

MediaPack™ Series

Analog VoIP Media Gateways

MGCP & MEGACO Protocols

User's Manual

MP-1xx & MP-124



Version 6.6

June 2014

Document # LTRT-71405



Table of Contents

1	Introduction	9
1.1	About the MediaPack Gateway.....	9
1.2	MediaPack Features.....	10
1.3	Functional Block Diagrams	11
2	Software Package.....	13
2.1	Installing the Software Package	13
2.1.1	Installing/Unzipping When Using a Windows™ Operating System	13
2.1.2	Unzipping When Using a Linux™/Solaris™ Operating System	13
2.2	Software Directory Contents & Structure	14
3	Getting Started	15
3.1	Assigning the MediaPack IP Address	15
3.2	Assigning an IP Address Using HTTP	16
3.3	Assigning an IP Address Using BootP	17
3.4	Restoring Networking Parameters to their Default Values	18
4	Device Initialization & Configuration Files.....	19
4.1	Boot Firmware & Operational Firmware.....	19
4.2	MediaPack Startup	19
4.3	Using BootP/DHCP	21
4.3.1	BootP/DHCP Server Parameters	21
4.3.1.1	Command Line Switches.....	22
4.3.2	Host Name Support	23
4.3.3	Selective BootP	24
4.3.4	Microsoft™ DHCP/BootP Server.....	24
4.4	Configuration Parameters and Files	25
4.4.1	Initialization (ini) File	25
4.4.1.1	Parameter Value Structure.....	26
4.4.1.2	Tables of Parameter Value Structure.....	27
4.4.1.3	Binary Configuration File Download.....	30
4.4.2	Auxiliary Files.....	30
4.4.2.1	Downloading Auxiliary Files via TFTP During the Blade Startup	30
4.4.2.2	Automatic Update Facility.....	31
4.4.2.3	Downloading the dat File to a Device.....	34
4.5	Backup Copies of ini and Auxiliary Files	35
4.6	Upgrading Device Software	35
5	Automatic Configuration Options.....	37
5.1	Option A - Local Configuration Server with BootP/TFTP	37
5.2	Option B - DHCP-based Configuration Server	38
5.3	Option C - HTTP-based Automatic Updates	39
5.4	Option D - Configuration using DHCP Option 67	40
5.5	Option E - Configuration using FTP or NFS.....	41
5.6	Option F - TFTP Configuration using DHCP Option 66.....	41
5.7	Option G - Configuration using AudioCodes EMS	41
6	Configuration Using the Web Interface	43
6.1	Limiting the Web Interface to Read-Only Mode	43

6.1.1	Encrypted HTTP Transport (HTTPS - SSL)	44
6.1.2	Limiting Web Access to a Predefined List of Client IP Addresses	44
6.1.3	Managing Web Server Access Using a RADIUS Server	44
6.2	Accessing the Web Interface	45
6.3	Using Internet Explorer to Access the Web Interface	46
6.4	Areas of the GUI	47
6.4.1	Toolbar	48
6.4.2	Navigation Tree	49
6.4.2.1	Displaying Navigation Tree in Basic and Full View	49
6.4.2.2	Showing / Hiding the Navigation Pane	50
6.4.3	Help Infrastructure	51
6.4.4	Working with Configuration Pages	52
6.4.4.1	Accessing Pages	52
6.4.4.2	Viewing Parameters	52
6.4.4.3	Displaying Basic and Advanced Parameters	53
6.4.4.4	Showing / Hiding Parameter Groups	54
6.4.4.5	Modifying Parameter Values	54
6.4.5	Saving Configuration Changes	55
6.4.6	Searching for Configuration Parameters	55
6.4.7	Creating a Login Welcome Message	56
6.4.8	Logging Off the Web Interface	57
6.4.9	Getting Help	58
6.4.10	Using the Home Page	59
6.4.11	MediaPack Home Page	60
6.4.12	Viewing the Active Alarms Table	61
6.4.13	Viewing Channel Information	62
6.4.14	Viewing Ethernet Port Information	63
6.4.15	Viewing Ethernet Port Information	63
6.4.16	Viewing Trunk Settings	64
6.4.17	Assigning a Name or Brief Description to a Port	64
6.4.18	Resetting an Analog Channel	65
6.5	Configuration	66
6.5.1	System	66
6.5.1.1	Application Settings	66
6.5.1.2	Syslog Settings	68
6.5.1.3	Regional Settings	68
6.5.1.4	TLS Contexts	69
6.5.1.5	Management	75
6.5.2	VoIP	88
6.5.2.1	Network	88
6.5.2.2	IP Interface Table	88
6.5.2.3	Static Route Table	89
6.5.2.4	Network Settings	90
6.5.2.5	QoS Settings	91
6.5.2.6	Security Settings	92
6.5.2.7	Media	100
6.5.2.8	Quality of Experience	115
6.5.2.9	Call Control	116
6.6	Maintenance	122
6.6.1	Maintenance	122
6.6.1.1	Maintenance Actions	122
6.6.2	Software Update	126
6.6.2.1	Load Auxiliary Files	126
6.6.2.2	Software Upgrade Key	127
6.6.2.1	Software Upgrade Wizard	130
6.6.2.2	Configuration File	136
6.7	Status and Diagnostic Menu	139

6.7.1	System Status.....	139
6.7.1.1	Message Log.....	139
6.7.1.2	Device Information	140
6.7.1.3	Ethernet Port Information	141
6.7.1.4	Carrier-Grade Alarms	141
6.7.2	VoIP Status.....	143
6.7.2.1	Active IP Interfaces	143
6.7.2.2	Performance Statistics	144
7	Troubleshooting.....	145
7.1	Troubleshooting MediaPack Devices via the RS-232 Port.....	145
7.1.1	Viewing the Gateway's Information	145
7.1.2	Changing the Networking Parameters.....	146
7.1.3	Determining MediaPack Initialization Problems	146
7.1.4	Reinitializing the MediaPack.....	147
7.2	LED Indicators.....	149
7.2.1	MediaPack Front View LED Indicators	149
7.3	MediaPack Self-Testing.....	150
7.3.1	FXS Line Testing	150
7.3.2	FXO Line Testing.....	151
7.4	Self-Test.....	152
7.4.1	Operating the Syslog Server	153
7.4.1.1	Sending the Syslog Messages.....	153
7.4.1.2	Activating the Syslog Client.....	153
7.4.1.3	Setting Syslog Server IP Address, Enabling Syslog, in an ini File (Example)	153
8	List of Abbreviations.....	155
9	Technical Specifications	159

Reader's Notes

Notice

This document provides you with information on installation, configuration, and operation of MP-1X8 (8-port), MP-1X4 (4-port), MP-1X2 (2-port) the MP-124 (24-port) Media Gateways.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published, nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: June-10-2014

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

Reader's Notes

1 Introduction

This document provides you with information on installation, configuration, and operation of the MP-124 (24-port), MP-1X8 (8-port), MP-1X4 (4-port) and MP-1X2 (2-port) Media Gateways. As these units have similar functionality (except for the number of channels and some minor features), they are referred to collectively as the MediaPack. Prior knowledge of regular telephony and data networking concepts is preferred.

1.1 About the MediaPack Gateway

The MediaPack series analog VoIP gateways are cost-effective, cutting edge technology products. These stand-alone analog VoIP gateways provide superior voice technology for connecting legacy telephones, fax machines and PBX systems with IP-based telephony networks, as well as for integration with new IP-based PBX architecture. These products are designed and tested to be fully interoperable with leading softswitches and servers.

The MediaPack gateways incorporate up to 24 analog ports for connection, either directly to an enterprise PBX (FXO), to phones, or to fax (FXS), supporting up to 24 simultaneous VoIP calls.

Additionally, the MediaPack units are equipped with a 10/100 Base-TX Ethernet port for connection to the network.

The MediaPack gateways are best suited for small to medium size enterprises, branch offices or for residential media gateway solutions.

The MediaPack gateways enable users to make free local or international telephone / fax calls between the distributed company offices, using their existing telephones / fax. These calls are routed over the existing network ensuring that voice traffic uses minimum bandwidth.

The MediaPack gateways are compact devices that can be installed as a desk-top unit or on the wall or in a 19-inch rack.

1.2 MediaPack Features

The following provides a high-level overview of some of the many MediaPack supported features.

- Superior, high quality Voice, Data and Fax over IP networks.
- Toll quality voice compression.
- Vocoder configuration options include:
 - G.711 A/u-law PCM, G.726 ADPCM, G.727 ADPCM, G.723.1, G.729 A B, EG.711, G.722 (in Analog modules)
- Enhanced capabilities including MWI, long haul, metering, CID and outdoor protection.
- Proven integration with leading PBXs, IP-PBXs, Softswitches and servers.
- Spans a range of 2 to 24 FXS/FXO analog ports.
- Selectable G.711 or multiple Low Bit Rate (LBR) coders per channel.
- T.38 fax with superior performance (handling a round-trip delay of up to nine seconds).
- Echo Canceler, Jitter Buffer, Voice Activity Detection (VAD) and Comfort Noise Generation (CNG) support.
- Comprehensive support for supplementary services.
- Web Management for easy configuration and installation.
- EMS for comprehensive management operations (FCAPS).
- Simple Network Management Protocol (SNMP) and Syslog support.
- SMDI support for Voice Mail applications.
- Multiplexes RTP streams from several users together to reduce bandwidth overhead.
- T.38 fax fallback to PCM (or NSE).
- Can be integrated into a VLAN-aware environment.
- Capable of automatically updating its firmware version and configuration.
- Web access (HTTPS) and Telnet access using SSL / TLS.

1.3 Functional Block Diagrams

Figure 1: Typical MP-11x Application Diagram

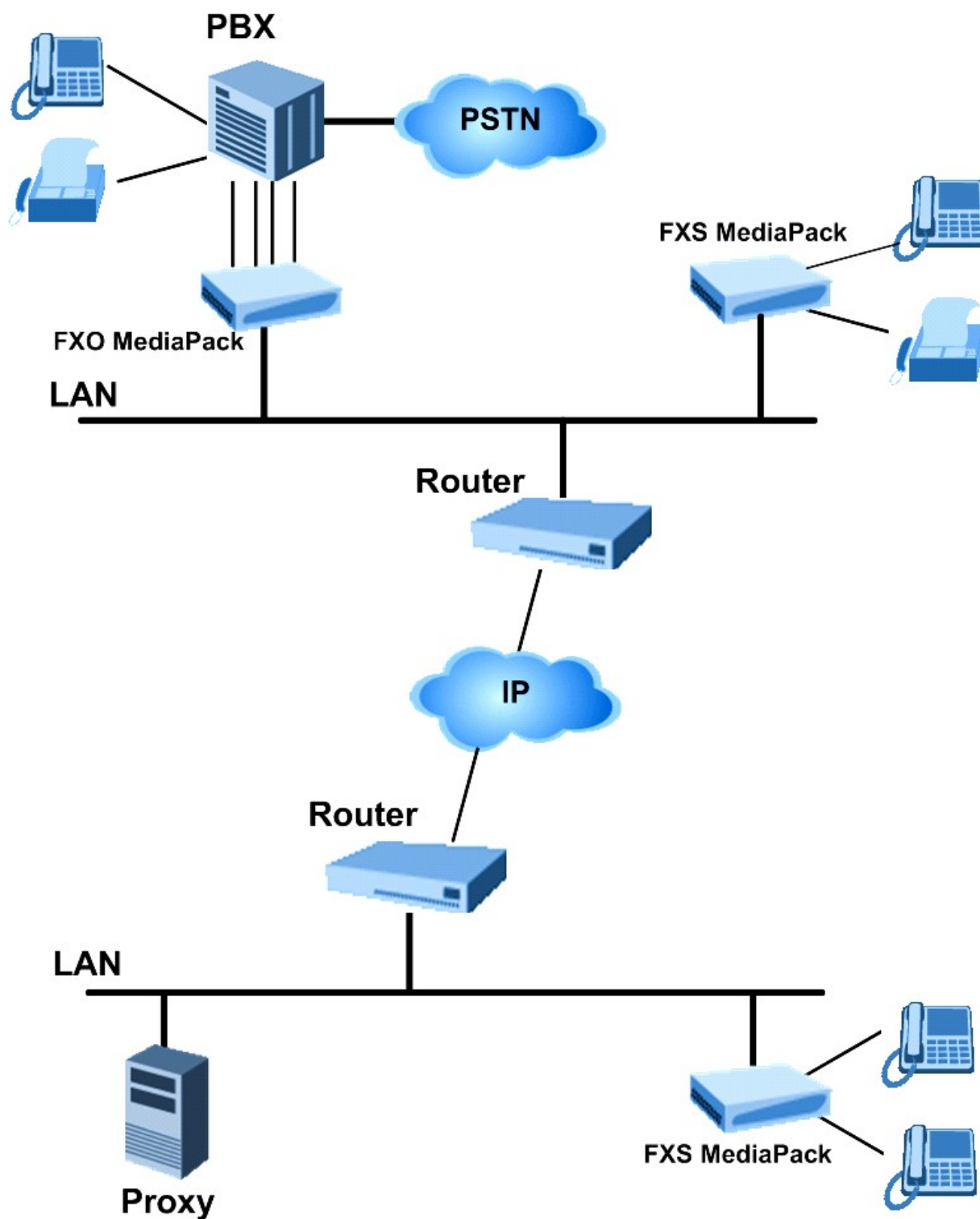
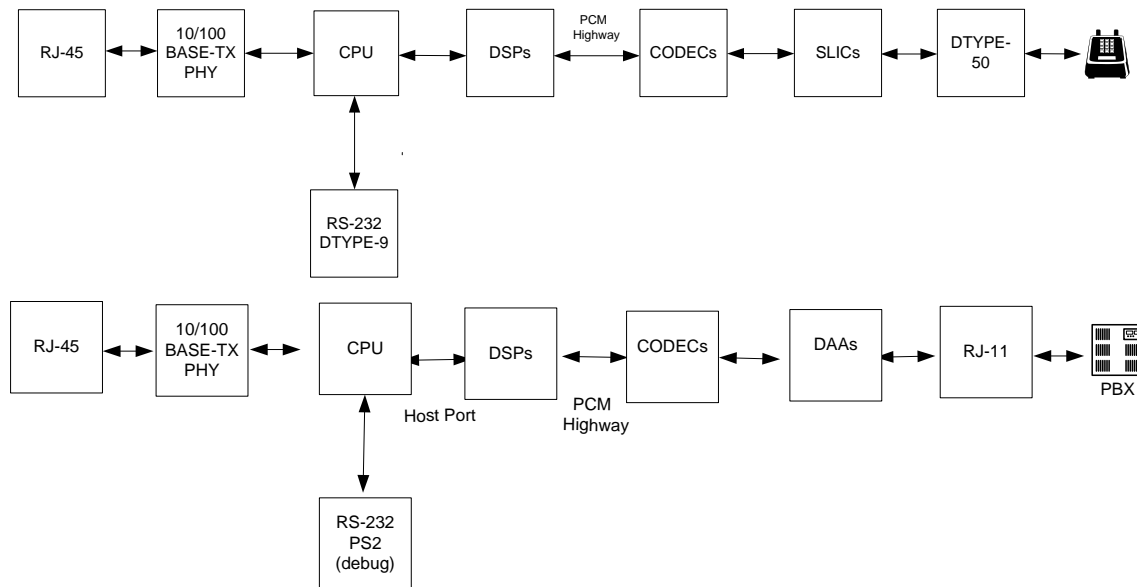
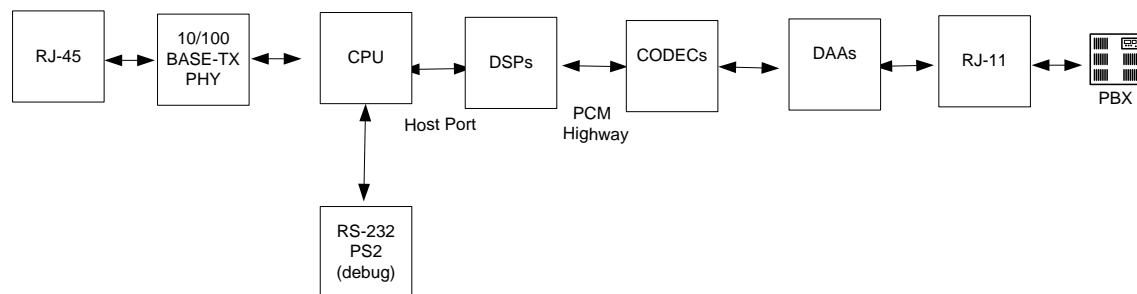
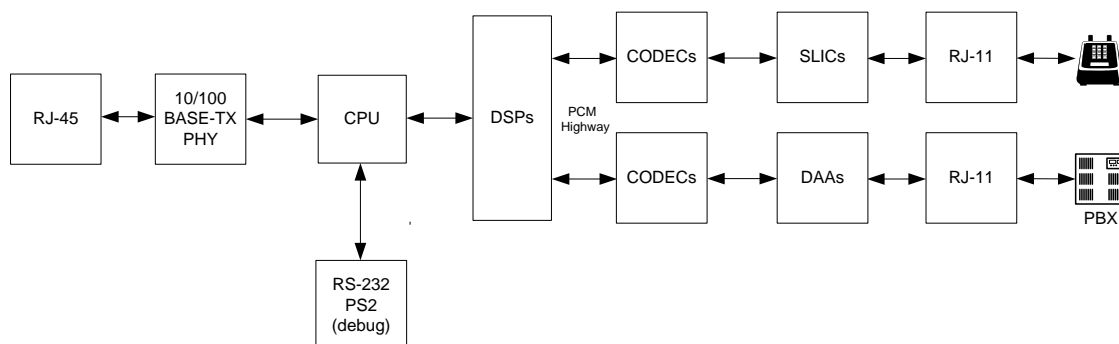


Figure 2: MP-124D Block Diagram

Figure 3: MP-11x FXS Block Diagram

Figure 4: MP-11x FXO+FXS Functional Block Diagram


2 Software Package

After installing and powering up the device, you are ready to install the utilities that are included in the software package. This software package must be installed on the host PC/machine to be used to manage the device. The software package can be downloaded by registered users from the AudioCodes Web site at www.audiocodes.com/support.

To become a registered user, follow the instructions on the Web site.

➤ **To get started:**

1. To install the software package refer to Installing the Software Package on page 13.
2. Check the software package contents (refer to 'Software Directory Contents & Structure' on page 14.)
3. Perform 'Getting Started' on page 15.

2.1 Installing the Software Package

The software package is available on the AudioCodes' FTP Web site.

- Customers using a Windows™ operating system may choose to install the package via the installation wizard, or choose to unzip the software package from the supplied zip file (refer to "Installing/Unzipping When Using a Windows™ Operating System" below).

2.1.1 Installing/Unzipping When Using a Windows™ Operating System

➤ **To install the package:**

1. Double-click on the setup.exe executable file.
2. Follow on-page instructions.

➤ **To unzip when using a Windows™ Operating System:**

1. Using a tool like WinZip™, open the zip file.
2. Click the 'Extract' button; the 'Extract' page opens.
3. Navigate to the directory that you require to be the root directory for the installation and click the 'Extract' button; the files are extracted to the location you specified.

2.1.2 Unzipping When Using a Linux™/Solaris™ Operating System

➤ **To unzip when using a Linux™/Solaris™ Operating System:**

1. To open the tar.Z archive, un-compress the tar.Z file.
2. Enter the command: `tar -xvf xxxxxx.tar`.

2.2 Software Directory Contents & Structure

Software Package Contents

Contents	Directory	Description
Auxiliary Files	.\Auxiliary_Files\MIB_Files	Various MIB files, e.g., SNMP MIB files: ACL.my, RTP.my, ds1.my, MIB_2.my, V2_MIB.my.
	.\Auxiliary_Files\Sample_Call_Progress_Files	Contains examples of Call Progress Tones configuration files.
	.\Auxiliary_Files\Sample_CAS_Protocol_Files	Contains examples of CAS protocol files.
	.\Auxiliary_Files\Sample_Ini_Files	Contains examples of configuration (ini) files. Users can utilize these sample files as a baseline for creating customized configuration files.
Firmware	.\Firmware	Contains cmp files, loaded to the device when changing the version of the software. When the device is supplied to customers, it is already configured with pre-installed firmware.
Utilities	AudioCodes' utilities provide you with user-friendly interfaces that enhance device usability and smooth your transition to the new VoIP infrastructure.	
	.\Utilities\DConvert	Contains the TrunkPack Downloadable Construction Utility. Use the utility to build Call Progress Tones, Voice Prompts, and CAS files.
	.\Utilities\PSTN_TRACE_UTILITY	This utility is designed to convert Wireshark log files containing the PSTN trace to text format.
	.\Utilities\WiresharkPlugins	Contains the plugins for the Wireshark network diagnostic tool. The plugin registers itself to handle a dissection of AudioCodes' proprietary protocol.
Documentation	All relevant product documentation	



Note: All the demo programs described above are for reference only. Flawless operation and stability of these applications cannot be guaranteed.

3 Getting Started

The MediaPack is supplied with application software already resident in its flash memory (with factory default parameters). The MediaPack is also supplied with a Web interface.

For detailed information on how to fully configure the gateway refer to Device Initialization & Configuration Files and the Web interface chapter below.

3.1 Assigning the MediaPack IP Address

➤ To assign an IP address to the MediaPack use one of the following methods:

- HTTP using a Web browser (see 'Assigning an IP Address Using HTTP' on page 16).
- BootP (see 'Assigning an IP Address Using BootP' on page 17).
- DHCP (see 'Using BootP/DHCP' on page 21).
- Serial communication software (e.g., HyperTerminal™) connected to the MediaPack via the RS-232 port.

You can use the Reset button to restore the MediaPack networking parameters to their factory default values (refer to Restoring Networking Parameters to their Initial State on page 18).

The default device IP Addresses are shown below.

MediaPack Default IP Parameters

FXS/FXO Interfaces	Default IP Address
FXS	10.1.10.10
FXO	10.1.10.11
FXS & FXO	10.1.10.10
Default Subnet Mask	255.255.0.0
Default Gateway IP Address	0.0.0.0

3.2 Assigning an IP Address Using HTTP

➤ **To assign an IP address using HTTP:**

1. Connect your PC to the device. Either connect the network interface on your PC to a port on a network hub / switch (using an RJ-45 Ethernet cable), or use an Ethernet cross-over cable to directly connect the network interface on your PC to the RJ-45 jack on the device.
2. Change your PC's IP address and subnet mask to correspond with the device factory default IP address and subnet mask, shown in the table above. For details on changing the IP address and subnet mask of your PC, refer to Windows™ Online Help (Start>Help and Support).
3. Access the Web interface (refer to the Web interface chapter in the Product Reference Manual).
4. Click Reset and click OK in the prompt. The device applies the changes and restarts. This takes approximately 1 minute to complete. When the device has finished restarting, the Ready and LAN LEDs on the front view are lit green.



Tip: Record and retain the IP address and subnet mask you assign the device. Do the same when defining a new username or password. If the Web interface is unavailable (for example, if you've lost your username and password), use a BootP/TFTP configuration utility to access the device, "reflash" the load and reset the password.

5. Disconnect your PC from the device or from the hub / switch (depending on the connection method you used in step 1 above).
6. Reconnect the device and your PC (if necessary) to the LAN.
7. Restore your PC's IP address & subnet mask to what they originally were. If necessary, restart your PC and re-access the device via the Web interface with its new assigned IP address.

3.3 Assigning an IP Address Using BootP

**Notes:**

- The BootP procedure should be performed using any standard compatible BootP server.
- For Mediant 3000 HA, in order to get the BootP reset request from the blade, perform a double reset on the system, as described in Private IP Address and System (Global) IP Address.



Tip: You can also use BootP to load the auxiliary files to the device (refer to 'Using BootP/DHCP' on page 29).

➤ **To assign an IP address using BootP:**

1. Obtain and install a BootP server application on your PC.
2. Add the client configuration for the device.
3. Reset the gateway physically causing it to use BootP. The device changes its network parameters to the values provided by BootP.

3.4 Restoring Networking Parameters to their Default Values

You can use the Reset button to restore the MediaPack networking parameters to their factory default values (described in Default Device IP Addresses) and to reset the username and password.

Note that this process also restores the MediaPack parameters to their factory settings, therefore you must load your previously backed-up ini file, or the default ini file (received with the software kit) to set them to their correct values.

➤ **To restore parameters to their initial state, take these 6 steps:**

1. Back up the ini file. Refer to Backup Copies of ini and Auxiliary Files on page 35.
2. Disconnect the MediaPack from the power and network cables.
3. Reconnect the power cable; the gateway is powered up. After approximately 45 seconds, the Ready LED turns to green and the Control LED blinks for about 3 seconds.
4. While the Control LED is blinking, use a paper clip to press shortly on the reset button (located next to the AudioCodes logo on the front view). The gateway resets a second time and is restored with factory default parameters (username: Admin, password: Admin - both case-sensitive).
5. Reconnect the network cable.
6. Load your previously backed-up ini file, or the default ini file (received with the software kit). To load the ini file via the Web interface, refer to 'Software Upgrade Wizard'.

4 Device Initialization & Configuration Files

This section describes the Initialization Procedures and Configuration Options for the device. It includes:

- Startup Process (see below)
- Configuration Parameters and Files (refer to Configuration Parameters and Files on page 25)
- BootP/DHCP (see Using BootP/DHCP on page 21)

4.1 Boot Firmware & Operational Firmware

The MediaPack runs two distinct software programs: Boot firmware and operational firmware.

- Boot firmware - Boot firmware (also known as flash software) resides in the MediaPack's non-volatile memory. When the MediaPack is reset, Boot software is initialized and the operational software is loaded into the SDRAM from a TFTP server or integral non-volatile memory. Boot software is also responsible for obtaining the MediaPack's IP parameters and ini file name (used to obtain the MediaPack's configuration parameters) via integral BootP or DHCP clients. The Boot firmware version can be viewed on the Embedded Web Server's GUI ('Embedded Web Server' on page 43). The last step the Boot firmware performs is to jump to invoke in the operational software.
- cmp Operational firmware file - The device is supplied with a cmp file pre-installed on its flash memory. Therefore, this file is not included on the supplied CD. However, if you are an AudioCodes registered customer, you can obtain the latest cmp version files (as well as documentation and other software listed in the table above) from AudioCodes Web site at www.audiocodes.com/support (customer registration is performed online at this Web site). If you are not a direct customer of AudioCodes, please contact the AudioCodes' Distributor and Reseller from whom this product was purchased.



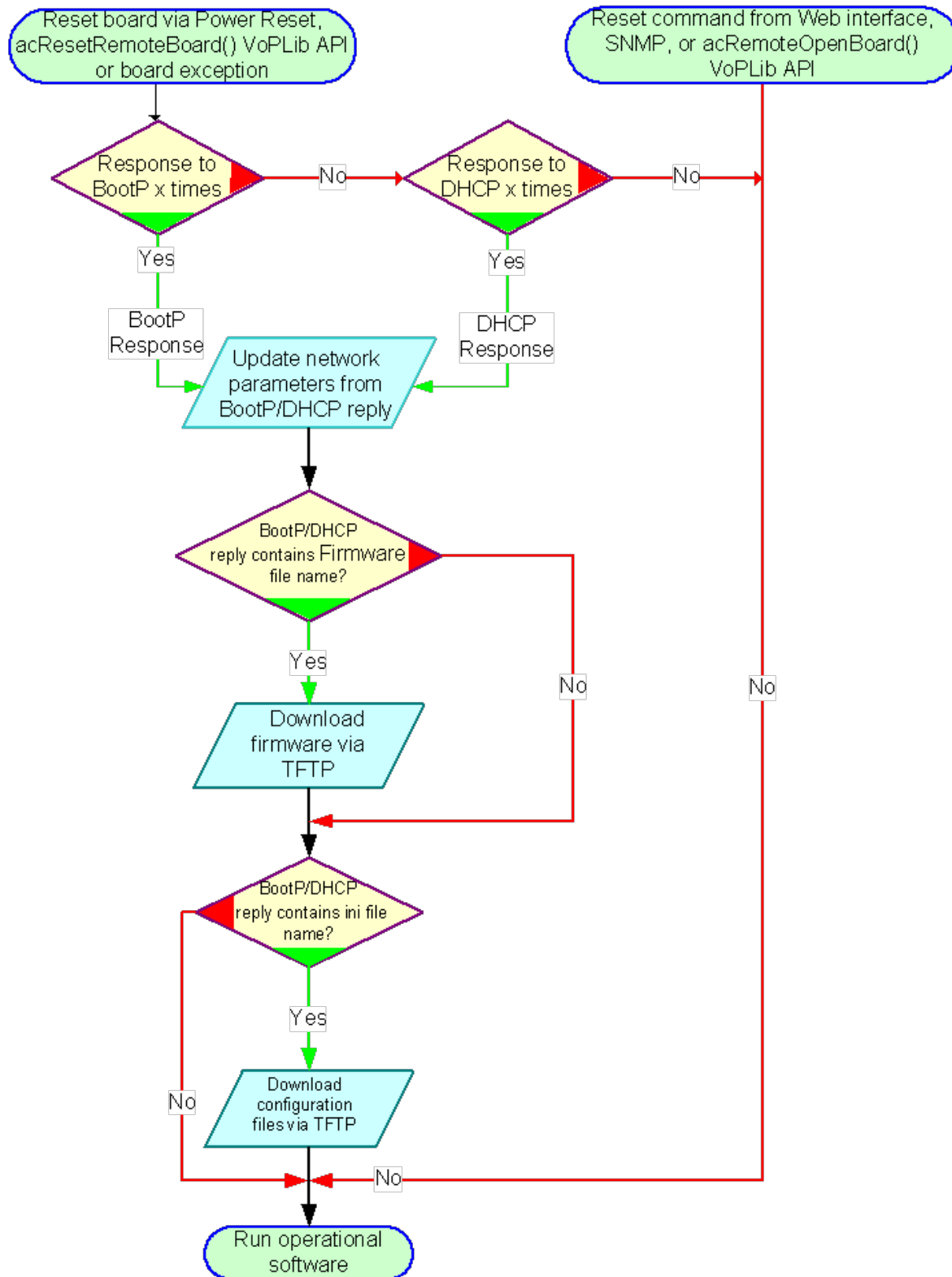
Note: The ini, MIB and Utility files are shipped with the device in CD format

4.2 MediaPack Startup

The MediaPack's startup process begins when the MediaPack is reset. The startup process ends when the operational firmware is running. The startup process includes how the MediaPack obtains its IP parameters, firmware and configuration files.

The MediaPack is reset when one of the following scenarios occurs:

1. The MediaPack is manually reset.
2. `acOpenRemoteBoard()` is called with `RemoteOpenBoardOperationMode` set to Full Configuration Mode (valid for VoPLib API users only).
3. There is a device irregularity.
4. Users perform a reset in the Embedded Web Server GUI or SNMP manager.
5. The flowchart in the figure below illustrates the process that occurs in these scenarios.

Figure 5: MediaPack Startup Process Diagram


4.3 Using BootP/DHCP

**Notes:**

- This sub-section is not applicable to Mediant 3000 HA.
- The BootP/DHCP server should be defined with an ini file name when you need to modify configuration parameters or when you're working with a large Voice Prompt file that is not stored in non-volatile memory and must be loaded after every reset.
- The default time duration between BootP/DHCP requests is set to 1 second. This can be changed by the BootPDelay ini file parameter. Also, the default number of requests is 3 and can be changed by the BootPRetries ini file parameter. Both parameters can also be set using the Command Line Switches in the BootP reply packet.
- The ini file configuration parameters are stored in non-volatile memory after the file is loaded. When a parameter is missing from the ini file, a default value is assigned to this parameter and stored in non-volatile memory (thereby overriding any previous value set for that parameter). Refer to Using BootP/DHCP below.

The device uses the Bootstrap Protocol (BootP) and the Dynamic Host Configuration Protocol (DHCP) to obtain its networking parameters and configuration automatically after it is reset. BootP and DHCP are also used to provide the IP address of a TFTP server on the network, and files (cmp and ini) to be loaded into memory.

Both DHCP and BootP are network protocols that enable a device to discover its assigned IP address; DHCP differs from BootP in that it provides a time-limited "lease" to the assigned address. Both protocols have been extended to enable the configuration of additional parameters specific to the device.

While BootP is always available, DHCP has to be specifically enabled in the device configuration, before it can be used.

A BootP/DHCP request is issued after a power reset or after a device exception.



Note: BootP is normally used to initially configure the device. Thereafter, BootP is no longer required as all parameters can be stored in the gateway's non-volatile memory and used when BootP is inaccessible. For example, BootP can be used again to change the private (local) IP address of the device.

4.3.1 BootP/DHCP Server Parameters

BootP/DHCP can be used to provision the following parameters (included in the BootP/DHCP reply. Note that some parameters are optional):

- IP address, subnet mask - These mandatory parameters are sent to the device every time a BootP/DHCP process occurs. Note that in High Availability (HA) mode, this IP address is only private (local) and is not the HA System (global) IP address that must be configured separately through the Interface Table.
- Default gateway IP address - An optional parameter that is sent to the device only if configured in the BootP/DHCP server.

- TFTP server IP address - An optional parameter that contains the address of the TFTP server from which the firmware (cmp) and ini files are loaded.
- DNS server IP address (primary and secondary) - Optional parameters that contain the IP addresses of the primary and secondary DNS servers. These parameters are available only in DHCP and from Boot version 1.92.
- Syslog server IP address - An optional parameter that is sent to the device only if configured in the BootP/DHCP server. This parameter is available only in DHCP.
- Firmware file name – An optional parameter that contains the name of the CMP firmware file to be loaded to the gateway via TFTP.
- ini file name - An optional parameter that contains the name of the ini file to be loaded to the gateway via TFTP. The ini file name shall be separated from the CMP file name using a semicolon.



Note: After programming a new cmp software image file, all configuration parameters and tables are erased. Re-program them by downloading the ini file.

- Configuration (ini) file name - The ini file is a proprietary configuration file with an ini extension, containing configuration parameters and tables. For more information on this file, refer to 'Configuration Parameters and Files' on page 25. When the device detects that this optional parameter field is defined in BootP, it initiates a TFTP process to load the file into the device. The new configuration contained in the ini file can be stored in the device's integral non-volatile memory. Whenever the device is reset and no BootP reply is sent to the blade or the ini file name is missing in the BootP reply, the device uses the previously stored ini file.

4.3.1.1 Command Line Switches

In the BootP/TFTP Server configuration, you can add command line switches in the Boot File field. Command line switches are used for various tasks, such as to determine if the firmware should be burned on the non-volatile memory or not. The table below describes the different command line switches.

➤ To use a command line switch:

1. In the Boot File field, leave the filename defined in the field as it is (e.g., ramxxx.cmp).
2. After "cmp", leave a space and type in the switch you require (refer to the table below).

Example: ramxxx.cmp -fb to burn flash memory

ramxxx.cmp -fb -em 4 to burn flash memory and for Ethernet Mode 4 (auto-negotiate)

The table below lists and describes the available switches.

Command Line Switch Descriptions

Switch	Description
-fb	Burn ram.cmp in non-volatile memory. Only the cmp file (the compressed firmware file) can be burned to the device's non-volatile memory.
-em#	Use this switch to set Ethernet mode. 0 = 10 Base-T half-duplex 1 = 10 Base-T full-duplex 2 = 100 Base-TX half-duplex 3 = 100 Base-TX full-duplex 4 = auto-negotiate (default) Auto-negotiate falls back to half-duplex mode when the opposite port is not in auto-negotiate but the speed (10 Base-T or 100 Base-TX) in this mode is always configured correctly.
-br	BootP retries: 1 = 1 BootP retry, 1 sec 2 = 2 BootP retries, 3 sec 3 = 3 BootP retries, 6 sec 4 = 10 BootP retries, 30 sec 5 = 20 BootP retries, 60 sec 6 = 40 BootP retries, 120 sec 7 = 100 BootP retries, 300 sec 15 = BootP retries indefinitely Use this switch to set the number of BootP retries that the device sends during start-up. The device stops issuing BootP requests when either a BootP reply is received or Number Of Retries is reached. This switch takes effect only from the next device reset.
-bd	BootP delays. 1 = 1 sec (default), 2 = 10 sec, 3 = 30 sec, 4 = 60 sec, 5 = 120 sec. This sets the delay from the device's reset until the first BootP request is issued by the device. The switch only takes effect from the next reset of the device.
-bs	Selective BootP: The device ignores BootP replies where option 43 does not contain the name "AUDC". Refer to Selective BootP on page 24.
-be	Use -be 1 for the device to send client information back to the DHCP server. See the "Vendor Specific Information" section below for more information.

4.3.2 Host Name Support

If DHCP is selected, the device requests a device-specific Host Name on the DNS server by defining the Host Name field of the DHCP request. The host name is set to ACL_nnnnnnn, where nnnnnnn is the serial number of the device (the serial number is equal to the last 6 digits of the MAC address converted to decimal representation). The DHCP server usually registers this Host Name on the DNS server. On networks which support this setting, this feature allows users to configure the device via the web browser by providing the following URL: http://ACL_nnnnnnn (instead of using the device's IP address).

4.3.3 Selective BootP

The Selective BootP mechanism, allows the integral BootP client to filter out unsolicited BootP replies. This can be beneficial for environments where more than one BootP server is available and only one BootP server is used to configure AudioCodes devices.

- To activate this feature, add the command line switch -bs 1 to the Firmware File Name field. When activated, the device accepts only BootP replies containing the text AUDC in the Vendor Specific Information field (option 43).
- To de-activate, use -bs 0.

4.3.4 Microsoft™ DHCP/BootP Server

The device can be configured with any BootP server, including the Microsoft™ Windows™ DHCP server, to provide the device with an IP address and other initial parameter configurations.

To configure the Microsoft™ Windows™ DHCP Server to configure an IP address to BootP clients, add a reservation for each BootP client.

For information on how to add a reservation, view the "Managing Client Reservations Help" topic in the DHCP console.

The reservation builds an association between MAC address (12 digits), provided in the accompanying device documentation) and the IP address. Windows™ Server provides the IP address based on the device MAC address in the BootP request frame.

To configure the Microsoft™ Windows™ DHCP server to provide Boot File information to BootP clients, edit the BootP Table in the DHCP console. The BootP Table should be enabled from the Action > Properties dialog, select the option "Show the BootP Table Folder" and press OK. For information on editing the BootP Table, view the "Manage BOOTP and remote access clients" Help topic in the DHCP console.

The following parameters must be specified:

- Local IP address - The device's IP address
- Subnet mask
- Gateway IP address - Default Gateway IP address
- BootP File name - Optional (refer to the following Note)



Note: The BootP File field should normally not be used. The field is only used for software upgrade (refer to Upgrading Device Software on page 35).

4.4 Configuration Parameters and Files

The device's configuration is stored in two file groups.

- The Initialization file - an initialization (ini) text file containing configuration parameters of the device.
- The Auxiliary files - dat files containing the raw data used for various tasks such as Call Progress Tones, Voice Prompts, logo image, etc.

These files contain factory-pre-configured parameter defaults when supplied with the device and are stored in the device's non-volatile memory. The device is started up initially with this default configuration. Subsequently, these files can be modified and reloaded using either of the following methods:

- BootP/TFTP during the startup process (refer to 'Using BootP/DHCP' on page 21).
- Web Interface (refer to Configuration Using the Web Interface on page 43).
- Automatic Update facility (refer to Automatic Update Facility on page 31).

The modified auxiliary files are burned into the non-volatile memory so that the modified configuration is utilized with subsequent resets. The configuration file is always stored on the non-volatile memory. There is no need to repeatedly reload the modified files after reset.



Notes:

- Users who configure the device with the Web interface do not require ini files to be downloaded and have no need to utilize a TFTP server.
- SNMP users configure the device via SNMP. Therefore a very small ini file is required which contains the IP address for the SNMP traps.

4.4.1 Initialization (ini) File

The ini file name must not include hyphens or spaces. Use underscores instead.

The ini file can contain a number of parameters. The ini file structure supports the following parameter value constructs:

- Parameter = Value (refer to 'Parameter = Value Constructs' on page 163). The lists of parameters are provided in the ini File Parameters chapter of the Product Reference Manual.
- Tables of Parameter Value (refer to 'Table of Parameter Value Constructs' on page 27).

The example below shows a sample of the general structure of the ini file for both the Parameter = Value and Tables of Parameter Value Constructs.

```
[Sub Section Name]
Parameter_Name = Parameter_Value
Parameter_Name = Parameter_Value
.
..

; REMARK

[Sub Section Name]
```

```
...

; Tables Format Rules:
[Table_Name]
; Fields declaration
Format Index_Name_1 ... Index_Name_N = Param_Name_1 ...
Param_Name_M
; Table's Lines (repeat for each line)
Table_Name Index_1_val ... Index_N_val = Param_Val_1 ...
Param_Val_M
[\Table_Name]
```

4.4.1.1 Parameter Value Structure

The following are the rules in the ini File structure for individual ini file parameters (Parameter = Value):

- Lines beginning with a semi-colon ';' (as the first character) are ignored.
- A carriage-return/line-feed must be the final character of each line.
- The number of spaces before and after "=" is not relevant.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter value field can cause unexpected errors (because parameters may be set to the incorrect values).
- Sub-section names are optional.
- String parameters, representing file names, for example, CallProgressTonesFileName, must be placed between two inverted commas ('...').
- The parameter name is NOT case sensitive; the parameter value is usually case sensitive.
- Numeric parameter values should be entered only in decimal format.
- The ini file should be ended with one or more empty lines.

The example below shows a sample ini file for the MediaPack.

```
[MGCP]
EndpointName = 'ACgw'
CallAgentIP = 192.1.10.3
CallAgentPort = 2427
BaseUDPPort = 4000

FlashHookPeriod = 700

[Channel Params]
DJBufferMinDelay = 75
RTPRedundancyDepth = 1
```

```
[Files]
CallProgressTonesFilename = 'CPUSA.dat'
VoicePromptsFilename = 'tpdemo_723.dat'
FXSLOOPCHARACTERISTICSFILENAME = 'coeff.dat'
```



Note: Before loading an ini file to the device, make sure that the extension of the ini file saved on your PC is correct: Verify that the checkbox Hide extension for known file types (My Computer>Tools>Folder Options>View) is unchecked. Then, verify that the ini file name extension is xxx.ini and NOT erroneously xxx.ini.ini or xxx~.ini.

The lists of individual ini file parameters are provided in ini File Parameters.

4.4.1.2 Tables of Parameter Value Structure

Tables group the related parameters of a given entity. Tables are composed of rows and columns. The columns represent parameters types, while each row represents an entity. The parameters in each row are called the line attributes. Rows in tables may represent (for example) a trunk, SS7 Link, list of timers for a given application, etc.

Examples of the structure of the tables are provided below. For a list of supported tables please refer to the ini File Table Parameters section in the Product Reference Manual.

```
[ SS7_SIG_INT_ID_TABLE ]
FORMAT SS7_SIG_IF_ID_INDEX = SS7_SIG_IF_ID_VALUE,
SS7_SIG_IF_ID_NAME, SS7_SIG_IF_ID_OWNER_GROUP,
SS7_SIG_IF_ID_LAYER, SS7_SIG_IF_ID_NAI, SS7_SIG_M3UA_SPC;
SS7_SIG_INT_ID_TABLE 1 = 101, AMSTERDAM1, 3, 3, 1, 4;
SS7_SIG_INT_ID_TABLE 5 = 100, BELFAST12, 3, 3, 0, 11;

[ \SS7_SIG_INT_ID_TABLE ]
```

The table below is shown in document format for description purposes:

Table Structure Example

IF ID Index	IF ID Value	SS7_SIG_IF_ID _NAME	SS7_SIG_IF_ID OWNER_GROUP	SS7_SIG_IF_ID _LAYER	SS7_SIG_IF_ ID_NAI	SS7_SIG_ M3UA_SPC
1	101	AMSTERDAM1	3	3	1	4
5	100	BELFAST12	3	3	0	11

4.4.1.2.1 Table Structure Rules

Tables are composed of four elements:

- **Table-Title** - The Table's string name in square brackets. In the example above, the Table Title is:
[SS7_SIG_INT_ID_TABLE].
- **Format Line** - This line specifies the table's fields by their string names. In the example above, the format line is: `FORMAT SS7_SIG_IF_ID_INDEX = SS7_SIG_IF_ID_VALUE, SS7_SIG_IF_ID_NAME, SS7_SIG_IF_ID_OWNER_GROUP, SS7_SIG_IF_ID_LAYER, SS7_SIG_IF_ID_NAI, SS7_SIG_M3UA_SPC`
 - The first word **MUST** be "FORMAT" (in capital letters), followed by indices field names, and after '=' sign, all data fields names should be listed.
 - Items must be separated by ',' sign.
 - The Format Line must end with ';' sign.
- **Data Line(s)** - The actual values for parameters are specified in each Data line. The values are interpreted according to the format line. The first word must be the table's string name.
 - Items must be separated by a comma (',' sign).
 - A Data line must end with a semicolon (';' sign).
 - Indices (in both the Format line and the Data lines) must all appear in order, as determined by the table's specific documentation. The Index field must NOT be omitted. Each row in a table must be unique. For this reason, each table defines one or more Index fields. The combination of the Index fields determines the 'line-tag'. Each line-tag may appear only once. In the example provided in the table above, Table Structure Example', there is only one index field. This is the simplest way to mark rows.
 - Data fields in the Format line may use a sub-set of all of the configurable fields in a table only. In this case, all other fields are assigned with the pre-defined default value for each configured line.
 - The order of the Data fields in the Format line is not significant (unlike the Index-fields). Field values in Data lines are interpreted according to the order specified in the Format line.
 - Specifying '\$\$' in the Data line causes the pre-defined default value assigned to the field for the given line.
 - The order of Data lines is insignificant.
 - Data lines must match the Format line, i.e. must contain exactly the same number of Indices and Data fields and should be in exactly the same order.
 - A line in a table is identified by its table-name and its indices. Each such line may appear only once in the ini file.
- **End-of-Table-Mark**: Marks the end of a table. Same as Table title, but the string name is preceded by '\'.

Below is an example of the table structure in an ini file.

```
; Table: Items Table.
; Fields: Item_Name, Item_Serial_Number, Item_Color, Item_weight.
; NOTE: Item_Color is not specified. It will be given default
value.
[Items_Table]
; Fields declaration
Format Item_Index = Item_Name, Item_Serial_Number, Item_weight;
```



```
Items_Table 0 = Computer, 678678, 6;  
Items_Table 6 = Computer-page, 127979, 9;  
Items_Table 2 = Computer-pad, 111111, $$;  
[\Items_Table]
```

4.4.1.2.2 Secret Tables

A table is defined as a secret table if it contains at least one secret data field or if it depends on such a table. A secret data field is a field that must not be revealed to the user. An example of a secret field can be found in an IPSec application. The IPSec tables are defined as secret tables because the IKE table contains a pre-shared key field, which must not be revealed. The SPD table depends on the IKE table. Therefore, the SPD table is defined as a secret table.

There are two major differences between tables and secret tables:

- The secret field itself cannot be viewed via SNMP, Web Server or any other tool.

ini File behavior: These tables are never uploaded in the ini File (e.g., 'Get INI-File from Web'). Instead, there is a commented title that states that the secret table is present at the blade, and is not to be revealed.

Secret tables are always kept in the blade's non-volatile memory, and may be over-written by new tables that should be provided in a new ini File. If a secret table appears in an ini File, it replaces the current table regardless of its content. The way to delete a secret table from a blade is, for example, to provide an empty table of that type (with no data lines) as part of a new ini File. The empty table replaces the previous table in the blade.

4.4.1.2.3 Tables in the Uploaded ini File

Tables are grouped according to the applications they configure.

When uploading the ini file, the policy is to include only tables that belong to applications, which have been configured. (Dynamic tables of other applications are empty, but static tables are not.) The trigger for uploading tables is further documented in the applications' specific sections.

4.4.1.2.4 Secret Tables

A table is defined as a secret table if it contains at least one secret data field or if it depends on such a table. A secret data field is a field that must not be revealed to the user. An example of a secret field can be found in an IPSec application. The IPSec tables are defined as secret tables because the IKE table contains a pre-shared key field, which must not be revealed. The SPD table depends on the IKE table. Therefore, the SPD table is defined as a secret table.

There are two major differences between tables and secret tables:

- The secret field itself cannot be viewed via SNMP, Web Server or any other tool.
- ini File behavior: These tables are never uploaded in the ini File (e.g., 'Get INI-File from Web'). Instead, there is a commented title that states that the secret table is present at the blade, and is not to be revealed.

Secret tables are always kept in the blade's non-volatile memory, and may be over-written by new tables that should be provided in a new ini File. If a secret table appears in an ini File, it replaces the current table regardless of its content. The way to delete a secret table from a blade is, for example, to provide an empty table of that type (with no data lines) as part of a new ini File. The empty table replaces the previous table in the blade.

4.4.1.3 Binary Configuration File Download

The ini file contains sensitive information required for appropriate functioning of the device. The ini file is uploaded to the device or downloaded from the gateway using TFTP or HTTP protocols. These protocols are unsecured (and thus vulnerable to a potential hacker). Conversely, if the ini file is encoded, the ini file would be significantly less vulnerable to outside harm.

4.4.1.3.1 Encoding Mechanism

The ini file to be loaded and retrieved is available with or without encoding. When an encoded ini file is downloaded to the device, it is retrieved as encoded from the device. When a decoded file is downloaded to the device, it is retrieved as decoded from the device.

In order to create an encoded ini file, the user must first create an ini file and then apply the DConvert utility to it in order to encode it.

In order to decode an encoded ini file retrieved from the device, the user must retrieve an encoded ini file from the device using the Web server (refer to "Downloading Auxiliary Files" below) and then use the DConvert utility in order to decode it.

(Refer to the Utilities chapter in the Product Reference Manual for detailed instructions on ini file encoding and decoding.)

Downloading the ini file with or without encoding may be performed by utilizing either TFTP or HTTP.

4.4.2 Auxiliary Files

The auxiliary files are *.dat files containing raw data used for a certain task such as Call Progress Tones, Voice Prompts, logo image, etc. The *.dat files are created using the DConvert utility (refer to the Utilities chapter in the Product Reference Manual), which converts auxiliary source files into dat files. Some sample auxiliary source files are available in the software package under: .\Auxiliary_Files*.dat files. These *.dat files are downloaded to the device using TFTP (see below) or HTTP via the Software Upgrade Wizard (refer to Upgrading Device Software on page 35.) This section describes the various types of auxiliary files.



Note: The auxiliary source files use the same ini file extension type as the ini configuration file, however, the functionality is different. Whenever the term, "ini file" is used, it refers to the configuration file and NOT to the auxiliary files.

4.4.2.1 Downloading Auxiliary Files via TFTP During the Blade Startup

Each auxiliary file has a corresponding ini file parameter in the form of [AuxiliaryFileType]FileName. This parameter takes the name of the auxiliary file to be downloaded to the device. If the ini file does not contain a parameter for a specific auxiliary file type, the device uses the last auxiliary file that was stored on the non-volatile memory.

The following list contains the ini file parameters for the different types of auxiliary files that can be downloaded to the device:

- **CoderTblFileName** – The name (and path) of the file containing the coder table. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the device.

- **VoicePromptsFileName** - The name (and path) of the file containing the voice prompts. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the MediaPack. The Voice Prompt buffer size in the blade is 1 Mbyte.

The Voice Prompt buffer size is also controlled by the software upgrade key. For more information contact an AudioCodes representative.

- **CallProgressTonesFilename** - The name (and path) of the file containing the Call Progress and User-Defined Tones definition.
- **PrerecordedTonesFileName** - The name (and path) of the file containing the Prerecorded Tones. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the device.
- **DialPlanFileName** - The name (and path) of the file containing dial-plan configuration for CAS protocols. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the device.
- **FXSLoopCharacteristicsFileName** - The name (and path) of the file providing the FXS line characteristic parameters.
- **SaveConfiguration** - (default = 1 = enabled) This parameter replaces the following parameters: **BlastCallProgressSetupFile**, **BlastVoicePromptsFile**. When enabled, all configuration and downloadable files are stored in non-volatile memory.

4.4.2.2 Automatic Update Facility

The device is capable of automatically downloading updates to the ini file, auxiliary files and firmware image. Any standard Web server, FTP server or NFS server may be used to host these files.

The Automatic Update processing is performed:

- Upon device start-up (after the device is operational)
- At a configurable time of day, e.g., 18:00 (disabled by default)
- At fixed intervals, e.g., every 60 minutes (disabled by default)
- If Secure Startup is enabled (refer to Secure Startup), upon start-up but before the device is operational.

The Automatic Update process is entirely controlled by configuration parameters in the ini file. During the Automatic Update process, the device contacts the external server and requests the latest version of a given set of URLs. An additional benefit of using HTTP (Web) servers is that configuration ini files would be downloaded only if they were modified since the last update.

The following is an example of an ini file activating the Automatic Update Facility.

```
# DNS is required for specifying domain names in URLs
DnsPriServerIP = 10.1.1.11

# Load extra configuration ini file using HTTP
INIFILEURL = 'http://webserver.corp.com/AudioCodes/inifile.ini'
# Load call progress tones using HTTPS
CPTFILEURL = 'https://10.31.2.17/usa_tones.dat'
# Load voice prompts, using user "root" and password "wheel"
VPFILEURL = 'ftps://root:wheel@ftpserver.corp.com/vp.dat'

# Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
```

Notes on Configuration URLs:

- Additional URLs may be specified, as described in the System ini File Parameters in the Product Reference Manual.
- Updates to non-ini files are performed only once. To update a previously-loaded binary file, you must update the ini file containing the URL for the file.
- To provide differential configuration for each of the devices in a network, add the string "<MAC>" to the URL. This mnemonic is replaced with the hardware (MAC) address of the device.
- To update the firmware image using the Automatic Update facility, use the CMPFILEURL parameter to point to the image file. As a precaution (in order to protect the device from an accidental update), you must also set AUTOUPDATECMPFILE to 1.
- URLs may be as long as 255 characters.



Note: For the following parameters, the URLs are reset to their default value on successful Autoupdate. Subsequent Autoupdates without re-initializing the parameters are not supported.

- CptFileUrl
- PrtFileUrl
- FXSCoeffFileUrl
- FXOCoeffFileUrl
- CasFileUrl
- DialPlanFileUrl
- TLSPkeyFileUrl
- TLSCertFileUrl
- TLSRootFileUrl
- WebLogoFileUrl
- V5PortConfigurationFileURL

➤ To utilize Automatic Updates for deploying the device with minimum manual configuration:

1. Set up a Web server (in this example it is <http://www.corp.com/>) where all the configuration files are to be stored.
2. On each device, pre-configure the following setting: (DHCP/DNS are assumed)

```
INIFILEURL = 'http://www.corp.com/master_configuration.ini'
```

3. Create a file named `master_configuration.ini`, with the following text:

```
# Common configuration for all devices
# -----
CptFileURL = 'http://www.corp.com/call_progress.dat'
# Check for updates every 60 minutes
AutoUpdateFrequency = 60

# Additional configuration per device
# -----
# Each device will load a file named after its MAC address,
# e.g. config_00908F033512.ini
IniFileTemplateURL = 'http://www.corp.com/config_<MAC>.ini'

# Reset the device after configuration has been updated.
# The device will reset after all files were processed.
RESETNOW = 1
```

4. You can modify the `master_configuration.ini` file (or any of the `config_<MAC>.ini` files) at any time. The device queries for the latest version every 60 minutes, and applies the new settings immediately.
5. For additional security, usage of HTTPS and FTPS protocols is recommended. The device supports HTTPS (RFC 2818) and FTPS using the AUTH TLS method (RFC 4217) for the Automatic Update facility.
6. To download configuration files from an NFS server, the file system parameters should be defined in the configuration ini file. The following is an example of a configuration ini file for downloading files from NFS servers using NFS version 2:

```
# Define NFS servers for Automatic Update
[ NFSServers ]
FORMAT NFSServers_Index = NFSServers_HostOrIP,
NFSServers_RootPath, NFSServers_NfsVersion;
NFSServers 1 = 10.31.2.10, /usr/share, 2 ;
NFSServers 2 = 192.168.100.7, /d/shared, 2 ;
[ \NFSServers ]

CptFileUrl =
'file://10.31.2.10/usr/share/public/usa_tones.dat'
VpFileUrl =
'file://192.168.100.7/d/shared/audiocodes/voiceprompt.dat'
```

If you implement the Automatic Update mechanism, the device must not be configured using the Web interface. If you configure parameters in the Web interface and save (burn) the new settings to the device's flash memory, the `IniFileURL` parameter (defining the URL to the ini file for Automatic Updates) is automatically set to 0 (i.e., Automatic Updates is disabled).

The Web interface provides a safeguard for the Automatic Update mechanism. If the `IniFileURL` parameter is defined with a URL value (i.e., Automatic Updates is enabled), then by default, the 'Burn To FLASH' field under the Reset Configuration group in the Web interface's 'Maintenance Actions' page is automatically set to "No". Therefore, this prevents an unintended burn-to-flash when resetting the device.

However, if configuration settings in the Web Interface were burnt to flash, you can reinstate the Automatic Update mechanism, by loading to the device, the ini file that includes the correct `IniFileURL` parameter setting, using the Web interface or BootP.

4.4.2.3 Downloading the dat File to a Device

The purpose of the coeff.dat configuration file is to provide the best termination and transmission quality adaptation for different line types. The file consists of a set of parameters for the signal processor of the loop interface devices. This parameter set provides control of the following AC and DC interface parameters:

- DC (V / I curve and max current)
- AC impedance matching
- Transmit gain
- Receive gain
- Hybrid balance
- Frequency response in transmit and receive direction
- Hook thresholds (FXS only)
- Ringing generation and detection parameters
- Metering parameters

This means, for example, that changing impedance matching or hybrid balance requires no hardware modifications, so that a single device can meet user-specific requirements. The digital nature of the filters and gain stages also ensures high reliability, no drifts (over temperature or time) and simple variations between different line types.

The .dat configuration file is produced by AudioCodes for each market after comprehensive performance analysis and testing and can be modified on request. The current file supports US line type of 600 ohm AC impedance (and for FXS, 40 V RMS ringing voltage for REN = 2).

The following list describes which coeff.dat file is to be used with which MP device. The files are located in the Analog_Coefficients_Files folder:

For MP-11x and MP-124RevD FXS coefficients file types:

- MP11x-02-1-FXS_16KHZ.dat - supports generation of 16 KHz metering tone and complies with USA standard.
- MP11x-02-2-FXS_16KHZ.dat - supports generation of 16 KHz metering tone and complies with TBR21 standard (Pan European).
- MP11x-02-1-FXS_12KHZ.dat - supports generation of 12 KHz metering tone and complies with USA standard.
- MP11x-02-2-FXS_12KHZ.dat - supports generation of 12 KHz metering tone and complies with TBR21 standard (Pan European).

In a situation where the selection of the metering type (16Khz or 12 KHz) is not important, use MP11x-02-1-FXS_16KHZ.dat.

The dat configuration file is produced by AudioCodes for each market after comprehensive performance analysis and testing, and can be modified on request. The current file supports US line type of 600 ohm AC impedance and 40 V RMS ringing voltage for REN = 2.

In future software releases, it is to be expanded to consist of different sets of line parameters, which can be selected in the ini file, for each port.

To support different types of countries and markets, it is necessary to support loading of a new Coefficients.ini file. This file consists of AC and DC line parameters for the peripheral devices.

➤ **To send the Coeff.dat file to the device:**

Use either the Web interface GUI's Auxiliary Files. Refer to Software Upgrade Wizard in the product's User's Manual.

or

The BootP/TFTP Server to send to the device the ini file (which simultaneously downloads the Call Progress Tone ini file, provided that the device's CallProgressTonesFilename ini file parameter is defined, and provided that both ini files are located in the same directory. (Refer to 'BootP/TFTP Server').

4.5 Backup Copies of ini and Auxiliary Files

Be sure to separately store a copy of the ini file and all auxiliary files, as well as a note of the software version for use should a device require replacement.

4.6 Upgrading Device Software

To upgrade the device's software (firmware), load the upgraded firmware cmp file into the device (and optionally burn it into integral non-volatile memory) using:

1. Web interface - For a complete description of this option refer to Software Upgrade Wizard.
2. BootP/TFTP Server - Use the -fb BootP command line switch. The device downloads the specified firmware name via TFTP and also "burns" the firmware on the non-volatile memory.



Note: Upgrading the device's firmware requires reloading the ini file and re-burning the configuration files. A Software Upgrade Key may be required (refer to 'Software Upgrade Wizard').

Reader's Notes

5 Automatic Configuration Options

Large-scale deployment of MP-1xx devices calls for automated installation and setup capabilities. In some cases, the devices are shipped to the end-customer directly from manufacturing, while in other cases they pass through a staging warehouse. Configuration may therefore take place at the staging warehouse or at the final customer premises.

The devices may sometimes be pre-configured during the manufacturing process by AudioCodes (commonly known as "private labeling"). A two-stage configuration process will be employed, such that the initial configuration includes just the bare minimum, and final configuration is achieved when the device is deployed in a live network.

The following details the available options for fast automatic configuration.

5.1 Option A - Local Configuration Server with BootP/TFTP

This is the most straightforward alternative:

- A computer running BootP and TFTP software is placed in a staging warehouse.

A standard device configuration *.ini file is prepared and placed in the TFTP directory.

- BootP is configured with the MAC address of each device.
- Each device should be connected to the network and powered-up.

The BootP reply would contain the *.cmp and *.ini file names in the "bootfile" field. The device will retrieve these files and store them in flash.

If auxiliary files are required (coefficients, call progress tones etc.) they may be specified in the *.ini file and downloaded from the same TFTP server.

- When the LEDs turn green, the device may be disconnected and shipped to the end customer.
- Local IP addressing at the customer site would normally be provided by DHCP.

This alternative requires the configuration to take place at a staging warehouse.

5.2 Option B - DHCP-based Configuration Server

This alternative is similar to Option A, except that DHCP is used instead of BootP. The DHCP server may be specially configured to automatically provide AudioCodes devices with a temporary IP address, so that individual MAC addresses are not required.

Below is a sample configuration file for Linux DHCP server (dhcpd.conf). The devices will be allocated temporary IP addresses in the range 10.31.4.53 to 10.31.4.75.

TFTP is assumed to be on the same machine as the DHCP server (the "next-server" directive may be used otherwise).

```
ddns-update-style ad-hoc;
default-lease-time 60;
max-lease-time 60;

class "audiocodes" {
    match if(substring(hardware, 1, 3) = 00:90:8f);
}
subnet 10.31.0.0 netmask 255.255.0.0 {
    pool {
        allow members of "audiocodes";
        range 10.31.4.53 10.31.4.75;
        filename "MP118_SIP_5.00A.001.cmp -fb;mp118.ini";
        option routers                10.31.0.1;
        option subnet-mask            255.255.0.0;
    }
}
```

This alternative requires configuration to take place at a staging warehouse.

5.3 Option C - HTTP-based Automatic Updates

An HTTP (or HTTPS) server can usually be placed in the customer's core network, where configuration and software updates will be available for download.

For example, assume the core network HTTP server is `https://www.corp.com`.

A master configuration *.ini file should be placed on the HTTP server, e.g. `https://www.corp.com/audiocodes/master.ini`. This *.ini file could point to additional *.ini files, auxiliary files (voice prompts, call progress tones, coefficients etc.) and software upgrades (CMP files), all on the HTTP server or other HTTP servers in the core network.

The major advantage of this method is that the HTTP configuration can be checked periodically, when the device is deployed at the end customer site; HTTP(S) is not sensitive to NAT devices, allowing configuration to take place as needed, without on-site intervention.

For additional security, the URL may contain a different port and a username+password.

The MP-1xx devices should only be configured with the URL of the initial *.ini file. There are several ways of doing this:

- Using Options A or B above - via TFTP at a staging warehouse. The INI file parameter controlling the configuration URL is `IniFileURL`.
- Private labeling at AudioCodes.
- Using DHCP option 67 (see method D below).
- Manually on-site, using the RS-232 port or web interface.

When the device is deployed at the end-customer site, local DHCP provides IP addressing and DNS server information. The MP-1xx can then contact the HTTP server at the core network and complete its configuration.

The URL can be a simple file name, or contain the device MAC address or IP address, e.g.:

`http://corp.com/config-<MAC>.ini` turns into `http://corp.com/config-00908f030012.ini`

`http://corp.com/<IP>/config.ini` turns into `http://corp.com/192.168.0.7/config.ini`

Software upgrades may be performed using the parameter `CmpFileURL`. Inclusion of this parameter in the master INI file will cause the MP-1xx to download and store the specified software image.

Refer to the user documentation for additional examples of Automatic Updates.

This alternative does not require additional servers at the customer premises.

This alternative is NAT-safe.

5.4 Option D - Configuration using DHCP Option 67

This option is suitable for deployments where DHCP server configuration is feasible at the end customer site. Most DHCP servers allow configuring individual DHCP option values for different devices on the network; the DHCP configuration should be modified so that the MP-1xx device will receive a configuration URL in option 67, along with IP addressing and DNS server information.

The DHCP response will be processed by the MP-1xx upon startup, and consequently the HTTP server specified by the configuration URL will be contacted in order to complete the configuration.

The following is a sample Linux DHCP configuration file (dhcpd.conf) illustrating the required format of option 67.

```
ddns-update-style ad-hoc;

default-lease-time 3600;
max-lease-time 3600;

class "audiocodes" {
    match if(substring(hardware, 1, 3) = 00:90:8f);
}

subnet 10.31.0.0 netmask 255.255.0.0 {
    pool {
        allow members of "audiocodes";
        range 10.31.4.53 10.31.4.75;
        option routers                10.31.0.1;
        option subnet-mask            255.255.0.0;
        option domain-name-servers    10.1.0.11;
        option bootfile-name
"INI=http://www.corp.com/master.ini";
        option dhcp-parameter-request-list 1,3,6,51,67;
    }
}
```

This alternative does not require additional servers at the customer premises.

This alternative is NAT-safe.

5.5 Option E - Configuration using FTP or NFS

Some networks block access to HTTP(S). The Automatic Update facility provides limited support for FTP/FTPS connectivity, however it should be noted that periodic polling for updates is not possible (since these protocols do not support conditional fetching, i.e. update the file only if it is changed on the server).

The difference between this option and options C and D is simply the protocol in the URL - ftp instead of http.

NFS v2/v3 is supported as well, see the user documentation for additional configuration required to enable NFS.

Note that FTP is NAT-safe, while NFS is not.

5.6 Option F - TFTP Configuration using DHCP Option 66

This option is suitable for cases where the end customer network contains a provisioning TFTP server for all network equipment, without the possibility of distinction between AudioCodes and non-AudioCodes devices.

Upon startup, the MP-1xx will look for option 66 in the DHCP response. If option 66 contains a valid IP address, a TFTP download will be attempted for a file named after the device MAC address, e.g. "00908f0130aa.ini".

The configuration file loaded in this method is a one-time action; the download will not be repeated until the device is manually restored to factory defaults (pressing the reset button for 10 seconds while the Ethernet cable is not connected).

This alternative requires a configuration server at the customer premises.

TFTP access into the core network is not NAT-safe.

5.7 Option G - Configuration using AudioCodes EMS

AudioCodes EMS server functions as a core-network provisioning server. The MP-1xx should be configured with the IP address of the EMS server as the SNMP Manager, using one of the options detailed above.

As soon as a registered device contacts the EMS server via SNMP, the EMS server handles all required configuration automatically, upgrading software as needed.

This alternative does not require additional servers at the customer premises. This alternative is NAT-safe.

Reader's Notes

6 Configuration Using the Web Interface

The device contains a Web interface to be used for configuration and for run-time monitoring. The Web interface enables users equipped with any standard Web-browsing application such as Microsoft™ Internet Explorer™ (Version 6.0 and higher) or Firefox™ (Versions 5 through 9.0) to:

- Provision devices (refer to Configuration on page 66).
- Verify configuration changes in the Status pages (refer to 'Status and Diagnostic Menu' on page 139) or Toolbar (refer to Getting Acquainted with the Web Interface on page 47).
- Load the CMP file (refer to Software Upgrade Wizard).
- Load the ini, CAS, Voice Prompt, CPT, Prerecorded Tones, Dial Plan, Coder Table, and AMD Sensitivity Files (refer to Load Auxiliary Files on page 126).



Note: Although the Web Interface's recommended resolutions are 1024 x 768 and 1280 x 1024 pixels, AudioCodes supports other advanced resolutions.

6.1 Limiting the Web Interface to Read-Only Mode

Initially, the Web interface displays the default parameters that are pre-installed in the device. These parameters can be modified using the Web interface, either by modifying parameters on the various pages or by loading a text configuration ini file to the device.

Administrators can limit the Web interface to read-only mode by changing the value of the DisableWebConfig ini file parameter. The read-only mode feature can be used as a security measure. This security level provides protection against unauthorized access (such as Internet hacker attacks), particularly important to users without a firewall.

➤ **To limit the Web Server to read-only mode:**

- Set the ini file parameter DisableWebConfig to 1 (Default = 0, i.e. read-write mode) and send the modified ini file to the device. All Web pages are presented in read-only mode. The ability to modify configuration data is disabled. In addition, users do NOT have access to any "File Loading", "Regional Settings", "Web User Accounts", "Maintenance Actions" and "Configuration File" pages.



Notes:

- 'Read Only' policy can also be employed by setting DisableWebConfig to 0, setting the secondary account to User_Monitor access level and distributing the Main and Secondary accounts' user name password pairs according to the organization's security policy.
- When DisableWebConfig is set to 1, all users are demoted to 'Read Only' privileges regardless of their access level.

6.1.1 Encrypted HTTP Transport (HTTPS - SSL)

Data transport between the Web server and the Web client may be conducted over a secured SSL link that encrypts the HTTP layer. The Web server may be configured to accept communications only on a secured link (HTTPS) or both on a secured link (HTTPS) and a non-secured link (HTTP). For further details refer to the Security chapter in the Product Reference Manual.

6.1.2 Limiting Web Access to a Predefined List of Client IP Addresses

When client IP addresses are known in advance, administrators can define a list of up to 10 client IP addresses that are to be accepted by the Web server. Any client that does not bear an IP address in the pre-defined list is unable to connect to the Web server. For further details refer to the Security chapter in the Product Reference Manual.

6.1.3 Managing Web Server Access Using a RADIUS Server

Users are given the option to manage the web server's password-username pairs via a RADIUS server. For further details refer to the Security chapter in the Product Reference Manual.

6.2 Accessing the Web Interface

➤ **To access the Web interface:**

1. Open any standard Web-browser application, such as Microsoft™ Internet Explorer™ (Ver. 6.0 and higher) or Firefox™ (Versions 5 through 9.0).



Note: The browser must be Java-script enabled. If java-script is disabled, a message box with notification of this is displayed.

2. Specify the IP address of the device in the browser's URL field (e.g., <http://10.1.229.17> or <https://10.1.229.17> for an SSL secure link). The browser's Password page appears.

The default user-name and password are both "Admin" (case-sensitive).

Figure 6: Enter Network Password Screen

The image shows a 'Web Login' form. It has a title 'Web Login' at the top. Below it are two input fields: 'Username' and 'Password'. Below the 'Password' field is a checkbox labeled 'Remember Me'. To the right of the checkbox is a blue button labeled 'Login'.

6.3 Using Internet Explorer to Access the Web Interface

Internet Explorer's security settings may block access to the Gateway's Web browser if they're configured incorrectly. If this happens, the following message appears:

Unauthorized

Correct authorization is required for this area. Either your browser does not perform authorization or your authorization has failed. RomPager server.

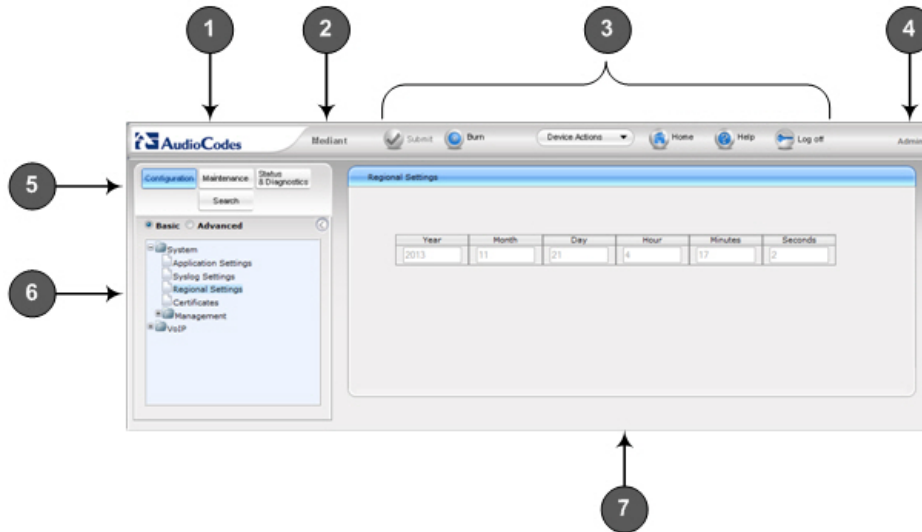
➤ **To troubleshoot blocked access to Internet Explorer:**

1. Delete all cookies from the Temporary Internet files folder. If this does not clear up the problem, the security settings may need to be altered. (Continue to Step 2).
2. In Internet Explorer, from the Tools menu, select Internet Options. The Internet Options dialog box appears.
3. Select the Security tab, and then, at the bottom of the dialog box, click Custom Level. The Security Settings dialog box appears.
4. Scroll down until the Logon options are displayed and change the setting to Prompt for user name and Password. Click OK.
5. Select the Advanced tab.
6. Scroll down until the HTTP 1.1 Settings are displayed and verify that the Use HTTP 1.1 option is checked.
7. Restart the browser. This fixes any issues related to domain use logon policy.

6.4 Areas of the GUI

The areas of the Web interface's GUI are shown in the figure below and described in the subsequent table.

Figure 7: Areas of the Web GUI








Description of the Web GUI Areas

Item #	Description
1	Displays AudioCodes (corporate) logo image.
2	Displays the product name.
3	Toolbar, providing frequently required command buttons. For more information, see Toolbar on page 48
4	Displays the username of the Web user that is currently logged in.
5	Navigation bar, providing the following tabs for accessing various functionalities in the Navigation tree: Configuration, Maintenance, and Status & Diagnostics tabs: Access the configuration menus (see Working with Configuration Pages on page 52) Search tab: Enables a search engine for searching configuration parameters (see Searching for Configuration Parameters on page 55)
6	Navigation tree, displaying a tree-like structure of elements (configuration menus, Scenario steps, or search engine) pertaining to the selected tab on the Navigation bar.
7	Work pane, displaying the configuration page of the selected menu in the Navigation tree. This is where configuration is done. For more information, (see Working with Configuration Pages on page 52).

6.4.1 Toolbar

The toolbar provides command buttons for quick-and-easy access to frequently required commands. The toolbar buttons are described in the table below:

Description of Toolbar Buttons

Icon	Button Name	Description
	Submit	Applies parameter settings to the device (refer to Saving Configuration Changes on page 55). Note: This icon is grayed out when not applicable to the currently opened page.
	Burn	Saves parameter settings to flash memory (refer to Saving Configuration Changes on page 55).
--	Device Actions	Opens a drop-down menu list with frequently needed commands: Load Configuration File: Opens the 'Configuration File' page for loading an ini file (refer to 'Restoring and Backing Up the device Configuration'). Save Configuration File: Opens the 'Configuration File' page for saving the ini file to a PC (refer to 'Restoring and Backing Up the device Configuration'). Reset: Opens the 'Maintenance Actions' page for resetting the device (refer to Maintenance on page 122). Restore Defaults: Opens the 'Configuration File' page for restoring the parameters default values (refer to Restoring Networking Parameters to their Default Values on page 18). Software Upgrade Wizard: Opens the 'Software Upgrade Wizard' page for upgrading the device's software (refer to Software Upgrade Wizard). Switch Over: Opens the "High Availability Maintenance" page for switching between Active and Redundant Boards (refer to High Availability Maintenance). Reset Redundant: Opens the "High Availability Maintenance" page for resetting the Redundant Board (refer to High Availability Maintenance).
	Home	Opens the Home page (refer to Using the Home Page).
	Help	Opens the Online Help topic of the currently opened configuration page in the Work pane (refer to Getting Help on page 58).
	Log off	Logs off a session with the Web interface (refer to Logging Off the Web Interface on page 57).



Note: If you modify parameters that only take effect after a device reset, after you click the Submit button, the toolbar displays the word "Reset" (in red color). This is a reminder for you to later save ('burn') your settings to flash memory and reset the device.

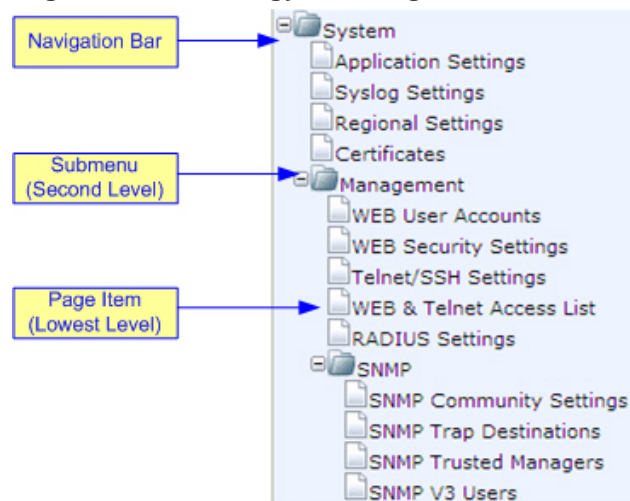
6.4.2 Navigation Tree

The Navigation tree, located in the Navigation pane, displays the menus (pertaining to the tab selected on the Navigation bar) used for accessing the configuration pages. The Navigation tree displays a tree-like structure of menus. You can easily drill-down to the required page item level to open its corresponding page in the Work pane.

The terminology used throughout this manual for referring to the hierarchical structure of the tree is as follows:

- Menu: first level (highest level)
- Submenu: second level - contained within a menu.
- Page item: last level (lowest level in a menu) - contained within a menu or submenu.

Figure 8: Terminology for Navigation Tree Levels



➤ To view menus in the Navigation tree:

- On the Navigation bar, select the required tab (Configuration, Maintenance, or Status & Diagnostics).

➤ To navigate to a page:

1. Navigate to the required page item, by performing the following:
 - Drilling-down using the plus \oplus signs to expand the menus and submenus
 - Drilling-up using the minus \ominus signs to collapse the menus and submenus
2. Select the required page item; the page opens in the Work pane.

6.4.2.1 Displaying Navigation Tree in Basic and Full View

You can view an expanded or reduced Navigation tree display regarding the number of listed menus and submenus. This is relevant when using the configuration tabs (Configuration, Maintenance and Status & Diagnostics) on the Navigation bar.

The Navigation tree menu can be displayed in one of two views:

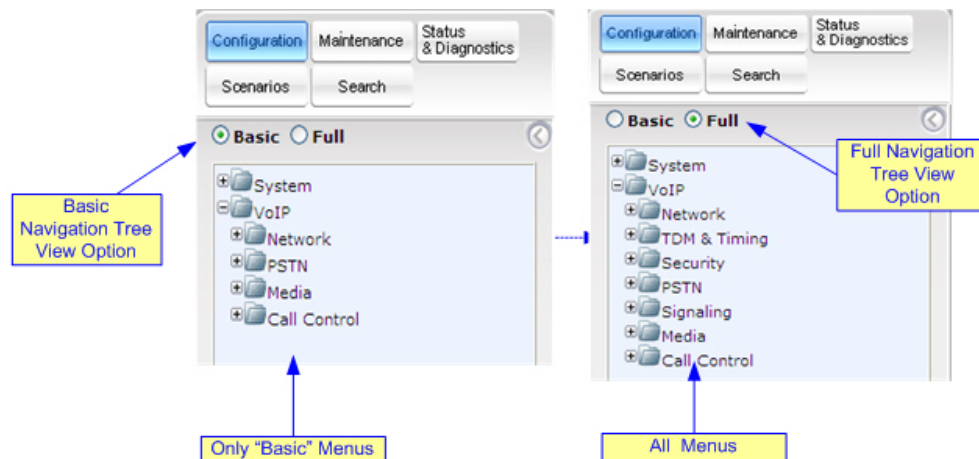
- Basic - Displays only commonly used menus
- Full - Displays all the menus pertaining to a configuration tab

The advantage of the Basic view is that it prevents "cluttering" the Navigation tree with menus that may not be required. Therefore, a Basic view allows you to easily locate required menus.

➤ **To toggle between Full and Basic view:**

Select the Basic option (located below the Navigation bar) to display a reduced menu tree; select the Full option to display all the menus. By default, the Basic option is selected.


Figure 9: Navigation Tree in Basic and Full View



Note: When in Scenario mode (refer to Working with Scenarios), the Navigation tree is displayed in 'Full' view (i.e., all menus are displayed in the Navigation tree).

6.4.2.2 Showing / Hiding the Navigation Pane

The Navigation pane can be hidden to provide more space for elements displayed in the Work pane. This is especially useful when the Work pane displays a page with a table that's wider than the Work pane and to view the all the columns, you need to use scroll bars. The arrow button located just below the Navigation bar is used to hide and show the Navigation pane.

To hide the Navigation pane: click the left-pointing arrow ; the pane is hidden and the button is replaced by the right-pointing arrow button.


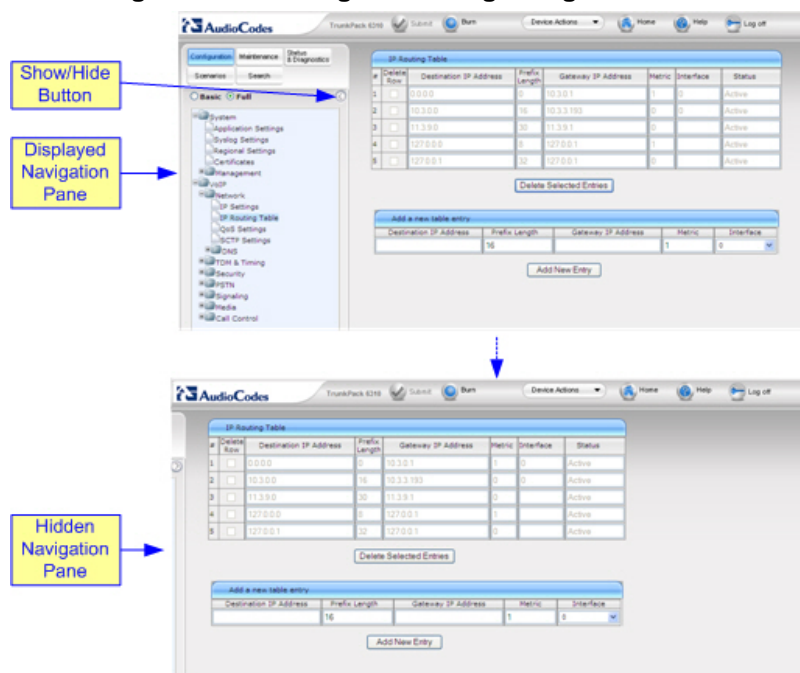
To show the Navigation pane: click the right-pointing arrow ; the pane is displayed and the button is replaced by the left-pointing arrow button.

Figure 10: Showing and Hiding Navigation Pane



6.4.3 Help Infrastructure

Almost every page contains a Help Pop-up function which describes the parameter's description.

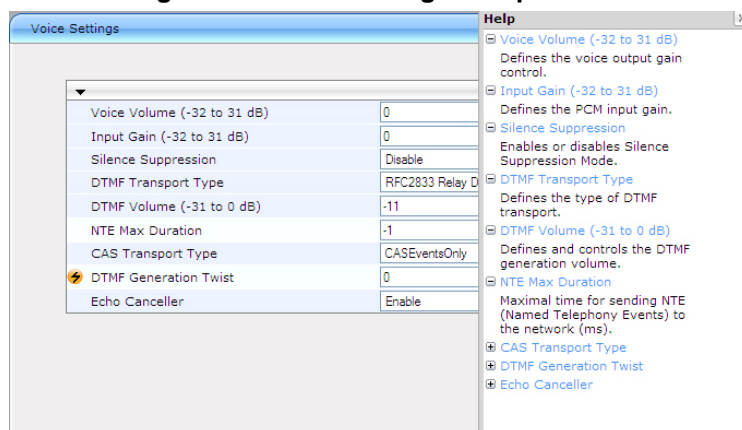
To get the Help for a specific page, just click on the Help icon:




You can find this icon on the top frame of the Web interface. After clicking this button, a new box will appear and contain the Help of that page.

For example, in the Voice Settings page, when clicking on the Help button, the Voice Settings specific Help appears as shown below.

Figure 11: Voice Settings - Help Screen



Clicking the plus sign opens the description and while clicking the minus sign closes it.

When finished, click on the  in the right-hand-side of the help box to close it.

6.4.4 Working with Configuration Pages

The configuration pages contain the parameters for configuring the device. The configuration pages are displayed in the Work pane, which is located to the right of the Navigation pane.

6.4.4.1 Accessing Pages

The configuration pages are accessed by clicking the required page item in the Navigation tree.

➤ **To open a configuration page in the Work pane:**

1. On the Navigation bar, click the required tab (Configuration, Maintenance, and Status & Diagnostics); the menu options of the selected tab appear in the Navigation tree.
2. In the Navigation tree, drill-down to the required page item; the page opens in the Work pane.

You can also access previously opened pages, by clicking your Web browser's Back button until you have reached the required page. This is useful if you want to view pages in which you have performed configurations in the current Web session.

Notes:

- You can also access certain pages from the Device Actions button located on the toolbar (refer to Getting Acquainted with the Web Interface on page 47).
- To view all the menus in the Navigation tree, ensure that the Navigation tree is in 'Full' view (refer to Getting Acquainted with the Web Interface on page 47).
- To get Online Help for the currently opened page, refer to Getting Help on page 58.
- Certain pages may not be accessible or may only be read-only if your Web user account's access level is low (refer to Web User Accounts on page 75). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.



6.4.4.2 Viewing Parameters

For convenience, some pages allow you to view a reduced or expanded display of parameters. A reduced display allows you to easily identify required parameters, enabling you to quickly configure your device.

The Web Interface provides you with two methods for handling the display of page parameters:

- Display of "Basic" and "Advanced" parameters
- Display of parameter groups



Note: Certain pages may only be read-only if your Web user account's access level is low (refer to Configuring the Web User Accounts). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.

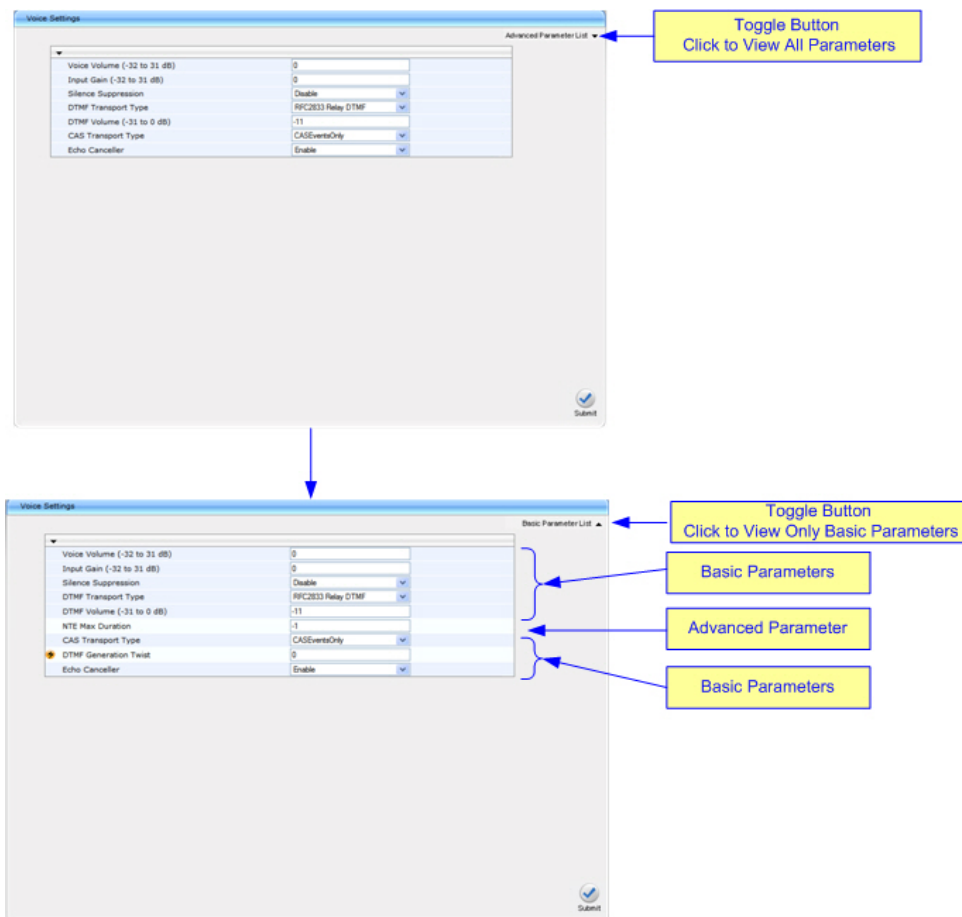
6.4.4.3 Displaying Basic and Advanced Parameters

Some pages provide you with an Advanced Parameter List / Basic Parameter List toggle button that allows you to show or hide advanced parameters (in addition to displaying the basic parameters). This button is located on the top-right corner of the page and has two states:

- Advanced Parameter List button with down-pointing arrow: click this button to display all parameters.
- Basic Parameter List button with up-pointing arrow: click this button to show only common (basic) parameters.

The figure below shows an example of a page displaying basic parameters only, and then showing advanced parameters as well, using the Advanced Parameter List button.

Figure 12: Displaying Basic and advanced Parameters



For ease of identification, the basic parameters are displayed with a darker blue color background than the advanced parameters.



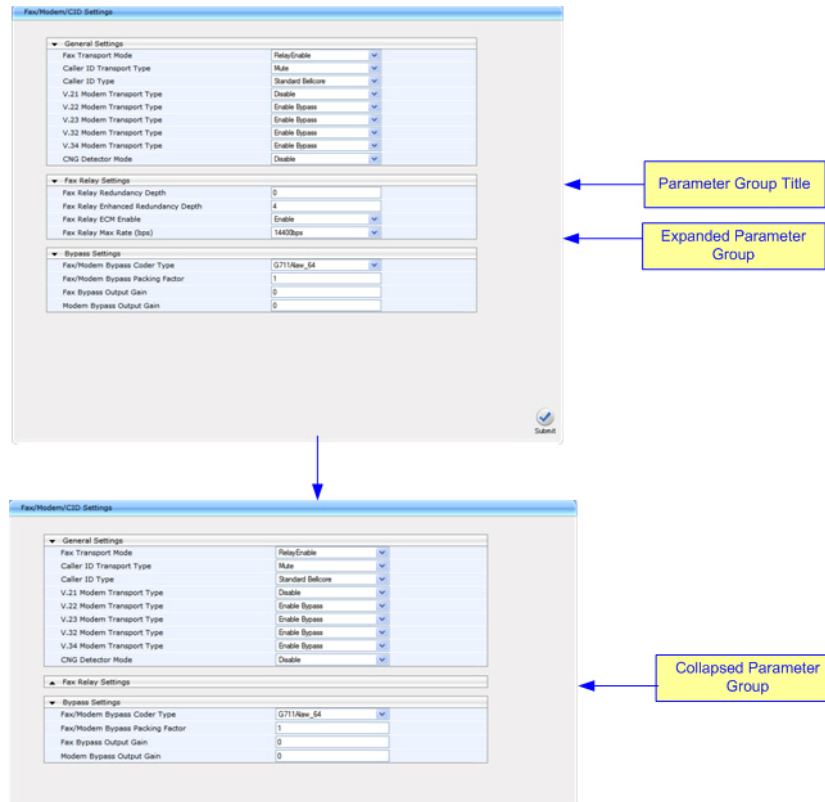
Notes:

- When the Navigation tree is in 'Full' mode, configuration pages display all their parameters (i.e., the 'Advanced Parameter List' view is displayed).
- If a screen contains only basic parameters, the Basic Parameter List button will not be shown.

6.4.4.4 Showing / Hiding Parameter Groups

Some pages provide groups of parameters, which can be hidden or shown. To toggle between hiding and showing a group, simply click the group name button that appears above each group. The button appears with a down-pointing or up-pointing arrow, indicating that it can be collapsed or expanded when clicked, respectively.

Figure 13: Expanding and Collapsing Parameter Groups



6.4.4.5 Modifying Parameter Values


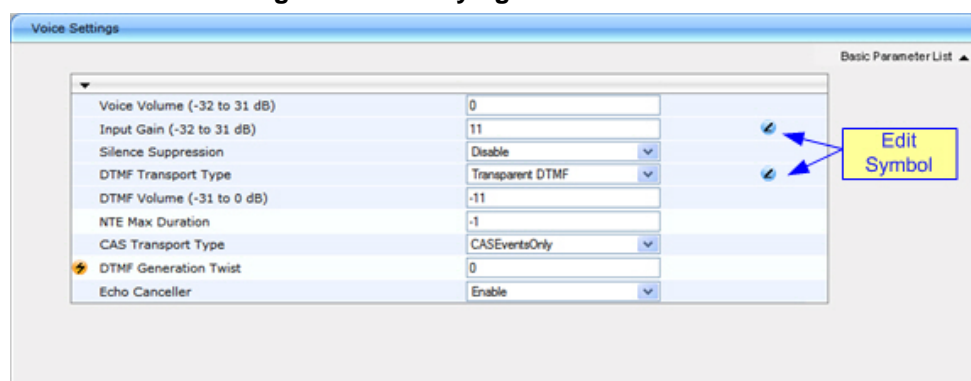
When you enter parameter values on a configuration page, the Edit  symbol appears to the right of these value fields. This feature is especially useful when modifying many parameters in a configuration page in that it helps to remind you of the parameters that you have currently modified (before applying the changes, i.e., clicking the Submit button).

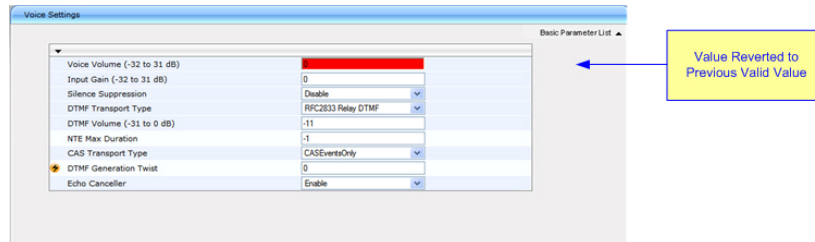
Figure 14: Modifying Parameter Values



Once you apply your parameter changes by clicking the Submit button, the Edit symbols disappear.

If you enter an invalid parameter value and then click Submit, a message box appears notifying you of the invalid value. In addition, the parameter value reverts back to its previous value and is highlighted in red, as shown in the figure below:

Figure 15: Value Reverts to Previous Valid Value



6.4.5 Saving Configuration Changes

To apply configuration changes to the device's volatile memory (RAM), click the Submit



button, which is located on the page in which you are working. Modifications to parameters with on-the-fly capabilities are immediately applied to the device; other parameters are applied only after a device reset.

However, parameters saved to the volatile memory revert to their previous settings after a hardware or software reset (or if the device is powered down). Therefore, to ensure that parameter changes (whether on-the-fly or not) are retained, you need to save ('burn') them to the device's non-volatile memory (i.e., flash). To save parameter changes to flash, refer to Saving Configuration.



Note: Parameters preceded by the lightning ⚡ sign are not changeable on-the-fly and require a device reset.

6.4.6 Searching for Configuration Parameters

The Web interface provides a search engine that allows you to search any ini file parameter that is configurable by the Web interface (i.e., has a corresponding Web parameter). You can search for a specific parameter (e.g., "EnableIPSec") or a sub-string of that parameter (e.g., "sec"). If you search for a sub-string, all parameters that contain the searched sub-string in their names are listed.

➤ **To search for ini file parameters configurable in the Web interface:**

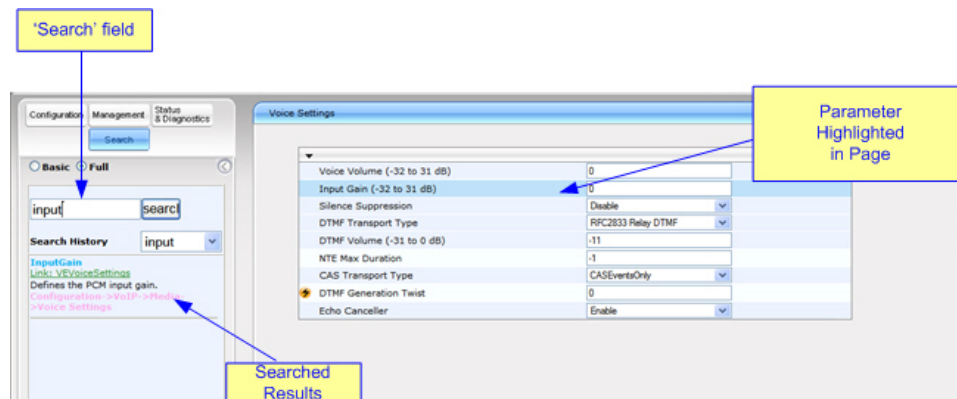
1. On the Navigation bar, click the Search tab; the Search engine appears in the Navigation pane.
2. In the 'Search' field, enter the parameter name or sub-string of the parameter name that you want to search. If you have performed a previous search for such a parameter, instead of entering the required string, you can use the 'Search History' drop-down list to select the string (saved from a previous search).
3. Click Search; a list of located parameters based on your search appears in the Navigation pane. Each searched result displays the following:
 - Link (in green) to its location (page) in the Web interface
 - Brief description of the parameter

4. In the searched list, click the required parameter (link in green) to open the page in which the parameter appears; the relevant page opens in the Work pane and the searched parameter is highlighted for easy identification, as shown in the figure below:



Note: If the searched parameter is not located, the "No Matches Found For This String" message is displayed.

Figure 16: Searched Result Screen



6.4.7 Creating a Login Welcome Message

You can create a Welcome message box (alert message) that appears after each successful login to the device's Web interface. The WelcomeMessage ini file parameter table allows you to create the Welcome message. Up to 20 lines of character strings can be defined for the message. If this parameter is not configured, no Welcome message box is displayed after login.

An example of a Welcome message is shown in the figure below:

Figure 17: User-Defined Web Welcome Message after Login



ini File Parameter for Welcome Login Message

Parameter	Description
WelcomeMessage	<p>Defines the Welcome message that appears after a successful login to the Web interface.</p> <p>The format for this ini file parameter table is as follows:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "..."; WelcomeMessage 2 = "..."; WelcomeMessage 3 = "...";</pre>

ini File Parameter for Welcome Login Message

Parameter	Description
	<p>[WelcomeMessage]</p> <p>For Example:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "*****" ; WelcomeMessage 2 = "***** This is a Welcome message *****" ; WelcomeMessage 3 = "*****" ; [WelcomeMessage]</pre> <p>Note: Each index represents a line of text in the Welcome message box. Up to 20 indices can be defined.</p>

6.4.8 Logging Off the Web Interface

You can log off the Web interface and re-access it with a different user account. For detailed information on the Web User Accounts, refer to User Accounts.

➤ To log off the Web Interface:

1. On the toolbar, click the Log Off  button; the 'Log Off' confirmation message box appears:

Figure 18: Log Off Confirmation Box



2. Click OK; the Web session is logged off. The "Web page for the session is logged off" message box appears, with a "Log In" button.
3. To log on again, simply click any page item in the navigation tree, and then in the 'Enter Network Password' dialog box, enter your user name and password.

6.4.9 Getting Help

The Web interface provides you with context-sensitive Online Help. The Online Help provides you with brief descriptions of most of the parameters you'll need to successfully configure the device. The Online Help provides descriptions of parameters pertaining to the currently opened page.

➤ **To view the Help topic for a currently opened page:**


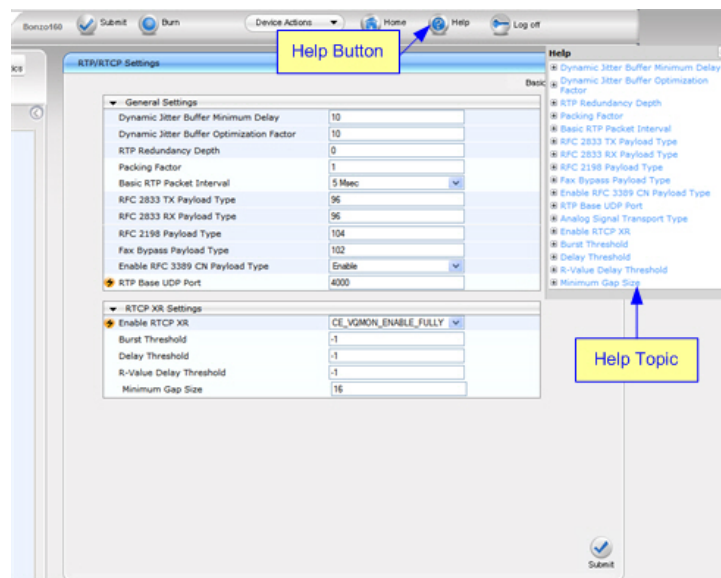




1. Using the Navigation tree, open the required page for which you want Help.
2. On the toolbar, click the Help  button; the Help topic pertaining to the opened page appears, as shown below:

Figure 19: Help Topic for Current Page



3. To view a description of a parameter, click the plus  sign to expand the parameter. To collapse the description, click the minus  sign.
4. To close the Help topic, click the close  button located on the top-right corner of the Help topic window or click the HELP  button.



Note: Instead of clicking the **Help** button for each page you open, you can open it once for a page, and then simply leave it open. Each time you open a different page, the Help topic pertaining to that page is automatically displayed.

6.4.10 Using the Home Page

The Home icon, located on the toolbar, opens the 'Home' page. This page provides you with a graphical display of the device's front panel. This page allows you to monitor the functioning of the device by its color-coded icons. The 'Home' page also displays general information in the 'General Information' pane such as the device's IP address and firmware version.

➤ To access the Home page, take this step:

On the toolbar, click the Home  icon; the 'Home' page is displayed:



Note: The following 'Home' pages are applicable to MediaPack.

Figure 20: MP-11x Home Page

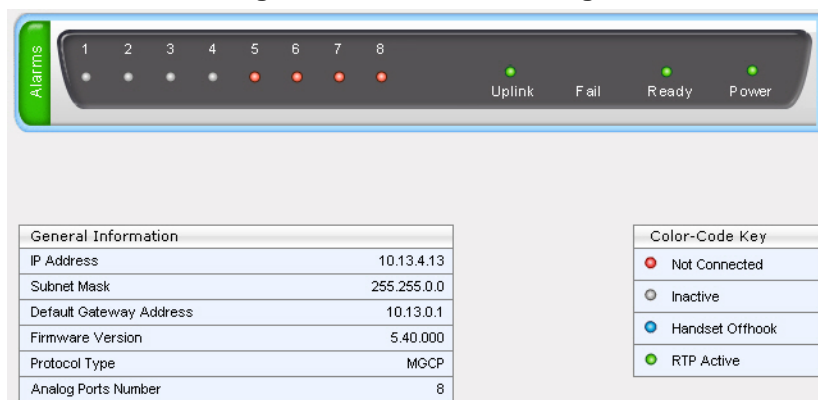
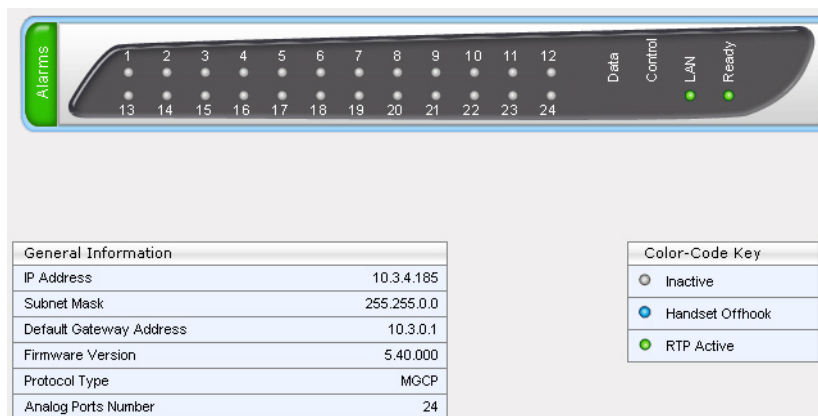


Figure 21: MP-124 Home Page



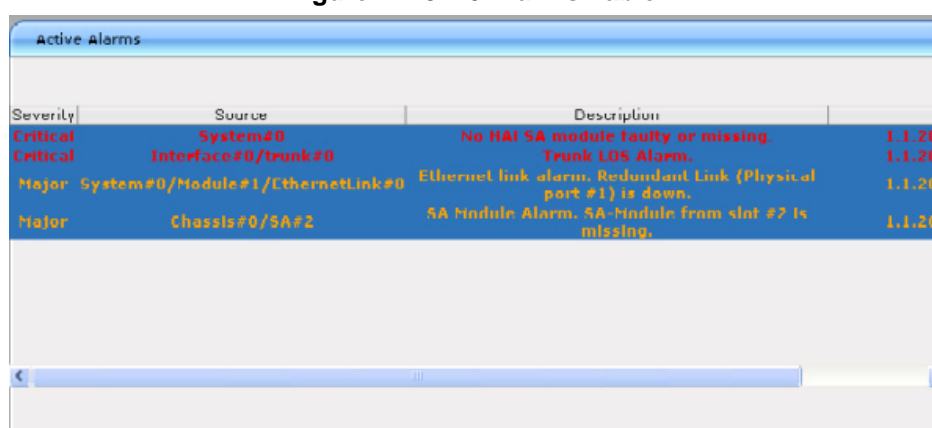
MediaPack Home Page Descriptions

Item# / Label	Description
Alarms	<p>Displays the highest alarm severity raised (if any) by the device:</p> <p>Green = no alarms.</p> <p>Orange = alarms have been raised and are listed in the 'Active Alarms' table.</p> <p>To view the list of alarms in the 'Active Alarms' table, click the Alarms area (refer to Viewing the Active Alarms Table on page 61).</p>
Channel / Ports	<p>Displays the status of the ports (channels):</p> <ul style="list-style-type: none"> ● (red): line not connected (only applicable to FXO devices) ● (grey): channel inactive ● (blue): handset is off-hook ● (green): active RTP stream <p>You can also view the channel's port settings (refer to Viewing Channel Information), reset the port (refer to Resetting an Analog Channel on page 65), and assign a name to the port (refer to Assigning a Name or Brief Description to a Port).</p>
Uplink (MP-11x) LAN (MP-124)	If clicked, the 'Ethernet Port Information' page opens, displaying Ethernet port configuration settings (refer to Viewing Ethernet Port Information).
Fail	Currently not supported.
Ready	Currently not supported.
Power	Always lit green, indicating power received by the device.

6.4.11 MediaPack Home Page

To navigate to the Alarm Table, click on the alarms chassis. The Active Alarms screen appears as shown below:

Figure 22: 8410 Alarms Table



Severity	Source	Description	
Critical	System#0	No HAI SA module faulty or missing.	1.1.20
Critical	Interface#0/trunk#0	Trunk LOS Alarm.	1.1.20
Major	System#0/Module#1/EthernetLink#0	Ethernet link alarm. Redundant Link (Physical port #1) is down.	1.1.20
Major	Chassis#0/SA#2	SA Module Alarm. SA Module from slot #2 is missing.	1.1.20

6.4.12 Viewing the Active Alarms Table

The 'Home' page allows you to view a list of currently active alarms. These alarms are displayed in the 'Active Alarms' page. In addition, the color of the 'Alarms' area in the 'Home' page indicates the highest alarm severity currently listed in the 'Active Alarms' page.

➤ **To view the list of alarms:**

On the 'Home' page, click the Alarms area, next to the Fan Tray unit (labeled as item #2 in the figures in Using the 'Home' page above); the 'Active Alarms' page appears:

Figure 23: Viewing Active Alarms

Sequential number	Severity	Source	Description	Date
2	Major	System#0/Module#1/EthernetLink#0	Ethernet link alarm. Redundant Link (Physical port #2) is down.	16.8.2011, 13:42:13
3	Minor	Chassis#0/PemCard#1	PEM Module Alarm. PEM power cable is missing	16.8.2011, 13:42:22
6	Major	System#0/Module#3	Ethernet link alarm. Redundant module's Ethernet link (Physical port #2) is down.	16.8.2011, 13:47:27
8	Major	System#0	Configuration mismatch in the system. SYS_HA: Active and Redundant modules have different feature keys.	16.8.2011, 13:47:27

For each alarm, the following is displayed:

- Severity: severity level of the alarm:
 - Critical: alarm displayed in red
 - Major: alarm displayed in orange
 - Minor: alarm displayed in yellow
- Source: unit from which the alarm was raised
- Description: brief explanation of the alarm
- Date: date and time that the alarm was generated

6.4.12.1 Viewing Alarm History

The Alarms History page displays a list of alarms that have been raised and traps that have been cleared.

➤ **To view the list of history alarms:**

Open the Alarms History page (Status & Diagnostics tab > System Status menu > Carrier-Grade Alarms > Alarms History).

Figure 24: Viewing Alarm History

Sequential number	Severity	Source	Description	Date
1	Major	Board#1	Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010, 14:1:26
2	Cleared	Board#1	Alarm cleared: Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010, 14:1:30
3	Major	Board#1	Controller failure alarm Proxy Set ID 0	6.1.2010, 14:1:26
4	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	6.1.2010, 14:1:29
5	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	6.1.2010, 14:1:29
6	Major	Board#1	NTP server alarm. No connection to NTP server.	6.1.2010, 14:11:14

For each alarm, the following information is provided:

- Severity: severity level of the alarm:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
 - Cleared (green)
- Source: unit from which the alarm was raised
- Description: brief explanation of the alarm
- Date: date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the Go to page button.

➤ **To delete all the alarms in the table:**

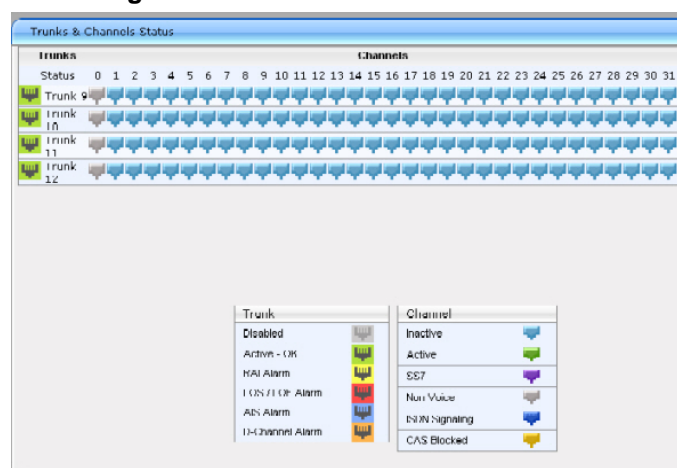
1. Click the Delete History Table button; a confirmation message box appears.
2. Click OK to confirm.

6.4.13 Viewing Channel Information

➤ **To view Trunks and Channels Status:**







1. To view the Trunks and Channel Status screen, click on the **Status & Diagnostics** link on the Navigation Bar.
2. From the navigation tree on the left, click on the **Trunks & Channels Status** link. The Trunks & Channels Status screen is displayed.

Figure 25: Trunks and Channels Status



The color-coding for the trunk's status is described in the table above. For color-coding of the trunk's channels, refer to the table below:

Color-Coding for Status Trunk's Channels

Indicator	Color	Label	Description
	Light blue	Inactive	Configured, but currently no call
	Green	Active	Call in progress (RTP traffic)
	Purple	SS7	Configured for SS7 (Currently not supported)
	Grey	Non Voice	Not configured
	Blue	ISDN Signaling or V5 Signaling (TP-8410)	Configured as a D-channel
	Yellow	CAS Blocked	--

3. To view the configuration settings of the trunk and / or to modify the trunk's settings, in the 'Trunks & Channels Status' screen, click the Trunk icon, and then from the shortcut menu, choose Port Settings; The 'Trunk Settings' screen appears. (For detailed information on configuring the trunk in this screen, refer to Trunk Settings.)
4. To view information of a specific trunk's channel, in the 'Trunks & Channels Status' screen, click the required Channel icon.

6.4.14 Viewing Ethernet Port Information

➤ To view Ethernet port settings via the Home page:

1. Click on the 'Home' page icon.
2. Click the Ethernet port for which you want to view port settings; the 'Ethernet Port Information' page opens:

Figure 26: Ethernet Port Information

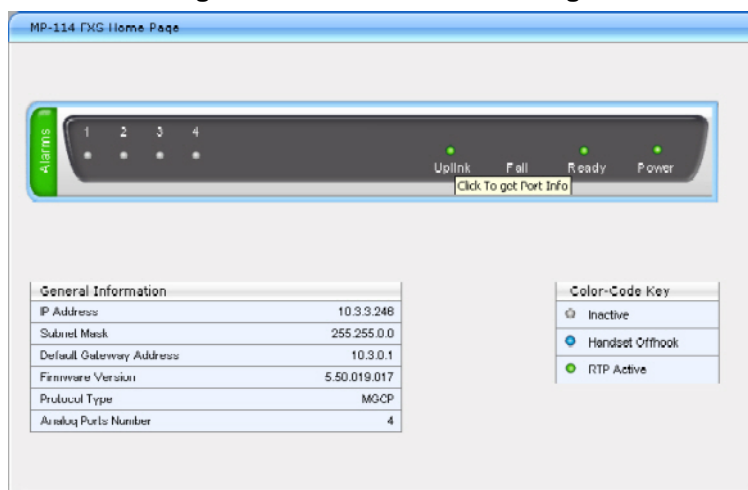
Ethernet Information	
Active Port	2
Port 1 Duplex Mode	Not Available
Port 1 Speed	Not Available
Port 2 Duplex Mode	Full Duplex
Port 2 Speed	100 Mbps

6.4.15 Viewing Ethernet Port Information

➤ To view Ethernet port information via the Home page:

1. Click on the 'Home' page icon.
2. Click on the 'Uplink' light to view the port information.

Figure 27: MediaPack Home Page



3. The Ethernet port information appears.

Figure 28: Ethernet Port Information

Ethernet Information	
Port 1 Duplex Mode	Half Duplex
Port 1 Speed	100 Mbps

6.4.16 Viewing Trunk Settings

The Home page allows you to view the settings of a selected port in the 'Trunk Settings' page. Accessing this page from the Home page provides an alternative to accessing it from the Advanced Configuration menu (Trunk Settings).

➤ To view Port Settings:

1. On the Home page, click a required trunk port LED on the blade (labeled as items #3 and #5 in the figure in Accessing the Home Page); a shortcut menu appears.
2. From the shortcut menu, choose Port Settings; the 'Trunk Settings' page opens.

6.4.17 Assigning a Name or Brief Description to a Port

The 'Home' page allows you to assign an arbitrary name or a brief description to each port. This description appears as a tooltip when you move your mouse over the port.

➤ To add a port description:

1. Click the required port icon; a shortcut menu appears.

Figure 29: MP-124 - Update Port Information

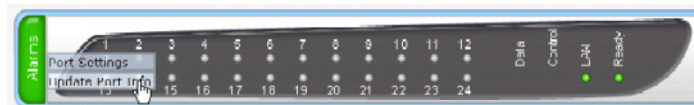
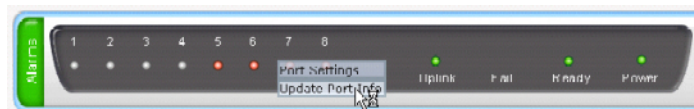


Figure 30: MP-11x - Update Port Information



2. From the shortcut menu, choose Update Port Info; a text box appears.

Figure 31: MP-124 - Apply Port Info

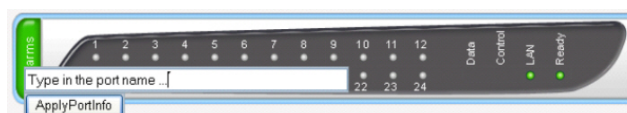
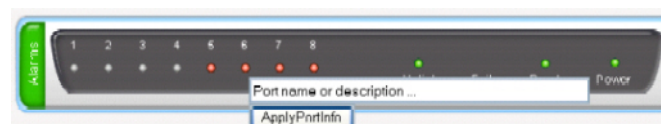


Figure 32: MP-11x - Apply Port Info



Type a brief description for the port, and then click Apply Port Info.

6.4.18 Resetting an Analog Channel



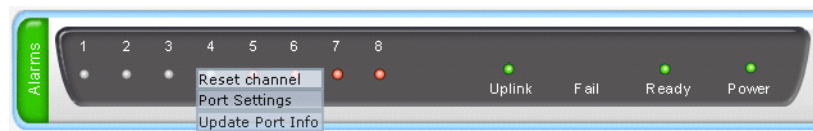
Note: The following sub-section on Resetting an Analog Channel is only applicable to MediaPack.

The 'Home' page allows you to inactivate (reset) an FXO or FXS analog channel. This is sometimes useful in scenarios, for example, when the device (FXO) is connected to a PBX and the communication between the two can't be disconnected (e.g., when using reverse polarity).

➤ **To reset a channel:**

Click the required FXS or FXO port icon, and then from the shortcut menu, choose Reset Channel; the channel is changed to inactive (i.e., LED is displayed in grey).

Figure 33: MP-11x - Reset Channel



6.5 Configuration

Configuration menu options are described below.

6.5.1 System

System sub-menu options are described below.

6.5.1.1 Application Settings

Application Settings include the following features: NTP, Daylight Saving Time, STUN, NFS and DHCP Settings.

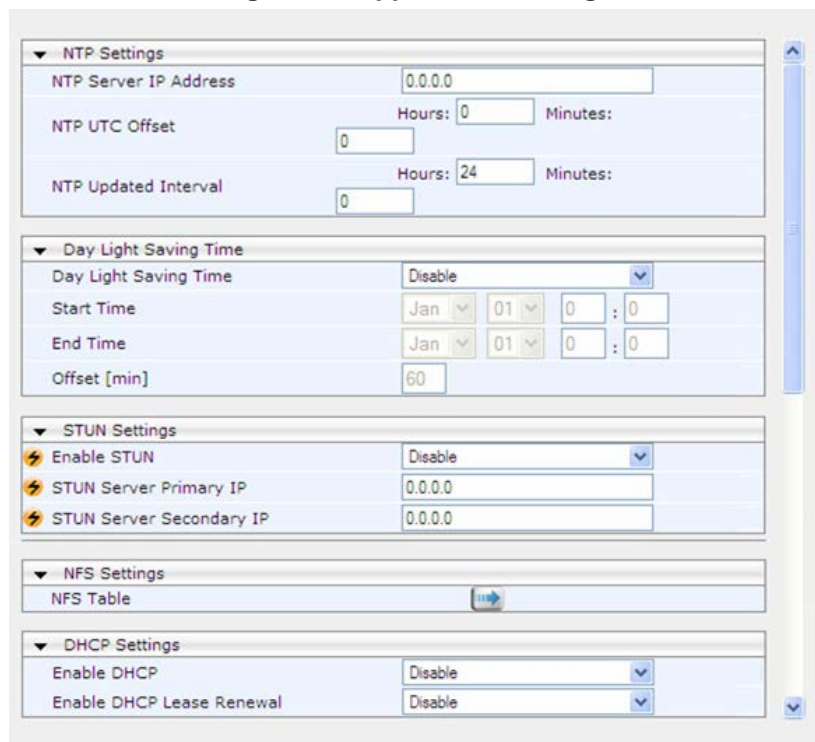
In this option, the following can be configured:

- NTP Server
- Day Light Saving Time
- STUN Settings
- NFS Servers Settings
- Enable the DHCP client

➤ To configure the Application Settings:

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 34: Application Settings



The screenshot shows the 'Application Settings' page with the following sections:

- NTP Settings:**
 - NTP Server IP Address: 0.0.0.0
 - NTP UTC Offset: Hours: 0, Minutes: 0
 - NTP Updated Interval: Hours: 24, Minutes: 0
- Day Light Saving Time:**
 - Day Light Saving Time: Disable (dropdown)
 - Start Time: Jan 01 00:00
 - End Time: Jan 01 00:00
 - Offset [min]: 60
- STUN Settings:**
 - Enable STUN: Disable (dropdown)
 - STUN Server Primary IP: 0.0.0.0
 - STUN Server Secondary IP: 0.0.0.0
- NFS Settings:**
 - NFS Table: [button]
- DHCP Settings:**
 - Enable DHCP: Disable (dropdown)
 - Enable DHCP Lease Renewal: Disable (dropdown)

2. To configure this page, refer to the System Parameters sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the Submit button. The changes are entered into the system and the page is refreshed.


➤ **To configure the NFS Settings:**

Network File System (NFS) enables the device to access a remote server's shared files and directories and to handle them as if they're located locally. The device can use NFS to load cmp, ini, and auxiliary files through the Automatic Update mechanism (refer to the Product Reference Manual).

You can configure up to 16 different NFS file systems. As a file system, the NFS is independent of machine types, operating systems and network architectures. Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the device.

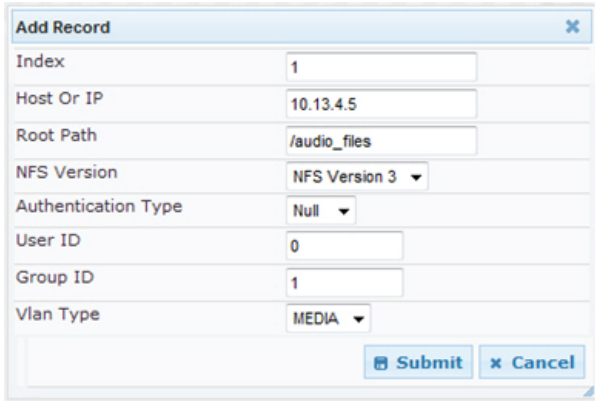
➤ **To add remote NFS file systems:**

1. Open the Application Settings page (Configuration tab > System menu > Application Settings).

Under the 'NFS Settings' group, click the NFS Table  button; the NFS Table page appears.

2. Click the Add button; the Add Record dialog box appears:

Figure 35: Add Record Dialog Box - NFS



Index	1
Host Or IP	10.13.4.5
Root Path	/audio_files
NFS Version	NFS Version 3
Authentication Type	Null
User ID	0
Group ID	1
Vlan Type	MEDIA

3. Configure the NFS parameters according to the table below.
4. Click the Submit button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.
5. To save the changes to flash memory, see Saving Configuration on page 125.

Notes:

- To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on that remote NFS file system.
- The combination of 'Host Or IP' and 'Root Path' must be unique for each row in the table. For example, the table must include only one row with a Host/IP of 192.168.1.1 and Root Path of /audio.
- The NFS table can also be configured using the table ini file parameter NFSServers (refer to the 'NFS Parameters' in the Product Reference Manual).



6.5.1.2 Syslog Settings

The procedure below describes how to configure Syslog.

➤ **To configure Syslog:**

1. Open the Syslog Settings page (Configuration tab > System menu > Syslog Settings).

Figure 36: Syslog Settings

▼ Syslog Settings	
Enable Syslog	Enable
Syslog Server IP Address	10.8.2.4
Syslog Server Port	514
Debug Level	5

▼ Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	<input type="checkbox"/>
Auxiliary Files Loading	<input type="checkbox"/>
Device Reset	<input type="checkbox"/>
Flash Memory Burning	<input type="checkbox"/>
Device Software Update	<input type="checkbox"/>
Access to Restricted Domains	<input type="checkbox"/>
Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>
Login and Logout	<input type="checkbox"/>

2. Enable the Syslog feature by setting the 'Enable Syslog' to Enable.
3. Define the Syslog server using the 'Syslog Server IP Address' and 'Syslog Server Port' parameters.
4. Configure the debug level using the 'Debug Level' parameter.
5. Under the 'Activity Types to Report ...' group, select the activities to report.
6. Click Submit to apply your changes.

6.5.1.3 Regional Settings

The Regional Settings page allows setting the system date and time.

➤ **To access the Regional Settings page:**

- Open the Regional Settings page (Configuration tab > System menu > Regional Settings).

Figure 37: Regional Settings

Year	Month	Day	Hour	Minutes	Seconds
2010	2	4	10	21	46

➤ **To set the date and time:**

1. Enter the date and/or time using the YYYY, MM, and DD field for Year, Month and Day and HH, MM, and SS fields for Hour, Minutes and Seconds.
2. Click Submit. The date and time is set on the device, accordingly.



Note: When the NTP feature is enabled (the NTP server is defined in the Application Settings page), the date and time are in Read Only mode as they are set by the NTP server.

6.5.1.4 TLS Contexts

This page allows managing the security certificates loaded on the device. The device is shipped with a working certificate configuration. Use this page only as needed. For further information, refer to the Security chapter in the Product Reference Manual.

The Certificates page allows you to configure X.509 certificates, which are used for secure management of the device, secure SIP transactions, and other security applications.



Note: The device is shipped with an active TLS setup. Thus, configure certificates only if required.

6.5.1.4.1 Replacing the Device's Certificate

The device is supplied with a working TLS configuration consisting of a unique self-signed server certificate. If an organizational Public Key Infrastructure (PKI) is used, you may wish to replace this certificate with one provided by your security administrator.

➤ **To replace the device's certificate:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPOnly) to **HTTP and HTTPS**. This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
4. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the DNS name.
 - b. Fill in the rest of the request fields according to your security provider's instructions.

- ### Figure 6-38: Certificate Signing Request Group

- Copy the text and send it to your security provider. The security provider, also known as Certification Authority or CA, signs this request and then sends you a server certificate for the device.
- Save the certificate to a file (e.g., cert.txt). Ensure that the file is a plain-text file containing the "BEGIN CERTIFICATE" header, as shown in the example of a Base64-Encoded X.509 Certificate below:

7. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the cert.txt file, and then click **Send File**.
8. After the certificate successfully loads to the device, save the configuration with a device reset; the Web interface uses the provided certificate.
9. Open the Certificates page again and verify that under the **Certificate information** group (at the top of the page), the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator:

Figure 6-39: Private key "OK" in Certificate Information Group

▼ Certificate information	
Certificate subject:	/CN=ACL_3845462
Certificate issuer:	/CN=ACL_3845462
Time to expiration:	7261 days
Key size:	1024 bits
Private key:	OK

10. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then return it to HTTPS by setting the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only**, and then reset the device with a flash burn.

**Notes:**

- The certificate replacement process can be repeated when necessary (e.g., the new certificate expires).
- It is possible to use the IP address of the device (e.g., 10.3.3.1) instead of a qualified DNS name in the Subject Name. This is not recommended since the IP address is subject to change and may not uniquely identify the device.
- The device certificate can also be loaded via the Automatic Update Facility by using the HTTPSCertFileName *ini* file parameter.

6.5.1.4.2 Loading a Private Key

The device is shipped with a self-generated random private key, which cannot be extracted from the device. However, some security administrators require that the private key be generated externally at a secure facility and then loaded to the device through configuration. Since private keys are sensitive security parameters, take precautions to load them over a physically-secure connection such as a back-to-back Ethernet cable connected directly to the managing computer.

➤ **To replace the device's private key:**

1. Your security administrator should provide you with a private key in either textual PEM (PKCS #7) or PFX (PKCS #12) format. The file may be encrypted with a short pass-phrase, which should be provided by your security administrator.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' field (HTTPOnly) to **HTTP and HTTPS**. This ensures that you have a method for accessing the device in case the new configuration does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**) and scroll down to the **Upload certificate files from your computer** group.

Figure 6-40: Upload Certificate Files from your Computer Group



4. Fill in the 'Private key pass-phrase' field, if required.
5. Click the **Browse** button corresponding to the 'Send Private Key' field, navigate to the key file, and then click **Send File**.
6. If the security administrator has provided you with a device certificate file, load it using the 'Send Device Certificate' field.
7. After the files successfully load to the device, save the configuration with a device reset; the Web interface uses the new configuration.
8. Open the Certificates page again, and verify that under the **Certificate information** group (at the top of the page) the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then enable it by setting the 'Secured Web Connection (HTTPS)' field to **HTTPS Only**.

6.5.1.4.3 Mutual TLS Authentication

By default, servers using TLS provide one-way authentication. The client is certain that the identity of the server is authentic. When an organizational PKI is used, two-way authentication may be desired - both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the managing PC and loading the root CA's certificate to the device's Trusted Root Certificate Store. The Trusted Root Certificate file may contain more than one CA certificate combined, using a text editor.

Since X.509 certificates have an expiration date and time, the device must be configured to use NTP to obtain the current date and time. Without the correct date and time, client certificates cannot work.

➤ **To enable mutual TLS authentication for HTTPS:**

1. Set the 'Secured Web Connection (HTTPS)' field to **HTTPS Only** to ensure you have a method for accessing the device in case the client certificate does not work. Restore the previous setting after testing the configuration.
2. Open the Certificates page (see 'Replacing the Device's Certificate' on page 69).
3. In the **Upload certificate files from your computer** group, click the **Browse** button corresponding to the 'Send Trusted Root Certificate Store ...' field, navigate to the file, and then click **Send File**.
4. When the operation is complete, set the 'Requires Client Certificates for HTTPS connection' field to **Enable** (see 'Configuring Web Security Settings' on page 86).
5. Save the configuration with a device reset.

When a user connects to the secured Web interface of the device:

- If the user has a client certificate from a CA that is listed in the Trusted Root Certificate file, the connection is accepted and the user is prompted for the system password.
- If both the CA certificate and the client certificate appear in the Trusted Root Certificate file, the user is not prompted for a password (thus, providing a single-sign-on experience - the authentication is performed using the X.509 digital signature).
- If the user does not have a client certificate from a listed CA or does not have a client certificate, the connection is rejected.



Notes:

- The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your operating system documentation, and/or consult your security administrator.
- The root certificate can also be loaded via the Automatic Update facility, using the HTTPSRootFileName ini file parameter.
- You can enable the device to check whether a peer's certificate has been revoked by an Online Certificate Status Protocol (OCSP) server.

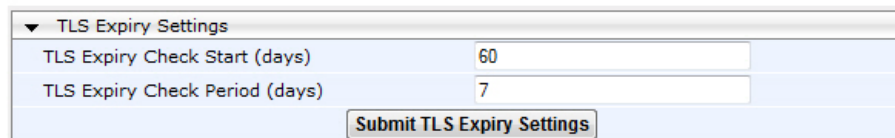
6.5.1.4.4 TLS Server Certificate Expiry Check

The device can periodically check the validation date of the installed TLS server certificate. This periodic check interval is user-defined. In addition, within a user-defined number of days before the installed TLS server certificate expires, the device can be configured to send the SNMP trap, acCertificateExpiryNotification to notify of the impending certificate expiration.

➤ **To configure TLS certificate expiry checks and notification:**

1. Open the Certificates page.
2. In the 'TLS Expiry Check Start' field, enter the number of days before the installed TLS server certificate is to expire at which the device must send a trap to notify of this.

Figure 41: TLS Expiry Settings



TLS Expiry Settings	
TLS Expiry Check Start (days)	60
TLS Expiry Check Period (days)	7
Submit TLS Expiry Settings	

3. In the 'TLS Expiry Check Period' field, enter the periodical interval (in days) for checking the TLS server certificate expiry date. By default, the device checks the certificate every 7 days.
4. Click the Submit TLS Expiry Settings button.

6.5.1.5 Management

Management - Contains a drop-down list with the following options:

- Web User Accounts - Refer to Web User Accounts on page 75
- Web Security Settings - Refer to Web Security Settings on page 82
- Telnet/SSH Settings - Refer to Telnet/SSH Settings on page 83
- Web & Telnet Access List - Refer to Web & Telnet Access List on page 83
- Authentication Settings - Refer to
- SNMP - Refer to SNMP on page 85
 - SNMP Community Settings - Refer to SNMP Community Settings on page 85
 - SNMP Trap Destinations - Refer to SNMP Trap Destinations on page 86
 - SNMP Trusted Managers - Refer to SNMP Trusted Managers on page 87
 - SNMP V3 Users - Refer to SNMP V3 Users on page 87

6.5.1.5.1 Web User Account Configuration

You can create up to 10 Web user accounts for the device. Up to five Web users can simultaneously be logged in to the device's Web interface. Web user accounts prevent unauthorized access to the Web interface, enabling login access only to users with correct credentials (i.e., username and password). Each Web user account is composed of the following attributes:

- Username and password: Credentials that enable authorized login access to the Web interface.
- Access level (user type): Access privileges specifying what the user can view in the Web interface and its read/write privileges. The table below describes the different types of Web user account access levels:

Access Levels of Web User Accounts

User Access Level	Numeric Representation*	Privileges
Master	220	Read / write privileges for all pages. Can create all user types, including additional Master users and Security Administrators. It can delete all users except the last Security Administrator.
Security Administrator	200	Read / write privileges for all pages. It can create all user types and is the only one that can create the first Master user. Note: There must be at least one Security Administrator.
Administrator	100	Read / write privileges for all pages except security-related pages, which are read-only.
Monitor	50	No access to security-related and file-loading pages; read-only access to other pages.
No Access	0	No access to any page. Note: This access level is not applicable when using advanced Web user account configuration in the Web Users table.
* The numeric representation of the access level is used only to define accounts in a RADIUS server (the access level ranges from 1 to 255).		

By default, the device is pre-configured with the following two Web user accounts:

Pre-configured Web User Accounts

User Access Level	Username (Case-Sensitive)	Password (Case-Sensitive)
Security Administrator	Admin	Admin
Monitor	User	User

After you log in to the Web interface, the username is displayed on the toolbar.

If the Web session is idle (i.e., no actions are performed) for more than five minutes, the Web session expires and you are once again requested to login with your username and password. Users can be banned for a period of time upon a user-defined number of unsuccessful login attempts. Login information (such as how many login attempts were made and the last successful login time) can be presented to the user.

➤ **To prevent user access after a specific number of failed logins:**

1. From the 'Deny Access On Fail Count' drop-down list, select the number of failed logins after which the user is prevented access to the device for a user-defined time (see next step).
2. In the 'Deny Authentication Timer' field, enter the interval (in seconds) that the user needs to wait before a new login attempt from the same IP address can be done after reaching the number of failed login attempts (defined in the previous step).

Notes:

- For security reasons, it's recommended that you change the default username and password.
- The Security Administrator user can change all attributes of all Web user accounts. Web users with access levels other than Security Administrator can change only their password and username.
- To restore the two Web user accounts to default settings (usernames and passwords), set the ini file parameter ResetWebPassword to 1.
- To log in to the Web interface with a different Web user, click the Log off button and then login with a different username and password.
- You can set the entire Web interface to read-only (regardless of Web user access levels), by using the ini file parameter DisableWebConfig (refer to the 'Web and Telnet Parameters' in the Product Reference Manual).
- You can define additional Web user accounts using a RADIUS server (refer to the 'Configuring RADIUS Settings' in the Product Reference Manual).



6.5.1.5.1.1 Basic User Accounts Configuration

This section describes basic Web user account configuration. This is relevant only if the two default, pre-configured Web user accounts - Security Administrator ("Admin") and Monitor ("User") - are sufficient for your management scheme.

For the Security Administrator, you can change only the username and password; not its access level. For the Monitor user, you can change username and password as well as access level (Administrator, Monitor, or No Access).



Notes:

- The access level of the Security Administrator cannot be modified.
- The access level of the second user account can be modified only by the Security Administrator.
- The username and password can be a string of up to 19 characters. When you log in to the Web interface, the username and password string values are case-sensitive, according to your configuration.
- Up to two users can be logged in to the Web interface at the same time, and they can be of the same user.

➤ To configure the two pre-configured Web user accounts:

1. Open the Web User Accounts page (**Configuration** tab > **System** menu > **Web User Accounts**). If you are logged in as Security Administrator, both Web user accounts are displayed (as shown below). If you are logged in with the second user account, only the details of this user account are displayed.

Figure 42: Web User Accounts Screen - Security Administrator Level

The screenshot shows the 'Web User Accounts' configuration page. At the top, it says 'Current Logged Users: Admin'. Below this, there are two sections for user configuration.

Account Data for User: Admin

- User Name: Admin (with a 'Change User Name' button)
- Access Level: Security Administrator (dropdown menu)
- Section: Fill in the following 3 fields to change the password
 - Current Password: [text box]
 - New Password: [text box]
 - Confirm New Password: [text box] (with a 'Change Password' button)

Account Data for User: User

- User Name: User (with a 'Change User Name' button)
- Access Level: User Monitor (dropdown menu) (with a 'Change Access Level' button)
- Section: Fill in the following 3 fields to change the password
 - Current Password: [text box]
 - New Password: [text box]
 - Confirm New Password: [text box] (with a 'Change Password' button)

2. To change the username of an account:
 - a. In the 'User Name' field, enter the new user name.
 - b. Click Change User Name; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
 - c. Log in with your new user name.

3. To change the password of an account:
 - a. In the 'Current Password' field, enter the current password.
 - b. In the 'New Password' and 'Confirm New Password' fields, enter the new password.
 - c. Click Change Password; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
 - d. Log in with your new password.
4. To change the access level of the optional, second account:
 - a. Under the Account Data for User: User group, from the 'Access Level' drop-down list, select a new access level user.
 - b. Click Change Access Level; the new access level is applied immediately.

6.5.1.5.1.2 Advanced User Accounts Configuration

This section describes advanced Web user account configuration. This is relevant if you need the following management scheme:

- Enhanced security settings per Web user (e.g., limit session duration)

More than two Web user accounts (up to 10 Web user accounts)

- Master users

This advanced Web user configuration is done in the Web Users table, which is initially accessed from the Web User Accounts page (see procedure below). Once this table is accessed, subsequent access immediately opens the Web Users table instead of the Web User Accounts page.



Notes:

- Only the Security Administrator user can initially access the Web Users table.
- Only Security Administrator and Master users can add, edit, or delete users.
- Admin users have read-only privileges in the Web Users table. Monitor users have no access to this page.
- If you delete a user who is currently in an active Web session, the user is immediately logged off by the device.
- All users can change their own passwords. This is done in the WEB Security Settings page (see Web Security Settings on page 82).
- To remove the Web Users table and revert to the Web User Accounts page with the pre-configured, default Web user accounts, set the ResetWebPassword ini file parameter to 1. This also deletes all other Web users.
- Once the Web Users table is accessed, Monitor users and Admin users can only change their passwords in the Web Security Settings page (see Web Security Settings on page 82). The new password must have at least four different characters than the previous password. (The Security Administrator users and Master users can change their passwords in the Web Users table and in the Web Security Settings page.)

➤ **To add Web user accounts with advanced settings:**

1. Open the Web Users Table page:
 - Upon initial access:
 - a. Open the Web User Accounts page (**Configuration** tab > **System** menu > **Web User Accounts**).
 - b. Under the Web Users Table group, click the Create Table button.
 - Subsequent access: **Configuration** tab > **System** menu > **Web User Accounts**.
The Web Users table appears, listing the two default, pre-configured Web use accounts - Security Administrator ("Admin") and Monitor ("User"):

Figure 43: Web Users Table Page

Index	Username	Password	Status	Password Age	Session Limit	Session Timeout	Block Duration	User Level
0	Admin	*	Valid	0	2	60	60	SecAdmin
1	User	*	Valid	0	2	60	60	Monitor

Page 1 of 1 View 1 - 2 of 2

2. Click the **Add** button; the following dialog box is displayed:

Figure 44: Web Users Table - Add Record Dialog Box

Add Record ✕

Index

Username

Password

Status

New ▼

Password Age

Session Limit

Session Timeout

Block Duration

User Level

Monitor ▼

Submit

✕ Cancel

3. Add a user as required. For a description of the parameters, see the table below.
4. Click Submit.

Web User Parameters Description

Parameter	Description
Web: Username	Defines the Web user's username. The valid value is a string of up to 40 alphanumeric characters, including the period ".", underscore "_", and hyphen "-" signs.

Parameter	Description
Web: Password	<p>Defines the Web user's password.</p> <p>The valid value is a string of 8 to 40 ASCII characters, which must include the following:</p> <ul style="list-style-type: none"> At least eight characters At least two letters that are upper case (e.g., "AA") At least two letters that are lower case (e.g., "aa") At least two numbers At least two signs (e.g., the dollar "\$" sign) No spaces in the string At least four characters different to the previous password
Web: Status	<p>Defines the status of the Web user.</p> <ul style="list-style-type: none"> New = (Default) User is required to change its password on the next login. When the user logs in to the Web interface, the user is immediately prompted to change the current password. Valid = User can log in to the Web interface as normal. <p>Failed Access = This state is automatically set for users that exceed a user-defined number of failed login attempts, set by the 'Deny Access on Fail Count' parameter (see 'Configuring Web Security Settings' on page). These users can log in only after a user-defined timeout configured by the 'Block Duration' parameter (see below) or if their status is changed (to New or Valid) by a System Administrator or Master.</p> <p>Old Account = This state is automatically set for users that have not accessed the Web interface for a user-defined number of days, set by the 'User Inactivity Timer' (see 'Configuring Web Security Settings' on page). These users can only log in to the Web interface if their status is changed (to New or Valid) by a System Administrator or Master.</p> <p>Notes:</p> <ul style="list-style-type: none"> The Old Account status is applicable only to Admin and Monitor users; System Administrator and Master users can be inactive indefinitely. For security, it is recommended to set the status of a newly added user to New in order to enforce password change.
Web: Password Age	<p>Defines the duration (in days) of the validity of the password. When this duration elapses, the user is prompted to change the password; otherwise, access to the Web interface is blocked.</p> <p>The valid value is 0 to 10000, where 0 means that the password is always valid. The default is 90.</p>
Web: Session Limit	<p>Defines the maximum number of Web interface sessions allowed for the user. In other words, this allows the same user account to log in to the device from different sources (i.e., IP addresses).</p> <p>The valid value is 0 to 5. The default is 2.</p> <p>Note: Up to 5 users can be logged in to the Web interface at any given.</p>

Parameter	Description
Web: Session Timeout	<p>Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface.</p> <p>The valid value is 0 to 100000. The default is according to the settings of the 'Session Timeout' global parameter (see Web Security Settings on page 82).</p>
Web: Block Duration	<p>Defines the duration (in seconds) for which the user is blocked when the user exceeds a user-defined number of failed login attempts. This is configured by the 'Deny Access On Fail Count' parameter (see Web Security Settings on page 82).</p> <p>The valid value is 0 to 100000, where 0 means that the user can do as many login failures without getting blocked. The default is according to the settings of the 'Deny Authentication Timer' parameter ((see Web Security Settings on page 82).</p> <p>Note: The 'Deny Authentication Timer' parameter relates to failed Web logins from specific IP addresses.</p>
Web: User Level	<p>Defines the user's access level.</p> <ul style="list-style-type: none"> Monitor = (Default) Read-only user. This user can only view Web pages and access to security-related pages is denied. Admin = Read/write privileges for all pages, except security-related pages including the Web Users table where this user has only read-only privileges. SecAdmin = Read/write privileges for all pages. This user is the Security Administrator. Master-User = Read/write privileges for all pages. This user also functions as a security administrator. <p>Notes:</p> <ul style="list-style-type: none"> At least one Security Administrator must exist. The last remaining Security Administrator cannot be deleted. The first Master user can be added only by a Security Administrator user. Additional Master users can be added, edited and deleted only by Master users. If only one Master user exists, it can be deleted only by itself. Master users can add, edit, and delete Security Administrators (but cannot delete the last Security Administrator). Only Security Administrator and Master users can add, edit, and delete Admin and Monitor users.

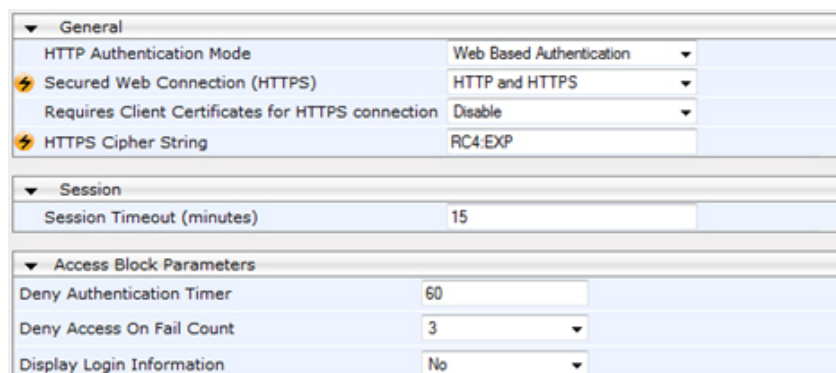
6.5.1.5.1.3 Web Security Settings

The Web Security Settings page is used to define a secure Web access communication method. For a description of these parameters, see 'Web and Telnet Parameters' in the Product Reference Manual

➤ **To define Web access security:**

1. Open the WEB Security Settings page (**Configuration** tab > **System** menu > **Management** > **WEB Security Settings**).

Figure 45: Web Security Settings



General	
HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTP and HTTPS
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	RC4:EXP
Session	
Session Timeout (minutes)	15
Access Block Parameters	
Deny Authentication Timer	60
Deny Access On Fail Count	3
Display Login Information	No

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see Saving Configuration on page 125.

6.5.1.5.1.4 Web Login Authentication using Smart Cards

You can enable Web login authentication using certificates from a third-party, Common Access Card (CAC) with user identification. When a user attempts to access the device through the Web browser (HTTPS), the device retrieves the Web user's login username (and other information, if required) from the CAC. The user attempting to access the device is only required to provide the login password. Typically, a TLS connection is established between the CAC and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Therefore, this feature implements a two-factor authentication - what the user has (i.e., the physical card) and what the user knows (i.e., the login password).

This feature is enabled using the EnableMgmtTwoFactorAuthentication parameter.



Note: For specific integration requirements for implementing a third-party smart card for Web login authentication, contact your AudioCodes representative.

➤ **To log in to the Web interface using CAC:**

1. Insert the Common Access Card into the card reader.
2. Access the device using the following URL: `https://<host name or IP address>`; the device prompts for a username and password.
3. Enter the password only. As some browsers require that the username be provided, it's recommended to enter the username with an arbitrary value.

6.5.1.5.2 Telnet/SSH Settings

➤ **To enable Telnet:**

1. Open the Telnet/SSH Settings page (**Configuration** tab > **System** menu > **Management** > **Telnet/SSH Settings**).

Figure 46: Telnet/SSH Settings

Telnet Settings	
Embedded Telnet Server	Enable Unsecured
Telnet Server TCP Port	23
Telnet Server Idle Timeout	0

SSH Settings	
Enable SSH Server	Disable
Server Port	22
Admin Key	
Require Public Key	Disable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3

2. To configure this page, refer to the Secure Telnet sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.1.5.2.1 Web & Telnet Access List

➤ **To configure the Web & Telnet Access List:**

1. Open the Web & Telnet Access List page (**Configuration** tab > **System** menu > **Management** > **Web & Telnet Access List**).

Figure 47: Web & Telnet Access List

Web & Telnet Access List

Add an authorized IP address

Add New Entry

Delete Row	Authorized IP Address
1 <input type="checkbox"/>	10.3.2.7

Delete Selected Addresses

2. To add a new authorized IP address, in the Add a new Authorized IP Address field at the bottom portion of the page, enter the required IP address and click Add New Entry.

3. To delete an authorized IP address, in the upper portion of the page, click a checkmark into the checkbox of the required IP address row (checkmarks in more than one row is permissible) and click Delete Selected Addresses.



Notes:

- When all authorized IP addresses are deleted, this security feature becomes disabled (all IP addresses are allowed to connect).
- When adding the first authorized IP address, you should add your own terminal's IP address, in order to be able to connect to the Web interface. If entered incorrectly, reset the device to restore configuration from non-volatile memory and regain web access.

6.5.1.5.3 Authentication Settings

➤ To configure the Authentication Settings:

1. Open the RADIUS Settings page (**Configuration** tab > **System** menu > **Management** > **Authentication Settings**).

Figure 48: Authentication Settings

General Login Authentication Settings	
Use Local Users Database	When No Auth Server Defined
Behavior upon Authentication Server Timeout	Verify Access Locally
Password Local Cache Mode	Reset Timer Upon Access
Password Local Cache Timeout (sec)	900
Default Access Level	200

RADIUS Settings	
⚡ Enable RADIUS Access Control	Disable
Use RADIUS for Web/Telnet Login	Disable
⚡ RADIUS Authentication Server IP Address	0.0.0.0
⚡ RADIUS Authentication Server Port	1645
⚡ RADIUS Shared Secret	••••••••
RADIUS VSA Vendor ID	5003
RADIUS VSA Access Level Attribute	35

2. To configure this page, refer to the Authentication Settings sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.1.5.4 SNMP

The device provides an embedded SNMP Agent that allows it to be managed by AudioCodes Element Management System (EMS) or a third-party SNMP Manager (e.g., element management system). The SNMP Agent supports standard Management Information Base (MIBs) and proprietary MIBs, enabling a deeper probe into the interworking of the device. The SNMP Agent can also send unsolicited events (SNMP traps) towards the SNMP Manager. All supported MIB files are supplied to customers as part of the release.

AudioCodes EMS is an advanced solution for standards-based management that covers all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of the device. The standards-compliant EMS uses distributed SNMP-based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a feature-rich management framework. It supports fault management, configuration and security.

The following provides configuration relating to SNMP management.

6.5.1.5.4.1 SNMP Community String

A SNMP Community String is a basic form of SNMP security. It describes the association between an SNMP server and clients. This string is like a password that controls the client's access to the server.

➤ **To configure the SNMP Community String:**

1. Open the SNMP Community String page (**Configuration** tab > **System** menu > **Management** > **SNMP** > **SNMP Community String**).

Figure 49: SNMP Community Settings

Community String	Access Level
<input type="text"/>	Read Only
<input type="text"/>	Read Only
<input type="text"/>	Read Only
<input type="text"/>	Read Only
<input type="text"/>	Read Only
<input type="text"/>	Read / Write
<input type="text"/>	Read / Write
<input type="text"/>	Read / Write
<input type="text"/>	Read / Write
<input type="text"/>	Read / Write

⚡ Disable SNMP		No
Trap Community String		trapuser
Trap Manager Host Name		<input type="text"/>

2. To add a Community String, enter a name in the Community String field in the "Read Only" or "Read/Write" section, (depending on the needed Access Level) and then click the Submit button, to apply the settings.



Note: Up to five "Read Only" or "Read/Write" Community Strings are permitted.

3. To delete a Community String, select the Delete check-box of the Community String to be deleted and then click the Submit button, to apply the settings.
4. To configure this page, refer to the SNMP Interface Details sub-section in the Product Reference Manual.
5. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.1.5.4.2 SNMP Trap Destinations

➤ **To configure the SNMP Trap Destinations:**

1. Open the SNMP Trap Destinations page (**Configuration** tab > **System** menu > **Management** > **SNMP** > **SNMP Trap Destinations**).

Figure 50: SNMP Trap Destinations

		IP Address	Trap Port	Trap User	Trap Enable
<input checked="" type="checkbox"/>	SNMP Manager 1	0.0.0.0	162	v2cParams ▼	Enable ▼
<input checked="" type="checkbox"/>	SNMP Manager 2	0.0.0.0	162	hq-snmpv3 ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 3	0.0.0.0	162	v2cParams ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 4	0.0.0.0	162	v2cParams ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 5	0.0.0.0	18	v2cParams ▼	Enable ▼

2. To configure this page, refer to the Multiple SNMP Trap Destinations sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.1.5.4.3 SNMP Trusted Managers

➤ **To configure the SNMP Trusted Managers:**

1. Open the SNMP Trusted Managers page (**Configuration** tab > **System** menu > **Management** > **SNMP** > **SNMP Trusted Managers**).

Figure 51: SNMP Trusted Managers

Delete	Trusted Managers IP Address	
<input type="checkbox"/>	SNMP Trusted Manager 1	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 2	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 3	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 4	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 5	<input type="text" value="0.0.0.0"/>

2. To configure this page, refer to the SNMP parameters sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.1.5.4.4 SNMP V3 Users

➤ **To configure the SNMP V3 Users:**

1. Open the SNMP v3 Users page (**Configuration** tab > **System** menu > **Management** > **SNMP** > **SNMP V3 Users**).
2. Click **Add**; the following dialog box appears:

Figure 52: SNMP V3 Users

Add Record

Index

0

User Name

Authentication Protocol

None

Privacy Protocol

None

Authentication Key

Privacy Key

Group

Read-Write

Submit

Cancel

3. To configure this page, refer to the SNMPv3 USM Users sub-section in the Product Reference Manual.
4. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2 VoIP

VoIP menu options are described below.

6.5.2.1 Network

This section describes the network-related configuration.

➤ **To configure the IP Settings:**

1. Open the IP Settings page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interface Table**).
2. Follow the guidelines in the Product Reference Manual when configuring/modifying the IP Settings, in the IP Settings page.
3. After configuring/modifying the parameter fields, click **DONE**. This will validate your configuration.
4. For configuration guidelines, refer to the MGCP/MEGACO Product Reference Manual.

6.5.2.2 IP Interface Table

➤ **To configure the IP Interface table:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interface Table**).
2. Click the **Add** button; the following dialog box appears:

Figure 53: IP Interface Table

Add Record	
Index	1
Application Type	OAMP + Media + Cont ▼
IP Address	0.0.0.0
Prefix Length	16
Default Gateway	0.0.0.0
VLAN ID	1
Interface Name	if 1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

3. Click **Submit** to apply your settings.

6.5.2.2.1 Changing VLAN Mode and 'Native' VLAN ID

The Interface Table web page allows the user to change the VLAN Mode (enable or disable VLANs), as well as to change the value of the 'Native' VLAN ID.

When configuring more than one network interface, VLANs must be enabled.

In order to change one of these parameters, open the Network Settings->IP Settings page. The VLAN Mode and 'Native' VLAN ID parameters are displayed below the Interface Table.

Note that any change of these parameter values will only be applied after burning the configuration and booting from Flash (not using a BOOTP/DHCP server).

Refer to the Interface Table Configuration Summary and Guidelines section in the MGCP/MEGACO Product Reference Manual, to ensure a successful configuration.

6.5.2.3 Static Route Table

The IP Routing Table page allows you to define up to 30 static IP routing rules for the device. These rules can be associated with a network interface (defined in the Multiple Interface table) and therefore, the routing decision is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. Traffic destined to the subnet specified in the routing rule is re-directed to the defined gateway, reachable through the specified interface. Before sending an IP packet, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway.

➤ **To configure static route:**

1. Open the IP Routing Table page (**Configuration** tab > **VoIP** menu > **Network** > **Static Routing Table**).
2. Click the **Add** button; the following dialog box appears:

Figure 54: Static Route Table

Destination	Prefix Length	Gateway
Add Record		
Index	0	
Interface Name	Unknown	
Destination	0.0.0.0	
Prefix Length	16	
Gateway	0.0.0.0	
Description		

3. Click **Submit** to apply your settings.



Notes:

- You can delete only inactive routing rules.
- The IP Routing table can also be configured using the table ini file parameter, StaticRouteTable.

6.5.2.4 Network Settings

You can configure the device's handling of ICMP Redirect messages. These messages can either be rejected (ignored) or permitted.



Note: You can also configure this feature using the ini file parameter DisableICMPRedirects (see 'Routing Parameters' in the Product Reference Manual).

➤ **To configure the handling of ICMP Redirect messages:**

1. Open the Network Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Network Settings**).

Figure 55: Network Settings

▼	
Send and Receive ICMP Redirect Messages	Enable ▼
Send ICMP Unreachable Messages	Enable ▼

2. Click **Submit** to apply your changes.

6.5.2.5 QoS Settings

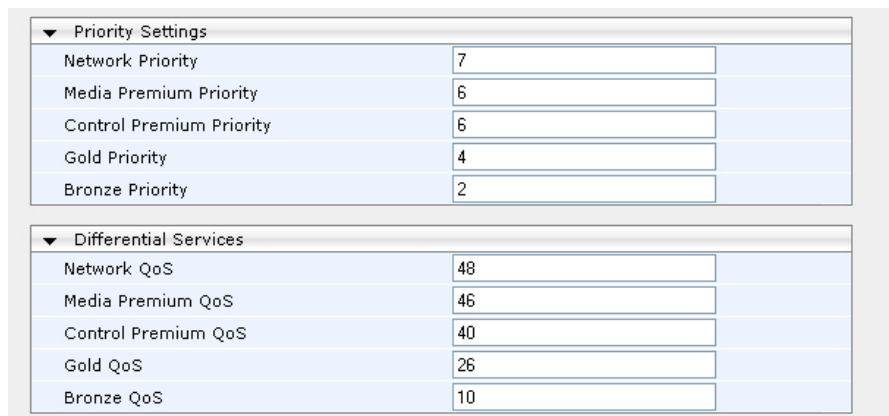
This page allows the user to configure values for the priority field of the VLAN tag, and the DiffServ field of the IP Header. Refer to QoS Parameters in the Product Reference Manual, for more information.

In order to access this page, set the configuration mode on the Navigation Pane to Full.

➤ **To configure the QoS Settings:**

1. Open the QoS Settings page (**Configuration** tab > **VoIP** menu > **Network** > **QoS Settings**).

Figure 56: QoS Settings



The screenshot displays the QoS Settings configuration page. It is divided into two main sections: 'Priority Settings' and 'Differential Services'. Each section contains a table with five rows of configuration parameters. The 'Priority Settings' section has parameters for Network Priority, Media Premium Priority, Control Premium Priority, Gold Priority, and Bronze Priority, with values 7, 6, 6, 4, and 2 respectively. The 'Differential Services' section has parameters for Network QoS, Media Premium QoS, Control Premium QoS, Gold QoS, and Bronze QoS, with values 48, 46, 40, 26, and 10 respectively. Each parameter is shown in a table with a label, a value field, and a submit button.

▼ Priority Settings		
Network Priority	7	
Media Premium Priority	6	
Control Premium Priority	6	
Gold Priority	4	
Bronze Priority	2	

▼ Differential Services		
Network QoS	48	
Media Premium QoS	46	
Control Premium QoS	40	
Gold QoS	26	
Bronze QoS	10	

2. To configure this page, refer to the Infrastructure ini File Parameters sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.6 Security Settings

Security Settings - Contains a drop-down list with the following options:

- Firewall Settings - Refer to Firewall Settings on page 93
- 802.1x Settings – Refer to 802.1x Settings on page 96.
- General Security Settings - Refer to General Security Settings on page 97
- IPSec Proposal Table - Refer to IP Security Proposal Table on page 98
- IPSec Association Table - Refer to IP Security Associations Table on page 99



Note: For more information, related to these pages, refer to the Security chapter in the Product Reference Manual.

6.5.2.6.1 Firewall Settings

The following describes Firewall settings.



Note: Refer to the Internal Firewall sub-section of the Security chapter for more information regarding Firewall Settings.

The device provides an internal firewall that enables you to configure network traffic filtering rules (access list). You can add up to 25 firewall rules. The access list offers the following firewall possibilities:

- Block traffic from known malicious sources
- Allow traffic only from known "friendly" sources, and block all other traffic
- Mix allowed and blocked network sources
- Limit traffic to a user-defined rate (blocking the excess)
- Limit traffic to specific protocols, and specific port ranges on the device

For each packet received on the network interface, the table is scanned from top to bottom until the first matching rule is found. This rule can either permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted.



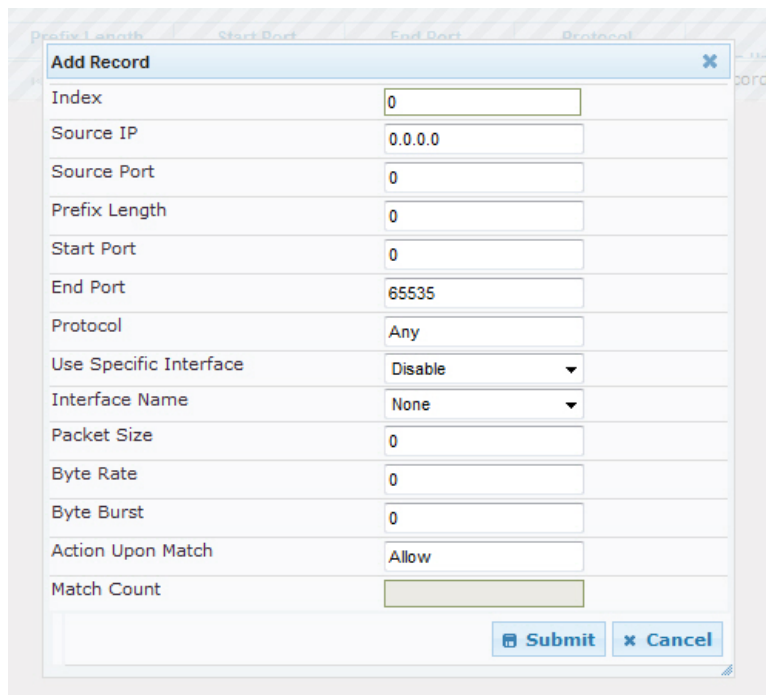
Notes:

- This firewall applies to a very low-level network layer and overrides all other security-related configuration. Thus, if you have configured higher-level security features (e.g., on the Application level), you must also configure firewall rules to permit this necessary traffic. For example, if you have configured IP addresses to access the Web and Telnet interfaces in the Web Access List (see Web & Telnet Access List on page 83), you must configure a firewall rule that permits traffic from these IP addresses.
- Only Security Administrator users or Master users can configure firewall rules.
- Setting the 'Prefix Length' field to 0 means that the rule applies to all packets, regardless of the defined IP address in the 'Source IP' field. Therefore, it is highly recommended to set this parameter to a value other than 0.
- It is recommended to add a rule at the end of your table that blocks all traffic and to add firewall rules above it that allow required traffic (with bandwidth limitations). To block all traffic, use the following firewall rule:
 - Source IP: 0.0.0.0
 - Prefix Length: 0 (i.e., rule matches all IP addresses)
 - Start Port - End Port: 0-65535
 - Protocol: Any
 - Action Upon Match: Block
- You can also configure the firewall settings using the table ini file parameter, AccessList (see 'Security Parameters' in the Product Reference Manual).

➤ **To add firewall rules:**

1. Open the Firewall Settings page (**Configuration** tab > **VoIP** menu > **Security** > **Firewall Settings**).
2. Click the **Add** button; the following dialog box appears:

Figure 57: Firewall Settings



Parameter	Value
Index	0
Source IP	0.0.0.0
Source Port	0
Prefix Length	0
Start Port	0
End Port	65535
Protocol	Any
Use Specific Interface	Disable
Interface Name	None
Packet Size	0
Byte Rate	0
Byte Burst	0
Action Upon Match	Allow
Match Count	

3. Configure the firewall parameters, as required.
4. Click **Submit** to add the new firewall rule to the table.
5. Reset the device to activate the rules.

The table below provides an example of configured firewall rules:

Firewall Rule Examples

Parameter	Value per Rule				
	1	2	3	4	5
Source IP	12.194.231.76	12.194.230.7	0.0.0.0	192.0.0.0	0.0.0.0
Prefix Length	16	16	0	8	0
Start Port and End Port	0-65535	0-65535	0-65535	0-65535	0-65535
Protocol	Any	Any	icmp	Any	Any
Use Specific Interface	Enable	Enable	Disable	Enable	Disable
Interface Name	WAN	WAN	None	Voice-Lan	None
Byte Rate	0	0	40000	40000	0
Burst Bytes	0	0	50000	50000	0
Action Upon Match	Allow	Allow	Allow	Allow	Block

The firewall rules in the above configuration example do the following:

- Rules 1 and 2: Typical firewall rules that allow packets ONLY from specified IP addresses (e.g., proxy servers). Note that the prefix length is configured.
- Rule 3: A more "advanced" firewall rule - bandwidth rule for ICMP, which allows a maximum bandwidth of 40,000 bytes/sec with an additional allowance of 50,000 bytes. If, for example, the actual traffic rate is 45,000 bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40,000 bytes/sec is dropped. If the actual traffic rate then slowed to 30,000 bytes/sec, the allowance would be replenished within 5 seconds.
- Rule 4: Allows traffic from the LAN voice interface and limits bandwidth.
- Rule 5: Blocks all other traffic.

6.5.2.6.2 802.1x Settings

The 802.1x Settings page is used to configure IEEE 802.1X Ethernet security. The device can function as an IEEE 802.1X supplicant. IEEE 802.1X is a standard for port-level security on secure Ethernet switches; when a device is connected to a secure port, no traffic is allowed until the identity of the device is authenticated.

A typical 802.1X deployment consists of an Authenticator (secure LAN switch), an Access Server (e.g. RADIUS), and one or more supplicants. The Authenticator blocks all traffic on the secure port by default and communicates with the supplicant via EAP-over-LAN frames. The supplicant provides credentials which are transmitted to the Access Server. If the Access Server determines that the credentials are valid, it instructs the Authenticator to authorize traffic on the secure port.

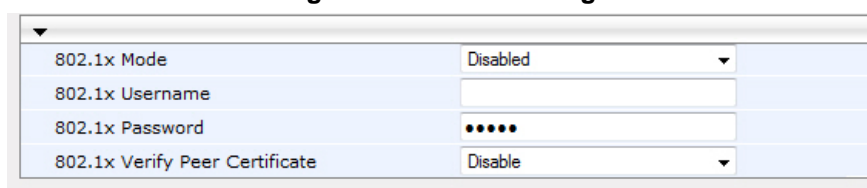
The device supports the following Extensible Authentication Protocol (EAP) variants:

- MD5-Challenge (EAP-MD5): Authentication is done with a user-defined 802.1X username and password.
- Protected EAP (PEAPv0 with EAP-MSCHAPv2): Authentication is done with a user-defined 802.1X username and password, however, the protocol is MSCHAPv2 over an encrypted TLS tunnel.
- EAP-TLS: The device's certificate is used to establish a mutually-authenticated TLS session with the Access Server. This requires prior configuration of the server certificate and root CA. The user-defined 802.1X username is used to identify the device, however, the 802.1X password is ignored.

➤ **To configure the 802.1x parameters:**

1. Open the 802.1x Settings page (**Configuration** tab > **VoIP** menu > **Security** > **802.1x Settings**).

Figure 58: 802.1x Settings



802.1x Mode	Disabled
802.1x Username	
802.1x Password	•••••
802.1x Verify Peer Certificate	Disable

2. Configure the parameters as required, and then click Submit.

6.5.2.6.3 General Security Settings

➤ To configure the General Security Settings:

1. Open the General Security Settings page (**Configuration** tab > **VoIP** menu > **Security** > **General Security Settings**).

Figure 59: General Security Settings

▼ IPsec Setting	
⚡ Enable IP Security	Disable ▼
IKE Certificate Ext Validate	Disable ▼
▼ TLS Settings	
TLS Version	SSL 2.0-3.0 and TLS 1.0 ▼
Strict Certificate Extension Validation	Disable ▼
⚡ FIPS140 Mode	Disable ▼
Client Cipher String	ALL:!ADH
▼ OCSP Settings	
Enable OCSP Server	Disable ▼
Primary Server IP	0.0.0.0
Secondary Server IP	0.0.0.0
Server Port	2560
Default Response When Server Unreachable	Reject ▼

2. Use the *.ini files as a reference when configuring/modifying the fields in the General Security Settings page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

6.5.2.6.4 IP Sec Proposal Table

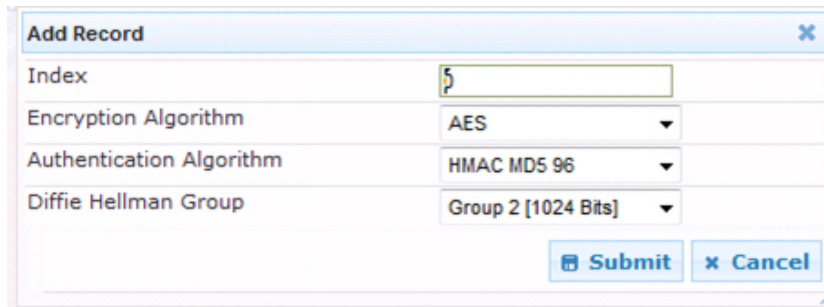


Note: IP Security Proposal Settings availability is in accordance with the device's Software Upgrade Key.

➤ **To configure the IP Security Proposal Table:**

1. Open the IP Security Proposal Table page (**Configuration** tab > **VoIP** menu > **Security** > **IPSec Proposal Table**).
2. Click the Add button; the following dialog box appears:

Figure 60: IP Security Proposals Table - Add Record Dialog Box



3. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the parameter fields in the page.
4. After configuring/modifying the parameter fields, click Submit. The changes are entered into the system and the page is refreshed.
5. To commit the changes to non-volatile (flash) memory, click Reset on the Toolbar. The Reset page appears. If you are modifying multiple pages, perform the reset after you are finished modifying all of the pages you intended and NOT after each page.
6. Select the **Burn** option and click **Reset**.

6.5.2.6.5 IP Sec Associations Table



Notes:

- IP Security Associations Settings availability is in accordance with the device's Software Upgrade Key.
- Refer to the IPSec ini file parameters in the ini file parameters section of the Product Reference Manual.
- Refer to the IP Security sub-section in the Security chapter of the Product Reference Manual.

➤ **To configure the IP Security Associations table:**

1. Open the IP Security Associations Table page (**Configuration** tab > **VoIP** menu > **Security** > **IPSec Association Table**).
2. Click the **Add** button; the following dialog box appears:

Figure 61: IP Security Associations Table

Add Record	
Index	1
Remote Endpoint Addr	10.3.2.73
Authentication Method	Pre-shared Key
Shared Key	*****
Source Port	0
Destination Port	0
Protocol	0
IKE SA Lifetime	28800
IpSec SA Lifetime (Secs)	3600
IpSec SA Lifetime (Kbs)	0
Dead Peer Detection Mode	DPD Periodic
Operational Mode	Transport
Remote Tunnel Addr	0.0.0.0
Remote Subnet Addr	0.0.0.0
Remote Prefix Length	16
Interface Name	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure the parameters, as required. In the above figure, a single IPsec/IKE peer (10.3.2.73) is configured. Pre-shared key authentication is selected with the pre-shared key set to 123456789. In addition, a lifetime of 28800 seconds is set for IKE and a lifetime of 3600 seconds is set for IPsec. For a description of the parameters, refer to the Product Reference Manual.
4. Click **Submit**.
5. To save the changes to flash memory, see Saving Configuration on page 125.

6.5.2.7 Media

Media - Contains a drop-down list with the following options:

- Voice Settings - Refer to 'Voice Settings' on page 100
- Fax/Modem/CID Settings - Refer to Fax/Modem/CID Settings on page 101
- RTP/RTCP Settings - Refer to RTP Settings on page 102
- IPMedia Settings - Refer to IPMedia Settings on page 103
- General Media Settings - Refer to General Media Settings on page 104
- Media Realm Configuration - Refer to Media Realm Configuration on page 106
- Media Security - Refer to Media Security on page 113

6.5.2.7.1 Voice Settings

➤ To configure the Voice Settings:

1. Open the Voice Settings page (**Configuration** tab > **VoIP** menu > **Media** > **Voice Settings**).

Figure 62: Voice Settings

Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
DTMF Transport Type	Transparent DTMF
MF Transport Type	RFC2833 Relay MF
DTMF Volume (-31 to 0 dB)	-11
NTE Max Duration	-1
CAS Transport Type	CASEventsOnly
⚡ DTMF Generation Twist	0
Echo Celler	Enable

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Media Settings parameter fields in the Media Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.2 Fax/Modem/CID Settings

➤ To configure the Fax/Modem/CID Settings:

1. Open the Fax/Modem/CID Settings page (**Configuration** tab > **VoIP** menu > **Media** > **Fax/Modem/CID Settings**).

Figure 63: Fax/Modem/CID Settings

▼ General Settings	
Fax Transport Mode	Bypass ▼
Caller ID Transport Type	Mute ▼
Caller ID Type	Standard Bellcore ▼
V.21 Modem Transport Type	Disable ▼
V.22 Modem Transport Type	Enable Bypass ▼
V.23 Modem Transport Type	Enable Bypass ▼
V.32 Modem Transport Type	Enable Bypass ▼
V.34 Modem Transport Type	Enable Bypass ▼
CNG Detector Mode	Disable ▼
▼ Fax Relay Settings	
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable ▼
Fax Relay Max Rate (bps)	14400bps ▼
▼ Bypass Settings	
Fax/Modem Bypass Coder Type	G711Alaw_64 ▼
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Fax/Modem/CID Settings parameter fields in the Fax/Modem/CID Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.3 RTP/RTCP Settings

➤ To configure the RTP/RTCP Settings:

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**).

Figure 64: RTP/RTCP Settings

General Settings	
Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable
⚡ RTP Base UDP Port	4000
Analog Signal Transport Type	Ignore Analog Signals

RTCP XR Settings	
⚡ Enable RTCP XR	CE_VQMON_DISABLE
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
Minimum Gap Size	16

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the RTP/RTCP Settings parameter fields in the RTP/RTCP Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.4 IPMedia Settings

➤ **To configure the IPMedia Settings:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** menu > **Media** > IPMedia Settings).

Figure 65: IP Media Settings

▼ IPMedia Settings	
⚡ IPMedia Detectors	Enable ▼
Enable Answer Detector	Disable ▼
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0 ▼
Answer Detector Sensitivity	0
Enable Energy Detector	Disable ▼
Energy Detector Quality Factor	4
Energy Detector Threshold	3
Enable Pattern Detector	Disable ▼
⚡ Active Speakers Min Interval	20
Configure Audio Playback	
Playback Audio Format	PCMA ▼
Configure Audio Recording	
End Of Record Time	0
⚡ Record Audio Format	PCMA ▼

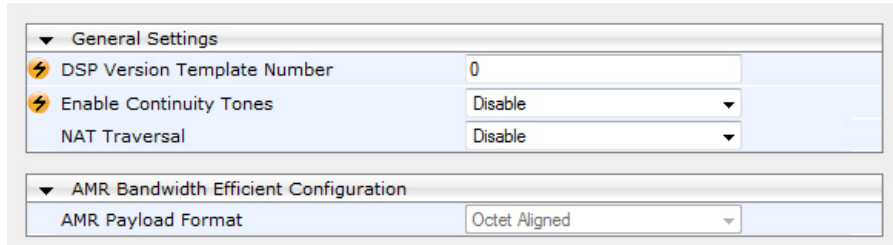
2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the IPMedia Settings parameter fields in the IPMedia Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.5 General Media Settings

➤ To configure the General Media Settings:

1. Open the General Media Settings page (**Configuration** tab > **VoIP** menu > **Media** > **General Media Settings**).

Figure 66: General Media Settings



General Settings	
DSP Version Template Number	0
Enable Continuity Tones	Disable
NAT Traversal	Disable

AMR Bandwidth Efficient Configuration	
AMR Payload Format	Octet Aligned

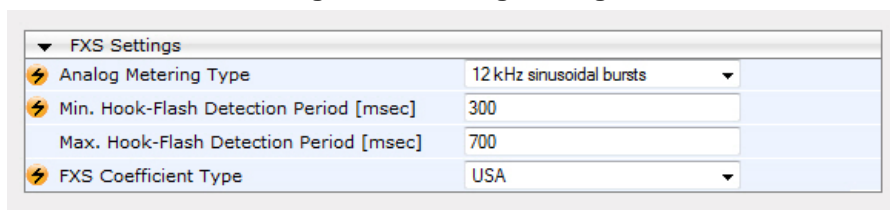
2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the General Media Settings parameter fields in the General Media Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.6 Analog Settings

The Analog Settings page allows you to configure various analog parameters.

1. Open the Analog Settings page (**Configuration** tab > **VoIP** menu > **Media** > **Analog Settings**).

Figure 67: Analog Settings



The screenshot shows a web interface for 'FXS Settings'. It contains a table with four rows of settings. Each row has a yellow lightning bolt icon in the first column, followed by the setting name, a text input field for the value, and a dropdown arrow in the third column.

FXS Settings		
⚡	Analog Metering Type	12 kHz sinusoidal bursts
⚡	Min. Hook-Flash Detection Period [msec]	300
	Max. Hook-Flash Detection Period [msec]	700
⚡	FXS Coefficient Type	USA

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Analog Settings parameter fields in the Analog Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

6.5.2.7.7 Media Realm Table

The Media Realm Table page allows you to define a pool of up to 64 media interfaces, termed Media Realms. Media Realms allow you to divide a Media-type interface, which is configured in the Multiple Interface table, into several realms, where each realm is specified by a UDP port range. You can also define the maximum number of sessions per Media Realm. Once configured, Media Realms can be assigned to IP Groups (see 'Configuring IP Groups' on page) or SRDs (see 'Configuring SRD Table' on page).

Once you have configured a Media Realm, you can configure it with the following:

Quality of Experience parameters for reporting to AudioCodes SEM server used for monitoring the quality of calls (see 'Configuring Quality of Experience Parameters per Media Realm' below)

Bandwidth management (see 'Configuring Bandwidth Management per Media Realm' below)



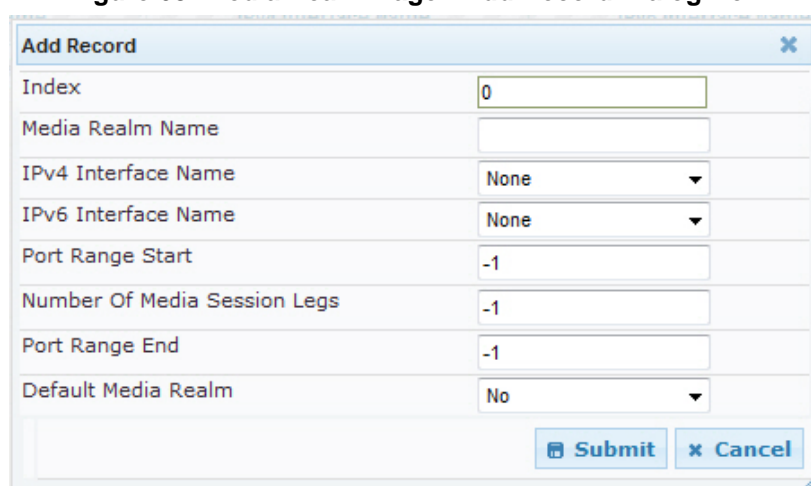
Notes:

- If different Media Realms are assigned to an IP Group and to an SRD, the IP Group's Media Realm takes precedence.
- For this setting to take effect, a device reset is required.
- The Media Realm table can also be configured using the table ini file parameter, CpMediaRealm.

➤ To define a Media Realm:

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Configuration**).
2. Click the **Add** button; the following appears:

Figure 68: Media Realm Page - Add Record Dialog Box



3. Configure the parameters as required. See the table below for a description of each parameter.
4. Click **Submit** to apply your settings.
5. Reset the device to save the changes to flash memory (see Saving Configuration on page 125).

Media Realm Table Parameter Descriptions

Parameter	Description
Index [CpMediaRealm_Index]	Defines the required table index number.
Media Realm Name [CpMediaRealm_MediaRealmName]	<p>Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is mandatory. ▪ The name assigned to the Media Realm must be unique. ▪ This Media Realm name is used in the SRD and IP Groups table.
IPv4 Interface Name [CpMediaRealm_IPv4IF]	Assigns an IPv4 interface to the Media Realm. This is name of the interface as configured for the Interface Name field in the Multiple Interface table.
IPv6 Interface Name [CpMediaRealm_IPv6IF]	Assigns an IPv6 interface to the Media Realm. This is name of the interface as configured for the Interface Name field in the Multiple Interface table.
Port Range Start [CpMediaRealm_PortRangeStart]	<p>Defines the starting port for the range of Media interface UDP ports.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ You must either configure all media realms with port ranges or all without; not some with and some without. ▪ The available UDP port range is calculated using the BaseUDPport parameter: ▪ Port ranges over 60,000 must not be used. ▪ Media Realms must not have overlapping port ranges.
Number of Media Session Legs [CpMediaRealm_MediaSessionLeg]	Defines the number of media sessions associated with the range of ports. This is the number of media sessions available in the port range. For example, 100 ports correspond to 10 media sessions, since ports are allocated in chunks of 10.
Port Range End [CpMediaRealm_PortRangeEnd]	Read-only field displaying the ending port for the range of Media interface UDP ports. This field is calculated by adding the 'Media Session Leg' field (multiplied by the port chunk size) to the 'Port Range Start' field. A value appears once a row has been successfully added to the table.
Is Default [CpMediaRealm_IsDefault]	<p>Defines the Media Realm as the default Media Realm. This default Media Realm is used when no Media Realm is configured for an IP Group or SRD for a specific call.</p> <ul style="list-style-type: none"> • [0] No (default) • [1] Yes <p>Notes:</p> <ul style="list-style-type: none"> • This parameter can be set to Yes for only one defined Media Realm. ▪ If this parameter is not configured, then the first Media Realm in the table is used as the default. ▪ If the table is not configured, then the default Media Realm includes all the configured media interfaces.

6.5.2.7.7.1 Configuring QoE per Media Realm

You can configure Quality of Experience (QoE) per Media Realm. This enables you to monitor and analyze media and signaling traffic, allowing you to detect problems causing service degradation. The device can save call information and statistics at call start, at call end, or at specific changes in the call. The information is stored as call records on an external server. The device connects, as a client, to the server using TLS over TCP.

You can specify the call parameters to monitor and configure their upper and lower thresholds. If these thresholds are exceeded, the device can be configured to do the following:

- Reports the change in the monitored parameter to the monitoring server (default).
- Sends RFC 2198 RTP redundancy packets on the call leg that crossed the threshold. This enables the device to adapt to the changed network status. In this option, you can also configure the redundancy depth. The channel configuration is unchanged if the change requires channel reopening. Currently, this option is applicable only when the monitored parameter is remote packet loss.

The device can be configured to monitor the following parameters on the local (i.e., at the device) or remote side:

- Packet loss
- Mean Opinion Score (MOS)
- Jitter
- Packet delay
- Residual Echo Return Loss (RERL)

At any given time during a call, each of these parameters can be in one of the following states according to its value in the last RTCP / RTCP XR packet:

- Gray - indicates that the value is unknown
- Green - indicates good call quality
- Yellow - indicates medium call quality
- Red - indicates poor call quality

The mapping between the values of the parameters and the color is according to the configured threshold of these parameters, per Media Realm. The call itself also has a state (color), which is the worst-state color of all the monitored parameters. Each time a color of a parameter changes, the device sends a report to the external server. A report is also sent at the end of each call.



Notes:

- The QoE feature is available only if the device is installed with the relevant Software License Key.
- To configure the address of the AudioCodes Session Experience Manager (SEM) server to where the device reports the QoE, see 'Configuring SEM Server for Media Quality of Experience' below.

➤ To configure Quality of Experience per Media Realm:

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Configuration**).
2. Select the Media Realm for which you want to configure Quality of Experience, and then click the Quality Of Experience link; the Quality Of Experience page appears.

- Click the **Add** button; the following dialog box appears:

Figure 69: Quality of Experience Page - Add Record Dialog Box

Add Record	
Index	1
Monitored Parameter	MOS
Direction	Device Side
Profile	Low Sensitivity
Green Yellow Threshold	3.4
Green Yellow Hysteresis	0.1
Yellow Red Threshold	2.7
Yellow Red Hysteresis	0.1
Green Yellow Operation	Notify
Green Yellow Operation Details	1
Yellow Red Operation	Notify
Yellow Red Operation Details	1
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

The figure above shows value thresholds for the MOS parameter, which are assigned using pre-configured values of the Low Sensitivity profile. In this example setting, if the MOS value changes by 0.1 (hysteresis) to 3.3 or 3.5, the device sends a report to the SEM indicating this change. If the value changes to 3.3, it sends a yellow state (i.e., medium quality); if the value changes to 3.5, it sends a green state.

- Configure the parameters as required. See the table below for a description of each parameter.
- Click **Submit** to apply your settings.

Quality of Experience Parameter Descriptions

Parameter	Description
Index [QOERules_RuleIndex]	Defines the table index entry. Up to four table row entries can be configured per Media Realm.
Monitored Parameter [QOERules_MonitoredParam]	Defines the parameter to monitor and report. <ul style="list-style-type: none"> [0] MOS (default) [1] Delay [2] Packet Loss [3] Jitter [4] RERL
Direction [QOERules_Direction]	Defines the monitoring direction. <ul style="list-style-type: none"> [0] Device Side (default) [1] Remote Side

Parameter	Description
Profile [QOERules_Profile]	<p>Defines the pre-configured threshold profile to use.</p> <ul style="list-style-type: none"> [0] No Profile = No profile is used and you need to define the thresholds in the parameters described below. [1] Low Sensitivity = Automatically sets the thresholds to low sensitivity values. Therefore, reporting is done only if changes in parameters' values is significant. [2] Default Sensitivity = Automatically sets the thresholds to a medium sensitivity. [3] High Sensitivity = Automatically sets the thresholds to high sensitivity values. Therefore, reporting is done for small fluctuations in parameters' values.
Green Yellow Threshold [QOERules_GreenYellowThreshold]	<p>Defines the parameter threshold values between green (good quality) and yellow (medium quality) states.</p>
Green Yellow Hysteresis [QOERules_GreenYellowHystersis]	<p>Defines the hysteresis (fluctuation) for the green-yellow threshold. When the threshold is exceeded by this hysteresis value, the device sends a report to the SEM indicating this change.</p>
Yellow Red Threshold [QOERules_YellowRedThreshold]	<p>Defines the parameter threshold values between yellow (medium quality) and red (poor quality). When this threshold is exceeded, the device sends a report to the SEM indicating this change.</p>
Yellow Red Hysteresis [QOERules_YellowRedHystersis]	<p>Defines the hysteresis (fluctuation) for the yellow-red threshold. When the threshold is exceeded by this hystersis value, the device sends a report to the SEM indicating this change.</p>
Green Yellow Operation [QOERules_GreenYellowOperation]	<p>Defines the action that is done if the green-yellow threshold is crossed.</p> <ul style="list-style-type: none"> [1] Notify = (Default) Device sends a report to the SEM server. [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg. <p>Note: This field is applicable only if the monitored parameter is remote packet loss.</p>
Green Yellow Operation Details [QOERules_GreenYellowOperationDetails]	<p>Note: This field is currently not supported.</p> <p>Defines the desired RTP redundancy depth. The actual redundancy depth on the relevant call leg is the minimum between the desired depth and the maximum supported depth on that call leg.</p> <p>Note: This field is applicable only if the 'Green Yellow Operation' field is set to Activate 2198.</p>
Yellow Red Operation [QOERules_YellowRedOperation]	<p>Note: This field is currently not supported.</p> <p>Defines the action that is done if the yellow-red threshold is crossed.</p> <ul style="list-style-type: none"> [1] Notify = (Default) Device sends a report to the SEM server. [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg. <p>Note: This field is applicable only if the monitored parameter is remote packet loss.</p>

Parameter	Description
Yellow Red Operation Details [QOERules_YellowRedOperationDetails]	<p>Note: This field is currently not supported.</p> <p>Defines the desired RTP redundancy depth. The actual redundancy depth on the relevant call leg is the minimum between the desired depth and the maximum supported depth on that call leg.</p> <p>Note: This field is applicable only if the 'Yellow Red Operation' field is set to Activate 2198.</p>

6.5.2.7.7.2 Configuring Bandwidth Management per Media Realm

Bandwidth management enables you to configure bandwidth utilization thresholds per Media Realm which when exceeded, the device can do one of the following:

- Generate an appropriate SNMP alarm, which is cleared when the bandwidth utilization returns to normal.
- Block any additional calls on the Media Realm.

Bandwidth management includes the following bandwidth utilization states:

- Normal
- High threshold
- Critical threshold

When a transition occurs between two bandwidth threshold states, based on threshold and hysteresis values, the device executes the configured action. The transition possibilities include Normal-High threshold state changes and High-Critical threshold state changes. Thus, up to two thresholds can be configured per Media Realm; one for each state transition.



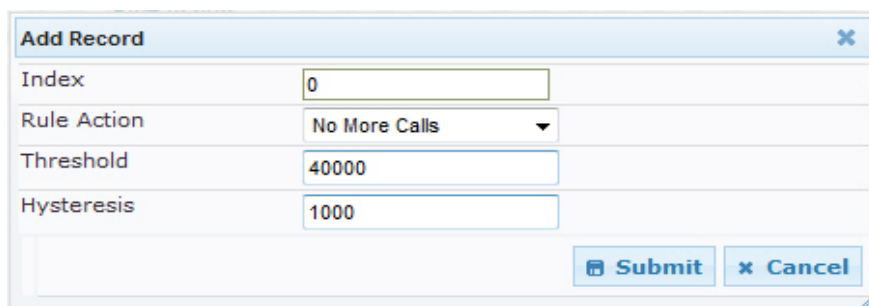
Notes:

- This feature is available only if the device is installed with the relevant Software License Key.
 - For your bandwidth management settings to take effect, you must reset the device.
- You can also use the BWManagement ini file parameter to configure bandwidth management per Media Realm.

➤ To configure bandwidth management rules per Media Realm:

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Configuration**).
2. Select the Media Realm for which you want to configure bandwidth management rules, and then click the Bandwidth Management link; the Bandwidth Management page appears.
3. Click the **Add** button; the following dialog box appears:

Figure 70: Bandwidth Management Page - Add record Dialog Box



The dialog box titled "Add Record" contains the following fields and controls:

- Index:** A text input field containing the value "0".
- Rule Action:** A dropdown menu with "No More Calls" selected.
- Threshold:** A text input field containing the value "40000".
- Hysteresis:** A text input field containing the value "1000".
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

The figure above shows an example where if the bandwidth for this Media Realm reaches 41,000 Bps (i.e., 40,000 plus 1,000 hysteresis), the device blocks any additional calls. If the bandwidth later decreases to 39,000 Bps (i.e., 40,000 minus 1,000 hysteresis), the device allows additional calls.

4. Configure the parameters as required. See the table below for a description of each parameter.
5. Click **Submit** to apply your settings.
6. Reset the device for your settings to take effect.

Bandwidth Management Parameter Descriptions

Parameter	Description
Index [BWManagement_ThresholdIndex]	Defines the index of the table row entry. This index determines the bandwidth threshold type for the rule: <ul style="list-style-type: none"> [0] High Threshold Rule [1] Critical Threshold Rule
Rule Action [BWManagement_RuleAction]	Defines the action that the device performs when the configured threshold is exceeded: <ul style="list-style-type: none"> [0] Report Only (default) [1] No more calls
Threshold [BWManagement_Threshold]	Defines the bandwidth threshold in bytes per second (Bps). The default is 0.
Hysteresis [BWManagement_Hysteresis]	Defines the bandwidth fluctuation (change) from the threshold value at which the device performs the configured action. The default is 0.

6.5.2.7.8 Media Security

The device supports Secured RTP (SRTP) according to RFC 3711. SRTP is used to encrypt RTP and RTCP transport for protecting VoIP traffic. SRTP requires a key exchange mechanism that is performed according to RFC 4568 – "Session Description Protocol (SDP) Security Descriptions for Media Streams". The key exchange is done by adding a 'crypto' attribute to the SDP. This attribute is used (by both sides) to declare the various supported cipher suites and to attach the encryption key. If negotiation of the encryption data is successful, the call is established.

SRTP supports the following cipher suites (all other suites are ignored):

- AES_CM_128_HMAC_SHA1_32
- AES_CM_128_HMAC_SHA1_80
- ARIA_CM_128_HMAC_SHA1_80
- ARIA_CM_192_HMAC_SHA1_80

When the device is the offering side, it generates an MKI of a size configured by the 'Master Key Identifier (MKI) Size' parameter. The length of the MKI is limited to four bytes. If the remote side sends a longer MKI, the key is ignored. The key lifetime field is not supported. However, if it is included in the key it is ignored and the call does not fail.

The device supports the following session parameters (as defined in RFC 4568, SDP Security Descriptions for Media Streams):

- UNENCRYPTED_SRTP
- UNENCRYPTED_SRTCP
- UNAUTHENTICATED_SRTP

Session parameters should be the same for the local and remote sides. When the device is the offering side, the session parameters are configured by the following parameter - 'Authentication On Transmitted RTP Packets', 'Encryption On Transmitted RTP Packets', and 'Encryption On Transmitted RTCP Packets'. When the device is the answering side, the device adjusts these parameters according to the remote offering. Unsupported session parameters are ignored, and do not cause a call failure.

Below is an example of crypto attributes usage:

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:PsKoMpHlCg+b5X0YLuSvNrImEh/dAe
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:IsPtLoGkBf9a+c6XVzRuMqHlDnEiAd
```

The device also supports symmetric MKI negotiation, whereby it can be configured to forward the MKI size received in the SDP offer crypto line in the SDP answer crypto line.

To configure the device's mode of operation if negotiation of the cipher suite fails, use the 'Media Security Behavior' parameter. This parameter can be set to enforce SRTP, whereby incoming calls that don't include encryption information are rejected.

**Notes:**

- For a detailed description of the SRTP parameters, refer to the SRTP Parameters in the Product Reference Manual.
- When SRTP is used, the channel capacity may be reduced.

➤ **To configure Media Security:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** > Media Security).

Figure 71: Configuring Media Security

General Media Security Settings		
Media Security	Disable	
Aria Protocol Support	Disable	
Media Security Behavior	Preferable	
Authentication On Transmitted RTP Packets	Active	
Encryption On Transmitted RTP Packets	Active	
Encryption On Transmitted RTCP Packets	Active	
SRTP Setting		
Master Key Identifier (MKI) Size	0	
Enable symmetric MKI negotiation	Disable	
SRTP offered Suites		
CIPHER SUITES AES CM 128 HMAC SHA1 80	<input checked="" type="checkbox"/>	
CIPHER SUITES AES CM 128 HMAC SHA1 32	<input checked="" type="checkbox"/>	
CIPHER SUITES ARIA CM 128 HMAC SHA1 80	<input checked="" type="checkbox"/>	
CIPHER SUITES ARIA CM 192 HMAC SHA1 80	<input checked="" type="checkbox"/>	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see Saving Configuration on page 125.

6.5.2.8 Quality of Experience

The following describes the Quality of Experience configuration.

6.5.2.8.1 Session Experience Manager Server

The device can be configured to report voice (media) quality of experience to AudioCodes Session Experience Manager (SEM) server, a plug-in for AudioCodes EMS. The reports include real-time metrics of the quality of the actual call experience and processed by the SEM.



Notes:

- To support this feature, the device must be installed with the relevant Software License Key.
- To configure the parameters to report and their thresholds per Media Realm, see Refer to Configuring QoE per Media Realm on page 108.
- For information on the SEM server, refer to the *EMS User's Manual*.

➤ **To configure QoE reporting of media:**

1. Open the Session Experience Manager Server page (**Configuration** tab > **VoIP** menu > **Quality of Experience** > **Session Experience Manager Server**).

Figure 6-72: Media Quality of Experience Page

Session Experience Manager Server	
Server IP	0.0.0.0
Redundant Server IP	0.0.0.0
Port	5000
Interface Name	OAMP

2. Configure the parameters as required
 - Server Ip (QOEServerIP) - defines the IP address of the SEM server
 - Redundant Server IP
 - 'Port' (QOEPort) - defines the port of the SEM server
 - 'Interface Name' (QOEInterfaceName) - defines the device's IP network interface on which the SEM reports are sent
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see Saving Configuration on page 125.

The device can be configured to report voice (media) quality of experience to AudioCodes Session Experience Manager (SEM) server, a plug-in for AudioCodes EMS. The reports include real-time metrics of the quality of the actual call experience and processed by the SEM.


Notes:

- To support this feature, the device must be installed with the relevant Software License Key.
- To configure the parameters to report and their thresholds per Media Realm, see Configuring QoE per Media Realm on page 108.
- For information on the SEM server, refer to the EMS User's Manual.

6.5.2.9 Call Control

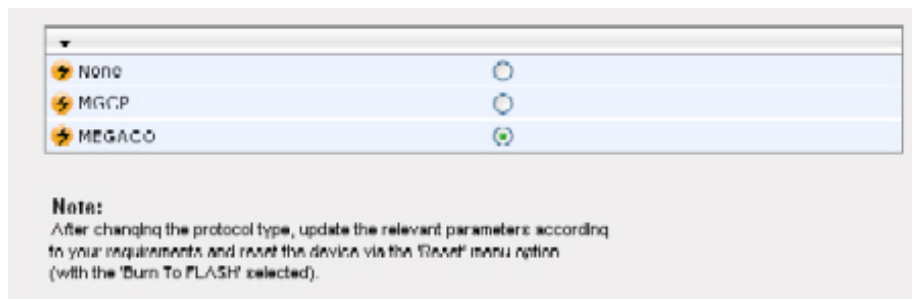
Call Control menu options are described below.

6.5.2.9.1 Protocol Selection

➤ **To select the Control Protocol Type:**

1. Open the Control Protocol Selection page (**Configuration** tab > **VoIP** menu > **Call Control** > **Protocol Selection**).

Figure 73: Protocol Selection



2. Click the radio button of the required protocol.



Note: Changing the protocol type requires a device reset. When you have completed configuring the required parameters, the device must be reset using the Reset screen for the changes to be implemented.

6.5.2.9.2 Control Interface Settings

Control Interface Settings enable the user to configure several gateway parameters with the option to partition a physical gateway into several virtual gateways. If only one gateway configuration is present, the gateway operates without Virtual Gateway separation.



Note: At least one gateway must be configured. If none are configured, a default configuration will be created on startup.

➤ **To configure Control Interface Settings:**

1. Open the Virtual GW Config Table page (**Configuration** tab > **VoIP** menu > **Call Control** > **Control Interface Settings**); the Virtual GW Config Table appears.
2. Click **Add**; the following screen appears:

Figure 74: MEGACO Control Interface Settings

Add Record	
Index	0
Virtual GW Name	
IPv4 Interface Name	DEFAULT
IPv6 Interface Name	DEFAULT
Local Port	2944
Associated Members List	
Service Change Profile	TGW
Megaco Version	2
Message Identifier	
Media Realm Name	
Load Weight	1
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure the gateway parameters for this virtual gateway.
4. Click **Submit**.

6.5.2.9.3 Basic Configuration

➤ **To configure the Basic Configuration:**

1. Open the MEGACO Basic Protocol Settings page (Configuration tab > VoIP menu > Call Control > Basic Configuration).

Figure 75: MEGACO Basic Protocol Settings

Naming Parameters	
SDP Session Owner	-
Physical Name Pattern	A*
Logical RTP Name Pattern	rtpp/*
Control IP Diff Serv	0

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Basic Configuration parameter fields in the 'Basic Configuration' page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

6.5.2.9.4 General Parameters

➤ **To configure the General Parameters:**

1. Open the MEGACO General Protocol Settings page (**Configuration** tab > **VoIP** menu > **Call Control** > **General Parameters**).

Figure 76: General Protocol Settings - MEGACO

Profile	
SDP Profile	
▼ Codex Settings	
Default Codex	PCMU
Default Packetization Period	20
▼ ID Parameters	
Randomize Transaction ID	Yes
Transaction ID Base	2000
Transaction ID Range	999997999
Physical Start Number	0
RTP Start Number	0
Context ID Offset	0
▼ Service Change Parameters	
Restart Maximum Waiting Delay	2500
▼ Misc. Parameters	
Reject Non-Provisioned MGCS	Yes
Trunking To Analog Profile	Disable

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the General Parameters, in the General Parameters page.

3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.
4. When clicking on the SDP Profile icon, the SDP Profile page appears. The user can check one or more of the following options.

Figure 77: SDP Profile - MEGACO

SDP Profile	
Support RFC3407	<input type="checkbox"/>
Support V.152 (VBD)	<input type="checkbox"/>
Support RFC3264	<input type="checkbox"/>
Strict Negotiation	<input type="checkbox"/>
T,S,O Lines Display	<input type="checkbox"/>
10ms PTIME for transparent coder	<input type="checkbox"/>
Always reply with Local SDP	<input type="checkbox"/>
Use G711 as Bypass coder	<input type="checkbox"/>
Symmetric payloads	<input type="checkbox"/>
Use Audio port for T38 call	<input type="checkbox"/>
Do not reject command with illegal PTIME	<input type="checkbox"/>
Default FAX mode is T38 relay	<input type="checkbox"/>
Prefer local coder in SDP coder negotiation	<input type="checkbox"/>

6.5.2.9.5 Channel Configuration

➤ **To configure the Channel Configuration:**

1. Open the MEGACO Channel Protocol Settings page (**Configuration** tab > **VoIP** menu > **Call Control** > **Channel Configuration**).

Figure 78: Channel Protocol Settings - MEGACO

Digit Map Parameters	
Default Digit Map	<input type="text"/>
Default Digit Map Name	<input type="text"/>
Digit Map Timeout [sec]	-1
Short Timer [msec]	-1
Long Timer [msec]	-1
DTMF Signal Parameters	
DTMF Signal Time Duration [msec]	100
DTMF Signal Interval Duration [msec]	100
RTP Parameters	
Transparent Coder Payload Type	-1
Media Channels Parameters	
TDM Hair-Pinning Mode	0

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Channel Protocol Settings, in the Channel Protocol Settings page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

6.5.2.9.6 Advanced Configuration

➤ To configure the Advanced Configuration:

1. Open the MEGACO Advanced Protocol Settings page (**Configuration** tab > **VoIP** menu > **Call Control** > **Advanced Protocol Settings**).

Figure 79: Advanced Protocol Settings

Communication Parameters	
Enable Keep Alive	Disable
Keep Alive Interval [sec]	12
Retransmission Timeout [msec]	200
Communication Layer Timeout [sec]	30
Target MG Response Time	200
MG Execution Time	100
MGC Execution Time	100
MG Provisional Response Time	100
MGC Provisional Response Time	100

Profiles	
SDP Negotiation Profile	132746
⚡ Compatibility Profile	296704

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Advanced Protocol Settings, in the Advanced Protocol Settings page.
3. After configuring/modifying the parameter fields, click Submit. The changes are entered into the system and the page is refreshed.

6.5.2.9.7 Media Services

➤ **To configure the Media Services:**

1. Open the MEGACO Media Server Settings page (**Configuration** tab > **VoIP** menu > **Call Control** > **Media Server Settings**).

Figure 80: Media Server Settings - MEGACO

▼ IVR	
Media Server Profile	0
APS IP Address	0.0.0.0
APS Port	0
APS Heartbeat Interval	100
Primary Language	APM BELGDUTCH
Secondary Language	APM BELGDUTCH
Advanced Audio Signals Profile	TD-51
Enable Voice Streaming	Disable
Voice Stream Upload Method	POST
Voice Stream Upload Post URI	/audioupload/servlet/AcAudioUpload
▼ Trunk Testing	
VXML Trunk Testing URL	
VXML File Name	
Enable VXML	Disable
Enable Trunk Testing Tones	Disable
▼ Conference Parameters	
Max Number Of Simultaneous Speakers	3
Max Number Of Participants	3
Enable Conference Signal Generation	Enable
▼ Provisioned Pools Size	
Provisioned Conf Size	50
Provisioned BCT Size	60
Provisioned Audio Size	60
Provisioned Trunk Testing Size	60

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the Media Server Settings, in the Media Server Settings page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

6.6 Maintenance

The Maintenance tab contains the following sub-menus:

- Maintenance - Refer to Maintenance on page 122
- Software Update - Refer to Software Update on page 126

6.6.1 Maintenance

6.6.1.1 Maintenance Actions

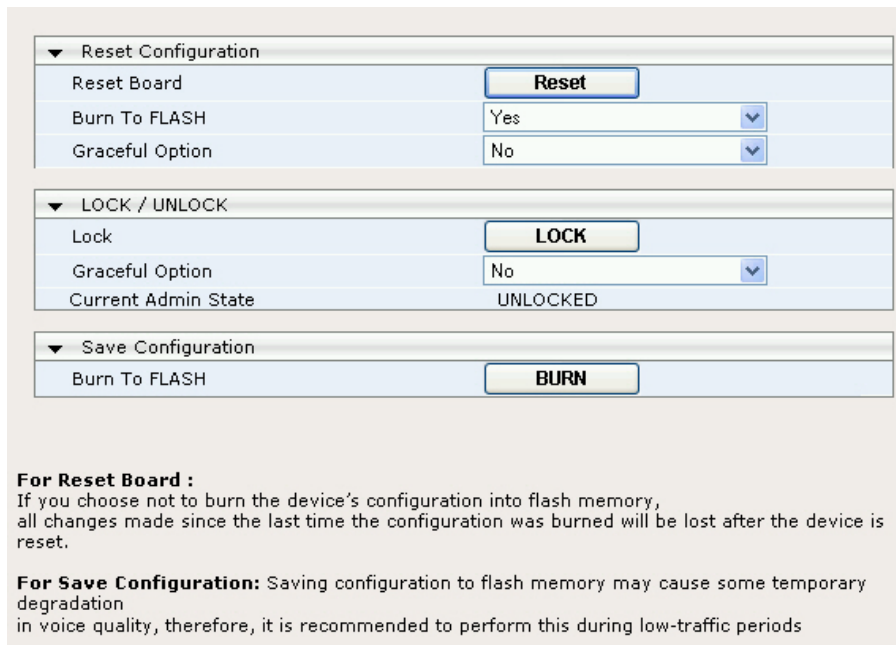
The 'Maintenance Actions' page allows you to perform the following operations:

- Reset the device (refer to Resetting the Device on page 123)
- Lock and unlock the device (refer to 'Locking and Unlocking the Device on page 124)
- Save the configuration to the device's flash memory (refer to Saving Configuration on page 125)

➤ **To access the Maintenance Actions page:**

- Open the Maintenance Actions page (**Maintenance** tab > **Maintenance Actions** menu).

Figure 81: Maintenance Actions



The screenshot displays the 'Maintenance Actions' page with three main sections:

- Reset Configuration:** Includes a 'Reset Board' button, a 'Burn To FLASH' dropdown set to 'Yes', and a 'Graceful Option' dropdown set to 'No'.
- LOCK / UNLOCK:** Includes a 'Lock' button, a 'Graceful Option' dropdown set to 'No', and a 'Current Admin State' label showing 'UNLOCKED'.
- Save Configuration:** Includes a 'Burn To FLASH' button labeled 'BURN'.

For Reset Board :
If you choose not to burn the device's configuration into flash memory, all changes made since the last time the configuration was burned will be lost after the device is reset.

For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods

6.6.1.1.1 Resetting the Device

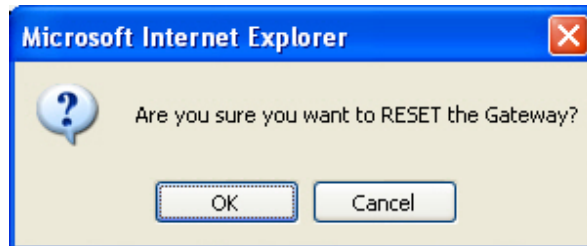
The 'Maintenance Actions' page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

- Save the device's current configuration to the device's flash memory (non-volatile).
- Perform a graceful shutdown, i.e., device reset starts only after a user-defined time expires (i.e., timeout) or after no more active traffic exists (the earliest thereof).

➤ **To reset the device:**

1. Open the 'Maintenance Actions' page (refer to Maintenance Actions on page 122).
2. Under the 'Reset Configuration' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
 - 'Yes': The device's current configuration is saved (burned) to the flash memory prior to reset (default).
 - 'No': Resets the device without saving the current configuration to flash (discards all unsaved modifications).
3. Under the 'Reset Configuration' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': Reset starts only after the user-defined time in the 'Shutdown Timeout' field (refer to Step 4) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': Reset starts regardless of traffic, and any existing traffic is terminated at once.
4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to 'Yes'), enter the time after which the device resets. Note that if no traffic exists and the time has not yet expired, the device resets.
5. Click Reset; a confirmation message box appears, requesting you to confirm.

Figure 82: Reset Confirmation Message Box



6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to 'Yes' (in Step 3), the reset is delayed and a page displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.



Notes:

- Throughout the Web interface, parameters preceded by the lightning ⚡ symbol are not applied on-the-fly to the device and require that you reset the device for them to take effect.
- If you modify parameters that only take effect after a device reset, after you click Submit, the toolbar displays the word 'Reset' (refer to Toolbar) to remind you to later reset the device.

6.6.1.1.2 Locking and Unlocking the Device

The Lock and Unlock options allow you to lock the device so that it doesn't accept any new incoming calls. This is useful when, for example, you are uploading new software files to the device and you don't want any traffic to interfere with the process.

➤ **To lock the device:**

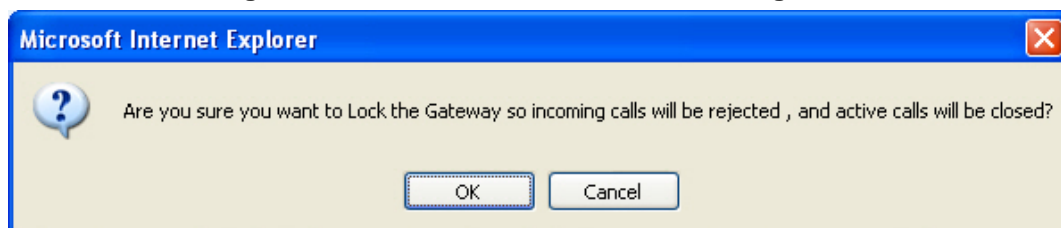
1. Open the 'Maintenance Actions' page (refer to Maintenance Actions on page 122).
2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': The device is 'locked' only after the user-defined time in the 'Lock Timeout' field (refer to Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': The device is 'locked' regardless of traffic. Any existing traffic is terminated immediately.



Note: These options are only available if the current status of the device is in the Unlock state.

3. In the 'Lock Timeout' field (relevant only if the parameter 'Graceful Option' in the previous step is set to 'Yes'), enter the time (in seconds) after which the device locks. Note that if no traffic exists and the time has not yet expired, the device locks.
4. Click **LOCK**; a confirmation message box appears requesting you to confirm device Lock.

Figure 83: Device Lock Confirmation Message Box



5. Click OK to confirm device Lock; if 'Graceful Option' is set to 'Yes', the lock is delayed and a page displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The 'Current Admin State' field displays the current state: LOCKED or UNLOCKED.

➤ **To unlock the device:**

1. Open the 'Maintenance Actions' page (refer to Maintenance Actions on page 122).
2. Under the 'LOCK / UNLOCK' group, click UNLOCK. Unlock starts immediately and the device accepts new incoming calls.

6.6.1.1.3 Saving Configuration

Changes made on the Web interface are volatile (in RAM). Changes to parameters with on-the-fly capabilities are immediately available, while other parameters (preceded by the lightning ⚡ symbol) are updated only after a device reset. Parameters that are only saved to the volatile memory, revert to their previous settings after a power failure or hardware reset.

To save changes so they are available after a power failure, you must save the changes to the non-volatile memory (flash). When the configuration is saved, all parameters and loaded files are saved to the non-volatile memory.

➤ **To save the changes to the non-volatile memory:**

1. Open the 'Maintenance Actions' page (refer to Maintenance Actions on page 122).
2. Under the 'Save Configuration' group, click BURN; a confirmation message appears when the configuration successfully saves.



Notes:

- Saving configuration to the non-volatile memory may disrupt traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (refer to Locking and Unlocking the Device on page 124).
- Throughout the Web interface, parameters preceded by the lightning ⚡ symbol are not applied on-the-fly to the device and require that you reset the device (refer to Resetting the Device on page 123) for them to take effect.

6.6.2 Software Update



Notes:

- Before upgrading a cmp version, verify that your license key supports the new cmp version. The most recent cmp version supported by the feature key can be viewed via the Web (Software Update -> Software Upgrade Key) or by the VoPLib (getlicensekey).
- If you upgraded your CMP and the "SW version mismatch" message appears in the Syslog or Web interface, you know that your license key does not support the new CMP version. Contact AudioCodes support for assistance.
- In addition, the Software Upgrade Key screen is provided for users to enter their updated Software Upgrade keys.

The Software Update menu offers two options for downloading current software update files: the Software Upgrade Wizard and Load Auxiliary Files page. In addition, the Software Upgrade Key page is provided for users to enter their updated Software Upgrade keys and the Configuration File page is used to save the current configuration or upload a new one.

- Load Auxiliary Files - Refer to Load Auxiliary Files on page 126.
- Software Upgrade Key - Refer to 'Software Upgrade Key' on page 127.
- Software Upgrade Wizard - Refer to Software Upgrade Wizard.
- Configuration File - Refer to Configuration File on page 130.


6.6.2.1 Load Auxiliary Files

The Auxiliary Files Download page facilitates the download of software updates using the HTTP protocol.

➤ To download an auxiliary file:

1. Open the Load Auxiliary Files page (Maintenance tab > Software Update menu > Load Auxiliary Files).

Figure 84: Load Auxiliary Files



2. Use the **Browse** button to locate the appropriate file on your PC.
3. Click **Send File**. The files are sent to the device.
4. To commit the changes to the non-volatile (flash) memory, click on the Burn button on the Toolbar.



Note: A device reset is required to activate a loaded CPT file, and may be required for the activation of certain ini file parameters. The Burn option must be selected.

6.6.2.2 Software Upgrade Key

The device is loaded with a Software Upgrade Key already pre-configured for each of its TrunkPack Modules.

Users can later upgrade their device features, capabilities and quantity of available resources by specifying the upgrades they require and the corresponding blade's or TPM's serial number (or MAC address), and ordering a new key to match their specification.

The Software Upgrade Key is sent as a string in a text file, to be loaded into the device. Stored in the device's non-volatile flash memory, the string defines the features and capabilities allowed by the specific key purchased by the user. The device allows users to utilize only these features and capabilities. A new key overwrites a previously installed key.



Note: The Software Upgrade Key is an encrypted key provided by AudioCodes only.

6.6.2.2.1 Backing up the Current Software Upgrade Key

Back up your current Software Upgrade Key before loading a new key to the device. You can always reload this backed-up key to restore your device capabilities to what they originally were if the 'new' key does not comply with your requirements.

➤ **To back up the current Software Upgrade Key:**

1. Open the Software Upgrade Key page (**Maintenance** tab > **Software Update** menu > **Software Upgrade Key**).
2. Copy the string from the Current Key field and paste it in a new file.
3. Save the text file with a name of your choosing.

6.6.2.2.2 Loading the Software Upgrade Key

After receiving the Software Upgrade Key file (do not modify its contents in any way), ensure that its first line is [LicenseKeys] and that it contains one or more lines in the following format:

S/N<Serial Number of TrunkPack module> = <long Software Upgrade Key>

For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

One S/N must match the S/N of your device TrunkPack module. The device's S/N can be viewed in the Device Information page (refer to 'Device Information' on page 140).

You can load a Software Upgrade Key using:

- The Web interface (refer to Loading the Software Upgrade Key Using the Web Interface below).
- BootP/TFTP startup (refer to 'Loading the Software Upgrade Key Using BootP/TFTP' on page 128).
- AudioCodes' EMS (refer to the EMS User's Manual or EMS Product Description).

Figure 85: Software Upgrade Key Status

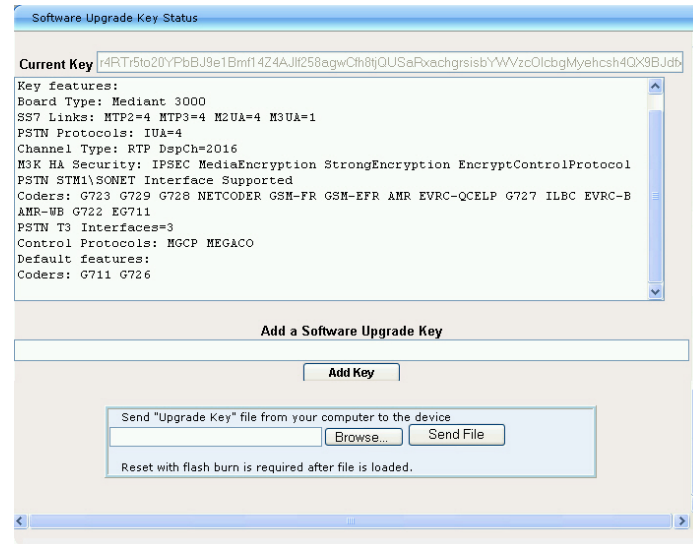
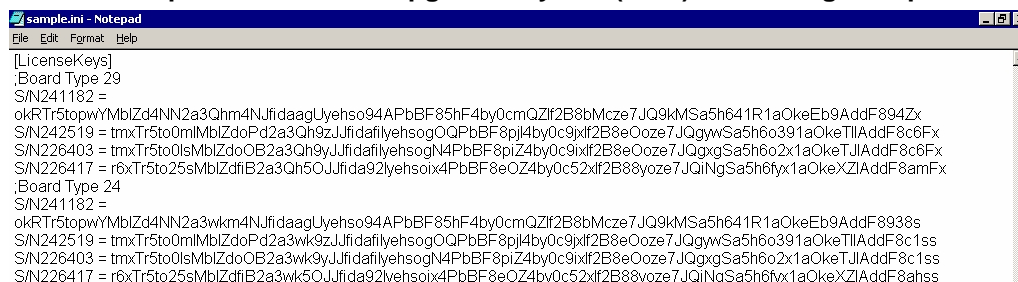


Figure 86: Example of a Software Upgrade Key File (*.out) Containing Multiple S/N Lines



6.6.2.2.3 Loading the Software Upgrade Key Using BootP/TFTP

- **To load the Software Upgrade Key file using BootP/TFTP:**
 1. Place the file in the same location you've saved the device's cmp file. Note that the extension of the Software Upgrade Key must be ini.
 2. Start your BootP/TFTP configuration utility and edit the client configuration for the device.
 3. Select the Software Upgrade Key file instead of the device's ini file.
 4. Reset the device; the device's cmp and Software Upgrade Key files are loaded to the device.

6.6.2.2.4 Verifying that the Key was Successfully Loaded

After installing the key, you can determine in the Web interface's read-only 'Key features:' panel (Software Update menu > Software Upgrade Key) that the features and capabilities activated by the installed string match those that were ordered. Refer to the Software Upgrade Key Status page above.

You can also verify that the key was successfully loaded to the device by accessing the Syslog server. When a key is successfully loaded, the following message is issued in the Syslog server:

"S/N____ Key Was Updated. The Board Needs to be Reloaded with ini file\n"

6.6.2.2.5 Troubleshooting an Unsuccessful Loading of a License Key

If the Syslog server indicates that a Software Upgrade Key file was unsuccessfully loaded (the SN_ line is blank), take the following preliminary actions to troubleshoot the issue:

- Open the Software Upgrade Key file and verify that the S/N line of the specific device whose key you want to update is listed in it. If it isn't, contact AudioCodes.
- Verify that you've loaded the correct file and that you haven't loaded the device's ini file or the CPT ini file by mistake. Open the file and ensure that the first line is [LicenseKeys].
- Verify that you did not alter in any way the contents of the file.

6.6.2.2.6 Abort Procedure

Reload the key you backed-up in 'Backing up the Current Software Upgrade Key' on page 127 to restore your device capabilities to what they originally. To load the backed-up key use the procedure described in 'Loading the Software Upgrade Key' on page 127.

6.6.2.1 Software Upgrade Wizard

The Software Upgrade Wizard allows the user to upgrade the device's software by loading a new *.cmp file together with a full suite of useful auxiliary files.

Loading a *.cmp file is mandatory in the Software Upgrade Wizard process. During the process, you choose from the auxiliary files provided for loading. For each auxiliary file type, you can choose between reloading an existing file, loading a new file or not loading a file at all.

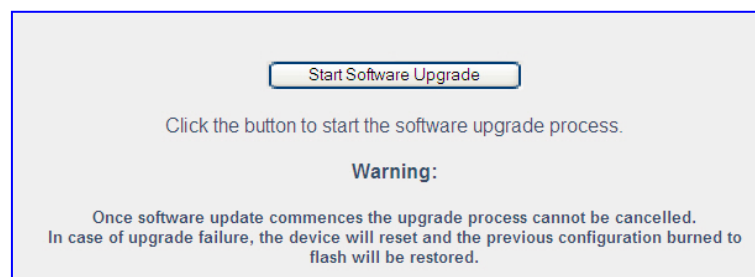
➤ **To use the Software Upgrade Wizard:**



Note: The Software Upgrade Wizard requires the device to be reset at the end of the process, which disrupts any existing traffic on the device. To avoid disrupting traffic, disable all traffic on the device before initiating the Software Upgrade Wizard.

1. Stop all traffic on the device (refer to the note above.)
2. Open the Software Upgrade Wizard page (**Maintenance** tab > **Software Update** menu > **Software Upgrade Wizard**).

Figure 87: Software Upgrade Wizard

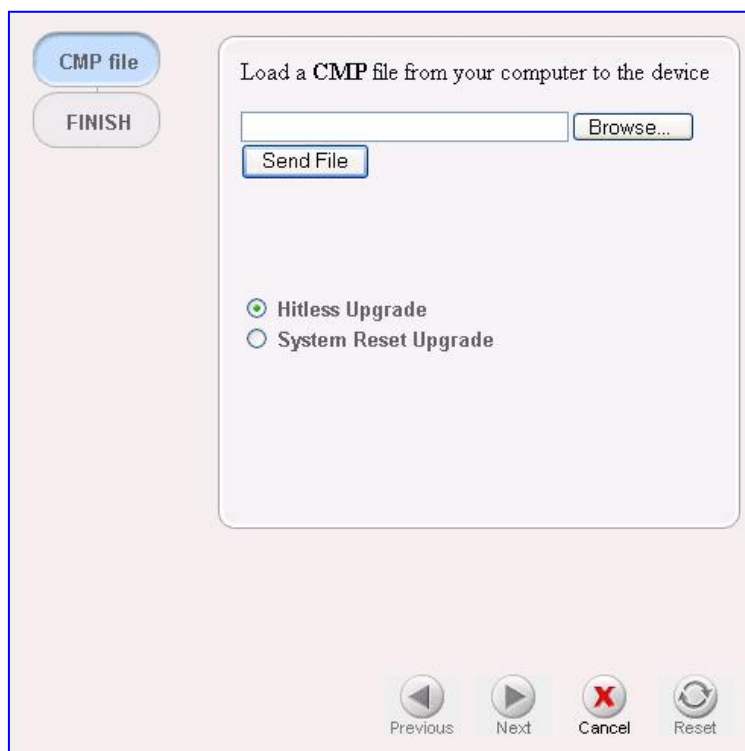


3. Click **Start Software Upgrade** to initiate the upgrade process. The File Loading page appears displaying the cmp file information. The background Web page is disabled. During the Software Upgrade process, the rest of the Web application is unavailable. After the Software Upgrade process has completed, access to the full Web application is restored.

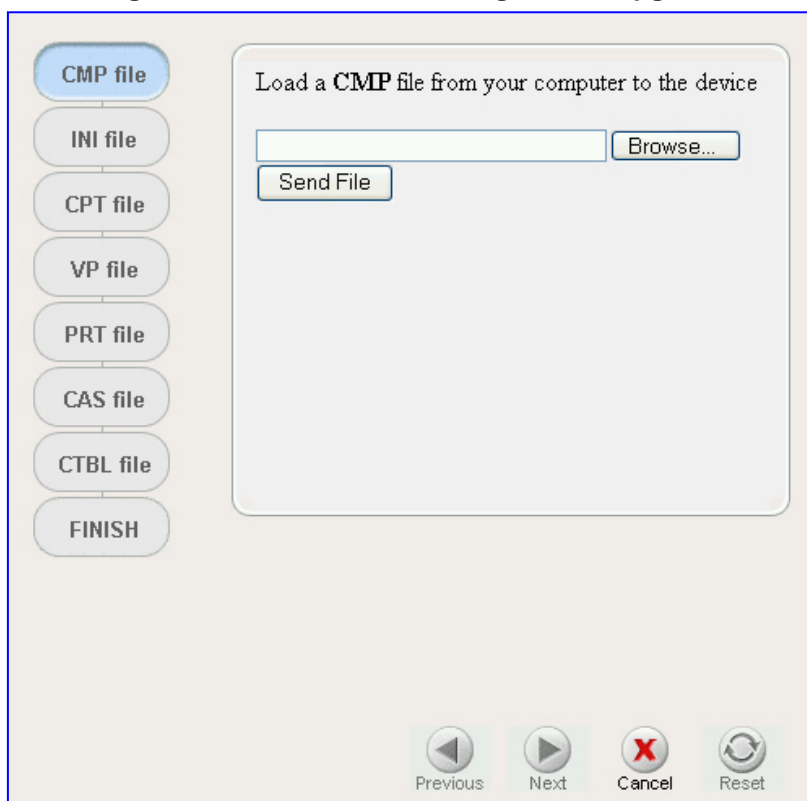


Note: At this point you may cancel the Software Upgrade process with no consequence to the device by using the cancel button. If you continue with the Software Upgrade process by clicking the Start Software Upgrade button, the process must be followed through and completed with a device reset at the end of the process. If you use the Cancel button, in any of the subsequent screen pages, the Software Upgrade process causes the device to be reset.

4. The software upgrade page will allow the user to choose between two upgrade modes before uploading a new CMP: Hitless and System-Reset (common for non-Mediant 3000 devices).

Figure 88: Load CMP File Dialog - Hitless

The dialog box for loading a CMP file for a hitless upgrade. It features a sidebar on the left with 'CMP file' (highlighted) and 'FINISH' buttons. The main area contains the instruction 'Load a CMP file from your computer to the device', a text input field, a 'Browse...' button, and a 'Send File' button. Below this, there are two radio buttons: 'Hitless Upgrade' (selected) and 'System Reset Upgrade'. At the bottom, there are four navigation buttons: 'Previous', 'Next', 'Cancel' (with a red X), and 'Reset' (with a circular arrow icon).

Figure 89: Load CMP File Dialog - Reset Upgrade

The dialog box for loading a CMP file for a system reset upgrade. It features a sidebar on the left with buttons for 'CMP file', 'INI file', 'CPT file', 'VP file', 'PRT file', 'CAS file', 'CTBL file', and 'FINISH'. The main area contains the instruction 'Load a CMP file from your computer to the device', a text input field, a 'Browse...' button, and a 'Send File' button. At the bottom, there are four navigation buttons: 'Previous', 'Next', 'Cancel' (with a red X), and 'Reset' (with a circular arrow icon).



Note: In Hitless mode, the user will be able to only upload a CMP file (no other auxiliary files will be available for upload at this stage). When the Finish button is clicked, a 3-stage process will begin. Each stage will be displayed to the user in the Web interface. When the Hitless process ends, the Home page will automatically be displayed.

Note the file type list in the left side of the page. This list contains the relevant file types that can be loaded via the wizard for this device type. The highlighted entry in the file type list indicates which file type is being displayed in the main part of the page. As you continue through the Software Upgrade process by clicking on the Next button, each of the relevant file type pages are presented, going down the list until the Finish page appears.



Note: The **Next** button is disabled until you load a *.cmp file. After a *.cmp file is selected, the wizard upgrade process continues and the Next button is enabled.

5. Click **Browse** and navigate to the location of the *.cmp file to be loaded. The path and file name appears in the field.
6. Click **Send File** to send the file to the device. The File Loading page appears with a progress bar indicating the loading period. When the loading is complete, a message is displayed indicated the file was successfully loaded into the device.

Figure 90: File Loading Dialog Screen



All four buttons (**Previous**, **Next**, **Cancel** and **Reset**) in the bottom portion of the page are activated.

7. You may choose between these options:
 - Loading Additional Auxiliary Files
 - Completing the Software Upgrade Process
 - Cancel Upgrade Process and revert to the Previous Configuration Files

8. Loading Additional Auxiliary Files

- To move to the next file type on the list to the left, click **Next**. The File Loading page appears with the next relevant file type highlighted.
- For each file type the user has three options:
 - ◆ Load a new auxiliary file to the device using the Browse and Send File button as described above.
 - ◆ Load the existing auxiliary file - A checkbox (checked by default as shown in the figure below) appears if relevant to the device. If this checkbox is checked, the existing file is used in the upgraded system.
 - ◆ Avoid loading any file at all - Clear the checkbox (if the checkbox appears).
- Continue through each of the file type pages by clicking Next and selecting one of the above options. As an example, the figure below displays the File Loading page with the CPT file type selected.

Figure 91: File Loading Dialog - INI Type Displayed

The screenshot shows a web interface for loading auxiliary files. On the left is a vertical list of file types: CMP file, INI file, CPT file, VP file, PRT file, CAS file, CTBL file, AMD file, and FINISH. The 'INI file' option is highlighted. The main area contains the text 'Load an *ini* file from your computer to the device' above a text input field and a 'Browse...' button. Below this is a 'Send File' button and a checked checkbox labeled 'Use existing configuration'. A warning message states: 'The Device will revert to default configuration if no configuration is chosen'. At the bottom are four navigation buttons: 'Previous' (left arrow), 'Next' (right arrow), 'Cancel' (X), and 'Reset' (circular arrow).

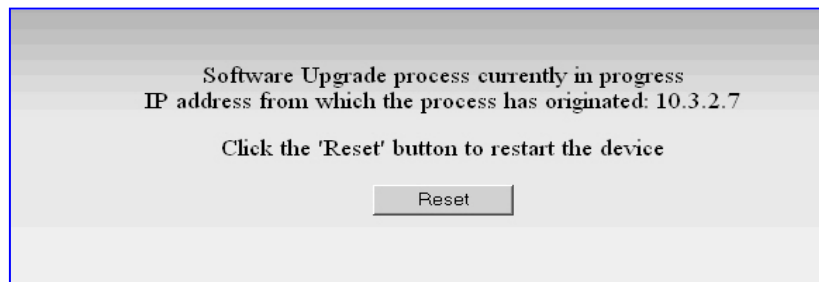
9. Completing the Software Upgrade Process:

- From any of the file type pages, you can complete the Software Upgrade process by clicking the Reset button. The device is reset utilizing the new files you have loaded up to that point, as well as using the existing files according to the checkbox status of each file type.

10. Revert to the Previous Configuration Files:

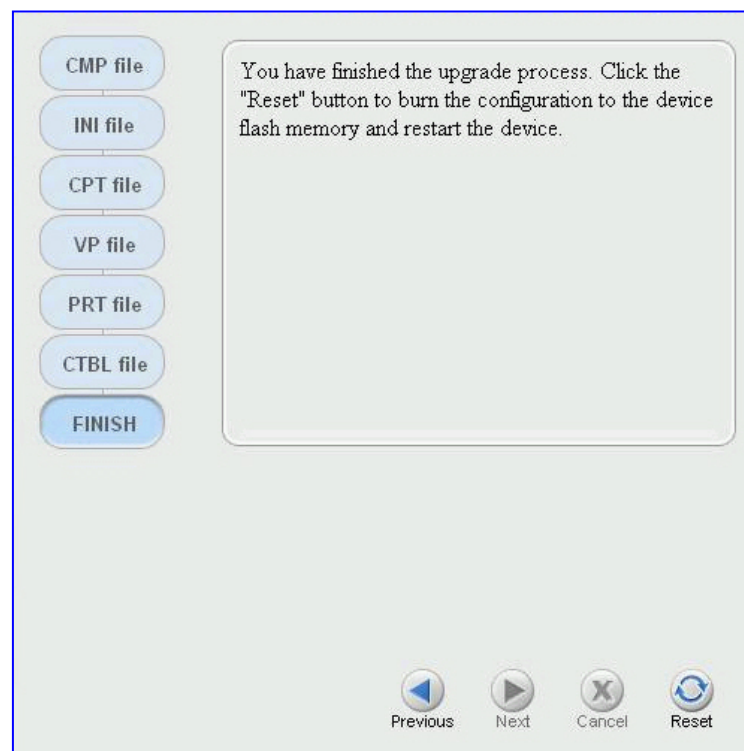
- From any of the file type pages, you can revert to the previous configuration by closing the File Loading Dialog page. The Software Upgrade process is terminated and the following page appears.

Figure 92: Software Upgrade Process



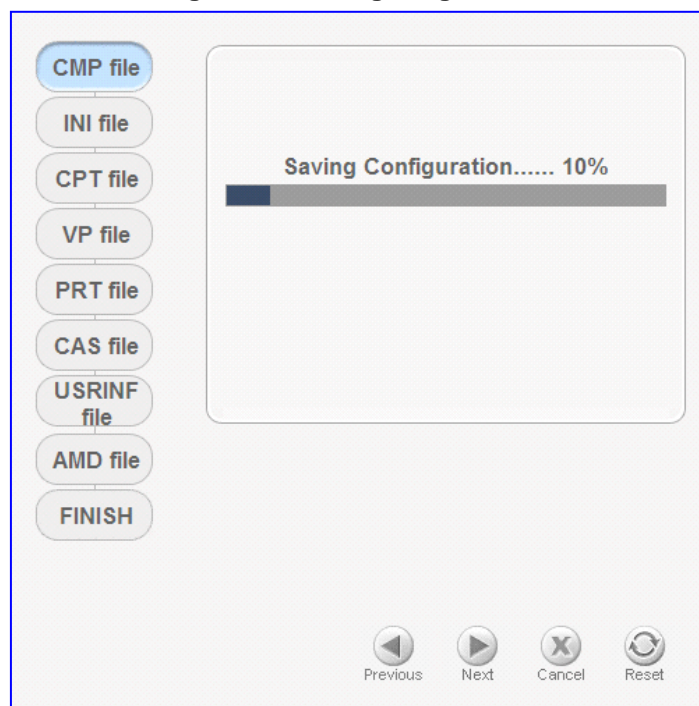
- Click the **Reset** button; the device is reset utilizing the previous configuration files.
11. When continuing through the Software Upgrade process, you complete the process from the Finish page by clicking the Reset button (the **Next** button is disabled).

Figure 93: File Loading Dialog Screen - Reset Button Stage



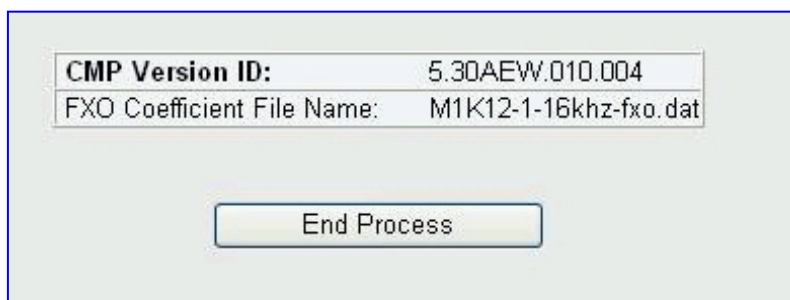
12. During the Reset process, the device 'burns' the newly loaded configuration to the non-volatile memory. The File Burning page appears displaying the File Burning to Flash Memory progress bar.

Figure 94: Saving Progress Bar



13. When this has completed, the Reset Device page appears displaying the Reset in progress bar. When this has completed, the End Of Process page appears displaying the current configuration information.

Figure 95: End of Process Dialog Screen



14. Click **End Process**.

6.6.2.2 Configuration File

The Configuration File page enables you to restore/change (download a new ini file to the Device) or backup the current configuration file that the device is using (make a copy of the VoIP device's ini file and store it in a directory on your PC).

- Restore your configuration - If the VoIP device has been replaced or has lost its programming information, you can restore the VoIP device configuration file from a previous backup or from a newly created ini file. To restore the VoIP device configuration from a previous backup you must have a backup of the VoIP device information stored on your PC. (For information about restoring ini file defaults or backup files, refer to 'Restoring and Backing Up the device Configuration'.)
- Back up your configuration - If you want to protect your VoIP device programming. The generated backup ini file contains values that have been set by the user or are other than the default values.



Note: The ini file generated on the Web interface contains only the set of parameters configurable on the Web interface. It is not possible to obtain a full backup in case the configuration may have been modified using other methods (e.g. uploading an ini file).

In the Configuration File page, you can bring an ini file from the device to a directory in your PC, and send the ini file from your PC to the device.

Protect the device configuration by bringing the ini file from the device to your PC. Later, if another device is replaced or loses its programming data, you'll be able to restore / send the ini file backed up on your PC to the device.

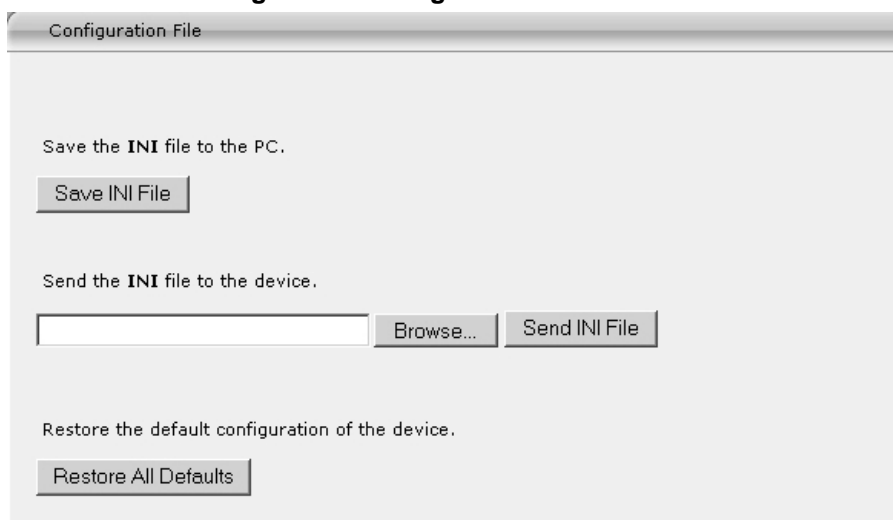
The ini file is a proprietary configuration text file containing configuration parameters and data. Sending the ini file to the device only provisions parameters that are contained in the ini file.

The ini file with parameters set at their default values is on the CD accompanying the device. The ini file can also be received as an e-mail attachment from AudioCodes' Technical Support. Users can also generate their own ini file using AudioCodes' DConvert utility (refer to the Utilities chapter in the Product Reference Manual).

➤ To save the ini file to the PC:

1. Open the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

Figure 96: Configuration File Screen



2. Click **Save ini File**. You are prompted to select a location in which to save it.



Note: The ini file that you save from the device to the PC contains only those parameters whose values you modified following receipt of the device. It does not contain parameters unchanged at their (original) default value.

In addition, the ini file generated on the Web interface contains only the set of parameters configurable on the Web interface. It is not possible to obtain a full backup in case the configuration may have been modified using other methods (e.g. uploading an ini file).

➤ **To load an ini file from the PC to the device:**

1. Click **Browse** next to the **Send INI File** button and navigate to the location of the predefined ini file. Refer to the figure below.
2. Click **Send INI File**. The file loading process is activated. When the loading is complete, a verification message is displayed at the bottom of the page: File XXXX was successfully loaded into the device.
3. From the Toolbar, select **Device Actions** and click **Reset**. The Reset page appears.
4. Select the **Burn** option and click **Reset**. Wait for the device to reset. After self-testing, the Ready and LAN LEDs on the device's front panel are lit green. Any malfunction causes the Ready LED to change to red.

Users can restore default parameters by clicking the **Restore All Defaults** button.

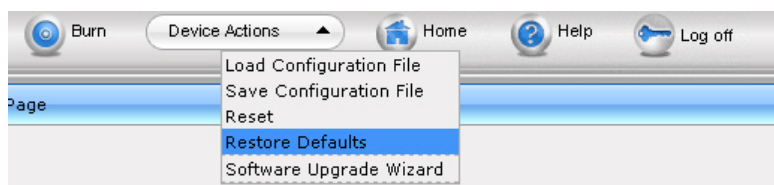
6.6.2.2.1 Downloading ini file with SS7 Configuration

➤ **To download ini file (after blade startup) with SS7 configuration:**

1. Click on the Device Actions drop-down menu on the Toolbar and select the Restore Defaults option.



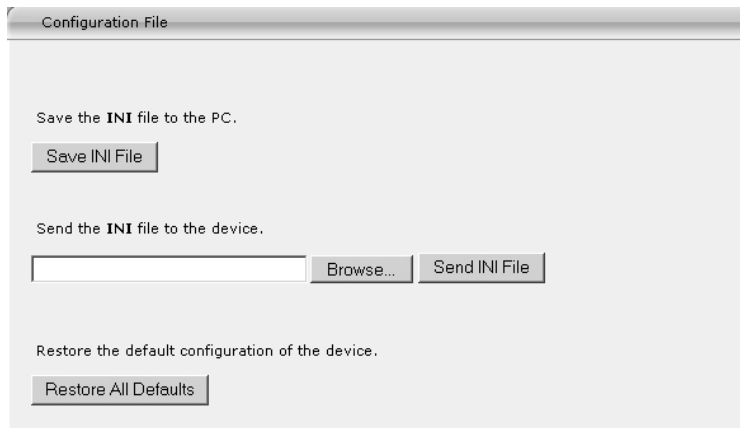
Note: The Restore Defaults option MUST be selected in order to successfully complete this process.



2. The Configuration File page appears. Click on the **Restore All Defaults** button.
3. Click on the **Browse** button and navigate to the appropriate folder in order to select the ini file.

4. Click the **Open** button on the Choose File page.

Figure 97: Configuration File



Configuration File

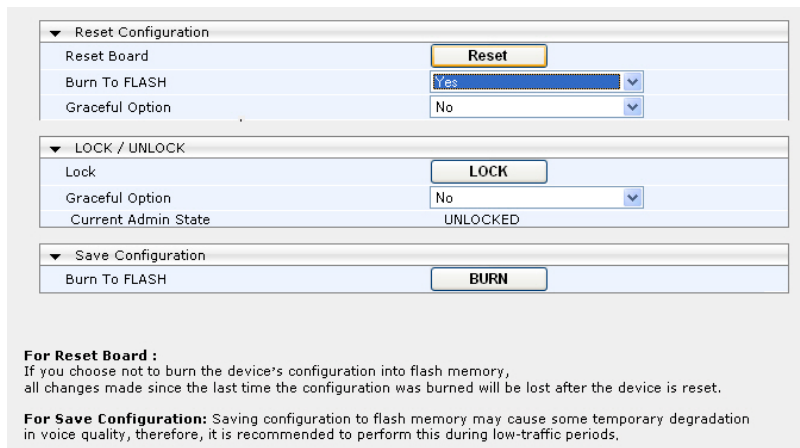
Save the **INI** file to the PC.

Send the **INI** file to the device.

Restore the default configuration of the device.

5. When the file has been selected, click on the Send INI File button to load the file from the PC to the device. The file loading process is activated. When the loading is complete, a verification message is displayed at the bottom of the page: File XXXX was successfully loaded into the device.
6. Select the **Device Actions** and then **Reset**. On the next Maintenance Actions page, ensure the Burn to Flash option under Reset Configuration, is set to **Yes**.

Figure 98: Maintenance Actions



▼ Reset Configuration

Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	<input type="button" value="Yes"/>
Graceful Option	<input type="button" value="No"/>

▼ LOCK / UNLOCK

Lock	<input type="button" value="LOCK"/>
Graceful Option	<input type="button" value="No"/>
Current Admin State	UNLOCKED

▼ Save Configuration

Burn To FLASH	<input type="button" value="BURN"/>
---------------	-------------------------------------

For Reset Board :
If you choose not to burn the device's configuration into flash memory, all changes made since the last time the configuration was burned will be lost after the device is reset.

For Save Configuration: Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods.

7. Click **Reset**. The new configuration will take effect once the blade has been loaded.

6.7 Status and Diagnostic Menu

➤ To access the Status and Diagnostics menu:

1. To access the Status & Diagnostics page, click on the **Status & Diagnostics** button on the Navigation Bar. The Status & Diagnostics appear in the Navigation Tree displaying the following menu options:
 - System Status
 - Message Log - Refer to Message Log on page 139
 - Device Information - Refer to Device Information on page 140
 - Ethernet Port Information - Refer to Ethernet Port Information on page 141
 - Carrier-Grade Alarms
 - ◆ Active Alarms - Refer to Active Alarms on page 141
 - Performance Monitoring
 - Trunk Utilization - Refer to Viewing Trunk Utilization
 - Viewing MOS per Media Realm - Refer to Viewing MOS per Media Realm
 - VoIP Status
 - Trunk & Channel Status - Refer to Trunk & Channel Status
 - IP Interface Status - Refer to IP Interface Status on page 143
 - Performance Statistics - Refer to Performance Statistics on page 144
 - Timing Module Information - Refer to Timing Module Information
 - Components Status - Refer to Components Status

6.7.1 System Status

6.7.1.1 Message Log

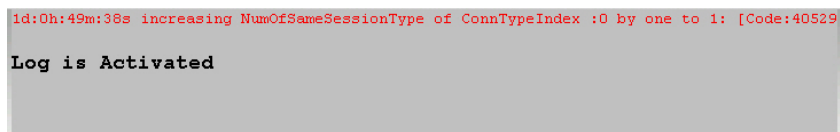
The Message Log is similar to a Syslog. It provides debug messages useful in pursuing troubleshooting issues.

The Message Log serves the Web Server and is similar to a Syslog server. It displays debug messages. It is not recommended to use the Message Log page for logging errors and warnings because errors can appear over a prolonged period of time, e.g., a device can display an error after running for a week. Similarly, it is not recommended to keep a Message Log session open for a prolonged period (refer to the Note below). For logging of errors and warnings, refer to 'Syslog'.

➤ To activate the Message Log:

1. Open the Message Log page (**Status & Diagnostics** tab > **System Status** menu > **Message Log**); the Message Log page is displayed and the log is activated.

Figure 99: Message Log Screen



2. After receiving messages - Using the scroll bar, select the messages, copy them and paste them into a text editor such as Notepad. Send this txt file to Technical Support for diagnosis and troubleshooting as needed.

3. To clear the page of messages, click on the sub-menu Message Log. The page is cleared. A new session is activated and new messages begin appearing.



Note: Do not keep the Message Log screen activated and minimized for a prolonged period as a long session may cause the PC workstation to overload. While the page is open (even if minimized), a session is in progress and messages are sent. Closing the window or moving to another link stops the messages and terminates the session.

6.7.1.2 Device Information

The Device Information page displays hardware, software device information and Device state information. This information can help you to expedite any troubleshooting process. Capture the page and email it to Technical Support personnel to ensure quick diagnosis and effective corrective action.

The page also displays any loaded files in the device.

➤ To display the Device Information page:

- Open the Device Information page (Status & Diagnostics tab > System Status menu > Device Information).

Figure 100: Device Information

▼ General Settings	
MAC Address:	00908f042b72
Serial Number:	273266
Board Type:	24
Device Up Time:	4d:4h:43m:22s:40th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [bytes]:	8388608
RAM Size [bytes]:	134217728
CPU Speed [MHz]:	200
▼ Versions	
Version ID:	5.80.010
DSP Type:	2
DSP Software Version:	58003
DSP Software Name:	624AE3
Flash Version:	192
Module FirmWare:	0x32
▼ Loaded Files	
Call Progress Tones File Name:	call_progress_defaults.dat Delete
Loaded Coder Table :	Default CODERTABLE

➤ To delete any loaded files:

1. From the toolbar, click on the **Status and Diagnostics** link. The Status and Diagnostics page appears.
2. From the navigation tree, click the **Device Information** link. The Device Information page appears.
3. In the Device Information table, click **Delete**. The file deletion takes effect only after a device reset is performed.
4. From the toolbar, click Device Actions followed by **Reset**. The Reset page appears.
5. Select the **Burn** option and click **Reset** to restart the device with the new settings.

6.7.1.3 Ethernet Port Information

- **To display the Ethernet Port Information page:**
 - Open the Ethernet Port Information page (Status & Diagnostics tab > System Status menu > Ethernet Port Information).

Figure 101: Ethernet Port Information

Ethernet Information	
Active Port	1
Port 1 Duplex Mode	Full Duplex
Port 1 Speed	100 Mbps
Port 2 Duplex Mode	Not Available
Port 2 Speed	Not Available

6.7.1.4 Carrier-Grade Alarms

This section describes how to view the following types of alarms:

- Active Alarms
- Alarms History

6.7.1.4.1 Viewing Active Alarms

The Active Alarms page displays a list of currently active alarms. You can also access this page from the Home page (see 'Viewing the Home Page' on page).

- **To view the list of active alarms:**

Open the Active Alarms page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Active Alarms**).

Figure 102: Viewing Active Alarms

Sequential number	Severity	Source	Description	Date
2	Major	System#0/Module#1/EthernetLink#0	Ethernet link alarm. Redundant Link (Physical port #2) is down.	16.8.2011 , 13:42:13
3	Minor	Chassis#0/PemCard#1	PEM Module Alarm. PEM power cable is missing	16.8.2011 , 13:42:22
6	Major	System#0/Module#3	Ethernet link alarm. Redundant module's Ethernet link (Physical port #2) is down.	16.8.2011 , 13:47:27
8	Major	System#0	Configuration mismatch in the system, SYS_HA: Active and Redundant modules have different feature keys.	16.8.2011 , 13:47:27

For each alarm, the following information is provided:

- Severity: severity level of the alarm:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
- Source: unit from which the alarm was raised
- Description: brief explanation of the alarm
- Date: date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

6.7.1.4.2 Viewing Alarm History

The Alarms History page displays a list of alarms that have been raised and traps that have been cleared.

➤ **To view the list of history alarms:**

Open the Alarms History page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Alarms History**).

Figure 103: Viewing Alarm History

Sequential number	Severity	Source	Description	Date
1	Major	Board#1	Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010 , 14:1:26
2	Cleared	Board#1	Alarm cleared: Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010 , 14:1:26
3	Major	Board#1	Controller failure alarm Proxy Set ID 0	6.1.2010 , 14:1:26
4	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	6.1.2010 , 14:1:29
5	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	6.1.2010 , 14:1:29
6	Major	Board#1	NTP server alarm. No connection to NTP server.	6.1.2010 , 14:11:14

For each alarm, the following information is provided:

- Severity: severity level of the alarm:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
 - Cleared (green)
- Source: unit from which the alarm was raised
- Description: brief explanation of the alarm
- Date: date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the Go to page button.

➤ **To delete all the alarms in the table:**

1. Click the **Delete History Table** button; a confirmation message box appears.
2. Click **OK** to confirm.

6.7.2 VoIP Status

6.7.2.1 Active IP Interfaces

➤ To display the **IP Interface Status** page:

1. Open the IP Interface Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Interface Status**).
2. This page details the currently Active network interfaces, when working in Multiple Interface mode.

Figure 104: IP Interface Status

Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	O+M+C	IPv4	IPv4 Manual	10.3.3.168	16	10.3.0.1	1	O+M+C
NA	Internal	IPv4	IPv4 Manual	11.3.9.1	30	0.0.0.0	0	InternalIF

VLAN Mode	Disabled
Native VLAN ID	1



Note: For a full description of the table fields, refer to the Network Configuration chapter in the Product Reference Manual.

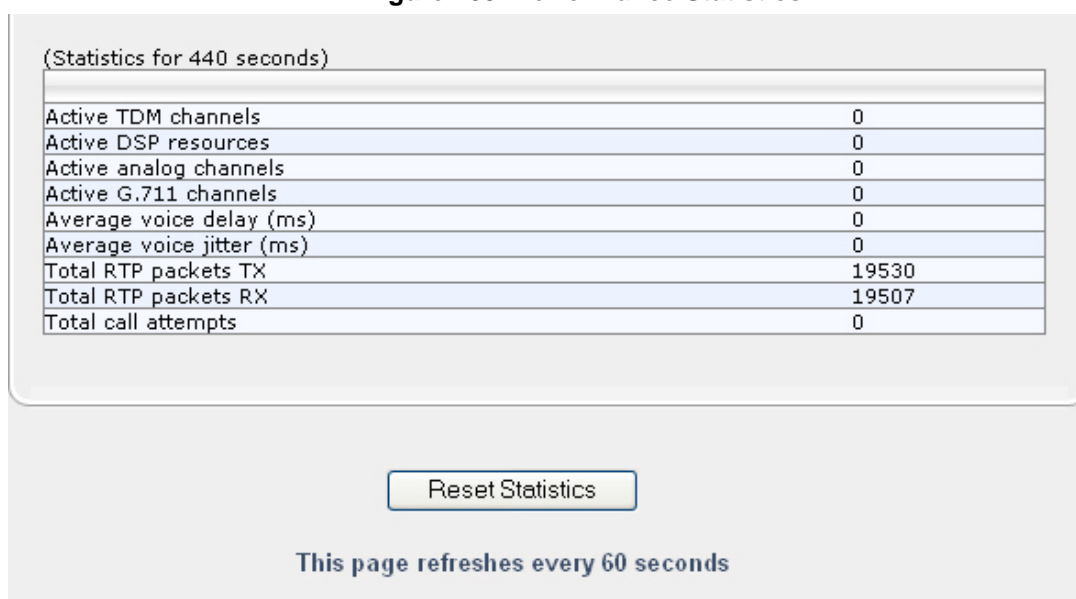
Please note the following:

- Every entry represents an interface index.
- The IP Interface Status page is relevant only when the Multiple Interfaces Table is configured.
- On IPv6 interfaces, the link-local address is displayed below the global address. It is prefixed by "*" to indicate that it is a link-local address. Additionally, there is a textual note at the bottom of the page explaining the meaning of the "*". The zone index is appended to the link-local address using the '%' as delimiter (e.g. fe80::1%2).

6.7.2.2 Performance Statistics

- To display the Performance Statistics page:
 - Open the Basic Statistics page (**Status & Diagnostics** tab > **VoIP Status** menu > **Performance Statistics**).

Figure 105: Performance Statistics



7 Troubleshooting

The following describes how to troubleshoot MediaPack devices.



Notes:

- MP-11x refers collectively to MP-118 8-port, MP-114 4-port and MP-112 2-port Media Gateways having similar functionality except for the number of channels (the MP-112 supports only FXS).
- MP-11x/FXS refers only to the MP-118/FXS, MP-114/FXS and MP-112/FXS gateways.
- MP-11x/FXO refers only to MP-118/FXO and MP-114/FXO gateways.
- MP-11x/FXS&FXO refers to MP-118/FXS&FXO and MP-114/FXS&FXO gateways only.

7.1 Troubleshooting MediaPack Devices via the RS-232 Port

To troubleshoot initialization problems and view the status and error messages of the MediaPack, use serial communication software (e.g., HyperTerminal™) to connect to the MediaPack via the RS-232 port. You can also use this connection to change the network settings (IP address, subnet mask and default gateway IP address) of the MediaPack.

To connect the MP-11x RS-232 port to your PC, refer to Connecting the MP-11x RS-232 Port to Your PC. To connect the MP-124 RS-232 port to your PC, refer to Connecting the MP-124 RS-232 Port to Your PC.

7.1.1 Viewing the Gateway's Information

After applying power to or resetting the gateway, the information, shown in the example below, appears on the terminal screen. This information is used to determine possible MediaPack initialization problems, such as incorrectly defined (or undefined) Local IP address, subnet mask, default router IP address, TFTP server IP address, BootFile name, ini file name and Full/Half duplex network state. Below is an example of Status and Error Messages.

```
MAC address = 00-90-8F-01-00-9E
Local IP address = 10.1.37.6
Subnet mask = 255.255.0.0
Default gateway IP address = 10.1.1.5
TFTP server IP address = 10.1.1.167
Boot file name = ram35136.cmp
INI file name = mp108.ini
Call agent IP address = 10.1.1.18
Log server IP address = 0.0.0.0
Full/Half Duplex state = HALF DUPLEX
Flash Software Burning state = OFF
Serial Debug Mode = OFF
Lan Debug Mode = OFF
BootLoad Version 1.75
Starting TFTP download... Done.
MP108 Version 3.80.00
```

7.1.2 Changing the Networking Parameters

You can use the serial connection to change the network settings (IP address, subnet mask and default gateway IP address) of the MediaPack.

➤ To change the network settings via RS-232:

1. At the prompt, type "conf" and press Enter. The configuration command shell is activated.
2. To check the current network parameters, at the prompt, type GCP IP and press Enter. The current network settings are displayed.
3. To change the network settings, type SCP IP [ip_address] [subnet_mask][default_gateway] (e.g., "SCP IP 10.13.77.7 255.255.0.0 10.13.0.1"). The new settings take effect immediately. Connectivity is active at the new IP address.



Notes:

- This command requires you to enter all three network parameters.
- Consult your network administrator before setting these parameters.

4. To save the configuration, at the prompt, type SAR. And press Enter. The MediaPack restarts with the new network settings.

7.1.3 Determining MediaPack Initialization Problems

Possible initialization problems encountered with the MediaPack can be determined by viewing the HyperTerminal screen after performing a hot hardware reset. Possible initialization problems are listed in the table below. (LED indicators located on the front view of the MediaPack provide first indication that the device has an initialization problem. Refer to LED Indicators on page 163 for a description of the LED visual indicators.)

Possible Initialization Problems

Parameter	Problem Definition
Local IP address	Undefined/incorrectly defined
Subnet Mask	Undefined/incorrectly defined
Default gateway IP address	Undefined/incorrectly defined
TFTP server IP address	Undefined/incorrectly defined
Boot file name	Undefined/incorrectly defined/missing
ini file name	Undefined/incorrectly defined/missing
Call Agent IP address	Undefined/incorrectly defined
Log server IP address	Undefined/incorrectly defined
Full/Half Duplex state	Undefined/incorrectly defined
Flash Software Burning state	Undefined/incorrectly defined
Serial Debug Mode	Undefined/incorrectly defined
BootLoad version	Incorrect

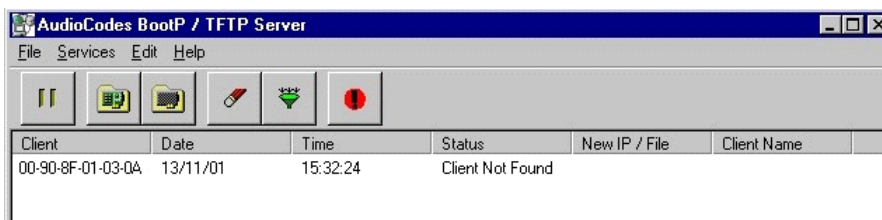
7.1.4 Reinitializing the MediaPack

If an initialization problem is encountered, reinitialize the MediaPack. To reinitialize the MediaPack, a BootP/TFTP Server application must be installed in your management PC. Reinitializing the MediaPack using the BootP/TFTP Server enables you to quickly get started with the MediaPack. For a detailed description of the BootP/TFTP Server Configuration Tool, including installation and configuration, refer to BootP Server.

➤ **To reinitialize the MediaPack:**

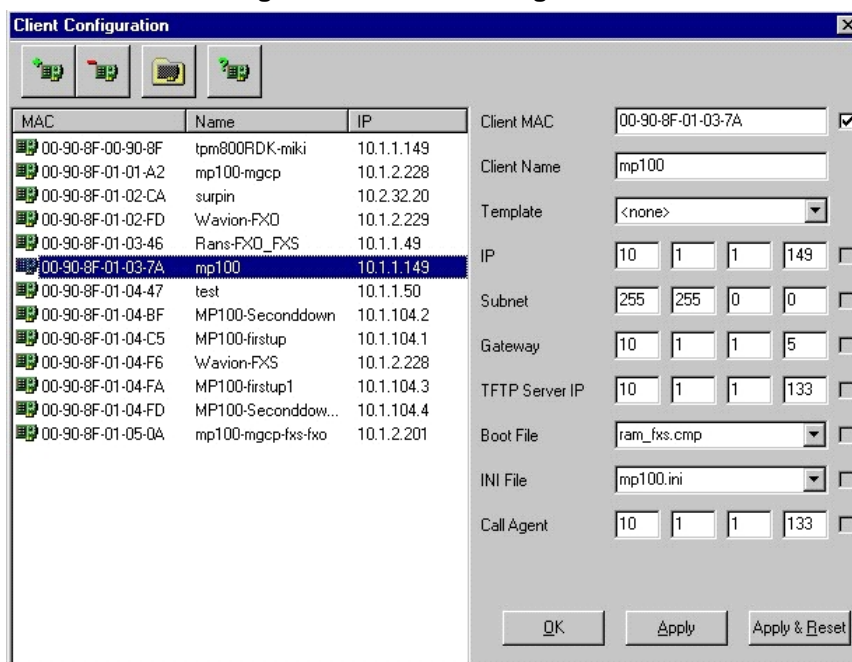
1. Install the BootP/TFTP Server Configuration Tool from the Software CD, Document # LSTC00005 (MediaPack Series), refer to BootP Server.
2. Open the BootP/TFTP Server from Start>Programs>BootP. The BootP/TFTP Server main screen opens:

Figure 106: BootP/TFTP Server Main Screen



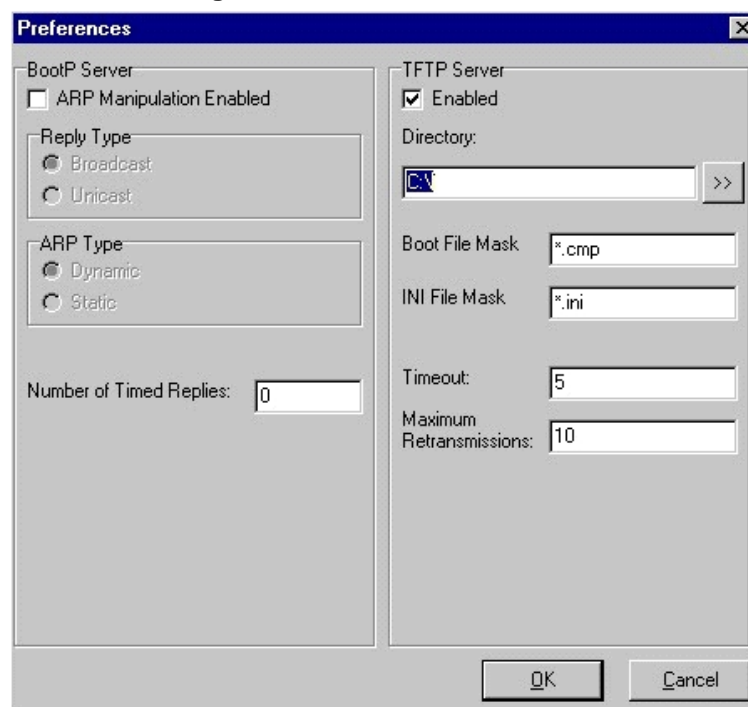
3. In the Services menu, choose Edit Clients. Alternately, double-click on the Client Not Found log entry. The Client Configuration screen appears. (Refer to the figure below). The parameter fields displayed on the right side of the screen constitute the MediaPack software profile configuration. For a Client Not Found, the parameter fields are all blank.

Figure 107: Client Configuration



4. Enter the reported MediaPack MAC address (labeled on the underside of the device) in the Client MAC field.
5. Enter the Client Name.
6. Enter the IP address (such as 10.1.1.33).
7. Enter the Subnet (such as 255.255.255.0) and set the Subnet to a valid value in accordance with the IP address. (That is, class C IP addresses can only have subnet starting with 255.255.255.X, while class B IP addresses can only have subnet starting with 255.255.X.X, and class A IP addresses can only have subnet starting with 255.X.X.X.)
8. Enter the IP address of the default Gateway. It can be any address within the subnet.
9. Enter the Call Agent IP address.
10. Upload the ram_fxs.cmp and the mp_fxs.ini configuration files by opening the Edit menu and choosing Preferences. The Preferences screen appears.

Figure 108: Preferences Screen



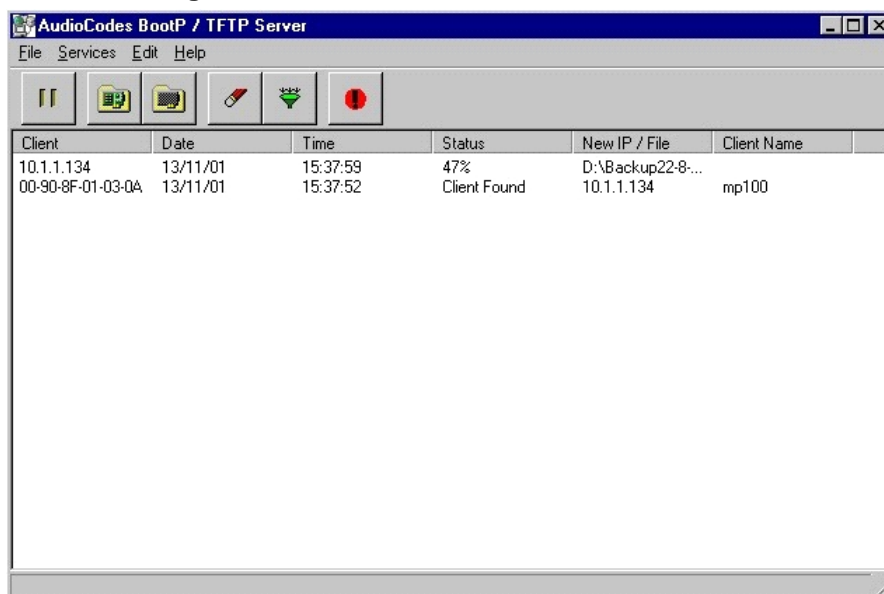
11. In the Directory field, click on the >> button and navigate to the directory of the source cmp and ini files.

If they are not already on your hard disk (C:), copy them to it (under a directory you should create called C:\AudioCodes\). If you do not have the MediaPack Software CD from which to copy the cmp and ini files, contact support@audiocodes.com.

12. Click **OK**. The cmp and ini files are uploaded.

13. Perform a hot hardware reset or cold reset. The MediaPack initializes and the following status messages should be displayed in the BootP/TFTP Server main screen:

Figure 109: BootP/TFTP Server - Client Found



The screenshot shows a window titled "AudioCodes BootP / TFTP Server". It has a menu bar with "File", "Services", "Edit", and "Help". Below the menu bar is a toolbar with icons for a folder, a document, a printer, a network card, and a red circle with a white exclamation mark. The main area of the window contains a table with the following data:

Client	Date	Time	Status	New IP / File	Client Name
10.1.1.134	13/11/01	15:37:59	47%	D:\Backup22-8...	
00-90-8F-01-03-0A	13/11/01	15:37:52	Client Found	10.1.1.134	mp100

7.2 LED Indicators

All LED indicators are described in the tables in Front LED Indicators and Rear LED Indicators.

7.2.1 MediaPack Front View LED Indicators

The full range of the MediaPack includes a front view displaying LED Indications of channel activity status, data, control and LAN status.

7.3 MediaPack Self-Testing

The MediaPack features a mechanism that performs tests on the telephone lines connected to FXS and FXO ports. These tests provide various line measurements. Line testing is executed via SNMP only (using the acAnalogFxoLineTestTable SNMP table for FXO and the acAnalogFxsLineTestTable SNMP table for FXS).

In addition to those tests (which are listed below), a keep alive test is also being performed every 100msec Vs each of the analog ports, in order to detect communication problems with the analog device and to detect any over-heating problems (only in case of FXS ports).



Note: The line testing mechanism must only be used for monitoring and never when there are calls in progress.

7.3.1 FXS Line Testing

The following line tests are available on FXS gateways:

- Hardware revision number
- Temperature (above or below limit, only if in case a thermometer is installed)
- Hook state
- Coefficients check sum
- Message waiting indication status
- Ring state
- Reversal polarity state

For MP-124, you can also use the following Command Shell commands to view line status and electrical measurements per FXS port or phone number:

LineTesting Port <port number> <test type>

- or -

LineTesting Term <TermName> <test type>

Where <test type> can be one of the following values:

- 0 = Line status, which includes the following:
 - Hook status – on-hook (0) or off-hook (1)
 - Message Waiting Indication (MWI) – off (0) or on (1)
 - Ring – off (0) or on (1)
 - Reversal polarity – off (0) or on (1)
- Line electrical measurements:
 - 1 = DC Voltage Tip-Ring [V]
 - 2 = DC Voltage Tip-Ground [V]
 - 3 = DC Voltage Ring-Ground [V]
 - 4 = AC Voltage Transmit(Tel2IP) [dbm]
 - 5 = AC Voltage Receive (IP2Tel) [dbm]
 - 6 = AC Voltage Transmit & Receive [dbm]
 - 7 = Current [mA]
 - 8 = Resistance Tip-Ring [Ohm]
 - 9 = Resistance Tip-Ground [Ohm]

- 10 = Resistance Ring-Ground [Ohm]
- 11 = Capacity Tip-Ring [F]
- 12 = Capacity Tip-Ground [F]
- 13 = Capacity Ring-Ground [F]
- 14 = AC Voltage Tip-Ring [V]
- 15 = AC Voltage Tip-Ground [V]
- 16 = AC Voltage Ring-Ground [V]
- 17 = All the above

**Notes:**

- Use the Analog Line testing mechanism only for monitoring and never when there are calls in progress.
- Line electrical measurements are supported only on certain MP-124 hardware assemblies. For more information, contact your AudioCodes' sales representative.

7.3.2 FXO Line Testing

The following line tests are available on FXO gateways:

- Line Current[mA]
- Line Voltage[V]
- Hook(0-Onhook, 1-Off hook)
- Ring(0-Off, 1-On)
- Line Connected(0-Disconnected, 1-Connected)
- Polarity state(0-Normal, 1-Reversed, 2-N/A)
- Line polarity(0-Positive, 1-Negative).
- Message Waiting Indication(0-Off, 1-On)



Note: Use the Analog Line testing mechanism only for monitoring and never when there are calls in progress.

7.4 Self-Test

The device features the following self-testing modes used to identify faulty hardware components:

- **Startup Tests:** These tests have minor impact in real-time. While the Startup tests are executed, the regular operation of the device is disabled. When the test terminates, the test results are reported via the EV_ENHANCED_BIT_STATUS event. Additionally, if an error is detected, an error message is sent to the Syslog, TPNCP Lib and SNMP trap. This phase consists of the following tests:
 - BIT_ELEMENT_ID_TSA_PCM
 - BIT_ELEMENT_ID_PSTN_FRAMERS
 - BIT_ELEMENT_ID_DSP_CHANNEL
 - BIT_ELEMENT_ID_VOICE_PATH_CONFIRM
- **Periodic Tests:** These tests are started after the device starts up. This is a short test phase in which the only error detected and reported is a failure in initializing hardware components or a malfunction on the running hardware components. If an error is detected, an error message is sent to the Syslog, TPNCP event and SNMP trap. This phase consists of the following tests:
 - BIT_ELEMENT_ID_TSA_PCM
 - BIT_ELEMENT_ID_PSTN_FRAMERS
 - BIT_ELEMENT_ID_DSP_CHANNEL
- **User-initiated tests (Detailed):** - The Detailed test is initiated by the user when the platform is offline (i.e. not used for regular service). When the test terminates, the test results are reported via the EV_ENHANCED_BIT_STATUS event. (Some of the tests are reported via the old END_BIT EV.) Additionally, if an error is detected, an error message is sent to the Syslog, TPNCP Lib and SNMP trap. This phase consist of the following tests:
 - BIT_ELEMENT_ID_SDRAM (enable diagnostics 1 ,2)
 - BIT_ELEMENT_ID_FLASH (enable diagnostics 1(short test) , 2(long test))
 - BIT_ELEMENT_ID_DSP_HPI (enable diagnostics 1 ,2)
 - BIT_ELEMENT_ID_HOST_MII_PHY(enable diagnostics 1 ,2)
 - BIT_ELEMENT_ID_ANALOG (enable diagnostics 1 ,2)

7.4.1 Operating the Syslog Server

7.4.1.1 Sending the Syslog Messages

The Syslog client, embedded in the firmware of the device, sends error reports/events generated by the device application to a Syslog server, using IP/UDP protocol.

There are presently five error levels reported by the Syslog client:

- Emergency level message:

<128>sctp socket setsockopt error 0xf0 [File:sctp.cpp Line:453]

- Warning level message

<132>Release contains no h.225 Reason neither q.931 Cause information stateMode:1 [File: Line:-1];

- Notice level message:

<133>(lgr_flow)(2546) | #0:ON_HOOK_EV

- Info level message:

<134>document http://ab.pisem.net/RadAAIP.txt was not found in documents table [File:vxml_handleDB.cpp Line:2348]

- Debug level message:

<135>SCTP port 2905 was initialized [File:csAPI.cpp Line:150] [CID:0]

7.4.1.2 Activating the Syslog Client

- **To activate the Syslog client:**

- Use the Embedded Web Server GUI (Advanced Configuration>Network Settings - screen section Logging Settings). (Refer to Advanced Configuration Screen and the Logging Settings figure above.)
- Alternately, use the Embedded Web Server GUI or the BootP/TFTP Server to send the ini configuration file containing the parameter EnableSyslog to the device. For detailed information on the BootP/TFTP Server, refer to BootP Server. For an ini file example showing this parameter, refer to the Setting the Syslog Server example below.

7.4.1.3 Setting Syslog Server IP Address, Enabling Syslog, in an ini File (Example)

The example below shows an ini file section with an example configuration for the address parameter SyslogServerIP and an example configuration for the client activation parameter EnableSyslog.

Example of Setting Syslog Server IP Address, Enabling Syslog, in an ini File

```
[Syslog]
SyslogServerIP=10.2.0.136
EnableSyslog =1
```

Reader's Notes

8 List of Abbreviations

List of Abbreviations

Abbreviation	Meaning
AAL1	ATM Adaptation Layer 1 – Used in North America for voice traffic. It provides support for constant bit rate (voice) traffic
AAL2	ATM Adaptation Layer 2 – Used to transmit standard and compressed voice transmissions including silence suppression. It can support both constant and variable bit rates.
ADPCM	Adaptive Differential PCM - voice compression
AIS	Alarm Indication Signal
ASN.1	Abstract Syntax Notation
ATM	Asynchronous Transmission Mode – A connection based transport mechanism that is based on 53 byte cells
A-law	European Compander Functionality Rule (see m-law)
bps	Bits per second
BLES	Broadband Loop Emulation Service by the DSL Forum
BRI	Basic Rate Interface in ISDN
CAS	Channel Associated Signaling
cPCI	Compact PCI (Industry Standard)
CLIP	Connected Line Identity Presentation
COLR	Connected Line Identity Restriction
DHCP	Dynamic Host Control Protocol
DID	Direct Inward Dial
DS1	1.544 Mbps USA Digital Transmission System (see E1 and T1)
DS3	44.736 Mbps USA Digital Transmission System, Encapsulates 28 T1 streams, Also called T3
DSL	Digital Subscriber Line
DSP	Digital Signal Processor (or Processing)
DTMF	Dual Tone Multiple Frequency (Touch Tone)
E1	2.048 Mbps European Digital Transmission System (see T1)
E-ADPCM	Enhanced ADPCM
ETSI	European Telecommunications Standards Institute
FR	Frame Relay
GK	Gatekeeper

List of Abbreviations

Abbreviation	Meaning
GW	Gateway
G.xxx	An ITU Standard - see References section for details
H.323	A range of protocol standards for IP-based networks
H.323 Entity	Any H.323 Component
IE	Information Element (ISDN layer 3 protocol, basic building block)
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPmedia	AudioCodes series of VoIP Media Processing blades
IPM-260/UNI	AudioCodes IPmedia PCI VoIP Media Processing blade, to 240 ports
IPM-1610	AudioCodes IPmedia cPCI VoIP Media Processing blade, to 240 ports
IPM-6310	AudioCodes IPmedia VoIP Media Processing blade, to 2016 voice/fax/data independent multiple LBR channels
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	Telecommunications section of the ITU
IVR	Interactive Voice Response
Jitter	Variation of interpacket timing interval
kbps	Thousand bits per second
LAPD	Line Access Protocol for the D-channel
LFA	Loss of Frame Alignment
LOF	Loss of Frame
Mbps	Million bits per second
MCU	Multipoint Control Unit (H.323)
Mediant	AudioCodes series of Voice over Packet Media Gateways
Mediant for Broadband	AudioCodes series of Broadband Access Gateways, including Cable and V5.2 Access Gateways
MEGACO	Media Gateway Control (Protocol, H.248)
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base

List of Abbreviations

Abbreviation	Meaning
MP-112	AudioCodes 2-port Analog MediaPack Media Gateway
MP-114	AudioCodes 4-port Analog MediaPack Media Gateway
MP-118	AudioCodes 8-port Analog MediaPack Media Gateway
MP-124	AudioCodes 24-port Analog MediaPack Media Gateway
ms or msec	Millisecond; a thousandth part of a second
MVIP	Multi-Vendor Integration Protocol
NIC	Network Interface Card
OSI	Open Systems Interconnection (Industry Standard)
PCI	Personal Computer Interface (Industry Standard)
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
POTS	Plain Old Telephone System or Service
PRI	Primary Rate Interface in ISDN
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAI	Remote Alarm Indication
RAS	Registration, Admission, and Status (control within H.323).
RDK	Reference Design Kit.
RFC	Request for Comment issued by IETF.
RTCP	Real Time Control Protocol.
RTP	Real Time Protocol.
SB-1610	AudioCodes TrunkPack VoIP/ 1610 cPCI media streaming blade, to 480 ports for Wireless systems
ScBus	Signal Computing Bus - part of SCSA
SCSA	Signal Computing System Architecture
SDK	Software Development Kit
SNMP	Simple Network Management Protocol
Stretto	AudioCodes series of Voice over Wireless Media Gateways
TCP	Transmission Control Protocol.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TFTP	Trivial File Transfer Protocol.

List of Abbreviations

Abbreviation	Meaning
TGCP	Trunking Gateway Control Protocol
TPNCP	AudioCodes TrunkPack Network Control Protocol.
TP-260/UNI	AudioCodes TrunkPack VoIP/260 Voice over IP PCI media streaming blade, up to 240 ports
TP-1610	AudioCodes TrunkPack VoIP cPCI media streaming blade, to 480 ports
TP-6310	AudioCodes TrunkPack VoIP Media Processing blade, to 2016 voice/fax/data independent multiple LBR channels
TPM-1100	AudioCodes TrunkPack Module
TrunkPack	AudioCodes series of voice compression blades
T1	1.544 Mbps USA Digital Transmission System (see E1 and DS1)
T3	44.736 Mbps USA Digital Transmission System, Encapsulates 28 T1 streams, also called DS3
UDP	User Datagram Protocol
VCC	Virtual Channel Connection
VoAAL2	Voice over AAL2 (see above)
VoATM	Voice over Asynchronous Transfer Mode
VoDSL	Voice over Digital Subscriber Line
VoFR	Voice over Frame Relay
VoIP	Voice over Internet Protocol
VoP	Voice over Packet(s)
VoPN	Voice over Packet Networks
VPN	Virtual Private Network
µs or µsec	microsecond; a millionth part of a second

9 Technical Specifications

The table below lists and briefly delineates the functional specifications of the MediaPack media gateway.

MP-11x & MP-124D Technical Specifications

Item	Characteristic
Channel Capacity	
Available Ports	MP-112R 2 ports* MP-114 4 ports MP-118 8 ports
	MP-124 24 ports * The MP-112R differs from the MP-114 and MP-118. Its configuration excludes the RS-232 connector, the Lifeline option and outdoor protection.
FXS Functionality	
FXS Capabilities	Short or Long Haul (Automatic Detection): REN2: Up to 10 km (32,800 feet) using 24 AWG line. REN5: Up to 3.5 km (11,400 feet) using 24 AWG line. Note: The lines were tested under the following conditions: ring voltage greater than 30 Vrms, offhook loop current greater than 20 mA (all lines ring simultaneously).
	MP-11x includes lightning and high voltage protection for outdoor operation.
	Caller ID generation: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, British and DTMF ETSI CID (ETS 300-659-1).
	Programmable Line Characteristics: Battery feed, line current, hook thresholds, AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains.
	Programmable ringing signal. Up to four cadences and frequency 15 to 200 Hz.
	Drive 4 phones per port simultaneously in offhook and Ring states. MP-11x Ring Equivalent Number (REN) = 5
	Over-temperature protection for abnormal situations as shorted lines.
	Loop-backs for testing and maintenance.

FXO Functionality	
FXO Capabilities Doesn't apply to the MP-112	Short or Long Haul.
	Includes lightning and high voltage protection for outdoor operation.
	Programmable Line Characteristics: AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains, ring detection threshold, DC characteristics. Note: For country-specific coefficients use the parameter CountryCoefficients.
	Caller ID detection: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, and DTMF ETSI CID (ETS 300-659-1).
Additional Features	
Polarity Reversal / Wink	Immediate or smooth to prevent erroneous ringing
Metering Tones	12/16 KHz sinusoidal bursts (FXS only)
Distinctive Ringing	By frequency (15-100 Hz) and cadence patterns
Message Waiting Indication	DC voltage generation (TIA/EIA-464-B), V.23 FSK data, Stutter dial tone and DTMF based.
Voice & Tone Characteristics	
Voice Compression	G.711 PCM at 64 kbps μ -law/A-law (10, 20, 30, 40, 50, 60, 80, 100, 120 msec) G.723.1 MP-MLQ at 5.3 or 6.3 kbps (30, 60, 90 msec) G.726 at 32 kbps ADPCM (10, 20, 30, 40, 50, 60, 80, 100, 120 msec) G.729 CS-ACELP 8 kbps Annex A / B (10, 20, 30, 40, 50, 60 msec) EG.711, G.722 (in Analog modules)
Silence Suppression	G.723.1 Annex A G.729 Annex B PCM and ADPCM - Standard Silence Descriptor (SID) with Proprietary Voice Activity Detection (VAD) and Comfort Noise Generation (CNG).
Packet Loss Concealment	G.711 Appendix 1 G.723.1 G.729 A / B
Echo Canceler	Echo Canceler G.165 and G.168 2000, 64 msec
Gain Control	Programmable
DTMF Transport (in-band)	Mute, transfer in RTP payload or relay in compliance with RFC 2833
DTMF Detection and Generation	Dynamic range 0 to -25 dBm, compliant with TIA 464B and Bellcore TR-NWT-000506.

Call Progress Tone Detection and Generation	32 tones: single tone, dual tones or AM tones, programmable frequency & amplitude; 64 frequencies in the range 300 to 1980 Hz, 1 to 4 cadences per tone, up to 4 sets of ON/OFF periods.
Output Gain Control	-32 dB to +31 dB in steps of 1 dB
Input Gain Control	-32 dB to +31 dB in steps of 1 dB
Fax/Modem Relay	
Fax Relay	Group 3 fax relay up to 14.4 kbps with auto fallback T.38 compliant, real time fax relay Tolerant network delay (up to 9 seconds round trip)
Modem Transparency	Auto switch to PCM or ADPCM on V.34 or V.90 modem detection
Protocols	
VoIP Signaling Protocol	MGCP RFC 3435
Communication Protocols	RTP/RTCP packetization. IP stack (UDP, TCP, RTP). Remote Software load (TFTP, HTTP and HTTPS).
Line Signaling Protocols	Loop start
Processor	
Control Processor	Motorola PowerQUICC 870
Control Processor Memory	SDRAM - 32 MB
Signal Processors	AudioCodes AC482 VoIP DSP
Interfaces	
FXS Telephony Interface	2, 4 or 8 Analog FXS phone or fax ports, loop start (RJ-11)
FXO Telephony Interface	4 or 8 Analog FXO PSTN/PBX loop start ports
Combined FXS / FXO	MP-118 4 FXS + 4 FXO ports MP-114 2 FXS + 2 FXO ports
Network Interface	10/100 Base-TX
RS-232 Interface	RS-232 Terminal Interface (requires a DB-9 to PS/2 adaptor).
Indicators	Channel status and activity LEDs
Lifeline	The Lifeline provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or the network fails. Combined FXS/FXO gateways provide a Lifeline connection available on all FXS ports. Note: The Lifeline splitter (for FXS gateways) is a special order option.

Connectors & Switches			
Rear View			
8 Analog Lines (MP-118)	8 RJ-11 connectors		
4 Analog Lines (MP-114)	4 RJ-11 connectors		
2 Analog Lines (MP-112R)	2 RJ-11 connectors		
AC power supply socket	100-240~0.3A max.		
Ethernet	10/100 Base-TX, RJ-45		
RS-232	Console PS/2 port		
Reset Button	Resets the MP-11x		
Physical			
MP-11x Dimensions	Height:	42 mm	1.65 inches
	Width:	172 mm	6.771 inches
	Depth:	220 mm	8.661 inches
	Weight:	0.5 kg	1.10 lbs
MP-124D Dimensions	Height:	44.5 mm	1.75 inches
	Width:	445 mm	17.5 inches
	Depth:	269 mm	10.6 inches
	Weight:	1.8 kg	3.96 lbs
Environmental	Operational:	5° to 40° C	41° to 104° F
	Storage:	25° to 70° C	-77° to 158° F
	Humidity:	10 to 90% non-condensing	
Mounting	Rack mount, Desktop, Wall mount. Note: The Rack mount tray is a special order option.		
Electrical	100-240 VAC Nominal 50/60 Hz		
Type Approvals			
Safety and EMC	UL 60950-1, FCC part 15 Class B CE Mark EN 60950-1, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 55024.		
Management			
Configuration	Gateway configuration using Web browser or ini files		
Management and Maintenance	SNMP v2c		
	Syslog, per RFC 3164		
	Local RS-232 terminal		
	Web Management via HTTP or HTTPS		
	Telnet		

Reader's Notes



User's Manual