
0

TOS entered = 0
Do you want configure MTA signaling TOS byte? [y/n] y
Please input TOS byte value for MTA's Signaling packet (hex)
0

TOS entered = 0
Do you want to enable TOS control for port 1? [y/n] y
Please input TOS byte value for Port 1(hex)
0

TOS entered = 0

Do you want to save the change to FLASH? (y/n)y

```

Information of VLAN Setting (Mv)

Use the "**Mv**" command to configure the VLAN Settings.

```

Mv

1. VLAN_TAGGING ENABLE!
2. VLAN_TOS_MAPPING DISABLE!

```

```

3. VLAN_ID: 0
4. VLAN_PRIORITY: 0

Which item do you want to change or n/No? 1

Set VLAN tagging ENABLE (Y/N) n
Set VLAN tagging DISABLE

If any change is made, Please reboot the system!

```

Setting endpoint start index (Mu)

The "**Mu**" command allows you to set the starting index of the endpoint aaln/x@[IP or FQDN]. Explicit supports up to 128 alphanumeric characters. If end point is explicitly configured, it must match with the ones defined in the call agent configuration. Otherwise, the call agent will reject the unknown end points. The automatic setting is recommended.

SAMPLE:

```

Mu

The Endpoint start index is automatic
Please input NEW value [-1: automatic, 0~128: start index,
return: keep old value

```

Configuring the Endpoint Name (Mx)

Use the "**Mx**" command to configure the endpoint name for each line.

```

Mx

The Endpoint Names are Automatic

Set Endpoint Name to be Automatic [0] or Explicit[1]:1

Select line [1-1]('F' to finish)1

Enter Endpoint Name: aaln/1
OK for Line 1, Name: aaln/1

Select line [1-1]('F' to finish) F
Do you want to save it to Flash? (Y/N)
Y
Writing to Flash, please wait...
Writing to Flash is done successfully.
Change has been written to Flash, please reboot System!
R

```

Pinging a Remote IP Address (P)

Use the "**P**" command to ping an IP address from MGCP device to verify the network connections.

SAMPLE:

```
P
input remote IP address...
Example: 192.45.6.4
172.16.1.66
IP address entered: 172.16.1.66
echo delay is 0 ms
```

Manually Forcing Security Provisioning (Qr)

Use "Qr" command to force the provisioning process to take place.

NOTE: You must use the "Me, 3" command to enable the provision process prior to use the "Qr" command

SAMPLE:

```
Qr
Sec_GetServAddr: HTTP srvName:172.16.0.123,
srvPort:8802,ticks:860283
IM_Http_Receive_TCP:timeout:10 ret:0
#####Decrypted Data:
Sec-HTTPPI PROV is DONE ,Total Items Found: 44
Sec_GetServAddr: HTTP srvName:172.16.0.123,
srvPort:8802,ticks:860559
```

VSP Security Provisioning Shell (Qv)

Use "Qv" command to configure the provisioning settings.

NOTES: You must use the "Me, 3" command to enable the provision process first. The values entered here must match the configuration on the server. You can also use the "Me, 8" command to configure provisioning settings. The default password for sec_vsp (816), sec_tftp (762), and SecHTTPPI (9768) is 12345678901234567890123456789012.

If you are using InnoMedia GVSP systems, enter GVSP IP address when you first configure provisioning. When the device provisions, it sends "GET" to GVSP redirect server. The GVSP redirect server sends back VSP-5000 IP information in "301 redirect message". The device then sends a "GET" to VSP-5000 IP to request for configuration file. The device updates VSP-5000 information and stores it in the flash. The next "GET" will always be sent to VSP-5000. Only when the device fails to reach the redirected VSP-5000, it then sends GET to GVSP.

SAMPLE:

```
Qv
The current mode is SecHTTPPI !
Your POST Message(0) Is Disabled!
MTA Cfg. File (Including Path): ""
Prov. Server: 172.16.14.151
Prov. Port: 8802
Re-Prov Interval: 0 (sec)
MTA Image URL: ""
```

```

Using Default Prov. Password.
Encryption type:NO Encryption
Please check your password when you use No Encryption Mode!
Because it might still be used for authentication!
You GVSP srv: 172.16.14.151:port:8802 is using!

c -- change Prov. settings
p -- print Prov. settings
w -- write changes to Flash(changes is permanent)
q -- quit.
h -- display the help menu
SecHTTP_Prov> c
Select the item you want to change: ('Q' to quit)
 1. Prov. Server
 2. Prov. Port
 3. Re-Prov. Interval
 4. Prov. Password
 5. Encrytion Type
 6. POST Message Enabled(1:Enabled, 0:Disabled)
 7. Prov. Cfg. File (Including Path)
1

Please enter Prov. Server(either FQDN or IP): 172.16.0.145
SecHTTP_Prov> w
INFO: read from NVS_PRIMARY (0xb79)
INFO: write to NVS_SECONDARY (0xb7a)
INFO: write to NVS_PRIMARY (0xb7a)
FS write: OK.
End of Sec Prov. Settings Configuring Shell.

Qv
The current mode is SecHTTPI !
Your POST Message(0) Is Disabled!
MTA Cfg. File (Including Path): ""
Prov. Server: 172.16.14.151
Prov. Port: 8802
Re-Prov Interval: 600 (sec)
MTA Image URL: "mgcpreliance6328.img_V1.2.0_4"
Using Default Prov. Password.
Encryption type:RC4
You reDir srv:172.16.21.56:port:8802 is using!

c -- change Prov. settings
p -- print Prov. settings
w -- write changes to Flash(changes is permanent)
q -- quit.
h -- display the help menu
SecHTTP_Prov>

```

If you do not have an InnoMedia GVSP system, configure your provisioning server IP address on the your MTA. Device will send a "GET" to your provisioning server to request for configuration file.

SAMPLE

Qv



```

The current mode is SecHTTPI !
Your POST Message(0) Is Disabled!
MTA Cfg. File (Including Path): ""
Prov. Server: 172.16.0.235
Prov. Port: 8802
Re-Prov Interval: 0 (sec)
MTA Image URL: ""
Using Default Prov. Password.
Encryption type:NO Encryption
Please check your password when you use No Encryption Mode!
Because it might still be used for authentication!
You GVSP srv:172.16.0.235:port:8802 is using!
c -- change Prov. Settings

p -- print Prov. settings
w -- write changes to Flash(changes is permanent)
q -- quit.
h -- display the help menu
SecHTTP_Prov> c
Select the item your want to change: ('Q' to quit)
 1. Prov. Server
 2. Prov. Port
 3. Re-Prov. Interval
 4. Prov. Password
 5. Encrytion Type
 6. POST Message Enabled(1:Enabled, 0:Disabled)
 7. Prov. Cfg. File (Including Path)
1

Please enter Prov. Server(either FQDN or IP): 172.16.2.36

SecHTTP_Prov> w
INFO: read from NVS_PRIMARY (0xb7b)
INFO: write to NVS_SECONDARY (0xb7c)
INFO: write to NVS_PRIMARY (0xb7c)
FS write: OK.
End of Sec Prov. Settings Configuring Shell.
Qv

The current mode is SecHTTPI !
Your POST Message(0) Is Disabled!
MTA Cfg. File (Including Path): ""
Prov. Server: 172.16.2.36
Prov. Port: 8802
Re-Prov Interval: 0 (sec)
MTA Image URL: ""
Using Default Prov. Password.
Encryption type:NO Encryption
Please check your password when you use No Encryption Mode!
Because it might still be used for authentication!
You GVSP srv:172.16.2.36:port:8802 is using!

c -- change Prov. settings
p -- print Prov. settings
w -- write changes to Flash(changes is permanent)

```



```
q -- quit.
h -- display the help menu
SecHTTP_Prov>
```

Configuring Router Functions (N)

The "N" command lets you set your PPPoE and NAT bandwidth.

PPPoE Setting configuration (N,1)

Use the "N, 1" command to configure PPPoE function.

SAMPLE:

```
N
Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS control
=====
=   PPPoE CONFIGURATION   =
=====
PPPoEDriver : DISABLE
Service ID: 2
User ID:InnoMedia
Autoconnect = ENABLE
IdleTimeOut = DISABLE
Authentication : PAP
LocalIPAddr 172.16.0.94
PPPSubNet 255.255.255.255
=====
Option 1)Configure 2)Dial 3)HangUp 4)Status 5)Quit:1
PPPoEDriver [DISABLE] 1)Enable 2)Disable :
```

PPPoE configuration Description for ISP

Service ID	= Specifies the service for the PPPoE connection. Your ISP should provide you with the Service ID. If not, enter NULL.
User ID	= Enter the user name for the PPPoE connection.
User Password	= Enter the password for the PPPoE connection
AutoConnect	= If AutoConnect were enabled, system will automatically connect to your ISP when the system boots up.
IdleTimeOut	= Specifies the number of minutes that the connection is idle before the device terminates the connection. A value of 0 disables this function and the connection is never terminated.
Authentication	= Select the authentication method: Password



Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). CHAP provides more security than PAP.

PPPoE Command Description

Configure	Use this command to configure PPPoE feature and settings.
Dial	If system has not connected to your ISP yet, user can use this command to make a connection. If system is currently connected, then this command has no effect.
HangUp	Use this command to terminate current connection. If system has no connection then the command has no effect.
Status	Use this command to obtain current system status. If system is connected to your ISP, then it will show the current Gateway IP, system IP and connection times.
Quit	Use this command to leave PPPoE operation.

Configuring DHCP Server (N, 2) (for Router Device Only)

Use the "N, 2" command to configure the DHCP server.

SAMPLE:

```

N
Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS control
2

Your current DHCP server configuration are:
DHCP server is enabled.
The lowest IP address used by the DHCP server:192.168.99.100
The highest IP address used by the DHCP server:192.168.99.199
The subnet Mask entered:255.255.255.0
Lease time used by the DHCP server:604800 (sec)
Do you want to change it? [y/n] y
Do you want to set configuration to default value? [y/n] n
Current DHCP server is Enabled
Do you want to enable DHCP server? [y/n] n

Disable DHCP server.

Do you want to store the changes permanently?[y/n]y

```



Configuring NAT (Port map) (N, 3) (for Router Device Only)

Port mapping is an advanced configuration in which the router forwards incoming protocols to computers on your local network. You will need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. This feature only works with a static IP assigned to your PC.

The following is an example of how to configure for a web server.

SAMPLE:

```

N
Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS control

3
Configuring NAT Port Map Database:
(each record is a tuple of [External Port No., Protocol,
Internal IP address ,Internal Port No.])
a -- add a new record
d# -- delete the n-th record in the database
w -- write changes to Flash(changes is permanent)
e -- erase all records from the database
p -- print all records in the database on screen
q -- quit.
h -- display the help menu
PortMap>p
Record No./Extnl Port No./Protocol/Internal IP
Address/Internal Port No.
0001          21          TCP          192.168.99.198
21
PortMap>a
Enter NAT external source port(0 ~ 65535): 80

Select porotocol (0)TCP (1)UDP: 0

Enter Internal source IP address: 192.168.99.197

Enter Internal source port:23

PortMap>p
Record No./Extnl Port No./Protocol/Internal IP
Address/Internal Port No.
0001          21          TCP          192.168.99.198
21

```



```

0002          23          TCP          192.168.99.197
23
PortMap>w

INFO: read from NVS_PRIMARY (0x9f8)
INFO: write to NVS_SECONDARY (0x9f9)
INFO: write to NVS_PRIMARY (0x9f9)
FS write: OK.add portmap 80

End of Configuring NAT Port Map Database.

```

Showing DHCP Server Leasing Information (N, 4) (for Router Device Only)

The " N, 4" command shows the DHCP server leasing Information.

SAMPLE:

```

N

Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing infomation
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS controll

4
Current Time is 15356284
Client IP      MAC address      Lease Length
Remaining Time
192.168.99.199 00.c0.9f.b5.59.d1 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.198 00.a0.cc.50.46.f6 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.197 00.a0.cc.d4.24.c9 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.195 00.0e.35.21.2d.07 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.196 00.12.17.66.3d.a6 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.194 00.a0.cc.61.59.cd 7 day(s) 00:00:00 6
day(s) 23:46:41
192.168.99.193 00.e0.eb.76.ac.c5 7 day(s) 00:00:00 6
day(s) 23:46:41

```

Accessing Filtering options (N, 5) (for Router Device Only)

Access filtering is a feature designed to help you regulate the access of internal PCs to the outside Internet. It is useful when you wish to block access to certain websites or addresses for individual PCs that are connected to the MTA.



The MTA offers four ways to control the access available to your internal PCs:

- IP Filtering – Allows you to control what IP, port, and protocol traffic to allow or disallow going out of MTA.
- Domain Filtering – Allows you to block access to specific domains and websites. This is useful for controlling access to certain web addresses. This filtering is a global setting that applies to all PCs connected to your MTA.
- URL Filtering – Allows you to block access to specific URLs. This is useful for controlling access to certain URLs. This filtering is a global setting that applies to all PCs connected to your MTA.
- MAC Filtering –allows you to prevent certain MAC addresses from accessing the Internet. It will also allow certain MAC Addresses to access the Internet and deny all others.

IP Filtering (N, 5, 1):

SAMPLE:

```

N
Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS controll
5
Enter 1 to configure LAN Filter Setting
Enter 2 to configure Domain Filter setting
Enter 3 to configure URL Filter setting
Enter 4 to configure MAC Filter setting
Enter w to write Filter setting to FLASH
Enter q to quit

NAT FILTER>1
a -- add a new record
d# -- delete the n-th record in the database
e -- erase all records from the database
m -- set filter mode
p -- print all records in the database on screen
s -- Enable/Disable this feature
q -- quit.
h -- display the help menu
NAT FILTER>a
Please enter starting IP address: 192.168.99.30

```



```

Please enter ending IP address: 192.168.99.50

Please enter starting Port Number, '*' for any port: *

Select protocol (0) Any (1) TCP (2) UDP: 0

Enter Scheduling mode (0:Scheduling,1:Always):0

Enter Scheduling mode(0:Scheduling,1:Always):0

Enter From-Days (from Sun.(0) to Sat.(6))0

Enter To-Days (from Sun.(0) to Sat.(6))6

Enter From-Times (0-23 hours) 0

Enter From-Times (0-59 min) 0

Enter To-Times (0-23 hours) 23

Enter To-Times (0-59 min) 0
NAT FILTER>s
Do you want to Enable this filter (y/n)?
y
Enabled

```

Domain Filtering (N, 5, 2):

SAMPLE:

```

NAT FILTER>2
a -- add a new record
d# -- delete the n-th record in the database
e -- erase all records from the database
m -- set filter mode
p -- print all records in the database on screen
s -- Enable/Disable this feature
q -- quit.
h -- display the help menu
NAT FILTER>a
Please enter the domain name you want to block
yahoo.com

NAT FILTER>a
Please enter the domain name you want to block
msn.com

NAT FILTER>p

(Domain)IP Filter is disabled

Record No. / Domain
1 yahoo.com
2 msn.com

```



```

NAT FILTER>s
Do you want to Enable this filter(y/n)?
y
Enabled

NAT FILTER>m
1 for block mode, 2 for allow mode
1
NAT FILTER>q

```

URL Filtering (N, 5, 3):

SAMPLE:

```

NAT FILTER>3

a -- add a new record
d# -- delete the n-th record in the database
e -- erase all records from the database
m -- set filter mode
p -- print all records in the database on screen
s -- Enable/Disable this feature
q -- quit.
h -- display the help menu
NAT FILTER>a
Please enter the URL you want to block
http://www.yahoo.com

NAT FILTER>m
1 for block mode, 2 for allow mode
1

NAT FILTER>s
Do you want to Enable this filter (y/n)? y
Enabled

NAT FILTER>p

URL Filter is enabled block mode

Record No. | URL
          1 | http://www.yahoo.com

NAT FILTER>

```

MAC Filtering (N, 5, 4):

SAMPLE:

```

NAT FILTER>4

a -- add a new record
d# -- delete the n-th record in the database
e -- erase all records from the database
m -- set filter mode

```



```

p -- print all records in the database on screen
s -- Enable/Disable this feature
q -- quit.
h -- display the help menu
NAT FILTER>a
Please enter MAC address (xx.xx.xx.xx.xx.xx):
00.84.00.00.48.3c

line:000000000001,TempEntry.MAC[0]:0x0,TempEntry.MAC[1]:0x84,
TempEntry.MAC[2]:0x0,TempEntry.MAC[3]:0x0,TempEn
try.MAC[4]:0x48,TempEntry.MAC[5]:0x3c

Please enter MAC address (xx.xx.xx.xx.xx.xx): q

NAT FILTER>p
MAC Filter is enabled

Record No. |          MAC
          1 | 00840000483c

NAT FILTER>h
a -- add a new record
d# -- delete the n-th record in the database
e -- erase all records from the database
m -- set filter mode
p -- print all records in the database on screen
s -- Enable/Disable this feature
q -- quit.
h -- display the help menu
NAT FILTER>s
Do you want to Enable this filter(y/n)?
y
Enabled

NAT FILTER>q
Quit from MAC filter configuration

Enter 1 to configure LAN Filter Setting
Enter 2 to configure Domain Filter setting
Enter 3 to configure URL Filter setting
Enter 4 to configure MAC Filter setting
Enter w to write Filter setting to FLASH
Enter q to quit

NAT FILTER>w
Write configuration to FLASH memory

```

Configuring MAC Cloning (N, 6) (for Router Device Only)

Use the "N, 6" command to configure the MAC cloning.

SAMPLE:



```

N

Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure NAT Bandwidth
Enter 8 to configure DMZ
Enter 1 to configure link setting

6
=====
MAC Clone Configuration
=====
MAC CLONING : DISABLED
CLONED MAC ADDRESS : 00.00.00.00.00.00

ENABLE MAC CLONING (y/n): y
Please enter the cloned MAC Address (xx.xx.xx.xx.xx.xx):
00.0a.cc.32.f0.fd

The cloned Ethernet MAC Address = 00.0a.cc.32.f0.fd
Do you want to store the changes permanently?[y/n] y
SAVE CONFIGURATION. PLEASE WAIT ...
INFO: read from NVS_PRIMARY (0x9d4)
INFO: write to NVS_SECONDARY (0x9d5)
INFO: write to NVS_PRIMARY (0x9d5)
FS write: OK.
OK
Please reboot the system!!

```

Configuring NAT Bandwidth (N, 7)

Bandwidth control/ Rate limiting is designed to provide QoS for voice packets by designating the amount of bandwidth available on the uplink and downlink ports on the MGCP DEVICE. The control of upstream data bandwidth is useful to prevent data clogging even though voice packets have higher priority over data packets. Rate limiting is only effective if the MGCP DEVICE detects presence of voice calls, and is done with the following steps:

- Upstream:
 - User inputs the WAN bandwidth
 - MGCP Device: Based on the number of active voice calls, calculates available LAN bandwidth = BW(WAN)-BW(voice)

Voice Reserved Bandwidth = Voice Overhead(for 10ms, 5400 Byte/S; for 20ms, 2700 Byte/s) + Voice Bandwidth(for G.711 10ms, 8000 Byte/S)

Data Bandwidth = Total Bandwidth Allocated - Voice Reserved Bandwidth x 1.25

Practical Data Bandwidth = Data Bandwidth - Data Overhead

If no voice call, free running.



- System limits the LAN BW.
- If no active voice calls are in progress, no bandwidth limiting is imposed on the LAN port.

SAMPLE

```

N
Enter 1 to configure PPPoE Setting
Enter 2 to configure DHCP Server setting
Enter 3 to configure Port mapping setting
Enter 4 to show DHCP server leasing information
Enter 5 to configure IP filter
Enter 6 to configure MAC cloning
Enter 7 to configure Bandwidth
Enter 8 to configure DMZ
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS control
7
The bandwidth control is Modifiable
The bandwidth control is Disabled
TCP MSS control for data packet is disabled
Do you want to change it? (y/n)
y
Do you want to make the bandwidth control NOT Modifiable? (y
or n)
n
Do you want to enable bandwidth Control? (y/n)
y
Please enter your total uplink speed (kbps)
256
The speed you entered is 256

Please enter your total downlink speed (kbps)
1500
The speed you entered is 1500

Do you want to save the change to FLASH? (y/n)
y
Please enter your total uplink speed (kbps)
64
The speed you entered is 64
Do you want to save the change to FLASH? (y/n)y

```

Configuring the Networking Mode (N, c)

Use the "N, c" command to set the MTA to be a Router or Switch.

SAMPLE

```

N
Enter 1 to configure PPPoE Setting
Enter 7 to configure Bandwidth
Enter c to configure the Networking Mode (Router or Switch)
Enter t to configure TOS control

```



```

c
The current Networking Mode is: Switch
Do you want to change it? (y or n)
y
Please select the mode: Switch=0, Router=1
1
The new mode is: Router. Do you want save the change and
REBOOT the system? (y or n)y

```

Debug Information (D)

These commands can be invoked when troubleshooting are debugging a faulty MGCP device unit.

Enable Debug Mode (D1) & (D0)

Use the "D1" command to enable debug mode or the "D0" to disable it.

SAMPLE:

```

D1
Debugging is enabled.
D0
Debugging is disabled.

```

Setting Project Variant (D1,Th, 1)

This command is used only with certain MGCP variants. Please contact InnoMedia if you need to use this feature. The password to get into "Th" is "InnoMedia".

Setting Line Reverse mode (D1, Th, 3)

The "D1, Th, 3" command allows you to control the device's reverse polarity feature to determine the start and end of a call for billing purposes. The password to get into "Th" is "InnoMedia".

SAMPLE:

```

D1
Debugging is enabled.
Th
Password:*****
input 17 for get help
1: Setting Project Variant
3: Setting Line Reverse mode

6: G.726 PACKING order is lsn

```



```

7: Configure Internal Network setting
8: MTA do not use UNIT Name for endpoint name
10: Reload the DSP
11: Re_enable DSP serial 0
12: Let DSP play 1KHZ 0dbM test tone to slic
13: Check the phy link status
15: Show and set production status
16: Channel jitter buffer length list
17: Help
18: Setting T38 Fax
19: Cisco T38 not Supported
20: MTA Ping Gateway Disable

22: G.728 PACKING order is lsn
24: Remote RTCP report disabled
25: slic control access
27: Telnet timeout (0 means no timeout, the valid range is 0-
180): No timeout
29: LOOP_START or GROUND_START setting of 2 channels.
30: Enabled detect FAX CNG tone
0: exit
31: Configure Prov 301 reDir Server
32: DSP command practice
33: fusiv chip debug
35: Hardware ID information setting
36: Disabled report remote peer fax/modem signal
37: Display Task & Memory information
38: Configure OSI workaround control
39: Ring mode setting
40: FLASHHOOK is not a persistent event(in MGCP only)
41: OFFHOOK is not a persistent event(in MGCP only)
42: ONHOOK is not a persistent event (in MGCP only)
43: TOS mode is IPV4TOS
44: Apply SLAC Vendor patch is Enabled
45: TIP to RING DC Voltage is 48V
46: Flash side MAC address default value setting
47: Configure the device name in Flash side for default value
48: Clear all configuration in Flash
49: RTP FCS check is Disable
51: Hardware watch dog control
52: Display Version Number with Extension
3
Currently Line Reverse is Enabled

Please enter Variant (1: enable, 0:disable): 1
The entered Variant = 1
Do you want to store the changes permanently? [y/n] y

```

G726 Configuration (D1, Th, 6)

You might need to change the G726 codec configuration in order to obtain optimal voice quality when using this codec. Use the "Th" command within the debugging mode to configure G726 settings. The password to get into "Th" is "InnoMedia".

SAMPLE:



```

D1
Debugging is enabled.
Th

Password: *****
input 17 for get help
6
Please input your choice. 0:lsn;1:msn
1
Do you want to store the changes permanently?[y/n]y

```

Setting T.38 Fax (D1, Th, 18)

When T38 Fax is enabled, ITU-T T.38 support is added, providing a standardized method of supporting reliable fax transmission in the network. When T.38 cannot be successfully initiated between devices, MGCP DEVICE's fax fallback feature allows fax pass-through using a G.711 codec.

In Debugging mode (D1), use the "Th" command to configure the T.38 Fax settings (18). The password to get into "Th" is "InnoMedia".

SAMPLE:

```

D1
Debugging is enabled.
Th

Password:*****
input 17 for get help

18
ch 1 T38 Fax is enabled
Do you want to change?(y or n)

Please input Ch number:(1-4)
1

Please input 1:T38 enabled, 0:T38 disabled
1

Current ch 0 T38 Fax is enabled

t38 jitter buffer is 160 ms (0 disabled)

Do you want to configure jitter buffer (y or n)
y
Please input new jitter buffer (0-240 ms)
200

Current jitter buffer is 200 ms

t38 T2 is 240 ms

Do you want to configure T38 T2 (y or n)
y

```

```
Please input new T38 T2 (0-800 ms , 0 disabled)
200

Current T38 T2 is 200 ms

t38 low speed redundancy is 3

Do you want to configure T38 low speed redundancy (y or n)
y
Please input new low speed T38 redundancy (0-4 , 0
disabled)
1

Current T38 low speed redundancy is 1

t38 high speed redundancy is 1

Do you want to configure T38 high speed redundancy (y or n)
y
Please input new high speed T38 redundancy (0-4, 0
disabled)
1

Current T38 high speed redundancy is 1

t38 bit rate is 14400

Do you want to configure T38 bit rate (y or n)
y
Please input new T38 bitrate (2400,4800,9600,14400)
2400

Current T38 bit rate is 2400

t38 ECM is on

Do you want to configure T38 ECM (y or n)
y
Please input new T38 ECM (0:off,1:on)
1

Current T38 ECM is on

t38 T38FaxMaxBuffer is 200

Do you want to configure T38FaxMaxBuffer (y or n)
y
Please input new T38FaxMaxBuffer (<=500)
300

Current T38FaxMaxBuffer is 2

t38 FaxMaxDatagram is 0

Do you want to configure T38FaxMaxDatagram (y or n)
y
```



```

Please input new T38FaxMaxDatagram (<=316)
300
Fax setting flag 1,port 40000

Fax is using voice port, it is 40000

Do you want to use voice port or fax port (y:voice port or
n: fax port)
y
Current fax port(voice port) is 0

Do you want to store them in flash memory (y or n)
y

```

T.38 Fax configuration description

Jitter Buffer = Enter the jitter buffer size (0-240 ms)

T2 = Timer for awaiting packets (0-800ms)

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. Range varies by platform from 0 (no redundancy) to 4

High speed redundancy = Number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. The value range varies by platform from 0 (no redundancy) to 4.
NOTE: Setting the High Speed redundancy parameter greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.

Bit rate = Enter the fax transmission speed to be attempted: 2400, 4800, 9600, or 14400

ECM = Error Correction Mode (ECM) for the gateway. By default ECM is not enabled.

Fax Max Buffer = Maximum buffer size (default value=200). This option indicates the maximum number of octets that can be stored on the remote device before an overflow condition occurs.

Fax Max Datagram = Maximum datagram size. This option indicates the maximum size of a UDPTL packet that can be accepted by the remote device (default value=300).

Use Voice/ Fax port = Enter y for voice port; enter n for fax port.

Cisco T38 Support (D1, Th, 19)

If you are using Cisco Gateway to terminate off net fax transmissions, use the "**D1, Th, 19**" command to enable the feature. The password to get into "Th" is "InnoMedia".

SAMPLE:

```

D1
Debugging is enabled.
Th
Password:*****
input 17 for get help
19
Please input your choice. 0:disable;1:enable
1

```



```
Do you want to store the changes permanently?[y/n]y
```

Pinging Gateway (D1, Th, 20)

Use the "**D1, Th, 20**" command to enable or disable MGCP device pinging remote gateway. The password to get into "Th" is "InnoMedia".

SAMPLE:

```
D1
Debugging is enabled.
Th

Password:*****
input 17 for get help
20

Please input your choice. 0:disable;1:enable
1
Do you want to store the changes permanently?[y/n]y
```

Enabling/Disabling Detect FAX CNG Tone (D1, Th, 30)

Use the "**D1, Th, 30**" command to enable or disable MGCP device to detect Fax CNG tones. Most faxes send audible beep tones called CNG tones. This tone is a distinct beep that repeats every three (3) seconds. Once a fax has dialed the destination fax number, it generates this tone while waiting for the receiving fax to answer. The password to get into "Th" is "InnoMedia".

SAMPLE:

```
D1
Debugging is enabled.
Th

Password:*****
input 17 for get help
30

Please input your choice. 0:disable; 1:enable
1
Do you want to store the changes permanently?[y/n]y
```

Configuring Provison 301 Redirect Server (D1, Th, 31)

Use the "**D1, Th, 31**" command to configure redirect server. The password to get into "Th" is "InnoMedia". InnoMedia GVSP system provides device provisioning and management functionality. It redirects devices to a provision server like InnoMedia VSP-5000 for remote device provisioning. For more info about 301 Redirect Server, please consult InnoMedia's GVSP Administrator's Guide.

SAMPLE:

```
D1
```



```

Debugging is enabled.
Th
Password:*****
input 17 for get help
31

Your Prov. reDir Server:10.1.1.56

Your Prov. reDir Server port:8802

You reDir srv:10.12.51.56:port:8802 is using!

Please input Your Prov. reDir Server
172.16.0.123

Your New Prov. reDir Server is 172.16.1.123

Please input Your Prov. reDir Server port
8802

Your New Prov. reDir Server port is 8802

Please input 0:to use GVSP,1:to use redirect
1

You reDir srv:172.16.0.123:port:8802 will be used!

Do you want to store the changes permanently?[y/n]y

```

Trace Settings (DI)

Use the "DI" command to configure the trace settings. For most debugging, set the trace level to 80.

SAMPLE:

```

DI
1:show
2:channel
3:group
4:verbose
5:level
6:task
7:store to flash
others: exit
1
UTIL_LOG_GROUP          0x1 -- Disabled
SYSTEM_LOG_GROUP        0x2 -- Disabled
UART_LOG_GROUP          0x4 -- Disabled
FLASH_LOG_GROUP         0x8 -- Disabled
WEB_SERVER_LOG_GROUP    0x10 -- Disabled
DSP_LOG_GROUP           0x20 -- Disabled
SNMP_LOG_GROUP          0x40 -- Disabled
VOIP_LOG_GROUP          0x80 -- Disabled
PROV_LOG_GROUP          0x100 -- Disabled

```



```

EMS_LOG_GROUP          0x200 -- Disabled
DHCPS_LOG_GROUP        0x400 -- Disabled
SYNC_LOG_GROUP         0x800 -- Disabled
TELNET_LOG_GROUP       0x2000 -- Disabled
DQOS_LOG_GROUP         0x4000 -- Disabled
T38_LOG_GROUP          0x10000 -- Disabled
RTCP_LOG_GROUP         0x20000 -- Disabled
JITTER_LOG_GROUP       0x40000 -- Disabled
MGCPSTACK_LOG_GROUP    0x80000 -- Disabled
NAT_LOG_GROUP          0x100000 -- Disabled
ETHERNET_LOG_GROUP     0x400000 -- Disabled
CALL_PROC_GROUP        0x800000 -- Disabled
Trace Group            = 0
Trace Channel          = 0
Trace Level            = 0
Trace Verbose          = Disabled
3
1. Enable VoIP related groups
2. Enable Provisioning & DMS groups
3. Enable ALL groups
4. Display list of all groups (Advanced)
3
All groups are enabled

```

DI Configuration Description

- 1: show – display the current trace settings
- 2: channel – specify the channel (0-7) to be traced. Press enter –1 to trace all the channels
- 3: group – specify the trace group/module. Enter “FFFFFF” to trace all the groups. Enter “0” to turn off all the groups. MGCP device has following Group Settings:

```

UTIL_LOG_GROUP          0x1
SYSTEM_LOG_GROUP        0x2
UART_LOG_GROUP          0x4
FLASH_LOG_GROUP         0x8
WEB_SERVER_LOG_GROUP    0x10
DSP_LOG_GROUP           0x20
SNMP_LOG_GROUP          0x40
VOIP_LOG_GROUP          0x80
PROV_LOG_GROUP          0x100
EMS_LOG_GROUP           0x200
DHCPS_LOG_GROUP         0x400
SYNC_LOG_GROUP          0x800
TELNET_LOG_GROUP        0x2000
DQOS_LOG_GROUP          0x4000
T38_LOG_GROUP           0x8000
RTCP_LOG_GROUP          0x10000
JITTER_LOG_GROUP        0x20000
MGCPSTACK_LOG_GROUP     0x40000
NAT_LOG_GROUP           0x80000
ETHERNET_LOG_GROUP      0x20000
CALL_PROC_GROUP         0x40000

```

- 4: verbose – enable or disable trace verbose. To see more detailed trace log, enable this function; otherwise, disable it.



5: level – specify the trace level to limit the information you would like to see. Enter 0 to disable the trace function, 40 for basic debugging, 60 to access the DSP information, and 80 for most debugging.

6: task – enable or disable tasks.

7: store to flash – Save your debug settings to flash. If you choose not to save the new settings, you will lose the setting at the next reboot.

Displaying List of All Configured Values (Dc)

Use command "**Dc**" to display list of all configured values on your MTA.

SAMPLE:

```
List of all the configuration
Your current configuration:
Your WAN port setting:
Ether Address      = 00:10:99:01:ac:34;
You are using DHCP.
Local IP           = 172.16.0.203;
Local IP Mask      = 255.255.0.0;
Local Default GW IP = 172.16.0.1;
Local Default GW Mask = 255.255.0.0;
Primary DNS Server IP = 172.16.0.2;
Your MTA's FQDN    =
System Enable Provisioning Process = FALSE;

Virtual device :
IP address       = 192.168.99.1
Subnet mask      = 255.255.255.0
Gateway IP address = 192.168.99.1
-----

CURRENT PHYSICAL INTERFACE No. : 0
VLAN OUTPUT TAGGING : Disabled
IP TOS TO 802.1p PRIORITY MAPPING : Disabled
VLAN Strict mode Disabled
VLAN PVID apply to untagged packet is Disabled
VLAN ID : 0x000
802.1p PRIORITY : 0
VLAN ID for voice RTP data: 0x000
802.1p PRIORITY for voice RTP data: 0
VLAN ID for voice signalling: 0x000
802.1p PRIORITY for voice signalling: 0
VLAN ID for voip data: 0x000
802.1p PRIORITY for voip data: 0

CURRENT PHYSICAL INTERFACE No. : 1
VLAN OUTPUT TAGGING : Disabled
IP TOS TO 802.1p PRIORITY MAPPING : Disabled
VLAN Strict mode Disabled
VLAN PVID apply to untagged packet is Disabled
VLAN ID : 0x000
802.1p PRIORITY : 0
-----

InnoMedia DMS is Disabled
```



```
DMS Server is:0.0.0.0:5200
DMS Local port:5200
DMS device type is 1
DMS regionID:1
DMS Heartbeat type is 0
-----
Currently SNTP Server = ;

Currently SysLOG Server = [0.0.0.0];
1: system log feature control is currently Disabled
-----
Current timeout setting:
busy tone timeout is 180 seconds
dial tone timeout is 360 seconds
off hook warning tone timeout is 360 seconds
inter_digit_timeout is 16 seconds
ring timeout is 180
-----

RFC 3389 (Comfort Noise) is disabled
-----

Voice service is enabled

The Local signaling port is 2427
The Local voice port start at 6024
The Endpoint start index is automatic
The Endpoint Names are Automatic
Call Agent configuration:
ch 1 's call agent are:
Primary Call agent ID is      :      ;
Secondary Call agent ID is    :      ;
call agent listen port is    :      2727;
ch 2 's call agent are:
Primary Call agent ID is      :      ;
Secondary Call agent ID is    :      ;
call agent listen port is    :      2727;
-----
Currently line (1) is enabled
Currently line (2) is enabled
-----

2833 feature is enabled

Signalling control MTA DTMF 2833 feature
-----
CODEC:G729E, payloadtype:96
CODEC:G726-16, payloadtype:97
CODEC:G726-24, payloadtype:98
CODEC:G726-40, payloadtype:99
CODEC:TELEPHONE-EVENT, payloadtype:100
CODEC:TEL-EVE-BLK, payloadtype:101
CODEC:ILBC, payloadtype:102
CODEC:G729B, payloadtype:103
CODEC:G729D, payloadtype:104
-----
```



```

DHCP enable
SW_UPGRADE disable
DHCP Check Option 43 disable
MTA does not take DHCP option 12 and 15
-----
NO Provisioning, For ZTE_MGCP; CNC SNMP mibs
Currently provisioned maximum waiting delay is 0 seconds
-----
1. TFTP Prov. Server Name           =
2. TFTP Prov. Default directory    =
3. TFTP Prov. Interval              = 0 seconds
4. TFTP Encryption Key              = *****-----
-----

Flash_Hook_timer = 800 ms,range is [10-1270 ms,this value
depends on your telephone]

Jitter Buffer Size = 60 ms, Adaptive
the echo timer is disabled
-----

Current RX Gain level is 0
Current TX Gain level is 0
-----

The current TOS setting are:
TOS control for voice Packet is disabled!
TOS control for port 1 is disabled
TOS for MTA Sigaling: 0
-----

1. SNMP Manager Address: 0.0.0.0
2. SNMP Community Name #1: (empty)
3. SNMP Community Name #2: (empty)
Bullet packet is disabled
Current bullet packet format is "x-fresh"

=====
=      PPPoE  CONFIGURATION      =
=====

PPPoEDriver : DISABLE
Service ID:
User      ID: UserID
Autoconnect = DISABLE
IdleTimeOut = 30
Authentication : PAP
LocalIPAddr 172.16.0.203
PPPSubNet 255.255.255.255
=====

Your current DHCP server configuration are:
DHCP server is enabled.
The lowest IP address used by the DHCP server:192.168.99.100
The highest IP address used by the DHCP server:192.168.99.199
The subnet Mask entered:255.255.255.0
Lease time used by the DHCP server:604800 (sec)

The current Networking Mode is: Router

```



```
The bandwidth control is Modifiable
The bandwidth control is Disabled
TCP MSS control for data packet is disabled
-----
Admin Name:Admin
Operator Name:User
-----

Current Call Agent Variant = ZTE_MGCP(3001)
Currently RTP MUX(2833 coding) are not enabled
-----

Currently Line Reverse is Enabled
G.726 PACKING order is lsn
G.728 PACKING order is lsn
MTA do not use UNIT Name for endpoint name
-----

Line 1 T38 Fax is disabled
Line 2 T38 Fax is disabled

**** Fax Configuration ****
Jitter Buffer:160 (0-240 ms)
T38 T2: 240 (0-800 ms)
Low Speed Redundancy: 3 (0-4)
High Speed Redundancy:1 (0-20)
Bitrate: 14400 (2400,4800,9600 or 14400)
ECM: On
Max Buffer: 200 (<=500)
Max Datagram: 300 (<=316)
Cisco T38 not Supported
-----

MTA Ping Gateway Disable
Remote RTCP report disabled
Telnet timeout (0 means no timeout, the valid range is 0-
180): No timeout
ch 1 is loop start
ch 2 is loop start
Enabled detect FAX CNG tone
-----

Your Prov. reDir Server:

Your Prov. reDir Server port:0

Your GVSP is using srv::port:0
fusiv lan is Enabled
-----

Disabled report remote peer fax/modem signal
Currently OSI workaround control is On
only le88241/le88231 support unbalance ring
ch 1 is balanced ring
ch 2 is balanced ring
FLASHHOOK is not a persistent event(in MGCP only)
OFFHOOK is not a persistent event(in MGCP only)
ONHOOK is not a persistent event(in MGCP only)
TOS mode is IPV4TOS
Apply SLAC Vendor patch is Enabled
```



```
TIP to RING DC Voltage is 48V
RTP FCS check is Disable
-----
currently, watch dog is Enabled
The Image Version is V1.1.30.1
```

Showing the State of Connections for All Endpoints (Dn)

Use command "**Dn**" to show the state of connections for all endpoints.

SAMPLE:

```
Dn
-----
EndpointName 1: aaln/0
-----
EndpointName 2: aaln/1
-----
```

Showing Notification Information for All Endpoints (Ds)

Use command "**Ds**" to show notification information for all endpoints.

SAMPLE:

```
Ds
-----
Notification Info for aaln/0
-----
[Call Agent Info]
  Primary IP:
  Secondary IP:
    Port: 2727
[Notified Entity]
  IP:
    Port: 2727
Signaling Rx port: 2427
Request ID:
Max Waiting Delay: 0
Event Queue: <>
Hook Switch State: On-Hook
-----
Notification Info for aaln/1
-----
[Call Agent Info]
  Primary IP:
  Secondary IP:
    Port: 2727
[Notified Entity]
  IP:
    Port: 2727
Signaling Rx port: 2427
Request ID:
Max Waiting Delay: 0
```



```
Event Queue: <>
Hook Switch State: On-Hook
```

Showing DHCP Lease Information (Dt)

Use command "**Dt**" to Show DHCP lease information.

SAMPLE

```
Dt
DHCP lease information
-----
Assigned IP address:      172.16.0.203
Subnet mask:             255.255.0.0
Lease time:              604800
T1 timer:                302400
T2 timer:                529200
Server IP address:      172.16.0.2
TFTP server name:
TFTP boot file:
Num time servers:       0
Num DNS servers:        2
DNS server addr #1:     172.16.0.2
DNS server addr #2:     192.168.0.2
Num log servers:        0
Num Gateway:            1
Gateway addr list #1:   0.0.0.0
```

Showing RTP Statistics (Du)

Use command "**Du**" to show RTP statistics.

SAMPLE:

```
Du
[Received packet statistics]
Line   Call_ID                packets   Jitter
Pkt_Loss Avg_Delay
-----
[Transmitted packet statistics]
Line   Call_ID                packets   Jitter
Pkt_Loss
-----
```

MGCP Device Version Information (V)

Use command "**V**" to check MGCP device's current software version.

SAMPLE:

V

```
Umbrella_Version = 1.1.30 Tue Mar 25 15:04:22 2008
Control Code Version = 1.0.18 Tue Mar 25 15:04:22 2008
NO Provisioning, For ZTE_MGCP;
DSP Code Version = 2.5.2 Fri Dec 07 14:24:33 2007;
BBS Code Version = 7.2.36 Tue Mar 25 13:17:10 2007
hardware watch dog is enabled
```

Restoring System Default

The following procedures are used for restoring the default settings of an MGCP DEVICE.

Press <system restore> button on the backside of the MGCP DEVICE for about 5 seconds. Then the message below will show on HyperTerminal.

```
Restoring default setting...
Writing to Flash, please wait...
Writing to flash is done successfully.

Done!
System will RESET after 10 seconds...
```

When the reset finished, the Username and password will return to the system default "Admin" and "adminpass".



Chapter 3

MGCP Device Firmware Updates

Overview

InnoMedia is dedicated to continually improving the quality and features of MGCP DEVICE. This entails regular upgrades to the Digital Signal Process code (DSP) and to the Controller codes. The following section describes the procedure for uploading MGCP DEVICE Firmware through Web interface, an external TFTP or HTTP server to the unit.

Manually Uploading MGCP Device Firmware via Web Interface

To upload the MGCP DEVICE Firmware through the Web interface, follow these steps:

Table 25. Uploading MGCP DEVICE Firmware by Web Interface

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MGCP device.
<i>2</i>	Enter your Username and Password.
<i>3</i>	When the MGCP device Configuration Web page appears, click on Management, and then Firmware Upload. Select the item you want to upgrade: (See Figure 29. Firmware Upgrades). <ul style="list-style-type: none"> ▪ System Image: for system image upgrade. ▪ Boot-loader: for Redboot code upgrade. (Not recommended for remote upgrade.)
<i>4</i>	Click the Browser button to select the image file, or enter directly the location and the file name.
<i>5</i>	Click the Upload button.

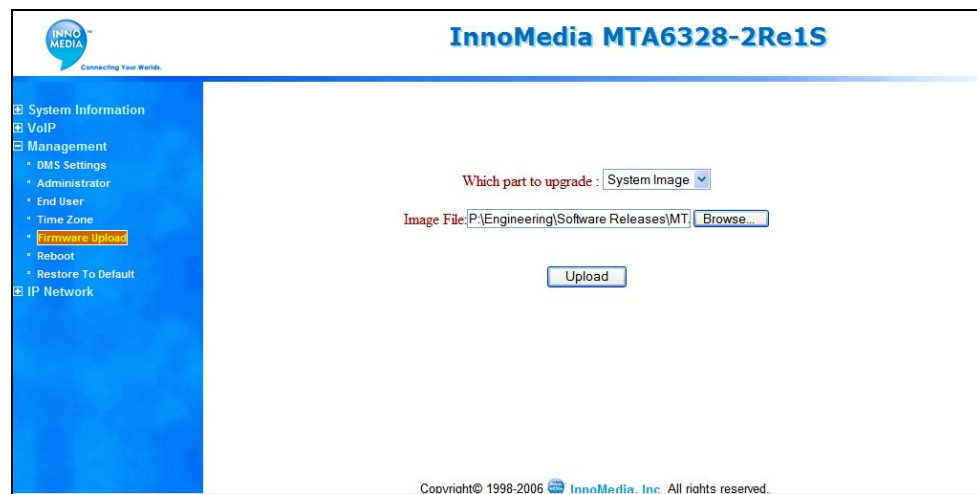


Figure 29. Firmware Upgrades



Auto-upgrading MGCP Device Software Code from Server Side

MGCP device can be upgraded automatically via provisioning process. To perform the procedure, follow these steps:

Table 24. Upgrading MGCP Device Software Code

<i>Step</i>	<i>Action</i>
1	Upload the new firmware to the correct directory on the provisioning server.
2	Change firmware to the intended version in the configuration file
3	Configure your MGCP device: <ul style="list-style-type: none"> • Use the "Me, 3" command to enable and configure provisioning mode (see page 42) • For HTTP provisioning – use the "Me, 8" or "Qv" command to configure the provisioning server settings. For TFTP provisioning – use "Me, b" or "Qv" to configure provisioning server name, default directory, interval, and encryption key (see page 42). • Use the "Qr" command to force provisioning process to begin. (see page 50).
4	MGCP Device will grab the configuration file from the server at the interval set.
5	MGCP Device will compare the file it has with the one specified in the configuration. If the file name is different, MGCP Device will request the new firmware image from the server.



APPENDIX A: MGCP Device LED Indicators

The front panel of the VoIP cable modem has LED indicators that should be understood before configuration. The below table describes each LED indicator.

LED	Blinking State	MGCP Device State
PWR	Steady - Green	The device power is on.
	Off	The device power is off.
RUN	Blinking - Red	The device failed to download a configuration or an image file
	Blinking - Amber	The device is actively downloading a configuration file or a firmware update.
	Steady - Green	The device has been configured successfully and is running normally.
	Off / Other	The device is malfunctioning.
WAN	Blinking – Green (10 Base T) Blinking – Amber (100 Base T)	PC or Voice Data is being transferred.
	Steady – Green (10 Base T) Blinking – Amber (100 Base T)	The device is connected to a broadband network.
	Off	The device is not connected to a broadband network.
LAN	Blinking – Green (10 Base T) Blinking – Amber (100 Base T)	PC Data is being transferred.
	Steady – Green (10 Base T) Blinking – Amber (100 Base T)	The device is connected to an external PC.
	Off	The device is not connected to an external PC.
VoIP	Steady - Green	The VoIP module is internally initialized and the unit is ready to make calls.
	Off	Unit failed to register with all lines
PHONE 1-2	Blinking – Amber	The connected telephone handset is on the hook (not in use) and there are new voice mail messages.

LED	Blinking State	MGCP Device State
	Steady - Green	The connected telephone handset is off the hook
	Off	The connected telephone handset is on the hook (not in use) and there are no new voice mail messages.

NOTE: Blinking rates are to be 1 sec On and 1 sec Off



APPENDIX B - HTTP Provisioning for MGCP Device

Table 26 is a list of provisionable parameters supported in the InnoMedia HTTP provisioning mechanism. You may find some provisioning tags (separated by comma) sharing the same description, that means they are used to set the same variable. For example: Prov_Interval,Provisioning_Interva and Repeat_Interval,Prov_Config_Time,Provisioning_Intervaare both for provisioning Time Zone.

Table 26 MGCP Device Provisioning Tags

PROVISIONING TAGS	PURPOSE	SYNTAX/ EXAMPLE VALUE
MTAVOICESERVICEENABLE	Enable/Disable VOIP Call	Integer (1: Enable; 0: Disable)/ "1"
SNMPMANAGERID	SNMP Manager Address	IPv4 or hostname / "10.90.10.2"
callagentid_x	portx primary call agent (x is port number)	IPv4 or hostname / "12.239.69.100"
callagentid_x_1	portx secondary call agent	IPv4 or hostname / "55.55.55.55"
callagentport_x	portx signaling port	Integer/ "2427"
TOSSIGNALING	Set UDP TOS Value	Hex/ "0xFC"
TRANSMITVOICEGAIN	Voice transmit path gain	Integer (0-18) / "3"
RECEIVEVOICEGAIN	Voice receive path gain	Integer (0-18) / "3"
ADMUSERNAME	Set Admin Login	String / "Admin"
ADMPASSWORD	Set Admin Password	String / "adminpass"
SNMPCOMMUNITY1	SNMP Community 1	String / "public"
SNMPCOMMUNITY2	SNMP Community 2	String / "public"
MGCPCALLAGENTVENDOR	Set Protocol Variant	Integer / "1101"
LINE_REVERSE_ENABLE	Enable/Disable Line Reversal	Integer (1: Enable; 0: Disable)/ "1"
USERAUTHPASSWORD	Set User Login	string / "User"
USERPRIVPASSWORD	Set User Password	string / "userpass"
EndpointInteger_Enable_Line_x	enable/disable line per x	Integer (1: Enable; 0: Disable)/ "1"
AUTOMATIC_ENDPOINT_NAME	use automatic endpointInteger naming and explicit naming.	Integer (1: Enable; 0: Disable)/ "1"
EndpointInteger_Name_Line_x	Assign EndpointInteger Name per line x	String/ "line1"
ENDPOINT_START_INDEX	Set start number of EndpointInteger	Integer (0 to 128)/ "0"
ECHO_TIMER	Set Echo timer	Integer / "0"
BULLET_TIMER	Set null bullet packet timer	Integer / "15"
SET_TIP_TO_RING_VOLT	set tip to ring voltage to 45V or 48 V	Integer/ "45 or 48"
DMS_Enabled	Device EMS enabled or disabled	Integer(1: Enable; 0: Disable)/ "1"
DMS_deviceType	DMS device type	Integer (default=1, valid from 1 to 254)/ "1"
local_DMS_Port	Device dms port to dms proxy	Integer (1024 to 65535)/ "5200"
DMS_Proxy_Addr	DMS Proxy IP	IPv4/ "xxx.xxx.xxx.xxx"
DMS_regionID	Region ID for DMS	Integer / "0"
DMS_HBType	HB Type for DMS	Integer (0-2) / "0"
DMS_Key	Encryption key for DMS	string
PAYLOAD_TYPE_G726_16	Set payload type for G726_16	Integer (96-127) / 96
PAYLOAD_TYPE_G726_24	Set payload type for G726_24	Integer (96-127) / 97
PAYLOAD_TYPE_G726_40	Set payload type for G726_40	Integer (96-127) / 98
PAYLOAD_TYPE_G729E	Set payload type for G729	Integer (96-127) / 99
PAYLOAD_TYPE_TELEPHONE_EVENT	Set payload type for telephone event	Integer (96-127) / 100
PAYLOAD_TYPE_ILBC	Set payload type for ILBC	Integer (96-127) / 104
PAYLOAD_TYPE_TELEPHONE_EVENT_BLOCK	Set payload type for redundancy 2833 block	Integer (96-127) / 101



PROV_ENABLE	Disable Provisioning	Integer (1: Enable; 0: Disable)/ "1"
PROV_SERVER_NAME	Set Provisioning Server Name/IP	IPv4 or hostname / "172.16.3.33"
Prov_Server_Port	Set provisioning server port	Integer / "8802"
PROV_WAIT_DELAY	Set provisioning delay	Integer / "0"
Prov_POST_Enabled	Enable/Disable POST message to prov server	Integer (0:disable 1:enable) / "0"
BULLET_FORMAT	Set bullet format x-Refresh/ X-keepalive	Integer (1: Enable; 0: Disable)/ "1"
SNMP_MIBS	Set SNMP MIBS	string / "11"
SOFTWARE_UPGRADE	Enable Software Upgrade	string / "0-9"
DHCP_OPTION_43	Enable/Disable DHCP option 43	Integer (1: Enable; 0: Disable)/ "1"
DHCP_OPTION_12_AND_15	Enable/Disable DHCP option 12 and 15	Integer (1: Enable; 0: Disable)/ "1"
FLASH_HOOK_TIMER	Set Flash hook timer	Integer (0-800)/ "800"
JITTER_BUFFER_SIZE	Set jitter buffer size	Integer / "60"
FIXED_JITTER	Set fixed or adaptive jitter buffer	Integer (1: Adaptive; 0: Fixed)/ "1"
LOCAL_SIGNALING_PORT	Set MTA local signaling port	Integer / "2427"
LOCAL_RTP_PORT	Set RTP port for voice	Integer / "6024"
HOSTNAME	set device hostname	string / "mta6328re"
ENABLE_VOICE_PORT	Enable voice ports/lines	Integer (1: Enable; 0: Disable)/ "1"
DOMAINNAME	Set device Domain Name	string / "innomedia.com"
PPPOE_ENABLE	Enable/Disable PPPoE	Integer (1: Enable; 0: Disable)/ "1"
PPPOE_SERVICEID	PPPoE Service ID	string / "abcdefg"
PPPOE_USERID	PPPoE User ID	string / "abc"
PPPOE_USERPW	PPPoE User Password	string / "xyz"
PPPOE_AUTOCONNECT	Auto Connection	Integer (1: Enable; 0: Disable)/ "1"
PPPOE_IDLETIMEOUT	Idle Time out	Integer / "3600"
PPPOE_AUTH_PROTOCOL	Authentication Protocol: PAP or CHAP	String / "PAP"
G726_PACKING_ORDER	Select G726 packing order	Integer (1: lsn; 0: msn)/ "1"
G728_PACKING_ORDER	Select G728 packing order	Integer (1: lsn; 0: msn)/ "1"
NTP_TIME_OFFSET	Set the time offset for NTP	Integer / "-5"
SNTP_SERVER	Set the server address for SNTP	IPv4 or FQDN/ "time.nist.gov"
VIRTUAL_LOCAL_IP	Set the virtual IP of LAN adapter	IPv4 / "192.168.99.1"
VIRTUAL_LOCAL_IP_MASK	Set the submask of LAN adapter	IPv4 / "255.255.255.0"
VIRTUAL_GATEWAY_IP	Set the default gateway of LAN adapter	IPv4 / "192.168.1.254"
Enable_DHCP	Enable DHCP client for WAN adapter	Integer (1: Enable; 0: Disable)/ "1"
Local_IP	Set static IP for WAN adapter	IPv4 / "172.16.1.254"
Local_IP_Mask	Set submask for WAN adapter	IPv4 / "255.255.0.0"
Gateway_IP	Set default gateway for WAN adapter	IPv4 / "172.16.0.1"
DNS_IP_addr	Set DNS server1 address for WAN adapter	IPv4 / "172.16.0.2"
DNS_IP_addr_2	Set DNS server2 address for WAN adapter	IPv4 / "172.16.0.3"
CPE_Tos_Enabled	Control CPE side tos apply status	Integer (1: Enable; 0: Disable)/ "1"
LAN1_Tos_Enabled	Control Lan1 tos apply status	Integer (1: Enable; 0: Disable)/ "1"
LAN2_Tos_Enabled	Control Lan2 tos apply status	Integer (1: Enable; 0: Disable)/ "1"
CPE_Tos_Byte	CPE port TOS setting	hex value/ "0xFC"
LAN1_Tos_Byte	Lan1 port TOS setting	hex value/ "0xE0"
LAN2_Tos_Byte	Lan2 port Tos setting	hex value/ "0xD0"
UPGRADE_URL	Address of firmware upgrade file	http://200.60.54.71:8802/config/mta6328R_1_1_28_us.img
ENABLE_VLAN_ALL	enable/disable vlan	Integer (1: Enable; 0: Disable)/ "1"
ENABLE_VLAN_ENGRESS_WAN	En/Disable VLAN tag on WAN	Integer (1: Enable; 0: Disable)/ "1"



SET_VLAN_STRICT_MODE_WAN	Set VLAN strict mode on WAN	Integer (1: Enable; 0: Disable)/ "1"
ENABLE_PVID_TO_UNTAG_PKT	En/Disable PVID to untagged packet	Integer(1: Enable; 0: Disable)/ "1"
SET_VLAN_ID_WAN	Set VLAN ID on WAN	Integer 3 digits/ "001"
ENABLE_TOS_MAPPING_WAN	Enable/Disable TOS priority mapping	Integer (1: Enable; 0: Disable)/ "1"
SET_TOS_VALUE_WAN	Set TOS Value on WAN	Integer (0-7)/ "5"
SET_VLAN_ID_VOICE	Set VLAN ID on VOICE	Integer 3 digits/ "001"
SET_VLAN_ID_SIGNAL	Set VLAN ID on VOICE SIGNAL	Integer 3 digits/ "001"
SET_VLAN_ID_DATA	Set VLAN ID on DATA	Integer 3 digits/ "001"
SET_TOS_VALUE_VOICE	Set TOS Value on VOICE	Integer (0-7)/ "5"
SET_TOS_VALUE_SIGNAL	Set TOS Value on VOICE SIGNAL	Integer (0-7)/ "5"
SET_TOS_VALUE_DATA	Set TOS Value on DATA	Integer (0-7)/ "5"
SET_FILLTER_WAN	Set VLAN ID Filter on WAN	vID strings separated with semicolon ";"
ENABLE_VLAN_ENGRESS_LAN1	En/Disable VLAN tag on LAN1	Integer (1: Enable; 0: Disable)/ "1"
SET_VLAN_STRICT_MODE_LAN1	Set VLAN strict mode on LAN1	Integer (1: Enable; 0: Disable)/ "1"
ENABLE_PVID_TO_UNTAG_PKT_LAN1	En/Disable PVID to untagged packet	Integer (1: Enable; 0: Disable)/ "1"
SET_VLAN_ID_LAN1	Set VLAN ID on LAN1	Integer 3 digits/ "001"
ENABLE_TOS_MAPPING_LAN1	Enable/Disable TOS priority mapping	Integer (1: Enable; 0: Disable)/ "1"
SET_TOS_VALUE_LAN1	Set TOS Value on LAN1	Integer (0-7)/ "5"
SET_FILLTER_LAN1	Set VLAN ID Filter on LAN1	vID strings separated with semicolon ";"
ENABLE_VLAN_ENGRESS_LAN2	En/Disable VLAN tag on LAN2	Integer (1: Enable; 0: Disable)/ "1"
SET_VLAN_STRICT_MODE_LAN2	Set VLAN strict mode on LAN2	Integer (1: Enable; 0: Disable)/ "1"
ENABLE_PVID_TO_UNTAG_PKT_LAN2	En/Disable PVID to untagged packet	Integer (1: Enable; 0: Disable)/ "1"
SET_VLAN_ID_LAN2	Set VLAN ID on LAN2	Integer 3 digits/ "001"
ENABLE_TOS_MAPPING_LAN2	Enable/Disable TOS priority mapping	Integer (1: Enable; 0: Disable)/ "1"
SET_TOS_VALUE_LAN2	Set TOS Value on LAN2	Integer (0-7)/ "5"
SET_FILLTER_LAN2	Set VLAN ID Filter on LAN2	vID strings separated with semicolon ";"