Mediant™ 3000

VoIP Digital Media Gateway

MGCP & MEGACO Protocols

User's Manual

Mediant 3000 with TP-6310 & TP-8410

Version 6.6

December 2015

Document # LTRT-95211

Table of Contents

1 Introduction 9

1.1 General Features 11
1.2 High Availability 13
1.2.1 Mediant 3000 HA System with TP-6310 13
1.2.2 Mediant 3000 HA System with TP-8410 14
1.2.3 Private IP Address and System (Global) IP Address(es) 15
1.2.3.1 Private (Local) IP Address 15
1.2.3.2 System (Global) IP Address 15
1.3 Functional Block Diagram - TP-6310 16
1.4 Functional Block Diagram - TP-8410 17

2 Software Package 19

2.1 Installing the Software Package 19
2.1.1 Installing/Unzipping When Using a Windows™ Operating System 19
2.2 Software Directory Contents & Structure 20

3 Getting Started 21

3.1 Assigning the Device IP Address 21
3.1.1 Assigning an IP Address Using HTTP 21
3.1.2 Assigning an IP Address Using BootP 22
3.2 Assigning the IP Addresses for High Availability Mode 23

4 System Initialization Process 25

4.1 Boot Firmware & Operational Firmware 25
4.2 Startup Process 26
4.3 Configuration Parameters and Files 28
4.3.1 Initialization (ini) File 28
4.3.1.1 Parameter Value Structure 29
4.3.1.2 Tables of Parameter Value Structure 31
4.3.1.3 Binary Configuration File Download 33
4.3.2 Auxiliary Files 33
4.3.2.1 Downloading Auxiliary Files via TFTP During the Blade Startup 34
4.3.3 Automatic Update Facility 34
4.4 Backup Copies of ini and Auxiliary Files 37
4.5 Upgrading Device Software 38
4.6 Software Upgrade Key 38
4.7 High Availability 39
4.7.1 Initializing the Mediant 3000 System 39
4.7.2 Device Initialization Process 39
4.7.3 Special System Specific Behavior 39
4.7.3.1 Rebooting the Blade 39
4.7.3.2 High Availability and Syslog 40
4.7.4 Actions upon Detecting Blade Failure 40
4.7.4.1 Failure in the Active Blade 40
4.7.4.2 Failure in the Redundant Blade 40
4.7.5 Hitless Software Upgrade 40

5 Configuration Using the Web Interface 43

5.1 Limiting the Web Interface to Read-Only Mode 43
5.2 Disabling the Web Interface 44

5.2.1 Encrypted HTTP Transport (HTTPS - SSL) 44
5.2.2 Limiting Web Access to a Predefined List of Client IP Addresses 44
5.2.3 Managing Web Server Access Using a RADIUS Server....44
5.3 Initial Device Configuration using the Web Interface....44
5.4 Accessing the Web Interface 45
5.5 Using Internet Explorer to Access the Web Interface....46
5.6 Getting Acquainted with the Web Interface....47
5.6.1 Toolbar....48
5.6.2 Navigation Tree 49
5.6.2.1 Displaying Navigation Tree in Basic and Full View....49
5.6.2.2 Showing / Hiding the Navigation Pane....50
5.6.3 Working with Configuration Pages 51
5.6.3.1 Accessing Pages....51
5.6.3.2 Viewing Parameters 52
5.6.3.3 Displaying Basic and Advanced Parameters 52
5.6.3.4 Showing / Hiding Parameter Groups....53
5.6.3.5 Modifying Parameter Values 54
5.6.4 Saving Configuration Changes....55
5.6.5 Searching for Configuration Parameters 55
5.6.6 Working with Scenarios 56
5.6.6.1 Creating a Scenario....57
5.6.6.2 Editing a Scenario 60
5.6.6.3 Saving a Scenario to a PC 61
5.6.6.4 Loading a Scenario to the Device 62
5.6.6.5 Exiting Scenario Mode 62
5.6.6.6 Deleting a Scenario 62
5.6.7 Creating a Login Welcome Message....63
5.6.8 Getting Help....64
5.6.9 Logging Off the Web Interface....65
5.7 Using the Home Page 66
5.7.1 TP-6310....66
5.7.2 TP-8410....69
5.7.3 Viewing the Active Alarms Table....70
5.7.4 Viewing Ethernet Port Information....71
5.7.5 High Availability Configuration....72
5.7.5.1 Manual Switch Over / Redundant Board Reset 73
5.8 Configuration....74
5.8.1 System....74
5.8.1.1 Application Settings....74
5.8.1.2 Syslog Settings....76
5.8.1.3 Regional Settings 76
5.8.1.4 Certificates 77
5.8.1.5 Management 78
5.8.2 VoIP 91
5.8.2.1 Network 91
5.8.2.2 TDM & Timing 102
5.8.2.3 Security Settings 108
5.8.2.4 PSTN....113
5.8.2.5 Media....122
5.8.2.6 Call Control....136
5.8.2.7 V5.2 Configuration (For TP-8410 Only) 141
5.9 Maintenance....142
5.9.1 Maintenance 142
5.9.1.1 Maintenance Actions....142
5.9.1.2 High Availability Maintenance 145
5.9.2 Software Update....146
5.9.2.1 Load Auxiliary Files 147

5.9.2.2 Software Upgrade Key 148
5.9.2.3 Software Upgrade Wizard 151
5.9.2.4 Configuration File 157
5.10 Status and Diagnostic Menu....161
5.10.1 System Status....161
5.10.1.1 Message Log....161
5.10.1.2 Device Information 162
5.10.1.3 Ethernet Port Information 163
5.10.1.4 Carrier-Grade Alarms....163
5.10.2 Performance Monitoring 165
5.10.2.1 Viewing Trunk Utilization....165
5.10.2.2 Viewing MOS per Media Realm 166
5.10.3 VoIP Status....168
5.10.3.1 Viewing Trunk and Channel Status....168
5.10.3.2 Viewing NFAS Groups and D-Channel Status....169
5.10.3.3 Active IP Interfaces 170
5.10.3.4 Performance Statistics 171
5.10.3.5 Timing Module Information....171
5.10.4 Components Status 172
5.11 Device High Availability Mode 173

6 Troubleshooting....175

6.1 TP-6310 Self-Test 175
6.2 TP-8410 Self-Test 176

7 Technical Specifications 177

7.1 Mediant 3000 with TP-6310/TP-8410 Technical Specification 177

8 List of Abbreviations....183

9 Index....187

This page is intentionally left blank.

Notice

This document describes the AudioCodes Mediant 3000 MGCP & MEGACO media gateway, housed with TP-8410 SIP blade(s) or TP-6310 blade(s).

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.

This document is subject to change without notice.

Date Published: December 13, 2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 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.

Related Documentation

The documentation package contains the following publications, available on the AudioCodes Web site:

- MGCP MEGACO Product Reference Manual - provides an extremely comprehensive description of MGCP and MEGACO Network Control Protocols and their compliance.
- User's Manual contains the product overview; software package, startup and initialization; Web GUI-based management; Diagnostics and Product Specification.
- MEGACO Release Notes - describes for each new version the various new features and functionality, issues from the previous version that have been solved, and known constraints of this new software version.

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 mentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

1 Introduction

The Mediant 3000 is a VoIP gateway, offering integrated voice gateway functionality capable of delivering 2016 simultaneous calls, the Mediant 3000 supports all necessary functions for voice and fax streaming over IP networks.

Supporting up to 2016 voice channels with up to 63 E1 / 84 T1 trunks and with various PSTN interfaces, the Mediant 3000 addresses mid-density applications deployed in IP networks. The Mediant 3000 supports a wide variety of VoIP and cellular vocoders, standards-compliant signaling and call control.

There are two types of VoP communication blades supported by the Mediant 3000:

- Based on TP-6310 blades - The Mediant 3000 with TP-6310 blades incorporates 1+1 Protected OC-3/STM-1 PSTN or three T3 PSTN telephony interfaces, either directly to the PSTN or to an enterprise PBX.
- Based on TP-8410 blades – The Mediant 3000 with TP-8410 blades incorporates up to 63 E1 or 84 T1 PSTN interfaces and it also allows the user to have different and dedicated physical Ethernet ports for each network type (Media, OAMP and Control).

The Mediant 3000 supports a broad selection of voice processing related algorithms, including:

- G.711, G.723.1, G.729A and multiple UMTS, GSM and CDMA Vocoders
- G.168-2000 compliant echo cancellation
- T.38 real-time Fax over IP
- A wide selection of In-band and Out-of-band tone detection and generation
- Signaling protocol support including ISDN PRI

The Mediant 3000 is available in the following operating modes:

- Simplex Mode (one VoP communication blade and one SA/M3K Synchronization and Alarm blade). In this mode there is an optional integrated CPU (iCPU) for 3rd party applications.
- High Availability 1+1 Mode (two VoP communication blades, two RTM and two SA/M3K Synchronization and Alarm blades - one is active and the other is in standby mode).

For High Availability, the Mediant 3000's hardware design contains redundant modules for every part in the system, including redundant network connectivity, comprehensive switchover processing and backup data storage and access, as well as applicable load-sharing schemes.

To achieve high-availability, the software itself resides on redundant components and monitors system components to detect a hardware failure, as well as handling the switchover procedures to overcome a possible failure. In addition, components are hot-swappable so that they can be replaced while the system is fully operational with no disruption to service.

The Mediant 3000 contains:

- Up to two VoP communication blades
- RTM (Rear Transition Module) blades:
- In a Simplex configuration, up to two RTM blades for a TP-8410 based system, or a single RTM for a TP-6310 based system.
- In 1+1 system configuration, two RTM blades.
- Up to two SA/M3K Synchronization and Alarm blades
- Two Power Entry Modules (PEM/DC/3K)
- Two Power Supplies (PS/DC/3K)

These components function in either an Active / Standby redundant or load-sharing configuration to provide full continuous performance coverage and are ideal building blocks for deploying high-density, high availability Voice over Packet systems.

For more details on the High Availability 1+1 system, refer to 'The High Availability 1+1 System' on page 13.

1.1 General Features

The Mediant 3000 has the following features:

- Up to 2016 voice/fax/data independent multiple LBR channels
- PSTN interfaces:
  - Up to 63 E1 / 84 T1 interfaces (with TP-8410)
  - 1 + 1 Protected STM-1/OC-3 interface (with TP-6310)
  - Three T3 interfaces (with TP-6310)
- Packet interface:
  - Dual GbE link ports (for redundancy)
  - Four Fast links for multiple IP configurations (with TP-8410)
- VoP and Voice Processing capabilities:
  - Superior, high quality VoIP calls and FoIP transmissions
  - Packet telephony standard compliant
  - Vocoder configuration options include:
    - AMR, AMR WB, EVRC, EVRC-B, G.711 A/u-law PCM, G.722, G.723.1, G.726 ADPCM, G.727 ADPCM, G.729 A B, G.729.1 (up to 12 kbps), G.729.1 (up to 32 kbps), G.729E, GSM-EFR, GSM-FR, iLBC, MS GSM & EG.711
  - Independent vocoder selection per channel
  - VoIP packet streaming (RTP/ RTCP) per RFC 3550/2551
  - RTP stream multiple destination connection
  - IP to IP Mediation capabilities
  - IP to IP Transcoding (G.711 to and from LBR, to GSM Vocoders, to UMTS vocoders and to CDMA vocoders)
  - Real-time Fax over IP/T.38 with superior performance (round trip delay of up to 9 sec)
  - Automatic Fax Bypass modes
  - DTMF Detection and Generation according to TIA 464B
  - DTMF Relay according RFC 2833
  - Tone detection and generation (MF, DTMF, RFC 2833)
  - Extensive media processing functions
  - G.168-2000 compliant Echo Cancelation with a 32, 64 or 128 msec tail
  - Silence Suppression supporting VAD (Voice Activity Detection) and CNG (Comfort Noise Generation)
- “TDM- Switching” – for transferring TDM streams between timeslots
- Call Control and Signaling support:
  - Call Control: MGCP (RFC 3435), MEGACO (H.248) standard control protocols
  - PSTN Signaling: CAS, ISDN, PRI, (and V5 for TP-8410)
  - MF-R1, MFC-R2 and Call Progress Tone detection and generation

- Management Interfaces:
  - SNMPv2, Web interface, EMS (Optional), SNMPv3
- Mediant 3000 Platform capabilities:
  - Flexible deployment and multiple density options
  - Redundant Active / Standby configuration
  - Load-sharing power supply configuration with separate power sources
  - Carrier Grade Alarm System
  - NEBS Level 3 compliant

1.2 High Availability

The High Availability architecture of the Mediant 3000 provides the following functionality:

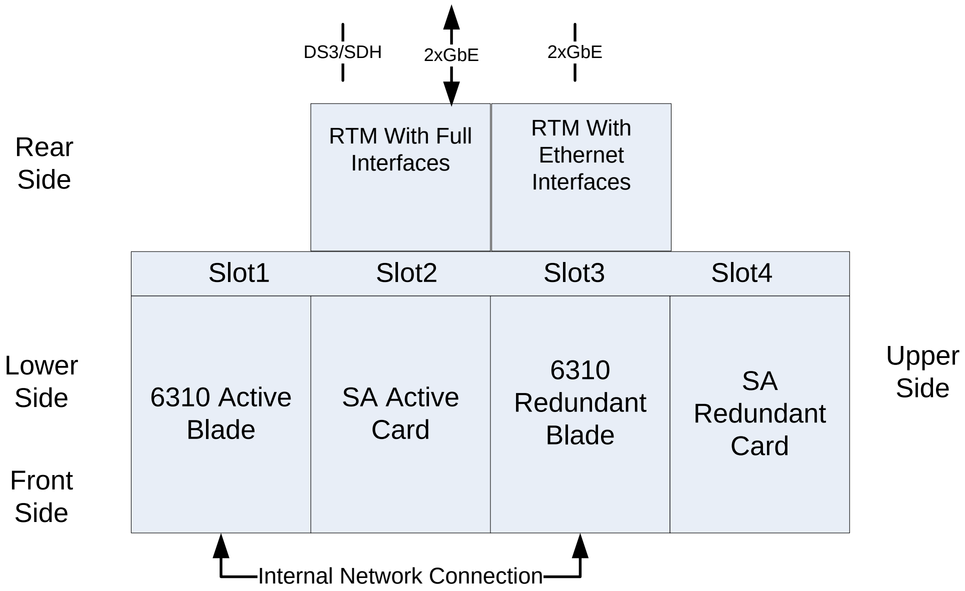
- Redundant Active / Standby configuration
- Support for both TP-6310 & TP-8410 blades
- One or many global System IP addresses
- Private IP address for each blade for maintenance and fallback.
- Upgrading software without disrupting current calls (Hitless Software Upgrade)

1.2.1 Mediant 3000 HA System with TP-6310

The system includes two TP-6310 blades. One of the blades is the active (working) blade and the other blade is the redundant (standby) blade.

The figure below illustrates the general architecture of the Mediant 3000 with 1+1 High Availability.

Figure 1: Mediant 3000 with TP-6310 System HA 1+1 Architecture



If both TP-6310 blades are installed at the time the system is powered up, the TP-6310 blade in Slot 1 always initially assumes the Active functionality and the TP-6310 blade in Slot 3 always initially assumes the Redundant functionality. If only one blade is installed, (no matter which slot it is occupying) it always assumes the Active functionality. If at a later time, a second TP-6310 blade is added, this second TP-6310 blade assumes the redundant functionality.

There is one internal Ethernet link between the Active and Redundant blades, which is used for the management of the high availability feature. This link is automatically and internally configured and is used by both of the blades.

Slots 2 and 4 in the front are occupied with the SA/M3K blades. One SA/M3K blade assumes the Active functionality, while the other SA/M3K blade assumes the Redundant functionality, according to each blade state.

On the rear of the chassis, a RTM-6310 is located in slot number 2. Its PSTN connections and GbE interface are always connected to the Active TP-6310 blade in the front in slot 1. The RTM-6310/Redundant is located in slot 3 and supplies the GbE interfaces to the TP-6310 blade in the front in slot 3.

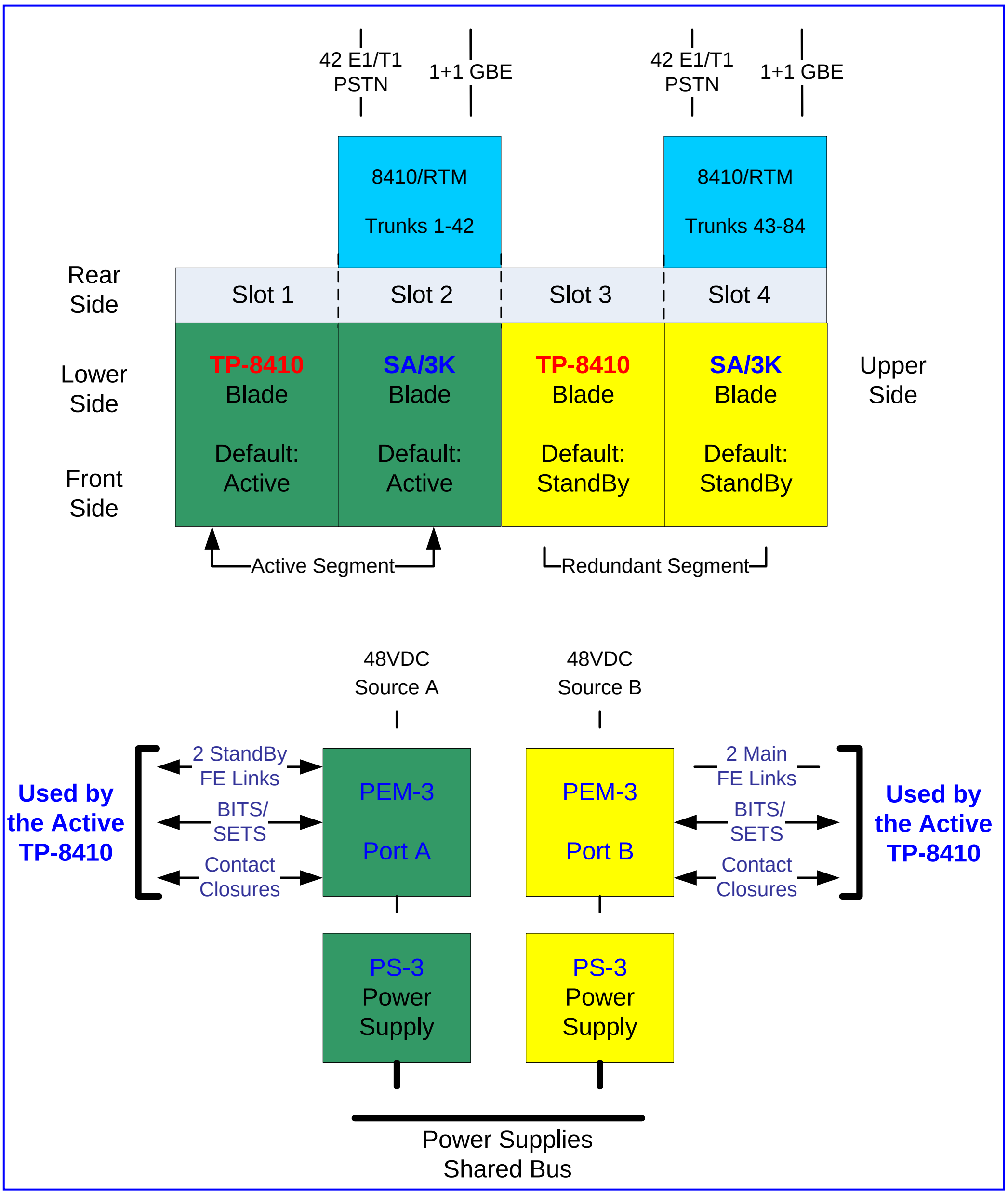
Two GbE links can be connected to each blade through each RTM-6310. At least one link per blade must be connected, but two are recommended for LAN redundancy. After system initialization is complete, network access is available only to the Active blade. The Redundant GbE links have no network access.

1.2.2 Mediant 3000 HA System with TP-8410

The HA (High Availability) system includes two TP-8410 blades, two RTM-8410s (Rear Transition Modules) and two SA/M3K Synchronization and Alarm blades

One of each of the blades is the active (working) blade and the other blade is the redundant (standby) blade, as illustrated below:

Figure 2: Mediant 3000 with TP-8410 System HA 1+1 Architecture



If both TP-8410 blades are installed at the time the system is powered up, the TP-8410 blade in Slot 1 always initially provides the Active functionality and the TP-8410 blade in Slot 3 always initially provides the Redundant functionality. If only one blade is installed, (no matter which slot it is occupying) it always provides the Active functionality. If at a later time, a second TP-8410 blade is added, this second TP-8410 blade provides the redundant functionality.

There is one internal Ethernet (ETH) link between the Active and Redundant blades, which is used for the management of the High Availability feature. This link is automatically and internally configured and is used by both of the blades.

Slots 2 and 4 in the front are occupied with the SA/M3K blades. One SA/M3K blade provides the Active functionality, while the other SA/M3K blade provides the Redundant functionality, according to each blade's state.

On the rear of the chassis, an RTM-8410 is located in slot # 2. This RTM is connected to trunks 1-42. Its PSTN connections and ETH interface are always connected to the Active TP-8410 blade in the front in slot # 1. The second RTM-8410 is located in slot # 4. This 2nd RTM is connected to trunks 43-84. Trunks connected to this RTM are directed to the Active blade. ETH interfaces are directed to the TP-8410 blade in the front in slot # 3.

Two GbE links can be connected to each blade through each RTM-8410. At least one link per blade must be connected, but two are recommended for LAN redundancy. After system initialization is complete, network access is available only to the Active blade. The Redundant GbE links have no network access.

Each blade has its own local IP address (acquired via BootP/DHCP) used for loading the software by TFTP. In order for the system to be set to HA, the system address must be configured via the interface table.

1.2.3 Private IP Address and System (Global) IP Address(es)

Each blade on HA systems, has a single Private (Local) IP address and one or more System (Global) IP Addresses.

Please refer to 'Assigning the Device IP Address' on page 21 to configure the Private and System IP Addresses.

1.2.3.1 Private (Local) IP Address

This is a single IP address (and subnet) per blade that is acquired via BootP/DHCP and used for loading the software by TFTP.

1.2.3.2 System (Global) IP Address

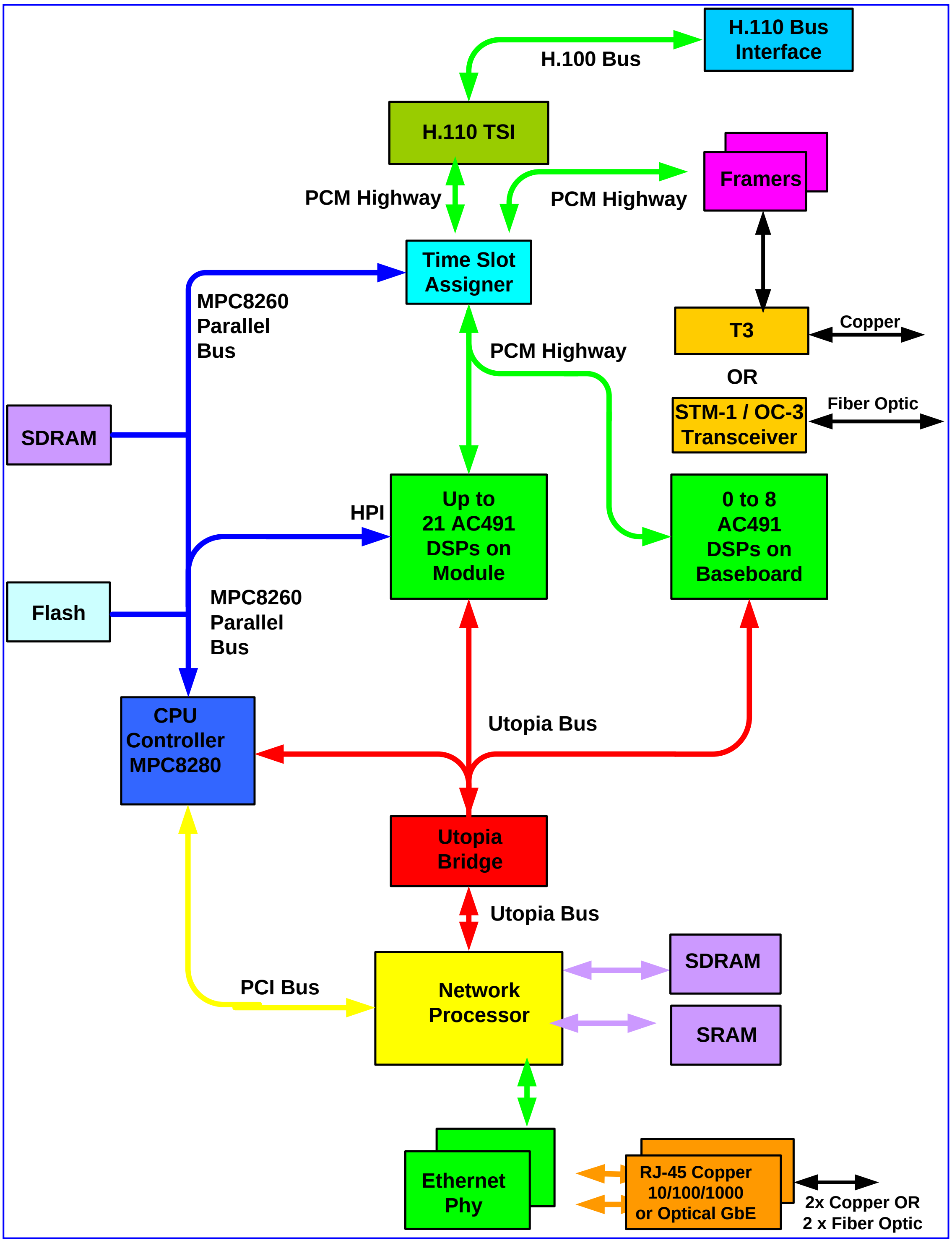
The Global IP address(es) of the HA system are the IP Address(es) that are used by the Active blade for Media, OAMP and Control. These IP Address(es) are configured using an interface table.

Note: In HA systems, the local IP addresses (one of each blade) are rarely used (only when a major failure occurs). It is necessary to configure these addresses to be valid IP addresses on the network with full access to the Syslog server, so in case of a major failure, the blades will be able to report to the Syslog server. Moreover, it is recommended that these private IP addresses will be on same subnet as the OAMP system IP address.

1.3 Functional Block Diagram - TP-6310

The figure below illustrates the functionality of the blade.

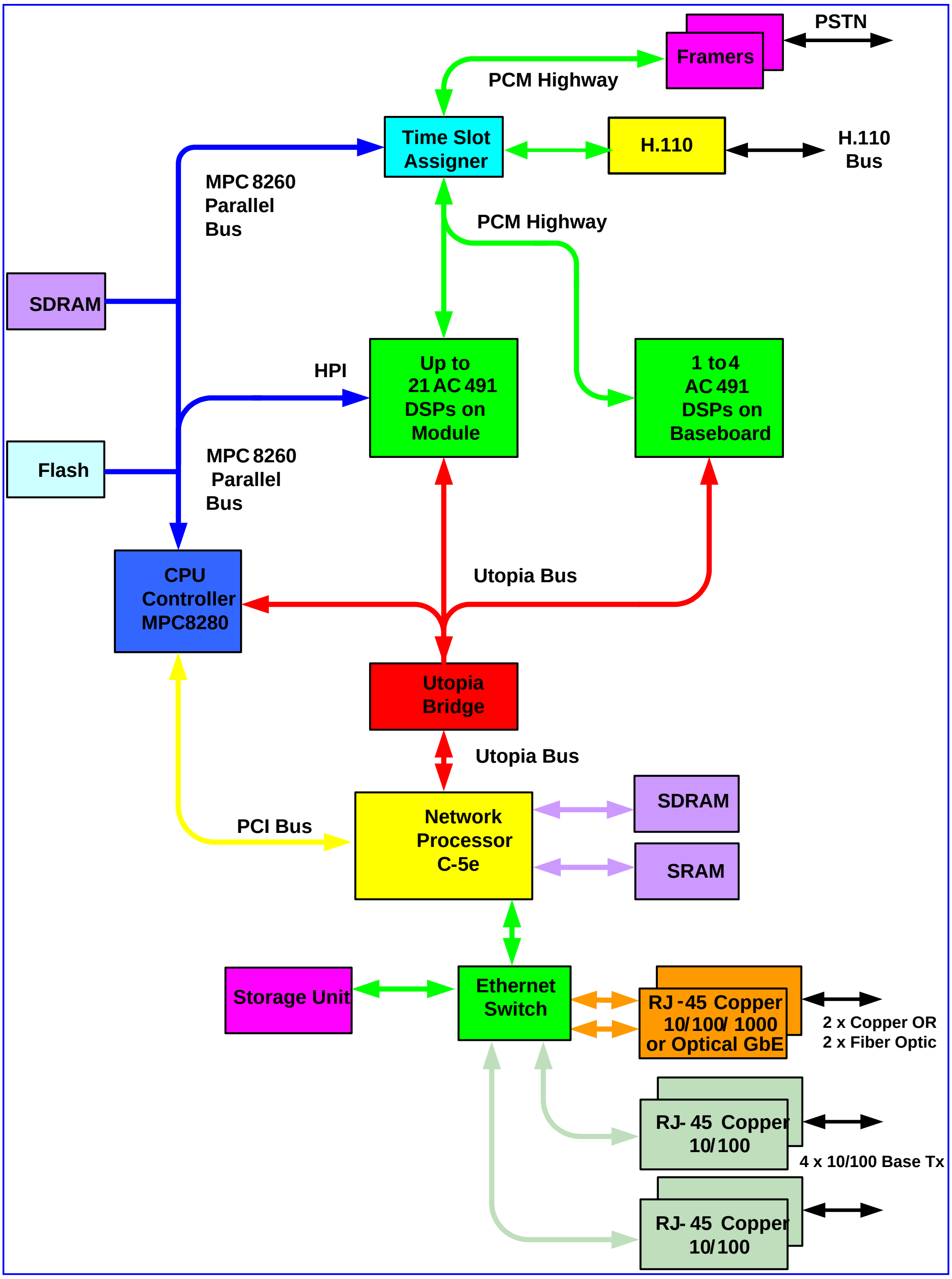
Figure 3: 6310 Functional Block Diagram



1.4 Functional Block Diagram - TP-8410

The figure below illustrates the functionality of the blade.

Figure 4: TP-8410 Functional Block Diagram



This page is intentionally left blank.

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 19.
2. Check the software package contents (refer to "Software Directory Contents & Structure" on page 20.)
3. Perform "Getting Started" on page 21.

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.

2.2 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\Wireshark Plugins	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 Mediant 3000 is supplied with application software already resident in its flash memory (with factory default parameters). The Mediant 3000 is also supplied with a Web interface.

For detailed information on how to fully configure the gateway refer to 'Device Initialization & Configuration Files' on page 25 and 'Configuration Using the Web Interface' on page 43.

The Mediant 3000 HA can be configured via EMS (refer to LTRT-9480x EMS Configuration Guide) or the Web interface (refer to 'Configuration Using the Web Interface' on page 43).

3.1 Assigning the Device IP Address

To assign an IP address to the Mediant 3000 use one of the following methods:

- HTTP using a Web browser (refer to "Assigning an IP Address Using HTTP" on page 21).
- BootP (refer to "Assigning an IP Address Using BootP" on page 22).
- DHCP (refer to 'Using BootP/DHCP').

The default device IP Addresses are shown below.

Default Networking Parameters

- Default IP address: 10.1.10.10
- Default subnet mask is 255.255.0.0
- Default gateway IP address is 0.0.0.0

3.1.1 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.

3.1.2 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' on page 15.

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

➢ **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.

3.2 Assigning the IP Addresses for High Availability Mode

The private IP address is assigned to the Active and Redundant blades (for maintenance) by using the BootP/DHCP.

➢ To assign Private IP addresses to the Mediant 3000 blades:

1. Start your BootP/DHCP Server application.
2. Add a client configuration for the Mediant 3000 that you wish to initialize and insert a local (private) IP address for each of the two Mediant 3000 blades.

> **Note:** Do not load a cmp or an ini file using a BootP/DHCP Server application. This action will erase the previous configuration that was stored to the flash memory of the Mediant 3000 device.

3. Power down the Mediant 3000.
4. Power up the Mediant 3000 system for 30 seconds.
5. Power down the Mediant 3000.
6. Power up the Mediant 3000 system within 15 seconds.
7. Using a BootP/DHCP Server application, verify that both blades in Slots 1 and 3 have received their local IP addresses.

> Note: A repeat power down and power up cycle, as described above, is necessary. By default the redundant and active blades are set to load the IP addresses from the flash memory and do not automatically send a BootP request.

➢ To assign an IP address via the CLI:

In the event that a BootP or DHCP server is not available in the network, the following method can be used to assign local (private) IP addresses to the Mediant 3000 blades.

1. Connect the blade’s RS-232 port to either COM1 or COM2 communication port on your PC using the serial cable supplied with the Mediant 3000.
2. Use a serial communication application (e.g., HyperTerminalTM) with the following communications port settings:

• Baud Rate:	115,200 bps
• Data Bits:	8
• Parity:	None
• Stop Bits:	1
• Flow Control:	None

3. The CLI prompt appears.
4. At the prompt, type **conf**, and then press <Enter>; the configuration folder is accessed.
5. Type **scp** ip <new private ip address> <netmask> <default gw>
(‘scp’ command stands for SetConfigParam) and then press <Enter>.

6. The new ip address is immediately being used (unless the blade is the active blade and it already uses the network IF table – global addresses).
7. Type **sar**.
   (save and reset) for saving and restarting with configured address.

Note: The **gcp ip** command can be used to see a current configured private address.

This private address are used for maintenance purposes and also used as a fallback in case of major system problem which prevents the system from working in HA mode.

In order for the system to be set to HA, the system's IP address(es) must be configured. The configured system address configuration is performed via the Interface Table using the EMS (Refer to LTRT-9480x EMS Configuration Guide) or Web interface (refer to Network on page 91). The configured system addresses should differ from private addresses. Managing the system is done by connecting to the Active blade private address (the Redundant blade management is blocked). If you don’t know which of the two private addresses belongs to the active blade, try both. Only one will answer to the EMS/Web connection attempt.

Note: HA will not be enabled until the system address has been configured.

4 System Initialization Process

This section describes the Initialization Procedures and Configuration Options for the Mediant 3000 System. It includes:

- Startup Process (see below)
- Configuration Parameters and Files (refer to 'Configuration Parameters and Files' on page 28)
- BootP/DHCP (refer to Using BootP/DHCP)
- Software Upgrade
- High Availability Aspects

4.1 Boot Firmware & Operational Firmware

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

- Boot firmware - Boot firmware (also known as flash software) resides in the device's non-volatile memory. When the device is reset, Boot firmware is initialized and the operational software is loaded into the SDRAM from a TFTP server or integral non-volatile memory. Boot firmware is also responsible for obtaining the device's IP parameters and ini file name (used to obtain the device's configuration parameters) via integral BootP or DHCP clients. The Boot firmware version can be viewed on the Web Interface. The last step the Boot firmware performs is to invoke the operational firmware.
- 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.

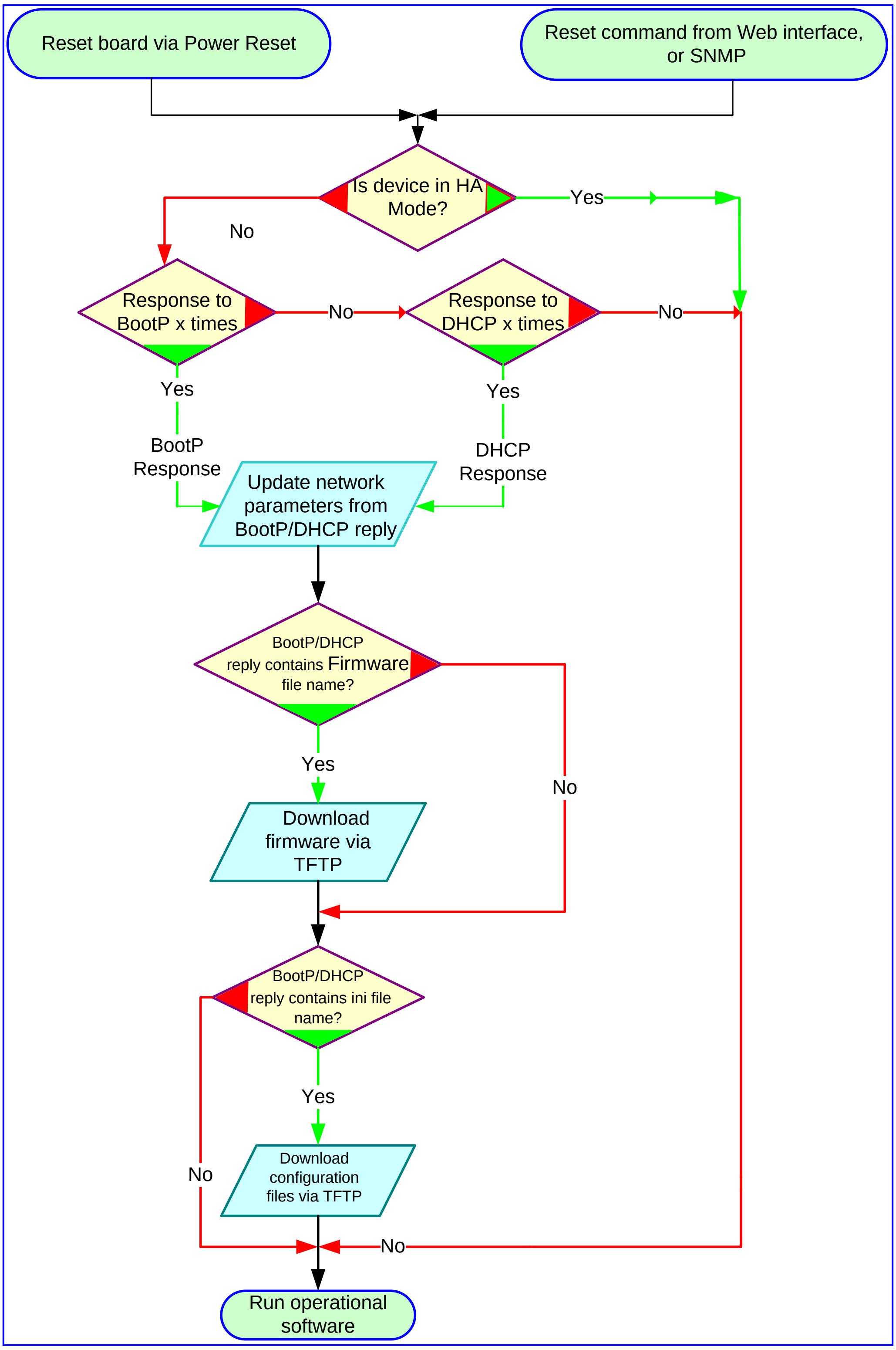
For more information on BootP/DHCP, refer to the Product Reference Manual.

Note: The ini, MIB and Utility files are available on the CD supplied with the device.

4.2 Startup Process

For more information on BootP/DHCP, refer to the Product Reference Manual.

Figure 5: Startup Process Diagram


Reset board via Power Reset
Reset command from Web interface, or SNMP
Is device in HA Mode?
Yes
No
Response to BootP x times
No
Response to DHCP x times
No
Yes
Yes
BootP Response
DHCP Response
Update network parameters from BootP/DHCP reply
BootP/DHCP reply contains Firmware file name?
Yes
No
Download firmware via TFTP
BootP/DHCP reply contains ini file name?
Yes
No
Download configuration files via TFTP
No
Run operational software

Notes:

- 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.

4.3 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').
- Web Interface (refer to 'Configuration Using the Web Interface' on page 43).
- Automatic Update facility (refer to 'Automatic Update Facility' on page 34).

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.

4.3.1 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'). 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 31).

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]
```

4.3.1.1 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.

ini File Examples

The example below shows a sample ini file for MGCP.

```

[TDM BUS configuration]
; 1=aLaw 3=ulaw
PCMLawSelect = 1
BaseUDPPort = 4000
[Trunk Configuration]
;E1_trans_31
ProtocolType = 5
; USER_TERMINATION_SIDE
TerminationSide = 0
; EXTENDED_SUPER_FRAME
FramingMethod = 0
;HDB3
LineCode = 2
[MGCP]
EndpointName = 'ACgw'
CallAgentIP = 10.1.2.34
[Channel Params]
DJBufferMinDelay = 75
RTPRedundancyDepth = 1
```

```
[Files]
CallProgressTonesFilename = 'CPUSA.dat'
VoicePromptsFilename = 'tpdemo_723.dat'
CasFilename = 'E_M_WinkTable.dat'

The example below shows a sample ini file for MEGACO.
[MEGACO]

; List of Call agents, separated by ','.
; The default is the loading computer.
PROVISIONEDCALLAGENTS = 10.2.1.254
; List of ports for the above Call Agents, separated by ','. The
default is 2944.
PROVISIONEDCALLAGENTSPORTS = 2944

; The next 2 fields are the termination names patterns.
; The first is the pattern for the physical termination, and the
; second is the pattern for the RTP termination. The '*' stands
for ; a number.
PHYSTERMNAMEPATTERN   = gws*c*
LOGICALRTPTERMPATTERN = gwRTP/*
; This parameter activates MEGACO. If omitted, MGCP will be active
MGCONTROLPROTOCOLTYPE = 2

; The following disables the keep-alive mechanism if set to 0,
; else it is enabled. Note that the recommended KeepAlive method
is
; the use of the inactivity timer package - 'it'.
KEEPALIVEENABLED = 1
;
; This parameter defines the profile used, and it is a bitmask
MGCPCOMPATIBILITYPROFILE = 2
```

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.

4.3.1.2 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, list of timers for a given application, etc.

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

4.3.1.2.1 Table Structure Rules

Tables are composed of four elements:

- Table-Title - The Table's string name in square brackets~~.~~
- Format Line - This line specifies the table's fields by their string names.
- 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]
```

4.3.1.2.2 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.

4.3.1.3 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.

4.3.1.3.1 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.

4.3.2 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 38.) 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.

4.3.2.1 Downloading Auxiliary Files via TFTP During the Blade Startup

Note: This is not applicable in HA mode.

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 device. The Voice Prompt buffer size in the blade is 10 Mbytes.
- 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.
- CASFileName_0…CASFileName_7 (or CASFileName) - The names (and path names) of the files containing the CAS protocol configuration. It is possible to use 1 to 8 files. The CASFileName name is still supported and can be used instead of the enumerated names when using only one CAS protocol file.
- CASTablesNum - Indicates how many CAS protocol configuration files are loaded. Its range is 1-8. It should match the number of "CASFileName_X" fields.
- CASTableIndex_TrunkNum (TrunkNum should be an integer) - This field is a CAS protocol file index. It indicates the CAS protocol file to use in a specific Trunk. The index value corresponds to the number in the field “CASFileName_X”.

4.3.3 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'


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
```

3. 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.
4. 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.
5. 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 re-instate 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 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.

4.5 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.
3.

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').

4.6 Software Upgrade Key

The Software Upgrade Key is a string stored in the device's non-volatile flash memory, defining the features and capabilities allowed by the specific license purchased by the customer. Customers specify the features and capabilities they require at the time they order the device. The device only allows users to utilize those features allowed by the integral Software Upgrade Key.

The device is supplied already pre-configured with a Software Upgrade Key according to the customer's order. Users can verify which features are allowed by the license using the Web interface GUI. (Refer to ''Software Upgrade Key'' on page 148).

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

4.7 High Availability

4.7.1 Initializing the Mediant 3000 System

For the system to be set up for High Availability, the following installation phases must be carried out:

- Hardware configuration setup as described in the Mediant 3000 and IPmedia 3000 SIP-MEGACO-MGCP Installation Manual. The system can be set up initially with only one blade and one SA/M3K blade, however, High Availability mode is only functional with a second blade and SA/M3K blade is added.
- The feature key includes the high availability feature and is installed on both of the blades. Refer to 'Software Upgrade Key - Web Server' on page 148. (If the High Availability feature was specified at the time the system was purchased, then it is already included on both of the blades).
- The Global IP Address is set using the Networking IF table blade parameter (burned to flash or received by the ini file, or set by SNMP – in which case the blade must be re-booted for the change to take effect) in the active blade to a valid IP address that is different than the local IP address of the blades, but with the same subnet. Refer to 'Assigning the IP Addresses for High Availability Mode' on page 23.
- System was loaded from flash (when loading from BootP/TFTP, on first configuration setup the High Availability mode is disabled).

4.7.2 Device Initialization Process

- Each blade is initialized as Active or Redundant according to its placement in the chassis and the status of the SDH interface.
- An Active blade is identified by a green light in ACT led on the blade front panel.
- Synchronization between active and redundant blades can take several minutes in which the active blade forwards to the redundant blade, all its current configuration data, including files such as voice prompt, call progress tone and even its software (cmp file). If necessary, a second boot of the redundant blade is issued in order to apply the new configuration.
- After the synchronization has ended, the redundant blade is identified by a blinking yellow light in ACT led.
- The redundant blade is disconnected from the external network and has an internal connection with the active blade only. This means that the user does not interact directly with the redundant blade.

4.7.3 Special System Specific Behavior

4.7.3.1 Rebooting the Blade

Both blades are set to load from Flash, even after power-off /power-on reset.

The system needs to load from BootP/TFTP in the following cases:

- when the private IP addresses need to be set (at the first configuration or if they need to be changed)
- when the system cannot be loaded from Flash (bad configuration, etc.)

If the system needs to be loaded from BootP/TFTP, a double hardware reset is needed. After the first reset, wait approximately 20 seconds and then perform a second hardware reset.

4.7.3.2 High Availability and Syslog

All High Availability main operations and events are printed to the Syslog with the prefix: "M3K_HA".

All Syslog messages and events of the redundant blade are printed to the Syslog by the active blade with the appropriate message prefix.

4.7.4 Actions upon Detecting Blade Failure

4.7.4.1 Failure in the Active Blade

In the event that an Active blade fails, the Redundant (Standby) blade issues a switch-over operation. As part of this switch-over operation, the failed blade is reset and the initially Redundant (Standby) blade becomes the Active blade in Simplex mode, until a redundant blade is detected.

If the failure in the active blade is fixed after reset, it is initialized as the redundant blade and the Device system returns to High Availability mode.

4.7.4.2 Failure in the Redundant Blade

In the event that a Redundant blade fails, the Active blade resets the redundant blade and switches to Simplex mode until the redundant blade is returned to functional operation.

If the failure in the redundant blade is fixed after reset, it is initialized as the redundant blade again and the Device system returns to High Availability mode.

4.7.5 Hitless Software Upgrade

The Mediant 3000 HA system allows you to upgrade the software (SW) version (i.e., cmp file) running on the device, without disrupting current calls. This non-effecting traffic upgrade feature is referred to as Hitless Software Upgrade.

The Hitless Software Upgrade process is as follows:

The user loads a new software version file to the device using the EMS/Web. The file is received by the Active blade, which then forwards it to the Redundant blade.

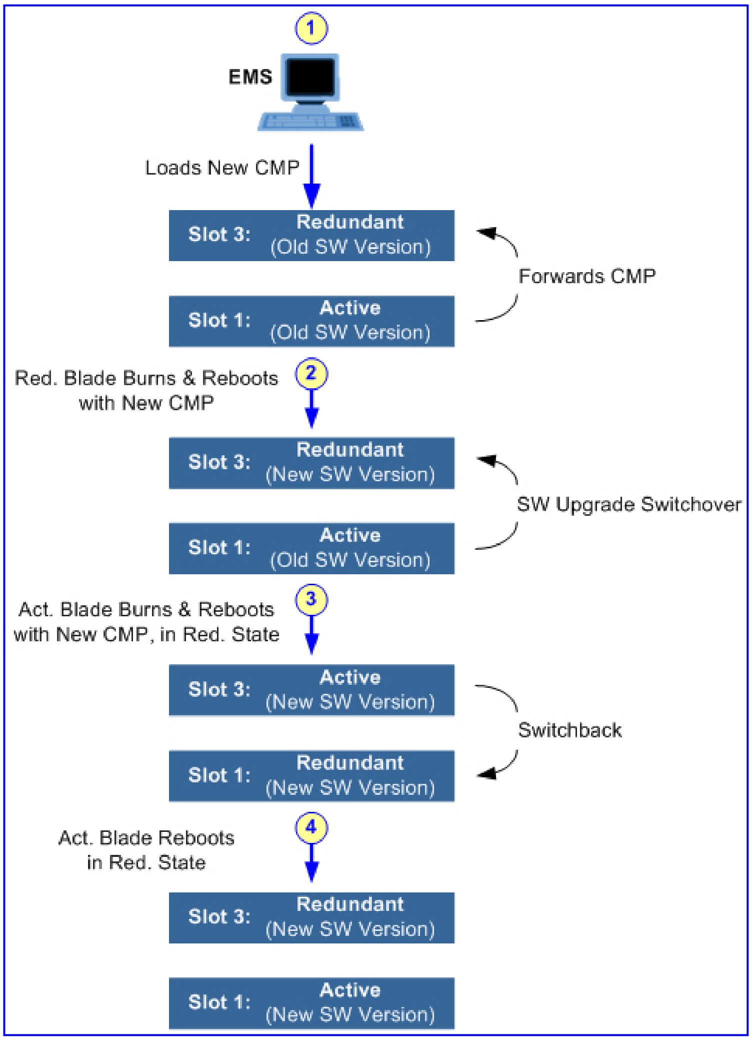
The Redundant blade 'burns' the file to its flash memory, and then resets (loading the new software file saved in the flash memory).

The Redundant blade performs a switchover from the Active blade (running the previous software version). This switchover process includes translation of all required database and blade states. After switchover, existing calls continue as normal. The Redundant blade now becomes active and from this stage, the system operates with the new SW version.

The previously Active blade burns the new software version file to its flash memory, and then resets in Redundant mode.

Both blades now operate with the new software version and a switchback is issued to return the system to its original state. The previously Active blade now becomes active, and the previously Redundant blade resets once more to return to redundant state.

Figure 6: Hitless Software Upgrade


1
EMS
Loads New CMP
Slot 3: Redundant (Old SW Version)
Slot 1: Active (Old SW Version)
Forwards CMP
Red. Blade Burns & Reboots with New CMP
2
Slot 3: Redundant (New SW Version)
Slot 1: Active (Old SW Version)
SW Upgrade Switchover
Act. Blade Burns & Reboots with New CMP, in Red. State
3
Slot 3: Active (New SW Version)
Slot 1: Redundant (New SW Version)
Switchback
Act. Blade Reboots in Red. State
4
Slot 3: Redundant (New SW Version)
Slot 1: Active (New SW Version)

This page is intentionally left blank.

5 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 74).
- Verify configuration changes in the Status pages (refer to ''Status and Diagnostic Menu'' on page 161) or Toolbar (refer to 'Getting Acquainted with the Web Interface' on page 47.
- Load the CMP file (refer to 'Software Upgrade Wizard' on page 151).
- Load the ini, CAS, Voice Prompt, CPT, Prerecorded Tones, Dial Plan, Coder Table, and AMD Sensitivity Files (refer to 'Load Auxiliary Files' on page 147).

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

5.1 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.

5.2 Disabling the Web Interface

5.2.1 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.

5.2.2 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.

5.2.3 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.

5.3 Initial Device Configuration using the Web Interface

When configuring a device for the first time using the Web interface, change the PC's IP address and Subnet Mask to correspond with the device's factory default IP address and Subnet Mask shown below. For details on changing the IP address and Subnet Mask, refer to the Help information provided by the Operating System used.

- Default IP Address: 10.1.10.10
- Default Subnet Mask: 255.255.0.0

5.4 Accessing the Web Interface

➢ **To access the Web interface:**

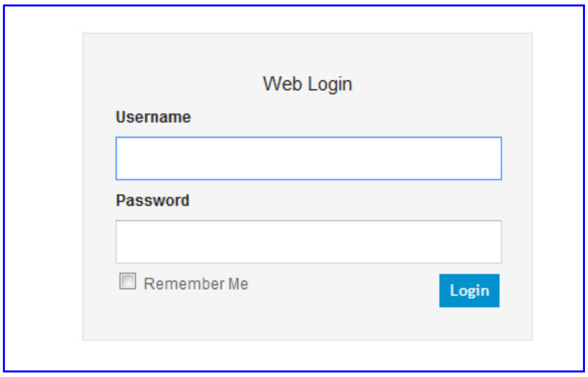
1. Open any standard Web-browser application, such as Microsoft™ Internet Explorer™ (Ver. 6.0 and higher) or Firefox™ (Ver. 2.5 and higher).

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 7: Enter Network Password Screen



5.5 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.
```

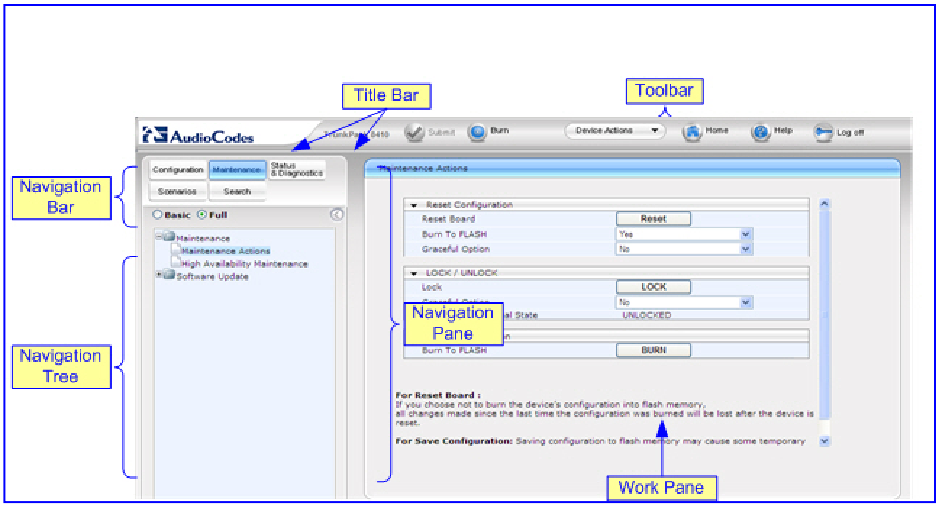
➢ **To troubleshoot blocked access to Internet Explorer:**

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.

5.6 Getting Acquainted with the Web Interface

The figure below displays the general layout of the GUI of the Web interface:

Figure 8: Areas of the Web GUI



Reset Board: Reset
Burn To FLASH: Yes
Graceful Option: No
Lock: LOCK
Graceful Option: No
Operational State: UNLOCKED
Burn To FLASH: 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

The Web GUI is composed of the following main areas:

- Title Bar: Displays the corporate logo and device name. For replacing the logo with another image or text, refer to Replacing the Corporate Logo. For customizing the device name, refer to Customizing the Product Name.
- Toolbar: Provides frequently required command buttons for configuration (refer to 'Toolbar' below).
- Navigation Pane: Consists of the following areas:
  - Navigation bar: Provides tabs for accessing the configuration menus (refer to 'Navigation Tree' below), creating a Scenario (refer to 'Working with Scenario' on page 56), and searching ini file parameters that have corresponding Web interface parameters (refer to 'Searching for Configuration Parameters' on page 55 below).
  - Navigation tree: Displays the elements pertaining to the tab selected on the Navigation bar (tree-like structure of the configuration menus, Scenario Steps, or Search engine).
- Work pane: Displays configuration pages where all configuration is performed (refer to 'Working with Configuration Pages' on page 51).

5.6.1 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 142). Restore Defaults: Opens the 'Configuration File' page for restoring the parameters default values (refer to Restoring Networking Parameters to their Default Values). 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' on page 145). Reset Redundant: Opens the "High Availability Maintenance" page for resetting the Redundant Board (refer to 'High Availability Maintenance' on page 145).
🏠	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 64).
🔑	Log off	Logs off a session with the Web interface (refer to 'Logging Off the Web Interface' on page 65).

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.

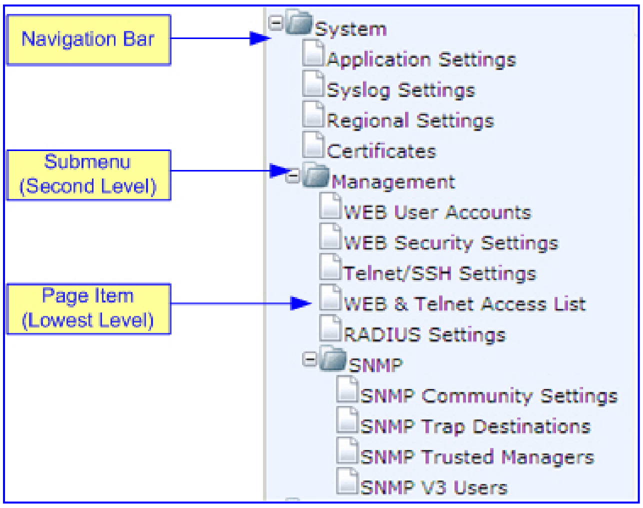
5.6.2 Navigation Tree

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 9: 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:**

8. Navigate to the required page item, by performing the following:
   - Drilling-down using the plus ⊞ signs to expand the menus and submenus
   - Drilling-up using the minus ⊟ signs to collapse the menus and submenus
9. Select the required page item; the page opens in the Work pane.

5.6.2.1 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:

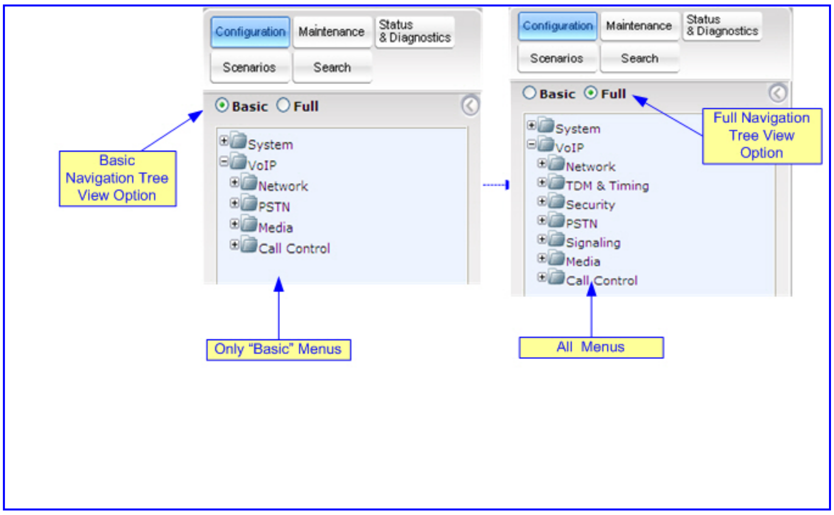
- Basic - Displays only commonly used menus
- Full - Displays all the menus pertaining to a configuration tab

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 10: Navigation Tree in Basic and Full View



Note: When in Scenario mode (refer to 'Working with Scenarios' on page 56), the Navigation tree is displayed in 'Full' view (i.e., all menus are displayed in the Navigation tree).

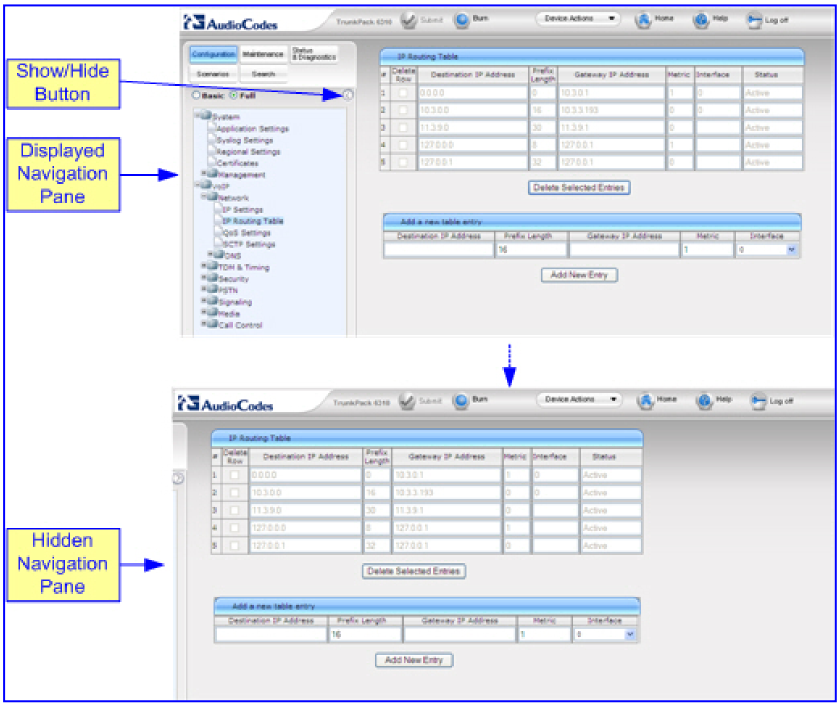
5.6.2.2 Showing / Hiding the Navigation Pane

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 11: Showing and Hiding Navigation Pane



IP Routing Table

#	Delete Row	Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface	Status
1	□	0.0.0.0	0	10.3.0.1	1	0	Active
2	□	10.3.0.0	16	10.3.3.193	0	0	Active
3	□	11.3.9.0	30	11.3.9.1	0		Active
4	□	127.0.0.0	8	127.0.0.1	1		Active
5	□	127.0.0.1	32	127.0.0.1	0		Active

Add a new table entry

Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface
	16		1	0

5.6.3 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.

5.6.3.1 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 64.
- 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 78). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.

5.6.3.2 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.

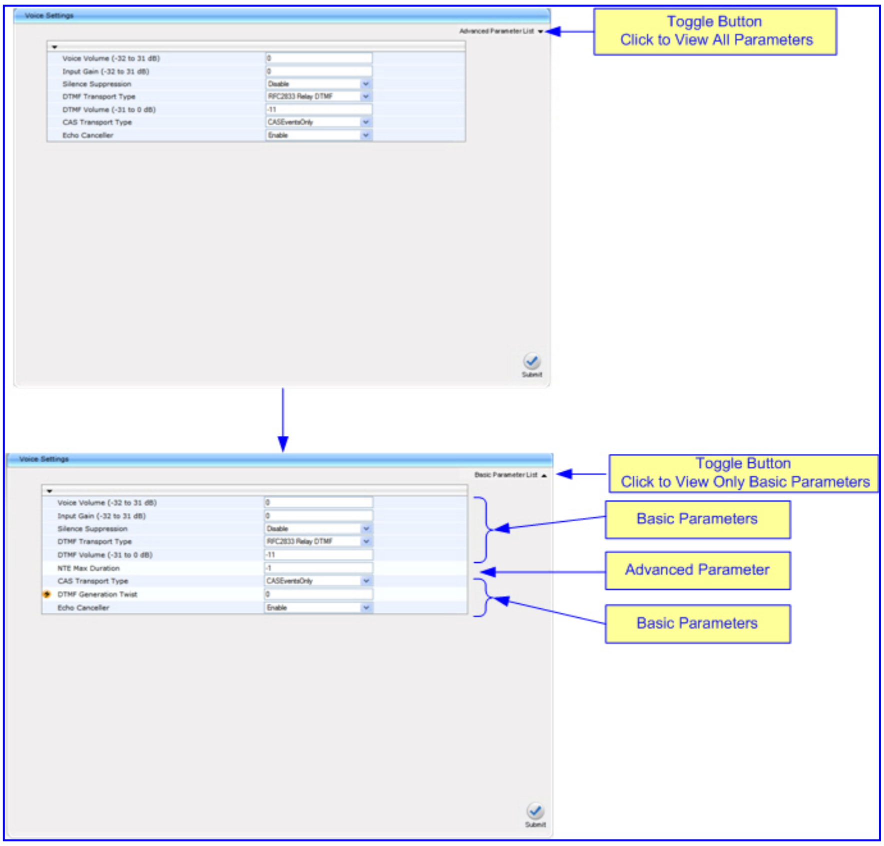
5.6.3.3 Displaying Basic and Advanced Parameters

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: Basic and Advanced Parameters



Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
DTMF Transport Type	RFC2833 Relay DTMF
DTMF Volume (-31 to 0 dB)	-11
CAS Transport Type	CASEventsOnly
Echo Canceller	Enable

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

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

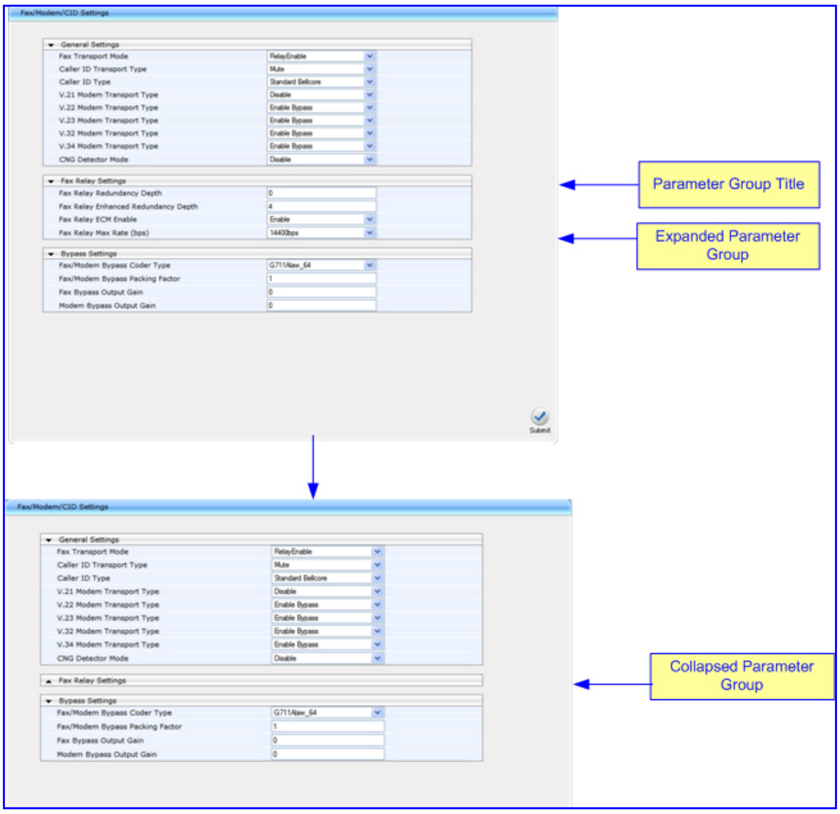
Notes:

- 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.

5.6.3.4 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



Fax/Modem/CID Settings

General Settings

Fax Transport Mode	RelayEnable
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

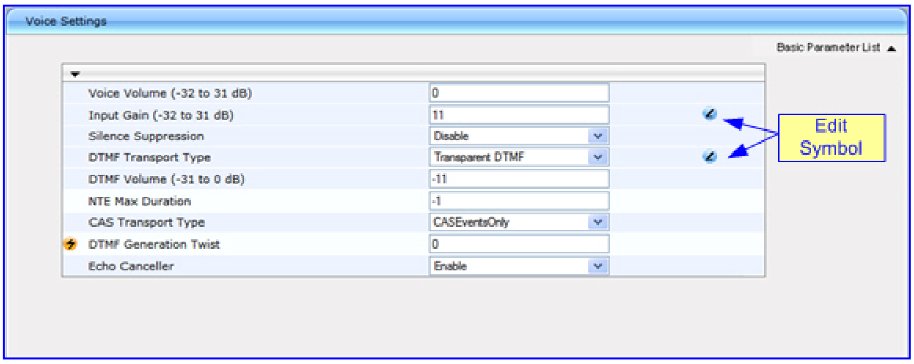
Bypass Settings

Fax/Modem Bypass Coder Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

5.6.3.5 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



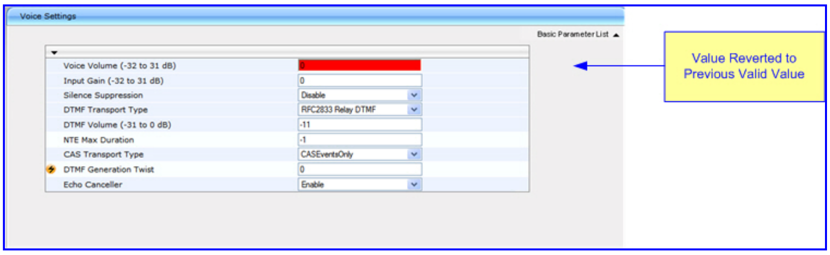
Voice Settings

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

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



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

Value Reverted to Previous Valid Value

5.6.4 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.

5.6.5 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.

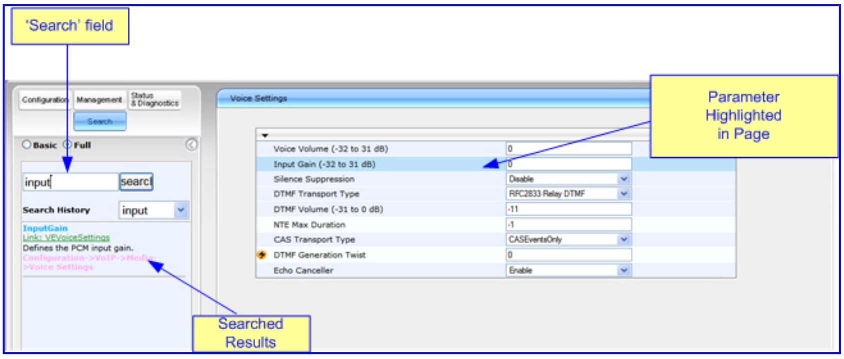
➢ **To search for ini file parameters configurable in the Web interface:**

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



input

Search History: input

InputGain
Link: VEVoiceSettings
Defines the PCM input gain.
Configuration->VoIP->Media->Voice Settings

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

5.6.6 Working with Scenarios

The Web interface allows you to create your own "menu" with up to 20 pages selected from the menus in the Navigation tree (i.e., pertaining to the Configuration, Maintenance, and Status & Diagnostics tabs). The "menu" is a set of configuration pages grouped into a logical entity referred to as a Scenario. Each page in the Scenario is referred to as a Step. For each Step, you can select up to 25 parameters in the page that you want available in the Scenario. Therefore, the Scenario feature is useful in that it allows you quick-and-easy access to commonly used configuration parameters specific to your network environment. When you login to the Web interface, your Scenario is displayed in the Navigation tree, thereby, facilitating your configuration.

Instead of creating a Scenario, you can also load an existing Scenario from a PC to the device (refer to 'Loading a Scenario to the Device' on page 62).

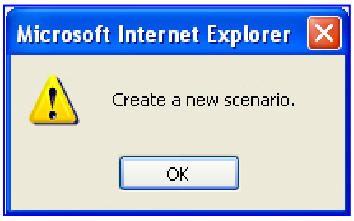
5.6.6.1 Creating a Scenario

The Web interface allows you to create one Scenario with up to 20 configuration pages, as described in the procedure below:

➢ **To create a Scenario:**

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm creation of a Scenario:

Figure 17: Scenario Confirm Message Box



Microsoft Internet Explorer

Create a new scenario.

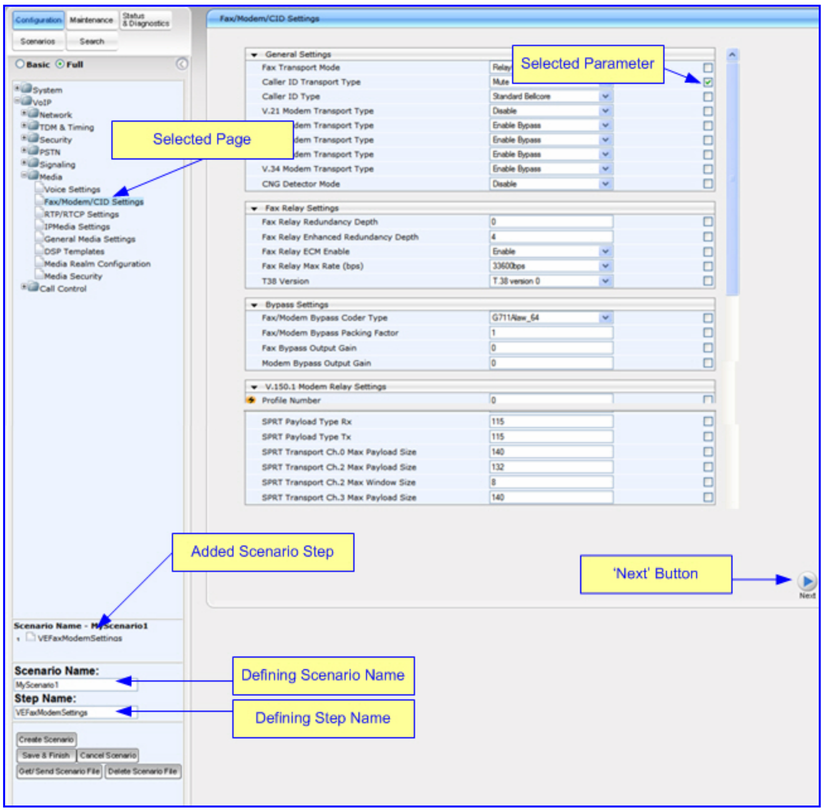
Note: If a Scenario already exists, the Scenario Loading message box appears.

2. Click **OK**; the Scenario mode appears in the Navigation tree as well as the menus of the Configuration tab.

Note: If a Scenario already exists and you wish to create a new one, click the **Create Scenario** button, and then click **OK** in the subsequent message box.

3. In the 'Scenario Name' field, enter an arbitrary name for the Scenario.
4. On the Navigation bar, click the Configuration or Maintenance tab to display their respective menus in the Navigation tree.
5. In the Navigation tree, select the required page item for the Step, and then in the page itself, select the required parameters by selecting the check boxes corresponding to the parameters.
6. In the 'Step Name' field, enter a name for the Step.
7. Click **Next** located at the bottom of the page; the Step is added to the Scenario and appears in the Scenario Step list:

Figure 18: Creating a Scenario



Fax/Modem/CID Settings

General Settings

Fax Transport Mode	Relay	□
Caller ID Transport Type	Mute	☑
Caller ID Type	Standard Bellcore	□
V.21 Modem Transport Type	Disable	□
dem Transport Type	Enable Bypass	□
dem Transport Type	Enable Bypass	□
dem 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)	33600bps	□
T38 Version	T.38 version 0	□

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	□

V.150.1 Modem Relay Settings

Profile Number	0	□
SPRT Payload Type Rx	115	□
SPRT Payload Type Tx	115	□
SPRT Transport Ch.0 Max Payload Size	140	□
SPRT Transport Ch.2 Max Payload Size	132	□
SPRT Transport Ch.2 Max Window Size	8	□
SPRT Transport Ch.3 Max Payload Size	140	□

Scenario Name - MyScenario1

VEFaxModemSettings

Scenario Name: MyScenario1

Step Name: VEFaxModemSettings

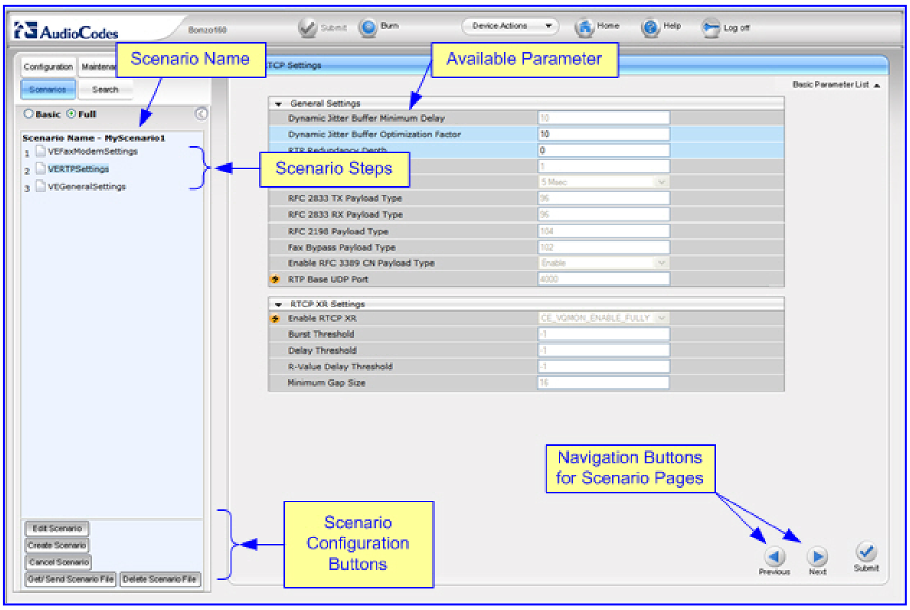
8. Repeat steps 5 through 8 to add additional Steps (i.e., pages).
9. When you have added all the required Steps for your Scenario, click **Save & Finish** located at the bottom of the Navigation tree; a message box appears informing you that the Scenario has been successfully created.
10. Click **OK**; the Scenario mode has ended and the menu tree of the Configuration tab appears in the Navigation tree.

Once you have created the Scenario, you can access it at any time by following the procedure below:

➢ To access the Scenario:

- On the Navigation bar, select the Scenario tab; the Scenario appears in the Navigation tree, as shown in the example figure below:

Figure 19: Scenario Example



General Settings

Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
	1
	5 Msec
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

RTCP XR Settings

Enable RTCP XR	CE_VQMON_ENABLE_FULLY
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
Minimum Gap Size	16

When you select a Scenario Step, the corresponding page is displayed in the Work pane. The available parameters are indicated by a dark-blue background; the unavailable parameters are indicated by a gray or light-blue background.

To navigate between Scenario Steps, you can perform one of the following:

- In the Navigation tree, click the required Scenario Step.
- In an opened Scenario Step, use the following navigation buttons:
  - ▶ Next: opens the next Step listed in the Scenario.
  - ◀ Previous: opens the previous Step listed in the Scenario.

Notes:

- Up to 20 Steps can be added to a Scenario, where each Step can contain up to 25 parameters.
- If you reset the device while in Scenario mode, after the device resets you are returned once again to the Scenario mode.
- When in Scenario mode, the Navigation tree is in 'Full' display (i.e., all menus are displayed in the Navigation tree) and the configuration pages are in 'Advanced Parameter List' display (i.e., all parameters are shown in the pages). This ensures accessibility to all parameters when creating a Scenario. For a description on the Navigation tree views, refer to Navigation Tree.
- If you previously created a Scenario and you click the Create Scenario button, the previous Scenario is deleted and replaced with the one you are creating.

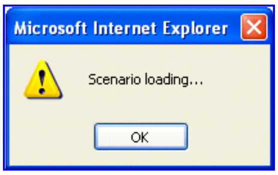
5.6.6.2 Editing a Scenario

You can modify a Scenario anytime by adding or removing Steps (i.e., pages) or parameters, and changing the Scenario name and the Steps' names.

➢ **To edit a Scenario:**

On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm Scenario loading.

Figure 20: Scenario Loading Message Box



Microsoft Internet Explorer

Scenario loading...

1. Click **OK**; the Scenario appears with its Steps in the Navigation tree.
2. Click the **Edit Scenario** button located at the bottom of the Navigation pane; the 'Scenario Name' and 'Step Name' fields appear.
3. You can perform the following operations:
   - **Add Steps:**
     a. On the Navigation bar, select the required tab (i.e., Configuration or Maintenance); the tab's menu appears in the Navigation tree.
     b. In the Navigation tree, navigate to the required page item; the corresponding page opens in the Work pane.
     c. In the page, select the required parameter(s) by marking the corresponding check box(es).
     d. Click **Next**.
   - **Add or Remove Parameters:**
     a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
     b. To add parameters, select the check boxes corresponding to the required parameters; to remove parameters, clear the check boxes corresponding to the parameters that you want removed.
     c. Click **Next**. A message box appears informing you that the Scenario step has been successfully modified.
     d. Click **OK**.
   - **Edit the Step Name:**
     a. In the Navigation tree, select the required Step.
     b. In the 'Add Step name' field, modify the Step name.
     c. In the page, click **Next**.
   - **Edit the Scenario Name:**
     a. In the 'Scenario Name' field, edit the Scenario name.
     b. In the displayed page, click **Next**.
   - **Remove a Step:**
     a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
     b. In the page, clear all the check boxes corresponding to the parameters.
     c. Click **Next**.
     d. After clicking Next, a message box appears notifying you of the change. Click **OK**.

4. Click **Save & Finish**; a message box appears informing you that the Scenario has been successfully modified. The Scenario mode is exited and the menus of the Configuration tab appear in the Navigation tree.

> **Note:** To delete a Scenario, you can either load an empty dat file (refer to 'Loading a Scenario to the Device' on page 62) or load an ini file with the ScenarioFileName value set to a file that has no content.

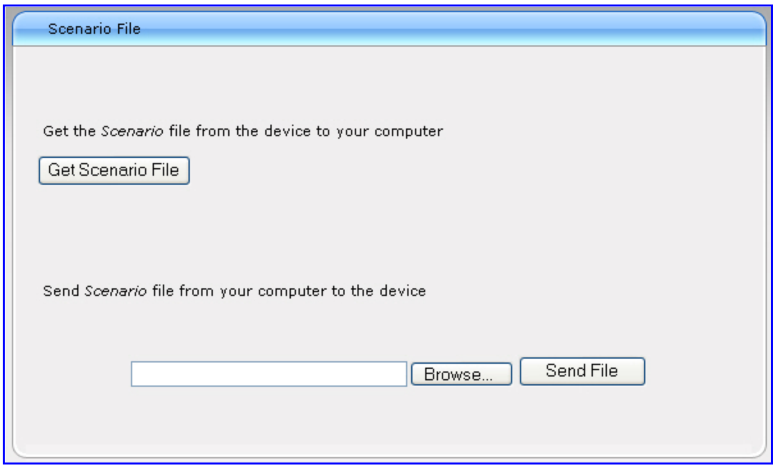
5.6.6.3 Saving a Scenario to a PC

You can save a Scenario to a PC (as a dat file). This is especially useful when you require more than one Scenario to represent different environment setups (e.g., where one includes PBX interoperability and another not). Once you create a Scenario and save it to your PC, you can then keep on saving modifications to it under different Scenario file names. When you require a specific network environment setup, you can simply load the suitable Scenario file from your PC (refer to 'Loading a Scenario to the Device' on page 62).

➢ **To save a Scenario to a PC:**

1. On the Navigation bar, click the Scenarios tab; the Scenario appears in the Navigation tree.
2. Click the Get/Send Scenario File button (located at the bottom of the Navigation tree); the 'Scenario File' page appears, as shown below:

Figure 21: Scenario File Page



Scenario File

Get the *Scenario* file from the device to your computer

Send *Scenario* file from your computer to the device

3. Click **Get Scenario File**.

5.6.6.4 Loading a Scenario to the Device

Instead of creating a Scenario, you can load a Scenario file (data file) from your PC to the device.

➢ **To load a Scenario to the device:**

1. On the Navigation bar, click the Scenarios tab; the Scenario appears in the Navigation tree.
2. Click the Get/Send Scenario File button (located at the bottom of the Navigation tree); the 'Scenario File' page appears (refer to 'Saving a Scenario to a PC' on page 61).
3. Click the **Browse** button, and then navigate to the Scenario file stored on your PC.
4. Click the **Send File** button.

Notes:

- The loaded Scenario replaces any existing Scenario.
- Instead of using the Web Interface, you can load an ini file to the device with the ScenarioFileName ini file parameter.

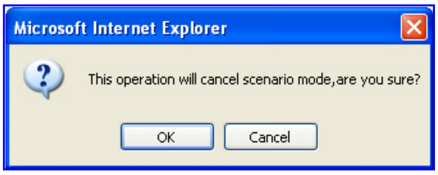
5.6.6.5 Exiting Scenario Mode

When you want to close the Scenario mode after using it for device configuration, follow the procedure below:

➢ **To close the Scenario mode:**

1. Simply click any tab (besides the Scenarios tab) on the Navigation bar, or click the Cancel Scenarios button located at the bottom of the Navigation tree; a message box appears, requesting you to confirm exiting Scenario mode, as shown below.

Figure 22: Confirmation Message for Exiting Scenario Mode



This operation will cancel scenario mode,are you sure?

2. Click **OK** to exit.

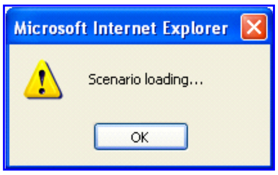
5.6.6.6 Deleting a Scenario

You can delete the Scenario by using the Delete Scenario File button, as described in the procedure below:

➢ **To delete the Scenario:**

1. On the Navigation bar, click the Scenarios tab; a message box appears, requesting you to confirm:

Figure 23: Scenario Loading Message Box

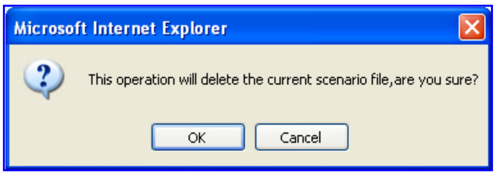


Scenario loading...

2. Click **OK**; the Scenario mode appears in the Navigation tree.

3. Click the Delete Scenario File button; a message box appears requesting confirmation for deletion.

Figure 24: Message Box for Confirming Scenario Deletion



This operation will delete the current scenario file,are you sure?

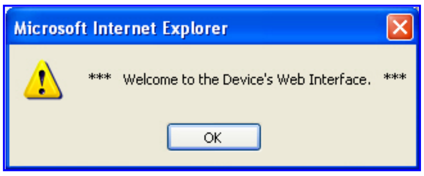
4. Click **OK**; the Scenario is deleted and the Scenario mode closes.

5.6.7 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 25: User-Defined Web Welcome Message after Login



*** Welcome to the Device's Web Interface. ***

ini File Parameter for Welcome Login Message

Parameter	Description
WelcomeMessage	Defines the Welcome message that appears after a successful login to the Web interface. The format for this ini file parameter table is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "..." ; WelcomeMessage 2 = "..." ; WelcomeMessage 3 = "..." ; [\WelcomeMessage] For Example: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "***********************************" ; WelcomeMessage 2 = "********* This is a Welcome message ***" ; WelcomeMessage 3 = "***********************************" ; [\WelcomeMessage] Note: Each index represents a line of text in the Welcome message box.

ini File Parameter for Welcome Login Message

Parameter	Description
	Up to 20 indices can be defined.

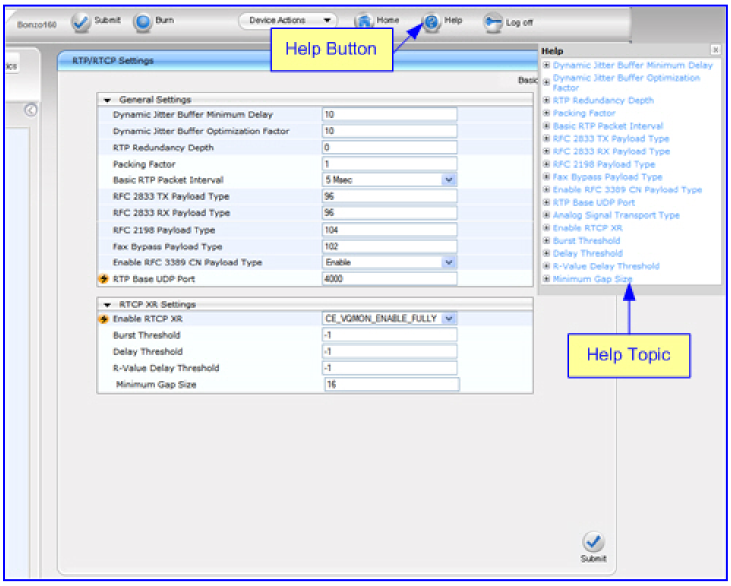
5.6.8 Getting Help

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 26: Help Topic for Current Page



RTP/RTCP Settings

General Settings

Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	5 Msec
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

RTCP XR Settings

Enable RTCP XR	CE_VQMON_ENABLE_FULLY
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
Minimum Gap Size	16

Help

- ⊞ Dynamic Jitter Buffer Minimum Delay
- ⊞ Dynamic Jitter Buffer Optimization Factor
- ⊞ RTP Redundancy Depth
- ⊞ Packing Factor
- ⊞ Basic RTP Packet Interval
- ⊞ RFC 2833 TX Payload Type
- ⊞ RFC 2833 RX Payload Type
- ⊞ RFC 2198 Payload Type
- ⊞ Fax Bypass Payload Type
- ⊞ Enable RFC 3389 CN Payload Type
- ⊞ RTP Base UDP Port
- ⊞ Analog Signal Transport Type
- ⊞ Enable RTCP XR
- ⊞ Burst Threshold
- ⊞ Delay Threshold
- ⊞ R-Value Delay Threshold
- ⊞ Minimum Gap Size

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.

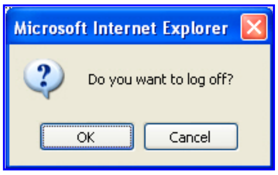
5.6.9 Logging Off the Web Interface

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 27: Log Off Confirmation Box



Do you want to log off?

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.

5.7 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, firmware version and the High Availability status.

Using a High Availability configuration, the ‘General Information’ pane displays additional information showing the High Availability status and the Active Board Slot Number. In MEGACO It also includes information about the status of the connection to the call agent.

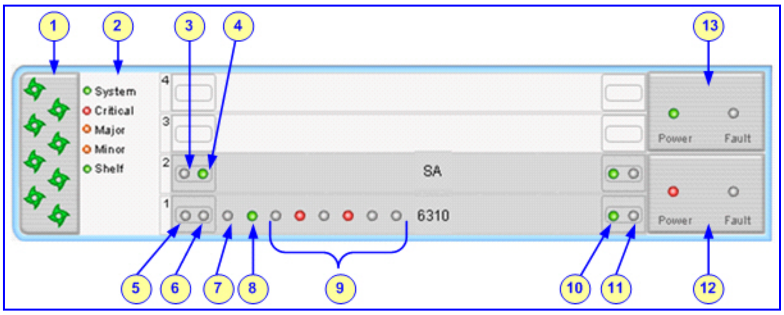
5.7.1 TP-6310

➢ **To access the Home page:**

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

Note: The following 'Home' page is applicable to the 6310/3000 devices using Simplex configuration (without High Availability). Refer to 'High Availability Configuration' on page 72 for more information.

Figure 28: 6310/3000 Home Page using Simplex Configuration



6310/3000 Home Page Descriptions

Item# / Label	Description
1	Fan Tray unit displaying operating status of fans: ✣ (green): normal operation ✣ (red): fan failure or fan missing You can also view current alarms, by clicking anywhere in this area (refer to 'Viewing the Active Alarms Table' on page 70).
2	System unit displaying chassis severity alarm LEDs: ● (green): no alarm - normal functioning. ● (red): Critical, Shelf, and / or System alarm raised ●(orange): Major and / or Minor alarm raised

6310/3000 Home Page Descriptions

Item# / Label	Description
3	SA/M3K Alarms and Status blade's FAIL LED: ● (gray): Normal functioning. ● (red): Blade failure.
4	SA/M3K Alarms and Status blade's ACT LED: ● (gray): Single blade. ● (green): Active blade. ● (orange): Standby blade.
5	6310 blade's FAIL LED: ● (gray): Normal functioning. ● (red): Blade failure.
6	6310 blade's ACT LED: ● (gray): Single blade. ● (green): Active blade. ● (orange): Standby blade.
7 & 8	Dual Ethernet port status LEDs (Eth 1 and Eth 2): ● (gray): No link. ● (green): Active Ethernet link. ● (yellow): Redundant link. (Not applicable to IPM) You can also view detailed information (in the 'Ethernet Port Information' page) of an Ethernet port, by clicking the LED icon (refer to 'Viewing Ethernet Port Information' on page 71).
9	PSTN LEDs grouped in pairs, each displaying a PSTN Link LED (left LED) with a PSTN Alarm LED (right LED). The PSTN Link LED indicates the status of the PSTN link, while the PSTN Alarm LED indicates the traffic loss alarm type associated with the PSTN link. PSTN Link LED: ● (gray): No link. ● (green): Active link (for optical STM1/OC3 interface) or “DS3 Synchronized” (for DS3 interface). ● (yellow): Standby link. ● (red): PSTN alarm. PSTN Alarm LED: ● (gray): No alarm (for optical STM1/OC3 interface) or “No Near-end Alarm” (for DS3 interface). ● (red): PSTN alarm exists. ● (orange): D-channel alarm (ISDN only) ● (dark orange): NFAS alarm (ISDN only) You can also view and modify PSTN link settings, by clicking the PSTN Settings - Transmission Settings menu option in the Web Interface (refer to Viewing and Modifying PSTN Settings).

6310/3000 Home Page Descriptions

Item# / Label	Description
10	Power status (PWR LED) of the blade: 🟢 (green): Power received by blade. 🔴 (red): No power received by blade.
11	Slot status of installed blade in the chassis (SWAP Ready LED).
12 & 13	Power supply units (PS/DC/3K modules) LED (Power Supply Number 1 & 2 LED): 🟢 (green): Normal functioning. 🔴 (red): Power failure.

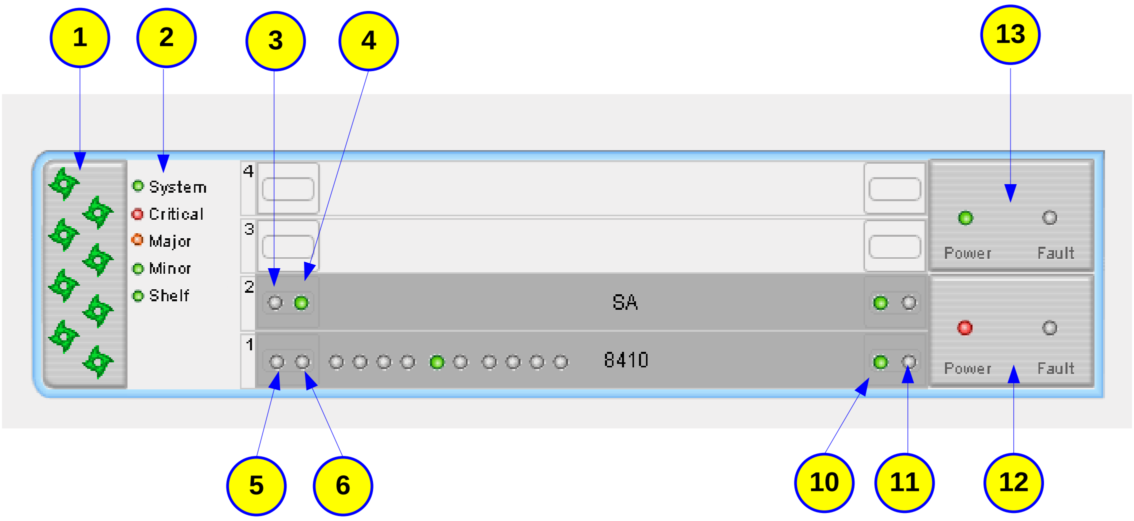
5.7.2 TP-8410

➢ **To access the Home page, take this step:**

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

> **Note:** The following 'Home' page is applicable to the 8410/3000 devices using the Simplex configuration (without High Availability). Refer to 'High Availability Configuration' on page 72 for more information.

Figure 29: TP-8410 Home Page



Mediant 3000/TP-8410 Home Page Descriptions

Item# / Label	Description
1	Fan Tray unit displaying operating status of fans: ✤ (green): normal operation ✤ (red): fan failure or fan missing You can also view current alarms, by clicking anywhere in this area (refer to 'Viewing the Active Alarms Table' on page 70).
2	System unit displaying chassis severity alarm LEDs: ● (green): no alarm - normal functioning. ● (red): Critical, Shelf, and / or System alarm raised ●(orange): Major and / or Minor alarm raised
3	SA/M3K Alarms and Status blade's FAIL LED: ● (gray): Normal functioning. ● (red): Blade failure.

Mediant 3000/TP-8410 Home Page Descriptions

Item# / Label	Description
4	SA/M3K Alarms and Status blade's ACT LED: ● (gray): Single blade. ● (green): Active blade. ● (orange): Standby blade.
5	8410 blade's FAIL LED: ● (gray): Normal functioning. ● (red): Blade failure.
6	8410 blade's ACT LED: ● (gray): Single blade. ● (green): Active blade. ● (orange): Standby blade.
10	Power status (PWR LED) of the blade: ● (green): Power received by blade. ● (red): No power received by blade.
11	Slot status of installed blade in the chassis (SWAP Ready LED).
12 & 13	Power supply units (PS/DC/3K modules) LED (Power Supply Number 1 & 2 LED): ● (green): Normal functioning. ● (red): Power failure

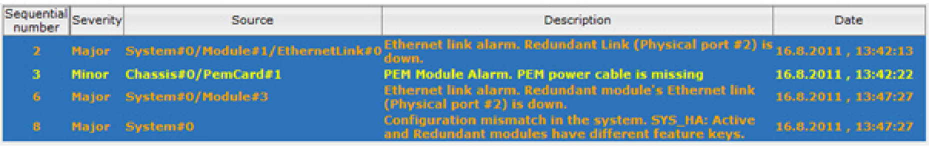
5.7.3 Viewing the Active Alarms Table

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 30: 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

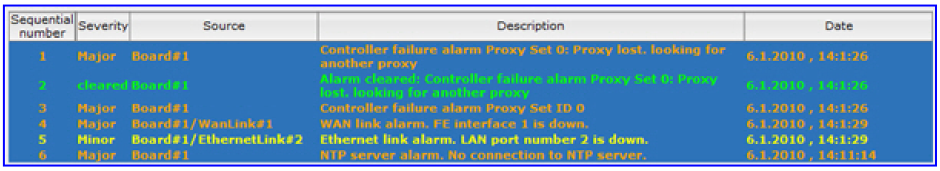
5.7.3.1.1 Viewing Alarm History

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 31: 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 (range)
- 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:**

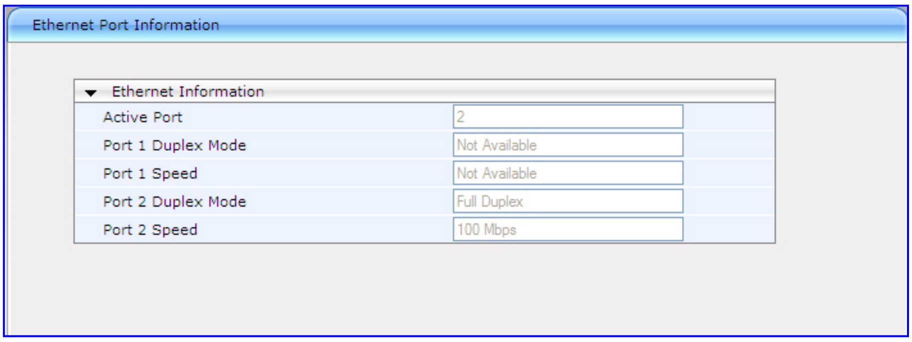
2. Click the **Delete History Table** button; a confirmation message box appears.
3. Click **OK** to confirm.

5.7.4 Viewing Ethernet Port Information

➢ **To view Ethernet port settings via the Home page:**

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

Figure 32: Ethernet Port Information



Ethernet Port Information

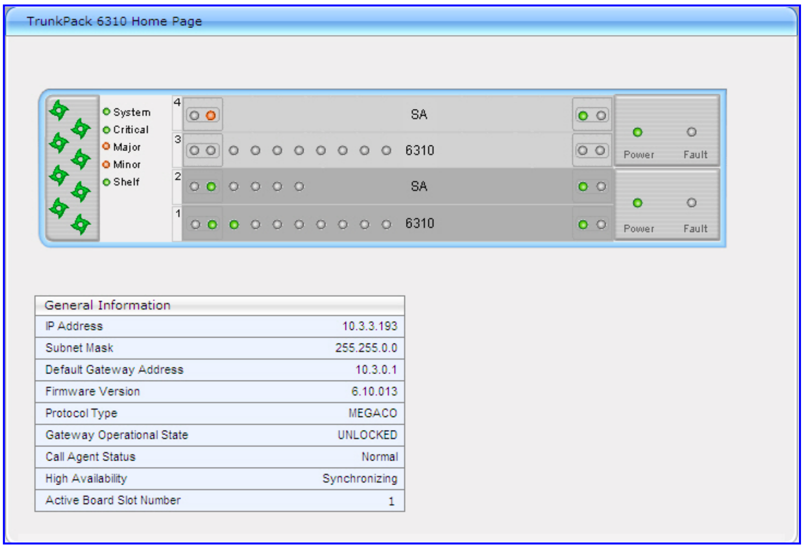
▼ Ethernet Information

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

5.7.5 High Availability Configuration

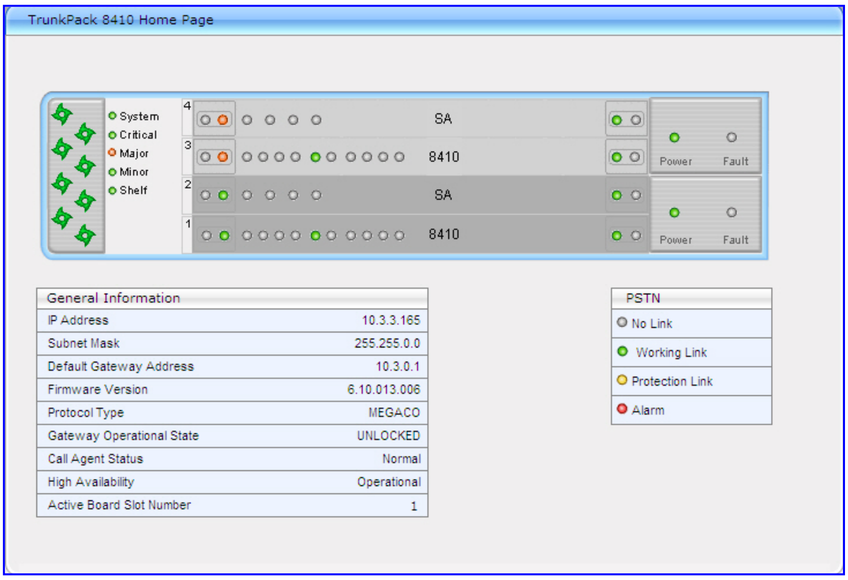
Once the Mediant 3000 setup is using High Availability, additional information and options will be available via the Web interface. A sample Mediant 3000 Home Page with High Availability is shown below.

Figure 33: Mediant 3000 with TP-6310 Home Page using High Availability Setup



General Information	
IP Address	10.3.3.193
Subnet Mask	255.255.0.0
Default Gateway Address	10.3.0.1
Firmware Version	6.10.013
Protocol Type	MEGACO
Gateway Operational State	UNLOCKED
Call Agent Status	Normal
High Availability	Synchronizing
Active Board Slot Number	1

Figure 34: Mediant 3000 with TP-8410 Home Page using High Availability Setup



General Information	
IP Address	10.3.3.165
Subnet Mask	255.255.0.0
Default Gateway Address	10.3.0.1
Firmware Version	6.10.013.006
Protocol Type	MEGACO
Gateway Operational State	UNLOCKED
Call Agent Status	Normal
High Availability	Operational
Active Board Slot Number	1

PSTN
○ No Link
● Working Link
○ Protection Link
● Alarm

Refer to the Home Page figure in 'Using the Home Page - Mediant 3000/TP-6310' on page 66 for a full led reference.

The active board is indicated both by “Active Board Slot Number” in the “General Information” pane and by appearing shaded in darker color. The “High Availability” status shows whenever the system is High Availability ready, synchronizing or in case of an error, the error reason.

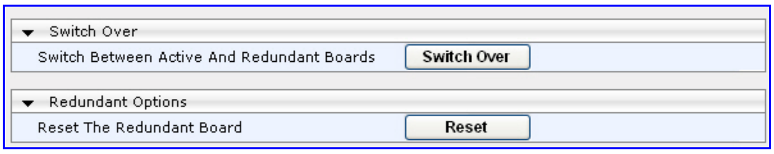
5.7.5.1 Manual Switch Over / Redundant Board Reset

A High Availability system has two additional options:

- Manually switching over between the active and redundant board
- Manually resetting the redundant board

These options are available on the High Availability Maintenance Home Page accessible otherwise by selecting “Switch Over” or “Reset Redundant” via the Device Actions, or, by navigating through Maintenance - High Availability Maintenance. Selecting either option requires an additional confirmation.

Figure 35: Mediant 3000 - High Availability Maintenance


Switch Over
Switch Between Active And Redundant Boards
Switch Over
Redundant Options
Reset The Redundant Board
Reset

Note: Selecting either option will result in no High Availability for a period of time.

5.8 Configuration

5.8.1 System

5.8.1.1 Application Settings

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

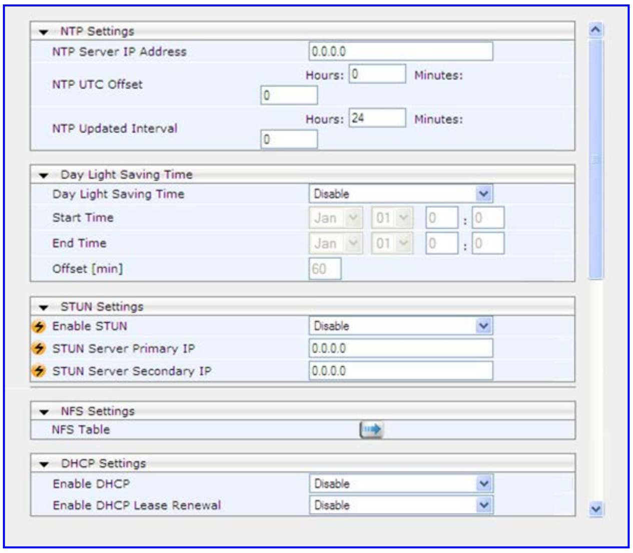
In this option, the following can be configured:

- 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 36: Application Settings



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
Start Time	Jan 01 0 : 0
End Time	Jan 01 0 : 0
Offset [min]	60

STUN Settings

Enable STUN	Disable
STUN Server Primary IP	0.0.0.0
STUN Server Secondary IP	0.0.0.0

NFS Settings

NFS Table

DHCP Settings

Enable DHCP	Disable
Enable DHCP Lease Renewal	Disable

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.

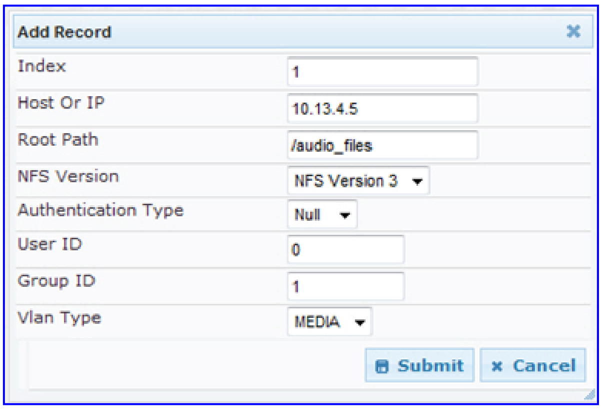
➢ To add remote NFS file systems:

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 37: Add Record Dialog Box - NFS



Add Record

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 145.

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).

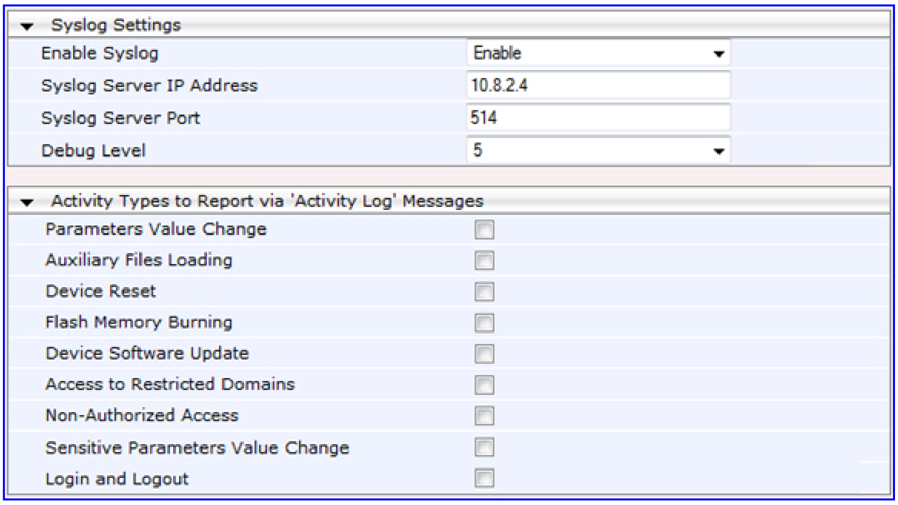
5.8.1.2 Syslog Settings

The procedure below describes how to configure Syslog.

➢ **To configure Syslog:**

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

Figure 38: 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	□
Auxiliary Files Loading	□
Device Reset	□
Flash Memory Burning	□
Device Software Update	□
Access to Restricted Domains	□
Non-Authorized Access	□
Sensitive Parameters Value Change	□
Login and Logout	□

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.

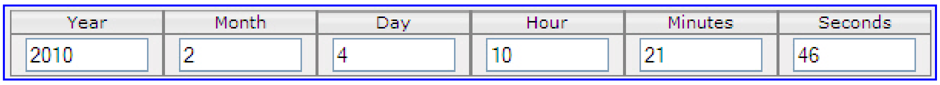
5.8.1.3 Regional Settings

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 39: 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.

5.8.1.4 Certificates

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.

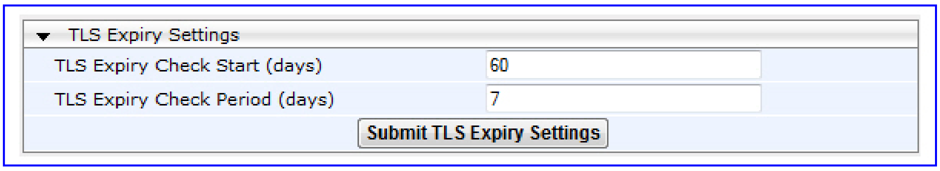
5.8.1.4.1 TLS Server Certificate Expiry Check

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, acCertificateExpiryNotifiaction 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 40: TLS Expiry Settings



▼ TLS Expiry Settings

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

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.

5.8.1.5 Management

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

- Web User Accounts - Refer to 'Web User Accounts' on page 78
- Web Security Settings - Refer to 'Web Security Settings' on page 85
- Telnet/SSH Settings - Refer to 'Telnet/SSH Settings' on page 86
- Web & Telnet Access List - Refer to 'Web & Telnet Access List' on page 86
- RADIUS Settings - Refer to 'RADIUS Settings' on page 87
- SNMP - Refer to 'SNMP' on page 88
  - SNMP Community Settings - Refer to 'SNMP Community Settings' on page 88
  - SNMP Trap Destinations - Refer to 'SNMP Trap Destinations' on page 89
  - SNMP Trusted Managers - Refer to 'SNMP Trusted Managers' on page 89
  - SNMP V3 Users - Refer to 'SNMP V3 Users' on page 90

5.8.1.5.1 Web User Accounts

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.

User Access Level	Numeric Representation*	Privileges
* 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).

5.8.1.5.2 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).

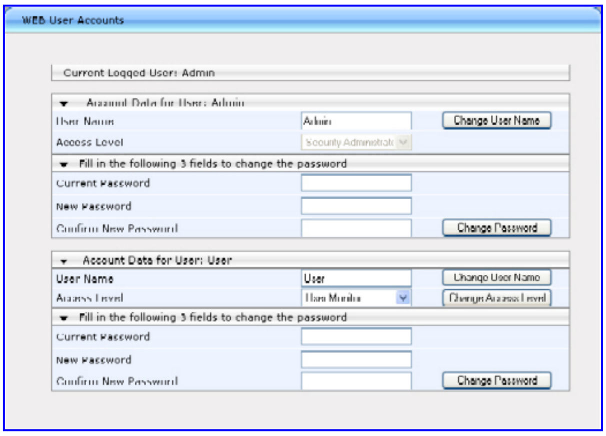
Notes:

- 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 41: Web User Accounts Screen - Security Administrator Level



WEB User Accounts

Current Logged User: Admin

Account Data for User: Admin

User Name: Admin

Access Level: Security Administrator

Fill in the following 3 fields to change the password

Current Password

New Password

Confirm New Password

Account Data for User: User

User Name: User

Access Level: User Monitor

Fill in the following 3 fields to change the password

Current Password

New Password

Confirm New Password

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.

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.

5.8.1.5.3 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.

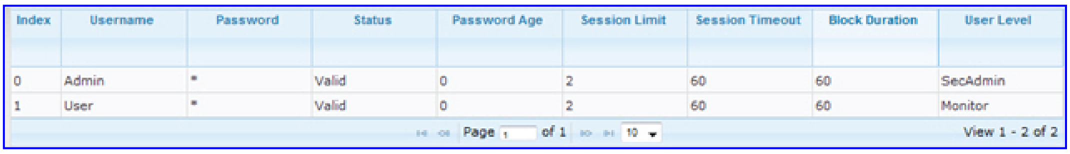
Notes:

- 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 85).
- 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 85). 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 42: Web Users Table Page

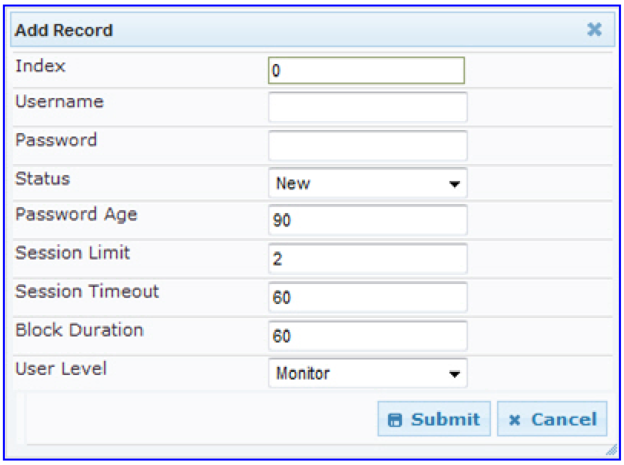


Index	Username	Password	Status	Password Age	Session Limit	Session Timeout	Block Duration	User Level
0	Admin	*	Valid	0	2	60	60	SecAdmin
1	User	*	Valid	0	2	60	60	Monitor

Page 1 of 1 10 View 1 - 2 of 2

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

Figure 43: Web Users Table - Add Record Dialog Box



Add Record

Index	0
Username	
Password	
Status	New
Password Age	90
Session Limit	2
Session Timeout	60
Block Duration	60
User Level	Monitor

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.

Web User Parameters Description

Parameter	Description
Web: Password	Defines the Web user's password. The valid value is a string of 8 to 40 ASCII characters, which must include the following: - 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	Defines the status of the Web user. - 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. 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. 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. **Notes:** - 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	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. The valid value is 0 to 10000, where 0 means that the password is always valid. The default is 90.
Web: Session Limit	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). The valid value is 0 to 5. The default is 2. Note: Up to 5 users can be logged in to the Web interface at any given.

Web User Parameters Description

Parameter	Description
Web: Session Timeout	Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface. 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 85).
Web: Block Duration	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 85). 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 85). Note: The 'Deny Authentication Timer' parameter relates to failed Web logins from specific IP addresses.
Web: User Level	Defines the user's access level. ▪ 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. **Notes:** ▪ 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.

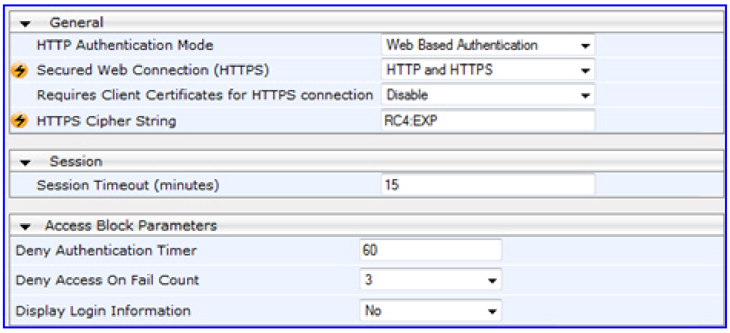
5.8.1.5.4 Web Security Settings

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 submenu** > **WEB Security Settings**).

Figure 44: 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 145.

5.8.1.5.5 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:**

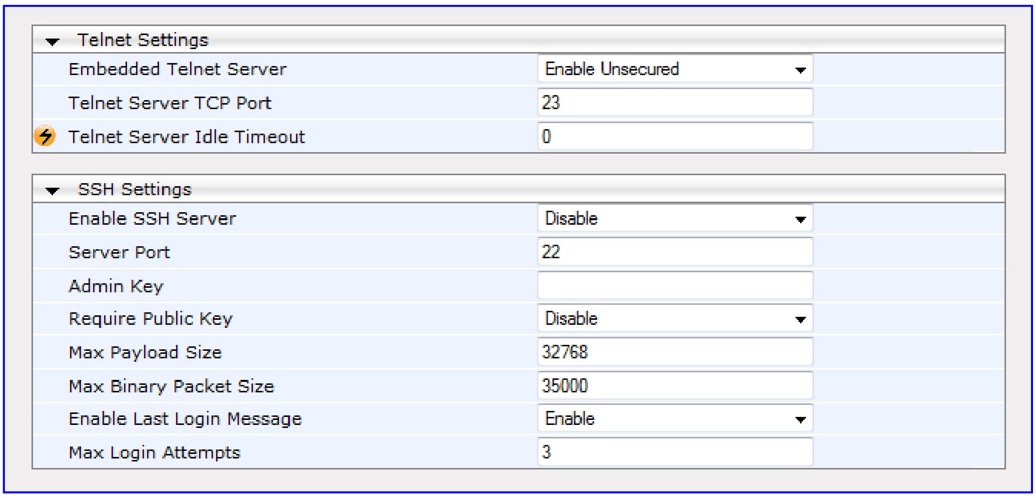
1. Insert the Common Access Card into the card reader.
2. Access the device using the following URL: https://<host name or IP address>; the device prompts for a username and password.
3. Enter the password only. As some browsers require that the username be provided, it’s recommended to enter the username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

5.8.1.5.6 Telnet/SSH Settings

➢ **To enable Telnet:**

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

Figure 45: 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.

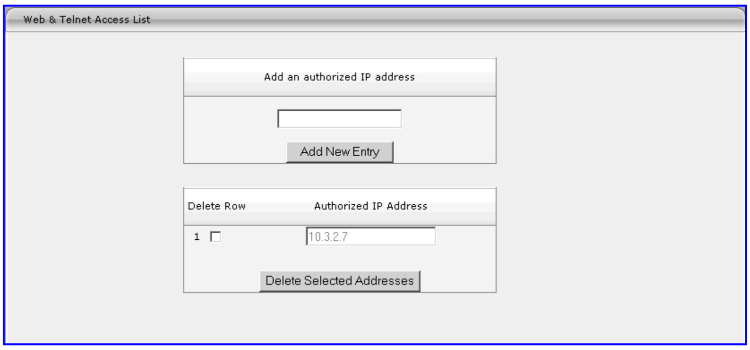
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

5.8.1.5.7 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 46: Web & Telnet Access List



Web & Telnet Access List

Add an authorized IP address

Delete Row	Authorized IP Address
1 ☐	10.3.2.7

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:

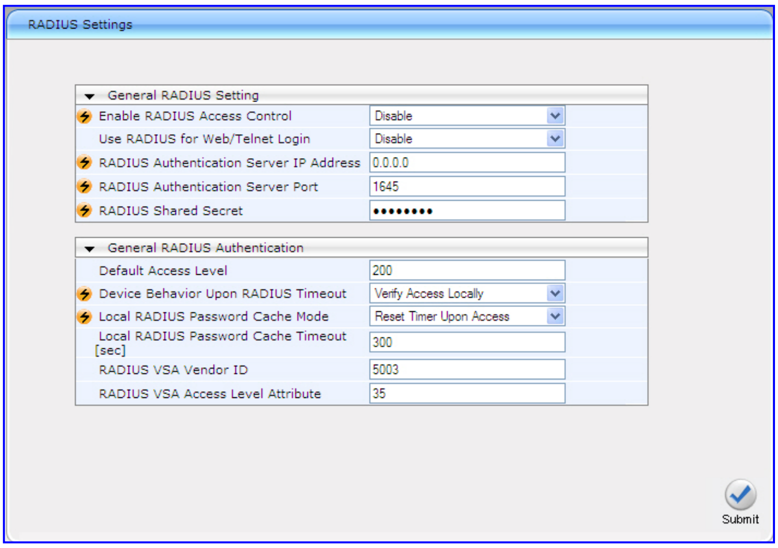
- When all authorized IP addresses are deleted, this security feature becomes disabled (all IP addresses are allowed to connect).
- When adding the first authorized IP address, you should add your own terminal's IP address, in order to be able to connect to the Web interface. If entered incorrectly,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

5.8.1.5.8 RADIUS Settings

- **To configure the RADIUS Settings:**

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

Figure 47: RADIUS Settings



RADIUS Settings

General RADIUS Setting	
⚡ 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	••••••••

General RADIUS Authentication	
Default Access Level	200
⚡ Device Behavior Upon RADIUS Timeout	Verify Access Locally
⚡ Local RADIUS Password Cache Mode	Reset Timer Upon Access
Local RADIUS Password Cache Timeout [sec]	300
RADIUS VSA Vendor ID	5003
RADIUS VSA Access Level Attribute	35

2. To configure this page, refer to the Radius Support 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.

5.8.1.5.9 SNMP

The following describes SNMP settings.

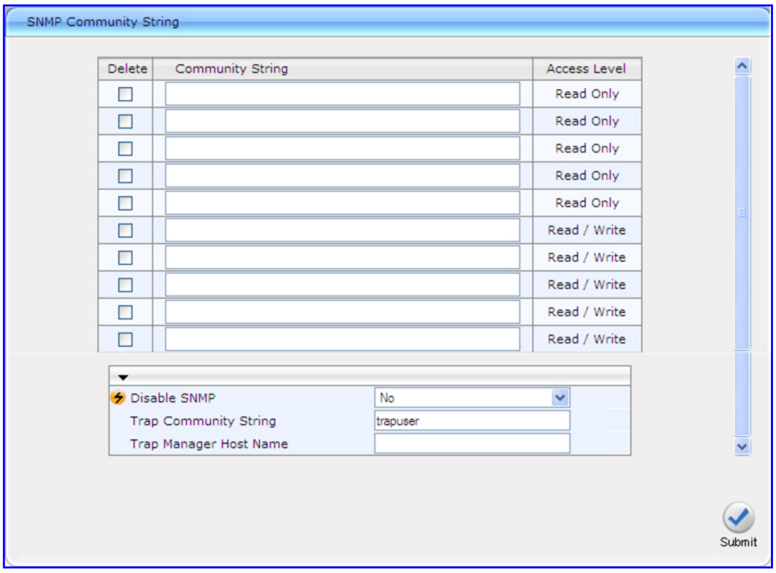
5.8.1.5.9.1 SNMP Community String

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 submenu > SNMP submenu > SNMP Community String).

Figure 48: SNMP Community Settings



SNMP Community String

Delete	Community String	Access Level
□		Read Only
□		Read Only
□		Read Only
□		Read Only
□		Read Only
□		Read / Write
□		Read / Write
□		Read / Write
□		Read / Write
□		Read / Write

Disable SNMP	No
Trap Community String	trapuser
Trap Manager Host Name	

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.

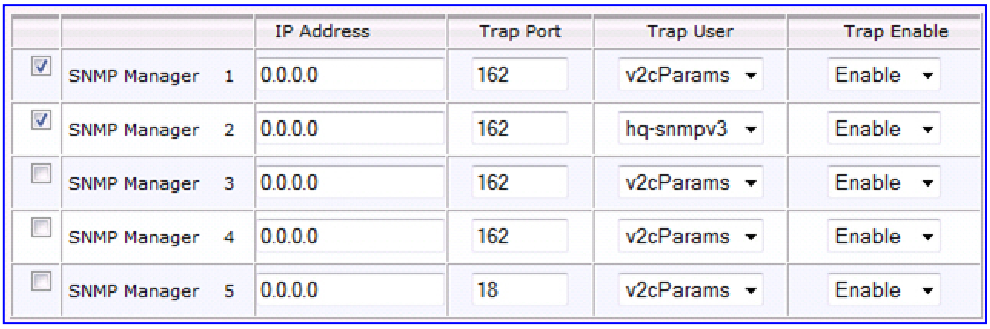
3. To delete a Community String, select the Delete check-box of the Community String to be deleted and then click the **Submit** button, to apply the settings.
4. To configure this page, refer to the SNMP Interface Details sub-section in the Product Reference Manual.
5. After configuring/modifying the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

5.8.1.5.9.2 SNMP Trap Destinations

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

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

Figure 49: SNMP Trap Destinations



		IP Address	Trap Port	Trap User	Trap Enable
☑	SNMP Manager 1	0.0.0.0	162	v2cParams	Enable
☑	SNMP Manager 2	0.0.0.0	162	hq-snmpv3	Enable
□	SNMP Manager 3	0.0.0.0	162	v2cParams	Enable
□	SNMP Manager 4	0.0.0.0	162	v2cParams	Enable
□	SNMP Manager 5	0.0.0.0	18	v2cParams	Enable

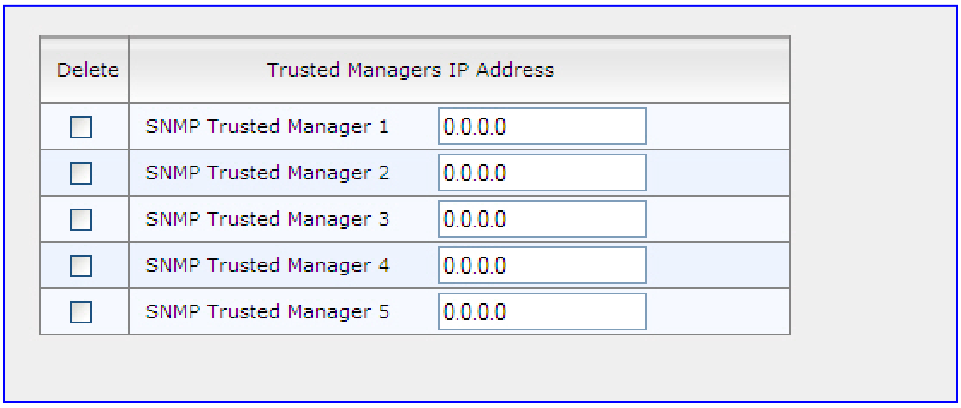
2. To configure this page, refer to the Multiple SNMP Trap Destinations sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

5.8.1.5.9.3 SNMP Trusted Managers

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

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

Figure 50: SNMP Trusted Managers



Delete	Trusted Managers IP Address	
□	SNMP Trusted Manager 1	0.0.0.0
□	SNMP Trusted Manager 2	0.0.0.0
□	SNMP Trusted Manager 3	0.0.0.0
□	SNMP Trusted Manager 4	0.0.0.0
□	SNMP Trusted Manager 5	0.0.0.0

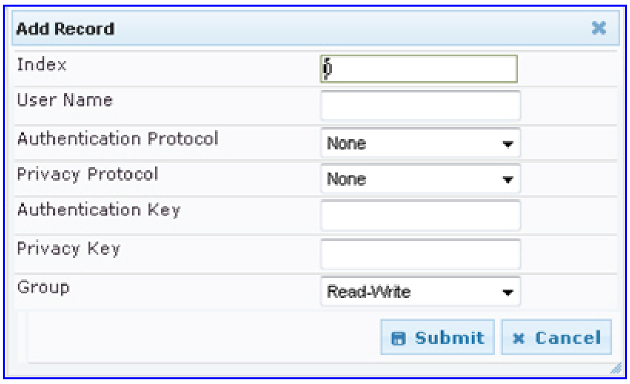
2. To configure this page, refer to the SNMP parameters sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed.

5.8.1.5.9.4 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 51: SNMP V3 Users



Add Record

Index	0
User Name	
Authentication Protocol	None
Privacy Protocol	None
Authentication Key	
Privacy Key	
Group	Read-Write

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.

5.8.2 VoIP

The following describes VoIP settings.

5.8.2.1 Network

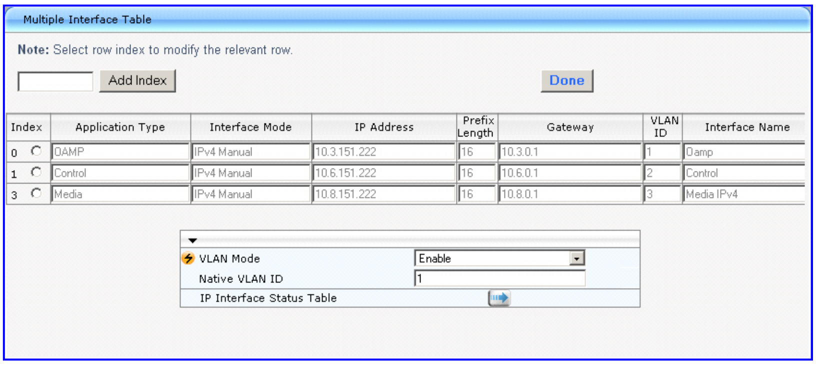
Network - Contains a drop-down list with the following options:

- IP Settings - Refer to "IP Settings" on page 91
- IP Routing Table - Refer to "Routing Table" on page 98
- QoS Settings- Refer to 'QoS Settings' on page 99
- SCTP Settings - Refer to "SCTP Settings" on page 100
- Network Settings - Refer to Network Settings on page 100

5.8.2.1.1 IP Settings

Log on to the Web Interface. From the navigation tree on the left, open the IP Settings page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**). The Multiple Interface Table page is displayed.

Figure 52: Multiple Interface Table - TP-6310



Multiple Interface Table

Note: Select row index to modify the relevant row.

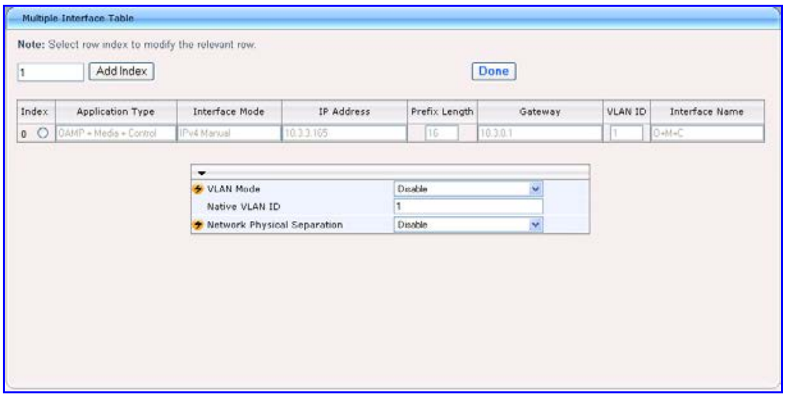
Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	○	OAMP	IPv4 Manual	10.3.151.222	16	10.3.0.1	1	Oamp
1	○	Control	IPv4 Manual	10.6.151.222	16	10.6.0.1	2	Control
3	○	Media	IPv4 Manual	10.8.151.222	16	10.8.0.1	3	Media IPv4

VLAN Mode	Enable
Native VLAN ID	1
IP Interface Status Table	

At this point, you can add rows to the table, edit existing rows and remove rows. In this page you can also change the VLAN Mode value and choose the 'Native' VLAN ID.

For TP-8410, you can select the value for Network Physical Separation.

Figure 53: Multiple Interface Table - TP-8410



Multiple Interface Table

Note: Select row index to modify the relevant row.

1

Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	○	OAMP + Media + Control	IPv4 Manual	10.3.3.105	16	10.3.0.1	1	O+M+C

VLAN Mode	Disable
Native VLAN ID	1
Network Physical Separation	Disable

At this point, you can add rows to the table, edit existing rows and remove rows. In this page you can also change the VLAN Mode value, choose the 'Native' VLAN ID and select the value for Network Physical Separation.

> **Note:** For Mediant 3000 HA, the default IP Settings page is the Multiple Interface Table. If the system was loaded without an Interface Table configuration in the ini file, the following message is displayed.
>
> "For the system to operate in High Availability mode, ensure that at least one IP address has been defined."

➢ **To configure the IP Settings:**

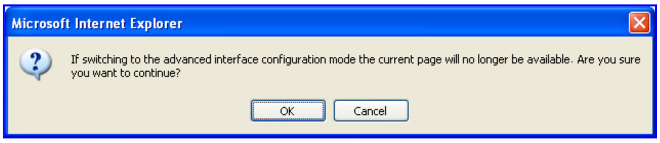
1. Open the IP Settings page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).
2. Follow the guidelines in the Product Reference Manual when configuring/modifying the IP Settings, in the IP Settings page.
3. After configuring/modifying the parameter fields, click **DONE**. This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

5.8.2.1.1.1 Multiple Interface Table

➢ **To configure the Multiple Interface Table:**

1. Click on the Multiple Interface Table link in the IP Settings page above; the following message appears:

Figure 54: Multiple Interface Table Message

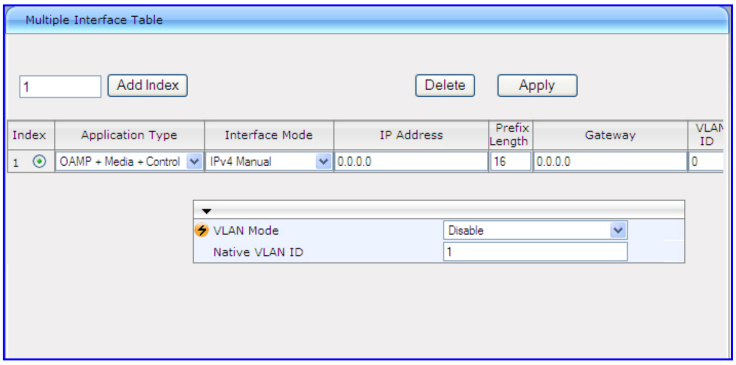


Microsoft Internet Explorer

If switching to the advanced interface configuration mode the current page will no longer be available. Are you sure you want to continue?

2. Confirm moving the configuration to the Multiple Interface Table, when clicking OK. The following table appears:

Figure 55: Multiple Interface Table



Multiple Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID
1 ●	OAMP + Media + Control	IPv4 Manual	0.0.0.0	16	0.0.0.0	0

VLAN Mode	Disable
Native VLAN ID	1

You may now add, edit or delete an existing row using the Interface Table.

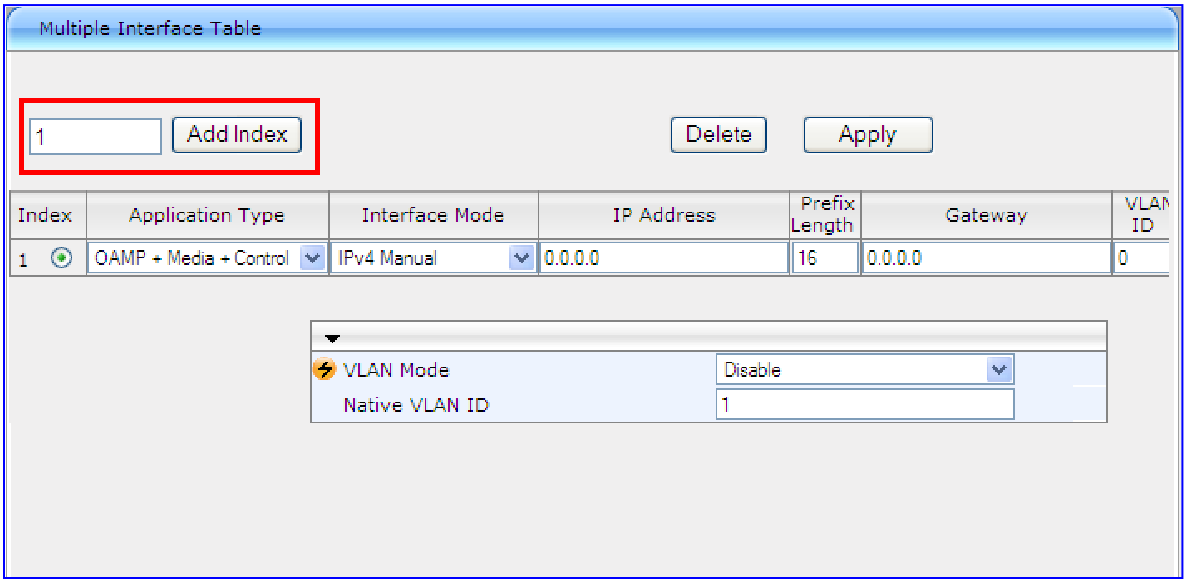
Note: It is highly recommended to click on Done after changing the Networking configuration. This will trigger a validation process which ensures the configuration is complete and valid.

5.8.2.1.1.2 Adding a New Interface Table Row

➢ **To add a new Interface Table row:**

1. To add a new Interface Table row, enter a row number in the field shown below and click the **Add Index** button.

Figure 56: Interface Table - Add Row



Multiple Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID
1 ●	OAMP + Media + Control	IPv4 Manual	0.0.0.0	16	0.0.0.0	0

VLAN Mode	Disable
Native VLAN ID	1

2. Enter the appropriate values in the available fields and click **Apply**.
3. Click **Done** for validation.

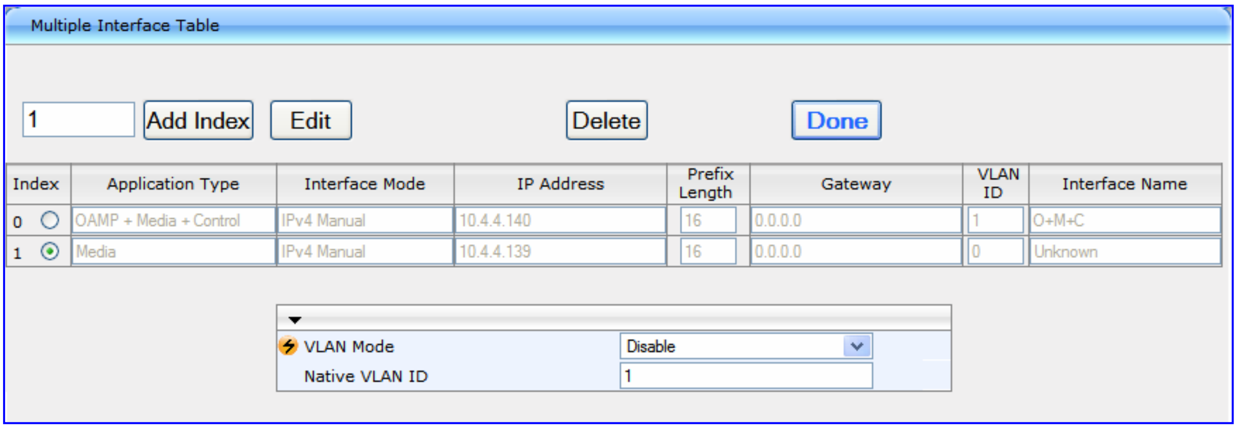
Note: When adding more than one network interface, VLANS must be enabled. Please refer to the Product Reference Manual for more information and guidelines.

5.8.2.1.1.3 Editing an Interface Table Row

- **To edit an existing Interface Table row:**

1. Select the line to be edited by clicking the radio button on the appropriate row.

Figure 57: Interface Table - Edit Row



Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	○	OAMP + Media + Control	IPv4 Manual	10.4.4.140	16	0.0.0.0	1	O+M+C
1	●	Media	IPv4 Manual	10.4.4.139	16	0.0.0.0	0	Unknown

VLAN Mode	Disable
Native VLAN ID	1

2. Click on the **Edit** button and make the necessary changes; click **Apply**.
3. Click **Done** for validation.

5.8.2.1.1.4 Deleting an Interface Table Row

- **To delete an existing Interface Table row:**

1. Open the IP Settings page (**Configuration** tab > VoIP menu > Network submenu > IP Settings).
2. Click on the radio button next to the row you wish to remove, and then click on the **Delete** button. The table row is removed.
3. Click **Done**. The new configuration will be available after saving the configuration and restarting the module.
4. Refer to the Interface Table Configuration Guidelines sub-section in the Product Reference Manual to ensure a successful Interface Table configuration.

5.8.2.1.1.5 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.

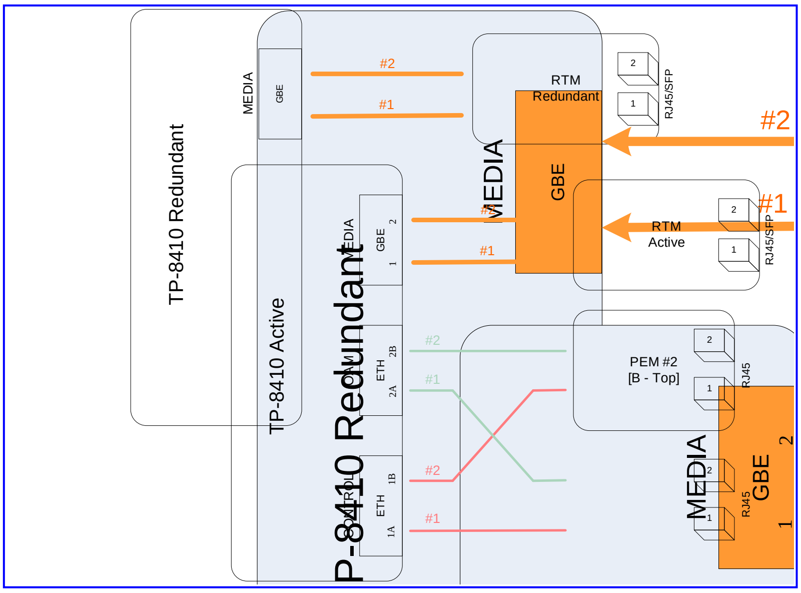
Note that any change of these parameter values will only be applied after burning the configuration and booting from Flash (not using a BOOTP/DHCP server).

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

5.8.2.1.1.6 Using Network Physical Separation - TP-8410 Only

A Mediant 3000 with TP-8410 blades allows the user to have different physical port for each network type (Media, OAMP and Control). This feature eliminates the need for a VLAN aware switch in order to separate the different traffic of each network. The Mediant 3000 is basically implementing VLANs architecture inside the system. This also means that user VLANs are not supported with this feature. This section provides information on how to enable or disable this mode of operation.

Figure 58: Network Physical Separation in Mediant 3000 + TP-8410 Block Diagram



Each TP-8410 (Active and Redundant) blade has its own dedicated and redundant GbE (Gigabit Ethernet) port for Media traffic. This interface is directly available via the RTM module. The four Ethernet ports are available via the PEM, but they are shared by the two blades. The active blade is connected to these ports.

Changing the mode of operation, with network physical separation or without, is done by setting the following parameter:

```
EnableNetworkPhysicalSeparation = 1
```

Note: Physical Network Separation is currently supported only for three interface configurations. Users must configure an interface for each traffic type (i.e., OAMP, Control and Media).

5.8.2.1.1.7 Switching into/out of Multiple IP's and Network Physical Separation configuration.

When the Mediant 3000 operates with multiple IP's, it uses a single physical Ethernet port, located on its RTM, to connect to the networks. By using VLANs and an external VLAN aware switch, the user can separate the different traffic types and connect each of them to their dedicated network. Moving into a Network Physical Separation mode means you have a dedicated Ethernet port for each traffic type (Media, Control & OAMP). This also means that after the blade is set to work in this mode, its OAMP traffic (which includes BootP/TFTP traffic) will be sent/received to/from the dedicated port (on the PEM). This is not the port used in multiple IP's & VLANs without network physical separation.

5.8.2.1.1.8 Configuring System to Separate Physical Interfaces Scheme using *.ini file

➢ **To prepare the Mediant 3000 to work with Multiple Interfaces and network physical interfaces separation:**

1. Prepare an ini file with your parameters and make sure that the EnableNetworkPhysicalSeparation ini file parameter has been added and is set to "1".
2. Insert a single blade into the system. Each blade should be configured separately. There is no importance to the order.
3. Make sure that your Ethernet cable is connected to the RTM of the inserted blade.
4. Use BootP/TFTP to load the ini file you prepared in the first step to the blade (Multiple Interfaces and physical interfaces separation are available when booting from flash), or use the Web interface to set the configuration.
5. Verify that the following message is sent to the Syslog: "Updating Flash to work in Network Separation Mode in the next Boot".
6. Repeat steps 3 to 5 for the second blade.
7. Insert both blades into the system and connect a separate Ethernet cables for each network. Remember that your OAMP applications are now available at the PEM module. Power up the system.
8. Verify that the following message is sent to the Syslog from each blade: "Board Is Working in Network Separation Mode".

➢ **To prepare the Mediant 3000 to work with Multiple Interfaces and without Network Physical Interfaces Separation:**

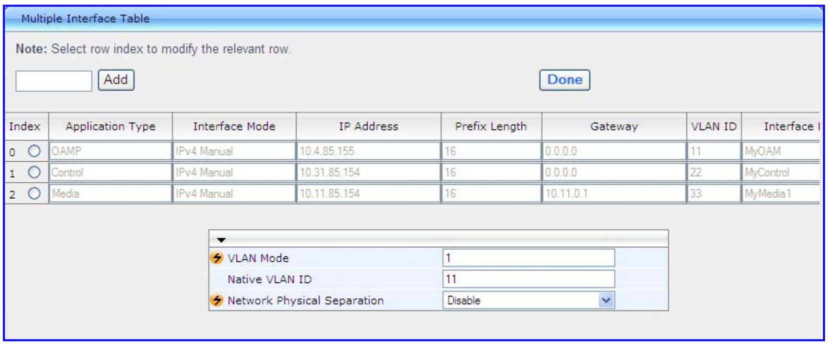
1. Prepare an ini file with your parameters and make sure that the ini file parameter “EnableNetworkPhysicalSeparation” is added and set to 0.
2. Insert a single blade into the system. Each blade should be configured separately, while the other blade is not inserted into the M3K. There is no importance to the order.
3. Make sure your Ethernet cable is connected to the PEM.
4. Use BootP/TFTP to load the INI file you prepared in the first step to the blade (Multiple Interfaces and VLANs are available when booting from flash), or use the Web interface to set the configuration.
5. Verify that the following message is sent to the Syslog: "Updating Flash to work in Non Network Separation Mode in the next Boot".
6. Repeat steps 4 to 5 with the second blade.
7. Insert both blades into the system and connect two separate Ethernet cables, one for each RTM. Remember that your OAMP applications are now available at the RTM module, as well as your Media and Call Control applications. Power up the system.

5.8.2.1.1.9 How to Switch to Multiple IP’s with Network Physical Separation

➢ **To prepare the Mediant 3000 to work in Multiple IP’s Network with network physical separation:**

1. Log on to the Web Interface. From the navigation tree on the left, click on the Network Settings - IP Settings link. The IP Settings page is displayed.
2. Configure exactly three interfaces, one for each traffic type, using the Multiple Interface table. (Refer to 'IP Settings' on page 91 for more information.)

Figure 59: Configuring Three Interfaces



Multiple Interface Table

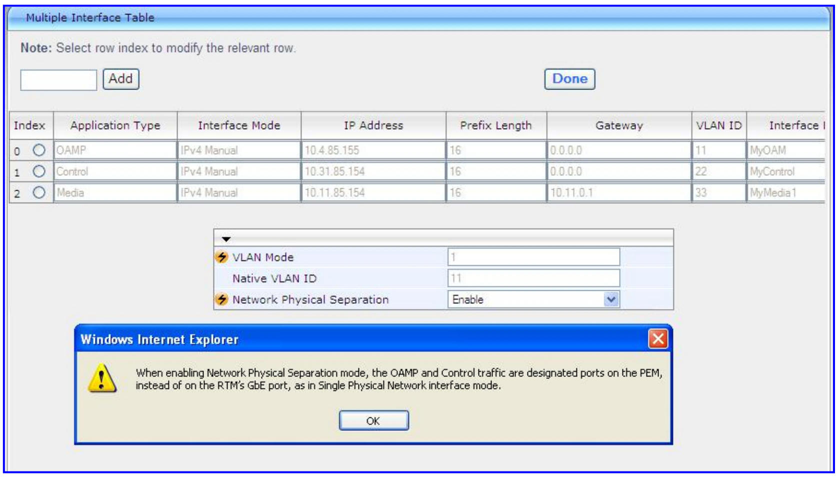
Note: Select row index to modify the relevant row.

Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface I
0	○	OAMP	IPv4 Manual	10.4.85.155	16	0.0.0.0	11	MyOAM
1	○	Control	IPv4 Manual	10.31.85.154	16	0.0.0.0	22	MyControl
2	○	Media	IPv4 Manual	10.11.85.154	16	10.11.0.1	33	MyMedia1

VLAN Mode	1
Native VLAN ID	11
Network Physical Separation	Disable

3. Set the Network Physical Separation field to Enable. You will be prompted to change the OAMP Ethernet cable to the PEM module.

Figure 60: Enable Network Physical Separation



Multiple Interface Table

Note: Select row index to modify the relevant row.

Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface I
0	○	OAMP	IPv4 Manual	10.4.85.155	16	0.0.0.0	11	MyOAM
1	○	Control	IPv4 Manual	10.31.85.154	16	0.0.0.0	22	MyControl
2	○	Media	IPv4 Manual	10.11.85.154	16	10.11.0.1	33	MyMedia1

VLAN Mode	1
Native VLAN ID	11
Network Physical Separation	Enable

Windows Internet Explorer

When enabling Network Physical Separation mode, the OAMP and Control traffic are designated ports on the PEM, instead of on the RTM's GbE port, as in Single Physical Network interface mode.

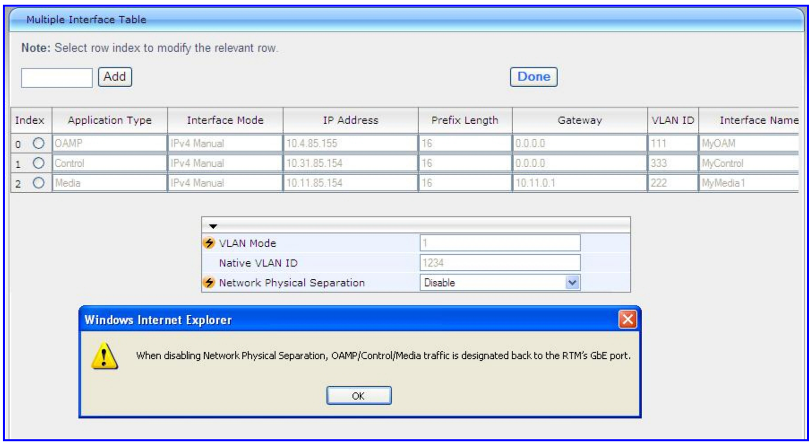
4. Click on OK and then on the Done button to set the new configuration. A new prompt will ask you to restart the system in order for the new configurations to take place.
5. Reset the blade using the Reset function on the Maintenance web page.
6. Change the OAMP Ethernet cable to the PEM's relevant OAMP ports. Connect the other Ethernet network ports to the system.

5.8.2.1.1.10 How to Switch out of Multiple IP's with Network Physical Separation

➢ **To prepare the Mediant 3000 to work in Multiple IP's Network without network physical separation:**

1. Log on to the Web Interface. From the navigation tree on the left, click on the Network Settings - IP Settings link. The IP Settings page is displayed.
2. Set the Network Physical Separation field to Disable.
3. Configure your new multiple interfaces using the Multiple Interface Table. (Refer to 'IP Settings' on page 91 for more information.)
4. Click on **OK** and then on the Done button to set the new configuration. A new prompt will ask you to restart the system in order for the new configurations to take place.

Figure 61: Network Physical Separation Disabled



Multiple Interface Table

Note: Select row index to modify the relevant row.

Index		Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	○	OAMP	IPv4 Manual	10.4.85.155	16	0.0.0.0	111	MyOAM
1	○	Control	IPv4 Manual	10.31.85.154	16	0.0.0.0	333	MyControl
2	○	Media	IPv4 Manual	10.11.85.154	16	10.11.0.1	222	MyMedia1

VLAN Mode	1
Native VLAN ID	1234
Network Physical Separation	Disable

Windows Internet Explorer

When disabling Network Physical Separation, OAMP/Control/Media traffic is designated back to the RTM's GbE port.

5. Reset the blade using the Reset function on the Maintenance web page.
6. Change the OAMP Ethernet cable to the RTM's relevant OAMP ports. Disconnect the other Ethernet network ports from the system.

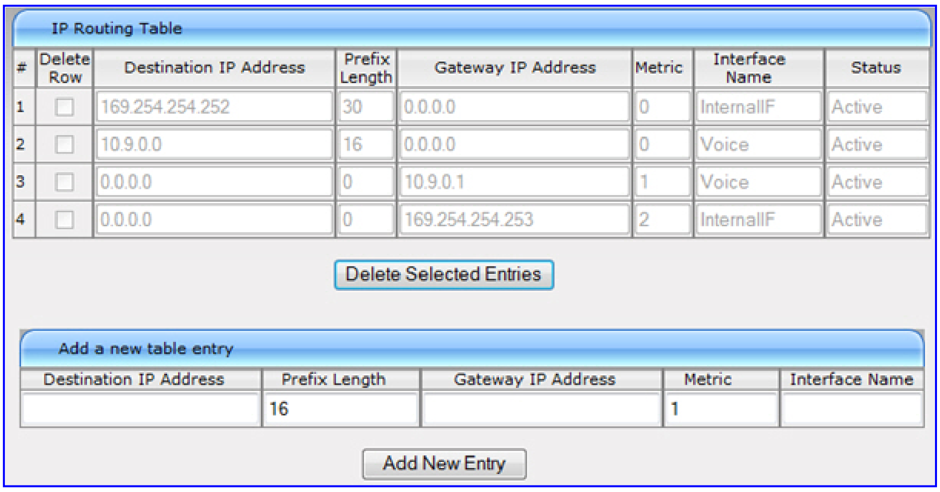
5.8.2.1.2 IP Routing Table

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 IP routing:**

1. Open the IP Routing Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Routing Table**).

Figure 62: IP Routing Table Page



IP Routing Table

#	Delete Row	Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface Name	Status
1	□	169.254.254.252	30	0.0.0.0	0	InternalIF	Active
2	□	10.9.0.0	16	0.0.0.0	0	Voice	Active
3	□	0.0.0.0	0	10.9.0.1	1	Voice	Active
4	□	0.0.0.0	0	169.254.254.253	2	InternalIF	Active

Add a new table entry

Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface Name
	16		1	

2. In the Add a new table entry table, add a new static routing rule according to the parameters described in the table below.
3. Click **Add New Entry**; the new routing rule is added to the IP routing table.

4. To delete a routing rule from the table, select the 'Delete Row' check box corresponding to the required routing rule, and then click Delete Selected Entries.

Notes:

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

5.8.2.1.3 QoS Settings

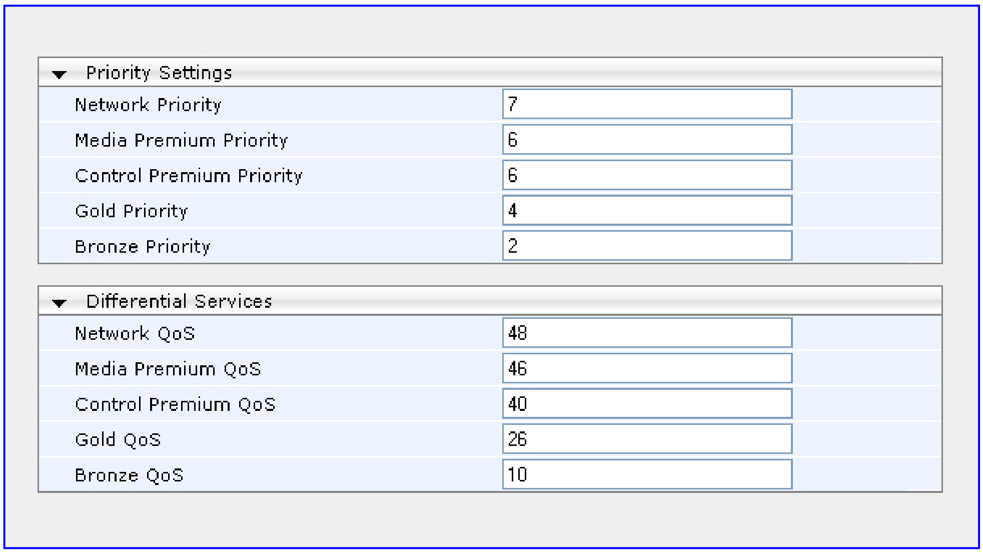
This page allows the user to configure values for the priority field of the VLAN tag, and the DiffServ field of the IP Header. Refer to QoS Parameters in the Product Reference Manual, for more information.

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 63: QoS Settings



▼ 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

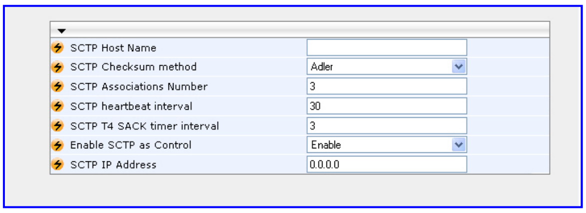
2. To configure this page, refer to the Infrastructure ini File Parameters sub-section in the Product Reference Manual.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into the system and the page is refreshed. Changes made to Class of Service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

5.8.2.1.4 SCTP Settings

➢ **To configure the SCTP Settings:**

1. Open the SCTP Settings page (Configuration tab > VoIP menu > Network submenu > SCTP Settings.

Figure 64: SCTP Settings



SCTP Host Name	
SCTP Checksum method	Adler
SCTP Associations Number	3
SCTP heartbeat interval	30
SCTP T4 SACK timer interval	3
Enable SCTP as Control	Enable
SCTP IP Address	0.0.0.0

2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the SCTP Settings, in the SCTP 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.

5.8.2.1.5 Network Settings

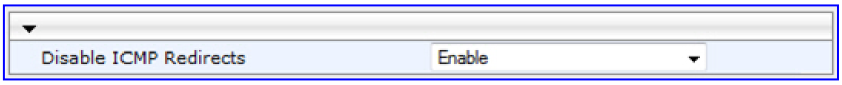
You can configure the device's handling of ICMP Redirect messages. These messages can either be rejected (ignored) or permitted.

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 submenu > Network Settings).

Figure 65: Disabling ICMP Redirect in Network Settings Page



Disable ICMP Redirects	Enable

2. From the 'Disable ICMP Redirects' drop-down list, select the required option.
3. Click **Submit** to apply your changes.

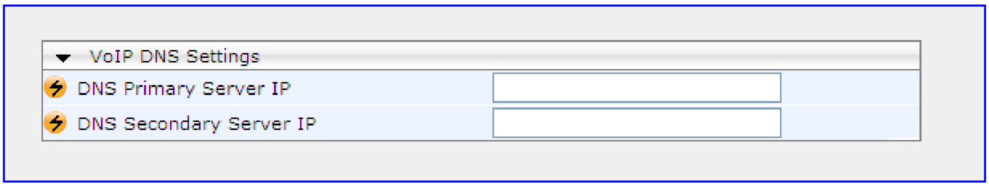
5.8.2.1.6 DNS Settings

The following describes DNS settings.

➢ **To configure the DNS Settings:**

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

Figure 66: VoIP DNS Settings



▾ VoIP DNS Settings

DNS Primary Server IP	
DNS Secondary Server IP	

2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the DNS 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.

5.8.2.2 TDM & Timing

TDM & Timing allows configuration of all TDM and Clock Timing related issues, from the Navigation Pane, on the left side of the page:

- **TDM** – TDM Refer to 'TDM' on page 102.
- **Digital PCM Settings** – PCM Law and Pattern configurations. Refer to 'Digital PCM Settings' on page 103.
- **System Timing** – System Clock and Timing configurations. Refer to 'System Timing Settings' on page 103.

Notes:

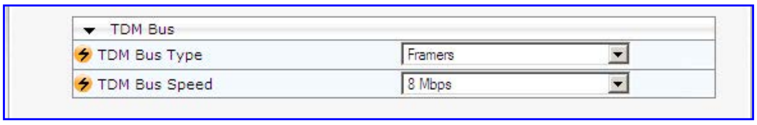
- A device reset may be needed in certain circumstances for the setup to be activated. Reset can be scheduled for a later time period when call traffic is at a minimum. If you choose to schedule the Reset for a later time, be sure to use the 'Save Configuration screen' to retain the changes to the device's non-volatile memory.
- 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.

5.8.2.2.1 TDM

➢ **To configure the TDM Bus settings:**

1. Open the TDM page (**Configuration** tab > VoIP menu > TDM & Timing submenu > TDM).

Figure 67: TDM Screen



TDM Bus

TDM Bus Type: Framers

TDM Bus Speed: 8 Mbps

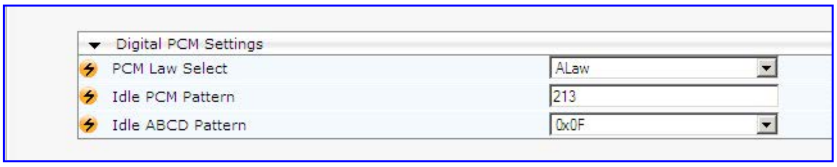
2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the parameter fields in the TDM Bus settings screen.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the screen is refreshed.
4. To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

5.8.2.2.2 Digital PCM Settings

➢ **To configure the Digital PCM settings:**

1. Open the Digital PCM Settings page (**Configuration** tab > **VoIP** menu > **TDM & Timing** > **Digital PCM Settings**).

Figure 68: Digital PCM Settings



Digital PCM Settings

⚡ PCM Law Select	ALaw
⚡ Idle PCM Pattern	213
⚡ Idle ABCD Pattern	0x0F

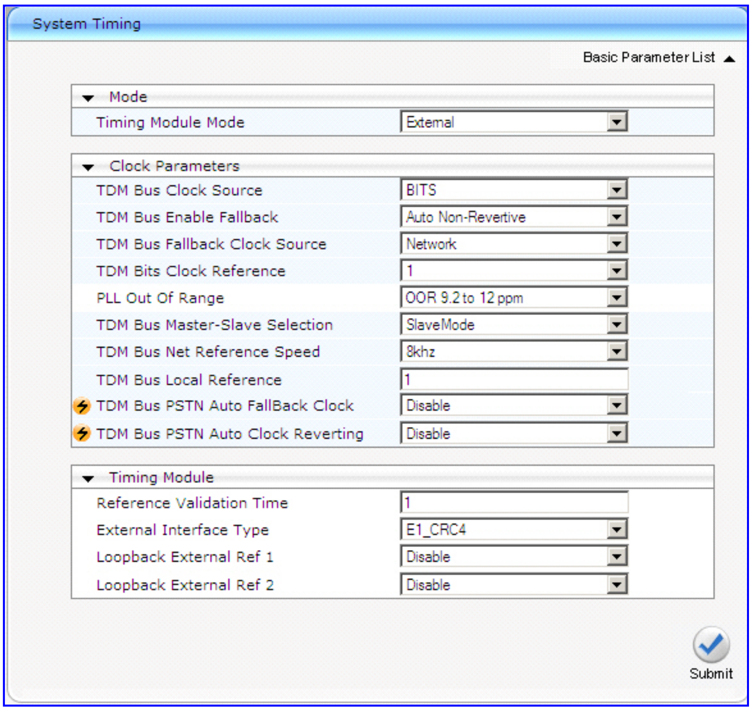
2. Use the appropriate tables in the Product Reference Manual as a reference when configuring/modifying the parameter fields in the Digital PCM Settings page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.
4. To 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.
5. Select the Burn option and click **Reset**.

5.8.2.2.3 System Timing

➢ **To configure the System Timing settings:**

1. Open the System Timing page (**Configuration** tab > **VoIP** menu > **TDM & Timing** > **System Timing**).

Figure 69: System Timing Page



System Timing

Mode

Timing Module Mode	External

Clock Parameters

TDM Bus Clock Source	BITS
TDM Bus Enable Fallback	Auto Non-Revertive
TDM Bus Fallback Clock Source	Network
TDM Bits Clock Reference	1
PLL Out Of Range	OOR 9.2 to 12 ppm
TDM Bus Master-Slave Selection	SlaveMode
TDM Bus Net Reference Speed	8khz
TDM Bus Local Reference	1
⚡ TDM Bus PSTN Auto FallBack Clock	Disable
⚡ TDM Bus PSTN Auto Clock Reverting	Disable

Timing Module

Reference Validation Time	1
External Interface Type	E1_CRC4
Loopback External Ref 1	Disable
Loopback External Ref 2	Disable

2. Use the appropriate tables in the Product Reference Manual) and refer to 'Clock Settings' on page 104 as a reference when configuring/modifying the parameter fields in the System Timing Settings page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.
4. 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.
5. Select the Burn option and click **Reset**.

5.8.2.2.4 Clock Settings

In a traditional TDM service network such as PSTN, both ends of the TDM connection must be synchronized. If synchronization is not achieved, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases, connection quality and reliability is affected.

The following section describes how to configure the Mediant 3000 clock-related parameters in order to achieve a synchronized system.

Notes:

- To configure the Clock parameters using the Web interface, refer to 'System Timing' on page 103. For SNMP, refer to the SNMP section in the Product Reference Manual.
- When the device is used in a 'non-span' configuration, the internal device clock must be used (as explained below).

5.8.2.2.5 Recovering the Clock from the Line interface (PSTN)

This sub-section describes the configuration parameters relevant to recovering the clock from the Line (Trunk/STM-1/OC-3/T3) interface.

Note: There are other interface-specific parameters which are relevant. Refer to the PSTN Physical Interface section of the Product Reference Manual.

- TDMBusClockSource = 4 (4 indicates ‘Network’ – i.e. recover clock from line interface)
- ClockMaster parameter is used to configure the PSTN trunk to recover/derive the clock into the Mediant 3000, or, transmit the clock to the remote side of the PSTN trunk. (i.e. clock slave or clock master)
- ClockMaster_x = 0/1 (where ‘x’ is the number of the trunk – ‘0’ means to recover/derive clock i.e., slave – ‘1’ means to transmit/drive clock i.e. master)
- To select from which trunk the clock of the Mediant 3000 system should be taken, use TDMBusLocalReference to select the specific trunk.
- TDMBusLocalReference = x (‘x’- trunk number, where 0 is the first trunk - default)
- The Mediant 3000 has an automatic mechanism to detect when a "local-reference" trunk (set by TDMBusLocalReference) is no longer capable of supplying the clock to the system, and can automatically switch to the next available trunk (according to the priority set by the AutoClockTrunkPriority parameter and TDMBusPSTNAutoClockRevertingEnable value).

- TDMBusPSTNAutoClockEnable = 1 (the device automatically selects one of the connected 'slave' trunks).

Notes:

- When working with the SDH/OC-3 PSTN interface the TDMBusLocalReference, TDMBusPSTNAutoClockEnable, AutoClockTrunkPriority and TDMBusPSTNAutoClockRevertingEnable parameters are not applicable.
- For more information on PSTN clock parameters refer to the PSTN Physical Interface section in the Product Reference Manual.

- When working with a Mediant 3000 system that has BITS capability, configure the following parameter in addition to the above parameters:
  - TMMode =2 (Defines the BITS mode. Set this to "2" for the line interface clock).

Notes:

- When working in line recover mode with a Mediant 3000 system that has the BITS timing HW installed, if the source link/trunk clock reference fails, both Active and Redundant blades change into "hold-over" mode.
- In a Mediant 3000 system that does not have the BITS timing HW installed, set TMMode to 0 (default).

5.8.2.2.6 Configuring BITS Synchronization Mode

Note: This sub-section is relevant only to Mediant 3000 systems that are Building Integrated Timing Source (BITS) capable.

This sub-section describes how to configure the Mediant 3000 to use BITS-clock-inputs to synchronize the system to an external BITS source. In this mode, the clock flows from the BITS to the line interfaces.

In BITS Synchronization mode, both Active and Redundant blades are synchronized by two BITS input trunks. The BITS trunks flow through two SAT blades (housed in the Mediant 3000 chassis), each with a designated timing module. Two SAT blades are required to ensure seamless clock operation in case of failure of one of the SATs timing-modules (i.e., clock redundancy).

- First define the external BITS reference transmission type for both primary and secondary interfaces connected to the Mediant 3000 -
  - TMExternalIFType = y (where y is one of the following) -
    - [0] E1 CRC4 (default)
    - [1] E1 CAS
    - [2] E1 FAS
    - [3] T1 D4
    - [4] T1 ESF
    - [5] T12

- Other physical characteristics of the BITS interface can be set with the following parameters:
  - TMT1LineBuildOut : To define the transmission power between the timing module on the SAT blade and the T1 external reference clock (External Reference Transmit Line Build Out).
  - TMT1LineBuildOut = y (where y is one of the following)
    - [0] = DSX 1.0 to 133 feet 0 dB CSU
    - [1] = DSX 1.133 to 266 feet (default)
    - [2] = DSX 1.266 to 399_feet
    - [3] = DSX 1.399 to 533 feet
    - [4] = DSX 1.533 to 655 feet
    - [7] = DSX 1.0 to 133 feet 0 dB CSU pulse enable transmit and receive gapped clock

    TME1LineBuildOut: Defines the transmission power (in ohm) between the timing module on the SAT blade and the E1 external reference clock.

  - TME1LineBuildOut = y (where y is one of the following):
    - [0] E 75 ohms normal
    - [1] E 120 ohms normal (default)
    - [4] E 75 ohms with high return loss
    - [5] E 120 ohms with high return loss
    - [6] E 75 ohms normal plus enable transmit and receive gapped clock
    - [7] E 120 ohms normal plus enable transmit and receive gapped clock
- In order for a BITS reference to be returned into service, the Mediant 3000 must validate the clock. Set the validation time with the following parameter:
  - TMReferenceValidationTime = [1 - 15] min (default 1 min) The duration in which a reference BITS input has its alarm cleared before it is declared as a valid reference.
- Select the mode of operation with BITS – set to 1 for using BITS inputs.
  - TMMode = 1 (set BITS mode)
- When one of the BITS reference clock sources fails, the Mediant 3000 automatically switches to the secondary BITS reference source for the entire Mediant 3000 system. When a BITS reference clock source with a higher priority returns to service after failure, the device may either revert to the higher-priority clock source or continue using the lower-priority clock source. This behavior is controlled using the TDMBusEnableFallback parameter. When both BITS reference clock sources fail, the device enters into clock holdover.
  - TDMBusEnableFallback =1 (Enable non-revertive clock fallback between BITS interfaces)

  or

  - TDMBusEnableFallback =2 (Enable auto-revertive clock fallback between BITS interfaces)

Note: For more information on PSTN clock parameters refer to the PSTN Physical Interface section in the Product Reference Manual.

5.8.2.2.7 Using the Internal Clock as the Clock Source

This sub-section describes how to configure the Mediant 3000 system to use its internal Stratum 4E compliant clock source.

When the system has no line interfaces, the system should be configured in the following mode:

1. Set the clock-source to be from internal oscillator device.
   - TDMBusClockSource = 1 (internal)
2. Set line to drive clock on all trunks.
   - ClockMaster = 1 (for all trunks)

When working with a Mediant 3000 system that has BITS capability, configure the following parameter in addition to the above parameters:

- TMMode = 0 (default value)

Note: For more information on PSTN clock parameters refer to the PSTN Physical Interface section in the Product Reference Manual.

5.8.2.3 Security Settings

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

- Firewall Settings - Refer to 'Firewall Settings' on page 108
- General Security Settings - Refer to 'General Security Settings' on page 110
- IPSec Proposal Table - Refer to 'IP Security Proposal Table' on page 111
- IPSec Association Table - Refer to 'IP Security Associations Table' on page 112

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

5.8.2.3.1 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.

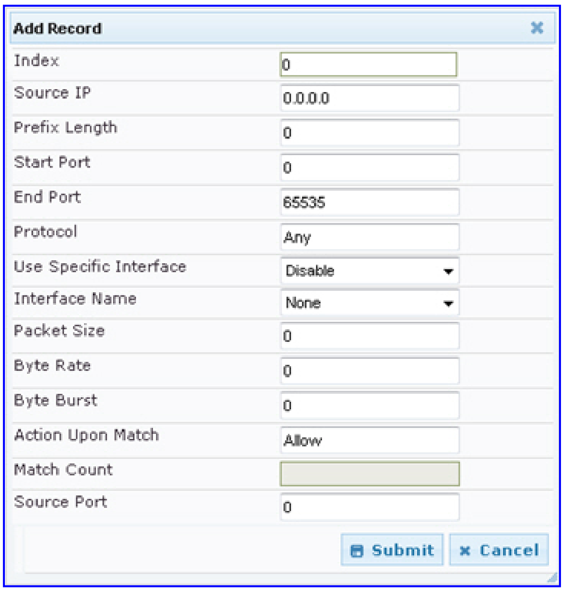
Notes:

- This firewall applies to a very low-level network layer and overrides all your 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 86), 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 70: Firewall Settings



Add Record

Index	0
Source IP	0.0.0.0
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	
Source Port	0

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:

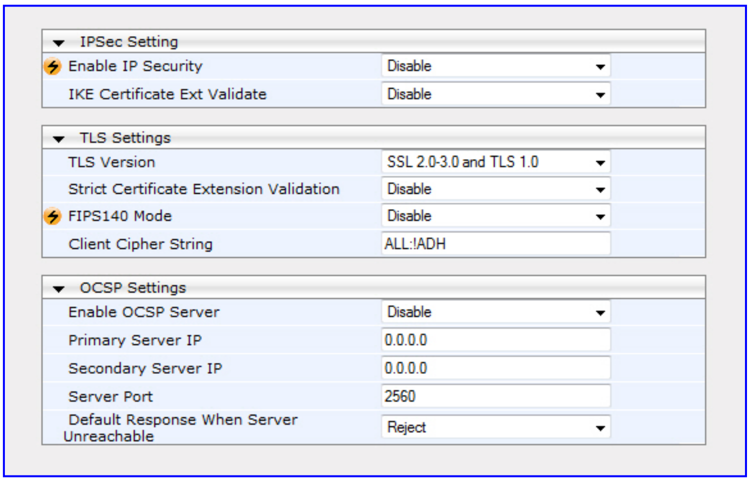
- Rules 1 and 2: Typical firewall rules that allow packets ONLY from specified IP addresses (e.g., proxy servers). Note that the prefix length is configured.
- Rule 3: A more "advanced" firewall rule - bandwidth rule for ICMP, which allows a maximum bandwidth of 40,000 bytes/sec with an additional allowance 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.

5.8.2.3.2 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 71: 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.

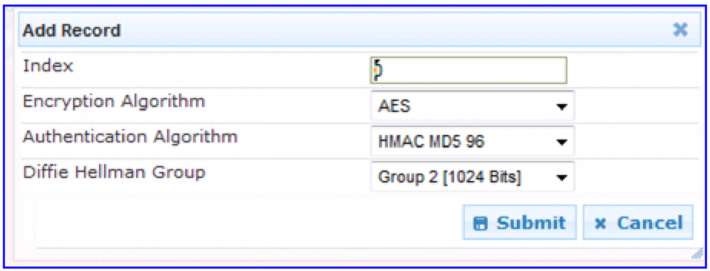
5.8.2.3.3 IP Sec Proposal Table

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 submenu > IPSec Proposal Table).
2. Click the **Add** button; the following dialog box appears:

Figure 72: IP Security Proposals Table - Add Record Dialog Box



Add Record

Index	5
Encryption Algorithm	AES
Authentication Algorithm	HMAC MD5 96
Diffie Hellman Group	Group 2 [1024 Bits]

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**.

5.8.2.3.4 IP Sec Associations Table

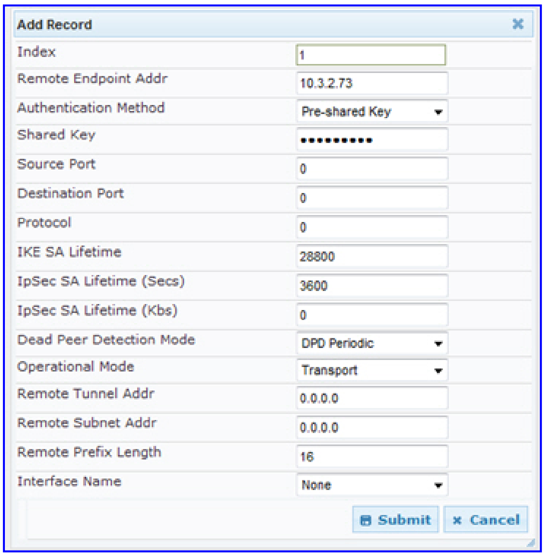
Notes:

- 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 73: 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

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 145.

5.8.2.4 PSTN

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

- Global Parameters - Refer to 'Global Parameters' on page 113
- Trunk Settings - Refer to 'Trunk Settings' on page 113
- Transmission Settings - For TP-6310 ONLY Refer to 'Transmission Settings' on page 118
- CAS State Machines - Refer to 'CAS State Machines' on page 120

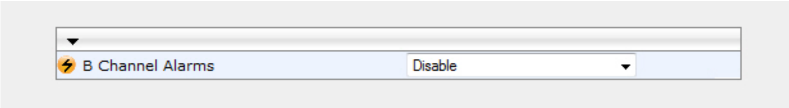
5.8.2.4.1 Global Parameters

The following describes how to configure PSTN Global Parameters. For a description of these parameter, refer to the Product Reference Manual.

➢ To configure PSTN Global Parameters:

1. Open the PSTN Global Parameters page (**Configuration** tab > VoIP menu > PSTN submenu > Global Parameters).

Figure 74: Global Parameters



B Channel Alarms: Disable

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.

5.8.2.4.2 Configuring Trunk Settings

The Trunk Settings page allows you to configure the device's trunks. This includes selecting the PSTN protocol and configuring related parameters. This page also provides the following features:

- Taking a Trunk Out of Service: Some parameters can be configured when the trunk is in service, while others require you to take the trunk out of service. This is done by clicking the Stop ⏹ button. Once you have "stopped" a trunk, all current calls are dropped and no new calls can be made on the trunk.
- Deactivating a Trunk: You can deactivate a trunk for maintenance. This is done by clicking the Deactivate Deactivate button. Deactivation temporarily disconnects (logically) the trunk from the PSTN network. Upon trunk deactivation, the device generates an AIS alarm on the trunk to the far-end. As a result, an RAI alarm signal may be received by the device. A subsequent trunk activation, done by clicking the Activate Activate button, reconnects the trunk to the PSTN network and clears the AIS alarm. Trunk deactivation is typically used for maintenance such as checking the trunk's physical integrity.
- Creating a Loopback Line: You can create (and remove) remote loopback for DS1 and DS3 lines. This is done by clicking the **Create Loopback** Create Loopback button. To remove the loopback, click the **Remove Loopback** Remove Loopback button.

For a description of the trunk parameters, refer to 'PSTN Parameters' in the Product Reference Manual.

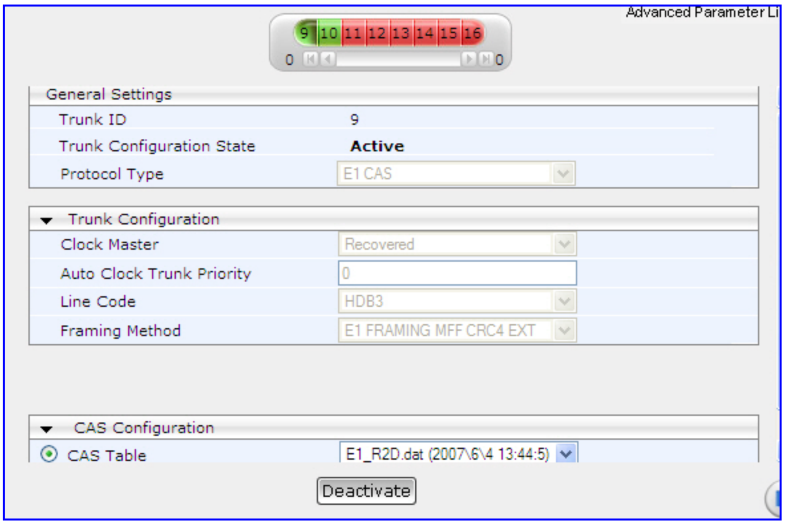
Notes:

- During trunk deactivation, trunk configuration cannot be performed.
- A stopped trunk cannot also be activated and a trunk cannot be deactivated if it has been stopped.

➢ To configure the Trunk Settings:

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

Figure 75: Trunk Settings - Stop Trunk



General Settings

Trunk ID	9
Trunk Configuration State	**Active**
Protocol Type	E1 CAS

Trunk Configuration

Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
Framing Method	E1 FRAMING MFF CRC4 EXT

CAS Configuration

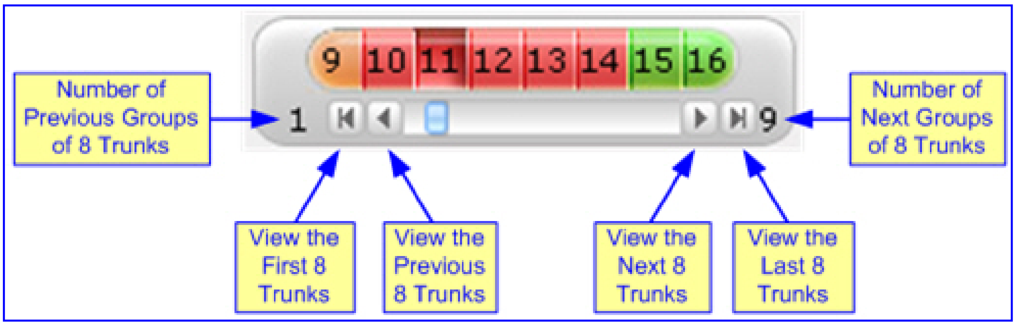
◉ CAS Table	E1_R2D.dat (2007\6\4 13:44:5)

On the top of the page, a bar with Trunk number icons displays the status of each trunk, according to the following color codes:

- **Grey:** Disabled
- **Green:** Active
- **Yellow:** RAI alarm (also appears when you deactivate a Trunk by clicking the Deactivate button)
- **Red:** LOS/LOF alarm
- **Blue:** AIS alarm
- **Orange:** D-channel alarm (ISDN only)

2. Select the trunk that you want to configure by clicking the desired Trunk number icon. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), see the figure below:

Figure 76: Trunk Scroll Bar


9
10
11
12
13
14
15
16
Number of Previous Groups of 8 Trunks
1
9
Number of Next Groups of 8 Trunks
View the First 8 Trunks
View the Previous 8 Trunks
View the Next 8 Trunks
View the Last 8 Trunks

Note: If the Trunk scroll bar displays all available trunks, the scroll bar buttons are unavailable.

After you have selected a trunk, the following is displayed:

- The read-only 'Trunk ID' field displays the selected trunk number.
- The read-only ‘Trunk Configuration State’ displays the state of the trunk ('Active' or 'Inactive').
- The displayed parameters pertain to the selected trunk only.

3. Click the **Stop Trunk** button (located at the bottom of the page) to take the trunk out of service so that you can configure the currently grayed out (unavailable) parameters. (Skip this step if you want to configure parameters that are available when the trunk is active). The stopped trunk is indicated by the following:
   - The ‘Trunk Configuration State’ field displays ‘Inactive’.
   - The Stop Trunk button is replaced by the Apply Trunk Settings button.

     When all trunks are stopped, the Apply to All Trunks button also appears.
   - All the parameters are available and can be modified.
4. Configure the trunk parameters as required.
5. Click **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunk**s to apply the changes to all trunks); the Stop Trunk button replaces Apply Trunk Settings and the ‘Trunk Configuration State’ displays 'Active'.
6. To save the changes to flash memory, see 'Saving Configuration' on page 145.

7. To reset the device, see 'Resetting the Device' on page 143.

Notes:

- If the ‘Protocol Type’ field displays 'NONE' (i.e., no protocol type is selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
- The displayed parameters depend on the protocol selected.
- All PRI trunks of the device must be of the same line type (i.e., E1 or T1). However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the device's Release Notes).
- If the protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can’t be stopped because it provides the device’s clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device’s clock or enable ‘TDM Bus PSTN Auto Clock’ in the TDM Bus Settings page (see 'TDM' on page 102).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

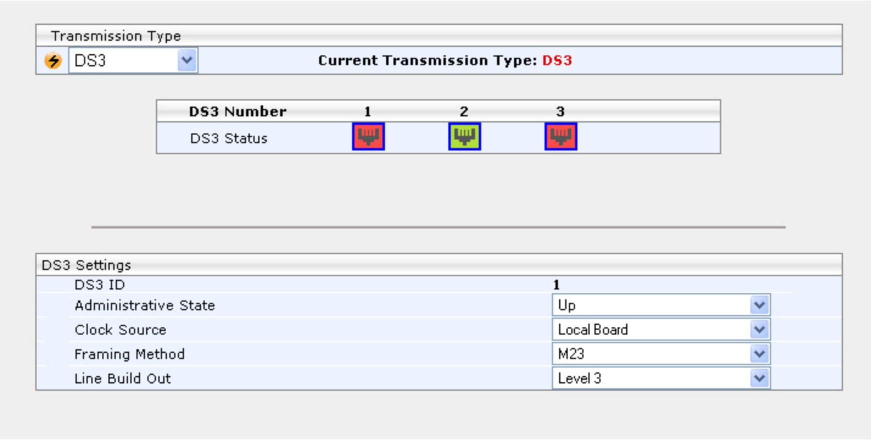
5.8.2.4.3 Transmission Settings - DS3

Note: 'T3' and 'DS3' are terms used interchangeably.

➢ **To configure the DS3 Settings, (when the current Transmission Type field is 'NONE'):**

1. Open the Transmission Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Transmission Settings**).
2. Select **DS3** from the drop-down Transmission Type list.

Figure 77: Transmission Settings - DS3



Transmission Type

DS3 — **Current Transmission Type: DS3**

DS3 Number	1	2	3
DS3 Status	🟥	🟩	🟥

DS3 Settings

DS3 ID	1
Administrative State	Up
Clock Source	Local Board
Framing Method	M23
Line Build Out	Level 3

3. The DS3 Settings appear. The DS3 Number and Status display are Read Only, showing the DS3 LED status and the DS3 parameters, as shown in the figure above. (The number of DS3 elements is hardware dependent.)

4. Configure/modify the DS3 Settings for individual DS3 interfaces according to the table below.

Transmission Type not Set to "DS3"

Parameter	Description
Administrative State	Selects Administrative State: Up or Down
Clock Source	Selects the clock source to be used: Local Board or External
Framing Method	Selects the physical DS3 framing method to be used: M13 or C-Bit
Line Build Out	Selects the DS3 Line Built Out

Note: The Administrative State Down value is only accepted if for all the 28 DS1s associated with a specific DS3 interface, Protocol Type is set to “None” (Trunk configuration state is “Not configured”).

5. Click **Submit**.

Note: The newly selected Transmission Type and DS3 Settings are only updated after clicking on the Burn Toolbar button and performing a Reset from the Device Actions pull-down menu.

➢ **To configure the DS3 Settings, (when the current Transmission Type field is already set to "DS3"):**

1. From the navigation tree on the left, click on the PSTN Settings - Transmission Settings link. The Transmission Settings page is displayed.

2. Configure/modify the DS3 Settings according to the table below.

Transmission Type is Previously Set to "DS3"

Parameter	Description
Administrative State	Selects Administrative State: Up or Down
Clock Source	Selects the clock source to be used: Local Board or External
Framing Method	Selects the physical DS3 framing method to be used: M13 or C-Bit
Line Build Out	Selects the DS3 Line Built Out

3. Click **Submit**. The changes take effect immediately.

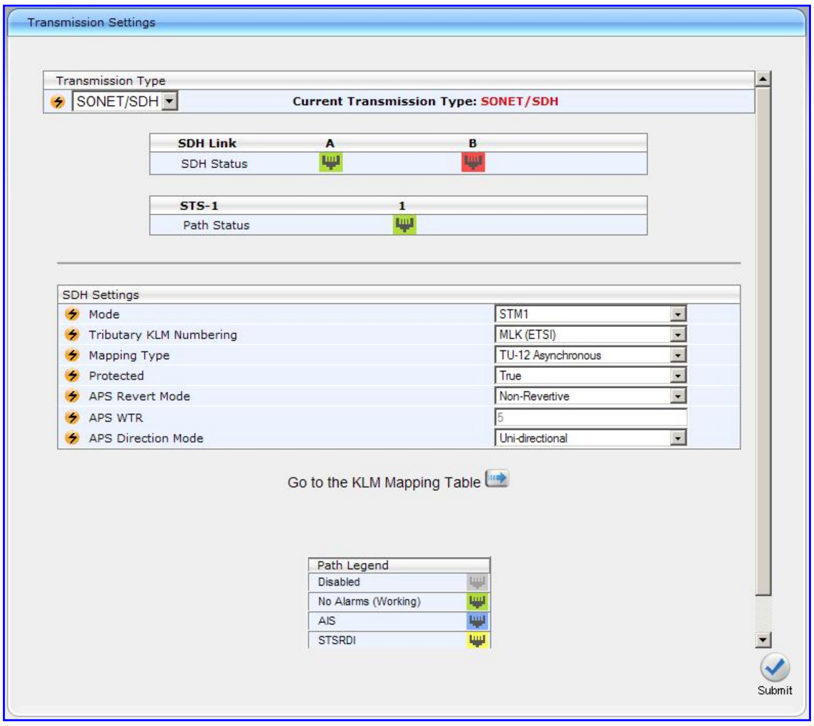
Note: Traffic disturbances may be encountered for a brief period.

5.8.2.4.4 Transmission Settings - SONET/SDH - For TP-6310 Only

➢ To configure the SONET or SDH Settings:

1. Open the Transmission Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Transmission Settings**). The default Transmission Type value is set to "NONE".
2. Select **SONET/SDH** from the drop-down Transmission Type list.

Figure 78: Transmission Settings - SONET/SDH



Transmission Settings

Transmission Type: SONET/SDH — Current Transmission Type: SONET/SDH

SDH Link	A	B
SDH Status	🟩	🟥

STS-1	1
Path Status	🟩

SDH Settings

Mode	STM1
Tributary KLM Numbering	MLK (ETSI)
Mapping Type	TU-12 Asynchronous
Protected	True
APS Revert Mode	Non-Revertive
APS WTR	5
APS Direction Mode	Uni-directional

Go to the KLM Mapping Table

Path Legend	
Disabled	⬜
No Alarms (Working)	🟩
AIS	🟦
STSRDI	🟨

3. The default Mode value is set to "Unknown". To change the mode to "OC3" (SONET) or "STM1" (SDH) from the drop-down list, select "OC3" or "STM1" appropriately.
4. The default Mapping Type is set to “Undefined”. To change the setting to VT1.5 (SONET) or VC12 (SDH), select “VT1.5 Asynchronous” or “TU-12 Asynchronous” from the drop-down list.
5. To change the Mapping Type setting to Asynchronous DS3 mapping (relevant only for Mode OC3), select “Asynchronous DS3” from the drop-down list. For the Asynchronous DS3 setting, KLM numbering is not relevant. Continue to Step 8.
6. Click on Go to the KLM Mapping Table to view the KLM Mapping Table.
7. To change the setting of the Tributary KLM Numbering to MLK, LMK or KLM, select “MLK (ETSI)”, “LMK (GR-253)” or “KLM (Timeslots)” from the drop-down list.
8. To change the setting of Protected field to “True” or “False”, select the appropriate value from the drop-down list.
9. To change the setting of the APS Revert Mode to “Revertive” or “Non-Revertive”, select the appropriate value from the drop-down list.
10. To change the setting of the APS WTR field (Wait-to-restore time), type the corresponding value in minutes that can change from 5 to 12 minutes. The field is available only when the APS Revert Mode field is set to “Revertive”.
11. To change the setting of APS Direction Mode to “Uni-directional” or “Bi-directional”, select the appropriate value from the drop-down list.
12. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference, when configuring/modifying the Transmission Settings parameters fields in the Transmission Settings page.

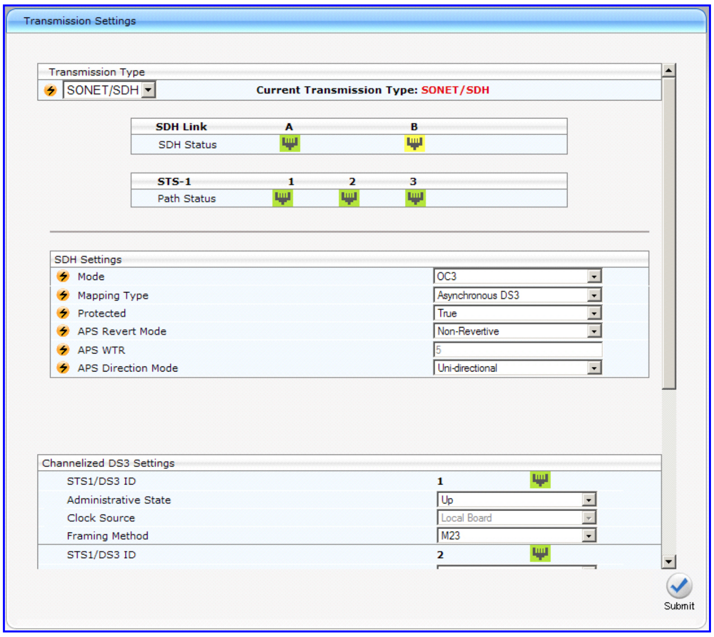
13. If Asynchronous DS3 mapping was selected in Step 5, the additional “Channelized DS3 Settings” pane becomes available. Proceed with the additional configuration steps as described in the Additional Configuration for Channelized DS3 Settings sub-section below, before continuing with Step 14.
14. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

> **Note:** The newly selected parameters, including Transmission Type, Mode, LP Mapping Type, Tributary KLM Numbering, etc., are only updated after clicking on the Burn Toolbar button and performing a Reset from the Device Actions pull-down menu.

5.8.2.4.5 Additional Configuration for Channelized DS3 Settings - For TP-6310 Only

The following describes an additional configuration for Channelized DS3 Settings.

Figure 79: Additional Configuration for Channelized DS3 Settings



Transmission Settings

Transmission Type: SONET/SDH — Current Transmission Type: SONET/SDH

SDH Link	A	B
SDH Status	🟩	🟩

STS-1	1	2	3
Path Status	🟩	🟩	🟩

SDH Settings

Mode	OC3
Mapping Type	Asynchronous DS3
Protected	True
APS Revert Mode	Non-Revertive
APS WTR	5
APS Direction Mode	Uni-directional

Channelized DS3 Settings

STS1/DS3 ID	1 🟩
Administrative State	Up
Clock Source	Local Board
Framing Method	M23
STS1/DS3 ID	2 🟩

1. The STS1/DS3 ID, the Status LED and the Clock Source fields are Read Only.
2. Configure/modify the DS3 Settings according to the following table:

Transmission Type is Set to "DS3"

Parameter	Description
Administrative State	Selects Administrative State: Up or Down
Framing Method	Selects the physical DS3 framing method to be used: M13 or C-Bit

Notes:

- The Administrative State Down value is only accepted if for all the 28 DS1s associated with a specific DS3 interface, Protocol Type is set to “None” (Trunk configuration state is “Not configured”).
- The following section is only applicable to the 3000/6310 device group.

5.8.2.4.6 CAS State Machines

A CAS file can be loaded only to trunks that support CAS protocols. To configure a CAS table, you must first stop all of the trunks relevant to the CAS table. Red Trunks are Active Trunks, which must be stopped in order to be configured.

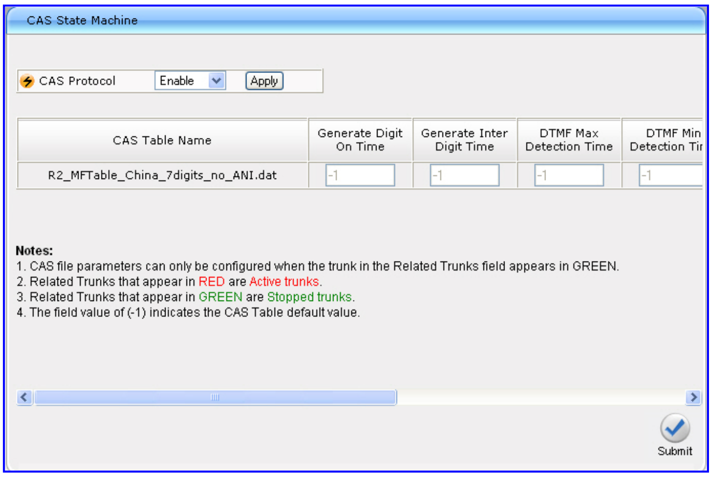
CAS Tables can be selected in either of two ways:

- Same CAS Table for the whole trunk - From the PSTN - Trunk Settings menu option, select the CAS Table per Trunk radio-button.
- Set CAS Table for each Channel group in a trunk - From the PSTN - Trunk Settings menu option, select the CAS Table per Channel radio-button and insert ‘0,0,0,1,1,1,2,2,2,0,0,0,1,1,1,0,1,2,0,2,1,2,2,2’ in the field. Alternatively, use the following ranges - ‘1-10:2,11-20:7,21-31:2’.

➢ To configure the CAS State Machines:

1. Open the CAS State Machines page (**Configuration** tab > **VoIP** menu > **PSTN** > **CAS State Machines**).

Figure 80: CAS State Machines



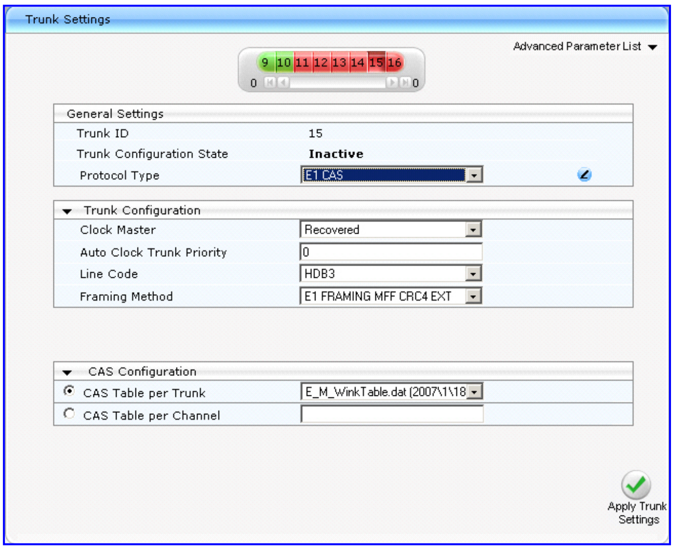
CAS Protocol: Enable

CAS Table Name	Generate Digit On Time	Generate Inter Digit Time	DTMF Max Detection Time	DTMF Min Detection Ti
R2_MFTable_China_7digits_no_ANI.dat	-1	-1	-1	-1

Notes:
1. CAS file parameters can only be configured when the trunk in the Related Trunks field appears in GREEN.
2. Related Trunks that appear in RED are Active trunks.
3. Related Trunks that appear in GREEN are Stopped trunks.
4. The field value of (-1) indicates the CAS Table default value.

2. The CAS file parameters can only be configured when trunks in the Related Trunks field are all green (meaning stopped). Stop all of the related trunks associated with the relevant CAS Table.
3. To stop a relevant trunk, click **Stop Trunk** on the Trunk Settings page.

Figure 81: Trunk Settings - View



General Settings

Trunk ID	15
Trunk Configuration State	**Inactive**
Protocol Type	E1 CAS

Trunk Configuration

Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	HDB3
Framing Method	E1 FRAMING MFF CRC4 EXT

CAS Configuration

● CAS Table per Trunk	E_M_WinkTable.dat (2007\1\18
○ CAS Table per Channel	

4. Stop each of the relevant trunks by repeating step 3.
5. Return to the CAS State Machine page. With all of the relevant trunks green, the row can be configured.
6. Configure the relevant fields of the row item.
7. Click **Submit**.
8. Configure the fields of the CAS table row.
9. To reactivate the relevant trunks, for each relevant trunk, click a trunk number on the Trunk Settings page. The Trunk Settings page appears.
10. Click **Apply Trunk Settings**. The trunk is activated and the status indicator is red.
11. Return to the CAS State Machine page and repeat steps 9 and 10 for each relevant trunk, until all of the relevant trunks are active and their status indicators are all red.

5.8.2.5 Media

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

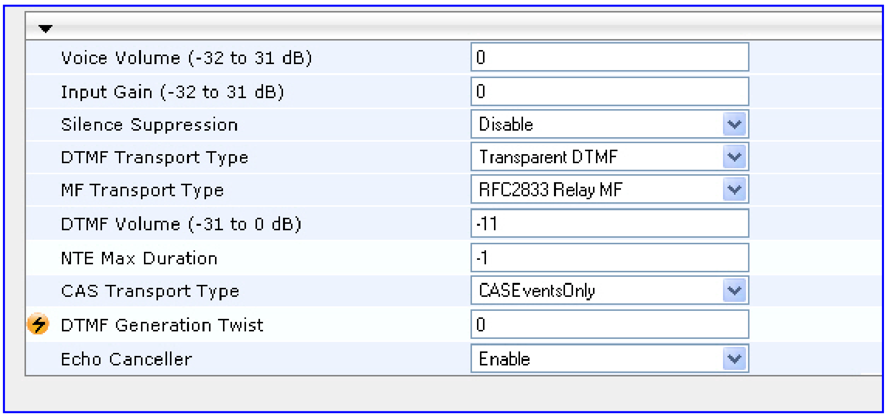
- Voice Settings - Refer to "Voice Settings" on page 122
- Fax/Modem/CID Settings - Refer to 'Fax/Modem/CID Settings' on page 123
- RTP/RTCP Settings - Refer to 'RTP Settings' on page 123
- IPMedia Settings - Refer to 'IPMedia Settings' on page 124
- General Media Settings - Refer to 'General Media Settings' on page 124
- DSP Templates - Refer to 'DSP Templates' on page 125
- AMR Policy Management - Refer to 'AMR Policy Management' on page 126t
- Media Realm Configuration - Refer to 'Media Realm Configuration' on page 126
- Media Security - Refer to 'Media Security' on page 133
- Media Quality of Experience - Refer to

5.8.2.5.1 Voice Settings

➢ **To configure the Voice Settings:**

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

Figure 82: 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 Canceller	Enable

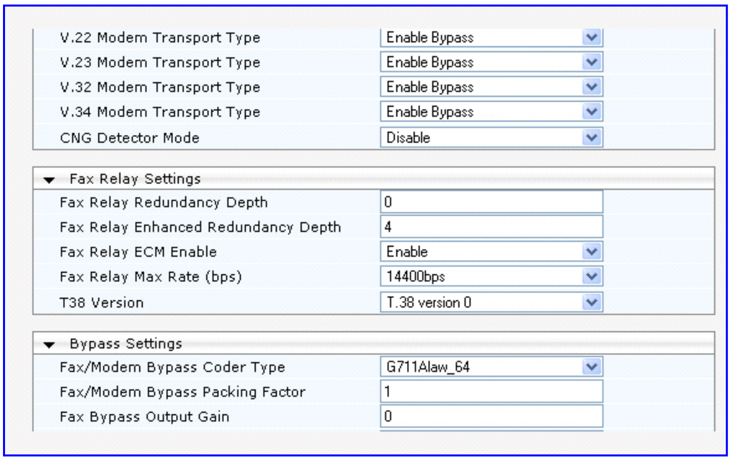
2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the Media Settings parameter fields in the Media Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered into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

5.8.2.5.2 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 83: Fax/Modem/CID Settings



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
T38 Version	T.38 version 0
▼ Bypass Settings	
Fax/Modem Bypass Coder Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0

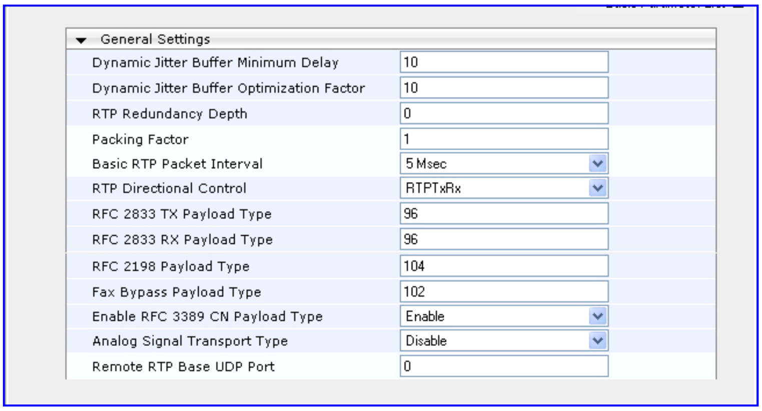
2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the Fax/Modem/CID Settings parameter fields in the Fax/Modem/CID Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes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

5.8.2.5.3 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 84: RTP/RTCP Settings



▼ General Settings	
Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	5 Msec
RTP Directional Control	RTPTxRx
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
Analog Signal Transport Type	Disable
Remote RTP Base UDP Port	0

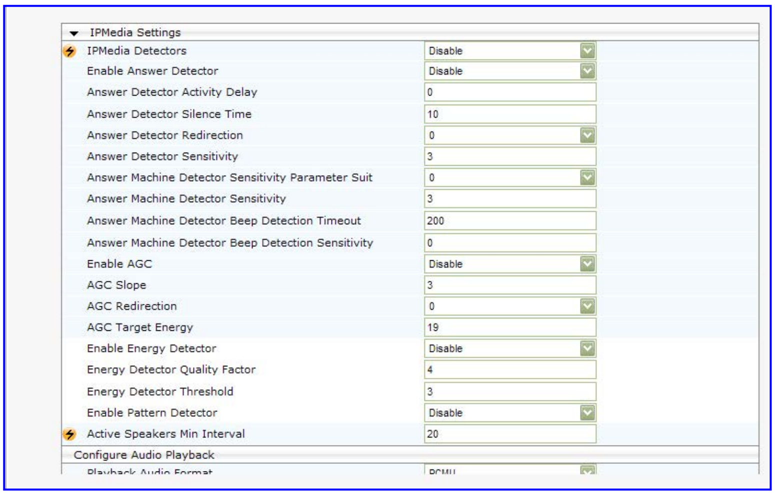
2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the RTP/RTCP Settings parameter fields in the RTP/RTCP Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered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

5.8.2.5.4 IPMedia Settings

➢ **To configure the IPMedia Settings:**

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

Figure 85: IP Media Settings



IPMedia Settings

IPMedia Detectors	Disable
Enable Answer Detector	Disable
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0
Answer Detector Sensitivity	3
Answer Machine Detector Sensitivity Parameter Suit	0
Answer Machine Detector Sensitivity	3
Answer Machine Detector Beep Detection Timeout	200
Answer Machine Detector Beep Detection Sensitivity	0
Enable AGC	Disable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19
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	PCMU

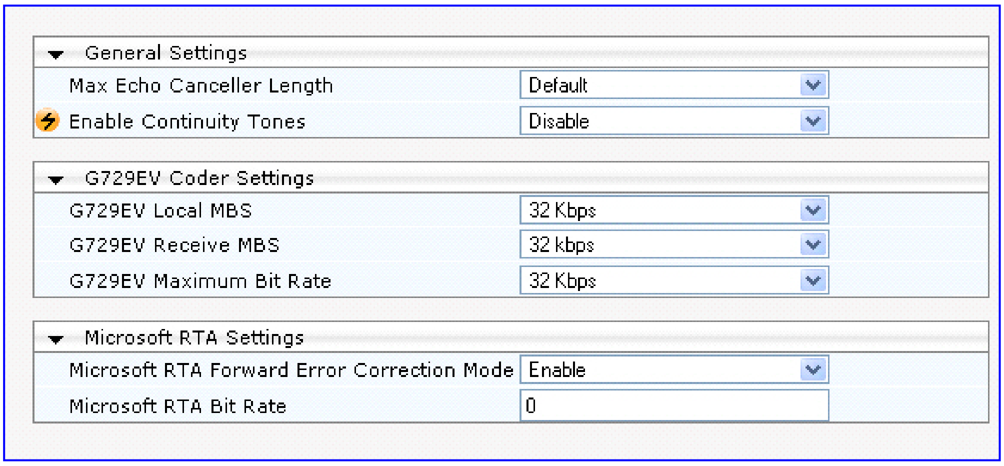
2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the IPMedia Settings parameter fields in the IPMedia Settings page.
3. After configuring/modifying the parameter fields, click the **Submit** button. The changes are entered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

5.8.2.5.5 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 86: General Media Settings



General Settings

Max Echo Canceller Length	Default
Enable Continuity Tones	Disable

G729EV Coder Settings

G729EV Local MBS	32 Kbps
G729EV Receive MBS	32 kbps
G729EV Maximum Bit Rate	32 Kbps

Microsoft RTA Settings

Microsoft RTA Forward Error Correction Mode	Enable
Microsoft RTA Bit Rate	0

2. Use the appropriate tables in ini File Parameters (see 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.

5.8.2.5.6 DSP Templates

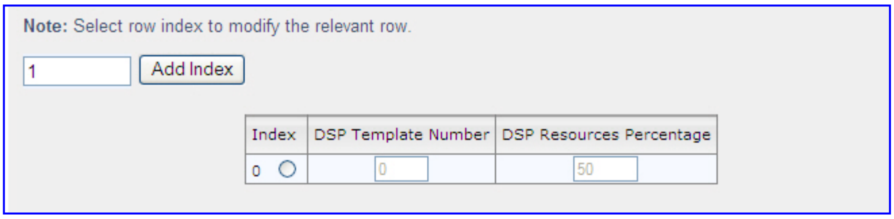
AudioCodes devices support several DSP templates, each with a different set of vocoders and add-on features. For further information about the DSP templates suitable for your network, contact AudioCodes Product Marketing.

Depending on the device hardware, either one or two DSP templates may be configured.

➢ **To configure DSP Templates:**

1. Open the DSP Templates page (**Configuration** tab > **VoIP** menu > **Media** > **DSP Templates**).
2. The DSP Templates page is displayed. In the case where only one DSP Version Template Number is used, type in the desired number and press the Set button.

Figure 87: DSP Template - Empty Table

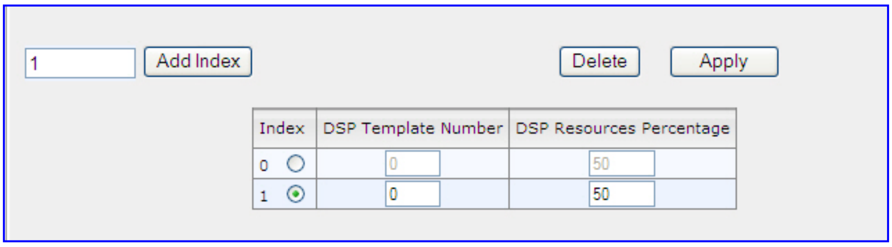


Note: Select row index to modify the relevant row.

Index	DSP Template Number	DSP Resources Percentage
0 ○	0	50

3. To configure multiple DSP templates, add a new row by clicking on Add Index. A new row appears on the page.

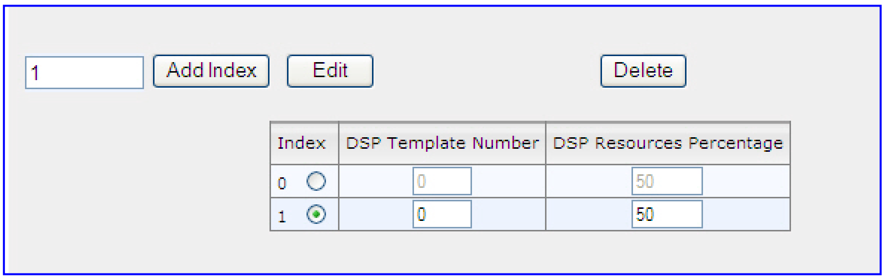
Figure 88: DSP Template - Add Row



Index	DSP Template Number	DSP Resources Percentage
0 ○	0	50
1 ●	0	50

4. To edit an existing row, first select the row by clicking on the appropriate Index number. The following page appears.

Figure 89: DSP Template Screen - Edit Row



Index	DSP Template Number	DSP Resources Percentage
0 ○	0	50
1 ●	0	50

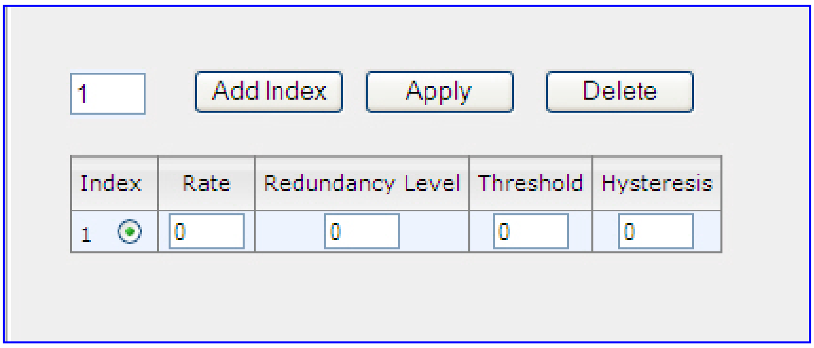
5. Click **Edit**. The following page appears. Make the necessary changes and click on Apply.
6. To delete a row, first select the row by clicking on the appropriate Index number.
7. Click **Delete** to delete the row.
8. Use the appropriate tables in 'Individual ini File Parameters' as a reference when configuring/modifying the DSP Template parameter fields.

5.8.2.5.7 AMR Policy Management

➢ **To configure AMR Policy Management:**

1. Open the AMR Policy Management page (**Configuration** tab > **Media** menu > **AMR Policy Management)**.

Figure 90: AMR Policy Management



Index	Rate	Redundancy Level	Threshold	Hysteresis
1 ●	0	0	0	0

2. The following command buttons are available in this table:
   - **Add Index:** Adds an index entry to the table.
   - **Apply:** Saves the configuration.
   - **Delete:** Deletes a selected index entry.

5.8.2.5.8 Configuring Media Realms

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)

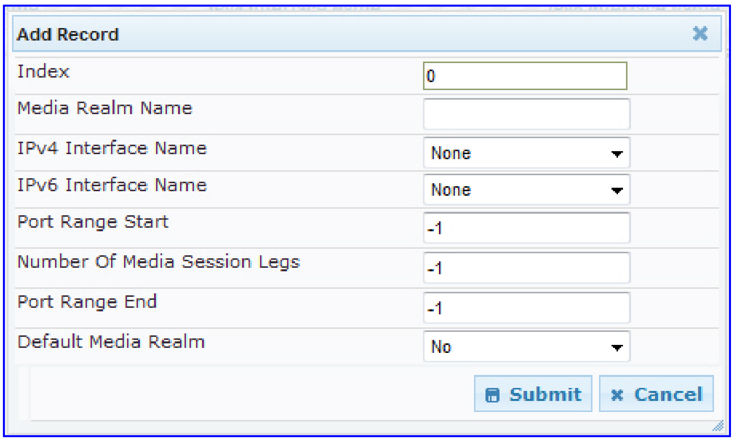
Notes:

- 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 91: Media Realm Page - Add Record Dialog Box



Add Record

Index	0
Media Realm Name	
IPv4 Interface Name	None
IPv6 Interface Name	None
Port Range Start	-1
Number Of Media Session Legs	-1
Port Range End	-1
Default Media Realm	No

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 145).

Media Realm Table Parameter Descriptions

Parameter	Description
Index [CpMediaRealm_ Index]	Defines the required table index number.
Media Realm Name [CpMediaRealm_ MediaRealmName]	Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters. **Notes:** ▪ 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.

Media Realm Table Parameter Descriptions

Parameter	Description
Port Range Start [CpMediaRealm_PortRangeStart]	Defines the starting port for the range of Media interface UDP ports. Notes: ▪ 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: ▪ **Mediant 3000/TP-6310:** BaseUDPport to BaseUDPport + 4031*10. For example, if BaseUDPPort is 6000 (default), then the available port range is 6000-46310 ▪ **Mediant 3000/TP-8410:** BaseUDPport to BaseUDPport + 4031*10 ▪ 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]	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. • **[0]** No (default) • **[1]** Yes **Notes:** 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.

5.8.2.5.9 Configuring Quality of Experience 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.

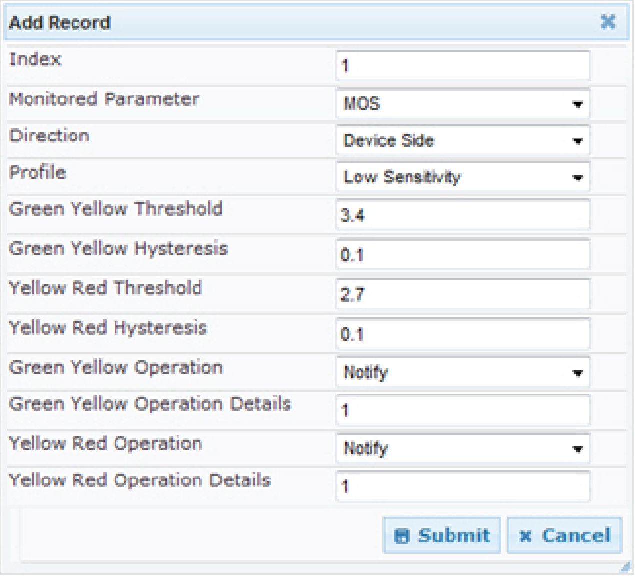
Notes:

- 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.
- You can also configure QoE per Media Realm using the table ini file parameter QOERules.

➢ 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.
3. Click the **Add** button; the following dialog box appears:

Figure 92: Quality of Experience Page - Add Record Dialog Box



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

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.

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

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. • **[0]** MOS (default) • **[1]** Delay • **[2]** Packet Loss • **[3]** Jitter • **[4]** RERL
Direction [QOERules_Direction]	Defines the monitoring direction. • **[0]** Device Side (default) • **[1]** Remote Side
Profile [QOERules_Profile]	Defines the pre-configured threshold profile to use. • **[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.

Parameter	Description
Green Yellow Threshold [QOERules_GreenYellow Threshold]	Defines the parameter threshold values between green (good quality) and yellow (medium quality) states.
Green Yellow Hysteresis [QOERules_GreenYellow Hystersis]	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.
Yellow Red Threshold [QOERules_YellowRedThreshold]	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.
Yellow Red Hysteresis [QOERules_YellowRed Hystersis]	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.
Green Yellow Operation [QOERules_GreenYellow Operation]	Defines the action that is done if the green-yellow threshold is crossed. • [1] Notify = (Default) Device sends a report to the SEM server. • [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg. • **Note:** This field is applicable only if the monitored parameter is remote packet loss.
Green Yellow Operation Details [QOERules_GreenYellowOperationDetails]	**Note:** This field is currently not supported. 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. **Note:** This field is applicable only if the 'Green Yellow Operation' field is set to Activate 2198.
Yellow Red Operation [QOERules_YellowRed Operation]	**Note:** This field is currently not supported. Defines the action that is done if the yellow-red threshold is crossed. • [1] Notify = (Default) Device sends a report to the SEM server. • [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg. **Note:** This field is applicable only if the monitored parameter is remote packet loss.
Yellow Red Operation Details [QOERules_YellowRedOperationDetails]	**Note:** This field is currently not supported. 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. **Note:** This field is applicable only if the 'Yellow Red Operation' field is set to Activate 2198.

5.8.2.5.10 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.

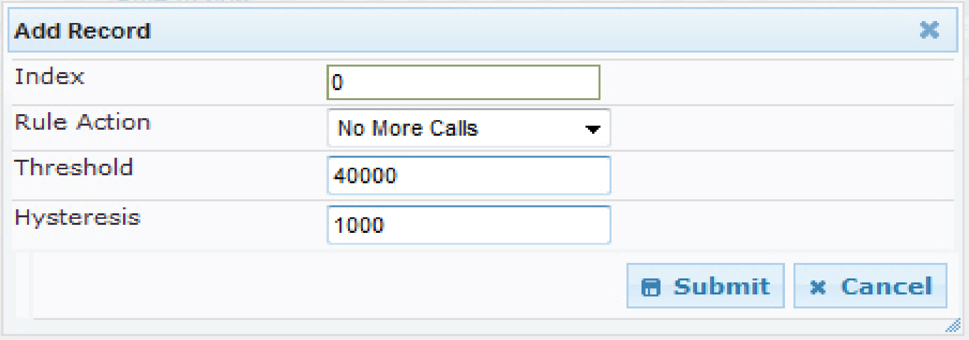
Notes:

- 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 93: Bandwidth Management Page - Add record Dialog Box



Add Record

Index	0
Rule Action	No More Calls
Threshold	40000
Hysteresis	1000

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: • **[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: • **[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.

5.8.2.5.11 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.

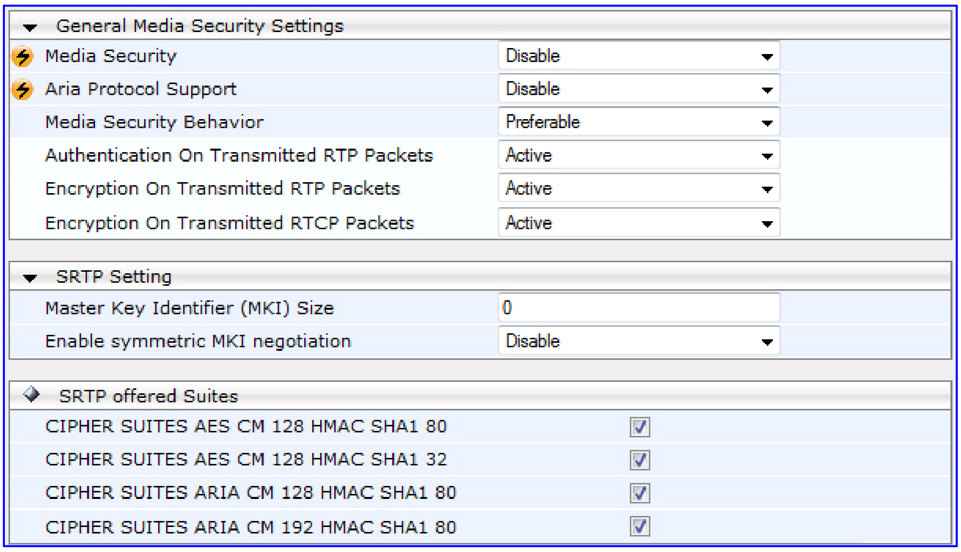
Notes:

- 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 94: 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	☑
CIPHER SUITES AES CM 128 HMAC SHA1 32	☑
CIPHER SUITES ARIA CM 128 HMAC SHA1 80	☑
CIPHER SUITES ARIA CM 192 HMAC SHA1 80	☑

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 145.

5.8.2.5.12Media Quality of Experience

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.

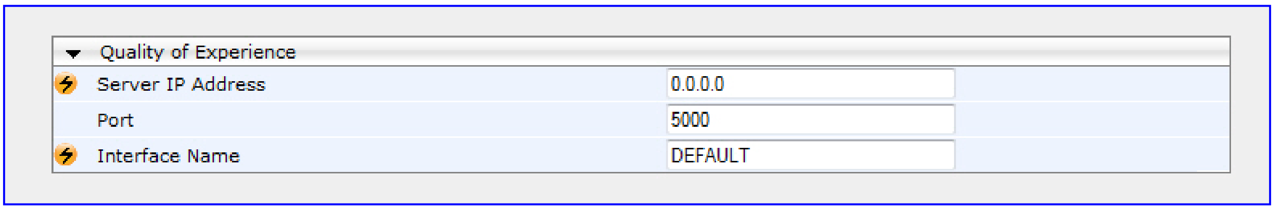
Notes:

- 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 Quality of Experience per Media Realm' on page 1.
- For information on the SEM server, refer to the EMS User's Manual.

➢ To configure QoE reporting of media:

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

Figure 95: Media Quality of Experience



Quality of Experience

Server IP Address	0.0.0.0
Port	5000
Interface Name	DEFAULT

2. Configure the parameters as required:
   - 'Server Ip' (QOEServerIP) - defines the IP address of the SEM server
   - '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
   - 'Use Mos LQ' (QOEUseMosLQ) - defines the reported MOS type (listening or conversational)
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 145.

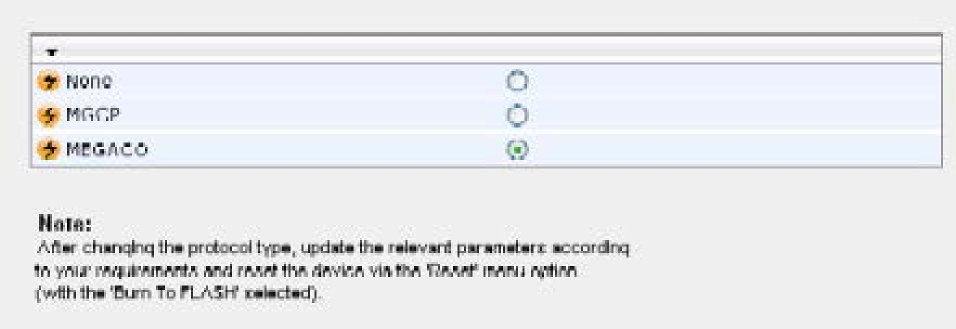
5.8.2.6 Call Control

5.8.2.6.1 Protocol Selection

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

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

Figure 96: Protocol Selection



None ○
MGCP ○
MEGACO ●

Note:
After changing the protocol type, update the relevant parameters according to your requirements and reset the device via the 'Reset' menu option (with the 'Burn To FLASH' selected).

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.

5.8.2.6.2 Control Interface Settings

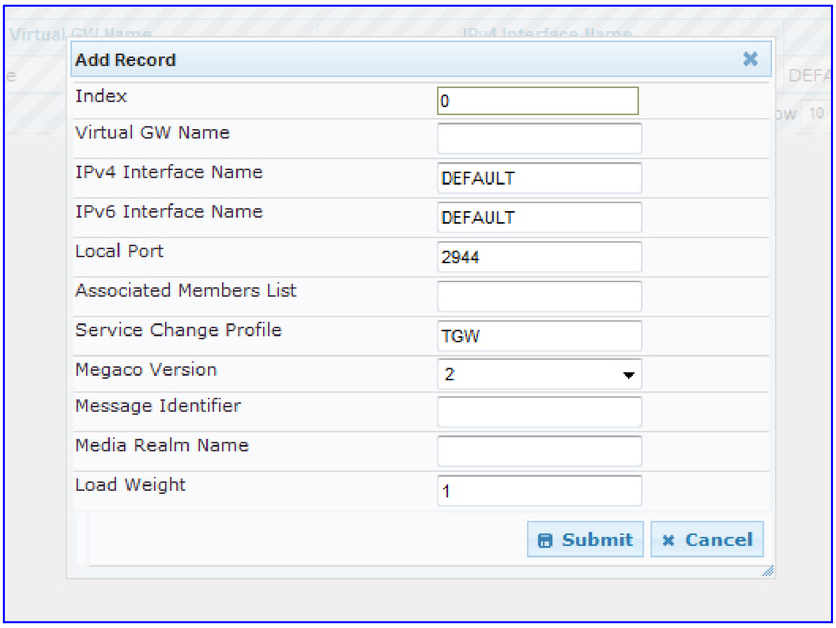
Control Interface Settings enable the user to configure several gateway parameters with the option to partition a physical gateway into several virtual gateways. If only one gateway configuration is present, the gateway operates without Virtual Gateway separation.

> **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**.

Figure 97: MEGACO Control Interface Settings



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

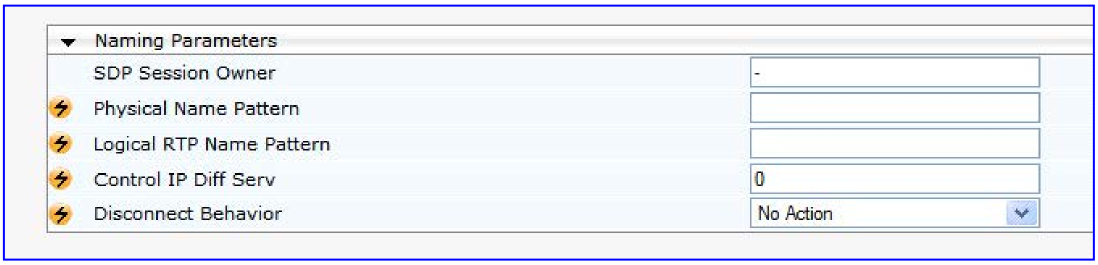
3. Configure the gateway parameters for this virtual gateway.
4. Click **Submit**.

5.8.2.6.3 Basic Configuration

➢ **To configure the Basic Configuration:**

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

Figure 98: MEGACO Basic Protocol Settings



SDP Session Owner	-
Physical Name Pattern	
Logical RTP Name Pattern	
Control IP Diff Serv	0
Disconnect Behavior	No Action

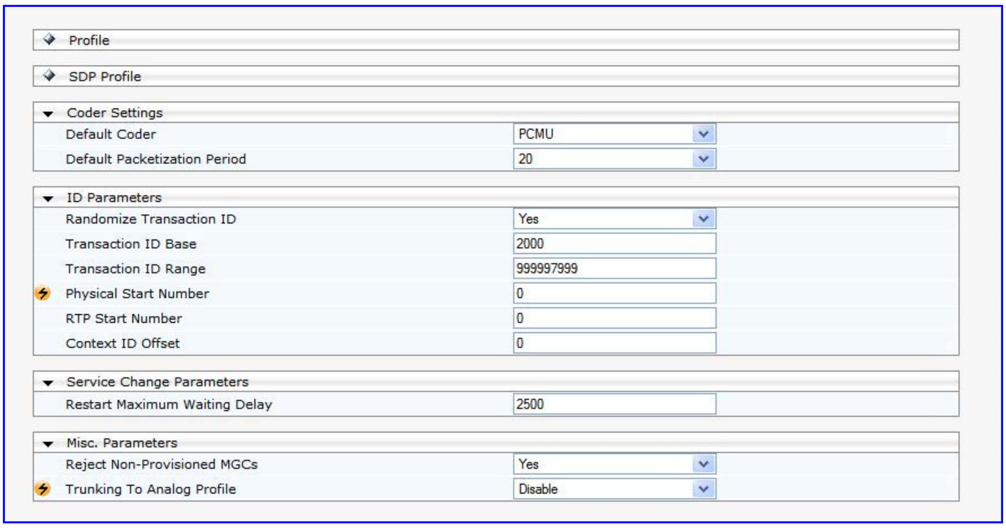
2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the Basic Configuration parameter fields in the ‘Basic Configuration’ page.
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered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

5.8.2.6.4 General Parameters

➢ **To configure the General Parameters:**

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

Figure 99: General Protocol Settings - MEGACO



Profile

SDP Profile

Coder Settings

Default Coder	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

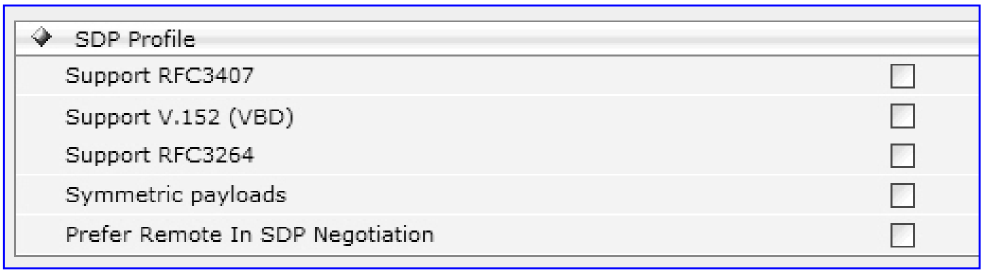
Restart Maximum Waiting Delay	2500

Misc. Parameters

Reject Non-Provisioned MGCs	Yes
⚡ Trunking To Analog Profile	Disable

2. Use the appropriate tables in ini File Parameters (see 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.

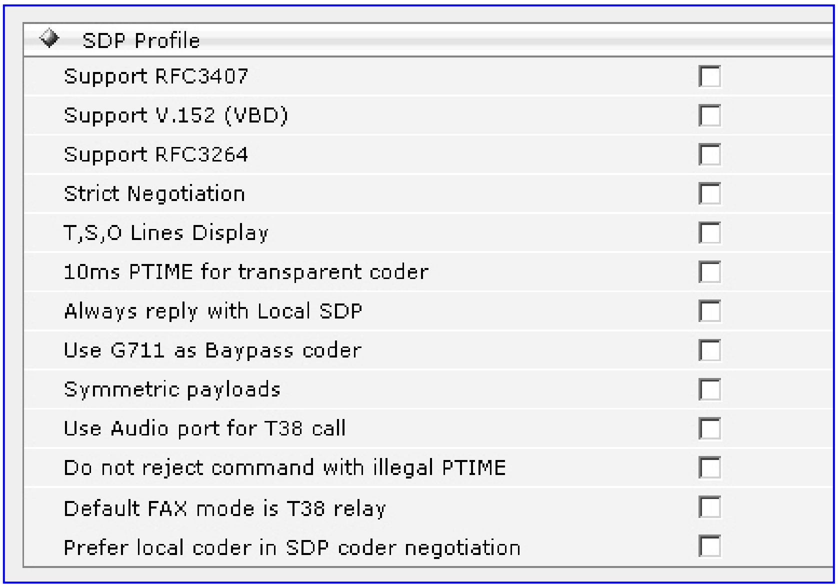
Figure 100: SDP Profile - MGCP



SDP Profile

Support RFC3407	□
Support V.152 (VBD)	□
Support RFC3264	□
Symmetric payloads	□
Prefer Remote In SDP Negotiation	□

Figure 101: SDP Profile - MEGACO



SDP Profile

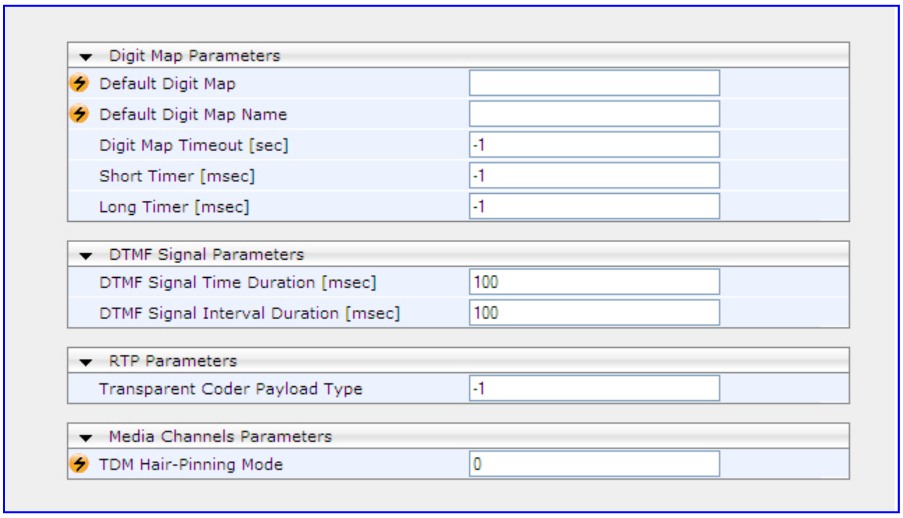
Support RFC3407	□
Support V.152 (VBD)	□
Support RFC3264	□
Strict Negotiation	□
T,S,O Lines Display	□
10ms PTIME for transparent coder	□
Always reply with Local SDP	□
Use G711 as Baypass coder	□
Symmetric payloads	□
Use Audio port for T38 call	□
Do not reject command with illegal PTIME	□
Default FAX mode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

5.8.2.6.5 Channel Configuration

➢ **To configure the Channel Configuration:**

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

Figure 102: Channel Protocol Settings - MEGACO



Digit Map Parameters	
Default Digit Map	
Default Digit Map Name	
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 ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the Channel Protocol Settings, in the Channel Protocol Settings page.

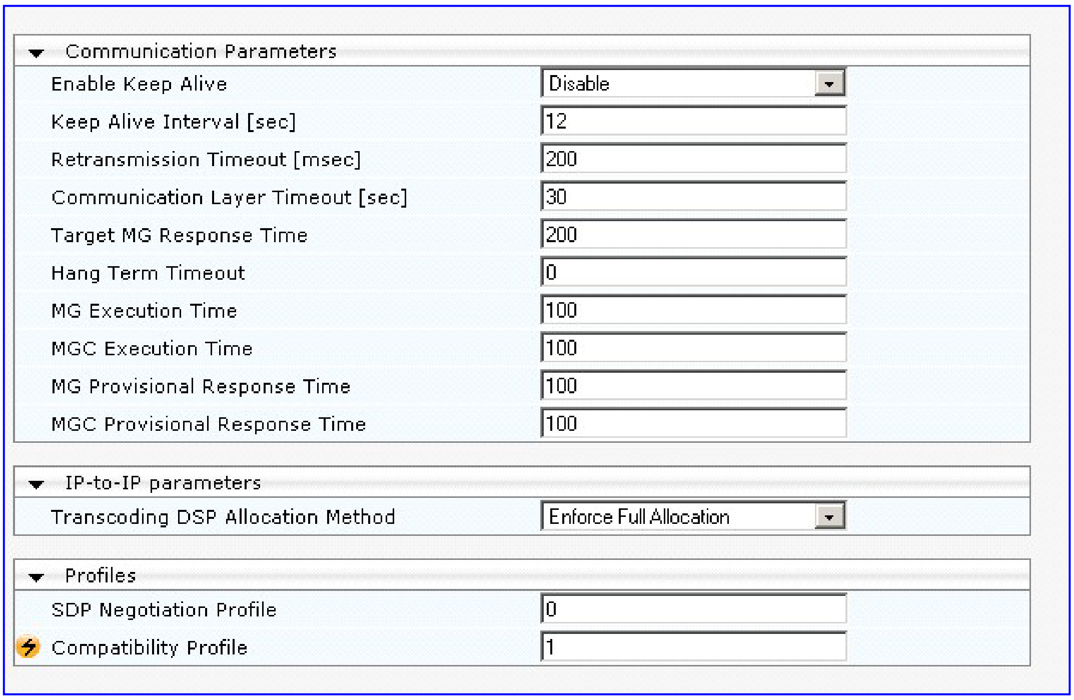
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

5.8.2.6.6 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 103: Advanced Protocol Settings - MEGACO



▼ 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
Hang Term Timeout	0
MG Execution Time	100
MGC Execution Time	100
MG Provisional Response Time	100
MGC Provisional Response Time	100

▼ IP-to-IP parameters

Transcoding DSP Allocation Method	Enforce Full Allocation

▼ Profiles

SDP Negotiation Profile	0
Compatibility Profile	1

2. Use the appropriate tables in ini File Parameters (see the Product Reference Manual) as a reference when configuring/modifying the Advanced Protocol Settings, in the Advanced Protocol Settings page.

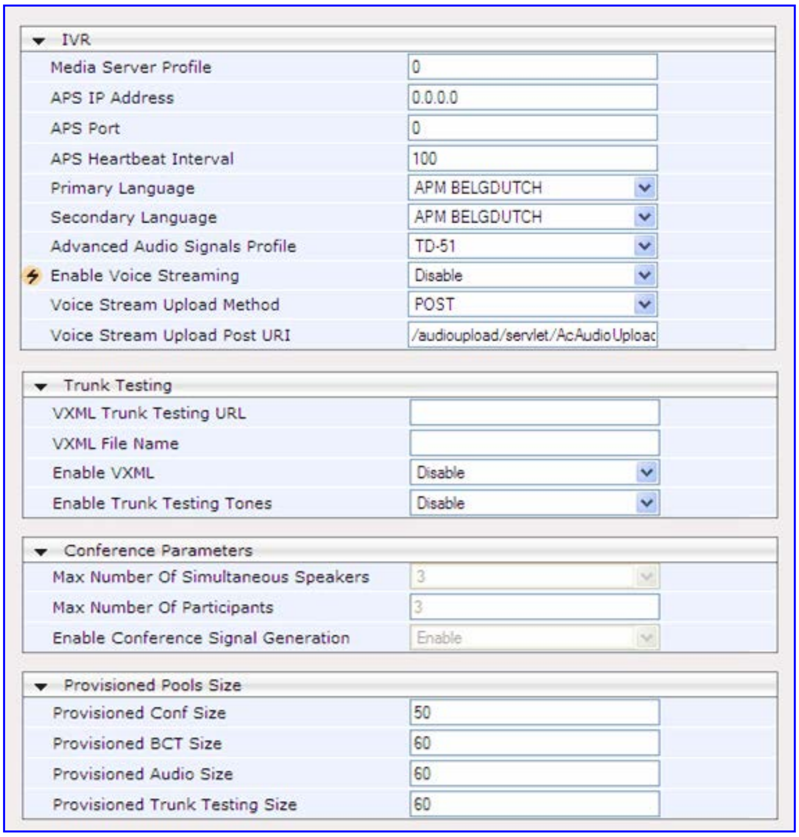
3. After configuring/modifying the parameter fields, click **Submit**. The changes are entered into the system and the page is refreshed.

5.8.2.6.7 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 104: 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/AcAudioUploac

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 ini File Parameters (see 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.

5.8.2.7 V5.2 Configuration (For TP-8410 Only)

For information on V5.2 Configuration, refer to the EMS User's Manual.

5.9 Maintenance

The Maintenance tab contains the following sub-menus:

- Maintenance - Refer to 'Maintenance' on page 142
- Software Update - Refer to 'Software Update' on page 146

5.9.1 Maintenance

5.9.1.1 Maintenance Actions

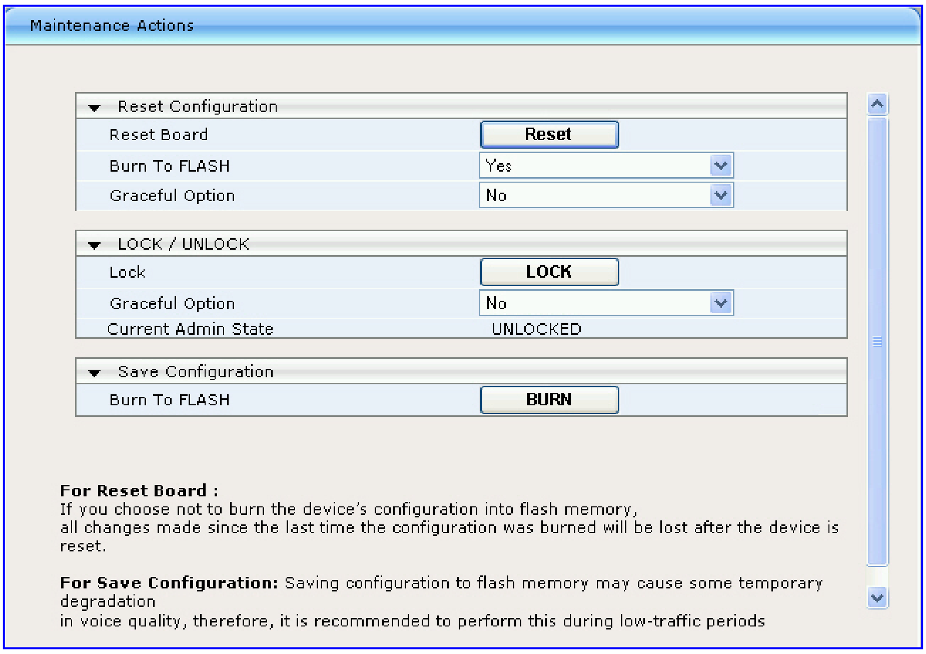
The 'Maintenance Actions' page allows you to perform the following operations:

- Reset the device (refer to 'Resetting the Device' on page 143)
- Lock and unlock the device (refer to ''Locking and Unlocking the Device' on page 144)
- Save the configuration to the device's flash memory (refer to 'Saving Configuration' on page 145)

➢ To access the Maintenance Actions page:

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

Figure 105: Maintenance Actions



Maintenance Actions

▼ Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

▼ LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Current Admin State	UNLOCKED

▼ Save Configuration

Burn To FLASH	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

5.9.1.1.1 Resetting the Device

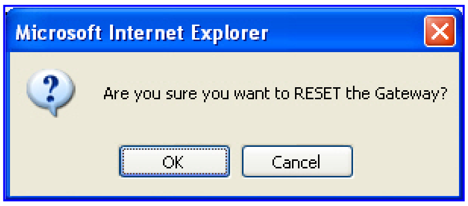
The 'Maintenance Actions' page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

- 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 142).
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 106: Reset Confirmation Message Box



Microsoft Internet Explorer

Are you sure you want to RESET the Gateway?

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.

5.9.1.1.2 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.

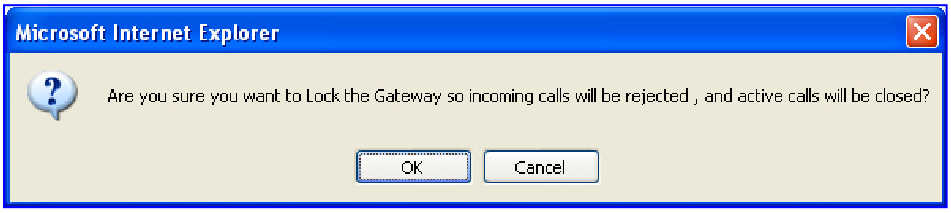
➢ **To lock the device:**

1. Open the 'Maintenance Actions' page (refer to 'Maintenance Actions' on page 142).
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 107: Device Lock Confirmation Message Box



Microsoft Internet Explorer

Are you sure you want to Lock the Gateway so incoming calls will be rejected , and active calls will be closed?

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 142).
2. Under the 'LOCK / UNLOCK' group, click **UNLOCK**. Unlock starts immediately and the device accepts new incoming calls.

5.9.1.1.3 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 142).
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 144).
- 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 143) for them to take effect.

5.9.1.2 High Availability Maintenance

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

- Switch Over - Switches between the Active and Redundant Boards
- Redundant Options - Resets the Redundant Board

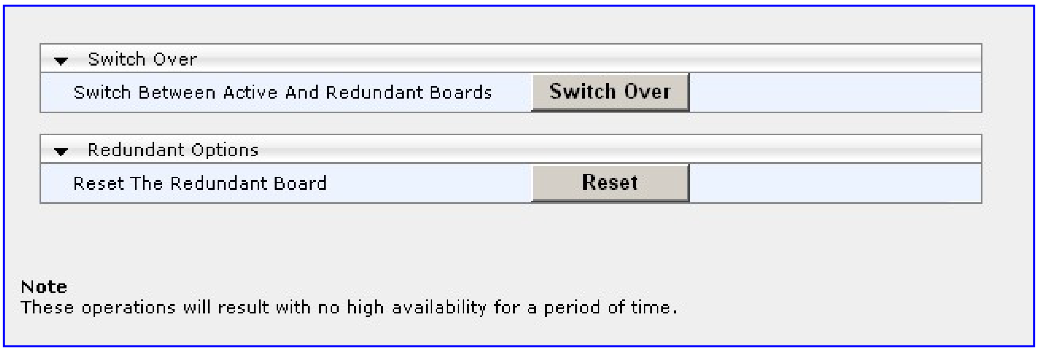
Note: The 'High Availability Maintenance' page can also be accessed from the Device Actions drop-down menu on the Toolbar. Refer to 'Toolbar' on page 48 for more information.

5.9.1.2.1 Switch Over

➢ To switch between the Active and Redundant Board:

1. Open the High Availability Maintenance page (**Maintenance** tab > **High Availability Maintenance**).
2. Click **Switch Over**.

Figure 108: High Availability Maintenance



▾ Switch Over
Switch Between Active And Redundant Boards
Switch Over
▾ Redundant Options
Reset The Redundant Board
Reset

Note

These operations will result with no high availability for a period of time.

5.9.1.2.2 Redundant Options

➢ **To reset the Redundant Board:**

1. Open the High Availability Maintenance page (**Maintenance** tab > **High Availability Maintenance**).
2. Click **Reset**.

5.9.2 Software Update

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 147.
- Software Upgrade Key - Refer to "Software Upgrade Key" on page 148.
- Software Upgrade Wizard - Refer to 'Software Upgrade Wizard' on page 151.
- Configuration File - Refer to 'Configuration File' on page 157.

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.

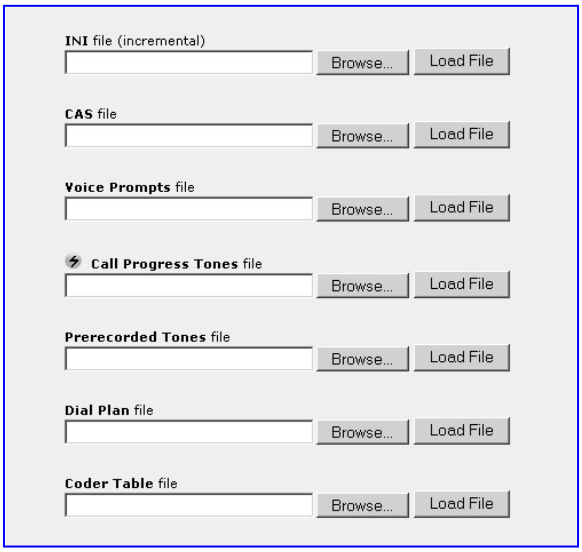
5.9.2.1 Load Auxiliary Files

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 109: 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.

5.9.2.2 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.

5.9.2.2.1 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.

5.9.2.2.2 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 162).

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 150).
- AudioCodes' EMS (refer to the EMS User's Manual or EMS Product Description).

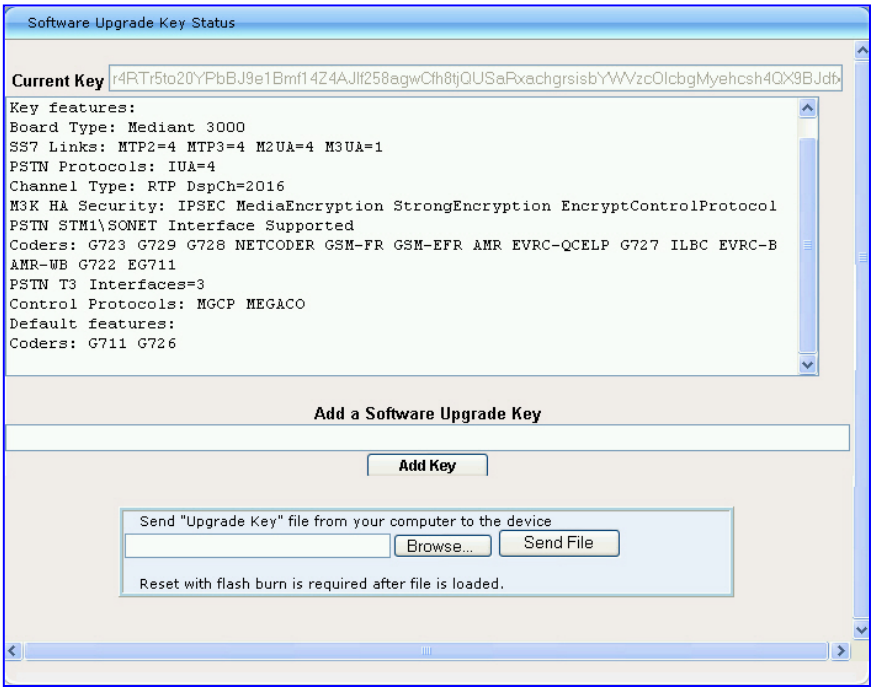
5.9.2.2.3 Loading the Software Upgrade Key Using the Web Interface

➢ To load a Software Upgrade Key using the Web interface:

1. Open the Software Upgrade Key page (Maintenance tab > Software Update menu > Software Upgrade Key).
2. When loading a single key S/N line to a device:
   - Open the Software Upgrade Key file (it should open in Notepad), select and copy the key string of the device's S/N and paste it into the Web field New Key. If the string is sent in the body of an Email, copy and paste it from there. Press the Add Key button.
3. When loading a Software Upgrade Key text file containing multiple S/N lines to a device:
   - (Refer to the figure, "Example of a Software Upgrade Key File Containing Multiple S/N Lines" on page 150)
   - Click **Browse** in the Send "Upgrade Key" file from your computer to the device field, and navigate to the Software Upgrade Key text file.
   - Click **Send File**; the new key is loaded to the device, validated and if valid is burned to memory. The new key is displayed in the Current Key field.
   - Validate the new key by scrolling through the 'Key features:' panel and verifying the presence / absence of the appropriate features.
4. After verifying that the Software Upgrade Key was successfully loaded, reset the device; the new capabilities and resources are active.

Note: For Mediant 3000 Systems, only use the Send "Upgrade key" functionality, with the Browse button, to select the file.

Figure 110: Software Upgrade Key Status



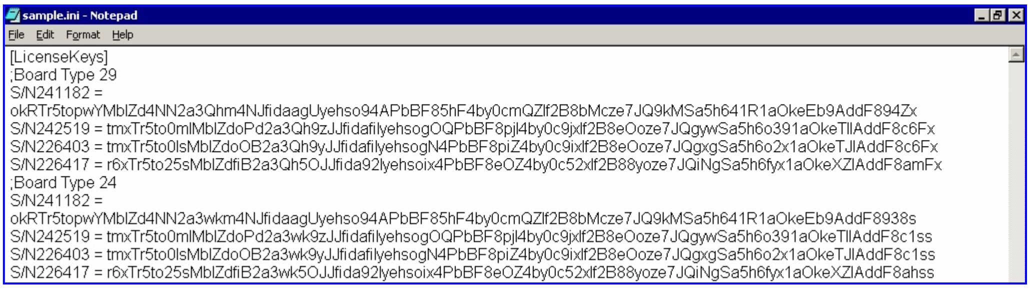
Current Key r4RTr5to20YPbBJ9e1Bmf14Z4AJlf258agwCfh8tjQUSaRxachgrsisbYWVzcOIcbgMyehcsh4QX9BJdb

```
Key features:
Board Type: Mediant 3000
SS7 Links: MTP2=4 MTP3=4 M2UA=4 M3UA=1
PSTN Protocols: IUA=4
Channel Type: RTP DspCh=2016
M3K HA Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
PSTN STM1\SONET Interface Supported
Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B
AMR-WB G722 EG711
PSTN T3 Interfaces=3
Control Protocols: MGCP MEGACO
Default features:
Coders: G711 G726
```

Add a Software Upgrade Key
Add Key
Send "Upgrade Key" file from your computer to the device
Browse...
Send File

Reset with flash burn is required after file is loaded.

Figure 111: Example of a Software Upgrade Key File (*.out) Containing Multiple S/N Lines



```
[LicenseKeys]
;Board Type 29
S/N241182 =
okRTr5topwYMblZd4NN2a3Qhm4NJfidaagUyehso94APbBF85hF4by0cmQZlf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF894Zx
S/N242519 = tmxTr5to0mlMblZdoPd2a3Qh9zJJfidafilyehsogOQPbBF8pjl4by0c9jxlf2B8eOoze7JQgywSa5h6o391aOkeTllAddF8c6Fx
S/N226403 = tmxTr5to0lsMblZdoOB2a3Qh9yJJfidafilyehsogN4PbBF8piZ4by0c9ixlf2B8eOoze7JQgxgSa5h6o2x1aOkeTJlAddF8c6Fx
S/N226417 = r6xTr5to25sMblZdfiB2a3Qh5OJJfida92lyehsoix4PbBF8eOZ4by0c52xlf2B88yoze7JQiNgSa5h6fyx1aOkeXZlAddF8amFx
;Board Type 24
S/N241182 =
okRTr5topwYMblZd4NN2a3wkm4NJfidaagUyehso94APbBF85hF4by0cmQZlf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF8938s
S/N242519 = tmxTr5to0mlMblZdoPd2a3wk9zJJfidafilyehsogOQPbBF8pjl4by0c9jxlf2B8eOoze7JQgywSa5h6o391aOkeTllAddF8c1ss
S/N226403 = tmxTr5to0lsMblZdoOB2a3wk9yJJfidafilyehsogN4PbBF8piZ4by0c9ixlf2B8eOoze7JQgxgSa5h6o2x1aOkeTJlAddF8c1ss
S/N226417 = r6xTr5to25sMblZdfiB2a3wk5OJJfida92lyehsoix4PbBF8eOZ4by0c52xlf2B88yoze7JQiNgSa5h6fyx1aOkeXZlAddF8ahss
```

5.9.2.2.4 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.

5.9.2.2.5 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"

5.9.2.2.6 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.

5.9.2.2.7 Abort Procedure

Reload the key you backed-up in "Backing up the Current Software Upgrade Key" on page 148 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 148.

5.9.2.3 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.

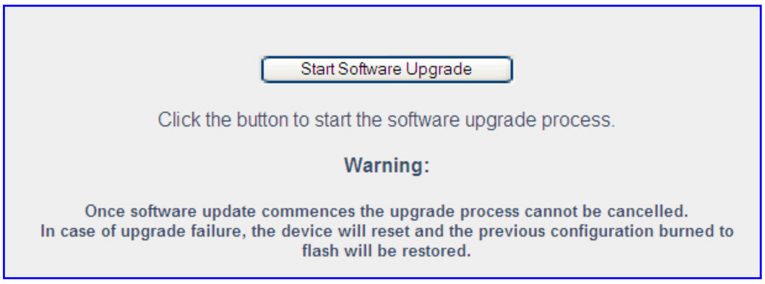
Loading a *.cmp file is mandatory in the Software Upgrade Wizard process. During the process, you choose from the auxiliary files provided for loading. For each auxiliary file type, you can choose between reloading an existing file, loading a new file or not loading a file at all.

➢ **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 112: Software Upgrade Wizard



Start Software Upgrade

Click the button to start the software upgrade process.

Warning:

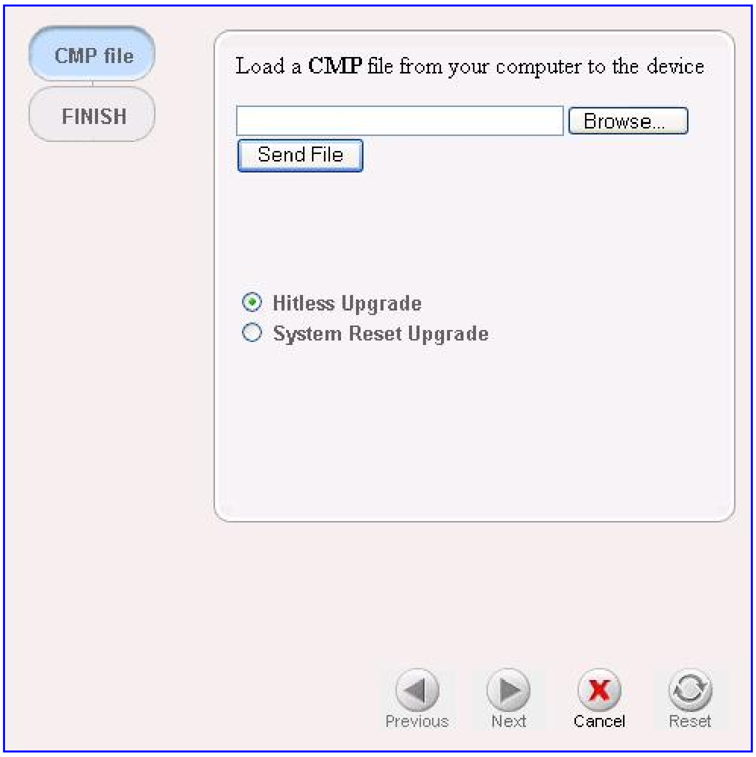
Once software update commences the upgrade process cannot be cancelled.
In case of upgrade failure, the device will reset and the previous configuration burned to flash will be restored.

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.

3. 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).

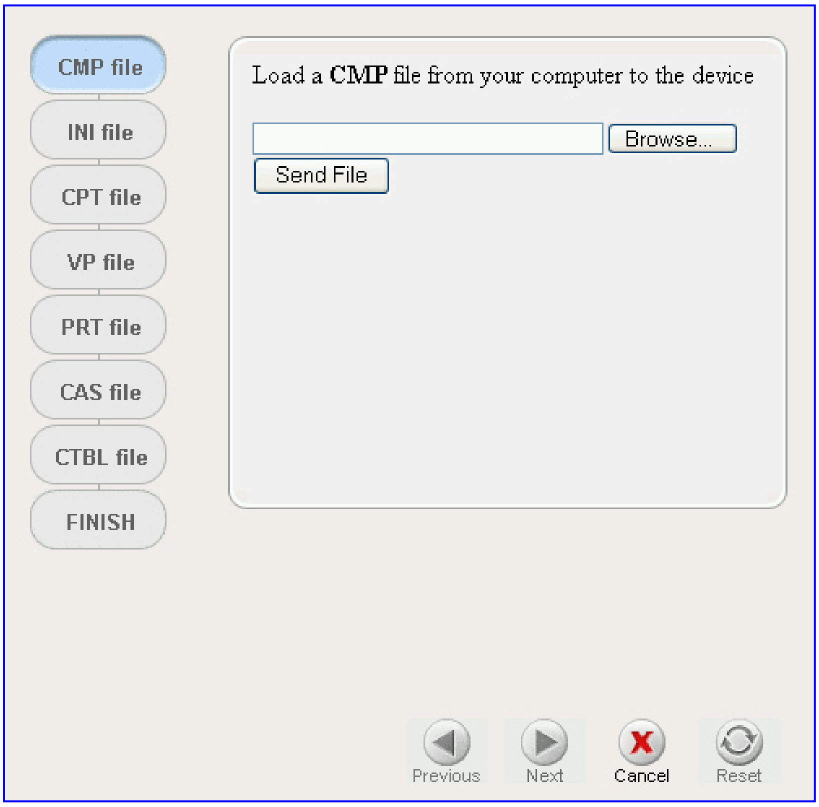
Figure 113: Load CMP File Dialog - Hitless



Load a CMP file from your computer to the device

● Hitless Upgrade
○ System Reset Upgrade

Figure 114: Load CMP File Dialog - Reset Upgrade



Load a CMP file from your computer to the device

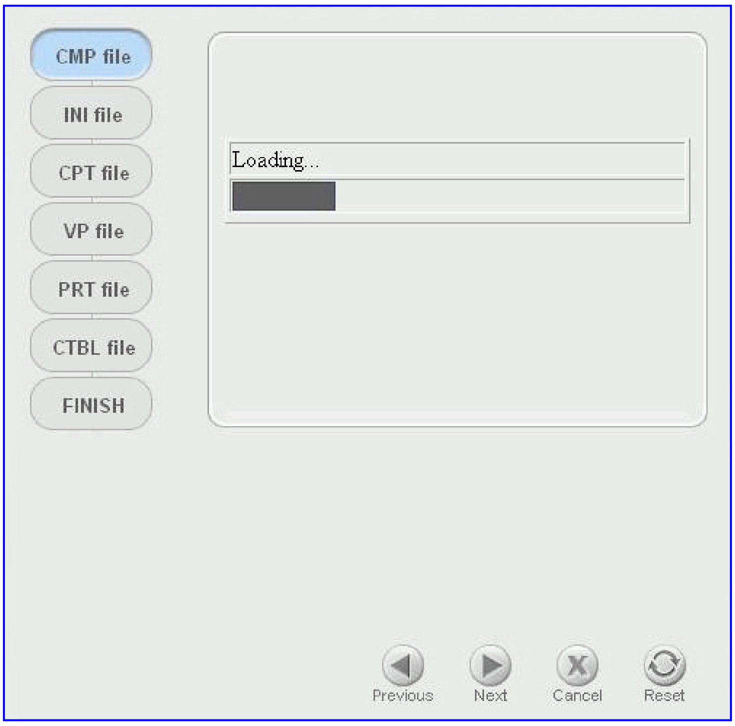
Note: In Hitless mode, the user will be able to only upload a CMP file (no other auxiliary files will be available for upload at this stage). When the Finish button is clicked, a 3-stage process will begin. Each stage will be displayed to the user in the Web interface. When the Hitless process ends,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

4. Click **Browse** and navigate to the location of the *.cmp file to be loaded. The path and file name appears in the field.
5. 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.

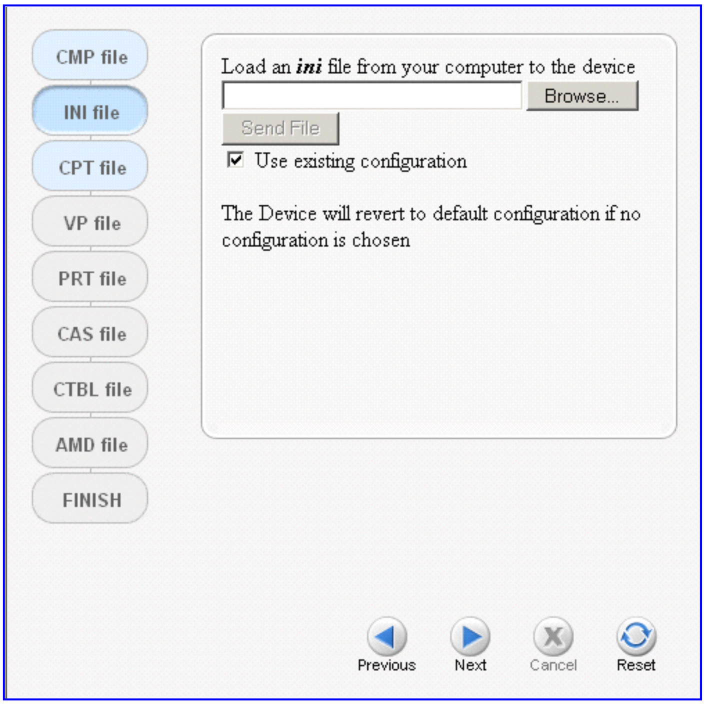
Figure 115: File Loading Dialog Screen



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

6. 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
7. 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 116: File Loading Dialog - INI Type Displayed



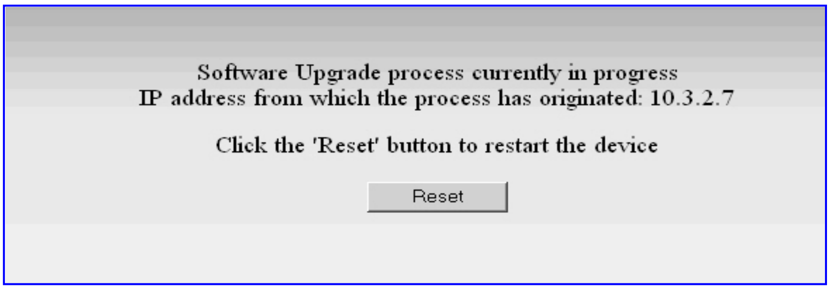
Load an ***ini*** file from your computer to the device

☑ Use existing configuration

The Device will revert to default configuration if no configuration is chosen

8. 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.
9. 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 117: Software Upgrade Process

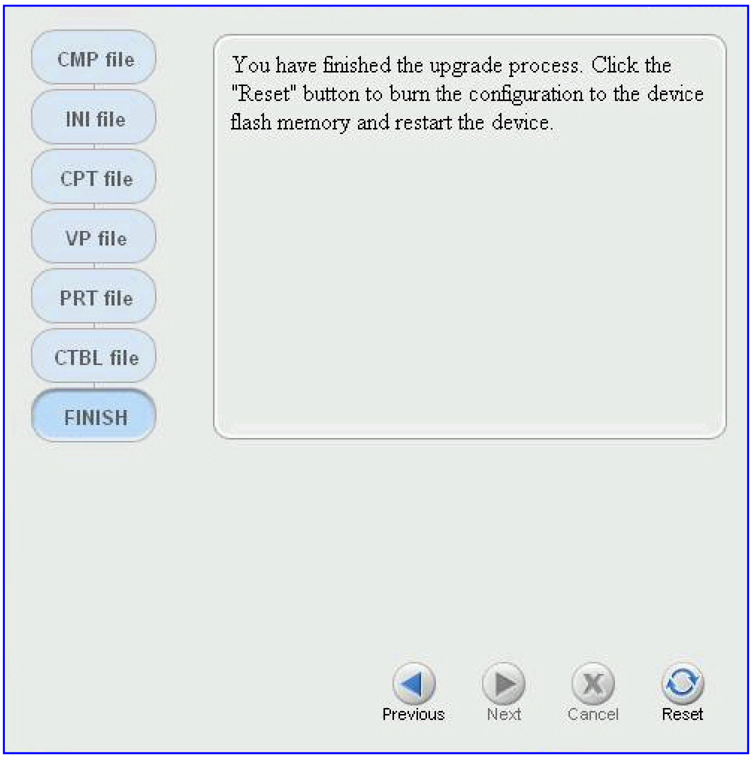


Software Upgrade process currently in progress
IP address from which the process has originated: 10.3.2.7

Click the 'Reset' button to restart the device

   - Click the **Reset** button; the device is reset utilizing the previous configuration files.
10. 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).

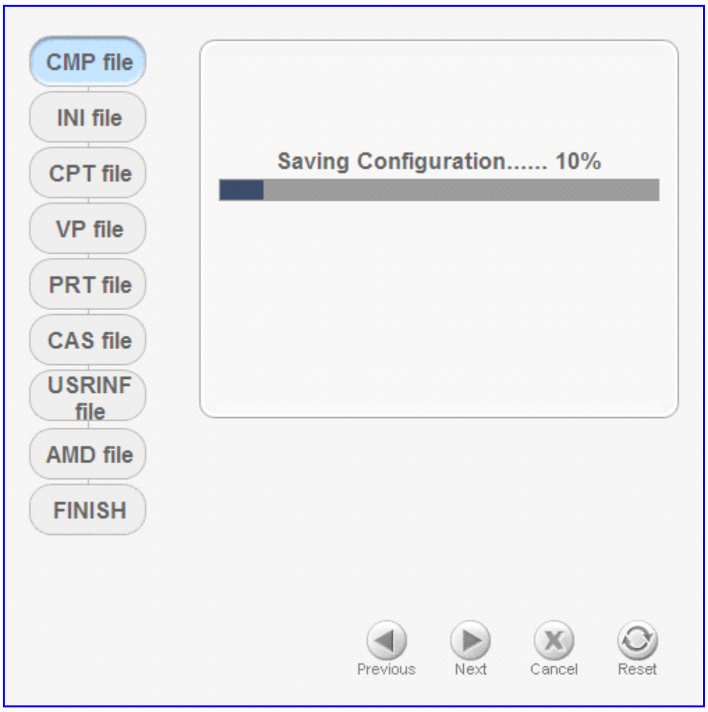
Figure 118: File Loading Dialog Screen - Reset Button Stage



You have finished the upgrade process. Click the "Reset" button to burn the configuration to the device flash memory and restart the device.

11. 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.

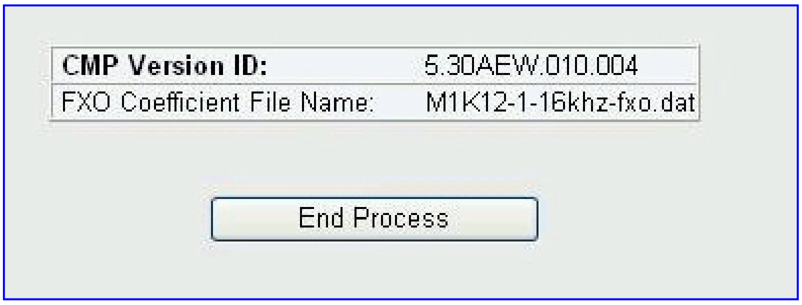
Figure 119: Saving Progress Bar



Saving Configuration...... 10%

12. 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 120: End of Process Dialog Screen



CMP Version ID:	5.30AEW.010.004
FXO Coefficient File Name:	M1K12-1-16khz-fxo.dat

13. Click **End Process**.

5.9.2.4 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.

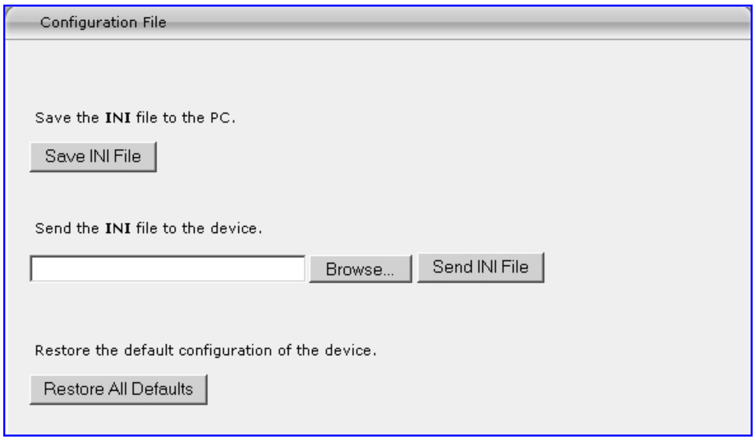
The ini file is a proprietary configuration text file containing configuration parameters and data. Sending the ini file to the device only provisions parameters that are contained in the ini file.

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 121: Configuration File Screen



Configuration File

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

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

Restore the default configuration of the device.

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.

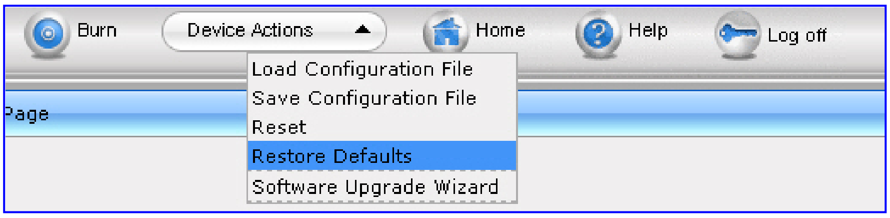
5.9.2.4.1 Downloading ini file

➢ **To download ini file (after blade startup):**

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

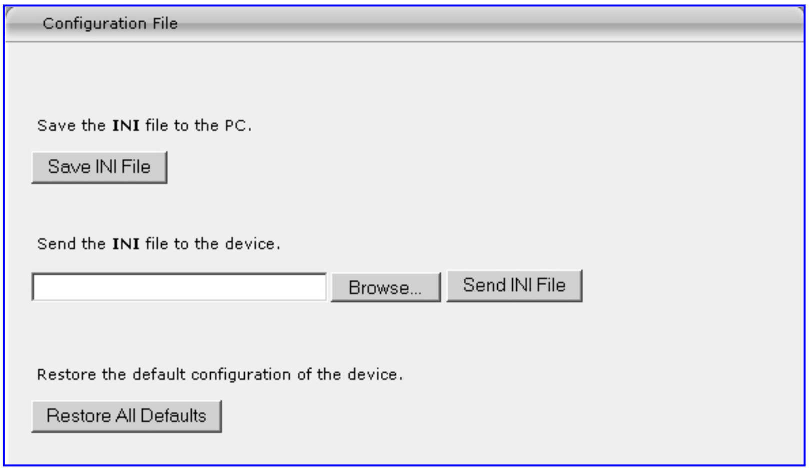
Note: The Restore Defaults option MUST be selected in order to successfully complete this process.

Figure 122: Device Actions



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 123: Configuration File


Configuration File

Save the INI file to the PC.

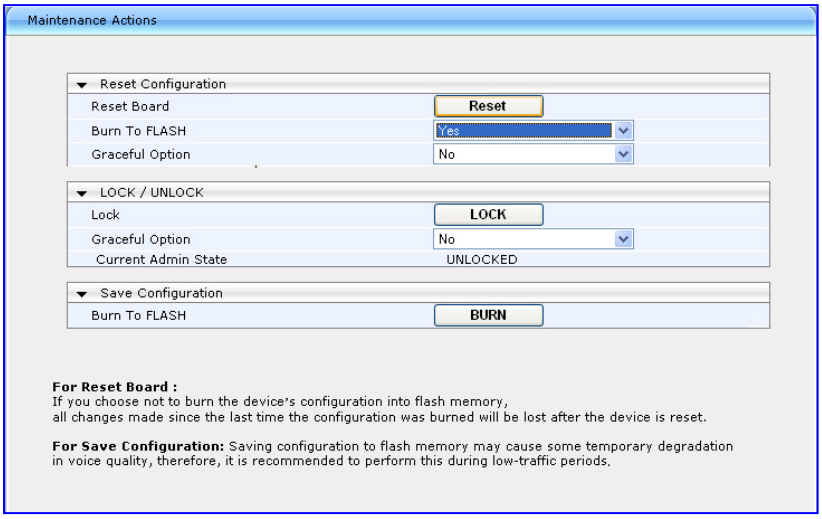
Send the INI file to the device.

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 124: Maintenance Actions



Maintenance Actions

▼ Reset Configuration

Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No

▼ LOCK / UNLOCK

Lock	LOCK
Graceful Option	No
Current Admin State	UNLOCKED

▼ Save Configuration

Burn To FLASH	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.

5.10 Status and Diagnostic Menu

➢ **To access the Status and Diagnostics menu:**

- 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 161
        - Device Information - Refer to 'Device Information' on page 162
        - Ethernet Port Information - Refer to 'Ethernet Port Information' on page 163
        - Carrier-Grade Alarms
            - ✓ Active Alarms - Refer to 'Active Alarms' on page 163
    - **Performance Monitoring**
        - Trunk Utilization - Refer to Viewing Trunk Utilization on page 165
        - Viewing MOS per Media Realm - Refer to 'Viewing MOS per Media Realm' on page 166
    - **VoIP Status**
        - Trunk & Channel Status - Refer to 'Trunk & Channel Status' on page 168
        - IP Interface Status - Refer to 'IP Interface Status' on page 170
        - Performance Statistics - Refer to 'Performance Statistics' on page 171
        - Timing Module Information - Refer to 'Timing Module Information' on page 171
        - Components Status - Refer to 'Components Status' on page 172

5.10.1 System Status

5.10.1.1 Message Log

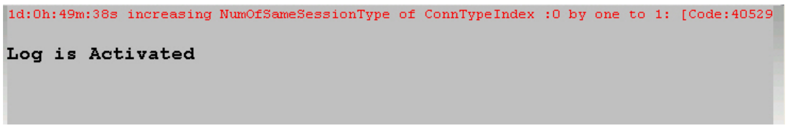
The Message Log is similar to a Syslog. It provides debug messages useful in pursuing troubleshooting issues.

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 recommend 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 125: Message Log Screen



```
1d:0h:49m:38s increasing NumOfSameSessionType of ConnTypeIndex :0 by one to 1: [Code:40529

Log is Activated
```

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.

5.10.1.2 Device Information

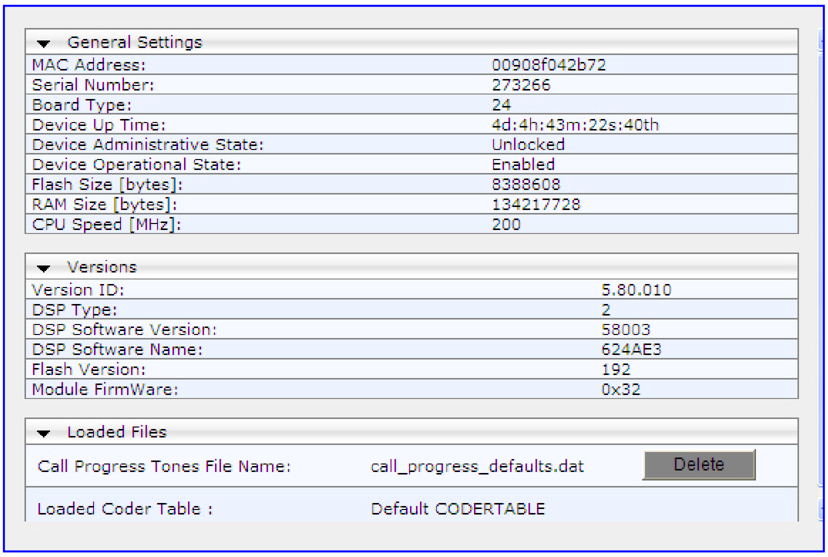
The Device Information page displays hardware, software device information and Device state information. This information can help you to expedite any troubleshooting process. Capture the page and email it to Technical Support personnel to ensure quick diagnosis and effective corrective action.

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 126: 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:

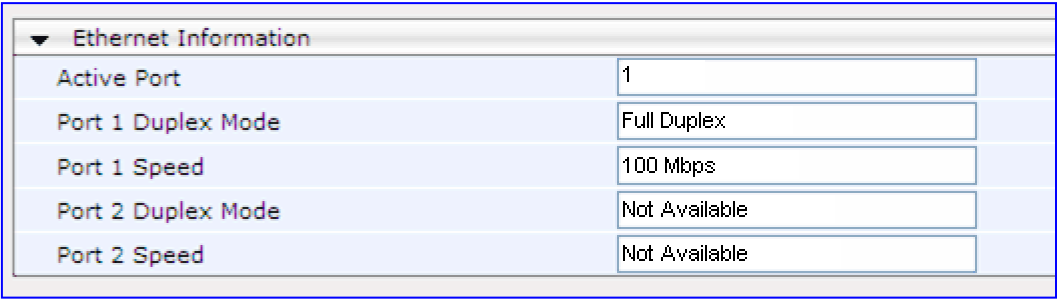
1. From the toolbar, click on the Status and Diagnostics link. The Status and Diagnostics page appears.
2. From the navigation tree, click the **Device Information** link. The Device Information page appears.
3. In the Device Information table, click **Delete**. The file deletion takes effect only after 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.

5.10.1.3 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 127: 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

5.10.1.4 Carrier-Grade Alarms

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

- Active Alarms
- Alarms History

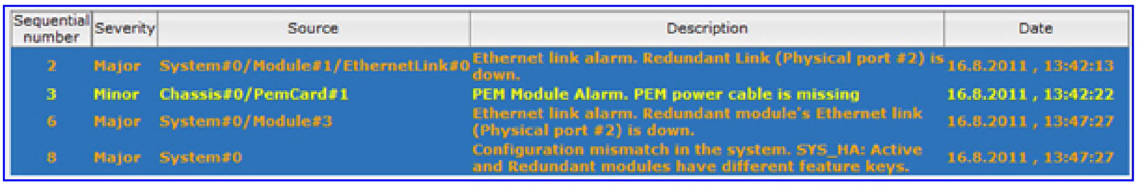
5.10.1.4.1Viewing Active Alarms

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 128: 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.

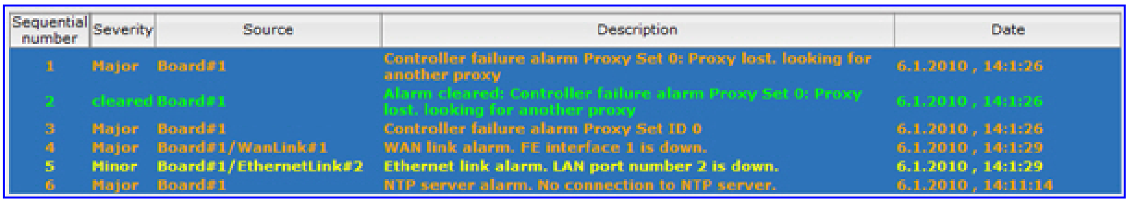
5.10.1.4.2Viewing Alarm History

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:**

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

Figure 129: 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

2. For each alarm, the following information is provided:

- Severity level of the alarm:
  - Critical (red)
  - Major (range)
  - 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.

5.10.2 Performance Monitoring

5.10.2.1 Viewing Trunk Utilization

The Trunk Utilization page provides an X-Y graph that displays the number of active channels per trunk over time. The x-axis indicates the time; the y-axis indicates the number of active trunk channels.

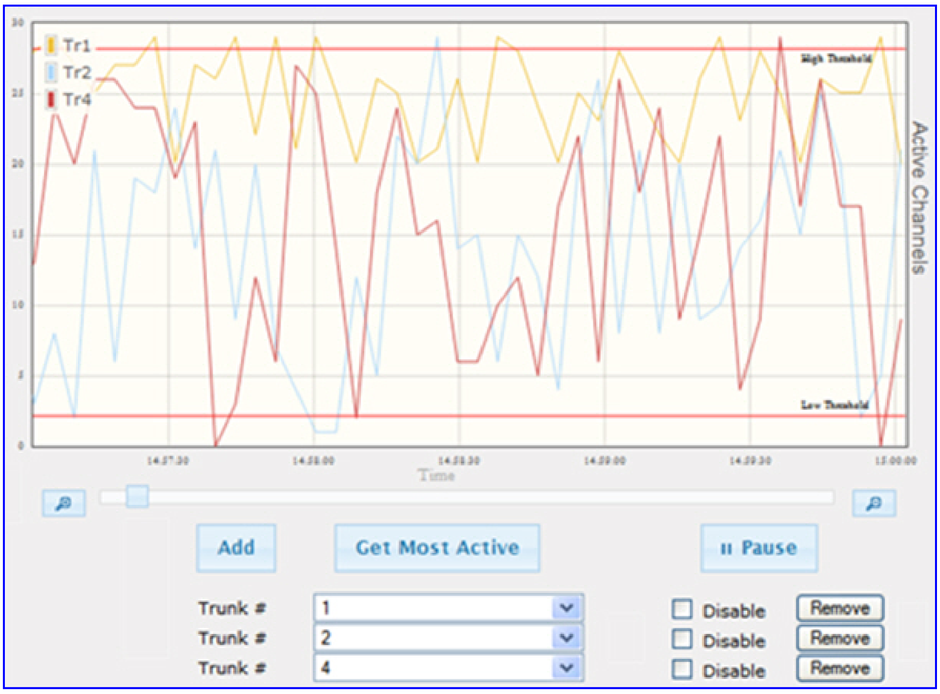
Notes:

- This page is available only if you have trunks and the SBC application is disabled.
- If you navigate to a different page, the data displayed in the graph and all its settings are cleared.

➢ **To view the number of active trunk channels**

1. Open the Trunk Utilization page (Status & Diagnostics tab > Performance Monitoring menu > Trunk Utilization).

Figure 130: Trunk Utilization Page



Trunk # 1 □ Disable

Trunk # 2 □ Disable

Trunk # 4 □ Disable

2. From the 'Trunk' drop-down list, select the trunk for which you want to view active channels.
3. For more graph functionality, see the following table:

Additional Graph Functionality for Trunk Utilization

Button	Description

Button	Description
Add button	Displays additional trunks in the graph. Up to five trunks can be displayed simultaneously in the graph. To view another trunk, click this button and then from the new 'Trunk' drop-down list, select the required trunk. Each trunk is displayed in a different color, according to the legend shown in the top-left corner of the graph.
Remove button	Removes the selected trunk display from the graph.
Disable check box	Hides or shows an already selected trunk. Select this check box to temporarily hide the trunk display; clear this check box to show the trunk. This is useful if you do not want to remove the trunk entirely (using the Remove button).
Get Most Active button	Displays only the trunk with the most active channels (i.e., trunk with the most calls).
Pause button	Pauses the display in the graph.
Play button	Resumes the display in the graph.
Zoom slide ruler and buttons	Increases or reduces the trunk utilization display resolution concerning time. The Zoom In 🔍 button increases the time resolution; the Zoom Out 🔍 button decreases it. Instead of using the buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

5.10.2.2 Viewing MOS per Media Realm

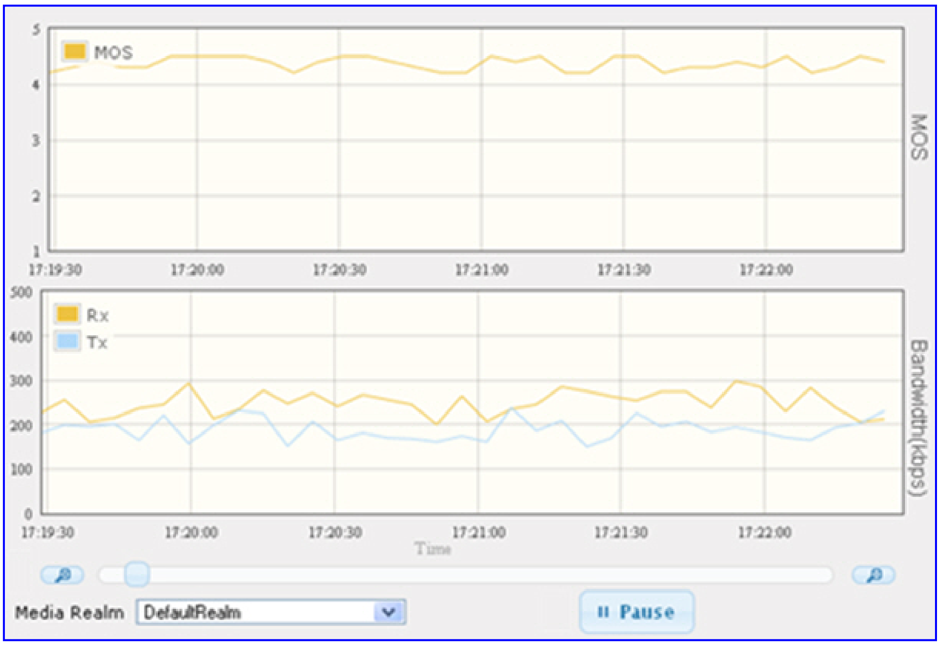
The MOS Per Media Realm page displays statistics on Media Realms (configured in 'Configuring Media Realms' on page). This page provides two graphs:

- **Upper graph:** Displays the Mean Opinion Score (MOS) quality in RTCP data per selected Media Realm.
- **Lower graph:** Displays the bandwidth of transmitted media (in Kbps) in RTCP data per Media Realm.

➢ To view the MOS per Media Realm graph:

1. Open the MOS Per Media Realm page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **MOS Per Media Realm**).

Figure 131: MOS Per Media Realm Graph



Media Realm: DefaultRealm

2. From the 'Media Realm' drop-down list, select the Media Realm for which you want to view.

3. Use the Zoom In 🔍 button to increase the displayed time resolution or the Zoom Out 🔍 button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

4. To pause the graph, click the **Pause** button; click **Play** to resume.

5.10.3 VoIP Status

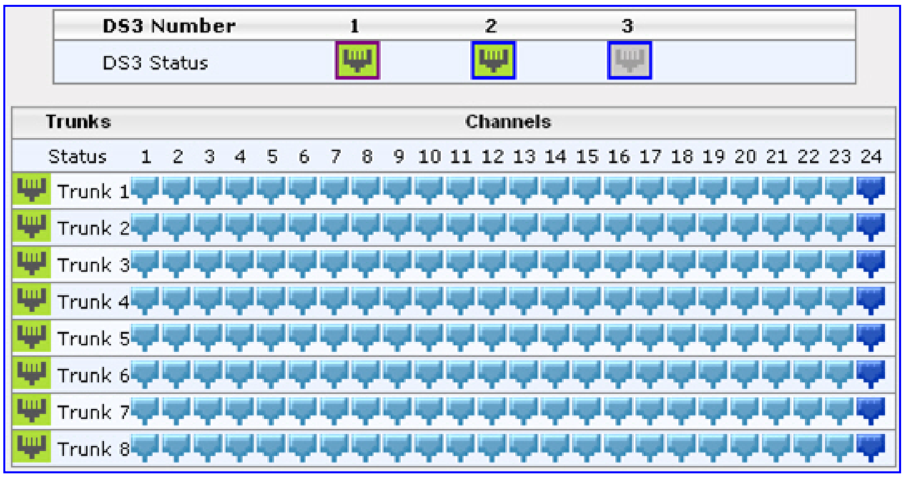
5.10.3.1 Viewing Trunk and Channel Status

The Trunks & Channels Status page displays the status of the device's trunks and corresponding channels. It also enables you to view trunk configuration and channel information.

➢ **To view the status of the device's trunks and channels:**

1. Open the Trunks & Channels Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **Trunks & Channels Status**). The page displays the first eight trunks and their channels:

Figure 132: Trunk and Channel Status - TP-6310



DS3 Number	1	2	3
DS3 Status	🟩	🟩	⬜

Trunks		Channels																							
Status		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
🟩	Trunk 1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 2	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 3	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 4	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 5	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 6	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 7	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
🟩	Trunk 8	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

The status of the trunks is depicted by color-coded icons, as described in the table below:

Description of Color-Coded Icons for Trunk Status

Icon	Color	Trunk	SDH	DS3
		Label	Description	Description
⬜	Gray	Disabled	Disabled	Disabled
🟩	Green	Active - OK	No Alarms (Working)	No Alarms
🟨	Yellow	RAI Alarm	No Alarms (Protection)	RAI Alarm
🟥	Red	LOS / LOF Alarm	LOS/LOF/MS-AIS/MS-RDI Alarm	LOS/LOF/AIS Alarm
🟦	Blue	AIS Alarm	-	-
🟧	Light Orange	D-Channel Alarm	-	DS3 Not Configured
🟧	Dark Orange	NFAS Alarm	-	-
🟪	Purple	Lower Layer Down (DS3 physical layer is disabled)	-	-

The status of the channels is depicted by color-coded icons, as described in the table below:

Description of Color-Coded Icons for Channel Status

Icon	Color	Label	Description
🟦	Light blue	Inactive	Channel is configured, but currently has no calls
🟩	Green	Active	Call in progress (RTP traffic) and no alarms
⬜	Gray	Non Voice	Channel is not configured
🟦	Blue	ISDN Signaling	Channel is configured as a D-channel
🟨	Yellow	CAS Blocked	-
🟧	Dark Orange	Maintenance	B-channel has been intentionally taken out of service due to maintenance
🟥	Red	Out Of Service	B-channel is out of service

To display a page with a summary of parameter information relevant to a channel, click on the channel. For more information, refer to Channel Status Screens.

5.10.3.2 Viewing NFAS Groups and D-Channel Status

The NFAS Group & D-Channel Status page displays the status of the device's D-channels and NFAS groups. The status of a D-channel and NFAS group can be "In Service" or "Out of Service". This page also indicates whether the D-channel is a primary or backup D-channel.

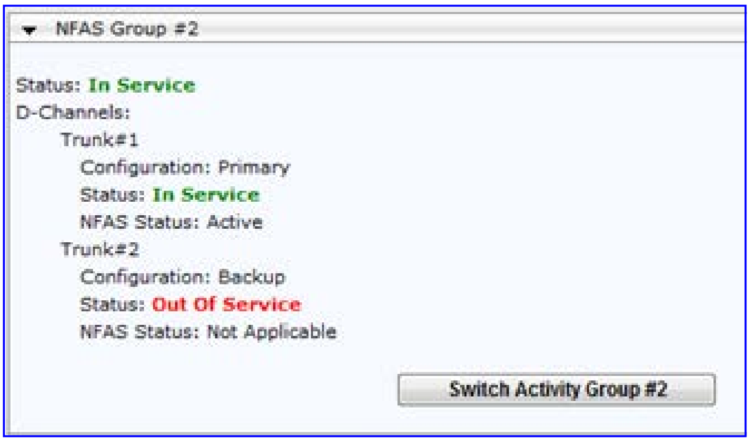
This page also enables you to manually switchover between active and standby D-channels belonging to the same NFAS group. This is done using the Switch Activity button.

⚠ **Note:** This page is applicable only to T1 ISDN protocols supporting NFAS, and only if the NFAS group is configured with two D-channels.

➢ **To view the status of the D-channels and NFAS groups:**

- Open the NFAS Group & D-Channel Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **NFAS Group & D-Channel Status**).

Figure 133: NFAS Group & D-Channel Status Page



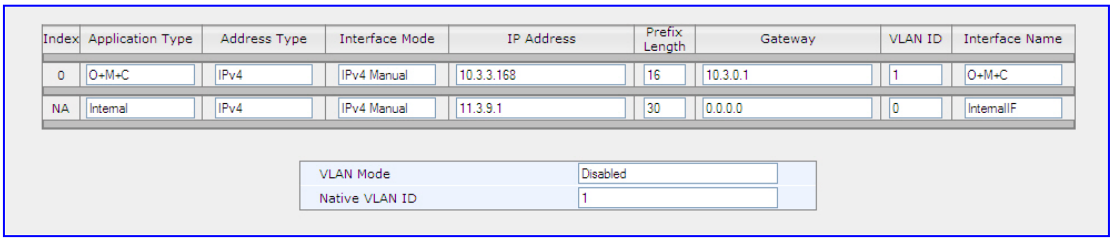
Status: In Service
D-Channels:
Trunk#1
Configuration: Primary
Status: In Service
NFAS Status: Active
Trunk#2
Configuration: Backup
Status: Out Of Service
NFAS Status: Not Applicable

5.10.3.3 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 134: 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:

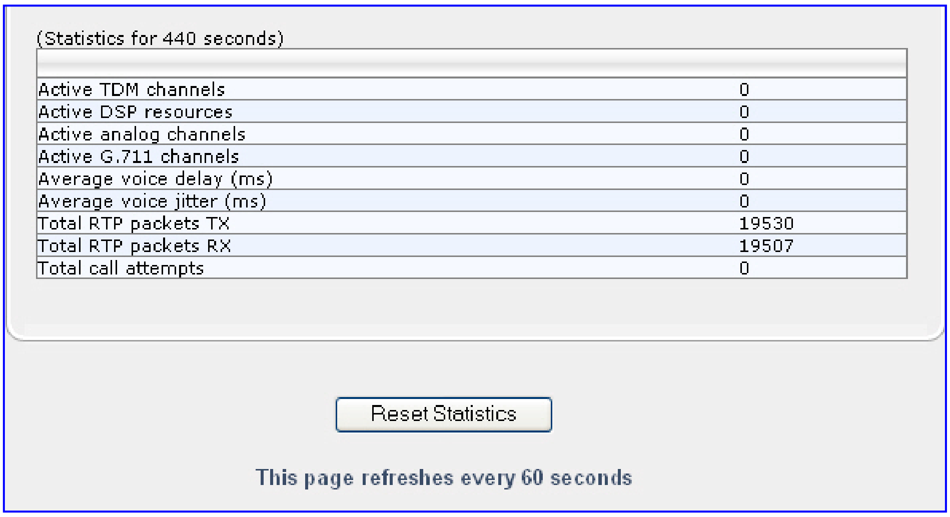
- Every entry represents an interface index.
- The IP Interface Status page is relevant only when the Multiple Interfaces Table is configured.
- On IPv6 interfaces, the link-local address is displayed below the global address. It is prefixed by '*' to indicate that it is a link-local address. Additionally, 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).

5.10.3.4 Performance Statistics

➢ **To display the Performance Statistics page:**

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

Figure 135: Performance Statistics



(Statistics for 440 seconds)

Active TDM channels	0
Active DSP resources	0
Active analog channels	0
Active G.711 channels	0
Average voice delay (ms)	0
Average voice jitter (ms)	0
Total RTP packets TX	19530
Total RTP packets RX	19507
Total call attempts	0

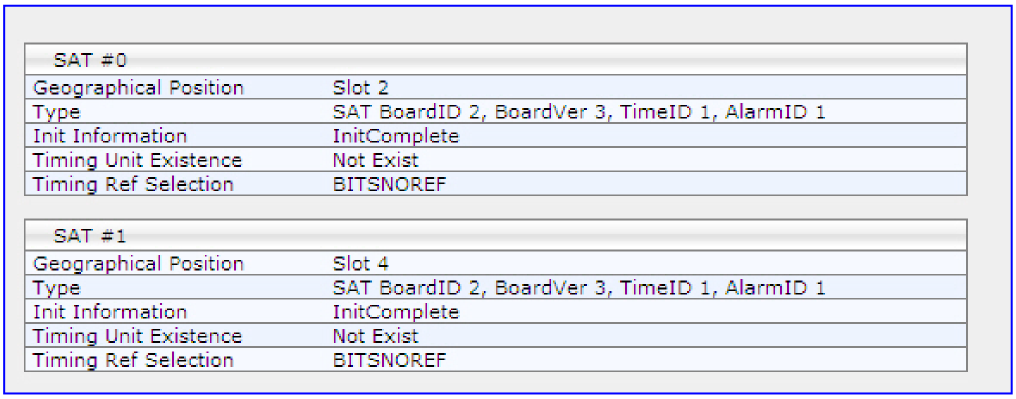
This page refreshes every 60 seconds

5.10.3.5 Timing Module Information

➢ **To display Timing Module Information:**

- Open the Timing Module Information page (**Status & Diagnostics** tab > **VoIP Status** menu > **Timing Module Information**).

Figure 136: Timing Module Information



SAT #0	
Geographical Position	Slot 2
Type	SAT BoardID 2, BoardVer 3, TimeID 1, AlarmID 1
Init Information	InitComplete
Timing Unit Existence	Not Exist
Timing Ref Selection	BITSNOREF

SAT #1	
Geographical Position	Slot 4
Type	SAT BoardID 2, BoardVer 3, TimeID 1, AlarmID 1
Init Information	InitComplete
Timing Unit Existence	Not Exist
Timing Ref Selection	BITSNOREF

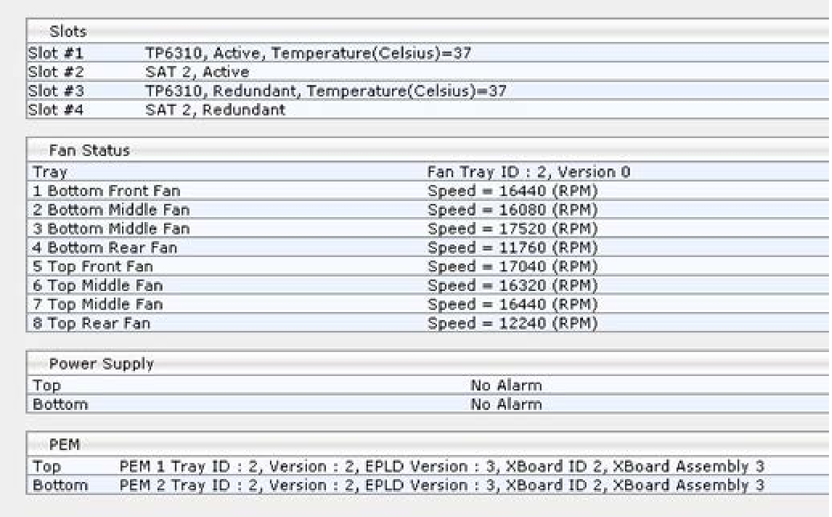
5.10.4 Components Status

The Components Status displays in real-time, the status of each slot (containing either boards or SA cards), Fans, Power Supplies and PEMs.

➢ **To display Components Status:**

- Open the Components Status page (**Status & Diagnostics** tab > **System Status** menu > **Components Status**).

Figure 137: TP-6310 Components Status



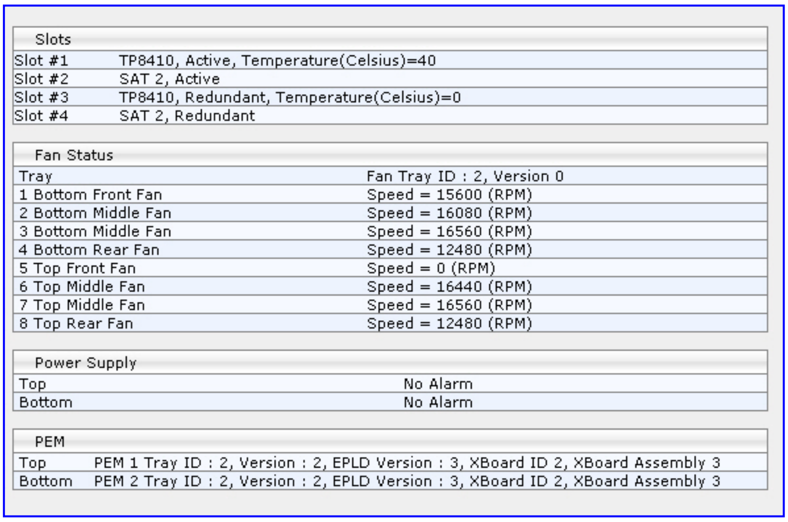
Slots	
Slot #1	TP6310, Active, Temperature(Celsius)=37
Slot #2	SAT 2, Active
Slot #3	TP6310, Redundant, Temperature(Celsius)=37
Slot #4	SAT 2, Redundant

Fan Status	
Tray	Fan Tray ID : 2, Version 0
1 Bottom Front Fan	Speed = 16440 (RPM)
2 Bottom Middle Fan	Speed = 16080 (RPM)
3 Bottom Middle Fan	Speed = 17520 (RPM)
4 Bottom Rear Fan	Speed = 11760 (RPM)
5 Top Front Fan	Speed = 17040 (RPM)
6 Top Middle Fan	Speed = 16320 (RPM)
7 Top Middle Fan	Speed = 16440 (RPM)
8 Top Rear Fan	Speed = 12240 (RPM)

Power Supply	
Top	No Alarm
Bottom	No Alarm

PEM	
Top	PEM 1 Tray ID : 2, Version : 2, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3
Bottom	PEM 2 Tray ID : 2, Version : 2, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3

Figure 138: TP-8410 Components Status



Slots	
Slot #1	TP8410, Active, Temperature(Celsius)=40
Slot #2	SAT 2, Active
Slot #3	TP8410, Redundant, Temperature(Celsius)=0
Slot #4	SAT 2, Redundant

Fan Status	
Tray	Fan Tray ID : 2, Version 0
1 Bottom Front Fan	Speed = 15600 (RPM)
2 Bottom Middle Fan	Speed = 16080 (RPM)
3 Bottom Middle Fan	Speed = 16560 (RPM)
4 Bottom Rear Fan	Speed = 12480 (RPM)
5 Top Front Fan	Speed = 0 (RPM)
6 Top Middle Fan	Speed = 16440 (RPM)
7 Top Middle Fan	Speed = 16560 (RPM)
8 Top Rear Fan	Speed = 12480 (RPM)

Power Supply	
Top	No Alarm
Bottom	No Alarm

PEM	
Top	PEM 1 Tray ID : 2, Version : 2, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3
Bottom	PEM 2 Tray ID : 2, Version : 2, EPLD Version : 3, XBoard ID 2, XBoard Assembly 3

5.11 Device High Availability Mode

Note: The following two bullets are only applicable to the Mediant 3000 devices.

- During the time when the Active blade synchronizes the Redundant blade’s configuration (while the Active and Redundant blades are inter-connected), all configuration changes are blocked until the system is moved to high availability mode, (examples of blocked actions are setting blade parameters and uploading files). The duration of this blocked state is up to several minutes.
- For Feature key updating, uploading the Feature key file must include the Feature key for both blades. If the redundant blade Feature key is missing or invalid the system is moved to mismatch configuration mode alerted by SNMP.

This page is intentionally left blank.

6 Troubleshooting

6.1 TP-6310 Self-Test

The device self-test capabilities are used to identify faulty hardware components on startup and during run time.

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_CPU_SPEED
    - BIT_ELEMENT_ID_TSA_PCM
    - BIT_ELEMENT_ID_PSTN_FRAMERS
    - BIT_ELEMENT_ID_DSP_CHANNEL
    - BIT_ELEMENT_ID_FPGA
    - BIT_ELEMENT_ID_GB_ETHERNET
    - 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 failure in initializing hardware components or a malfunction on running hardware components. If an error is detected, an error message is sent to the Syslog, TPNC 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
    - BIT_ELEMENT_ID_GB_ETHERNET
    - BIT_ELEMENT_ID_FPGA
    - BIT_ELEMENT_ID_VOICE_PATH_CONFIRM (on redundant board only)
- User-initiated tests (Detailed) - The Detailed test is initiated by the user when the platform is offline (i.e., it is 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 consists 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_TPM_UTOPIA_BRIDGE (enable diagnostics 2)

6.2 TP-8410 Self-Test

The device self-test capabilities are used to identify faulty hardware components on startup and during run time.
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_CPU_SPEED
- BIT_ELEMENT_ID_TSA_PCM
- BIT_ELEMENT_ID_DSP_CHANNEL
- BIT_ELEMENT_ID_FPGA
- 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 failure in initializing hardware components or a malfunction on running hardware components. If an error is detected, an error message is sent to the Syslog, TPNC event and SNMP trap. This phase consists of the following tests:

- BIT_ELEMENT_ID_TSA_PCM
- BIT_ELEMENT_ID_DSP_CHANNEL
- BIT_ELEMENT_ID_GB_ETHERNET
- BIT_ELEMENT_ID_FPGA
- BIT_ELEMENT_ID_VOICE_PATH_CONFIRM (on redundant blade only)

User-initiated tests (Detailed) - The Detailed test is initiated by the user when the platform is offline (i.e., it is 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 consists 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_TPM_UTOPIA_BRIDGE (enable diagnostics 2)

7 Technical Specifications

7.1 Mediant 3000 with TP-6310/TP-8410 Technical Specification

Mediant 3000 with TP-6310/TP-8410 Technical Specifications

Item	Characteristic
Channel Capacity	
Network Ports/DSP Calls (independent digital voice, fax or data ports)	▪ Up to 2016 simultaneous PSTN-to-IP calls ▪ Up to 1008 simultaneous IP-to-IP calls All media processing ports can be tied to IP-RTP, PSTN-DS0 Note: When using some coders channel capacity may be reduced for specific functions.
DSP Channel Configuration Options	▪ 2016 Universal ports
IP-to-IP RTP Forwarding	
Max RTP packet payload size	1000 bytes
Max RTP payload bit rate on a single session	384 kbps
Average RTP payload bit rate on full capacity	200 kbps
Voice Messaging	
Playback from Local Storage	▪ Voice Prompts (VP) and announcements playback: ▪ 10 MB integral memory of G.711 recorded prompts
Voice Coders	
Voice Compression (Independent dynamic vocoder selection per channel)	Wireline: ▪ G.711, PCM, 64 kbps (µ-law/A-law), G.722 (48, 56, 64 kbps) ▪ G.723.1 MP-MLQ, 6.3 kbps ACELP, 5.3 kbps ▪ G.729A CS-ACELP, 8.0 kbps ▪ Enhanced G.711, iLBC ▪ Microsoft RTA (Narrow Band) ▪ Wireless-UMTS: GSM-FR, GSM-EFR, MS-GSM and AMR (all rates), AMR WB ▪ Wireless-CDMA: EVRC, EVRC B (4GV)
Media Processing	
IP Transport	VoIP (RTP/ RTCP) per IETF RFC 3550 and RFC 3551
DTMF/MF Transport	DTMF/MF RTP Relay per RFC 4733, Mute, Transparent (transfer in coder as voice).
Echo Cancellation	G.165 and G.168 2000 with default 128 msec tail length (also configurable to 32 and 64 msec)

Mediant 3000 with TP-6310/TP-8410 Technical Specifications

Item	Characteristic
Fax Modem Relay/ByPass	▪ T.38 (IP) versions 0 & 3 fax relay for both T.30 & V.34 fax transport. ▪ Fax-bypass (switch to G.711) support ▪ Modem Bypass (incl.V.90)
In-band/Out-of-band Signaling	Packet side, DTMF and tone detection and generation
DTMF & Tone Signaling	DTMF detection and generation per TIA 464B
	MF-R1, MFC-R2, detection and generation
	Call progress Tone detection and generation
Gain Control	Programmable
Voice Quality Monitoring	RTCP XR (IETF RFC 3611)
Security	SRTP using AES and ARIA
Silence Suppression	Voice Activity Detection (VAD), Comfort Noise Generation (CNG) (According to standard coder support)
Control Protocols	
MGCP (RFC 3435)	Call control, Basic announcements package
MEGACO (H.248)	Call control, CAS and Basic announcements package and ETSI ES 283 018 I-BGF profile
Management Interfaces	
SNMP v2c, SNMP v3	Standard MIB-2 ALARM-MIB (RFC 3877), DS1-MIB (RFC 2495), DS3-MIB (RFC 3896), ENTITY-MIB (RFC 2737), IF-MIB (RFC 2863), IP-FORWARD (RFC 4292), IP-MIB (RFC 4293), NOTIFICATION-LOG-MIB (RFC 3014), RTCPXR-MIB, RTP-MIB (RFC 2959), SNMP-FRAMEWORK-MIB (RFC 3411), SNMPv2-TC, SONET-MIB (RFC 3592), TCP-MIB (RFC 4022), UDP-MIB (RFC 4113) and many others AudioCodes' proprietary MIBs.
Web Interface	Enabling device configuration and run-time monitoring with an Internet browser via HTTP or HTTPS
Maintenance	▪ Syslog (according to RFC 3164) ▪ Local RS-232 terminal ▪ Telnet / SSH
Signaling	
PSTN Protocols	▪ CAS - T1 robbed bit: WinkStart, delay dial, immediate start, FGB, FGD, etc. ▪ MFC/R2 numerous country variants ▪ Unique script for each country variant, enabling maximum flexibility of the entire state machine of each CAS protocol. ▪ CCS - ISDN PRI: ETSI EURO ISDN, ANSI NI2, DMS, 5ESS, Japan INS1500, QSIG Basic Call, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean MIC, France Telecom
High Availability	

Mediant 3000 with TP-6310/TP-8410 Technical Specifications

Item	Characteristic
1+1 System Setup	System is occupied with 2 blades, one is active in working mode and the other is redundant in "standby" mode.
Processor	
Control Processor	Motorola PowerQUICC 8280
Control Processor Memory	2016 channels: SDRAM - 512 MB
Signal Processors	AudioCodes AC491 VoIP DSP @ 300 MHz
Interfaces of Mediant 3000 with TP-6310	
Gigabit Ethernet (GbE)	1+1 redundant 10/100/1000 Base-TX ports Interface options: 10/100/1000 Base-TX: RJ-45 Connector Interface (CAT5 Twisted pair) or 10/100/1000 Based-RX: 1.25 Gbps optical SFP modules - Hot Swappable
OC-3/STM-1 PSTN	▪ 1+1 APS Redundancy ▪ 155.54 Mbps optical SFP modules; Hot Swappable ▪ Wavelength: 1310 nm Single-mode Transceiver
DS3 PSTN	▪ Three MiniSMB DS3 interfaces ▪ 44.736 Mbps signal ▪ 75 Ohm Coax
Interfaces of Mediant 3000 with TP-8410	
Gigabit Ethernet (GbE)	Four 10/100 Base-T: RJ-45 Connector Interface 1+1 redundant 10/100/1000 Base-TX ports Interface options: 10/100/1000 Base-TX: RJ-45 Connector Interface (CAT5 Twisted pair) or 10/100/1000 Based-SX: 1.25 Gbps optical SFP modules - Hot Swappable
PSTN Interfaces	E1/T1
Power	
AC Power Input	Power input range 100 to 240 VAC at a nominal 50/60 Hz line frequency.
AC Power Supply Voltages and Power Consumption (Typical)	Depends on installed blades and configuration: Configuration Power ▪ TP-8410 HA 63 E1/84 T1 3.3A @ 110VAC, 336W 1.6A @ 230VAC, 336W ▪ TP-8410 Simplex 63 E1/84 T1 2.1A @ 110VAC, 230W 1A @ 230VAC, 230W ▪ TP-8410 HA 16 E1/ 21 T1 2.1A@110V 230W 1A@230V, 230W

Mediant 3000 with TP-6310/TP-8410 Technical Specifications

Item	Characteristic
	▪ TP-8410 Simplex 16 E1/ 21 T1 1.5A@110V, 162W 0.7A@230V, 162W ▪ TP-6310 HA OC-3/STM-1 3.4A @ 110VAC, 373W 1.6A @ 230VAC, 373W ▪ TP-6310 Simplex OC-3/STM-1 2.1A @ 110VAC, 235W 1A @ 230VAC, 235W
DC Power Input	Power input range 40 to 60 VDC
DC Power Supply Voltages and Power Consumption (Typical)	Depends on installed blades and configuration: Configuration Power TP-8410 HA 63 E1/84 T1 7A @ 48 VDC, 336W TP-8410 Simplex 63 E1/84 T1 4.4A @ 48 VDC,211W TP-8410 HA 16 E1/ 21 T1 4.4A @ 48 VDC, 211W TP-8410 Simplex 16 E1/ 21 T1 3.1A @ 48 VDC, 150W TP-6310 HA OC-3/STM-1 7.1A @ 48 VDC, 343W TP-6310 Simplex OC-3/STM-1 4.5A @ 48 VDC, 216W
Physical	
Environmental	Humidity: 10 to 90% non-condensing
Hot Swap	▪ Full cPCI hot swap supported for media processing boards according to PICMG 2.1 ▪ Redundant Power Supplies provide protection but are non-Hot Swappable
Enclosure Dimensions	▪ 2U high, 19-inch wide rack mount, shelf or desk top, 4-slot cPCI chassis ▪ 8.8 x 48.26 x 29.68 cm ; 3.5 x19 x 11.87 inch (h x w x d) including mounting brackets ▪ cPCI chassis PICMG 2,0 R2.1 cPCI ▪ 2 middle mounting brackets - Optional
Weight	Total including packaging 12.2 KG; 5.6 lbs.
Rear Panel	
STM-1/OC-3 Interface (with TP-6310 only)	Two fiber optical 155.54-Mbps SFP modules (1+1 redundancy). The SFP modules accept twin single-mode fiber optic cables terminated with LC-type connectors (not supplied).
T3 Interface (with TP-6310 only)	Three SMB Tx/Rx connector pairs - receives RG-179/U coaxial cables terminated with 75-ohm male SMB connectors (not supplied).
E1/T1 Interface (with TP-8410 only)	Two 100-pin SCSI connectors for Trunks 1-25 and 43-67. Two 68-pin SCSI connectors for Trunks 26-42 and 68-84.
Gigabit Ethernet (GbE)	Two (1+1 redundancy) Gigabit Ethernet ports, full-duplex mode with auto-negotiation, available in one of the following (by customer ordered): 10/100/1000Base-TX RJ-45 connector interface (CAT 5 twisted pair) 10/100/1000Base-RX 1.25 Gbps optical SFP modules (Hot swappable)

Mediant 3000 with TP-6310/TP-8410 Technical Specifications

Item	Characteristic
ESD Connectors	ESD connectors
Alarm Terminal Block Closures	Connection mate (on PEM module) of type FK-MC 0.5/8-ST-2,5 Phoenix Contact
BITS/SETS	RJ-48 connector (on the PEM module)
AC Power	3-Prong IEC 60320 type AC power inlet on the PEM module.
DC Power	Two available connection types (on PEM module): ▪ 2-pin terminal block screw connection type, suitable for up to 10 AWG field wiring applications connecting DC Power connector: MSTB2.5/2-STF (5.08 mm) from Phoenix Contact. Cable connection mate: PC4/2-STF-7,62 (AudioCodes supplied) ▪ 2-pin terminal block crimp connection type, supplied with 14-16 AWG cable crimped to connector. [2 x crimp terminal female 10 AWG (Phoenix P/N: STG-MTN 1,5-2,5) and 1x terminal block shroud FML 7.62mm 2 POLE CBL MNT (Phoenix female P/N: STG-MTN 1,5-2,5)]
Front Panel	
Hardware Reset Button	Push button for resetting to default settings
RS-232	3-pin connector on blade for RS-232 serial configuration (DB9 to 3-pin cable adapter supplied)
Fiber Optic Cable	
PSTN (SDH) - Single-mode Fiber	▪ Input Sensitivity: -32 dBm typical; -28 dBm maximum ▪ Output Power: -15 dBm minimum; -8 dBm maximum
LAN (GbE) - Multi-mode	▪ Input Sensitivity: -29 dBm typical; -17 dBm maximum ▪ Output Power: -9.5 dBm minimum; -2 dBm maximum
Diagnostics	
Front panel LEDs	Provide visual status indications and alarms - on PEMs, TP-6310 boards, Power Supplies, Fan Tray
Syslog events	Supported by Syslog servers
Regulatory Compliance	
Telecommunications Standards	FCC part 68, TBR4 and TBR13
Safety and EMC Standards	UL 60950-1 FCC part 15 Class A CE mark (EN 55022 Class B, EN 60950-1, EN 55024, EN 300 386)
Environmental	Complies with NEBS Level 3 GR-63-Core, GR-1089-Core, Type 1&3, ETS 300 019 (Future Implementation)

This page is intentionally left blank.

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 □-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

List of Abbreviations

Abbreviation	Meaning
GK	Gatekeeper
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

List of Abbreviations

Abbreviation	Meaning
MIB	Management Information Base
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.

List of Abbreviations

Abbreviation	Meaning
TCP/IP	Transmission Control Protocol/Internet Protocol.
TFTP	Trivial File Transfer Protocol.
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
□law	American Compander Functionality Rule, (see A-law)
µs or µsec	microsecond; a millionth part of a second

9 Index

A

Abort Procedure 151
Accessing the Web Interface.........................45
Actions upon Detecting Blade Failure 40
Active IP Interfaces...............................161, 170
Advanced Configuration 140
AMR Policy Management 122, 126
Application Settings 74
Assigning an IP Address Using BootP 21, 22
Assigning an IP Address Using HTTP...........21
Assigning the Device IP Address 15, 21
Assigning the IP Addresses for High Availability Mode 23, 39
Automatic Update Facility........................28, 34
Auxiliary Files 33

B

Backing up the Current Software Upgrade Key 148, 151
Backup Copies of ini and Auxiliary Files 37
Binary Configuration File Download 33
Boot Firmware & Operational Firmware 25

C

Call Control 136
Carrier-Grade Alarms 163
CAS State Machines 113, 120
Certificates...77
Channel Configuration 139
Clock Settings..104
Configuration 43, 74
Configuration File 146, 157
Configuration Parameters and Files........25, 28
Configuration Using the Web Interface ..21, 28, 43
Configuring Trunk Settings 113
Control Interface Settings 136

D

Device High Availability Mode 173
Device Information.......................148, 161, 162
Device Initialization Process..........................39
Disabling the Web Interface 44
DNS 101
Downloading Auxiliary Files via TFTP During the Blade Startup 34
DSP Templates 122, 125

E

Encoding Mechanism 33
Encrypted HTTP Transport (HTTPS - SSL) ..44
Ethernet Port Information 161, 163

F

Fax/Modem/CID Settings................... 122, 123
Firewall Settings.. 108
Functional Block Diagram - TP-6310............ 16
Functional Block Diagram - TP-8410............ 17

G

General Features 11
General Media Settings 122, 124
General Security Settings 108, 110
Getting Acquainted with the Web Interface . 43, 47, 52
Getting Started....................................... 19, 21
Global Parameters 113

H

High Availability................................ 10, 13, 39
High Availability Maintenance............... 48, 145
Hitless Software Upgrade 40
How to Switch out of Multiple IP's with Network Physical Separation.................................. 97

I

Initial Device Configuration using the Web Interface 44
Initialization (ini) File 28
Installing the Software Package 19
Installing/Unzipping When Using a Windows™ Operating System.................................... 19
Introduction 9
IP Sec Associations Table 108, 112
IP Sec Proposal Table 108, 111
IP Settings...................................... 91, 96, 97
IPMedia Settings................................ 122, 124

L

Limiting the Web Interface to Read-Only Mode 43
Limiting Web Access to a Predefined List of Client IP Addresses.................................. 44
List of Abbreviations.................................. 183
Load Auxiliary Files...................... 43, 146, 147
Loading the Software Upgrade Key.... 148, 151
Loading the Software Upgrade Key Using BootP/TFTP.................................... 149, 150
Logging Off the Web Interface................ 48, 65

M

Maintenance 142
Management 78
Managing Web Server Access Using a RADIUS Server 44
Media 122
Media Quality of Experience...................... 134
Media Security 122, 133
Media Services - MEGACO Only................ 141

Mediant 3000 with TP-6310/TP-8410
  Technical Specification 177
Message Log 161

N

Network Settings 91, 100

P

Performance Monitoring 165
Performance Statistics.........................161, 171
Protocol Selection.......................................136
PSTN 113

Q

QoS Settings 91, 99

R

RADIUS Settings 78, 87
Regional Settings 76
RTP/RTCP Settings............................122, 123

S

SCTP Settings 91, 100
Searching for Configuration Parameters .47, 55
Security Settings..108
SNMP 78, 88
SNMP Community String.........................78, 88
SNMP Trap Destinations 78, 89
SNMP Trusted Managers 78, 89
SNMP V3 Users 78, 90
Software Directory Contents & Structure 19, 20
Software Package 19
Software Update.................................142, 146
Software Upgrade Key 38, 39, 146, 148
Software Upgrade Wizard 43, 146, 151
Special System Specific Behavior 39
Startup Process 26
Status and Diagnostic Menu..................43, 161
Switching into/out of Multiple IP’s and Network
  Physical Separation configuration. 95
Syslog Settings...76
System..74
System Initialization Process...................21, 25
System Status 161

T

Tables of Parameter Value Structure 28, 31
TDM & Timing..102
Technical Specifications 177
Telnet/SSH Settings 78, 86
Timing Module Information..................161, 171
TP-6310 Self-Test 175
TP-8410 Self-Test 176
Transmission Settings - DS3.......................116
Transmission Settings - SONET/SDH - For TP-
  6310 Only...113, 118
Troubleshooting..175
Troubleshooting an Unsuccessful Loading of a
  License Key... 151

U

Upgrading Device Software 33, 38
Using Internet Explorer to Access the Web
  Interface 46
Using Network Physical Separation - TP-8410
  Only 95
Using the Home Page............................ 66, 72

V

V5.2 Configuration (For TP-8410 Only)...... 141
Verifying that the Key was Successfully
  Loaded 151
Viewing Active Alarms 161, 163
Viewing MOS per Media Realm.......... 161, 166
Viewing NFAS Groups and D-Channel Status
  169
Viewing Trunk and Channel Status 161, 168
Viewing Trunk Utilization 161, 165
Voice Settings 122
VoIP 91
VoIP Status 168

W

Web & Telnet Access List............... 78, 86, 109
Web Security Settings 78, 81, 84, 85

This page is intentionally left blank.

User's Manual

www.audiocodes.com