

InnoMedia EMTA 6528-2(R)e Administrator's Guide

Document v1.0

September, 2006



Table of Contents

About This Document.....	7
Getting Started with the MTA.....	8
Setting up Your Computer.....	8
MTA Configuration.....	10
Overview	10
Configuring MTA via Web User Interface.....	10
Logging In.....	10
Configuring Network Settings	11
Configuring External IP Address	11
Configuring Internal IP Address	13
Configuring VLAN Setting.....	13
Configuring PPPoE Settings	14
PPPoE Status.....	15
Configuring Provisioning Settings.....	16
Configuring DMZ Settings	17
Configuring SNMP Settings	18
Configuring NAT Port Mapping.....	19
Configuring Voice QoS Setting	21
Configuring Access Filtering options	22
IP Filtering	22
Domain Filtering	23
URL Filtering.....	24
MAC Filtering.....	25
Configuring DHCP Server Information	26
Configuring MAC Cloning	29
Configuring VoIP Settings.....	30
Configuring Configuration File.....	30
Configuring SIP Proxy Settings	31
Configuring User Account	32
Information	34
Registration Status & Critical Messages	34
Management.....	34
Changing Administrator ID and Password.....	34
Changing End User ID and Password	35
Rebooting MTA	36
Restoring Factory Default.....	36
Configuring MTA via Telnet/ HyperTerminal Interface	38
Overview.....	38
Before You Begin	38
Logging In.....	38
Help (H)	38
Viewing the Current IP Information (Cf).....	40
Configuring IP Information (Ci).....	40
Configuring Local IP (Ci, 1)	41
Setting DNS (Ci, 2).....	42
Setting SIP Proxy Server IP (Ci, 3).....	43
Setting IP Settings for All (Ci, 4)	43
Configuring other Local Host settings (Ci, 5)	43
Other Local Host settings configuration description.....	44



Specifying the preferred CODEC (Ci ,5 , 1)	44
Configuring Jitter Buffer Size (Cj).....	45
Changing Voice Volume (Ga).....	45
Information about the System	46
Displaying the current setting of digitmap (Id)	46
Displaying Voice Volume Level (Ig).....	46
Displaying the State of All Ports/Lines (Is)	47
Displaying Network Connection (Ix).....	47
Displaying DMS parameters (Ik)	47
Display Fax parameters (If).....	47
Displaying FXS Setting Parameters (It)	48
Configuring Router Functions (N).....	48
PPPoE function configuration (N,1)	48
Configuring DHCP Server (N, 2).....	50
Configuring NAT (Port map) (N, 3)	51
Showing DHCP Server Leasing Information (N, 4).....	51
Accessing Filtering options (N, 5)	52
Configuring MAC Cloning (N, 6).....	53
Configuring NAT Bandwidth (N, 7)	53
Configuring DMZ (N, 8).....	54
Showing Configure Link Setting (N, 1)	55
Changing your User Name and Password.....	56
Other Commands	56
Configuring 2833 (C2).....	56
Enabling/Disabling Call Features (C3)	56
Configuring Digit Map (Cd)	57
Configuring SIP Settings (Cs).....	60
Configuring FXS settings parameters (Ct)	63
FXS Settings Parameters configuration description	63
Configuring SIP user account (Cu)	64
Enabling/Disabling Polarity Reversal (Cr).....	64
Configuring Virtual LAN Setting (Cv)	64
Configuring DMS (Cx)	65
Miscellaneous	66
Configuring Control Parameters (Me)	66
Configuring Flash Hook timer (Mf).....	67
Showing Syslog (Mh)	68
Configuring SNTP server (Mi)	68
Configuring Remote Services (Mm)	69
Selectable Configuration of IP Elements (Mn)	70
Phone Line Configuration (Mp).....	70
Configuring Phone lines (Mq).....	71
Configure Networking Mode (Mw)	71
Signing on to softswitch (Sn).....	71
Signing off of the softswitch (Sf).....	72
Provisioning	72
Configuring Provisioning Setting (Pv).....	72
Triggering Provisioning (Pr)	74
Pinging a Remote IP Address (P)	75
MTA Version Information (V)	75
Restoring System Default	75
MTA Firmware Updates.....	77
Overview.....	77
Manually Uploading MTA Firmware via Web Interface.....	77
Auto-upgrading MTA Software Code from Server Side	78
Working with the Cable Modem	79

Overview	79
Telnet to the Cable Modem	79
General Commands	79
help	79
!	80
?	80
REM	80
cd	81
dir	81
find_command	81
history	82
instances	82
ls	82
man	83
pwd	83
sleep	83
syntax	83
system_time	84
usage	84
TelMTA_console	84
emta_console	85
exit	85
ping	85
read_memory	86
reset	86
run_app	87
shell	87
version	87
write_memory	88
zone	88
HeapManager Table Commands	89
memShow	89
stats	89
threadUsage	90
trace	90
walk	90
walk_alloc	91
docsis_ctl Table Commands	91
binarySfid	91
bpiShow	91
cfg_hex_show	92
cfg_tlv_show	92
clear_image	92
comp_mac_to_phy	93
comp_phy_to_mac	93
copy_image	93
dload	94
dsdiag	94
dsx_show	95
goto_ds	95
goto_us	95
IgmpShow	96
ip_initialize	96
ip_show	96
log_messages	97
map_debug	97



modem_caps	98
rate_shaping_enable.....	98
rng_rsp	98
scan_stop.....	99
showFlows	99
state	99
stop_download	100
ucdShow.....	100
ucddiag.....	100
up_dis.....	101
us_phy_oh_show	101
usdiag.....	101
embedded_target Table Cammands	102
bcmalloc_show	102
embedded_target.....	102
cp0_read.....	102
cp0_write	103
dcache	103
icache	103
emta Table Commands	104
emta.....	104
addFirewallRule.....	104
announcementDload	104
anti_spoof.....	105
call_in_progress	105
cfgfile.....	105
deleteFirewallRule	106
dhcp_init	106
emta_console	106
firewallEnable	107
ifEntry	107
initState	107
ip_get	108
ip_initialize	108
lineState	108
log	109
new_line.....	109
option_get	109
release_lease	110
renew_lease.....	110
run_app	110
server_get.....	111
showAnnounce.....	111
showFirewallState.....	111
snmp_ip_update	111
soft_reset.....	112
suboption_get.....	112
test_v3.....	112
flash Table Commands	113
autoTest.....	113
cfi_show.....	113
close	114
configRegion.....	114
deinit	114
erase	115
init	115

open.....	115
read	116
readDirect.....	116
show	116
write	117
writeArray	117
Appendix A - EMTA LED Specification	118



About This Document

The InnoMedia EMTA Multimedia Terminal Adapter is a device that provides standard telephony service and broadband Internet access over a DOCSIS™ cable network. Designed for ease of installation and use, EMTA will allow you to place and receive regular telephone and fax calls.

The purpose of this manual is to give system integrators and service operators detailed reference information on EMTA commands necessary for unit's configuration and provisioning.

This manual can be used for both router (EMTA 6528-2Re) and non-router (EMTA 6528-2) EMTAs. If your EMTA does not have the router function, please skip the router configuration sections in this manual.

NOTE: Any UPS connected to the EMTA's UPS connector port must comply with UL and other related safety certifications. The power supply and cord must be earth grounded.



Getting Started with the MTA

Setting up Your Computer

By default, all MTAs are factory set to a static IP address of 192.168.99.1. Therefore, you will need to setup your PC to be on the same subnet so that you can configure the MTA.

Connect a PC to the port marked LAN on your MTA and follow these steps to configure the IP settings for your PC. We recommend that you reference your Operating System manual on how to configure your PC. We will give an example of how to do this with Windows XP below:

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

Table 1. 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 1. Setting up Your Computer – Network Connections).
5	Choose Properties.

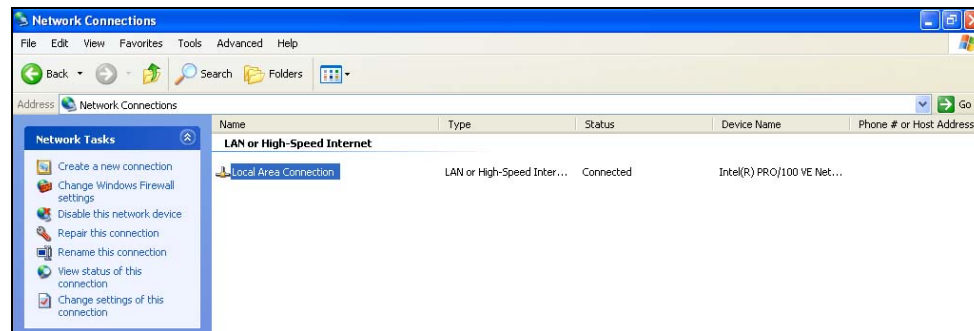


Figure 1. Setting up Your Computer – Network Connections

Table 2. Setting up Your Computer

<i>Step</i>	<i>Action</i>
6	Double Click on TCP/IP (See Figure 2. 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 MTA. The MTA has a default of 192.168.99.1 so if you enter 192.168.99.5, you should have no problem connecting to the MTA. (See Figure 3. Setting up Your Computer - Using a Static IP)
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.

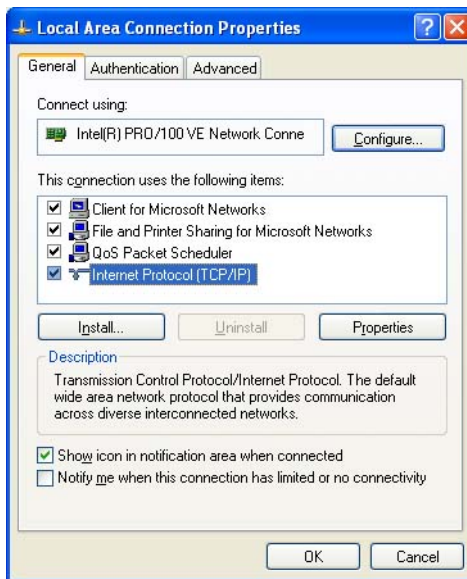


Figure 2. Setting up Your Computer - Local Area Connection Properties

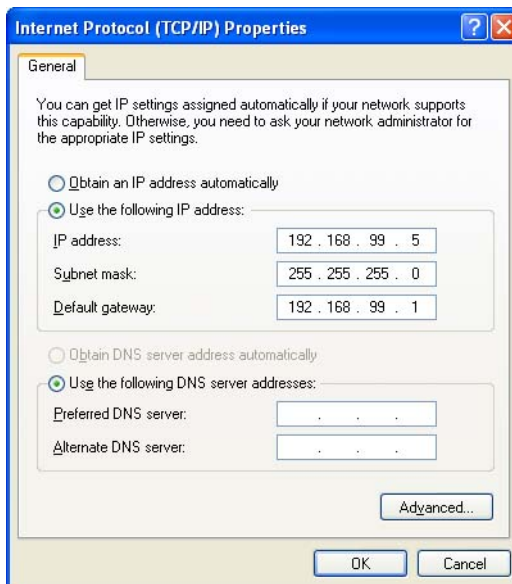


Figure 3. Setting up Your Computer - Using a Static IP

MTA Configuration

Overview

Setup and configuration of the MTA 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. If you have not completed the steps outlined in the Before you Begin section, please do so before proceeding the following.

The MTA 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 may be assigned by either DHCP or Static IP.

Configuring MTA via Web User Interface

Logging In

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

Table 3. Web User Interface - Logging in

<i>Step</i>	<i>Action</i>
1	Open your web browser and enter the IP address of the MTA. 192.168.99.1 is the default address. The Login Dialogue Box as shown in Figure 4 appears.
2	Enter your Username and Password. NOTE: The default User Name is "Admin" and Password is "password".
3	Click OK.



Figure 4. MTA Login Dialogue Box

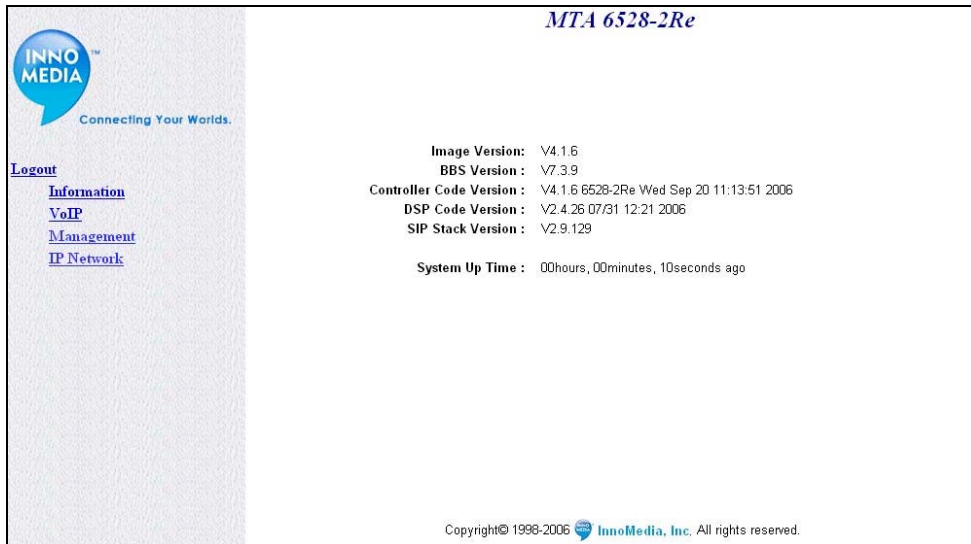


Figure 5. MTA Web User Interface - Main Page

Configuring Network Settings

MTA 6528-2(R)e needs two IP addresses, one is for WAN and one is for LAN. In MTA 6528-2(R)e the WAN port is referred to as "external" and LAN port is referred to as "internal" or "Virtual device".

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

The IP used by LAN is a "private" IP. The Default IP is 192.168.99.1.

Configuring External IP Address


To configure the external port, follow these steps:

Table 4. Configuring Network Setting

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA at http://192.168.99.1 (See Logging In on page 10 for more details).
2	Click on IP Network, then Interface Setting.
3	Select External Port from the drop-down list.
4	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 (Name of unit). This information should be supplied by your ISP or network administrator.
5	Select the Link Speed based on the device you connected to by clicking the appropriate radio button. Auto speed enables devices to automatically exchange information over a link and negotiate the speed based on the connection to the other end.
6	Select the Link Mode by clicking the appropriate radio button. Auto duplex enables devices to automatically exchange

	information over a link and negotiate the mode based on the connection to the other end.
7	Once data has been entered, please Save & Reboot or click the Reset button to undo your changes.

MTA 6528-2Re



Connecting Your Worlds.

[Logout](#)

[Information](#)

[VoIP](#)

[Management](#)

[IP Network](#)

[Interface Setting](#)

[Provisioning Setting](#)

[DMZ Setting](#)

[SNMP Setting](#)

[NAT PortMap](#)

[Voice QoS Settings](#)

[Access Filtering](#)

[DHCP Server](#)

[MAC Cloning](#)

[PPPoE Setting](#)

[PPPoE Status](#)

Configure Network Setting

External Port External Port

MAC Address 00:10:99:02:64:d1

VLAN Setting

☐ Enable VLAN Tagging

VLAN ID [0x000 - 0xFFF]

☐ Enable Priority Mapping (IP TOS -> 802.1p)

IEEE 802.1p Priority [0 - 7]

IP Setting

☒ Enable DHCP

IP Address

Subnet Mask

Default Gateway

DNS #1

DNS #2

FQDN

Link Speed

☒ Auto Speed ☐ 100MB ☐ 10MB

Link Mode

☒ Auto Duplex ☐ Full Duplex ☐ Half Duplex

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

Figure 6. Configuring Network Setting

Configuring Internal IP Address

To configure Internal IP Address, follow these steps:

Table 5. Configuring Internal IP Address

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on IP Network, then Interface Setting. From the pull down menu, select Internal Port.
3	Enter the IP Address for your Virtual Port, Subnet Mask, and Default Gateway. NOTE: The factory default for the MTA is 192.168.99.1. For most users, you may use the default settings and simply click the Save & Reboot button to continue.
4	Select the Link Speed based on the device you connected to by clicking the appropriate radio button. Auto speed enables devices to automatically exchange information over a link and negotiate the speed based on the connection to the other end.
5	Select the Link Mode by clicking the appropriate radio button. Auto duplex enables devices to automatically exchange information over a link and negotiate the mode based on the connection to the other end.
6	Once data has been entered, please Save & Reboot or click the Reset button to undo your changes.

Figure 7. Configuring Internal IP Address

Configuring VLAN Setting

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.

Table 6. Configuring VLAN Setting

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA at http://192.168.99.1 (See Logging In on page 10 for more details).
2	Click on IP Network, then Interface Setting.
3	Click the Enable the VLAN Tagging to enable the feature.
4	Enter the VLAN ID.
5	Click the option box to enable the Priority Mapping feature.
6	Enter the priority value in the field.
7	Once data has been entered, please Save & Reboot or click the Reset button to undo your changes.

MTA 6528-2Re

Configure Network Setting

External Port

MAC Address 00:10:99:02:64:d1

VLAN Setting

☒ Enable VLAN Tagging

VLAN ID [0x000 - 0xFFF] 0x0FFF

☒ Enable Priority Mapping (IP TOS -> 802.1p)

IEEE 802.1p Priority [0 - 7] 1

IP Setting

☒ Enable DHCP

IP Address 0.0.0.0

Subnet Mask 255.255.255.192

Default Gateway 0.0.0.0

DNS #1 10.241.14.2

DNS #2 0.0.0.0

FQDN 0010990264d1.cbt

Link Speed

☒ Auto Speed ☐ 100MB ☐ 10MB

Link Mode

☒ Auto Duplex ☐ Full Duplex ☐ Half Duplex

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

Figure 8. Configuring VLAN Setting

Configuring PPPoE Settings

If your ISP provides your external IP address using PPPoE, then you will need to configure your MTA 6528-2(R)e so that it will be able to establish a PPPoE connection. To configure PPPoE settings, follow these steps:

Table 7. Configuring PPPoE settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on IP Network, then PPPoE Settings.
3	Click Enable PPPoE to enable the service.
4	Enter your Service ID if provided by your ISP. Otherwise, leave this field blank.

5	Enter your User ID, sometimes referred to as Username.
6	Enter your Password.
7	Choose the Authentication Protocol.
8	Enter the idle time out in minutes. Entering 0 means the link is connected all the time.
9	Click Save & Reboot to save your settings and reboot the MTA, or click the Reset button if you want to undo your changes.

NOTE: If you are using a static IP, refer to Configuring External IP Address section 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.

MTA 6528-2Re

Configure PPPoE Settings

Please complete the following form to define or modify the PPPoE settings.

Enable PPPoE: ☒ • Check the box if you would like to enable PPPoE function.

Service ID: • Enter the Service ID here.

User ID: • Enter the User ID here.

Password: • Enter the Password here.

Authentication Protocol: • Select the Authentication Protocol.

Idle Time Out (min): • Enter the idle time out here. Entering 0 means the link is connected all the time.

• Modification will **not** take effect unless you click on the **Save & Reboot** button to save to flash memory and reboot.

• Click on the **Reset** button to restore old entries.

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

Figure 9. Configuring PPPoE settings

PPPoE Status

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



Figure 10. Current PPPoE Connection Status

Configuring Provisioning Settings

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

Table 8 Configuring Provision Settings

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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 the Save & Reboot button or click the Reset button to undo your changes.



MTA 6528-2Re

Configure Provisioning Setting

Please complete the following form to define or modify the Provisioning settings.

Enable Provisioning : ☒

Server Name : 172.16.0.123

Port number : 8802

- Check the box if you would like to enable provisioning function.
- Enter the provisioning server name.
- Enter the port number.
- Modification will **not** take effect unless you click on the **Save & Reboot** button to save to flash memory and reboot.
- Click on the **Reset** button to restore old entries.

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

Figure 11. Configuring Provisioning Settings

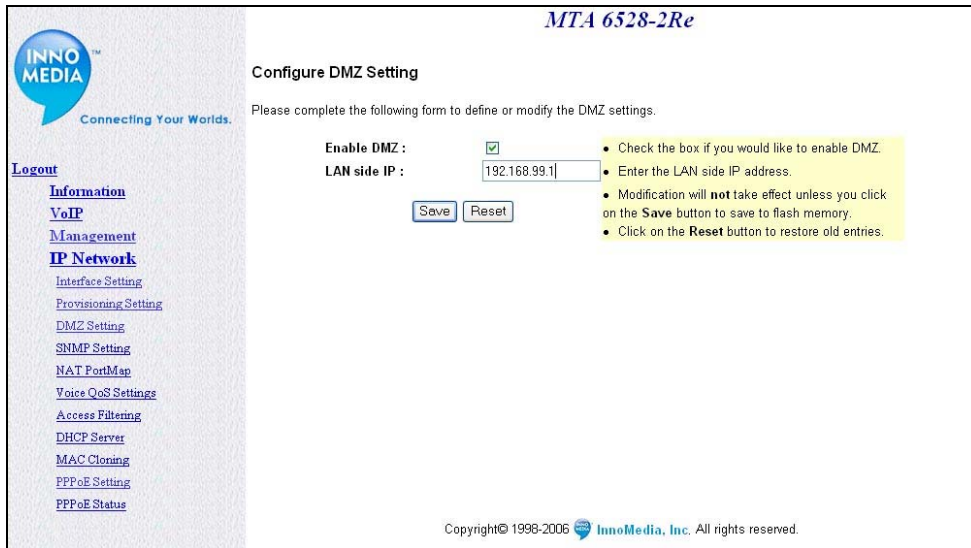
Configuring DMZ Settings

Demilitarized Zone (DMZ) removes the router's firewall protection from one PC, allowing it to be "seen" from the Internet. It is recommended that you set your computer with a static IP if you want to use DMZ. The DMZ feature allows a local user to be exposed to the Internet for using a special-purpose service such as Internet gaming or Video-conferencing.

To configure DMZ setting, do the following steps:

Table 9 Configuring DMZ Settings

Step	Action
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on IP Network, then DMZ Setting.
3	Check the option box to enable the DMZ feature.
4	Enter the IP address of your PC that is connected to the MTA.
5	Click the Save & Reboot button to save your changes, or click the Reset button to undo your changes.



MTA 6528-2Re

Configure DMZ Setting

Please complete the following form to define or modify the DMZ settings.

Enable DMZ : ☒

LAN side IP :

- Check the box if you would like to enable DMZ.
- Enter the LAN side IP address.
- Modification will **not** take effect unless you click on the **Save** button to save to flash memory.
- Click on the **Reset** button to restore old entries.

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

Figure 12. Configuring DMZ Settings

Configuring SNMP Settings

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

Table 10. Configuring SNMP Setting

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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 the Save & Reboot button to save your changes, or click the Reset button to undo your changes.



Figure 13. Configuring SNMP Setting

Configuring NAT Port Mapping


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 11. Configuring NAT Port Mapping

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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.

MTA 6528-2Re



Connecting Your Worlds.

Logout

[Information](#)

[VoIP](#)

[Management](#)

[IP Network](#)

[Interface Setting](#)

[Provisioning Setting](#)

[DMZ Setting](#)

[SNMP Setting](#)

[NAT PortMap](#)

[Voice QoS Settings](#)

[Access Filtering](#)

[DHCP Server](#)

[MAC Cloning](#)

[PPPoE Setting](#)

[PPPoE Status](#)

Configure NAT Port Map Database

Please complete the following form to add, update, and delete entries in the NAT Port Map database.

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
<input type="checkbox"/>	69	UDP	196.168.99.198	69	User Defined
<input type="checkbox"/>		UDP			User Defined
<input type="checkbox"/>		UDP			User Defined
<input type="checkbox"/>		UDP			User Defined
<input type="checkbox"/>		UDP			User Defined

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.

- Enter a new entry in any empty entry.
- Select an Application to set the default Port and Protocol.
- Check the box to the left of an entry and click **Save** to delete the entry.
- An example of Internal source IP address is 90.0.0.20.
- Modification will **not** take effect unless you click on the **Save** button to save to flash memory.
- Click on the **Reset** button to restore old entries.


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

Figure 14. Configuring NAT Port Mapping

EXAMPLE:

Figure 15 is a sample illustration of the NAT Port Mapping.

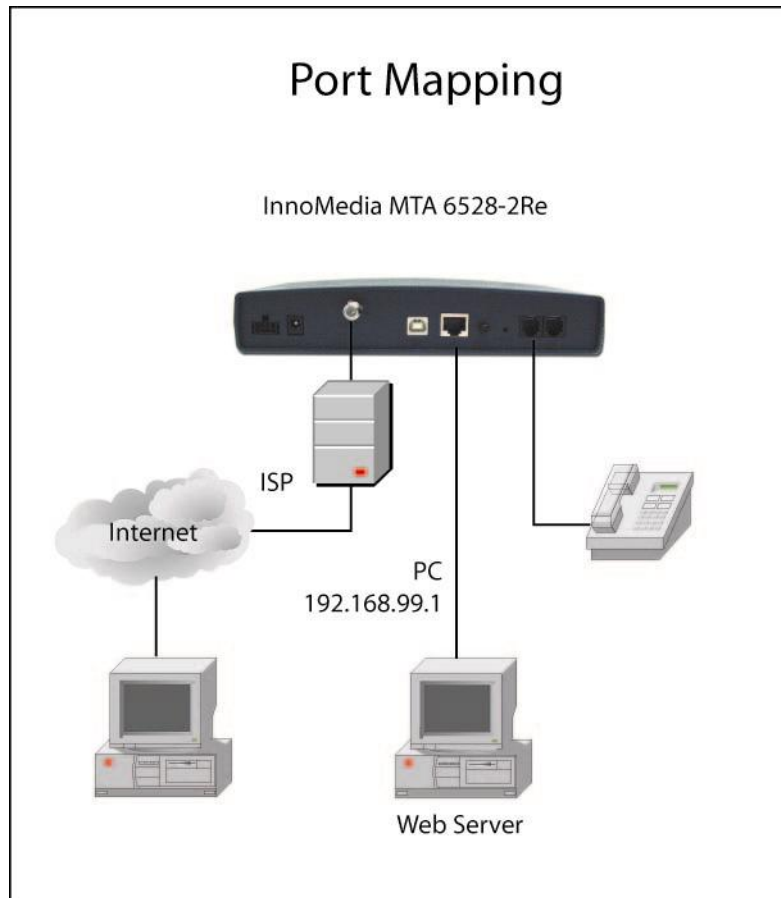


Figure 15. NAT Port Mapping

Configuring Voice QoS Setting

Voice QoS Settings allow the user to designate the amount of bandwidth available on the uplink and downlink ports of the MTA. When the QoS is enabled, the voice packets have higher priority over data packets. To configure the Voice QoS Settings, follow these steps:

Table 12. Configuring Voice QoS Setting

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
<i>2</i>	Click on IP Network, then Voice QoS Settings.
<i>3</i>	Check the box to enable Data Bandwidth Control.
<i>4</i>	Enter the Max. WAN Uplink and Downlink Speed.
<i>5</i>	Click the Save button to save your changes, or click the Reset button if you want to undo your changes.



Figure 16. Configuring Voice QoS Settings

Configuring Access Filtering options

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 6528-2(R)e 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. This filtering is assigned per MAC address.

IP Filtering

To configure the IP Filtering, follow these steps:

Table 13. Configuring IP Filtering

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
<i>2</i>	Click on IP Network, then Access Filtering
<i>3</i>	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 to undo your changes.

MTA 6528-2Re

Configure Access Filtering IP Filtering

☒ Enable IP Filtering

Restricted IP Addresses	Ports	Protocol	Schedule
192.168.99.190	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 23 : 25 To 23 : 30 Mon To Mon
192.168.99.195	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 0 : 0 To 0 : 0 Sun To Sun
192.168.99.198	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
192.168.99.198	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	0	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun
	65535	Any	<input checked="" type="radio"/> Always <input type="radio"/> FromTime 00 : 00 To 00 : 00 Sun To Sun

Figure 17. Configuring Access Filtering – IP Filtering

Domain Filtering

To configure the Domain Filtering, follow these steps:

Table 14. Configuring Domain Filtering

Step	Action
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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 to undo your changes..
---	--



Figure 18. Configuring Access Filtering – Domain Filtering

URL Filtering

To configure the URL Filtering, follow these steps:

Table 15. Configuring URL Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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 19. Configuring Access Filtering – URL Filtering

MAC Filtering

To configure the MAC Filtering, follow these steps:

Table 16. Configuring MAC Filtering

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
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.

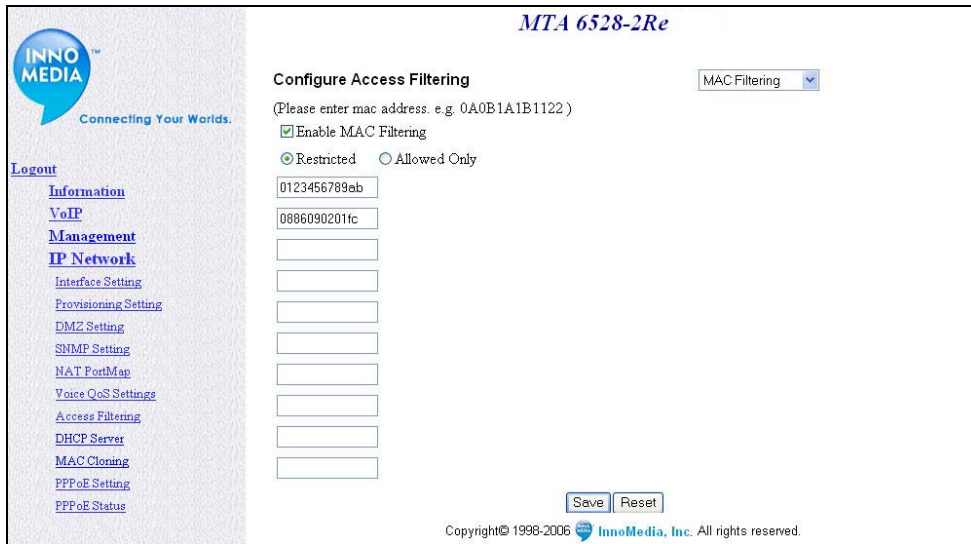


Figure 20. Access Filtering – MAC Filtering

Configuring DHCP Server Information

The MTA 6528-2(R)e has a DHCP Server function to assign dynamic IP addresses to multiple PCs via a hub or direct connection. To configure the DHCP Server function, follow these steps:


Table 17. Configuring DHCP Server Information

Step	Action
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on IP Network, then DHCP Server.
3	Click on Enable DHCP Server to enable the feature.
4	Enter the lowest IP address of a range of IP address(es) that will be associated with a particular configuration.
5	Enter the highest IP address of a range of IP address(es) that will be associated with a particular configuration.
6	Enter the Subnet mask to be present to the client.
7	Enter the Default Router IP address that the client should add to its routing table. This is also the address of the device's web configuration page.
8	Enter the Primary DNS Server IP address that the client should add to its routing table. The DNS addresses must be supplied by your ISP.
9	Enter the Secondary DNS Server IP address that the client should add to its routing table. The DNS addresses must be supplied by your ISP.
7	<p>You may also change how long your PC may keep its current IP address. For most users, the default times (one week) are appropriate and should not be modified. When the lease expires, MTA will automatically renew your PC's IP address.</p> <p>The DHCP Leasing Information is displayed on the lower screen. Click the "X" at the end of each row to remove the lease information.</p>



6

Click the Save and Reboot button to save your changes, or click the Reset button to undo your changes.



Connecting Your Worlds.

[Logout](#)

[Information](#)

[VoIP](#)

[Management](#)

[IP Network](#)

[Interface Setting](#)

[Provisioning Setting](#)

[DMZ Setting](#)

[SNMP Setting](#)

[NAT PortMap](#)

[Voice QoS Settings](#)

[Access Filtering](#)

[DHCP Server](#)

[MAC Cloning](#)

[PPPoE Setting](#)

[PPPoE Status](#)

MTA 6528-2Re

Configure DHCP Server Information

Please complete the following form to define or modify the DHCP server configuration.

Enable the DHCP Server: ☒

The lowest IP address: 192.168.99.100

The highest IP address: 192.168.99.199

Subnet Mask: 255.255.255.0

Default Router address: 192.168.99.1

Primary DNS Server: 10.241.14.2

Secondary DNS Server: 0.0.0.0

Default Lease Time: 1 Week

- Check the box if you need to enable the DHCP server.
- The lowest IP address of a range of IP address(es) that will be associated with a particular configuration.
- The highest IP address of a range of IP address(es) that will be associated with a particular configuration.
- Subnet mask to be present to the client.
- Default Router IP address that the client should add to its routing table. This is also the address of the device's web configuration page.
- Primary DNS Server IP address that the client should add to its routing table.
- Secondary DNS Server IP address that the client should add to its routing table.
- Default lease time for the binding that client will use.
- Modification will **not** take effect unless you click on the **Save & Reboot** button to save to flash memory and reboot.
- Click on the **Reset** button to restore old entries.

DHCP Leasing Information

Client IP	Mac Address	Lease Length	Remaining Lease Time	Remove Lease
192.168.99.198	00.01.02.89.75.dc	7 day(s) 00:00:00	6 day(s) 04:52:24	X
192.168.99.197	00.a0.cc.58.e8.02	7 day(s) 00:00:00	6 day(s) 04:52:24	X
192.168.99.199	00.10.99.10.01.30	7 day(s) 00:00:00	6 day(s) 04:52:24	X

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

Figure 21. Configuring DHCP Server Information

EXAMPLE 1:

Figure 22 illustrates the DHCP Server Configuration with One System Connected.

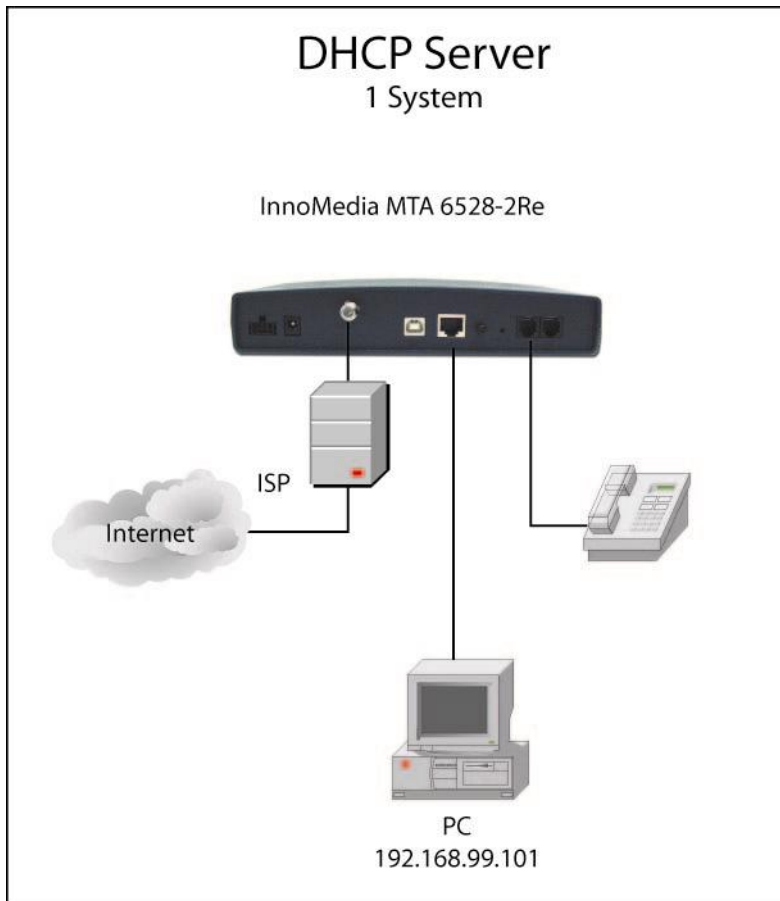


Figure 22. DHCP Sever Configuration-One System Connected

EXAMPLE 2:

Figure 23 is an example of MTA with multiple systems.

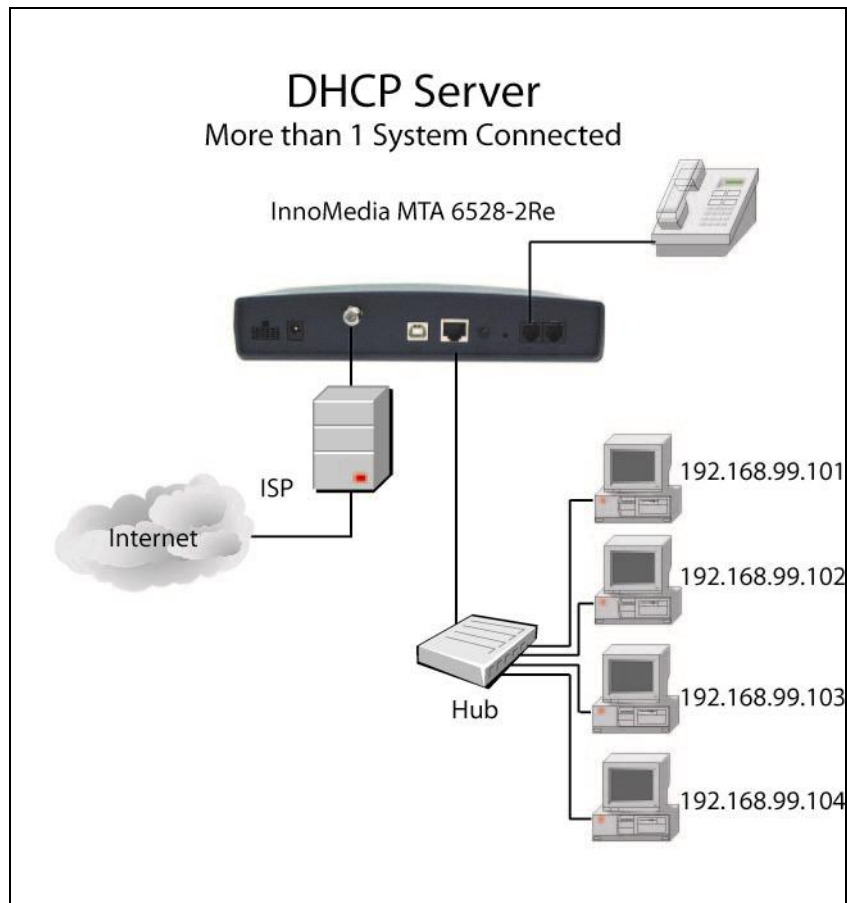


Figure 23. DHCP Sever Configuration-Multiple Connection

Configuring MAC Cloning

To use the MAC cloning feature, follow these steps:

Table 18. Configuring MAC Cloning

Step	Action
1	Open your web browser and connect to your MTA at http://192.168.99.1 (See Logging In on page 10 for more details).
2	Click on IP Network, then MAC Cloning.
3	Check the option box to enable MAC Address Cloning.
4	The MTA will automatically grab the MAC address of your PC's Ethernet card and display it on the screen. NOTE: This feature only works when you have your PC connected to the MTA's internal port. 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.

5	Click Save and Reboot to save the cloned MAC and reconnect to the network, or click the Reset button if you want to undo your changes.
---	--

MTA 6528-2Re

Configure MAC Address Cloning

☒ Enable MAC Address Cloning

Update Current Cloning MAC Address 位 位 位 位 位 位 with:

00 13 20 2d eb 7a

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

Figure 24. Configuring MAC Address Cloning

Configuring VoIP Settings

Configuring Configuration File

The MTA allows you to make a backup configuration file of the current configuration. You may import the file to another MTA, or save the file for future use in case you wish to restore the configuration to the MTA. To use this feature, follow these steps:

Table 19. Configuring Config. File

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click VoIP and then Config File.
3	To save the current configuration, click the Download button.
4	You may either save the file, or copy and paste the outputted text. The file extension must be .cfg
5	To upload a saved configuration, click the Browse button.
6	Locate the .cfg file and click Open
7	Click the Upload button to upload the configuration to the MTA.

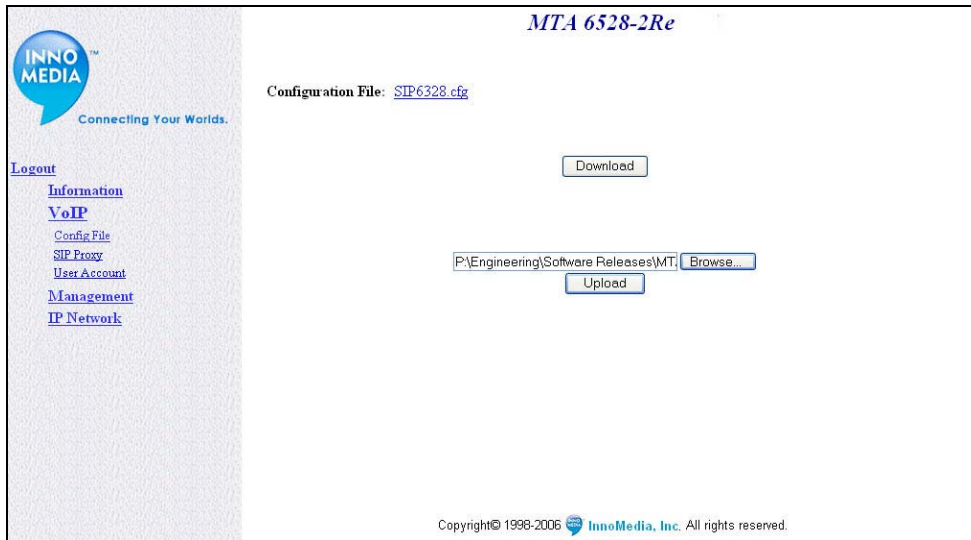


Figure 25. Configuring Configuration File



Figure 26. Sample Configuration File

NOTE: The sample configuration file only shows the minimum configuration of a MTA.

Configuring SIP Proxy Settings

To configure the SIP Proxy Settings, follow these steps:

Table 20. Configuring Call Agent

Step	Action
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click VoIP, and then SIP Proxy.
3	Enter the IP address of your SIP Proxy.
4	If you want to use outbound proxy, check the Use Outbound Proxy option box.
5	Enter the SIP Local Signaling Port number in the field. Default is 5060.

6	Enter the registration expiration time for the MTA to register with the SIP Proxy in seconds. MTA will automatically re-register with the SIP Proxy after each expiry interval to keep its registration up-to-date.
7	Select the Preferred CODECs from the pull-down menu. You can set up to 7 CODECs.
8	Click Save to save your changes to the MTA, or click the Reset button to undo your changes.

The screenshot shows the 'Configure SIP Proxy & Preferred CODECs Settings' page for 'MTA 6528-2Re'. On the left is a sidebar with links: Logout, Information, VoIP, Config File, SIP Proxy, User Account, Management, and IP Network. The main content area contains the following fields and options:

- SIP Proxy:** Text input field with '172.16.0.122' entered.
- Use Outbound Proxy:** A checked checkbox.
- SIP Local Signaling Port:** Text input field with '5060' entered.
- SIP Domain:** Text input field (empty).
- Registration Expiration Time (sec.):** Text input field with '3600' entered.
- Preferred CODECs List:** A list of seven dropdown menus. The first four are set to 'PCMU/8000', 'PCMA/8000', 'G729A/8000', and 'G723/8000'. The fifth is 'G726-32/8000', the sixth is 'G728/8000', and the seventh is '-NONE-'.

At the bottom right are 'Save' and 'Reset' buttons. At the bottom center is the copyright notice: 'Copyright© 1998-2006 InnoMedia, Inc. All rights reserved.'

Figure 27. Configuring SIP Proxy


Configuring User Account

To configure your MTA's User Account information, follow these steps:

Table 21. Configuring User Account information

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click VoIP, and then User Account.
3	Choose the line number from the drop-down menu.
4	Enter the User ID, Password, User Name, and the Authentication ID in the fields.
5	Select Yes if you want to Use the Hot Phone number. MTA will automatically connect to the hot phone number when the phone is off hook.
6	Enter the Hot Phone Number in the field.
7	Select Yes if you want to enable T38 Fax feature or select No to disable it.
8	Click Save to save your changes to the MTA, or click the Reset button to undo your changes.

MTA 6528-2Re



Connecting Your Worlds.

[Logout](#)

[Information](#)

[VoIP](#)

[Config File](#)

[SIP Proxy](#)

[User Account](#)

[Management](#)

[IP Network](#)

Configure User Account

Line No.	<input type="text" value="1"/>
User ID	<input type="text" value="14087895453"/>
User Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
User Name	<input type="text" value="JamesB"/>
Authentication ID	<input type="text"/>
Use Hot Phone Number:	<input type="button" value="Yes"/>
Hot Phone Number:	<input type="text" value="14089665699"/>
Enable T38 FAX	<input type="button" value="Yes"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

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

Figure 28. Configuring User Account Information

Information

Registration Status & Critical Messages

The MTA allows you to view its current registration status with the call agent, as well as any critical error messages regarding the MTAs internal operations. To access this information follow these steps:

Table 22. Registration Status

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
<i>2</i>	Click on Information, then Register Status & Critical Messages.
<i>3</i>	You will see two colored bars corresponding to Line 1 and Line 2 on the MTA
<i>4</i>	A red bar indicates that the line is not registered with the call agent. A green bar indicates that the line is registered with the call agent
<i>5</i>	Critical system operations messages are displayed in the text field.

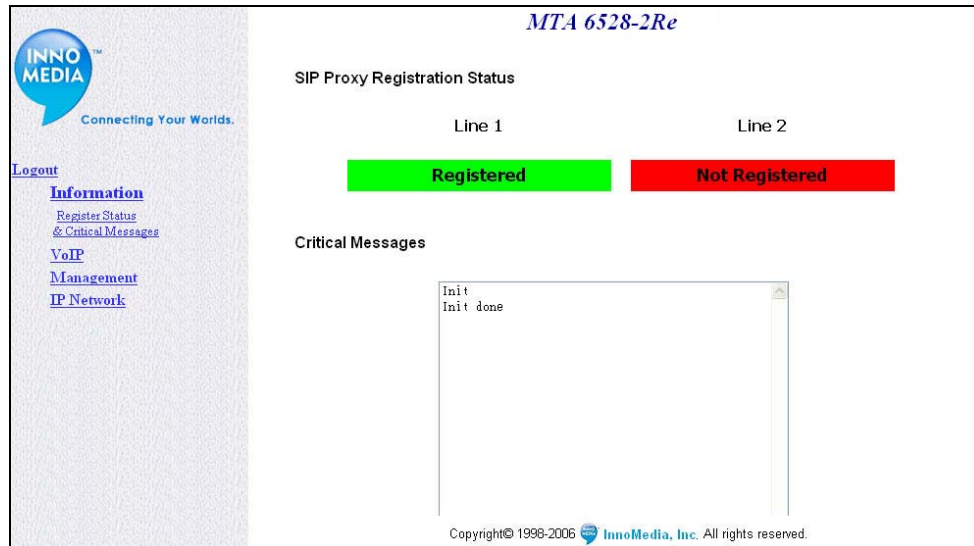


Figure 29. Registration Status

Management

Changing Administrator ID and Password

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

Table 22. Changing Administrator ID and Password

<i>Step</i>	<i>Action</i>
<i>1</i>	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
<i>2</i>	Click on Management, then Administrator.

3	Enter the new Administrator ID you wish to use.
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.
7	Restart your browser and relogin after changing ID or Password.

MTA 6528-2Re

Administrator ID and Password Change

Administrator ID:

New Password:

Confirm Password:

- ID and Password are case sensitive.
- Click 'Update' button to change to New ID and New Password.
- Please restart your browser and relogin after changing ID or Password.

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

Figure 30. Changing Administrator ID and Password

Changing End User ID and Password

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

NOTE: The default end user ID is “User” and password is “password”.

Table 23. Changing End User ID and Password

Step	Action
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on Management, then End User.
3	Enter the New End User ID for user to access the MTA.
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.
7	Restart your browser and relogin after changing ID or Password.

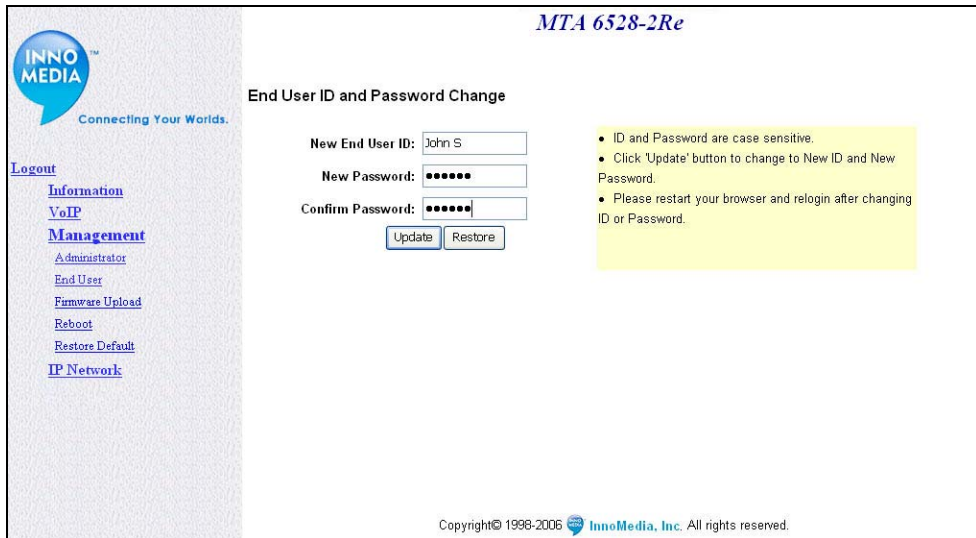


Figure 31. Changing End User ID and Password

Rebooting MTA

To reboot your MTA, follow these steps:

Table 24. Rebooting MTA

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).
2	Click on Management, then Reboot.
3	Click OK to reboot the MTA, or Cancel if you do not want to Reboot at this time.



Figure 32. Rebooting the system

Restoring Factory Default

To restore the factory default parameter values, 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 "password" respectively for the administrator account; "User" and "password" for the end user account.

Table 25. Restoring Factory Default

<i>Step</i>	<i>Action</i>
1	Open your web browser and connect to your MTA (See Logging In on page 10 for more details).

2	Click on Management, then Restore Default.
3	Click OK to restore the factory default values of the MTA.



Figure 33. Restoring Factory Default

Configuring MTA via Telnet/ HyperTerminal Interface

Overview

EMTA 6528-2(R)e 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 MTA's internal port (LAN).

If you are using Telnet:

1. From a windows machine open a Dos Box.
2. Type in Telnet 192.168.99.1 (or the IP address of your MTA), 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 (or the IP address of your MTA) and port number '23' in the fields.
4. Click OK.



Figure 31. Configuring Your MTA 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 MTA commands.

EXAMPLES:

H

Enter Username: **Admin**
 Enter Password: **password**

C: Configuration: Operation Database
 Cd: Configuring VoIP DigitMap
 Cj: Configuring Jitter Buffer Size
 Ct: Configure FXS Setting Parameters
 Cs: Configuring SIP Settings
 Cu: Configuring User Account Database
 Cv: Configure VLAN Setting
 Cr: Enable/Disable Polarity Reversal
 C3: Enable/Disable Call Features
 Cx: Configuring EMS

C: Configuration: IP Information
 Cf: Display the Current IP Information
 Ci: Configure the IP Information

Cw: Change Password

E: Exiting and Logout

G: Voice Volume Control
 Ga: Set Voice Volume for Each Channel

H: Help Menu

I: Information About this System
 Id: Display VoIP DigitMap
 Ig: Display Voice Volume Level
 Ij: Display Parameters for Jitter Buffer Operation
 Is: Display the State of All Ports/Lines
 Ix: Display network connection and UA registration status
 Ik: Display DMS parameters
 If: Display Fax parameters
 It: Display FXS Setting Parameters

M: Miscellaneous
 Me: Configure DHCP parameters
 Mf: Configure Hook Flash Timer
 Mn: Selectable Configuration of IP Elements
 Mp: Configure Phone lines
 Mh: Show Syslog
 Mi: Configure SNTP server
 Mq: Configure Syslog server
 Mm: Configure Remote Services
 Mw: Configure Networking Mode
 N: Configure Router function

P: Provisioning
 Pv: Configure Provisioning setting
 Pr: Trigger Provisioning



```
V: Version number
R: Reset System
```

Viewing the Current IP Information (Cf)

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

EXAMPLES:

Cf

```
Your current configuration:
Your MTA Name= MTA6338R
Ether Address      = 00:10:99:01:e5:de;
You are using DHCP.
Local IP           = 172.16.0.191;
Local IP Mask      = 255.255.0.0;
Local Default GW IP = 172.16.0.1;
Local Default GW Mask = 255.255.0.0;
Primary Domain Name Server = 172.16.0.2;
Secondary Domain Name Server = 192.168.0.2;
System Enable Provisioning Process = FALSE;
SYSLOG Server = 172.16.0.10;
SIP Proxy Server = 172.16.0.122;

Current Local Signaling Port 5060
STUN Disabled
CODECs: G711(PCMU) G711(PCMA) G729A G723 G726-32 G728
Voice Packetization: 60 ms active
RTP port: 10000 active
Silence Suppression: No active
Echo Cancellation: Yes
DSCP: 160,0xa0
Prov_Server_Name:172.16.0.123
DHCP Check Option 43 enable
System Up Time:21 hours, 55 minutes, 40 seconds ago

Project Variant: N
```

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 SIP proxy server (call agent). In addition, you may modify other host settings as described later in this document. Reboot the MTA when you finish the configuration.

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

EXAMPLES:

Ci

1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain



4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server (obsolete)
9. Configure MTA Web Port

Configuring Local IP (Ci, 1)

Select Option 1 to modify the current IP address information for the MTA. If you plan to use DHCP, answer Y when prompted. You must reboot in order for changes to take effect.

Using DHCP

EXAMPLES:

```

Ci

1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain
4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server(obsolete)
9. Configure MTA Web Server Port
1
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
Please wait for flash update...

INFO: read from NVS_PRIMARY (0x1d3)
INFO: write to NVS_SECONDARY (0x1d4)
INFO: write to NVS_PRIMARY (0x1d4)
INFO: read from NVS_PRIMARY (0x1d4)
FS write: OK.
Please reboot the system

```

Using a Static IP

EXAMPLES:

```

Ci
1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain
4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server (obsolete)
9. Configure MTA Web Port
1

```



```

Do you use DHCP to get dynamic IP address and IP mask? [y/n]
n

Please enter the Gateway FQDN:
MTA
Input name is: MTA
Please enter your IP address...
Example: 192.45.6.4
172.16.0.112
IP address entered: 172.16.0.112
Please enter your IP Mask...
255.255.255.0
IP Mask entered: 255.255.255.0
Please enter your Default Gateway IP addr...
172.16.0.113
Gateway IP address entered: 172.16.0.113

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 dynamic IP. 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

Setting DNS (Ci, 2)

Select Option 2 to modify the DNS information for the MTA. You may enter a Primary or Secondary or Both. You must reboot in order for changes to take effect.

EXAMPLES:

```

Ci
1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain
4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server(obsolete)
9. Configure MTA Web Port
2
You want to set IP address for:
1. Primary DNS only      2. Secondary DNS only      3. Both
1
Please enter the Primary DNS IP Address:
172.16.0.2
Primary DNS IP Entered: 172.16.0.2
Do you want to store the changes permanently?[y/n]
y
Please wait for flash update...

```



Please reboot the system

Setting SIP Proxy Server IP (Ci, 3)

Select Option 3 to specify the IP address of the SIP Proxy Server (Call Agent) that your MTA will be registering to. You must reboot in order for changes to take effect.

EXAMPLES:

```
Ci

1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain
4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server(obsolete)
9. Configure MTA Web Port
3
Enable Outbound Proxy?[y/n]
Y

Please enter either the FQDN or IP of SIP Outbound Proxy
Servers...
172.16.0.23
SIP Proxy Server IP Address Entered: 172.16.0.23

[Optional] Do you want to configure SIP Domain(y/n)?
n
Do you want to store the changes permanently?[y/n]
Y
Please wait for flash update...
Please reboot the system
```

Setting IP Settings for All (Ci, 4)

Select Option 4 to specify all of the MTAs IP settings, rather than individually. You must reboot in order for changes to take effect.

Configuring other Local Host settings (Ci, 5)

Select Option 5 to specify other settings for the MTA. You must reboot in order for changes to take effect.

EXAMPLES:

```
Ci

1. Configure Local IP
2. Set DNS IP(s)
3. SIP Proxy Server And SIP Domain
4. Change IP Settings for All
5. Configure other Local Host settings
6. Configure Provisioning Server(obsolete)
```



9. Configure MTA Web Port
- 5
0. Set Fax Answer Tone Trigger Flag
1. Select CODECs:
2. Set Voice Frame Packetization Time
3. Change Voice RTP port
4. Set Silence Suppression
5. Set DSCP(Differentiated Services Code Point) value
6. Set Bullet interval
7. Enable Pinging Gateway
8. Change All the above settings

Other Local Host settings configuration description

Fax Answer Tone Trigger Flag	= Turn on this feature if you want to trigger the fax when MTA receives the answer tone. Otherwise, turn it off, and MTA will trigger the fax when it receives V.21.
CODEC	= Specify the preferred CODEC to be used by the MTA
Voice Frames Packetization	= Specify time in ms for voice packets. The default is 20ms.
RTP Port	= Specify the RTP port number that is greater than 10,000.
Silence Suppression	= Select "On/OFF" for silence packet suppression
DSCP value	= Specify the DSCP value (0-7F) for IP packets
Bullet interval	= Specify the time interval in seconds for sending bullets to keep firewall opened
Pinging Gateway	= Select to allow MTA to periodically ping default GW to determine network connectivity
Change All	= Configure all of the above parameters

Specifying the preferred CODEC (Ci ,5 , 1)

Use the "**Ci ,5 , 1**" command to specify the preferred CODEC to be used by the MTA, and then select the codecs from the available codec list.

EXAMPLES:

```

Num. of Available Codecs = 7

0.      PCMU/8000
1.      PCMA/8000
2.      G729A/8000
3.      G723/8000
4.      G726-32/8000
5.      G728/8000
6.      G729/8000

Num. of Selected Codecs = 6 active

0.      PCMU/8000
1.      PCMA/8000
2.      G729A/8000
3.      G723/8000
4.      G726-32/8000

```



```

5.      G728/8000
Num. of Selected Codecs = 6 active

0.      PCMU/8000
1.      PCMA/8000
2.      G729A/8000
3.      G723/8000
4.      G726-32/8000
5.      G728/8000
Please enter selections: (a,b,c,d....):2

G729A/8000 is preferred!!

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

```

Configuring Jitter Buffer Size (Cj)

Jitter buffers are used to smooth out network introduced jitters and for the system to handle out-of-sequence packets. However, jitter buffers also introduce delays. The MTA supports adaptive jitter buffer based on packet arrival statistics to adjust the jitter buffer length (and delay to accommodate network jitters and minimizes overall delay at the same time. The "Cj" command is used to configure the Initial Delay. It is recommended that this be set at 60ms. The Maximum Jitter Buffer Length and Minimum Jitter Buffer Length are by default set at 400ms and 0 ms (even though the display may show a different value).

```

Cj
Jitter Buffer Size: 60 ms
Jitter Buffer Adaptivity: on
Enter Jitter Buffer Size(0-400 ms, 0 disable it)[60]: 90
Turn on Jitter Buffer Adaptivity?[y/n] y
Save changes permanently?[y/n]y

```

Changing Voice Volume (Ga)

Use the "Ga" command to change your MTA's voice volume. You may adjust the volume downwards by entering the absolute value in dB. MTA only supports negative dB values. For example, if you'd like to adjust the volume to -3 dB, enter "3". The recommended value is "0" dB.

EXAMPLES:

```

Ga
Current RX volume level for channel 1 = 0 dB
Current TX volume level for channel 1 = 0 dB
Current RX volume level for channel 2 = 0 dB
Current TX volume level for channel 2 = 0 dB

Please enter the channel No. for volume control (1-2) or
press e to exit: 1

Please enter RX volume level (0 ~ 18) or press <CR> to exit:
3

Please enter TX volume level (0 ~ 18) or press <CR> to exit:
3

```



```

Volume control succeeds!

Current RX volume level for channel 1 = -3 dB
Current TX volume level for channel 1 = -3 dB
Current RX volume level for channel 2 = 0 dB
Current TX volume level for channel 2 = 0 dB

Please enter the channel No. for volume control (1-2) or
press e to exit: e

Do you want to store the changes permanently? [y/n] y
Writing to Flash, please wait...
Writing to Flash is done successfully.

```

Information about the System

Displaying the current setting of digitmap (Id)

Use the "**Id**" command to view the current digit map stored in the MTA.

EXAMPLES:

```

Id

DisplayDigitmap: (1xxxxxxxxxx|***1|*90)

```

Displaying Voice Volume Level (Ig)

Use "**Ig**" command to view the voice volume level for each channel. RX sets the volume level of your incoming packet tones and TX sets the volume level of your outgoing packet tones.

EXAMPLES:

```

Ig

Current RX volume level for channel 1 = 0 dB
Current TX volume level for channel 1 = 0 dB
Current RX volume level for channel 2 = 0 dB
Current TX volume level for channel 2 = 0 dB

```

Display Parameters for Jitter Buffer Operation (Ij)

Use "**Ij**" command to view the parameters for jitter buffer operation.

EXAMPLES:

```

Ij

Jitter Buffer Delay = 90
Jitter Buffer is "adaptive"

```



Displaying the State of All Ports/Lines (Is)

Use "Is" command to view the state for each channel.

EXAMPLES:

Is

```
Channel #1 is in FXS_OnHook_State.  
Channel #2 is in FXS_OnHook_State.
```

Displaying Network Connection (Ix)

Use "Ix" command to view the state for each channel.

NOTE: Gateway pinging must be enabled first by (Ci->5->7->y)

EXAMPLES:

Ix

```
Default Gateway 172.16.0.1 is reachable  
Ch1 14084329503 is off  
Ch2 14081329504 is off
```

Displaying DMS parameters (Ik)

Use "Ik" command to view the InnoMedia DMS parameters.

EXAMPLES:

Ik

```
InnoMedia DMS feature is available, Disabled  
DMS device type is 1  
DMS Heartbeat type is 1  
DMS Proxy=172.16.0.25:5200  
DMS server port:5200  
DMS regionID:1
```

Display Fax parameters (If)

Use the "If" command to view the Fax settings.

EXAMPLES:

If

```
Your T38 settings are:  
ch 1 T38 Fax is enabled  
ch 2 T38 Fax is enabled
```



```
t38 jitter buffer is 160 ms
t38 T2 is 240 ms
t38 low speed redundancy is 3
t38 high speed redundancy is 1
t38 bit rate is 9600
t38 ECM is on
t38 NSF is cleaned out
t38 T38FaxMaxBuffer is 200
t38 FaxMaxDatagram is 300
Fax setting flag 0,port 10000
Fax is using voice port,it is 10000
t38 variant is Default
```

Displaying FXS Setting Parameters (It)

Use the "**It**" command to view the FXS settings.

EXAMPLES:

```
It

Ringing Timeout = 180 second
Dial Tone Timeout = 16 seconds
Echo Cancellation: Yes
Prefix Digit = NULL
```

Configuring Router Functions (N)

Use the "**N**" command to set the router function and view Server leases.

EXAMPLES:

```
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
```

PPPoE function configuration (N,1)

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

EXAMPLES:

```
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

1
=====
=      PPPoE  CONFIGURATION      =
=====
PPPoEDriver : DISABLE
Service ID:
User      ID: innomediaQA@sbcglobal.net
Autoconnect = ENABLE
IdleTimeOut = DISABLE
Authentication : PAP
LocalIPAddr 172.16.0.191
PPPSubNet 255.255.255.255
=====
Option 1)Configure 2)Dial 3)HangUp 4)Status 5)Quit:4
No_Connect
Option 1)Configure 2)Dial 3)HangUp 4)Status 5)Quit:1
PPPoEDriver [DISABLE] 1)Enable 2)Disable : Enable
Service ID [] 9=NULL:

NewUserID [innomediaQA@sbcglobal.net]:admina@freecall.com

NewPassword [*****]: admin123

AutoConnect [YES] 1)YES 2)NO : YES
IdleTimeOut_Minute [Disable] 0~999 0=Disable :0

Authentication [PAP] 1)PAP 2)CHAP :PAP
SaveChange (y/n)? y

```

PPPoE configuration Description for ISP

Service ID	= NULL string
User ID	= ISP registered name
User Password	= ISP registered password
AutoConnect	= If AutoConnect were enabled, system will automatically connect to your ISP when the system boots up.
IdleTimeOut	= Specifies how long the connection may remain idle (i.e., nothing being received) before PPPoE will automatically disconnect

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 time.
Quit	Use this command to leave PPPoE operation.

Configuring DHCP Server (N, 2)

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

EXAMPLES:

```

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

2
Your current DHCP server configuration is:
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] y

Enable DHCP server.
Currently the lowest IP address :192.168.99.100
Please enter the new lowest IP address :
192.168.99.10
The new lowest IP address :192.168.99.10
Currently the highest IP address:192.168.99.199
Please enter the new highest IP address :
192.168.99.15
The new highest IP address :192.168.99.15
The current subnet mask:255.255.255.0
Please enter the subnet Mask :
255.255.255.0
The subnet Mask entered:255.255.255.0

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

```



Configuring NAT (Port map) (N, 3)

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:

EXAMPLES:

```

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

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.|Extnal Port No.|Protocol|Internal IP
Address|Internal Port No.
0001          69          UDP          192.168.99.198
69
PortMap>a
Enter NAT external source port(0 ~ 65535): 80

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

Enter Internal source IP address: 192.168.99.197

Enter Internal source port:80

PortMap>p
Record No.|Extnal Port No.|Protocol|Internal IP
Address|Internal Port No.
0001          69          UDP          192.168.99.198
69
0002          80          UDP          192.168.99.197
80
PortMap>

```

Showing DHCP Server Leasing Information (N, 4)

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

EXAMPLES:



```

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

4
Client IP      MAC address      Lease Length
Remaining Time
192.168.99.197  00.a0.cc.58.e8.02    7 day(s) 00:00:00    6
day(s) 01:38:15
192.168.99.199  00.10.99.10.01.30    7 day(s) 00:00:00    6
day(s) 01:38:15

```

Accessing Filtering options (N, 5)

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 EMTA 6528-2(R)e 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.

EXAMPLES:

```

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

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

```

Configuring MAC Cloning (N, 6)

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

EXAMPLES:

```

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: ff.ff.ff.ff.ff.ff
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)

Use the "N, 7" command to configure the NAT Bandwidth based on your broadband Internet connection.

EXAMPLES:

```

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
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 NAT bandwidth Control? (y/n)
Y
Please enter your total uplink speed (kbps)
1500
The speed you entered is 1500

Please enter your total downlink speed (kbps)
256
The speed you entered is 256

Do you want to enable TCP MSS control for data packet
Y
Please enter TCP Maximum Segment Size
1500

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

```

Configuring DMZ (N, 8)

Use the "N, 8" command to configure the DMZ (Demilitarized Zone). The DMZ Host setting allows one local user to be exposed to the Internet to use a special-purpose service such as Internet gaming or Video-conferencing

EXAMPLES

```

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

8
DMZ is disabled
Do you want to change it? (y/n)Y
Do you want to enable DMZ? (y/n)Y
Please enter LAN side IP address for DMZ, it must be in the
same subnet with the virtual interface

Example: 192.45.6.4
192.168.99.121
IP address entered: 192.168.99.121

```



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

Showing Configure Link Setting (N, l)

Use the "N,l" command to configure link settings.

EXAMPLES:

```

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 r to show routing table
              Enter l to configure link setting

l
The current Ethernet link settings are:
WAN port:
Speed: Auto
Duplex: Auto
LAN1 port:
Speed: Auto
Duplex: Auto

Do you want to change it? y
WAN port:
Please enter linkspeed: 0=AUTO; 1=100M; 2=10M
2
Please enter Duplex mode: 0=AUTO; 1=FULL; 2=HALF
1
LAN1 port:
Please enter linkspeed: 0=AUTO; 1=100M; 2=10M
2
Please enter Duplex mode: 0=AUTO; 1=FULL; 2=HALF
1

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

```



Changing your User Name and Password

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

EXAMPLES:

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

Writing to Flash, please wait...
Writing to Flash is done successfully.
```

Other Commands

The following commands exist for the purpose of the backward compatibility and ease of configuration under initialization condition.

Configuring 2833 (C2)

Use "**C2**" command to enable/disable 2833.

EXAMPLES

```
C2
RFC2833 (SDP and 2833 packets) is NEGOTIATED!
Please input your new choice(0:always off,1:always on,
2:negotiated)
0
INFO: read from NVS_PRIMARY (0x9d5)
INFO: write to NVS_SECONDARY (0x9d6)
INFO: write to NVS_PRIMARY (0x9d6)
FS write: OK.
RFC2833 (SDP and 2833 packets) is ALWAYS OFF (The device
still able to receive 2
833 packets)!
```

Enabling/Disabling Call Features (C3)

Use the "**C3**" command to enable or disable call features. If the call features are to be disabled and all controls are processed on the softswitch, then you must blank out the local star codes by using the command C3, i and specifying a blank space for all the feature invoke strings.

EXAMPLES:



C3

Configuring Set Call Features:

```
c -- change a call feature setting
i -- change a client call feature invoke string
w -- write changes to Flash(changes is permanent)
p -- print all records in the database on screen
q -- quit.
h -- display the help menu
```

CallFeatures> **p**

```
String to invoke cancel call waiting: *70
String to invoke call transfer: *90
String to invoke Caller ID Block: *67
String to invoke Caller ID Display: *82
String to invoke call park: *98
String to invoke call retrieve: *99
String to invoke Do not Disturb Enable: *74#
String to invoke Do not Disturb Disable: #74#
```

Ch 1:

```
Call Waiting is enabled active
Three-Way Call and Call Transfer are enabled
Three-Way:active,B Tranx:active,C Tranx:active
Caller ID is enabled active
Reject Anonymous calls is disabled
```

Ch 2:

```
Call Waiting is enabled active
Three-Way Call and Call Transfer are enabled
Three-Way:active,B Tranx:active,C Tranx:active
Caller ID is enabled active
Reject Anonymous calls is disabled
```

CallFeatures>

Configuring Digit Map (Cd)

Use the "Cd" command to view the current digit map stored in the MTA and to change the existing digit map if necessary. The digit map can be up to 2048 characters.

EXAMPLES:

Cd

```
a -- add a new dialing pattern
d# -- delete the n-th pattern in the DigitMap
w -- write changes to Flash(permanent storage)
e -- erase the entire DigitMap
p -- print all patterns of the current Digitmap
q -- quit.
h -- display the help menu
```

DigitMap>**p**

```
No.      DigitMap Pattern
1        lxxxxxxxxxxx
```



```

2      ***1
3      *90
DigitMap>a
Enter a new Digitmap pattern: x.#

DigitMap>p
No.      DigitMap Pattern
1      1xxxxxxxxxxx
2      ***1
3      *90
4      x.#
DigitMap>

```

This command is used to load the MTA with a digit map that corresponds to the dial plan selected by the service operator. The digit map is expressed using a syntax derived from the UNIX system command, *egrep*. You must build the digit map based on the dialing plan you wish to support. Here is an example dialing plan:

0	Local operator
00	Long distance operator
xxxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
*xx	Star services
91xxxxxxxxxxx	Long distance number
9011 + up to 15 digits	International number

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

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

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

```

Digit ::= "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"
Timer  ::= "T" | "t" -- matches the detection of a timer
Letter ::= Digit | Timer | "#" | "*" | "A" | "a" | "B" | "b" | "C" | "c" | "D" | "d"
Range  ::= "X" | "x"      -- matches any digit
        | "[" Letters "]" -- matches any of the specified letters
Letters ::= Subrange | Subrange Letters
Subrange ::= Letter      -- matches the specified letter
        | Digit "-" Digit -- matches any digit between first and last
Position ::= Letter | Range
StringElement ::= Position -- matches an occurrence of the position
        | Position "."     -- matches an arbitrary number of occurrences
        -- of the position, including 0
String ::= StringElement | StringElement String
StringList ::= String | String "[" StringList
DigitMap ::= String | "(" StringList ")"

```

A DigitMap, according to this syntax, is defined either by a (case insensitive) "string" or by a "list of strings" over which the MTA will attempt to find a shortest possible match. Regardless of the above syntax, a timer is currently only allowed if it appears in the last position in a string. Each string in the list is an alternate numbering scheme. A MTA that detects digits, letters, or timers will:



1. Add the event parameter code for the digit, letter, or timer, as a token to the end of the "current dial string" internal state variable.
2. Apply the "current dial string" to the digit map table, attempting a match to all expressions in the Digit Map.
3. If the result is under-qualified (partially matches at least one entry in the digit map and doesn't completely match another entry), nothing further will be done.

If the result matches an entry, or is over-qualified (i.e. no further digits could possibly produce a match), the MTA will send the current dial string to the Call Agent and clear the "current dial string". A match, in this specification, can be either a "perfect match," exactly matching one of the specified alternatives, or an impossible match, which occurs when the dial string does not match any of the alternatives. Unexpected timers, for example, can cause "impossible matches". Both perfect matches and impossible matches trigger notification of the accumulated digits (which may include other events). Timer T is a digit input timer that can be used in two ways:

- When timer T is used with a digit map, the timer is not started until the first digit is entered, and the timer is restarted after each new digit is entered until either a digit map match or mismatch occurs. In this case, timer T functions as an inter-digit timer.
- When timer T is used without a digit map, the timer is started immediately and simply cancelled (but not restarted) as soon as a digit is entered. In this case, timer T can be used as an inter-digit timer when overlap sending is used.



Configuring SIP Settings (Cs)

Use the "Cs" command to change your SIP settings.

EXAMPLES:

```

Cs
Current SIP Proxy Servers      = 172.16.0.122
Use Outbound Proxy            = Yes
Current Local SIP Port        = 5060
Response Code for Retry Registration =
Retry Registration Interval    = 30 seconds
Current SIP Domain            =
Current Exponential Backoff    = 1000 ms
Current Exponential Cap        = 4000 ms
Current Non-INVITE retry       = 4 times
Current INVITE msg retry       = 4 times
Current REGISTER expiration    = 3600 seconds
Current Session Timer          = 0 seconds
Current Bullet Interval        = 0 seconds
Current Number of Codecs       = 6
Current Codec List             = G711(PCMU) G711(PCMA) G729A
                               G723 G726-32 G728
Digitmap Partial Match Timeout = 16
Digitmap Critical Timeout      = 4
Cancel Call Waiting Invoke String = *70
Call Transfer Invoke String    = *90
CID Block Invoke String        = *67
CID Display Invoke String      = *82
Call Park Invoke String        = *98
Call Retrieve Invoke String     = *99
Do not Disturb Enable Invoke String = *74#
Do not Disturb Disable Invoke String = #74#
Use User-Agent Header          = Yes
Set Jitter Buffer Adaptive      = Yes
Use SIP INFO for DTMF          = No
Re-registration Credential Enable = Yes
Current SIP PING Interval      = 0 seconds
Current SIP PING Proxy Require Header =
Current SIP External IP address =
Digitmap Early Quit            = Disabled
Digitmap Early Quit FW Number =
Use SIP INFO for Flash Event    = No
Use SIP NOTIFY for Flash Event  = No
PRACK Support Enable           = No
G729A Codec_Variant            = 0 (annexb=no)

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

Select the item your want to change: ('Q' to quit)

```



1. SIP Proxy Server List
2. Outbound Proxy Enable/Disable
3. SIP Local Signaling Port
4. SIP Domain
5. SIP cmd Retry Exponential Backoff (starting vlaue/ms)
6. SIP cmd Retry Exponential Backoff (cap/ms)
7. SIP cmd (Non-INVITE) Max Retry
8. SIP cmd (INVITE) Max Retry
9. SIP REGISTER Expiration (sec)
10. SIP Session Timeout(sec)
11. Bullet Interval (sec)
12. Select CODECs
13. Digitmap Partial (inter-digit) Timeout
14. Digitmap Critical Timeout
15. Configure Call Features & Invoke Strings
16. SIP User-Agent Header
17. Set Jitter Buffer Adaptive/Static
18. SIP INFO for DTMF
19. Set Response Code for Retry Registration
20. Retry Registration Interval
21. SIP PING Interval (sec)
22. SIP PING Proxy Require Header String
23. SIP External IP address
24. SIP Header size limitation Option Enable/Disable
25. Digitmap Early Quit Enable/Disable
26. Use SIP INFO or NOTIFY message to send flash event Enable/Disable
27. PRACK Support Enable/Disable
28. Digitmap Early Quit FW Number
29. G729A Variant for SDP offer

SIP Proxy Server List	= The IP addresses or FQDNs of the SIP proxy server (separated by comma or semicolon)
Outbound Proxy	= Enable or disable outbound proxy
SIP Local Signaling Port	= Port number of MTA's local signaling port. The signaling port is by default set to 5060 and it uses the UDP protocol. The MTA uses the same port for sending and receiving messages.
SIP Domain	= Enter the domain from which SIP service is provided
SIP cmd Retry Exponential Backoff (starting value)	= The starting time interval in milliseconds in which the MTA will re-send SIP messages in the case of no response from the SIP proxy
SIP cmd Retry Exponential Backoff (cap/ms)	= A cap on the exponentially increased interval in milliseconds, for which MTA will stop sending messages when the cap is reached.
SIP cmd (Non-INVITE) Max Retry	= The maximum number of times the MTA will resend NON-INVITE type SIP messages.
SIP cmd (INVITE) Max Retry	= The maximum number of times the MTA will resend INVITE type SIP messages.
SIP Registration Expiration	= Number of seconds in which the registration to the SIP proxy will expire.



SIP Session Timer	= Specific interval (in seconds) that MTA sends a message to refresh an established phone call and make sure it's still alive
Bullet Interval	= The time interval in seconds in which the MTA will send a bullet message to keep the firewall open
Number of Codecs/Codec List	= Shows the number of codecs available to MTA. The user can change the number of available codecs by selecting from a list
DigitMap Partial Match Timeout	= (A.K.A inter-digit timeout) The amount of time in seconds for which MTA will wait till user input a DTMF digit
DigitMap Critical Timeout	= Can be used as part of the dialing patterns specified in digitmap to be matched by MTA
Cancel Call Waiting Invoke String	= The digit combination user dials to cancel call waiting on a per-call-basis
Call Transfer Invoke String	= The digit combination user dials to invoke call transfer
CID Block Invoke String	= The digit combination user enters to invoke Caller ID blocking
User-Agent Header	= Specified whether "User-Agent" header shall be present or not in outgoing SIP messages
Jitter Buffer Adaptive/Static	= Set to adapt the jitter buffer to network conditions or set the jitter buffer at a constant delay
Use SIP INFO for DTMF	= Specify use SIP INFO for DTMF or not
Response Code for Retry Registration	= Set the response codes for MTA to attempt registration retry
Retry Registration Interval	= the time interval in seconds in which the MTA will retry registration when the cap is reached.
SIP PING Interval (sec)	= the time interval in seconds between every ping
SIP PING Proxy Require Header String	= Specify if SIP Ping Proxy require Header string or not
SIP External IP address	= External IP address of WAN router if MTA is connected to LAN of a SOHO router
Header size limitation	= Enable or disable header size limitation
Digitmap Early Quit	= Enable or disable digitmap Early Quit. When enabled, calls that do not match with any digitmap will not be sent to the proxy. Local plays busy tone.
SIP INFO or NOTIFY message	= Enable or disable use SIP INFO or NOTIFY message to send flash event.
PRACK Support	= Enable or disable PRACK (100rel) support in Invite and 180 messages.
Digitmap Early Quit FW Number	= The phone number to forward the call when there is no matched digitmap
G729A Variant for SDP offer	= Enable or disable applying G729A Variant for SDP offer.

Configuring FXS settings parameters (Ct)

Use the "Ct" command to configure your FXS settings.

EXAMPLES:

```
Ct

Ringing Timeout = 180 second
Dial Tone Timeout = 16 seconds
Echo Cancellation: Yes
Prefix Digit = NULL

FXS Config
Config FXS Setting
p: Display Current Setting
1: Set Ringing Time Out
2: Set Ringing Cadance
3: Set Ringing Repetition
4: Set Dial Tone Timeout
5: Set Echo Cancellation
6: Set Prefix Digit
7: Set Remote Busy Delay Time
8: Set Busy Timeout
9: Set Warning Timeout
w: Save Config Change
q: Exit FXS config

Choose Option:p

Ringing Timeout = 180 second
Ringing Cadence = 0
Ringing Repetition = 0
Dial Tone Timeout = 16 seconds
Echo Cancellation: Yes
Prefix Digit = NULL
Remote Busy Delay: 0
Busy Tone Timeout: 0
Warning Tone Timeout: 0

Choose Option:
```

FXS Settings Parameters configuration description

Ringing Timeout	= Time duration before the MTA stops ringing
Ringing Cadence	= Select a predefined Ringing Pattern.
Ringing Repetition	
Dial Tone Timeout	= Time duration before the MTA stops playing dial tone
Echo Cancellation	= Enable or disable echo cancellation
Prefix digit	= Enter the phone prefix up to 11 digits. Enter -1 for Null. By configuring the prefix, users can dial the local number without enter the country code and area code.
Remote Busy Delay	= Time delay before playing busy tone when remote party hangs up.
Busy Tone Timeout	= Time interval before busy tone stops playing.
Warning Tone Timeout	= Duration before warning tone stops playing.



Configuring SIP user account (Cu)

Use the "**Cu**" command to change your SIP user name and password.

EXAMPLES:

Cu

```
Configuring User Account Database:
(each record consists of an User ID)
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
UserID>p
No.    UserID      Passwd      Name      AuthID
0001   14087895453  5453       5453      ( 3
0001   14087895454  5454       5454      ( 3
UserID>a

Enter the Channel Number: (from 1 to 2 )1

Enter a new User ID: 14087895455

Enter a new password: 123456

Enter the user name: JohnS

Enter authentication (type 'null' for empty): null

UserID>p
No.    UserID      Passwd      Name      AuthID
0001   14087895455  123456     JohnS     ( 3
0001   14087895454  5454       5454      ( 3
UserID>
```

Enabling/Disabling Polarity Reversal (Cr)

Use "**Cr**" command to enable or disable Polarity Reversal function.

EXAMPLES:

Cr

```
You're currently using Polarity Reversal Feature!
Do you want to Enable Polarity Reversal at this MTA? (y/n)y
Writing to flash ... done.
```

Configuring Virtual LAN 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.

EXAMPLES:

```
Cv

=====
VLAN CONFIGURATION
=====
c -- change 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 TAGGING : DISABLED
IP TOS TO 802.1p PRIORITY MAPPING : DISABLED
                        VLAN ID : 0x000
                        802.1p PRIORITY : 0

CURRENT PHYSICAL INTERFACE No. : 1
                        VLAN TAGGING : DISABLED
IP TOS TO 802.1p PRIORITY MAPPING : DISABLED
                        VLAN ID : 0x000
                        802.1p PRIORITY : 0
VLAN> c
SELECT PHYSICAL INTERFACE [0-1] 0=WAN port, 1=LAN port: 0

ENABLE VLAN TAGGING (y/n): y
ENABLE IP TOS TO 802.1p PRIORITY MAPPING (y/n): y
PLEASE INPUT VLAN ID [0x000-0xFFFF]: 0xFFFF
PLEASE INPUT VLAN PRIORITY [0-7]: 0
VLAN>
```

Configuring DMS (Cx)

Use the "Cx" command to configure InnoMedia Device Management System (DMS) features if you have one installed in your network.

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

EXAMPLES:

```
Cx

InnoMedia DMS feature is available,Disabled
DMS device type is 1
DMS Heartbeat type is 0
DMS Proxy=
DMS Local port:0
DMS regionID:0
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] y
Please enter DMS Proxy FQDN(or IP address):Port...
Example: 192.45.6.4:5200
192.236.20.2:5200

DMS Proxy entered=192.236.20.2:5200

You current local DMS port is 0,Do you want to configure it?
[y/n]
y
Please input new local DMS port(UDP):
6000
You current deviceType(1 to 254) is 1,Do you want to
configure it? [y/n]
y
Please input new deviceType:
1
You current regionID(4 bytes integer) is 0,Do you want to
configure it? [y/n]
y
Please input new regionID:
20
You new regionID(4 bytes integer) is 20
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

Configuring Control Parameters (Me)

Use the "**Me**" command to view or change the current control parameters for Provisioning, 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. Under the "enabled" state, the MTA will always check for a newer software version as part of the provisioning process. If "disabled" then the MTA will never check for a new software version.

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

EXAMPLES:

```

Me

1. SW_UPGRADE disable

2. Disabled Provisioning

```



3. DHCP Check Option 43 enable
 4. SNMP mibs
 5. Credential on re-registration enable
 6. Proxy Authentication retry. Please see command Cs->19
- Do you want to change [1-6]

Me configuration description

- SW_UPGRADE = select this option to enable/disable software upgrade with the provisioning server. This option is only valid if provisioning is enabled
- Provisioning = select this option to enable provisioning and choose the protocol variant (see Provisioning Mode Description below).

Provisioning Mode Description:

For HTTP Provisioning

- Mode 2 - non-secure
- Mode 816 - secure and encryption type AES. Need InnoMedia utility programs to encrypt configuration file.
- Mode 9768 - secure and encryption type RC4. Need InnoMedia utility programs to encrypt configuration file.
- Mode 909 - secure and encryption type RC4. Need InnoMedia utility programs to encrypt configuration file.

For TFTP Provisioning

- Mode 762 - secure or non-secure
 - Encryption RC4. Need InnoMedia utility programs to encrypt configuration file.
 - Encryption AES_CBC_256. Use "openssl" to encrypt configuration file

DHCP Options 43 enable/disable = enable or disable Option 43

SNMP MIBs = select specific MIBs to be used by different vendor requirements/standard

Credential on re-registration = select this option to enable or disable sending credential on re-registration

Configuring Flash Hook timer (Mf)

Use the "**Mf**" command to change the default timer for the 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.

EXAMPLES:

Mf



```
Flash_Hook_timer = 800 ms,range is [10-1270 ms] according to
your phone
```

```
Please enter value:400
```

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

```
Reboot system to make new setting effective!
```

```
R
```

```
Are you sure you want to RESET system? [y/n] y
```

Showing Syslog (Mh)

The "Mh" command allows you to view Syslog events provided a Syslog server is configured.

```
Mh
```

```
How many records you want to see?
```

```
10
```

```
Input start point?
```

```
1
```

```
syslog 1: <181>Fri Apr 21 18:19:01 2006
```

```
MTA6328R
```

```
MTA6328_R:NOTICE-Power on Init.
```

```
Done
```

```
syslog 2: <182>Thu Jan 1 02:53:40 1970
```

```
MTA6328R
```

```
MTA6328_R:NOTICE - DHCP success
```

```
syslog 3: <182>Thu Jan 1 02:53:40 1970
```

```
MTA6328R
```

```
MTA6328_R:NOTICE - DHCP success
```

```
Do you need see more record? Y/N
```

```
n
```

Configuring SNTP server (Mi)

The "Mi" command allows you to configure SNTP time server settings and time offset settings.

EXAMPLES:

```
Mi
```

```
SNTP Server0 = 192.45.6.4;
```

```
SNTP Server1 = 192.45.6.4;
```

```
SNTP Server2 = 192.45.6.5;
```

```
Currently Time Zone offset is 0.0 hours
```

```
Currently Retry time is 300 seconds
```

```
Currently Daylight Saving Time is Disabled
```

```
Do you want to change SNTP server IP address?[y/n]y
```

```
Please enter SNTP server0...
```



```

Example: 192.45.6.4 or time.nist.gov or q to quit
192.168.99.26
IP address 0 entered: 192.168.99.26

Please enter SNTP server1...
Example: 192.45.6.4 or time.nist.gov or q to quit
192.168.99.27
IP address 1 entered: 192.168.99.27

Please enter SNTP server2...
Example: 192.45.6.4 or time.nist.gov or q to quit
192.168.99.25
IP address 2 entered: 192.168.99.25

Do you want to change time zone setting?[y/n]y
Please enter SNTP server time zone (-12 ~ 13)
-6

Do you want to change retry setting?[y/n]y
Please enter SNTP server retry time (seconds)
86400

Do you want to change Daylight Saving Time setting?[y/n]y
Please enter 0:disable, 1:enable for Daylight Saving Time
1

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

```

Configuring Remote Services (Mm)

The "**Mm**" command allows you to enable/disable interfaces to your MTA.

EXAMPLES:

```

Mm

Current Telnet access is:
Enabled for access from WAN

Current SNMP access is:
Enabled for access from WAN

Current Web server access is:
Enabled for access from WAN

Current LAN to Internet access is:
Enabled

Do you want to enable Telenet?
0).Disable
1).Enable access from WAN.
0
Do you want to enable Web Server?
0).Disable
1).Enable access from WAN.

```



```

1
Do you want to enable SNMP?
0).Disable
1).Enable access from WAN.
1
Do you want to enable LAN to Internet access?
0).Disable
1).Enable
1
Do you want to save changes to FLASH memory? (y/n):
1
Do you want to save changes to FLASH memory? (y/n): y

```

Selectable Configuration of IP Elements (Mn)

Use the "**Mn**" command to configure specific variable in the IP Settings. Enter the number of the setting you wish to change, and then enter your IP information.

EXAMPLES:

```

Mn

SystemStatus is :                1

Box Mac Address is :             00:10:99:01:e5:de
0. Local IP is :                 172. 16.  0.191
1. Local Default GW IP is :      172. 16.  0.  1
2. Local IP Mask is :           255.255.  0.  0
3. MTA's FQDN is :              localhost.InnoMedia.com
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 :
Please select the item number you want to change: 1

Please input Local Default GW IP: 10.0.0.11

INFO: read from NVS_PRIMARY (0x1e0)
INFO: write to NVS_SECONDARY (0x1e1)
INFO: write to NVS_PRIMARY (0x1e1)Local Default GW IP is :
10.0.0.11

If any change is made, Please reboot the system!

```

Phone Line Configuration (Mp)

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

EXAMPLES:

```

Mp

Currently line 1 is enabled

```



```

Currently line 2 is enabled
Do you want to change the configuration? [y/n] y
Do you want to enable line 1? [y/n] y
Line 1 enable.
Do you want to enable line 2? [y/n] n
Line 2 disable.
Do you want to store the changes permanently? [y/n] y
INFO: read from NVS_PRIMARY (0x1e1)
INFO: write to NVS_SECONDARY (0x1e2)
INFO: write to NVS_PRIMARY (0x1e2)

```

Configuring Phone lines (Mq)

The "Mq" command allows you to configure the IP address of Syslog server

EXAMPLES:

```

Mq

Currently SysLOG Server = [0.0.0.0];
Please enter SysLOG servr IP address...
Example: 192.45.6.4
172.16.0.10
IP address entered: 172.16.0.10

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

```

Configure Networking Mode (Mw)

Use the "Mw" command to configure the networking mode (i.e., router or switch).

NOTE: If you answer "Yes" to make the mode not modifiable, the user logging in with the enduser account will not be able to change the MTA mode.

EXAMPLES:

```

MW

The current Networking Mode is: Router and is Modifiable
Do you want to change it? (y or n)
y
Do you want to make the mode NOT Modifiable? (y or n)
y
Do you want save the change to Flash? (y or n)y

```

Signing on to softswitch (Sn)

Use the "Sn" command to sign on to the softswitch.

EXAMPLES:

```

Sn

1 - sign on channel 1

```



```

2 - sign on channel 2
all - sign on ALL channels
1
CH 1: MSG_SIP_REGISTER sent to MSG_Q_SIP

ch1: 14087895453 Sign In Ok! (ticks:8650618)

```

Signing off of the softswitch (Sf)

The "**Sf**" command is used to sign off from the softswitch.

EXAMPLES:

```

Sf

1 - sign off channel 1
2 - sign off channel 2
all - sign off ALL channels
all
  CH 1: MSG_SIP_SIGNOFF sent to MSG_Q_SIP
  CH 2: MSG_SIP_SIGNOFF sent to MSG_Q_SIP

ch1: 14087895453 Sign Off! (ticks:8655263)
ch2: 14087895454 Sign Off! (ticks:8655263)

```

Provisioning

Configuring Provisioning Setting (Pv)

Use the "**Pv**" command to configure the provisioning setting.

NOTE: You must enable and configure the provisioning mode first (see Configuring Control Parameters (Me, 2) on page 66) before you can use the "**Pv**" command to configure the provisioning setting.

Mode 2 - HTTP non-secure provisioning

EXAMPLES:

```

Pv

Prov mode: HTTP_D

HTTP Prov. Server FQDN or IP is:172.16.0.123
Prov Server Port Is 8802
Prov_Repeat_Interval Is 5 Seconds
HTTP Digest Variant:Digest
HTTP POST Message(0) is Disabled
Your reDir srv is not invalid now.

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

```



```

p -- print Prov. settings
q -- quit.
h -- display the help menu
Prov> c
Select the item your want to change: ('Q' to quit)
1. Prov. Server
2. Prov. Port
3. Re-Prov. Interval
4. Prov. Variant
7. Prov. POST Message Is Enabled or Disabled
1

Please enter Prov. Server(either FQDN or IP): 172.16.12.23

Prov> w
Please wait for flash update...

```

Mode 762 - TFTP secure provisioning

For the TFTP secure provisioning, a 32-byte encryption key must be configured (option 4 – Encryption Key). The key must match with the one used for encrypting configuration file on the provisioning server.

EXAMPLES:

```

Pv

Prov. Server: 192.168.3.100
Prov. Default Directory: /firmware/SIP
Prov. Interval: 7200 seconds
Prov. Encryption Type:AES_CBC_256
Encryption Key:

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

TFTP Provisioning> c
1. TFTP Server FQDN/IP
2. Default Directory
3. Prov Interval
4. Encryption Key
6. TFTP Encryption Type

Please enter item:
Please TFTP Server IP/FQDN:192.168.3.100

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

```



```

TFTP Provisioning> c
1. TFTP Server FQDN/IP
2. Default Directory
3. Prov Interval
4. Encryption Key
6. TFTP Encryption Type

Please enter item:4

Please enter 32-bytes Enc Key
(ascii):qazwsxedcrl234567890zxcvbnmjkl12

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

TFTP Provisioning> p
Prov. Server: 192.168.3.100
Default Prov. Directory: /IP_Phone/SIP
Prov. Interval: 7200 seconds
Prov. Encryption Type:AES_CBC_256
Encryption Key:

TFTP Provisioning> c
1. TFTP Server FQDN/IP
2. Default Directory
3. Prov Interval
4. Encryption Key
6. TFTP Encryption Type

Please enter item:6

Please enter Encryption Type (1:RC4,3:AES_CBC_256):3

TFTP Provisioning> w
INFO: read from NVS_PRIMARY (0x1144)
INFO: write to NVS_SECONDARY (0x1145)
INFO: write to NVS_PRIMARY (0x1145)
FS write: OK.
End of TFTP Prov. Settings Configuring Shell.

```

Triggering Provisioning (Pr)

Use the "**Pr**" command to manually trigger the provisioning process.

```

Pr

Send to 172.16.0.123:514
<182>Thu Dec 22 13:28:52 2005
InfoGate3020 IPPHONE3308: NOTICE - Configuration File
Download Succeed

```



```
AES CBC 256 Decryption Succeeded! Enc_Key[0]:49

Send to 172.16.0.123:514
<182>Thu Dec 22 13:28:52 2005
InfoGate3020 IPPHONE3308: NOTICE - No Firmware downloaded
```

Pinging a Remote IP Address (P)

Use the "**P**" command to ping a remote IP address from the MTA.

EXAMPLES:

```
P

Do you want ping a remote IP address from this MTA?[y/n]
Y
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
```

MTA Version Information (V)

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

EXAMPLES:

```
V

The Image Version is: 4.1.6

Control Code Version = 4.1.6 6528-2(R)e Wed Sep 20 11:13:51
2006
DSP Code Version = 2.4.26 07/31 12:21 2006
BBS Version=7.3.9
SIP Stack Version=2.9.129

Hardware version = 10.4.0.0
Layout Version = A0-0

System Up Time:00 hours, 12 minutes, 28 seconds ago
```

Restoring System Default

The following procedures are used for restore the default settings of an MTA.

Press <system restore> button on the backside of the MTA 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 local IP address will return to be the default value 90.0.0.1.
And the user name and password will return to the system default "InnoMedia".



MTA Firmware Updates

Overview

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

Manually Uploading MTA Firmware via Web Interface

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

Table 26. Uploading MTA Firmware by Web Interface

<i>Step</i>	<i>Action</i>
1	Open your web browser and type the IP address of your MTA.
2	Enter your Username and Password.
3	When the MTA's Configuration Web page appears, click on Management, and then Firmware Upload. Select the item you want to upgrade (See Figure 34. Firmware Upgrades): <ul style="list-style-type: none"> System Image: for system image upgrade. Boot-loader: for Redboot.
4	Click Browser button to select the image file, or enter directly the location and the file name.

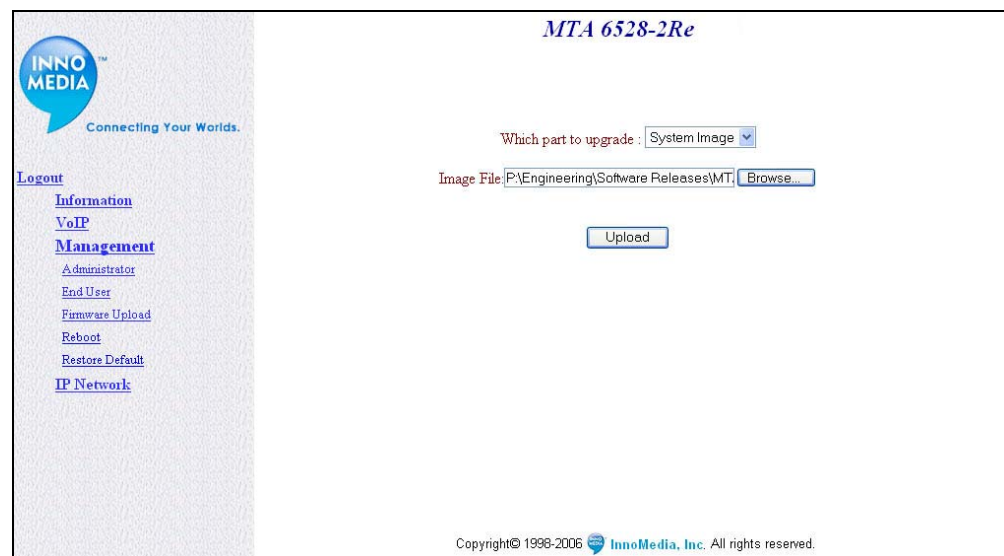


Figure 34. Firmware Upgrades

Auto-upgrading MTA Software Code from Server Side

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

Table 27. Upgrading MTA 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 MTA: <ul style="list-style-type: none"> • Use the "Me, 2" command to enable and configure provisioning mode (see page 66) • Use the "Pv" command to configure the provisioning settings (see page 72). • Use the "R" command to reboot your MTA
4	MTA will grab the configuration file from the server at the interval set.
5	MTA will compare the file it has with the one specified in the configuration. If the file name is different, MTA will request the new firmware image from the server.



Working with the Cable Modem

Overview

The console commands are organized into a number of groups that differ in functionality. Each group is called a *sub-table*. For ease of use in console mode, you don't have to type the full command at the prompt (for example, typing **sy** is the same as **syntax**).

Commands that are used more often than others are placed in the main (built-in) table in order to provide quick access to them. As can be seen in the commands list below, the sub-tables have a > (more than) symbol following their name.

All commands in all table levels are in alphabetical order, and are case-sensitive.

Telnet to the Cable Modem

To telnet to the cable modem, follow these steps:

1. Telnet xxx.xxx.xxx.xxx (if using the command prompt)
2. Enter user name "Admin" and password "adminpass" to login
3. Type scan_stop to stop system scanning

NOTE: Telnet is only accessible via WAN side. For Security reasons, LAN side Telnet to cable modem is disabled.

General Commands

help

TABLE: **built-in**

COMMAND: **help**

USAGE: help [-t|-l|-s|-i|-a|-lr] [command [...]{126}]

DESCRIPTION: Shows usage information about the specified command(s), or lists the set of commands available in the active table. If no parameters are specified, then an abbreviated list of all commands and subtables is displayed.

- t -- Shows the entire tree of command tables and commands (in abbreviated form).
- l -- Shows detailed information about all commands and subtables (this can print a LOT of information)!
- s -- Shows detailed information on just the subtables.
- i -- Shows detailed information on just the registered instances for the active table.
- a -- Does everything that the -l, -s, and -i options do.

Command is the name (or partial name) of one or more commands and subtables for which you want detailed help to be displayed.



EXAMPLES:

help	- This shows an abbreviated list of all commands and subtables.
help cd	- This shows detailed help on the 'cd' command.
help cd ! diag	-This shows detailed help on the 2 commands and subtable listed.
help -l	- Shows detailed help on all available commands and subtables.

!

TABLE: **built-in**COMMAND: **!**USAGE: **!** [Number{0..15}] [command{31}]

DESCRIPTION:

Executes the last command that was entered. If a command (or history number) is specified, then it executes that command from the history buffer. This works like the Unix '!' command

EXAMPLES:

!	-- This repeats the last command that was entered.
! cd	-- This repeats the last 'cd' command that was entered.

?

TABLE: **built-in**COMMAND: **?**USAGE: **?** [-t|-l|-s|-i|-a|-lr] [command [...]{126}]

DESCRIPTION:

Alias for 'help'. Type 'help help' for more information.

REMTABLE: **built-in**COMMAND: **REM**USAGE: **REM** [Remark text{126}]

DESCRIPTION:

Ignores the text that follows; used for remarks, scripting, etc.



EXAMPLES:

```
REM Started test here.  --
```

cdTABLE: **built-in**COMMAND: **cd**

USAGE: cd [subtable | .. | \ | / {31}]

DESCRIPTION:

Sets the specified command table as the active table. This works like the DOS or Unix 'cd' command where '.' takes you to the previous table, and '\' or '/' takes you to the root table. If no parameters are specified, then it shows the name of the currently active command table.

EXAMPLES:

```
cd classifiers  -- Makes the specified subtable the active
command table.
cd \           -- Makes the main command table active.
cd ..         -- Makes the previous (parent) command table
active.
cd            -- Shows the name of the active command
table.
cd \non\doc    -- You can specify partial names, and
multiple subdirs.
```

dirTABLE: **built-in**COMMAND: **dir**

USAGE: dir [-t|-l|-s|-i|-a|-lr] [command [...] {126}]

DESCRIPTION:

Alias for 'help'. Refer to 'help' for more information.

find_commandTABLE: **built-in**COMMAND: **find_command**

USAGE: find_command command {31}

DESCRIPTION:



Displays the name of all subdirectories which contain the specified command.

EXAMPLES:

```
find_command show --
```

history

TABLE: **built-in**

COMMAND: **history**

USAGE: history

DESCRIPTION:

Shows a list of commands that were previously typed.

EXAMPLES:

```
history --
```

instances

TABLE: **built-in**

COMMAND: **instances**

USAGE: instances [name{31}]

DESCRIPTION:

Shows the set of object instances that have registered with the active table. This is the same as 'help -i', except that it lets you specify a partial instance name in order to limit the list that is displayed (only instances whose names match the partial string are shown). The name is not case sensitive.

EXAMPLES:

```
instances -- Shows all instances registered with the
command table.
instances p -- Shows all instances whose name begins with
'p' or 'P'.
```

ls

TABLE: **built-in**

COMMAND: **ls**

USAGE: ls [-t|-l|-s|-i|-a|-lr] [command [...] {126}]

DESCRIPTION:



Alias for 'help'. Type 'help help' for more information.

man

TABLE: **built-in**

COMMAND: **man**

USAGE: man [-t|-l|-s|-i|-a|-lr] [command [...] {126}]

DESCRIPTION:

Alias for 'help'. Type 'help help' for more information.

pwd

TABLE: **built-in**

COMMAND: **pwd**

USAGE: pwd

DESCRIPTION:

Shows the name of the currently active command table. This is like the Unix 'pwd' command.

EXAMPLES:

```
pwd --
```

sleep

TABLE: **built-in**

COMMAND: **sleep**

USAGE: sleep Milliseconds

DESCRIPTION:

Causes the console to sleep for the specified number of milliseconds. This is useful for scripting, where you want to delay between commands.

EXAMPLES:

```
sleep 1000 -- Makes the console sleep for 1 second
```

syntax

TABLE: **built-in**

COMMAND: **syntax**



USAGE: syntax

DESCRIPTION:

Displays detailed information on command line syntax and how the parser works.

EXAMPLES:

```
syntax --
```

system_time

TABLE: **built-in**

COMMAND: **system_time**

USAGE: system_time

DESCRIPTION:

Displays the current system millisecond tick counter.

EXAMPLES:

```
system_time --
```

usage

TABLE: **built-in**

COMMAND: **usage**

USAGE: usage

DESCRIPTION:

Displays information about how the console works, and how to use it.

EXAMPLES:

```
usage --
```

TelMTA_console

TABLE: **built-in**

COMMAND: **TelMTA_console**

USAGE: TelMTA_console

DESCRIPTION:

Gives control of the console to the MTA.

EXAMPLES:



TelMTA_console

emta_console

TABLE: **built-in**

COMMAND: **emta_console**

USAGE: emta_console

DESCRIPTION:
Gives control of the console to the EMTA.

EXAMPLES:

emta_console

exit

Command Name: **exit**

Short Form: **e**

Command Usage: **e**

Command Action: Exits the current table and returns to a higher table in the hierarchy.

EXAMPLE:

<pre>MAIN> qos Quality of Service submenu qos> e MAIN></pre>

ping

TABLE: **built-in**

COMMAND: **ping**

USAGE: ping IpAddress

DESCRIPTION:
Pings the specified target IP address, sending 3 64-byte packets, and waiting up to 5 seconds for a response. This is a basic 'standard' ping. For more options or control over ping parameters and behavior, you will need to go to the Ping Command table ('cd pingHelper').

In order for this to work, the CM must either have successfully completed DHCP, or must otherwise have been configured with a valid IP address.

Note that this command causes the ping options to be reset to their default state.

This may be disabled if the platform doesn't provide an implementation of ping.

EXAMPLES:



```
ping 11.24.4.3 -- Ping IP address 11.24.4.3.
```

read_memory

TABLE: **built-in**

COMMAND: **read_memory**

USAGE: read_memory [-p] [-c] [-s ElementSize{1..4}] [-n NumberOfBytes{1..16384}] [StartAddress]

DESCRIPTION:

Displays the contents of memory (in hex and ASCII) to the console.

StartAddress: the address to start displaying (can be memory, registers, etc).

-s : sets the element size to be read (1, 2, or 4 bytes). Most useful for registers; defaults to 1.

-n : sets the number of bytes to be read. Defaults to 16. Note that this will always be padded out to a multiple of the element size.

-c : increments the start address by the number of bytes before reading. This is most useful for continuing the previous read (with the same parameters).

-p : prints the current options (which would be used if not otherwise supplied).

If no parameters are specified, it will perform the last read again.

NOTE: the parameters are remembered from one read to the next; e.g. if you set the element size to 4 bytes, then all subsequent reads will use this, unless explicitly overridden.

WARNING: it may be possible to make the system hang or crash if you read from an illegal address!

EXAMPLES:

```
read_memory -s 4 -n 64 0x80001234 -- Reads 64 bytes as 32-
                                   bit values.
read_memory -n 32 0x80001234      -- Reads 32 bytes starting
                                   with the specified
                                   address.
read_memory -c                    -- Reads the next 32
                                   bytes, continuing from
                                   the previous read.
```

reset

TABLE: **built-in**

COMMAND: **reset**

USAGE: reset



DESCRIPTION:

Causes the application to exit, shutting everything down and cleaning up resources. On embedded platforms, this usually also triggers the internal CPU reset logic, causing the h/w to reboot.

EXAMPLES:

```
reset --
```

run_app

TABLE: **built-in**

COMMAND: **run_app**

USAGE: run_app

DESCRIPTION:

If the application was stopped at the console (either via keypress or via non-vol setting that automatically stopped it), then this command will allow it to start running. If the application is already running, this will cause it to start over again.

EXAMPLES:

```
run_app --
```

shell

TABLE: **built-in**

COMMAND: **shell**

USAGE: shell

DESCRIPTION:

Causes the application to jump to eCos shell.

EXAMPLES:

```
shell --
```

version

TABLE: **built-in**

COMMAND: **version**

USAGE: version



DESCRIPTION:

Displays the current software version and feature codes by printing the startup banner. This allows the user to view the current version information without having to restart the application.

EXAMPLES:

```
version --
```

write_memory

TABLE: **built-in**

COMMAND: **write_memory**

USAGE: write_memory [-s ElementSize{1..4}] Address Value

DESCRIPTION:

Writes the specified value to the specified address.

Address : the address to write to (can be memory, registers, etc).

Value : the value to write.

-s : sets the element size to be written (1, 2 or 4 bytes). If not specified, the default is 1 byte.

NOTE: unlike read_memory, the parameters are not remembered from one write to the next.

WARNING: it is possible to make the system hang or crash if you write to an illegal address (or write over the application code)!

EXAMPLES:

```
write_memory 0x80001234 0x56          -- Write a byte to
                                     the address.
write_memory -s 4 0x80001234 0x12345678 -- Write 32 bits.
```

zone

TABLE: built-in

COMMAND: zone

USAGE: zone [Bitmask{0xffff}]

DESCRIPTION:

Prints or sets the HAL debug zones; this determines what debug messages will be displayed by HAL drivers. These bits correspond to the HAL debug zones:

0x0001 -- INIT



```
0x0002 -- TEST1
0x0004 -- TEST2
0x0008 -- TEST3
0x0010 -- TEST4
0x0020 -- TEST5
0x0040 -- TEST6
0x0080 -- BPI
0x0100 -- DOWNSTREAM
0x0200 -- UPSTREAM
0x0400 -- TUNER
0x0800 -- RANGING
0x1000 -- TESTSRAM
0x2000 -- TESTREG
0x4000 -- WARNING
0x8000 -- ERROR
```

EXAMPLES:

```
zone 0xc000 -- Enables ERROR and WARNING levels.
```

HeapManager Table Commands

memShow

TABLE: **HeapManager**

COMMAND: **memShow**

USAGE: memShow

DESCRIPTION:

Displays summary of available heap.

EXAMPLES:

```
memShow --
```

stats

TABLE: **HeapManager**

COMMAND: **stats**

USAGE: stats

DESCRIPTION:

Displays detailed heap manager counters and statistics.

EXAMPLES:

```
stats --
```

threadUsage

TABLE: **HeapManager**

COMMAND: **threadUsage**

USAGE: threadUsage

DESCRIPTION:
Displays total allocated memory per thread

EXAMPLES:

```
threadUsage --
```

trace

TABLE: **HeapManager**

COMMAND: **trace**

USAGE: trace tid [size]

DESCRIPTION:
Enables debug tracing for the specified thread ID or all threads if the parameter is 0

EXAMPLES:

```
trace 0x80b0a0a0 24      - enable 24 byte alloc tracing for
the thread with TID
0x80b0a0a0
trace 0x80b0a0a0        - enable all alloc tracing for the
thread with TID
0x80b0a0a0
trace 0                  - disable alloc tracing --
```

walk

TABLE: **HeapManager**

COMMAND: **walk**

USAGE: walk

DESCRIPTION:
Displays all of the free memory blocks.

EXAMPLES:

```
walk --
```



walk_alloc

TABLE: **HeapManager**

COMMAND: **walk_alloc**

USAGE: walk_alloc

DESCRIPTION:

Displays all of the allocated memory blocks. WARNING: This can print a LOT of information!

EXAMPLES:

```
walk_alloc --
```

docsis_ctl Table Commands

ClearCmCert

TABLE: **docsis_ctl**

COMMAND: **ClearCmCert**

USAGE: ClearCmCert

DESCRIPTION:

Clears the Cable Modem Certificate.

EXAMPLES:

```
ClearCmCert --
```

binarySfid

TABLE: **docsis_ctl**

COMMAND: **binarySfid**

USAGE: **binarySfid [true|false]**

DESCRIPTION:

Use binary SFID encoding in CM initiated DSD REQ.

EXAMPLES:

```
binarySfid true --
```

bpiShow



TABLE: **docsis_ctl**

COMMAND: **bpiShow**

USAGE: bpiShow

DESCRIPTION:

Prints the BPI State Machine Parameters.

EXAMPLES:

```
bpiShow --
```

cfg_hex_show

TABLE: **docsis_ctl**

COMMAND: **cfg_hex_show**

USAGE: cfg_hex_show

DESCRIPTION:

Prints last config file in ASCII hex format. eof byte 0xFF is omitted.

EXAMPLES:

```
cfg_hex_show --
```

cfg_tlv_show

TABLE: **docsis_ctl**

COMMAND: **cfg_tlv_show**

USAGE: cfg_tlv_show

DESCRIPTION:

Prints last config file in TLV format. eof byte 0xFF is omitted.

EXAMPLES:

```
cfg_tlv_show --
```

clear_image

TABLE: **docsis_ctl**

COMMAND: **clear_image**

USAGE: clear_image [-i Number]

DESCRIPTION:

This causes the specified image (stored in flash memory) to be erased. The -i parameter specifies the image number to be cleared (number of images depends on the platform).

WARNING: If you clear all images, then the system won't run!

EXAMPLES:

```
clear_image      -- Clears default image from flash memory.
clear_image -i1  -- Clears image1 from flash memory.
```

comp_mac_to_phy

TABLE: **docsis_ctl**

COMMAND: **comp_mac_to_phy**

USAGE: comp_mac_to_phy [-v] mac_bytes iuc{1..15}

DESCRIPTION:

Runs the UCD-based MAC-to-PHY computation for the specified number of MAC bytes on the specified IUC code. If -v is specified, then verbose debug output will be displayed.

EXAMPLES:

```
comp_mac_to_phy -v 1518 5 -- Does verbose computation for
1518 bytes on the Short Data IUC.
```

comp_phy_to_mac

TABLE: **docsis_ctl**

COMMAND: **comp_phy_to_mac**

USAGE: comp_phy_to_mac [-v] phy_mslots iuc{1..15}

DESCRIPTION:

Runs the UCD-based PHY-to-MAC computation for the specified number of PHY minislots on the specified IUC code. If -v is specified, then verbose debug output will be displayed.

EXAMPLES:

```
comp_phy_to_mac -v 20 5 -- Does verbose computation for 20
mslots on the Short Data IUC.
```

copy_image



TABLE: **docsis_ctl**

COMMAND: **copy_image**

USAGE: `copy_image SourceImage{1..2} DestinationImage{1..2}`

DESCRIPTION:

This causes the specified source image (stored in flash memory) to be copied to the specified destination image. The source image must be valid, and must be small enough to fit in the dest image slot.

EXAMPLES:

```
copy_image 2 1 -- Copies image2 to the imagel slot.
```

dload

TABLE: **docsis_ctl**

COMMAND: **dload**

USAGE: `dload [-i Number] [-s] [-l] [-f] [IpAddress] [Filename{127}]`

DESCRIPTION:

Causes the CM DOCSIS Control thread to download and store the specified image file via TFTP from the specified TFTP Server IP address. When the download is completed, the next reboot will run this image. If you omit the filename and/or IP address parameters, then we will use the ones stored in non-vol settings. The -i parameter specifies the image number to be overwritten (number of images depends on the platform). If omitted then the default image for the platform will be used. If present, the -s causes Secure Download to be used. The -l flag selects imagel as the target and allows a large image to be loaded, if allowed by the flash driver. The -f flag forces the image to be loaded even if the signature or compression types are not valid for the platform.

EXAMPLES:

```
dload 11.24.4.3 ram_sto.bin      -- TFTP's ram_sto.bin from
the server.
dload -il 11.24.4.3 ram_sto.bin  -- Same, but downloads to
imagel.
dload                            -- Uses the file/server
from non-vol                      settings.
dload -s 11.24.4.3 ram_sto.bin   -- Secure download.
dload -l 11.24.4.3 ram_sto.bin   -- Download large image
to imagel.
dload -f 11.24.4.3 ram3360_sto.bin -- Loads a 3360 image
onto a 3345 modem.
```

dsdiag

TABLE: **docsis_ctl**



COMMAND: **dsdiag**

USAGE: dsdiag

DESCRIPTION:

Shows concise information about the downstream state.

EXAMPLES:

```
dsdiag --
```

dsx_show

TABLE: **docsis_ctl**

COMMAND: **dsx_show**

USAGE: dsx_show

DESCRIPTION:

Shows the current state of the DSx Helper object.

EXAMPLES:

```
dsx_show --
```

goto_ds

TABLE: **docsis_ctl**

COMMAND: **goto_ds**

USAGE: goto_ds Frequency

DESCRIPTION:

Causes the CM to move to the Ds Freq specified. If the CM fails to lock at the specified frequency, then it will continue scanning. When it locks on a valid downstream, it will then range, perform IP initialization, and register. The value can be in units of Hz or MHz (if the value is less than 10,000, then it is assumed to be MHz).

EXAMPLES:

```
goto_ds 405000000 -- Goes to the CMTS at 405 MHz.  
goto_ds 327      -- Goes to the CMTS at 327 MHz.
```

goto_us

TABLE: **docsis_ctl**



COMMAND: **goto_us**

USAGE: goto_us US Channel{0..255}

DESCRIPTION:

Causes the CM to move to the US Channel specified, staying on the current downstream frequency. The CM must be locked to a downstream channel for this to work.

NOTE: Some CMTSs may not support this, though they all should.

EXAMPLES:

```
goto_us 3  -- Goes to upstream channel 3.
```

IgmpShow

TABLE: **docsis_ctl**

COMMAND: **igmpShow**

USAGE: igmpShow

DESCRIPTION:

Prints the IGMP Group Statistics.

EXAMPLES:

```
igmpShow  --
```

ip_initialize

TABLE: **docsis_ctl**

COMMAND: **ip_initialize**

USAGE: ip_initialize [dhcp]

DESCRIPTION:

This causes the IP stack to lock in it's canned DHCP settings (IP and router addresses), and enables forwarding of packets to all interfaces. If you use the 'dhcp' parameter, then it will do DHCP to get the address; otherwise, it will use the DHCP settings from non-vol memory.

EXAMPLES:

```
ip_initialize dhcp  -- Forces the IP stack to to do DHCP.
```

ip_show



TABLE: **docsis_ctl**

COMMAND: **ip_show**

USAGE: ip_show

DESCRIPTION:

Shows the DHCP settings that are being used by the IP stack.

EXAMPLES:

```
ip_show --
```

log_messages

TABLE: **docsis_ctl**

COMMAND: **log_messages**

USAGE: log_messages [Bitmask{0xffff}]

DESCRIPTION:

Enables/disables logging of DOCSIS MAC Management messages, along with TLV parsing/generation associated with them. You can enable logging of multiple messages by setting their bits to 1. These are the bit definitions:

```
0x0001 -- UCD
0x0002 -- RNG-REQ
0x0004 -- RNG-RSP
0x0008 -- Config file contents
0x0010 -- REG-REQ/RSP/ACK
0x0020 -- UCC-REQ/RSP, DCC-REQ/RSP/ACK
0x0040 -- DSx-REQ/RSP/ACK
0x0080 -- DCI-REQ/RSP
0x0100 -- UP-DIS
0x0200 -- gathering set of useable UCD's
0x0400 -- TST-REQ
0x0800 -- US phy overhead computations
0x1000 -- on the fly UCD change
0x4000 -- Log raw message octets
0x8000 -- Show TLV parsing/generation
```

EXAMPLES:

```
log_messages          -- Shows the bitmask of enabled message
logging.
log_messages 0x01      -- Enables logging of UCD messages.
log_messages 0x8001    -- Enables logging of UCD message TLV
parsing.
```

map_debug

TABLE: **docsis_ctl**



COMMAND: **map_debug**

USAGE: map_debug NumberOfMaps{0..32} [SID{0..16383}]

DESCRIPTION:

Enables logging of DOCSIS MAP messages; because there are a lot of MAPs on the downstream, you are required to enter a limited number of MAP messages to be logged. This keeps the system from crashing or otherwise misbehaving due to the amount of output. Additionally, you can filter the output on a particular SID, displaying only 'interesting' MAPs.

EXAMPLES:

```
map_debug 10          -- Logs the next 10 MAP messages.
map_debug 10 0x104    -- Logs the next 10 MAPs with grants to
                      SID 0x104.
```

modem_caps

TABLE: **docsis_ctl**

COMMAND: **modem_caps**

USAGE: modem_caps

DESCRIPTION:

Prints the modem capabilities from the REG-RSP.

EXAMPLES:

```
modem_caps --
```

rate_shaping_enable

TABLE: **docsis_ctl**

COMMAND: **rate_shaping_enable**

USAGE: rate_shaping_enable [true|false]

DESCRIPTION:

This enables/disables DOCSIS 1.0 Class of Service or DOCSIS 1.1 QoS rate shaping. If disabled, then no rate shaping will be performed.

EXAMPLES:

```
rate_shaping_enable true -- Enable CoS/QoS rate shaping.
```

rng_rsp

TABLE: **docsis_ctl**

COMMAND: **rng_rsp**



USAGE: rng_rsp [true|false]

DESCRIPTION:

Enables/disables the one-line RNG-RSP messages that are displayed when a ranging response message is received from the CMTS.

EXAMPLES:

```
rng_rsp false -- Disables the RNG-RSP messages.
```

scan_stop

TABLE: **docsis_ctl**

COMMAND: **scan_stop**

USAGE: scan_stop

DESCRIPTION:

Causes the CM to stop scanning for a downstream channel. You must use goto_ds to start scanning again.

EXAMPLES:

```
scan_stop --
```

showFlows

TABLE: **docsis_ctl**

COMMAND: **showFlows**

USAGE: showFlows

DESCRIPTION:

Prints the current Dynamic Flow STDs.

EXAMPLES:

```
showFlows --
```

state

TABLE: **docsis_ctl**

COMMAND: **state**

USAGE: state



DESCRIPTION:

Shows the current state of the CM DOCSIS Control Thread.

EXAMPLES:

```
state --
```

stop_download

TABLE: **docsis_ctl**

COMMAND: **stop_download**

USAGE: stop_download

DESCRIPTION:

If a software download is in progress, this will stop it in its tracks. The storage for the partially downloaded image will be cleared.

EXAMPLES:

```
stop_download --
```

ucdShow

TABLE: **docsis_ctl**

COMMAND: **ucdShow**

USAGE: ucdShow

DESCRIPTION:

Prints the current upstream channel description being used.

EXAMPLES:

```
ucdShow --
```

ucddiag

TABLE: **docsis_ctl**

COMMAND: **ucddiag**

USAGE: ucddiag

DESCRIPTION:

Shows concise information about the UCD state.

EXAMPLES:

```
ucddiag --
```



up_dis

TABLE: **docsis_ctl**

COMMAND: **up_dis**

USAGE: up_dis [-t Number]

DESCRIPTION:

Causes the DOCSIS state to be reset, deleting all flows, stopping BPI, deregistering from CMTS, stopping ranging, etc. This is equivalent to receiving an UP-DIS message. RFI-N-01049 added the timeout parameter, which you can specify with the -t parameter.

EXAMPLES:

```
up_dis          -- Simulates an UP-DIS message (timeout=forever)
up_dis -t 20    -- Simulates an UP-DIS message (timeout=20 ms).
```

us_phy_oh_show

TABLE: **docsis_ctl**

COMMAND: **us_phy_oh_show**

USAGE: us_phy_oh_show

DESCRIPTION:

Prints computed upstream phy overhead settings.

EXAMPLES:

```
us_phy_oh_show --
```

usdiag

TABLE: **docsis_ctl**

COMMAND: **usdiag**

USAGE: usdiag

DESCRIPTION:

Shows concise information about the upstream state.

EXAMPLES:

```
usdiag --
```



embedded_target Table Cammands

bcmalloc_show

TABLE: **embedded_target**

COMMAND: **bcmalloc_show**

USAGE: **bcmalloc_show** [-c]

DESCRIPTION:

Displays a snapshot of the current BcmAlloc memory pool statistics. If -c is specified, then the counters are also cleared.

EXAMPLES:

```
bcmalloc_show --
```

embedded_target

TABLE: **embedded_target**

COMMAND: **bcmalloc_walk**

USAGE: **bcmalloc_walk**

DESCRIPTION:

Displays information about the allocated and free BcmAlloc buffers.

NOTE: This can print a LOT of information!

EXAMPLES:

```
bcmalloc_walk --
```

cp0_read

TABLE: **embedded_target**

COMMAND: **cp0_read**

USAGE: **cp0_read** [-s RegisterSelect{0..7}] RegisterNumber{0..31}

DESCRIPTION:

Displays the contents of the coprocessor 0 register to the console.

RegisterNumber : the register number.

-s : the register select (defaults to 0)



EXAMPLES:

```
cp0_read 12      -- Reads the interrupt Status register.
cp0_read 16 -s 1 -- Reads the cache Config1 register.
```

cp0_writeTABLE: **embedded_target**COMMAND: **cp0_write**

USAGE: cp0_write [-s RegisterSelect{0..7}] RegisterNumber{0..31} RegisterValue

DESCRIPTION:

Writes the specified value to the specified coprocessor 0 register.

RegisterNumber: the register number.

-s : the register select (defaults to 0).

RegisterValue: the value to be written.

WARNING: it is possible to make the system hang or crash if you write to a nonexistent register or write an invalid value!

EXAMPLES:

```
cp0_write 12 0x1000fc00 -- Writes to the interrupt Status
register.
cp0_write 22 -s 5 0x20 -- Writes to register 22, select 5 (branch prediction).
```

dcacheTABLE: **embedded_target**COMMAND: **dcache**

USAGE: dcache [off|thru|back]

DESCRIPTION:

Turns the DCache off, or turns it on in writethru or writeback mode, as specified. The DCache will be flushed and invalidated so that any dirty cache lines will be sent to RAM.

EXAMPLES:

```
dcache off -- Turns the DCache off
```

icacheTABLE: **embedded_target**

COMMAND: **icache**

USAGE: icache [off|on]

DESCRIPTION:

Turns the ICache on or off, as specified.

EXAMPLES:

```
icache off -- Turns the ICache off
```

emta Table Commands

emta

TABLE: **emta**

COMMAND: **acquire_lease**

USAGE: acquire_lease

DESCRIPTION:

Acquire lease for EMTA

EXAMPLES:

```
acquire_lease
```

addFirewallRule

TABLE: **emta**

COMMAND: **addFirewallRule**

USAGE: addFirewallRule [port] [sourceIP] [subnetMask]

DESCRIPTION:

Adds an allowed port/subnet pair to the list of firewall rules

EXAMPLES:

```
addFirewallRule 21 10.24.16.21 255.255.255.255
```

announcementDload

TABLE: **emta**

COMMAND: **announcementDload**



USAGE: announcementDload [serverIP] [filename{254}] [index]

DESCRIPTION:

TFTP the specified announcement file from specified server into buffer with specified index

EXAMPLES:

```
announcementDload 10.24.192.200 myfile.bin 2 - tftp file into index 2
```

anti_spoof

TABLE: **emta**

COMMAND: **anti_spoof**

USAGE: anti_spoof [true|false]

DESCRIPTION:

Enable DHCP anti-spoofing measures for EMTAs IP stack

EXAMPLES:

```
anti_spoof
```

call_in_progress

TABLE: **emta**

COMMAND: **call_in_progress**

USAGE: call_in_progress [true|false]

DESCRIPTION:

Make-believe there is a call in progress, or not. This is mainly provided to test certain features which behave different ways when a call is up.

EXAMPLES:

```
call_in_progress true
```

cfgfile

TABLE: **emta**

COMMAND: **cfgfile**

USAGE: cfgfile [IP] [path{254}]

DESCRIPTION:

Load the specified config file. If IP or path are not specified, then the

settings from DOCSIS NV / dhcp settings will be used.

EXAMPLES:

```
cfgfile 10.24.192.200 /home/broadcom/cu.cfg
```

deleteFirewallRule

TABLE: **emta**

COMMAND: **deleteFirewallRule**

USAGE: deleteFirewallRule [port] [sourceIP] [subnetMask]

DESCRIPTION:

Deletes an allowed port/subnet pair from the list of firewall rules

EXAMPLES:

```
deleteFirewallRule 21 10.24.16.21 255.255.255.255
```

dhcp_init

TABLE: **emta**

COMMAND: **dhcp_init**

USAGE: dhcp_init

DESCRIPTION:

Sets up EMTA DHCP event callback to a function that prints the events when received

EXAMPLES:

```
dhcp_init
```

emta_console

TABLE: **emta**

COMMAND: **emta_console**

USAGE: emta_console

DESCRIPTION:

Gives control of the console to the EMTA.

EXAMPLES:

```
ip_initialize dhcp -- Forces the IP stack to to do DHCP.
ip_initialize      -- Inits with non-vol settings.
```

firewallEnable

TABLE: **emta**

COMMAND: **firewallEnable**

USAGE: firewallEnable [true/false]

DESCRIPTION:

Enables or disables the firewall snoop

EXAMPLES:

```
firewallEnable true
```

ifEntry

TABLE: **emta**

COMMAND: **ifEntry**

USAGE: ifEntry

DESCRIPTION:

Add an EMTA ifEntry as for a voice line.

EXAMPLES:

```
ifEntry
```

initState

TABLE: **emta**

COMMAND: **initState**

USAGE: initState dhcp|snmp_tftp|rsip|normal|prov|noprov

DESCRIPTION:

Sets the MTA init state

EXAMPLES:

```
initState dhcp
initState snmp_tftp
initState rsip
initState normal
```



ip_get

TABLE: **emta**

COMMAND: **ip_get**

USAGE: ip_get

DESCRIPTION:

Get the EMTA DHCP IP address

EXAMPLES:

```
ip_get
```

ip_initialize

TABLE: **emta**

COMMAND: **ip_initialize**

USAGE: ip_initialize [dhcp]

DESCRIPTION:

This causes the IP stack to lock in it's canned DHCP settings (IP and router addresses), and enables forwarding of packets to all interfaces. If you use the 'dhcp' parameter, then it will do DHCP to get the address; otherwise, it will use the DHCP settings from non-vol memory.

EXAMPLES:

```
ip_initialize dhcp -- Forces the IP stack to to do DHCP.
```

lineState

TABLE: **emta**

COMMAND: **lineState**

USAGE: lineState 1|2 on|off|fault

DESCRIPTION:

Sets the line state

EXAMPLES:

```
lineState 1 on
lineState 2 off
lineState 1 fault
```



log

TABLE: **emta**

COMMAND: **log**

USAGE: log [Bitmask{0x40007f}]

DESCRIPTION:

Configures the message log settings for this class to enable or disable various app-specific severities. These settings are inherited only when a call is started.

These are the bits supported:

- 0x01 -- Service flow setup info
- 0x02 -- EMTA buffer allocation failures
- 0x04 -- Detailed QoS flow settings

EXAMPLES:

```
log 0x2 -- Enable logging when EMTA voice packet buffer
allocation fails
```

new_line

TABLE: **emta**

COMMAND: **new_line**

USAGE: new_line

DESCRIPTION:

Adds an instance of the ETMA call simulator. A subtable will be added dynamically to this table to control all instances of the line simulator.

EXAMPLES:

```
new_line -- Create 1 new instance.
```

option_get

TABLE: **emta**

COMMAND: **option_get**

USAGE: option_get [optionCode]

DESCRIPTION:

Get an EMTA DHCP option

EXAMPLES:



```
option_get 1
```

release_lease

TABLE: **emta**

COMMAND: **release_lease**

USAGE: release_lease

DESCRIPTION:
Release lease for EMTA

EXAMPLES:

```
release_lease
```

renew_lease

TABLE: **emta**

COMMAND: **renew_lease**

USAGE: renew_lease

DESCRIPTION:
Renew lease for EMTA

EXAMPLES:

```
renew_lease
```

run_app

TABLE: **emta**

COMMAND: **run_app**

USAGE: run_app

DESCRIPTION:
If the EMTA application was stopped at the console (either via keypress or via non-vol setting that automatically stopped it), then this command will allow it to start running. This command is not available if the application is already running.

EXAMPLES:

```
run_app --
```

server_get

TABLE: **emta**

COMMAND: **server_get**

USAGE: server_get

DESCRIPTION:
Get the DHCP server IP address

EXAMPLES:

```
server_get
```

showAnnounce

TABLE: **emta**

COMMAND: **showAnnounce**

USAGE: showAnnounce

DESCRIPTION:
Shows the currently downloaded announcements

EXAMPLES:

```
showAnnounce
```

showFirewallState

TABLE: **emta**

COMMAND: **showFirewallState**

USAGE: showFirewallState

DESCRIPTION:
Shows the current state of the firewall

EXAMPLES:

```
showFirewallState
```

snmp_ip_update

TABLE: **emta**

COMMAND: **snmp_ip_update**

USAGE: snmp_ip_update

DESCRIPTION:

Update the EMTA SNMP agent's IP address, router, subnet, etc. from the EMTA's current settings. This is generally used in conjunction with the ip_init command when running with no EMTA library, in which case there is no path back to the SNMP agent after ip_init completes.

EXAMPLES:

```
snmp_ip_update
```

soft_reset

TABLE: **emta**

COMMAND: **soft_reset**

USAGE: soft_reset

DESCRIPTION:

Perform an EMTA soft reset.

EXAMPLES:

```
soft_reset
```

suboption_get

TABLE: **emta**

COMMAND: **suboption_get**

USAGE: suboption_get

DESCRIPTION:

Get a CM DHCP suboption

EXAMPLES:

```
suboption_get 2
```

test_v3

TABLE: **emta**

COMMAND: **test_v3**

USAGE: test_v3

DESCRIPTION:
{No command help available...}

flash Table Commands

autoTest

TABLE: **flash**

COMMAND: **autoTest**

USAGE: autoTest bootloader|image1|image2|perm|dyn [BlockNumber]

DESCRIPTION:
Does an automated test suite on the specified flash block (in the specified region) to ensure that all of the flash driver functions work correctly.

NOTE: any data in the specified block will be erased! Choose a block that is not being used for anything important! Use the 'show' command to list the blocks and how they are allocated.

If you omit the BlockNumber parameter, the test will be run over all blocks in the region (destroying any data that is in the blocks).

In July 2004, we had to change the flash driver in order to support multiple flash devices. As a result, you can no longer just specify the block number; you must also specify the region that the block is in (the region maps to a flash device, and the block number within that device will be tested). If you specify a region that does not contain the block, then the test will fail.

EXAMPLES:

```
autoTest image2 33 -- Performs the test suite on block 33
                    (which is in the image2 region)
autoTest image2    -- Performs the test suite on all blocks in the image2 region
```

cfi_show

TABLE: flash

COMMAND: cfi_show

USAGE: cfi_show bootloader|image1|image2|perm|dyn

DESCRIPTION:
Displays the CFI database for the flash device associated with the specified region (if the device is CFI-compliant).

EXAMPLES:



```
cfi_show image2 -- Displays CFI info for the flash device
associated with image2
```

close

TABLE: **flash**

COMMAND: **close**

USAGE: close

DESCRIPTION:

Closes the flash driver, allowing the rest of the application to use it. Calling this more than once has no effect.

EXAMPLES:

```
close --
```

configRegion

TABLE: flash

COMMAND: configRegion

USAGE: configRegion bootloader|image1|image2|perm|dyn SizeBytes

DESCRIPTION:

Configures the minimum acceptable size for a region. This takes effect the next time the driver is initialized. Specifying a size of 0 restores the default built in to the driver.

EXAMPLES:

```
configRegion perm 65536 -- Configures Perm NonVol to require
a minimum of 64k
```

deinit

TABLE: **flash**

COMMAND: **deinit**

USAGE: deinit

DESCRIPTION:

Deinitializes the flash driver, making it release resources. Note that the flash device will be unusable after this, until you run the init command.

EXAMPLES:



```
deinit --
```

erase

TABLE: **flash**

COMMAND: **erase**

USAGE: erase [-b BlockNumber] [-a Offset] [-r]

DESCRIPTION:

Erases the flash block specified by the block number (-b), address offset (-a) or erases all blocks in the region (-r).

EXAMPLES:

```
erase -b 3 -- Erases block number 3 (the fourth block)
```

init

TABLE: **flash**

COMMAND: **init**

USAGE: init

DESCRIPTION:

Initializes the flash driver, making it detect the flash device. This is usually done for you at system startup, but may be needed if you deinit the driver. This command has no effect if the driver is already initialized.

EXAMPLES:

```
init --
```

open

TABLE: **flash**

COMMAND: **open**

USAGE: open bootloader|image1|image2|perm|dyn

DESCRIPTION:

Opens the flash driver for use by the console (locking out the rest of the application!) so that you can use the read/write/erase commands. NOTE: If you do something that would cause the driver to be opened again (write nonvol, dload an image, etc), then the operation will be blocked until you run the close command, or it may fail.

EXAMPLES:

```
open image2 -- Opens the image2 region for read/write/erase
```



read

TABLE: **flash**

COMMAND: **read**

USAGE: read Size{1..4} Number{1..8192} Offset

DESCRIPTION:

Uses the read functions to access data in the flash device, printing to the console. You must specify the size of the read (1, 2, or 4 bytes), the number of bytes to read, and the offset into the region to start. The offset should be aligned correctly for the size specified.

EXAMPLES:

```
read 1 4 0      -- Reads 4 bytes at the beginning of the region
read 4 8 1024   -- Reads 2 dwords at offset 1k in the region
```

readDirect

TABLE: **flash**

COMMAND: **readDirect**

USAGE: readDirect Number{1..8192} Offset

DESCRIPTION:

Uses the read direct function to access the flash memory data directly, printing to the console. You must specify the number of bytes to read and the offset into the region to start.

EXAMPLES:

```
readDirect 128 0 -- Reads 128 bytes at the beginning of the
region
```

show

TABLE: **flash**

COMMAND: **show**

USAGE: show

DESCRIPTION:

Causes the flash driver to display its internal state.

EXAMPLES:

```
show --
```



write

TABLE: **flash**

COMMAND: **write**

USAGE: write Size{1..4} Offset Value

DESCRIPTION:

Uses the write functions to store data to the flash device. You must specify the size of the write (1, 2, or 4 bytes), the offset into the region to write, and the value. The offset should be aligned correctly for the size specified. The value will only be stored if the block was previously erased, or a bit is being changed from 1 to 0.

EXAMPLES:

```
write 1 0 0x12          -- Writes the byte value 0x12 to the
                        beginning of the region
write 4 1024 0x12345678 -- Writes the dword value to offset 1k in the region
```

writeArray

TABLE: **flash**

COMMAND: **writeArray**

USAGE: writeArray Number{1..131072} Offset

DESCRIPTION:

Uses the write array function to store an array of data (incrementing bytes) to the flash memory. You must specify the number of bytes to write and the offset into the region to start.

EXAMPLES:

```
writeArray 128 0 -- Writes 128 bytes at the beginning of the
region
```



Appendix A - EMTA LED Specification

LED / Control	Blinking State	EMTA 6528-2(R)e State
L1-L2	Blinking Amber	The connected telephone handset is on the hook (not in use) and there are new voice mail messages
	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
READY	Steady Green	The VoIP module is internally initialized and the unit is ready to make calls
	Off	Unit failed to register with both lines
RUN	Blinking Red	The VoIP Module failed to download a configuration or an image file
	Blinking Amber	The VoIP module is actively downloading a configuration file or a VoIP module firmware update
	Steady Green	The VoIP module has been configured successfully and is running normally
	Off / Off	The VoIP module is malfunctioning
STBY	Solid Amber	When STANDBY button is pressed and no data is allowed to be passed from the PC (USB or LAN Ethernet ports)
	Off	When STANDBY button is not pressed and data is allowed to be passed from the PC (USB or LAN Ethernet ports)
PC/ACT	Solid Green	When PC is connected to LAN Ethernet port
	Blinking Green	When Data is passed while PC is connected to LAN Ethernet port
	Solid Amber	When PC is connected to USB port
	Blinking Amber	When data is passed while PC is connected to USB port
	Off	No PC connected to USB or LAN Ethernet ports
ONLINE	Steady Green	The cable modem module has passed DOCSIS provisioning (including configuration file download) and is registered with the CMTS
	Blinking Green	The Cable modem module is attempting to register with CMTS
	Off	The cable modem module has not passed provisioning and has not registered with the CMTS
SEND	Steady Green	The cable modem module is locked to upstream frequency
	Blinking Green	The cable modem module is ranging on the upstream frequency
	Simultaneous Blinking with RECV	The cable modem module is currently upgrading
	Off	The cable modem module is not locked to upstream frequency



LED / Control	Blinking State	EMTA 6528-2(R)e State
RECV	Steady Green	The cable modem module is locked to downstream frequency
	Blinking Green	The cable modem module is searching for downstream frequency
	Simultaneous Blinking with SEND	The cable modem module is currently upgrading
	Off	The cable modem module is not locked to downstream frequency
PWR	Steady - Green	The device power is on.
	Off	The device power is off.