AudioCodes™ Media Gateway

Mediant 5000™

Product Description

Version 6.6

Document # LTRT-92520

AudioCodes

Contents

List of Figures

List of Tables

Reader's Notes

Notice

This manual describes the product features and components of the Mediant 5000.

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 can be viewed by registered customers at. www.audiocodes.com/downloads

This document is subject to change without notice.

Date Published: 24/9/2012

Trademarks

Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

WEE 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.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number.

Related Documentation

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

- **Mediant 5000 Product Description** - contains the description of the product features, components, standard control protocols and management protocols (*Document # LTRT-922xx*).
- **Mediant 5000 Installation, Operation & Maintenance Manual** - Provides steps and information for preparing the area where the equipment is to be set-up, supplies instructions on the physical and electrical installation of a chassis and includes operation instructions and maintenance guidelines/troubleshooting procedures. It is intended for skilled installers, system level technicians and system managers (*Document # LTRT-923xx*).
- **CLI Reference Guide** - Provides a predefined set of commands with a choice of options that comprehensively cover the maintenance tasks required on the media gateway*(Document # LTRT-892xx)*
- **Programmer's User's Manual** - The Programmer's User's Manual is written for System Integrators and Software Developers who need to quickly and easily develop an efficient Network solution, with the Mediant 5000 Media Gateway. (*Document # LTRT-914xx*).
- **EMS User's Manual** - The EMS (Element Management System) is an application that is used to configure and monitor all gateway elements from a remote location. Through the EMS, the system operator can also configure the Mediant 5000 to send EMS and Gateway alarms to different destinations using various filtering rules. The manual is intended for System level operators who are to use the EMS. The EMS can also be connected to an NMS (*Document # LTRT-963xx).*
- **Mediant 5000 and Mediant 8000 Alarm and Performance Monitoring Guide** - *Document # LTRT-237xxx*
- **Mediant 5000/8000 Media Gateway Release Notes** - *Document # LTRT-@@Release Notes doc#*
- **EMS Release Notes** - *Document # LTRT-912xx*

Open Source Software

The Mediant 5000 product may contain open source software that may be governed by and distributed under open source licenses, including, but not limited to, the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), BSD and other licenses.

To receive the relevant source code, refer to 'http://www.audiocodes.com/open-source' 'http://www.audiocodes.com/open-source'.

1 Introduction

The Gate**way** is a high channel density, Medium sized version of the AudioCodes series of market-ready, standards-compliant, VoIP, wireless, cables and wireline media gate**way** systems. The Mediant 5000 incorporates AudioCodes' leading Voice over Packet technology to enable Network Equipment Providers (NEP) and System Integrators rapid time-to-market and reliable cost-effective deployment of next-generation networks.

The Mediant 5000 is a robust, scalable and modular solution, designed for the medium to large enterprise environment, matching the density requirements for Medium deployments, while meeting Network Service Providers' demands for high available and reliable new voice infrastructure networks. For maximum reliability, the Mediant 5000 features protection switching and full redundancy of all common equipment.

1.1 General Features

The Mediant 5000 offers a comprehensive system containing the following General Networking Functionality features:

- Up to 3 Dual STM-1/OC-3 (replaceable Dual-LC-type optical connectors) towards the SDH/SONET PSTN backbone
- Up to 9 T3 Interfaces
- Integrated Automatic Protection Switching (APS) for SONET/SDH interfaces
- Up to 126 E1/T1 Interfaces
- MGCP, TGCP (PacketCable standard), MEGACO (H.248) and SIP media gateway control protocol
- Vocoder configuration options: PCM, G.723, G.729A, G.729E, iLBC, G.727, G.726, NetCoder, GSM FR, GSM EFR, QCELP 8/13 kbps, AMR (all 8 rates), EVRC, MS RTA – NB/WB.
- DTMF and Tone Detection and Generation according to TIA 464B
- DTMF Relay according to RFC 2833
- Real-time Fax over IP/T.38 with superior performance (round trip delay up to 9 sec)
- Integral Announcement support towards PSTN/TDM and IP
- G.168-2000 compliant Echo Cancelation with a 32, 64 or 128 msec tail (128 msec with reduced channel density)
- Silence Suppression supporting VAD (Voice Activity Detection) and CNG (Comfort Noise Generation)
- Up to 3 different IP Uplinks, supporting VLANs per IEEE 802.1q&p, different local Subnets and Diffserv rating per RFC 2474
- On-board, dual redundant Ethernet Switches, each with up to 3 Gigabit aggregated GbE electrical interfaces (Ethernet redundancy) from 5 external Ethernet port interfaces
- High availability with redundancy for all hardware modules.

- Full system security, supporting IPSec with pre-shared Key, SSH, SSL Security technology including Authentication, Confidentiality, Integrity and Access Control on system Interfaces.
- Complete gateway solution, designed for the medium to large enterprise environment
- Remote Online Software Upgrade

1.2 PSTN Signaling Features

The Mediant 5000 offers a comprehensive system containing the following PSTN Signaling features:

- PSTN protocol termination support
- PSTN Signaling: CAS, MelCAS, ISDN PRI, DPNSS and SS7 layer 3 termination
- SIGTRAN IUA, DUA, M2UA, M3UA over SCTP
- MF-R1, MFC-R2 and Call Progress Tone detection and generation
- M2UA / SigTran Narrow-band Interworking: Termination of MTP-1, MTP-2, layers and delivery of MTP3 messages over M2UA / SCTP / IP transport to a centralized MSC Server / Signaling Gateway
- M3UA / SigTran Narrow-band Interworking: Termination of all layers up to MTP3 layer and delivery of SCCP/ISUP messages over M3UA/SCTP/IP to a centralized MSC Server / Signaling Gateway Controller
- SS7 / Narrow-band Signaling Node, providing SP routing functionality
- SS7/MTP2 tunneling over IP backbone

1.3 3GPP Functionality

The Mediant 5000 offers a comprehensive system containing the following 3GPP IMS IM-MGW features:

- Flexible Core Network deployment options; able to interconnect to TDM and IP networks
- Mn interface - IMS Call Control, H.248 as per relevant sections of 3GPP TS 29.332
- VAD (per 3GPP 26.094)
- Silence Suppression and CNG (per 3GPP 26.092)
- GSM/UMTS/CDMA Vocoders: GSM-FR, GSM-EFR, AMR (all 8 rates), AMR2, EVRC, EVRC TTY, EVRC-B, QCELP, G.711; selection on a channel-by-channel basis

1.4 Cable Functionality (PacketCable 1.0)

The Mediant 5000 offers a comprehensive system containing the following PacketCable features:

- Supporting Media Gateway functionality per PacketCable 1.0 Architecture Framework Technical Report (PKT-TR-Arch)
- TGCP - CMS/MGC Call Control, MGCP per relevant sections of PKT-SP-TGCP
- PacketCable Vocoders: G.711 (A-law/μ–law), G.729E, iLBC, supporting PKT-SP-Codec
- Call Control Security, supporting IPSec with pre-shared Key, per relevant sections of PKT-SP-SEC
- Electronic Surveillance per relevant sections of PKT-SP-ESP

1.5 System Management Functionality

The Mediant 8000 offers a comprehensive system containing the following System Management features:

- Complete gateway solution, designed for the carrier environment
- High-availability implementation consisting of redundant modules, common modules with load-sharing and active/standby redundancy schemes and based on reliable design, intelligent switchover procedures, preventative self-testing, fault detection and fault isolation, supportive maintenance.
- OAM Single point of access via the System Controller; efficient precise management and provisioning with AudioCodes EMS and SNMP-based North Bound interface.
  - **Fault Management** - Monitors all hardware elements of the system: fans, power supplies, and boards. System status is provided through SNMP to the EMS and viewed on status screens.
  - **Configuration** - The software package, as well as full configuration of the chassis is maintained on the System Controller. The Media Gateway is provisioned by the EMS through SNMP. In addition, on-line software upgrade is supported.
  - **Performance Monitoring** - Performance Monitoring information is gathered from all boards and is retrieved via SNMP to the EMS. The information is gathered either in real-time or in the background (15 min. interval).
  - **Security** - OAM and Call Control interfaces are secured by IPSec, IKE and IP separation. Security is imposed through other means as well.
- **CLI** - command line interface at the System Controller which allows provisioning, status and debugging of the system in cases where EMS is disconnected from the Media gateway.
- Automatic and Manual Hardware and Software Diagnostic, BIT (Built in Test) fault detection, heart beat, chassis sub-systems monitoring.
- Line timing or external timing synchronization from any BITS/TSG/SSU/SETS clock source release.

- **Syslog event reporting** (according to RFC 3164) or local logfile accumulation of all Media Gateway boards fault/error events.
- **Remote Online software upgrade** - provides an efficient way to upgrade software versions on live systems running at remote field sites. Upgrade is accomplished without switching off the live traffic running through the system.
- Comprehensive EMS with NMS Northbound interface to operate and manage the Media gateway.
- Optimized for OEM customers

1.6 Hardware Platform Functionality

The Mediant 5000 offers a comprehensive system containing the following Hardware Platform features:

- Optimal, cost-effective channel density
- Small footprint
- Open platform, designed for the carrier environment
- Hot swap removal and insertion of all system elements
- Modular hardware expandability “pay-as-you-grow” system
  - Redundant power supply modules AC or DC
- Chassis health monitoring and recovery
- Supports the family of AudioCodes Media Gateway boards

1.7 Performance Highlights

- **Cost-effective Media Gateway**

  The Mediant 5000 VoIP Media Gateway matches the density requirements for Medium -sized deployments, while meeting Network Service Providers' demands for reliable new voice infrastructure networks.

- **Delivers New Solutions Faster**

  Immediately address new opportunities in emerging markets with the most flexible, large mid-size customizable solution available. The Mediant 5000 VoIP Gateway system's standards-based control interfaces, protocols, and open architecture ensure easy integration with new products and services.

- **Multiservice Media Gateway**

  The Mediant 5000 VoIP Gateway system enables operators to immediately address opportunities that utilize a myriad of legacy circuit-switched infrastructure features and functionality. The Mediant has a wide coverage when it comes to support for regional PSTN interfaces, voice coder options, signaling and control protocols.

- **Benefit From Extensive Gateway Experience**

  AudioCodes is one of the world's leaders in providing packet-enabled new voice infrastructure network technologies. AudioCodes' commitment to innovation yields consistently high-quality voice processing products that are flexible, intelligent and comprehensive.

  The Mediant 5000 is part of AudioCodes' complete family of VoIP gateway system solutions for new voice infrastructure networks.

- **Wide coverage wireline, wireless and cable applications**

  The Mediant has a wide coverage of applications when it comes to wireline, wireless and cable networks and large enterprise environments. The Mediant supports IP and PSTN interfaces, voice coder options, signaling and control protocols for the above applications, depending on the Mediant configuration.

Reader's Notes

2 Mediant 5000 Basic Feature Highlights

The Mediant 5000 Media Gateway offers a comprehensive system complete with the Voice Packet Processing, High Availability, and PSTN Signaling features essential for wireline, cable and cellular communications environment. Beside the PSTN Signaling features, SS7 Narrow-band & Broad-band Signaling features and 3GPP IMS services which were described in detail in the previous sections, there are Media Gateway basic features like Voice Packet Processing, High Availability and Management features.

The basic features of the Mediant 5000 can be summarized in the following areas:

- Voice Packet Processing
- Gateway Management
- Performance Management
- High Availability
- Clock Synchronization Modes
- Security
- Network Time Protocol (NTP) synchronization
- Remote Online Software Upgrade
- IP to IP Session Border Controller (SBC)

2.1 Voice Packet Processing

The Mediant 5000 provides a feature-rich set of voice-processing services required for its functionality as a media gateway. These services include:

- Echo Cancelation
- Voice and tone signaling discrimination
- Capacity and Voice compression
- Voice activity detection (VAD)
- Comfort noise generation (CNG)
- Tone processing
- AMR coder policy
- Voice, data and fax discrimination

2.1.1 Echo Cancelation

The Mediant 5000 supports Echo Cancelation (32, 64, 128 msec tail adaptive) on each voice channel per G.165 and G.168-2000. The echo cancelation algorithm reduces degradation originating from PSTN interfaces and improves the perceived voice quality.

2.1.2 Voice and Tone Signaling Discrimination

The Mediant 5000 constantly monitors PSTN input bit streams. When voice is detected, the incoming bit stream is forwarded to a speech encoder. When signaling is detected, its bit stream is forwarded to a signaling detector.

2.1.3 Capacity and Voice Compression

For the Mediant 5000 + TP-6310 /STM-1 configuration, the chassis accommodates up to 6,048 simultaneous calls (3+1 boards). A fully populated Mediant 5000 can support up to 3 protected STM-1/OC-3 PSTN links.

For the Mediant 5000 + TP-8410 configuration, the chassis accommodates up to 4 (3+1) TP-8410 Media Gateway boards per chassis, or 3,780 simultaneous calls. The total number of TDM ports supported by the Media gateway depends on the number of Media Gateway boards specified in the configuration of the Gateway. A fully populated Mediant 5000 can support up to 126 E1 / T1 + 42 links reserved to provide backup links.

For the Mediant 5000 + TP-6310 /T3 configuration, the chassis accommodates up to 6,048 simultaneous calls (3+1 boards). Each TP-6310 /T3 board supports 3 T3 interfaces and thus a fully populated Mediant 5000 can support up to 9 T3 Trunks.

The Mediant 5000 currently supports the following voice compression Vocoder algorithms:

- G.729A,B, iLBC, G.723.1, G.727, G.726, G.711, NetCoder
- GSM/UMTS/CDMA Vocoders: GSM-FR, GSM-EFR, AMR (all 8 rates), AMR-WB, EVRC, EVRC-B, G.729.1 (up to 12 kbps), MS GSM, G.722; selection on a channel-by-channel basis
- Microsoft Systems RTAudio – NB/WB.

The Mediant 5000 supports independent dynamic vocoder selection per channel.

IP to IP Transcoding is supported too, including wideband Transcoding. When connecting an IP leg with a G.722 coder to an IP leg with an AMR WB coder, the connection will be made using raw wideband format, maintaining the wideband quality of the originator.

Note: Some coders reduce the channel capacity. The list of required coders should be specified at the time the order is placed.

2.1.4 Voice Activity Detection and Comfort Noise Generation

The Mediant 5000 utilizes the Voice Activity Detection (VAD) mechanism, in which compression is maximized for silence between words, and comfort noise generation (CNG) mechanism, in which spectrum-linked noise at the remote site is reproduced. The VAD mechanism reduces power consumption both at the handset and at the base station.

2.1.5 Voice, Data and Fax Discrimination

The Mediant 5000 currently handles fax and modem transmissions according to standard IETF Fax over IP (FoIP) protocols or via V.152 VBD (Voice Band Data). Constantly monitoring PSTN input bit streams, the Gateway detects voice and forwards it to the Speech Encoder. When signaling is detected, its bit stream is forwarded to the Signaling Detector.

For reducing bandwidth and improving quality, the Mediant 5000 employs the ITU T.38 standard to detect and relay the fax transmissions to a remote gateway over the IP network. Use of fax relay allows fax transmission while using low bit-rate vocoders. Up to 14,400 bps can be supported.

For the UMTS CS Domain, the Mediant 5000 handles Transparent Synchronize Data transmissions for Support of Multimedia transmissions according to 3GPP Circuit Switch Data (CSD) standard (TR 23.910) for 64 kbps UDI and 56 kbps RDI services.

2.1.6 Tone Processing

The Mediant 5000 supports tone processing for VoIP and PSTN networks. Voice band tones are used in the PSTN for various functions such as dialing, indicating the call progress status, etc. The Mediant 5000 detects In Band Signaling (IBS) tones like DTMF, MF-R1, MFC-R2 and PSTN and UMTS Call progress Tones and generates them either toward the "Remote Termination" or into the "Connection/Contexts" over an IP or PSTN network.

User defined Call progress tones and DTMF tones can be detected and generated as well.

2.1.7 AMR Coder Policy

AMR voice coder supports adaptive rate change according to the network performance and voice quality.

The voice quality is determined by measuring the packet loss. When one side of the call detects that the packet loss exceeded a predefined value, it sends (in a special field in the AMR packet called CMR) a command to change the current AMR rate and/or the RTP redundancy. The values of packet loss and hysteresis are according to 3GPP 44.318 standard.

Default Policy Management Rules are defined by EMS and the MGC can change these rules during the call. Using these rules, the MGW changes the AMR vocoder rate and RTP Redundancy depth, based on voice quality degradation.

Note: When AMR coder policy is pre-configured on the Media Gateway board, a similar configuration should be applied to both Media Gateways that participate in the call.

2.2 Gateway Management

Residing on System Controllers (SC) boards, the system controller software manages all of the boards and modules within the system. The software orchestrates all of the boards with their varied functionality into one comprehensive media gateway, providing a single management interface for the whole chassis. This functionality makes the media gateway more self-reliant and hence ensures easier integration with other systems.

Some of the main management tasks performed on the Mediant 5000 chassis are:

- **OAM Single point of access via the System Controller** - Providing easy management and provisioning for all Mediant 5000 blades via standard SNMP Interface.
- **SNMPv2c/SNMPv3 Based Provisioning API** - While the Mediant 5000 is provided together with the EMS, which provides a comprehensive GUI to handle the provisioning tasks, the configuration of the SC board's data base can be changed via Simple Network Management Protocol (SNMP). This standard protocol is the most frequently used for managing Network elements and assures Mediant 5000 's interoperability with any standard network element system. The provisioning API is defined by RFC/ ITU standards, as well as a proprietary Management Information Base (MIB). It allows the provisioning of every parameter existing in the system.
- **Media Gateway Configuration** - Configuration of all boards within the Media Gateway is kept within the System Controller configuration database. The task of the System Controller is to relay the configuration to all the other boards within the system - according the configuration definition entered by the operator via the SNMP.
- **Backdoor Configuration** - The boards' field provisioning contains a formal backdoor for configuring board parameters that are not supported in the EMS. The Backdoor Configuration is preserved during the Online Software Upgrade procedure.
- **Periodically backup** -Automatic System Backup functionality.The SC periodically performs a backup of the configuration database and provides the user with the ability to "revert to specific restore point" (similar to the Windows System Restore functionality). The precise timing and amount of the stored backup data are configurable by users.
- **Online Software Upgrade (Hitless)** - Software Upgrade of all Mediant 5000 components without ongoing service interruption. The SC software upgraded is online. Media Gateway boards are upgraded one at a time in order to minimize the impact on Media Gateway's service (depending on the upgrade mode being used, see 'Remote Online Software Upgrade' on page 49); other blades operation is uninterrupted. In case of problems, roll back is supported; however, service lost may occur, depending on the stage when roll back was issued.
- **Health Monitoring** - Hardware elements' "Built-In-Test" (BIT) mechanism locates any hardware problem within the module's boundaries. The System Controller monitors the status of most of the hardware elements in the chassis. When a component fails, an alarm is sent to the management system, alerting the operator of the problem.

- **SNMPv2c/SNMPv3 Alarm Traps** - Alarms are reported to the management system by means of standard SNMP traps. These traps contain information about the source of the alarm location, type of problem and other vital information useful to the operator. The alarm fields comply with ITU X.733, X.736 management standard. The SNMP alarm traps can be sent to up to three different management systems (EMS, NMS and OSS).
- **Collecting Advanced Media Gateway Board Logs** - In addition to SNMP Alarm Traps, when the Media Gateway Board behaves abnormally and regular events/alarms are not sufficient for problem analysis, Advanced Media Gateway Board Logs may be used for problem troubleshooting.

  Media Gateway boards perform as a Syslog client and are capable of generating messages at 5 error levels:

  - Emergency level
  - Warning level
  - Notice level
  - Info level
  - Debug level

  The SC board performs as a Syslog server. It intercepts all syslog messages generated by the Media Gateway boards and stores them in the log files. The log files may be viewed via CLI command.
- **Collecting Media Gateway Board's Debug Recording Traces**

  The Media Gateway Board Debug Recording Traces is a powerful debugging tool that provides the ability to capture traffic being handled by the specific Media Gateway board. It may be used for analyzing different inter-operability scenarios or specific Media Gateway board malfunctions.

  The tool enables forwarding of the specific packets being handled by the Media Gateway board to the user-specified remote IP address. The remote IP address may belong to one of the following:

  - External PC
  - Standby SC board

  Flexible user-defined filtering rules may be applied to select traffic to be forwarded. For example, it is possible to select traffic between the Media Gateway board and the specific remote Media Gateway. Or, alternatively, select traffic that belongs to the specific call. Multiple filtering rules may be applied simultaneously.
- **Trunk and B-Channel/D-Channel Status**

  The EMS 'Trunks and Channels Status' page displays the status of the Trunks and the B/D channels pertaining to these trunks. The 'Trunks and Channels Status' page uses the following color-coding icons to indicate the status of the trunks and channels:

Table 2-1: Color Coding Icons for Channel Status

Channel Color	Channel Status
	Active
	Inactive
	Non-Voice
	SS7
	ISDN Signaling
	CAS Blocked

In addition, the Channels screen displays the current Trunk alarm name and color coding status. The following alarms and color coding are supported:

Table 2-2: Channel Status Alarms

Alarm Name	Color Coding
Disabled	Gray
Active OK	Green
RAI Alarm	Yellow
LOS/LOF Alarm	Red
AIS Alarm	Blue
D-Channel Alarm	Orange

- **License Keys** - Required License Key purchase enables and defines the capacity of certain features. The user must properly maintain the License keys for all of the Gateway boards (TP-6310 or TP-8410) in a Mediant 5000 system. Prior to the software upgrade, License Key upgrade may be required.

  The EMS provides mechanisms to download the License Keys as needed, as well as to review the Features List of the License Keys governing all of the system's Gateway boards.

  Information from the License Key is taken into account during the Gateway board provisioning and functionality is limited accordingly.

  - License Keys - Partial Features List
  - Maximum software version that may be loaded on a particular board
  - Number of IP to IP voice channels

- Number of PSTN E1/T1 Trunks
- Number of PSTN T3 Trunks
- SONET/ SDU Fiber Group Enable
- Number of MTP2 links
- Number of MTP3 links
- Number of M2UA links
- Number of M3UA links
- Number of IUA Interfaces.
- MGC control protocol type (MGCP, H.248, SIP)
- Availability of security features
- Media Coder Types availability

- **System Inventory information** - The Mediant 5000 Inventory feature is to represent hardware and software inventory of each of the boards contained in the Mediant 5000 system. This information is provided via the SC proprietary and standard MIBs.

  Beside the standard information, such as hardware and software version, the Mediant 5000 provides the Serial number, software patches, MAC addresses, memory size (depending to board type), as well as other parameters, which assist in controlling and troubleshooting the system.

2.3 Performance Management

Performance Monitoring is an essential feature of any element / network management system. The Mediant 5000 supports Performance Measurements (PM) utilization data for System Controllers (Active and Standby) and for all the Media Gateway blades and Interfaces. PMs are maintained on the Mediant 5000 System Controller (SC) and queried from the EMS or by Third-Party manager on an as-needed basis (via SNMP MIBs).

PM can be provided via SNMP MIBs in two view types:

- **Real-Time view** - shows the current values of one or more PMs on a graph (like Windows task manager performance view). The user clicks on a button and the Element Manager System (EMS) obtains the current values of the selected PMs from the SC.
- **Historic view -** shows the Maximum or Minimum or Average values during a configurable collection interval as indicated by the "Time Intervals" parameter. Those values are calculated by taking the Maximum or Minimum or Average of the sampled values during the Time intervals. Time Interval sampling as from version 3.2 is fixed at 15 minutes duration. The Historic view can be shown to the user via the EMS screen in the form of a table or a graph.

The historic report saves all "Time Interval" PM samples over a configurable period of time. As from version 3.2 release all the PMs are available in 15 minute buckets starting/ending at a configurable date and time. The Historic report is exported by the EMS as Comma Separated Value (CSV) files for use by network management systems. Files history storage is 30 days (based upon 15 minute buckets).

Performance Measurements are also available for a Third-Party Performance Monitoring System through an SNMP interface and can be polled at scheduled intervals by an external poller or utility in the management server or other off board system. The Mediant 5000 performance measurements are provided by several proprietary MIBs located under the "performance sub tree".

2.3.1 Performance Monitoring Threshold Alarms

This feature provides the customer with a powerful and flexible tool for monitoring the healthiness of the system.

User can define High and Low threshold values for any history PMs; an alarm is generated when the predefined High Threshold value is exceeded. The alarm is cleared when the PMs value passes below the predefined Low Threshold value.

The severity of the alarm to be generated is also configured by the user.

The feature is applicable for History PMs only, for both Counters and Gauge PM types. Up to 100 entries can be configured in PM thresholds table.

2.3.2 EMS Data Collector and Reduction Functions

The EMS's Performance Management is composed of real-time and historical data monitoring.

- **Real-Time Graphs** - Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. In a single graph, users can compare different parameters of the same gateway, or same parameter over different gateways.
- **Time Intervals Real -Time Data Collector (TIDC)** resides on the EMS server, collects Real Time PM Values from the SC on a configurable periodic basis and stores the values in a database. The data collector collects TIPM data for a default set of parameters and the user can override this set of parameters on a per blade basis as needed.
- **Background (History) Monitoring** - Historical data can be used for long-term network analysis and planning. PM profile, specifying those parameters that users want to collect from EMS background monitoring, can be easily transferred to OSS via CSV files.
- **Performance Monitoring Actions on Multiple Gateways** - Users can attach a master profile and start / stop background monitoring a single command for the entire set of gateways.

The historic performance management data is used in a number of ways. It can be accessed and displayed by the AudioCodes EMS. It can be exported as comma separated value (CSV) files for use by any network management systems.

AudioCodes EMS performs data reduction functions, including:

- Every 24 hours, summarize the most recent 24 hours of data and add the summary data to the database
- For data that has been summarized, remove the associated detailed data from the database after if it's been 7 days old

2.4 High Availability

High-Availability is a requirement for carriers, where a system must be continuously operational. To achieve the High-Availability goal, the Mediant 5000 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. As a well-designed system, the Mediant 5000 design avoids the occurrence of a single point-of-failure in the system.

Configured for 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 and can be replaced while the system is fully operational, with no disruption to service.

2.4.1 System Controller (SC) Boards (Active/Standby Configuration)

Two System Controller (SC) boards are included, each with an on-board hard disk. In this configuration, one SC board is in Active mode and the redundant SC board is in Standby mode. The software runs on both SC boards, whereby the two boards are continuously sending each other “heart beat” signals to monitor the other board's status. The Active SC manages the system, updates the Standby SC with current system configuration and internal status, as well as replicating all information to the local disk. The Standby SC receives the information from the Active SC and updates the database and local disk.

In case of an Active SC failure (heart beat is stopped) SC Switch Over process is started and the Standby SC assumes the SC's global IP address and takes over the control of the system without any interruptions to calls. The new Active SC updates the EMS accordingly and sends SC Switch Over alarms. For more information on the SC boards, refer to 'System Controller (SC) Board' on page 95.

2.4.2 Alarm (SA) Boards (Active/Standby Configuration)

Each of the two System Controllers is equipped with a System Alarm (SA)/RTM boards. This module provides the chassis management capabilities for the SC boards and the system synchronization to the BITS (Building Integrated Timing Supply) and Line Timing of the CO infrastructure.

Each of the SA is controlled by its attached SC and is responsible for monitoring and controlling the fans' rotational speed, backplane voltages and power supplies health. In this configuration, similar to the SC boards, one SA is in Active mode and the redundant SA is in Standby mode. In case of Active SA card failure, the Active SC causes SC switch over and the standby SC with his standby SA/RTM, takes over the control of the system. Refer to ' Synchronization and Alarm (SA) RTM.

2.4.3 Ethernet Switch Boards (Active/Standby Configuration)

Two Ethernet Switch boards are included, in which one Ethernet Switch board is in Active mode and the redundant Ethernet Switch board is in Standby mode. Although there could be situation where both Ethernet Switch boards process the traffic

between the Media Gateway and SC boards, only the Active Ethernet Switch board routes traffic between the System boards and the public IP Network. Both the Ethernet Switch boards interface to each of the Media Gateway boards, in a dual-star topology. In this configuration, the two Ethernet Switch boards provide dual, independent switch fabrics to every board in the System so that if a link, PHY (physical interface) or switching node fails, data is re-routed to an alternate path, sustaining network connections. For more information on the Ethernet Switch boards, refer to 'Ethernet Switch' on page 101.

The internal chassis networking is based on a PICMG 2.16 cPSB double star switched Ethernet configuration. Each of the two Ethernet Switch boards connects to the two star networks, providing redundant connectivity. Both hardware and software ensure that the internal networks are always available even if one of the boards or its uplink fails. For more information on the chassis, refer to 'The Chassis' on page 83.

2.4.4 Ethernet Uplink Redundancy

The Mediant 5000 provides '1+1' redundancy between both Ethernet Switches (ES).

Each of the Media uplink can aggregate up to three physical 1 GbE ports, forming a 3 Gbit Aggregation Group Uplink. In addition, two links for Control and OAM. If one of the "3 Gbit Aggregated" uplink or Control or Media links fails, the traffic continues through the other ES board.

OAM and Control Uplinks (when configured) are 1 + 1 redundant as well. If one uplink fails, the traffic continues through the other Ethernet Switch board.

The Ethernet Switch (ES) boards operate in the Active/Standby 1+1 redundancy mode, where one of the Ethernet Switches is assigned to be a Primary switch, and another one to be the Secondary switch. For preventing IP loops, there is no connection between both ESs and only the Primary Ethernet Switch board routes traffic between the System boards and to the outside IP Network. The SC allocates all boards on the Primary Ethernet Switch at start-up and during system operation.

The role of the switch (whether it is Active or Standby) is defined according to its up-links activity. Although both Ethernet Switches are operated, only one of the switches is allocated to send/receive the traffic between Media Gateway boards and to the external IP cloud. This means that from the external node's perspective, only one port from either Ethernet Switch boards is active at any given time.

2.4.5 Media Gateway Boards (N+1 Configuration)

The Media Gateway boards in the system can be optionally configured in an N+1 configuration. In such a configuration, a dedicated, standby Media Gateway board is selected to take over the function of a failing Media Gateway board's resources. Each Media Gateway board sends “heartbeat” messages to the active System Controller's (SC). If any Media Gateway board fails, the SC software redirects the Media Gateway board's trunks to the redundant, standby Board and assigns the IP address of the failed board to the redundant board. This feature is known as "PSTN Redundancy".

There are two redundancy modes:

- **Warm Redundancy** - Capacity sustaining redundancy. For boards configured with specific parameters which are different on the Redundant Board (while "make board redundant as" action) to the Media Gateway configuration. Active calls are dropped when Media Gateway board switchover takes place, because the redundant board is started from cold reboot. However, the Mediant 5000 Gateway regains original capacity automatically without the need of operator intervention.
- **Hot Redundancy** - Uninterrupted call redundancy. In this implementation, all of the network elements connected to the board (either IP or PSTN interfaces) treat the switchover process as a minor traffic interruption, but not as a failure. Therefore, in case of PSTN switchover, there is no risk of lower level network interfaces failing as a result of protocol timers expiring. The user may hear a transient reduction of voice quality.

  When IUA, DUA or M2UA/M3UA is configured, the SCTP association between the MGC and the Signaling Gateway is aborted and the MGC reestablishes it as a SCTP client. However, the failed board IUA/DUA /M2UA/M3UA configuration automatically downloads to the redundant board.

PSTN redundancy uses a unique hardware feature, which allows the PSTN signals to be routed to the redundant module. Hot Redundancy (uninterrupted call redundancy) utilizes this capability and maintains the configuration and state of the failed board and restores service on the redundant board without interrupting the trunk Interfaces (E1/T1, STM-1 or OC3) and the active calls.

2.4.5.1 SS7 Point Code Sharing

The Mediant 5000 contains Redundant MTP3 Group configuration enabling Hot redundancy of MTP3/M3UA application. In this configuration signaling node is distributed across multiple Media Gateway boards. Signaling links should be defined on either Media Gateway boards that belong to the Redundant MTP3 Group.

Currently up to two Media Gateway boards may be attached to the same Redundant MTP3 Group.

When a specific Media Gateway board fails, signaling node remains in service due to the other Media Gateway board and because the link-set is distributed across the two boards.

Failed board MTP2 signaling links are restored on the redundant Media Gateway board after Media Gateway boards' switchover– and thus capacity and capabilities of the whole MTP3 subsystem is preserved.

2.4.5.2 PSTN and IP to IP Applications Activation via Boards' License Key

For an IP-IP transcoding application, you can define the Gateway as either a standalone IP-IP Gateway, as a standalone PSTN-IP Gateway, or as a combined Gateway/IP-IP platform. These configurations are activated using the Boards' License Key.

The SC validates the Board's License Key on startup and determines the Board's functionality status as well as its High Availability position (Hot, Warm or Not protected). In case of a conflict between the Board's configuration and License Key, a "License Key Alarm" is sent.

2.4.6 Power Supply Modules (Load sharing N:1 Configuration)

The Mediant 5000 contains 3 power supply modules. The Power supply modules share their load, so when one of them fails they automatically redistribute the load among the remaining functional modules. For a fully populated Media gateway system, the power supply modules are sufficient to support that configuration even if one of the power supply modules fails. For more information on the power supply modules, refer to 'Power Supply and Power Entry Modules' on page 86.

2.4.7 Cooling Fans (Load sharing N:1 Configuration)

The FML-5 Fan Tray unit contains five fans. The FMR-5 auxiliary fan tray contains two additional fans to provides additional protection against overheating for the full system. The FML-5 Fan Tray Unit and associated air filter, as well as the FMR-5 are hot-swappable and efficient replacement can be accomplished without affecting the Mediant 5000's operation. For more information on the cooling system, refer to 'Cooling System' on page 84.

2.4.8 Multi-Redundancy Groups Procedures

Media Gateway boards are shared between the Redundancy Groups, according to the different boards' services and applications support, for gaining the Hot Redundancy for all application types. For example, SIP and H.248.

The Multi-Redundancy Group feature represents up to up to 2 Groups of all Media Gateway boards in the chassis. One board in the group has a Redundant RTM associated with it and is defined as the redundant board, providing backup for all of the other Media Gateway boards contained in the group. There is one Redundancy Group by default, to which all boards automatically belong, however, in case where more than one application is running on the same gateway, the user can define up to up to 2 Redundancy Groups.

When defining the redundant board in the Redundancy Group ("make board redundant" action), the active Media Gateway board configuration is copied to the redundant board.

The EMS displays the status of each board in the redundancy group; redundant or active.

From the EMS, the administrator can define the Failed Board Behavior either to Recover service by switching over to the Redundant board, or Stop Service mode . In Recover service mode, the administrator can automatically or manually switch back to the failed board, either after failed board recovery or replacement, or even manually as a forced switch back in the event that the redundant board is to be saved for an additional board failure.

2.4.9 Carrier Grade Alarm System

The Mediant 5000 's basic alarm system has been extended to a carrier-grade alarm system. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account EMS outages, network outages, and transport mechanism, such as SNMP over UDP.

The Mediant 5000's carrier-grade alarm system is characterized by the following:

- Active Alarm Table - The SC MIB maintains an active alarm table to allow a manager to determine which alarms are currently active in the Mediant 8000 system.
- Alarm History - The SC MIB maintains the history of the alarms that have been raised and traps cleared to allow a manager to recover any lost, raised or cleared traps.

This allows the EMS to synchronize its view of the Mediant 5000's active alarms.

2.4.9.1 Alarm Throttling

In rare circumstances, a specific alarm may be continuously raised and cleared at a high rate (e.g. PSTN alarm on a Trunk may be issued continuously when the Media Gateway is not properly synchronized with the PSTN trunk).If such a scenario occurs, the Media Gateway automatically suppresses alarms from the specific MO for a certain period of time.

An **Alarm Throttling Limit Exceeded** alarm will be generated when alarm throttling is activated.

2.5 Clock Synchronization Modes

The Mediant 5000 Media Gateway supports the following Clock Synchronization modes:

- **Standalone Board Sync mode**– each Media Gateway board synchronizes itself by the clock received on one of the PSTN interfaces (OC-3/STM-1 optical links or E1/T1 trunks) connected to it; there is no global clock synchronization between different Media Gateway boards. For more information, refer to .Stand Alone Board Clock Mode.
- **Timing Module BITS Sync mode** – all Media Gateway boards are synchronized with dual BITS (Building Integrated Timing Source) trunk clock sources connected to dual SA-1/RTMs; for more information, refer to 'Timing Module BITS Sync Clock Mode' on page 32.
- **Timing Module Line Sync mode** – all Media Gateway boards are synchronized by up to four “reference” OC-3/STM-1 links or DS3 trunks connected to the specific Media Gateway boards; for more information, refer to 'Timing Module Line Sync Clock Mode' on page 33.

The following sections describe each of the available clock synchronization modes in details.

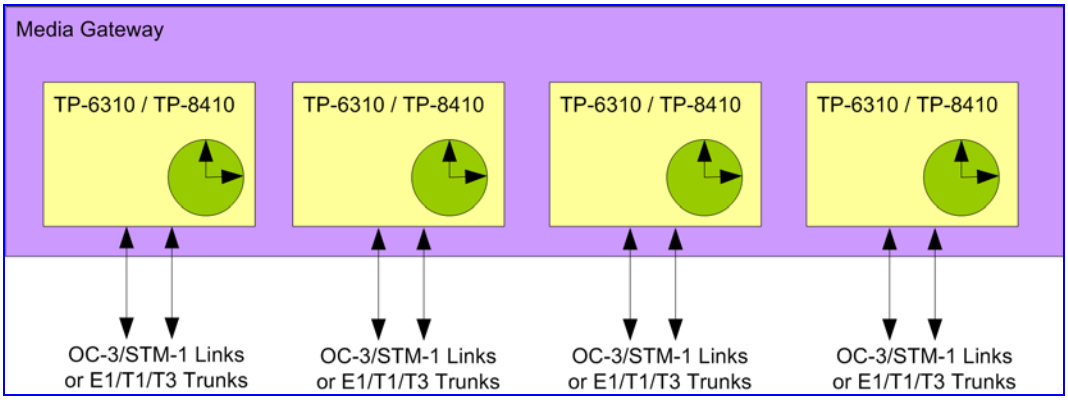
2.5.1 Standalone Sync Clock Mode

In Standalone Sync clock mode, each board synchronizes its own clock. The clock may be derived from the following sources:

- PSTN interface (OC-3/STM-1 optical links, or E1/T1/T3 trunks)
- Internal board's clock reference

There is no global clock synchronization across different Media Gateway boards.

Figure 2-1: Stand-Alone Clock Synchronization Mode



In Standalone Board Sync clock mode, the clock source is derived from the high-level communication layer protocol of the PSTN interface (OC-3, STM-1, T1 on T3 for 6310 or E1/T1 on 8410) or from the internal board's clock reference.

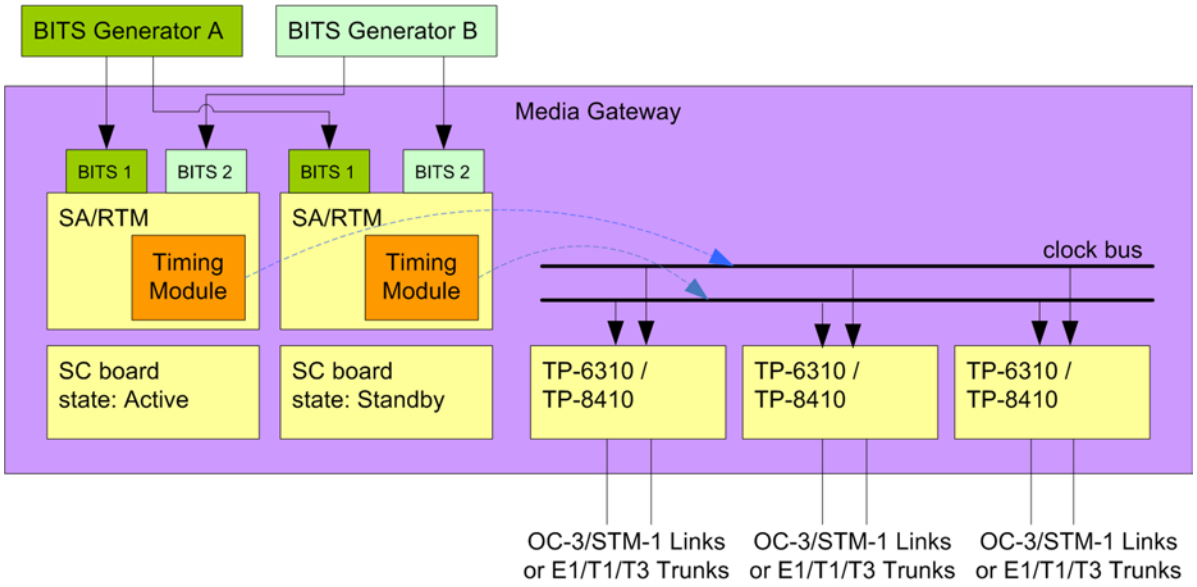
2.5.2 Timing Module BITS Sync Clock Mode

In Timing Module BITS Sync clock mode, all Media Gateway boards are synchronized by tworedundant E1/T1/T12 BITS Generators (Building Integrated Timing Source) trunks. These trunks are synchronized with the Media Gateway boards via two SA-1/RTMs, each with a designated timing module. Two SA-1/RTMs are required to ensure seamless clock operation in case of failure of one of the SA-1/RTMs modules.

Note: To activate the Timing Module BITS Sync clock mode, you must order SA-1/RTMs (SA/RTM with a resident Timing Module). To order the Media Gateway with this module, refer to the AudioCodes price list.

When one of the reference clock sources (BITS Generator) fails, the Timing Module automatically switches to another source and continues using it as a reference clock for the whole Media Gateway.

Figure 2-2: Timing Module BITS Sync Clock Mode



When both BITS trunks fail, the Timing Module continues to function as the clock ("clock holdover") for up to 24 hours. The clock provided by the Timing Module complies with STRATUM 3 (4.6ppm) requirements.

When clock source (BITS trunk) with a higher priority returns in service after the failure, the Timing Module may either revert to the higher-priority clock source or continue using the lower-priority clock source. The behavior is controlled via the **Auto Clock Reference Mode** parameter.

2.5.3 Timing Module Line Sync Clock Mode

In Timing Module Line Sync clock mode, all Media Gateway boards are synchronized with up to 4 redundant T1s on 6310-T3 or OC3/STM-1 on 6310-OC3/STM-1 Boards or E1/T1 on 8410. These trunks are synchronized with the Media Gateway boards via two timing modules. Two SA-1/RTMs are required to ensure seamless clock operation in case of failure of one of the SA-1/RTMs.

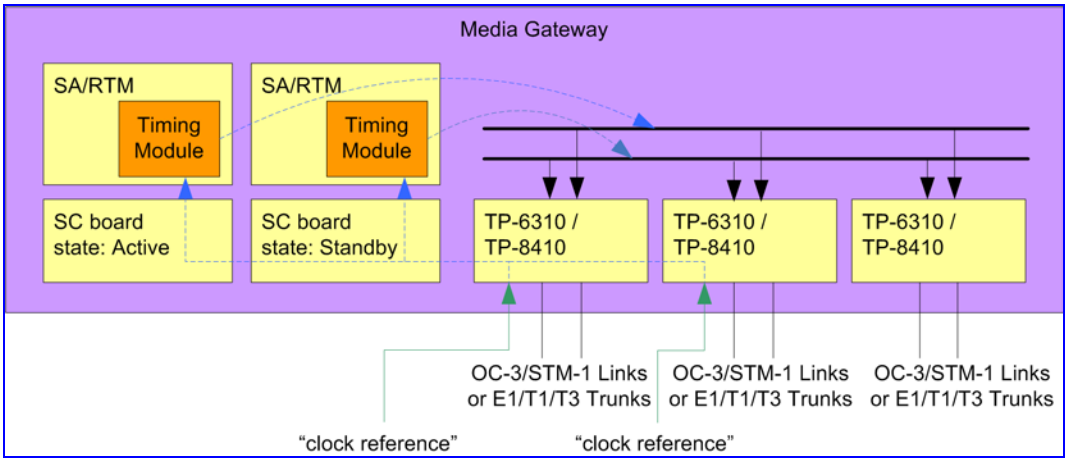
Note: To activate the Timing Module Line Sync clock mode, you must order SA-1/RTMs (SA/RTM with a resident Timing Module). To order the Media Gateway with this module, refer to the AudioCodes price list.

When one of the PSTN reference clock sources fails, the Timing Module automatically switches to a lower priority reference source and continues providing the whole Media Gateway clock.

When all reference PSTN trunks fail, the Timing Module continues to function as the clock ("clock holdover") for up to 24 hours. The clock provided by the Timing Module complies with STRATUM 3 (4.6ppm) requirements.

When clock source (PSTN trunk) with a higher priority returns in service after the failure, the Timing Module may either revert to the higher-priority clock source or continue using the lower-priority clock source. The behavior is controlled via the **Revert Clock Reference Mode** parameter.

Figure 2-3: Timing Module Line Sync Clock Mode



2.6 Security

The Mediant 5000 provides the capability to deliver enhanced secure communications services that implements the following goals:

- **Secure network communications** - All media packets and all sensitive signaling communication across the network are safe from eavesdropping. Unauthorized message modification, insertion, deletion and replays anywhere in the network are either detectable or do not affect proper network operation.
- **Network element interoperability** - All of the security services for any of the network elements inter-operate with the security services of the other network elements.

2.6.1 Media Gateway Threats

Media Gateway 's general threats are:

- Theft of Service Attacks:
  - **Subscription Fraud** - This attack is prevalent in today's telephony systems (i.e., the PSTN). It can be addressed with a Fraud Management system.
  - **Impersonate a Call Agent Server** - With proper cryptographic mechanisms, authorization and procedural security in place, this attack is unlikely, but has the potential for great damage.
  - **Protocol Manipulation** - Can occur only when security protocols are flawed or when not enough cryptographic strength is in place.

- Bearer Channel Information Disclosure Attacks:
  - **Simple Snooping** - This would happen if voice packets were sent in the clear over some segment of the network. Even if that segment appears to be protected, an insider may still compromise it. This is the only major attack on privacy.
  - **Protocol Manipulation** - A flawed protocol may somehow be exploited to discover bearer channel encryption keys.
  - **Off-line Crypto-analysis** - Even when media packets are protected with encryption, they can be stored and analyzed for long periods of time, until the decryption key is finally discovered. Such an attack is not likely to be prevalent; since it is justified only for particularly valuable customer-provided information. This attack is more difficult to perform on voice packets (as opposed to data). Still, customers are very sensitive to this threat and it can serve as the basis for a negative publicity campaign by competitors.
- Signaling Information Disclosure:

  This threat is a potential for bad publicity and customer sensitivity regarding keeping customers' numbers and location private.

  The attacks listed below also effect bearer channel privacy and Theft of Service:
  - Simple snooping
  - Call Agent clones
  - Protocol manipulation
  - Off-line crypto-analysis
  - Service disruption

2.6.2 Mediant 5000 Security Features

In order to protect the Media Gateway against the above threats, the Mediant 5000 supports the following security mechanisms over all external interfaces as well as protocols:

- **Authentication** - The process of verifying the claimed identity of an entity to another entity. Implementation is protocol depending (see table below) including IKE pre-shared key, X.509 certificates and digital signatures, username and password.
- **Confidentiality** - A way to ensure that information is not disclosed to anyone other than the intended parties. Information is encrypted to provide privacy. Implementation is protocol depending (see table below) including IPSec (ESP), SSL, HSS and TLS.
- **Integrity** - A way to ensure that information is not modified except by those who are authorized to do so. Implementation is an option for all protocols over IPSec, using MMH Message Authentication Code (MAC).
- **Access Control** - Limiting the flow of information from the resources of a system only to authorized persons, programs, processes, or other system resources on a network.

Table 2-3: Mediant 5000 Interfaces Security Profiles

Interface	Confidentiality	Authentication
EMS Server- Client	SSL	Application level - UserID + Password
EMS/NMS - Mediant 8000	SNMPv2 over IPSec (Transport ESP) or SNMPv3	IKE pre-shared key or SNMPv3
Call Control (MEGACO, MGCP, TGCP)	IPSec (ESP) Transport or Tunneling modes	IKE pre-shared key X.509-Optional
Call Control (SIP)	SSL/TLS	X.509
Media Streams RTP/RTCP	Secure RTP/ RTCP (SRTP) RFC 3711	Indirect (MGC)
Telnet (for debugging)	SSH /SSL	Application level - UserID + Password
FTP from remote download	SSH - SFTP	Application level - UserID + Password
Web - HTTP (for debugging)	SSL- HTTPS	Application level - UserID + Password X.509 - Optional

2.6.2.1 OS Hardening

When the Mediant 5000 Media Gateway software is installed on SC boards, it automatically configures the Solaris/Linux OS for secure operation mode. The following OS hardening tasks are performed:

- Unnecessary OS services and daemons that are shut down.
- File system permissions are modified to prevent security attacks.
- TCP/IP stack is tuned to prevent DoS attacks (including SYN and Smurf attacks).
- Unnecessary OS packages and binaries that contain potential security breaches are removed.
- Insecure communication protocols (Telnet, FTP and SNMPv2) are limited to the IPSEC associations only.

2.6.2.2 File System Integrity Check

The Media Gateway software implements a File System Integrity Check. This check provides an additional security mechanism that helps to mitigate security risks such as hacker intrusion and malicious software installation on the SC boards.

When the Media Gateway software is installed, a snapshot of the file system is created. This snapshot covers both Media Gateway software and OS components, and includes both binary and basic configuration files.

The Media Gateway software periodically scans the file system and compares it against the snapshot. When unauthorized modifications are detected, an SNMP alarm is sent to the EMS and the integrity status of SC board's file system is updated accordingly.

2.6.2.3 Denial-of-service (DoS) Attacks Protection

The Mediant 5000 is protected against malicious **denial-of-service** (DoS) attacks, some of which include:

- SYN floods - sending huge number of TCP SYN packets.
- Jolt (ping of death) - sending huge fragment Ping packet (64KB) when each fragment is very “small” (less than 100 bytes) to create a “shortcut” for receive network buffers.
- Ping floods - sending more than 1K PING packets per second
- Land attack - sending packets with the board network address (MAC/IP) as the source.

2.6.2.4 Auditing on Mediant 5000 Media Gateway

The Solaris™ 9/Linux OS, installed on the SC boards, provides the capability to log the activity on a system at a granular level. This logging or auditing ability is part of the Solaris SunSHIELD™ Basic Security Module (BSM). These auditing capabilities were added to provide the features required by the Trusted Computer System Evaluation Criteria (TCSEC) to a security level referred to as C2.

The TCSEC has been superseded by the newer updated and more internationally recognized Common Criteria security requirements. As part of these requirements, the Solaris OS has been evaluated under the Controlled Access Protection Profile (CAPP) at Evaluation Assurance Level (EAL) 4. The CAPP used for the Solaris OS evaluation includes all functionality covered by C2 evaluations.

The primary goal of auditing is to record user actions to detect malicious intent.

The secondary goal of auditing is to avoid performance degradation.

When an event occurs, it is recorded in the Audit Trail File. The latter file contains all relevant audit data in a binary form. Some tools are required to examine the data in a human readable format. An administrator should periodically examine the Audit Trail File and analyze system behavior based on the recorded events.

When the Mediant 5000 Media Gateway software is installed on the SC boards, it automatically configures the Solaris OS auditing subsystem to record all the most important security-related activity on the SC board. The list of recorded events complies with DoD IASE STIG and GR-815 security requirements.

The OS auditing is simultaneously performed on both active and standby SC boards. Each SC board contains audit trail data of its own.

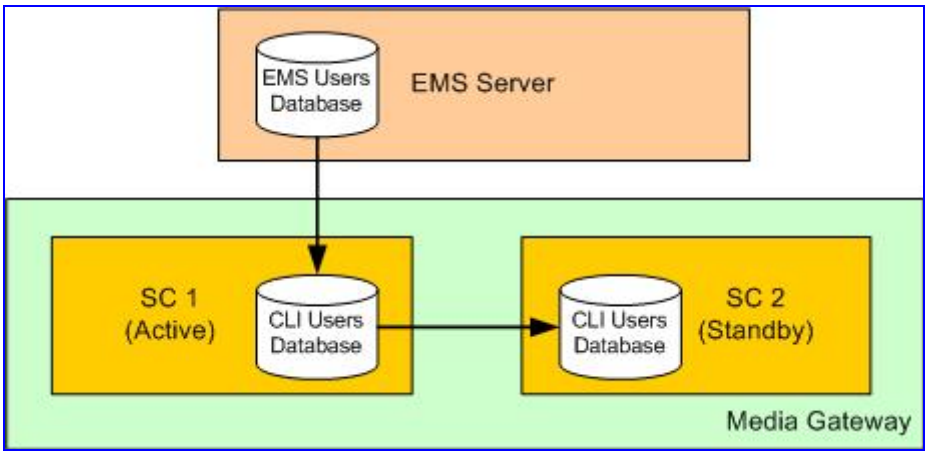
2.6.2.5 CLI Interface Access Control

SSH and Telnet services on SC boards are used to access the Media Gateway's Command Line Interface. In default configuration, these services are accessible from any IP address and user authentication is performed via username and password. For enhanced security, you may restrict access to the SSH and Telnet services on SC boards by specifying an explicit list of IP addresses that are allowed to access the CLI interface.

2.6.2.5.1 Synchronizing CLI Users Database with the EMS Server

In the typical Multi Systems deployment scenario, the same users, passwords and access levels are used for all available Systems management interfaces – EMS GUI and CLI. In order to simplify user maintenance in such scenario, the Mediant 5000 supports synchronization of the CLI Users Database with the EMS server. When this synchronization is activated, the Mediant 5000 will synchronize its local CLI users' database with the users' database on the EMS server. Any change to users' database on the EMS server will be updated to all Media Gateways within a short period of time. All EMS server user profile attributes, including access level and password expiration policy are updated on both SC boards of all Media Gateways connected to the EMS server.

Figure 2-4: Synchronizing CLI Users Database with EMS Server

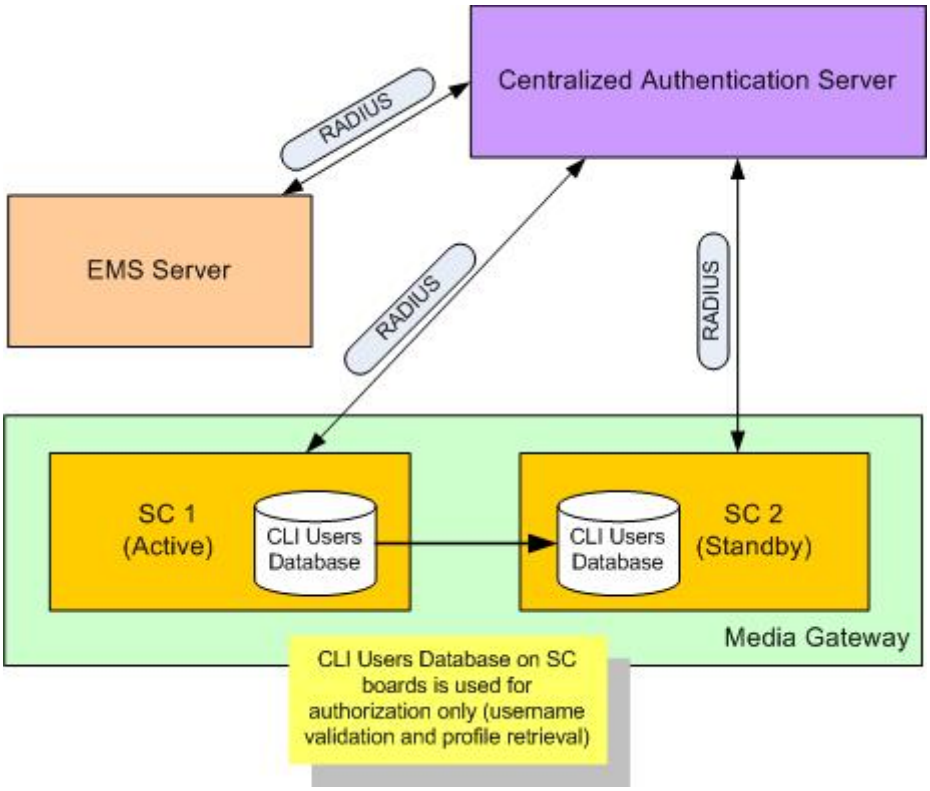


When the CLI Users Database is synchronized with the EMS server, all user maintenance operations (user addition, removal and password change) must be performed via the corresponding interfaces provided on the EMS server. Refer to the relevant IOM Manual for additional information.

2.6.2.5.2 Mediant 5000 CLI /EMS Centralized User Authentication via RADIUS Protocol

In some deployments, Centralized User Authentication servers are used for storing user information for all solution elements. For such deployments, Mediant 5000 supports centralized authentication of CLI users via RADIUS protocol. Together with the EMS servers' ability to perform EMS centralized authentication, this feature provides a complete solution for the Centralized User Management.

Figure 2-5: Centralized User Authentication via RADIUS Protocol



When the Media Gateway is configured to perform Centralized User Authentication, enhanced authentication schemes may be deployed by a Centralized Authentication Server. For example, the following schemes may be implemented:

- Time-of-day based login
- Password complexity enforcement
- Restricting access for specific user to specific equipment only
- Multi-factor authentication (e.g. RSA SecureID based on the combination of password and a hardware token)

The Mediant 5000 implements RADIUS client as defined in IETF RFC 2865. Up to 3 RADIUS servers are supported for redundancy purposes.

2.6.2.5.3 Mediant 5000 CLI /EMS Centralized User Authentication via TACACS+ Server

The EMS and the Media Gateway user external central server authentication and authorization can be performed using the TACACS+ protocol (in addition to the RADIUS server or a local EMS server). TACACS+ (Terminal Access Controller Access-Control System Plus) is defined in RFC 1492 and is considered as a more secure authentication and authorization server than RADIUS. TACACS+ provides separate authentication, authorization and accounting services, runs over TCP, encrypts the entire body of the packet and offers multiprotocol support.

The following TACACS+ services are supported:

- Authentication – for username/password validation.
- Authorization – for initial access to the CLI and for each Media Gateway CLI command (may be used to grant or revoke ability to execute specific CLI command by specific user or group).
- Accounting – for logging user activity.

2.6.2.5.4 CLI Password-less Access

The Mediant 5000 Gateway may be configured to perform CLI user authentication based on the RSA or DSA private/public key pair. When such authentication is enabled, users are granted access to the Mediant CLI without need to interactively enter password.

2.6.2.6 Intrusion Detection Events

When an incorrect username and/or password is detected, security-related events occur (e.g. attempt to enter the system). These events are recorded in the OS log file and are reported to the EMS/NMS as Intrusion Detection Events. Each Intrusion Detection Event contains detailed data about the event type, intrusion time and are reported by the SC.

In certain environments, an Intrusion Detection Event may be issued for normal activity. For example, there may be an automated network scanner that periodically attempts to access Media Gateway with incorrect credentials; in this case it is possible to prevent reporting of the specific events by modifying the Intrusion Detection Filter parameter.

2.6.2.7 Configuration Freeze and Configuration Change Event

For securing the Media Gateway provisioning, a Configuration Change Event could be sent (programmable) to EMS/NMS for any Media Gateway parameter change.

In a typical deployment, the Media Gateway is configured by authorized personnel as part of initial site setup and only routine maintenance tasks are performed later on. For such environments, the Media Gateway configuration may be frozen in order to prevent the case of mistaken configuration changes or for security reasons.

When a Media Gateway configuration is “frozen”, any attempt to modify the value of a parameter fails with a corresponding event.

2.6.3 Mediant 5000 Security Technology

2.6.3.1 IPSec and IKE

The IPSec and IKE protocols are part of the IETF as well as PacketCable standards for security issues. IPSec and IKE are used together on the Media Gateway to provide security for control and management protocols. The IPSec protocol is responsible for securing the data streams. The IKE protocol (Internet Key Exchange) is responsible for obtaining the IPSec encryption keys and encryption profile (known as IPSec Security Association). IPSec is used by the Mediant 5000 to assure confidentiality, authentication and integrity for the following media types:

- For Control traffic, such as H.248, MGCP and TGCP and OAM traffic such as SNMP and Telnet. . The Mediant 5000 could be configured to support IPSec Transport mode for peer to peer associations, as well as IPSec Tunneling mode, enables users to connect IPSec with conjunction end-point devices that don't support IPSec. The secured channel will be formed between the Mediant 5000 and an IPSec-capable device (e.g. Firewall, VPN…) in front of the end-point. Note that securing SIP traffic is accomplished using Transport Layer Security (TLS)
- Sigtran over SCTP traffic, such as M2UA, M3UA and IUA/DUA (with reduced channel capacity)
- Management traffic to EMS/ NMS/ OSS, such as SNMP, FTP and Telnet

2.6.3.1.1 IPSec

The IPSec protocol is responsible for encrypting and decrypting the IP streams.

IPSec specifications:

- Transport or Tunneling modes on OAM and Control
- Encapsulation Security Payload (ESP) only
- Support for Initialization Vector (IV) and Cipher Block Chaining (CBC)
- The encryption algorithms that are supported for IPSec SA are currently DES, 3DES and AES.
- Hash types for IPSec SA are SHA1 and MD5

2.6.3.1.2 IKE

The Internet Key Exchange protocol is used to obtain the IPSec Security Associations (SAs). The SA contains the encryption keys and profile used by IPSec to encrypt an IP stream.

IKE specifications:

- Authentication mode - pre-shared key only
- Both Main and Aggressive modes are supported for IKE Phase 1
- The encryption algorithms that are supported for IKE SA are DES, 3DES and AES.

- Hash types for IKE SA are SHA1 and MD5
- Support for modp1536, modp2048, modp3072, modp4092, modp6144 and modp8192 DH groups

2.6.3.2 SNMPv3

SNMPv3 is defined by RFC 3411–RFC 3418. SNMPv3 primarily includes security and remote configuration enhancements to SNMPv2.

The Mediant 5000 supports the following SNMP operational modes:

- SNMPv2c – compliant with RFC 1901 – RFC 1908; uses UDP transport and simple community-based security scheme
- SNMPv2c + IPSEC – adds pre-shared key based IPSEC/IKE encryption to the SNMPv2c protocol;
- SNMPv3 – uses enhanced User Security Model (USM) and supports message integrity, authentication and encryption.

Only one SNMP mode is supported at any time – e.g. if the Media Gateway is configured for SNMPv2c + IPSEC mode, all SNMP managers must use v2c of the protocol and have valid IPSEC/IKE associations with the Media Gateway . Mix of the SNMP operational modes (e.g. SNMPv3 for EMS server and SNMPv2c for 3rd party managers) degrades solution security and therefore is not supported.

SNMPv3 provides the following security features:

- Message integrity to ensure that a packet has not been tampered with in transit.
- Authentication to verify that the message is from a valid source.
- Encryption of packets to prevent snooping by an unauthorized source.

2.6.3.3 Firewall

The Mediant 5000 Voice Boards accommodate an internal access list facility, allowing the security administrator to define network traffic filtering rules associated either with all network interfaces of a specific VoIP Board, or with any specific Subnet of a specific VoIP board.

The access list provides the following features:

- Blocks traffic from known malicious sources
- Only allows traffic from known friendly sources, and blocks all others
- Allows a mix of allowed and blocked network sources
- Limits traffic to a predefined rate (blocking the excess)
- Limits traffic to specific protocols, and specific port ranges on the device

The access list consists of up to 20 rules. For each packet received on the network interface, the rules are scanned from the top until a matching rule is found either to block the packet or allow it. If the table's end is reached without a match, the packet is blocked.

Filtering criteria are source IP-address and subnet, destination port range, protocol type, packet size and traffic rate in bytes-per-second.

2.6.3.4 SSH

SSH (Secure Shell) provides secure encrypted communication between two distrusted hosts over an insecure network. SSH is the method used to secure the Mediant 5000's System Controller Telnet and FTP Server.

Specifications for the SSH implementation:

- SSH Protocol Version 2
- Supported encryption algorithms: AES-128, BLOWFISH, 3DES
- Supported authentication algorithms: SHA1, MD5
- User/password authentication on each login

The Mediant 5000 uses SSH to encrypt CLI management sessions. SSH connection is available even when secure operation mode is disabled and is a preferred connection type for the CLI management interface.

Secure Copy (SCP) and Secure FTP (SFTP) are associated protocols that support files transfer over SSH connections. They are used to transfer backup files and debug data to/from the Mediant 5000 Media Gateway .

2.6.3.5 SSL/TLS

SSL (the Secure Socket Layer), also known as TLS (Transport Layer Security), in addition to securing the SIP interface (if required) is the method used to secure the Mediant 5000's Media Gateway Boards Web server and telnet. The SSL protocol provides confidentiality, integrity and authenticity of the Web server.

Specifications for the SSL/TLS implementation:

- Supported transports: SSL 2.0, SSL 3.0, TLS 1.0
- Supported ciphers: DES, RC4 compatible
- Authentication: Username & Password, X.509 certificates

2.6.3.6 X.509 Certificates

ITU-T X.509 is the most widely used standard for Public Key Certificates. It is being adapted to the Internet by the IETF PKIX working group.

Public Key Certificate uses a digital signature to bind together a public key with an identity –; information such as the name of the person or organization and, their address. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature is issued by a certificate authority (CA) and is an attestation by the certificate signer that the identity information and the public key belong together.

X.509 Certificates are used to establish a user's identity by SSL/TLS and HTTPS protocols. They may also be used by IPSEC/IKE protocols as an alternative to pre-shared key authentication mode.

Note: HTTPS protocol is used for secure access to the Media Gateway board's advanced status summary. For more information, refer to Accessing Advanced Status of Media Gateway Board via WEB interface.

2.6.3.6.1 Using X.509 Certificates

In order to use X.509 Certificates, the following auxiliary files must be uploaded to the Media Gateway and properly configured:

- **Private Key File** – contains a private key that is used to perform decryption; it is the most sensitive part of security data and should never be disclosed to other entities.
- **Certificate File** – contains a digital signature that binds together Public Key with an identity information; Certificate may be issued by a CA or be self-signed (issued by the entity itself).
- **CA Certificate File** – certificate of the CA that issued a Certificate for the Mediant 5000; optional file that if present is used to validate the Certificate file.
- **Trusted Root Certificate File** – certificate of the Trusted Root; used to authorize certificates received from the remote parties, based on the identity of the CA that issued it; if the root certificate of this CA matches one of the Trusted Root Certificates, remote party is authorized.

Mediant 5000 supports the following X.509 functionality:

- Generation of Private Key and Self-Signed Certificate
- Generation of Certificate Signing Request (CSR)
- On-line provisioning of Private Key and Certificate files
- Support for up to 3 Trusted Root Certificate files
- Expiration alarm for each provisioned Certificate file

X.509 Certificates are shared by all boards inside the Media Gateway. This reduces the amount of the certification data required to fully provision the occupied Media Gateway and simplifies the hardware replacement procedure. It also makes the addition of the new Media Gateway board fully transparent to the security administrator.

2.6.3.6.2 Initial Configuration

Upon installation of the Media Server software, the Private Key and Self-Signed Certificate files are automatically generated, added to the Auxiliary Files repository and configured in the Media Gateway security settings. By default, all Media Gateway boards use these self-generated Private Key and Certificate files.

2.6.3.6.3 Self-Signed Certificate

Self-Signed Certificate is the most simple form of the X.509 Certificate that is issued by the participant on it's own without use of any Certificate Authority (CA). The Self-Signed Certificate consists of the Public Key of the party that is signed by the Private Key of the party itself. Self-Signed Certificate is typically considered to be a very weak form of the X.509 Certificate since it doesn't utilize CA trust relationships and it's authenticity cannot be verified.

Note: Use of the Self-Signed Certificates is not recommended for field deployments. You should establish PKI infrastructure and use certificates signed by the real CAs instead. Refer to the chapters below for detailed instructions.

When Self-Signed Certificates are used by both parties that participate in secure communication, Self-Signed Certificate of each party should be used by the other party as a Trusted Root Certificate.

The Media Gateway is pre-installed with a self-signed certificate upon installation. This certificate is primarily intended to enable internal communication between the SC and the Media Gateway boards. However, some users may wish to periodically re-generate self-signed certificate to improve its security properties (by enforcing use of the new Public Key that is part of the certificate data).

2.6.3.6.4 Generating Certificate Signing Request (CSR)

Certificate Signing Request (CSR) is a message sent from an applicant to a Certificate Authority (CA) in order to apply for a digital identity certificate. The CSR contains information identifying the applicant and the Public Key. The corresponding Private Key is not included in the CSR; however, is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proof of identity required by the Certificate Authority, and the Certificate Authority may contact the applicant for further information.

If the request is successful, the Certificate Authority will send back an identity certificate that has been digitally signed with the Private Key of the Certificate Authority. This certificate file, together with the certificate of the CA itself, must be added to the Media Gateway Auxiliary Files repository and configured in the Security Settings screen for the Media Gateway . You must also configure the Trusted Root Certificate file on the Media Gateway , depending on the identity of the CA who signed the certificate of the other participant (e.g. of the CA who issued the certificate for the Softswitch that communicates with the Media Gateway via SIP/TLS protocol).

Note: Never send the Private Key file to anybody. It contains the most sensitive security data and should never be disclosed. Use CSR instead as described below.

2.6.3.6.5 Generating New Private Key

Some users may wish to periodically re-generate the Private Key file in order to enhance security. When a new Private Key is generated, an accompanying Self-Signed Certificate is generated as well. This Self-Signed Certificate contains a matching Public Key. However, if you are implementing PKI infrastructure, you should generate a new CSR request. You then receive a signed certificate from the Certification Authority (CA), which can be applied to the new Private Key. In addition, you will have to reapply a new certificate to the private key when the original Certificate expires.

2.6.3.6.6 X.509 Expiration Date Alarm

Each X.509 Certificate File contains an expiration date. The Expiration date for each certificate is displayed in the EMS Security X.509 screens.

When a X.509 certificate is due to expire, the Media Gateway issues a Security Alarm to the EMS and/or NMS. This alarm is issued twice – a few days before the expiration, an alarm with warning severity is issued. When you see this alarm, contact CA immediately for a new identity certificate. User may configure the amount of time between these two alarms.

2.6.3.6.7 Supporting Online Certificate Status Protocol (OCSP)

Specific Public-Key Infrastructures support revoking of a certificate after it is issued. TP-6310/TP-8410 boards employing SSL/TLS and IPSec may be configured to verify whether a peer's certificate has been revoked via OCSP.

2.6.3.7 RTP Media Encryption – RFC 3711 Secured RTP or ARIA (Korean standard)

Secure RTP, a standard protocol defined by RFC 3711, provides confidentiality, message authentication and replay protection of the RTP & RTCP traffic. Key negotiation is not part of the SRTP. Instead, it is handled by higher-level protocols.

Secure RTP specifications:

- Encryption – AES 128 Secured RTP in Counter Mode, or 128 or 192 ARIA (Korean standard) for Media Security
- Authentication – HMAC-SHA1
- Support of Key Derivation
- Key management is provided via the Control Protocol.

2.7 Network Time Protocol (NTP) synchronization

The Media Gateway software requires precise time and date to be set correctly for normal operation. For example, the following features will not operate correctly when incorrect time and date are set:

- Operational and security logs (both on the SC and on the VoP boards)
- Real-time and historical performance measurements (see Performance
- Management)
- X.509 certificates (for managing certificate expiration time)
- Online provisioning of Auxiliary Files

The Mediant 5000 Media Gateway lacks a hardware clock that is precise enough and can survive a chassis power down/up cycle. Therefore Network Time Protocol (NTP) is used to synchronize the time and date of the Media Gateway (and all its components) with the external NTP servers.

The Media Gateway serves as an NTP client and supports the following features:

- Support for Version 4 of the NTP protocol (as defined on 'NTP' 'http://www.ntp.org')
- Backward-compatible with Version 3 of the NTP protocol (as defined in RFC 1305)
- Support for up to 4 external NTP servers are supported
- Using the EMS Server as an additional NTP server (default configuration).

At any time one of the available NTP servers with the most accurate clock source and the lowest Stratum level is selected as a “synchronization source”. Other servers are kept as “alternative candidates” in case connection with the selected source is broken or deteriorates.

2.7.1 NTP Synchronization and Status

The Media Gateway synchronizes with NTP server periodically and updates the **NTP Server Status** attribute accordingly.

In cases where the connection between the NTP Server and the Media Gateway is lost or in cases where the connection is re-established, the **NTP Server Status** attribute is not immediately updated.

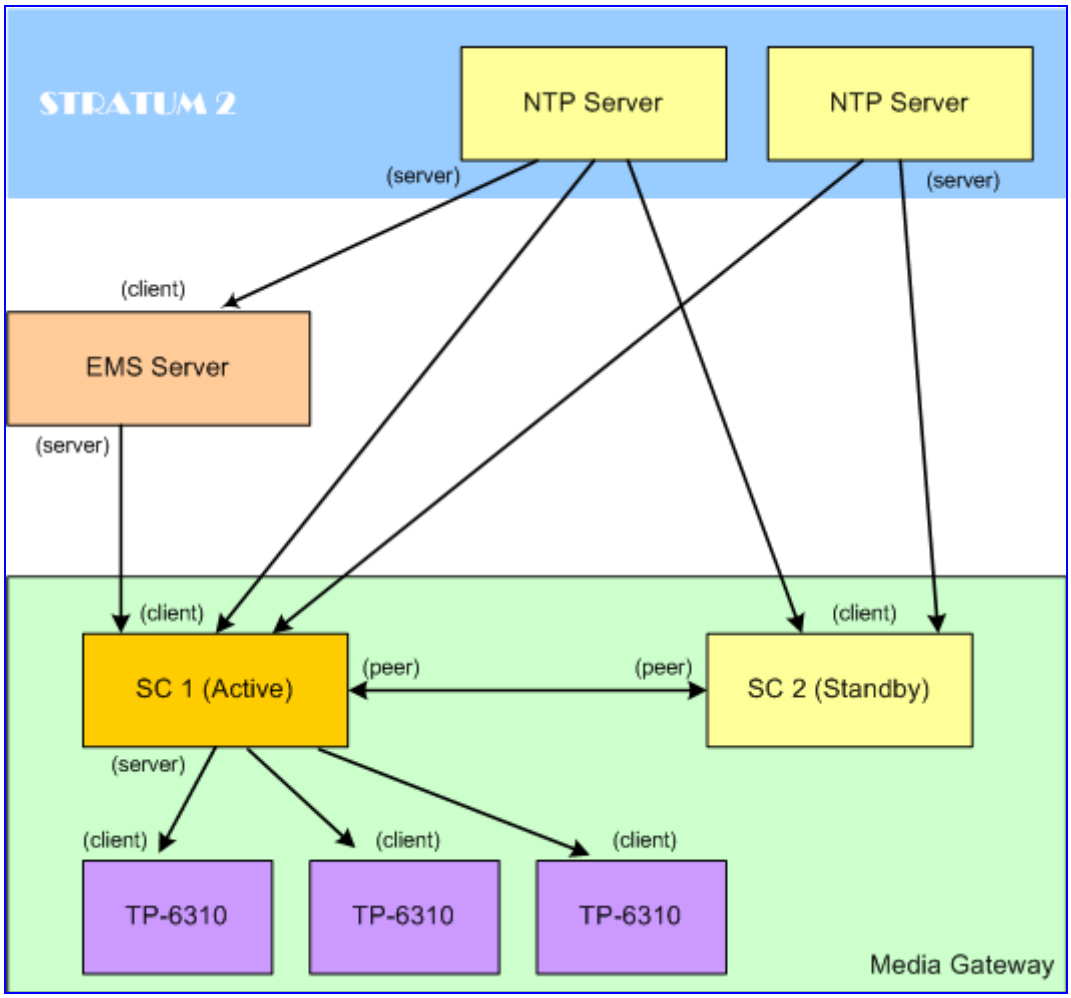
- If there is no “working” connection with any NTP server for more than 7 days, **NTP Server Status** is changed to ***Unsynchronized***.
- When a “working” connection with NTP server is established **NTP Server Status** is changed to Synchronized.

2.7.2 Internal NTP Implementation

The following figure illustrates internal implementation of the NTP service inside the Media Gateway chassis. Note the following:

- The SC boards operate as NTP clients towards the external NTP servers and the EMS server. The SC boards also operate as NTP servers for VoP boards inside the chassis, providing time and date synchronization to the latter.
- Peer connection between the SC boards ensures that time and date inside the chassis is preserved even when the connection to the external NTP servers is not available.
- The SC boards are capable of preserving accurate time and date for 7 days in case of the chassis isolation from external NTP servers.

Figure 2-6: Internal NTP Implementation



2.8 Remote Online Software Upgrade

The Online Software Upgrade is performed when the Mediant 5000 Media Gateway is up and running. Online Software Upgrade upgrades the software on all Media Gateway components, including:

- System Controller boards
- Media Gateway boards
- Ethernet Switch boards

The Media Gateway configuration is preserved throughout the upgrade and the effect on the Media Gateway service is minimized.

After upgrading each major system component (e.g.,the SC or Media Gateway board) the Online Software Upgrade process pauses and allows you to verify the basic functionality of the upgraded component. At these "stop points" you can decide whether to proceed with the upgrade or initiate a roll-back.

The Roll-back functionality enables user to return the Media Gateway to the pre-upgrade software version and configuration in case of any problem.

2.8.1 Hitless Upgrade Mode

Starting from version 5.2, Hitless Upgrade mode is supported for the upgrade of the Media Gateway boards. In this mode, activity switchover is performed between the Active and the Redundant Media Gateway boards. As a consequence, established calls are not affected during the Media Gateway boards upgrade. Calls that have not been established may be dropped.

2.8.2 Graceful Shutdown Mode

Graceful Shutdown mode is available for all Media Gateway boards' without any dependency on the Redundant Media Gateway board's availability or any specific configuration. In this mode, each Media Gateway board is upgraded after a definable Graceful Shutdown period. During this period, no new calls are established on the Media Gateway board; however, the remaining active calls are allowed to complete normally. The Graceful Shutdown period ends when either there are no more active calls on the Media Gateway board, or the defined time period ends. If the defined time period ends and there are still active calls, these calls are dropped and the Media Gateway board is restarted.

The Graceful Shutdown period helps to ensure that a negligible number of calls are dropped during a Media Gateway board's upgrade. In any case, the Media Gateway capacity is never reduced by more than a single Media Gateway board's capacity.

2.9 IP to IP Session Border Controller (SBC) Application

The SBC application supports up to 1000 SBC sessions per VoIP Board and provides the following main features:

- LAN and WAN physical Interface separation
- NAT traversal
- VoIP firewall and security for both signaling and media
- Topology hiding
- Routing:
  - IP-to-IP routing translations of SIP, UDP, TCP, TLS (when extensive transcoding is not required)
  - Load balancing and redundancy of SIP servers
  - Routing according to Request-URI\Specific IP address\Proxy\FQDN
  - Alternative routing
  - Routing between different Layer-3 networks (e.g., LAN and WAN)
- Load balancing\redundancy of SIP servers
- Internet Telephony Service Providers (ITSP) accounts
- SIP URI user and host name manipulations
- Coder Transcoding

2.9.1 Support for LAN and WAN Physical Interface Separation

This feature enables the user to physically separate LAN and WAN interfaces for secure installation .The Mediant SBC application supports different internal (private) and external (public) IP networks and Ethernet interfaces, thereby enabling IP-IP sessions to mediate and transcode between 2 legs on different LAN and WAN physical interfaces (with different Media subnets and VLANs).

2.9.2 NAT Traversal

The Mediant 5000 supports NAT traversal, for example, enabling communication with ITSPs with globally unique IP addresses (for LAN-to-WAN VoIP signaling (and bearer), using two independent legs. In addition, it also enables communication for "far-end" users located behind a NAT on the WAN.

2.9.3 VoIP Firewall

The device provides a firewall for VoIP:

- SIP signaling:
  - Deep and stateful inspection of all SIP signaling packets
  - SIP dialog initiations may be rejected based on the values of the incoming SIP INVITE message and other Layer-3 characteristics
  - Packets not belonging to an authorized SIP dialog are discarded
- RTP:
  - Opening pinholes (ports) in the device's firewall based on Offer-Answer SDP negotiations
  - Deep packet inspection of all RTP packets
  - Late rouge detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rouge traffic from the already terminated RTP and SIP context, the VoIP Firewall will prevent this from occurring
  - Disconnects call (after user-defined time) if the RTP connection is broken
  - Black/White lists for both Layer-3 firewall and SIP classification

2.9.4 Topology Hiding

The device supports topology hiding, which limits the amount of topology information displayed to external parties. For example, IP addresses of ITSPs' equipment (e.g. proxies, gateways, and application servers) can be hidden from outside parties.

The device's topology hiding is provided by implementing back-to-back user agent (B2BUA) leg routing:

- Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message.
- Each leg has its own Route/Record Route set
- Modifies SIP To, From, and Request-URI host names
- Generates a new SIP Call-ID header value (different between legs)
- Changes the SIP Contact header to the device's own address
- Layer-3 topology hiding, by modifying source IP address in the SIP IP header

2.9.5 SIP Normalization

The device supports SIP normalization whereby the SBC application can overcome interoperability problems between SIP user agents. This is achieved by the following:

- Manipulation of SIP URI user and host parts
- Connection to ITSP SIP trunks on behalf of an IP-PBX - the device can register and utilize user and password to authenticate for the IP-PBX

2.9.6 SIP Dialog Initiation Process

The device's SIP dialog initiation process handles all incoming SIP dialog initiation requests. This includes SIP methods such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER.

The SIP dialog initiation process consists of the following stages:

- Determining Source and Destination URL
- Source IP Group Classification
- IP-to-IP Routing
- IP-to-IP Inbound and Outbound Message Manipulation

2.9.7 User Registration and Internal Database

The Mediant 5000 allows registrations to traverse the SBC:

- Perform registrations and share the same serving proxy\registrar
- Possess identical SIP and media behavior
- Reside on the same Layer-3 network and are associated with the same SRD

Typically, the device is configured as the user agent's outbound proxy and the device is configured (using the IP2IP Routing table) to route requests received from these Users to the serving proxy and vice versa.

The device manages a dynamic database that is updated according to registration requests that traverse the SBC. Each database entry represents a binding between an AOR and one or more contacts. Database bindings are added upon successful registration responses. For specific registrations, the AOR is obtained from the SIP To header and the contact is taken from the SIP Contact header.

2.9.7.1 Registration Restriction Control

The device provides flexibility in controlling user's registration:

- **Limiting Number of Registrations per Users Group:** You can limit the number of users who can register with the device. This limitation can be applied per source Users Group.
- **Blocking Incoming Calls from Unregistered Users:** You can block incoming calls (INVITE requests) from unregistered users.

2.9.8 SBC Media Handling

Media behavior includes anything related to the establishment, management and termination of media sessions within the SIP protocol. Media sessions are created using the SIP "offer"/"answer" mechanism; if successful, the result is a bi-directional media (RTP) flow (e.g. audio, fax, modem, DTMF). Each offer/answer may create more than one media session of different types (e.g. audio and fax).

Even though the device usually does not change the negotiated media capabilities (mainly performed by the remote user agents), it does examine the media exchange to control negotiated media types (if necessary) and to know how to open the RTP media channels (IP addresses, coder type, payload type etc.).

The device is aware and sometimes active in the offer\answer process due to the following:

- NAT traversal: the device changes the SDP address to be its own address, thereby, resolving NAT problems.
- Firewall and security:
  - RTP pin holes - only RTP packets related to a successful offer\answer negotiation traverse the device: When the device initializes, there are no RTP pin holes opened; each RTP\RTCP packets destined to the device are discarded. Once an offer\answer transaction ends successfully, an RTP pin hole is opened and RTP\RTCP flows between the two remote user agents. Once a pin hole is opened, the payload type and RTP header version is validated for each packet. RTP pin holes close if one of the associated SIP dialogs is closed (may also be due to a lost connection).
  - Late rogue detection - once a dialog is disconnected, the related pin holes also disconnect.
  - Deep Packet inspection of the RTP that flows through the opened pin holes.
- Adding of media functionality to SIP user agents:
  - Transcoding
  - Broken connection

According to the above functionalities, the call can be configured to operate in one of the following modes:

- **Media Anchoring without Transcoding (Transparent):** RTP traverses the device with minimal RTP packet changes (no DSP resources required). This is typically used to solve NAT, firewall, and security issues. In this mode, all the "audio" coders in the received offer are included in the SBC outgoing offer.
- **Media Anchoring with Transcoding:** RTP traverses the device and each leg uses a different coder or coder parameters (DSP resources are required).
- **No Media Anchoring:** The RTP packet flow does not traverse the device. Instead, the two SIP UA's establish a direct RTP/SRTP flow between each another.

2.9.8.1 SRTP-RTP Interworking

The device supports the interworking between SRTP and RTP. The device can also enforce SBC legs to use SRTP\RTP, using the IP Profile parameters:

- SRTP: SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer\answer.
- RTP: SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer\answer.
- Both: each offer\answer is extended (if not already) to two media lines - one RTP and the other SRTP.

If two SBC legs (after offer\answer negotiation) use different security types (i.e., one RTP and the other SRTP), then the device performs RTP-SRTP interworking.

2.9.9 SIP Dialog Admission Control

The device allows you to limit the number of concurrent calls (SIP dialogs). These call limits can be applied per signaling routing domains (SRD) and per users (identified by its registered contact) - for example, limits on the number of concurrent calls, limits on the number of calls per second or other rules. This is especially important for SBC applications where VoIP and Data traffic contend on the WAN throughput, which may be limited by it. For example, DSL WAN access interface is very limited in the uplink. Therefore, by controlling the number of calls allowed, bandwidth can be reserved for Data applications. In addition, this feature can be useful for implementing Service Level Agreements (SLA) policies or preventing DoS attacks from WAN.

The SIP dialog limits can be defined per SIP request type and direction (inbound or outbound). These relate to requests that initiate SIP dialogs and not the subsequent requests that can be of different type and direction. The SIP dialog-initiating request types can include SIP INVITEs, REGISTER, and/or SUBSCRIBE, or it can be configured to include all dialogs. Requests that supersede the defined limit are rejected with a SIP 486 "Busy Here" response.

2.9.10 SBC Conditions

The device enables you to enhance the process of classifying an incoming SIP dialog to an IP Group (based on SIP message conditions). You can define SIP message conditions using the same syntax (match-condition) as for Message Manipulations (for example, header.to.host contains “company”). If a classification rule in the Classification table (using a new field, MessageCondition) is associated with a condition rule, the classification is used only if the classification rule and its associated condition rule are matched.

2.9.11 SBC Message Manipulation

SBC message manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type). Message manipulations are performed only after the classification, inbound manipulations and routing are successfully performed (i.e., manipulations are performed only in the outgoing leg).

2.10 IP-to-IP Routing Application

The Mediant 5000 supports IP-to-IP VoIP call routing (or SIP Trunking). The IP-to-IP call routing application enables enterprises to seamlessly connect their IP-based PBX (IP-PBX) to SIP trunks, typically provided by an Internet Telephony Service Provider (ITSP). By implementing the device, enterprises can then communicate with PSTN networks (local and overseas) through ITSP's, who interface directly with the PSTN. Therefore, the IP-to-IP application enables enterprises to replace the bundles of physical PSTN wires with SIP trunks provided by ITSP's and use VoIP to communicate within and outside the enterprise network, using its standard Internet connection. At the same time, the device can also provide an interface with the traditional PSTN network, enabling PSTN fallback in case of IP connection failure with the ITSP's.

In addition, the device supports multiple SIP Trunking. This can be useful in scenarios where if a connection to one ITSP fails, the call can immediately be transferred to another ITSP. In addition, by allowing multiple SIP trunks, where each trunk is designated a specific ITSP, the device can route calls to an ITSP based on call destination (e.g., country code).

Therefore, in addition to providing VoIP communication within an enterprise's LAN, the device allows the enterprise to communicate outside of the corporate LAN using SIP Trunking. This includes remote (roaming) IP-PBX users, for example, employees using their laptops to communicate with one another from anywhere in the world such as at airports.

The IP-to-IP application can be implemented by enterprises in the following example scenarios:

- VoIP between an enterprise's headquarters and remote branch offices
- VoIP between an enterprise and the PSTN via an ITSP.

The IP-to-IP call routing capability is feature-rich, allowing interoperability with different ITSP's or service providers:

- Easy and smooth integration with multiple ITSP SIP trunks.
- Supports SIP registration and authentication with ITSP servers (on behalf of the enterprise's IP telephony system) even if the enterprise's IP telephony system does no support registration and authentication.
- Supports SIP-over-UDP, SIP-over-TCP, and SIP-over-TLS transport protocols, one of which is generally required by the ITSP.
- Provides alternative routing to different destinations (to another ITSP or the PSTN) when the connection with an ITSP network is down.
- Provides fallback to the legacy PSTN telephone network upon Internet connection failure.
- Provides Transcoding for bandwidth reduction.
- Supports SRTP, providing voice traffic security toward the ITSP.
- IP-to-IP routing can be used in combination with the regular Gateway application. For example, an incoming IP call can be sent to an E1/T1 span or it can be forwarded to an IP destination.

Therefore, the device provides the ideal interface between enterprises' IP-PBX's and ITSP SIP trunks. To facilitate the understanding of the IP-to-IP feature, this section provides a configuration example.

In the IP-to-IP application, SIP Methods\Responses are handled and terminated at each leg independently:

2.10.1 Theory of Operation

The device's IP-to-IP SIP session is performed by implementing Back-to-Back User Agent (B2BUA). The device acts as a user agent for both ends (*legs*) of the SIP call (from call establishment to termination). The session negotiation is performed independently for each call leg, using global parameters, such as coders or using IP Profiles associated with each call leg to assign different configuration behaviors for these two IP-to-IP call legs.

IP transcoding on SIP can be performed via the following two methods:

- Using the SIP B2BUA application, in which the transcoding rules are determined internally.
- Using the IETF RFC 4117 or NETANN (Network Announcement) package for transcoding, in which the transcoding request arrives from the calling (external) application.

If transcoding or RTP-to-SRTP interworking is required, the RTP streams for IP-to-IP calls traverse through DSP channels.

2.11 IP to IP Interconnect Border Gateway Function (I-BGF)

From an IMS/TISPAN architecture perspective, the Session Border Controller (SBC) on the interconnect side is the integration of the Interconnect Border Control Function (I-BCF) and Interconnect Border Gateway Function (I-BGF). The SBC can be "decomposed", meaning the signaling functions can be on a separate hardware platform to the media relay functions i.e. the I-BCF can be physically separated from the Mediant 5000 I-BGF functions. The H.248 profile for controlling BGF in the Resource and Admission Control Subsystem (ES 283 018) is used by the signaling platform to control the media one.

For secure implementation, the Mediant I-BGF application supports different internals (private) and externals (public) IP Networks and Ethernet Interfaces, providing the H.248 IP-IP context capability to mediate and transcode between 2 legs on different LAN and WAN physical Interfaces with different IP Media Subnets and VLANs.

2.12 Message Manipulation

SIP header manipulation enables insertion, removal, and/or modification of SIP headers and parameters. This feature enables the normalization of SIP messaging fields between communicating network segments. For example, it allows service providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or leave their networks for policy or security reasons from a service provider. The manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

SIP messaging manipulation supports the following:

- Addition of new headers,Removal of headers ("Black list") and Modification of header components.
- Deletion of SIP body (e.g., if a message body isn't supported at the destination network this body is removed).
- Translating one SIP response code to another.
- Topology hiding
- Configurable identity hiding (information related to identity of subscribers for example, P-Asserted-Identity, Referred-By, Identity and Identity-Info).
- Apply conditions per rule - the condition can be on parts of the message or call's parameters. See Section 2.9.10 on page 58.
- Multiple manipulation rules on the same SIP message.

2.13 Support Stand-Alone Survivability (SAS)

The Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX; in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the Enterprise internal telephony service at any branch is lost between its offices, and with the external environment. In addition, these failures prevent emergency calls from being made (e.g., 911 in North America). Despite these possible points of failures, the SAS feature ensures that the Enterprise's telephony services (e.g., SIP IP phones or soft phones) are maintained, by routing calls to the PSTN (i.e., providing PSTN fallback).

The maximum number of SAS registered users supported by the board is 2000.

2.14 SIP Emergency Gateway

This feature provides support for E911 to NG911 gateway and ELIN Emergency calls handling. The user can define a list of Emergency numbers, set priority to these emergency calls and change 4XX to 503 for failure. It can also store calls for up to 30 minutes and direct a callback from the Emergency services to the user who made the original emergency call.

Reader's Notes

3 Network Interfaces

The Mediant 5000 offers two types of network interfaces: PSTN and IP. Voice calls can enter and exit over any of these interfaces with full transport mediation between them.

3.1 PSTN Interfaces

The Mediant 5000 provides PSTN interconnection via TDM trunks .

The Mediant 5000 provides one of the following PSTN interfaces:

- PSTN interconnection via STM-1/ Interfaces to SDH Ring interconnection
- PSTN interconnection via OC3 Interfaces to SONET Ring interconnection

  (Either of the above options are via Add Drop Multiplexer (ADM). Refer to the figure, "TP-6310 SDH/Sonet Ring Interface" below.)

  The following SDH/SONET mappings options are provided:

  - DS1->VT1.5->OC3 mapping for NA market.
  - DS3> STS1 > OC3 mapping for NA market.
  - E1->VC12->STM1 for European market.
- 3 T3 Trunks per each TP-6310/T3 blade.
- 42 E1/T1 Trunks per each TP-8410 blade.

3.1.1 PSTN Protocols

The Mediant 5000 supports the following PSTN protocols:

- CAS Protocols
- MF-R1
- MF-R1 (US)
- ISDN Protocols
- SS7 Protocol

  MG provides integrated signaling Gateway functionality for Narrow-band SS7 links, terminating all transport layers up to MTP-3 (MTP-1/MTP-2/MTP-3).

  Voice calls originating from the PSTN interface, are transported to the Mediant 5000's voice-processing mechanism for interconnection to the IP backbones or back to the PSTN backbones.

3.2 TDM Tunneling

The gateway TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the internal SIP routing capabilities of the gateway to receive voice and data streams from TDM spans or individual timeslots, convert them into packets and transmit them automatically over the IP network (using point-to-point or point-to-multipoint gateway distributions). A gateway opposite it (or several gateways, when point-to-multipoint distribution is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite gateway.

3.3 IP Interface

The Mediant 5000 supports VoIP services over Ethernet networks. VoIP may be used for transporting PSTN or cellular compressed calls over an IP backbone. The Mediant 5000 complies with the RTP/RTCP standard (RFC 3550/3551).

The following features are supported on the Mediant 5000 IP Interface

- Interfaces Separation - refer to the section below
- Subnet Separation - refer to the section below
- Static Route Table - refer to the section below
- Virtual LAN (VLAN) Configuration - refer to the section below
- Quality of Service (QoS) Capabilities - refer to the section below

The media gateway intra-system transport is a cPSB-compliant switched Ethernet network, which enables, using RTP/RTCP, voice connections between two voice channels residing on different Media Gateway boards.

3.3.1 IPv6 for Media Streams and Control Signaling

The overall philosophy and fundamental operational paradigm of IPv6 is essentially the same as IPv4: they are both packet networks using hop-by-hop routing, conforming to the end-to-end principle and favoring distributed algorithms wherever possible, however, IPv6 uses 128 bit addresses in place of the 32 bit addresses of IPv4.

Apart from expanding the addressing range so that it will support billions of hosts, IPv6 had a number of other design goals, including:

- Scalable Addressing and Routing
- Improving security and integrating it into the network layer
- Simplifying the IP header format to reduce the processing cost of handling IP packets
- Reducing administration costs
- Allowing for Mobility of hosts and networks
- Making transition from IPv4 to IPv6 easy, avoiding 'flag days'

Third generation wireless systems are likely to be the main drivers for the widespread operational deployment of IPv6. Especially in the Asia-Pacific region, where in the near future there will soon be insufficient IPv4 addresses to allow all the mobile phones that will be dependant on the network to have a globally unique address.

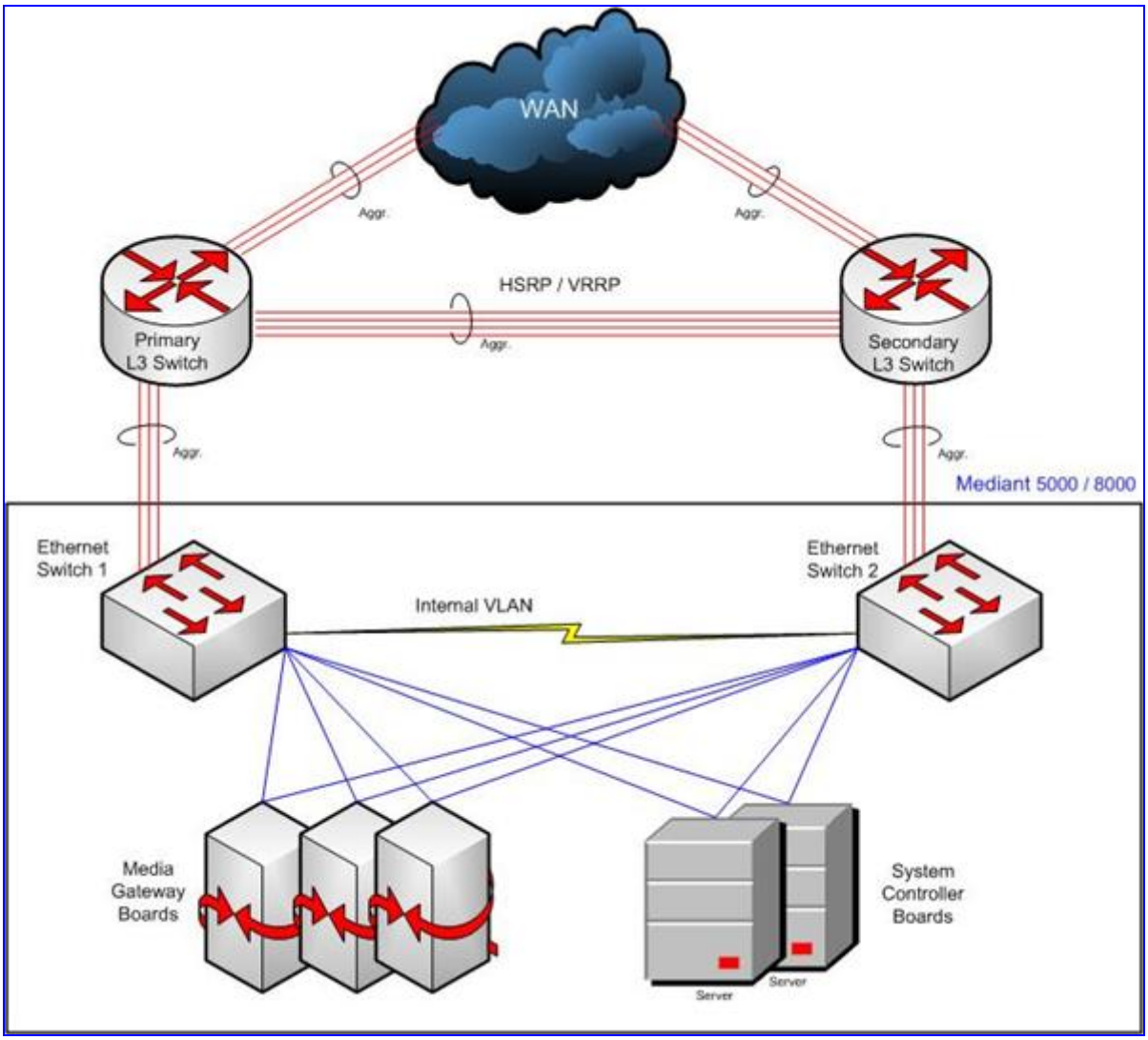
To ease the transition to IPv6, the Mediant 5000 provides ‘dual stack’ IPv4/IPv6 nodes. The IPv4/IPv6 dual stack nodes determine on a per remote node basis, whether to use IPv4 or IPv6 for communication.

3.3.2 Connecting to the IP Network

- **Single Network**

The figure below illustrates the connection method with a single network configuration with a cluster of two interconnected L-3 switches where the Mediant 5000 uplink is connected directly to L-3 switches.

Figure 3-1: Clustering of Two L-3 Switches



- The Media Gateway is connected to the IP backbone via '1+1' Ethernet Switches (ES).
- The two sets of aggregated uplinks of the Media Gateway should be connected to two different L2 networks.
- The L2 networks should have the same default Gateway (IP).Two L3 switches are clustered and recognize the same global IP.
- The L3 switches must be interconnected in layer 2 to provide connectivity between all the network elements.

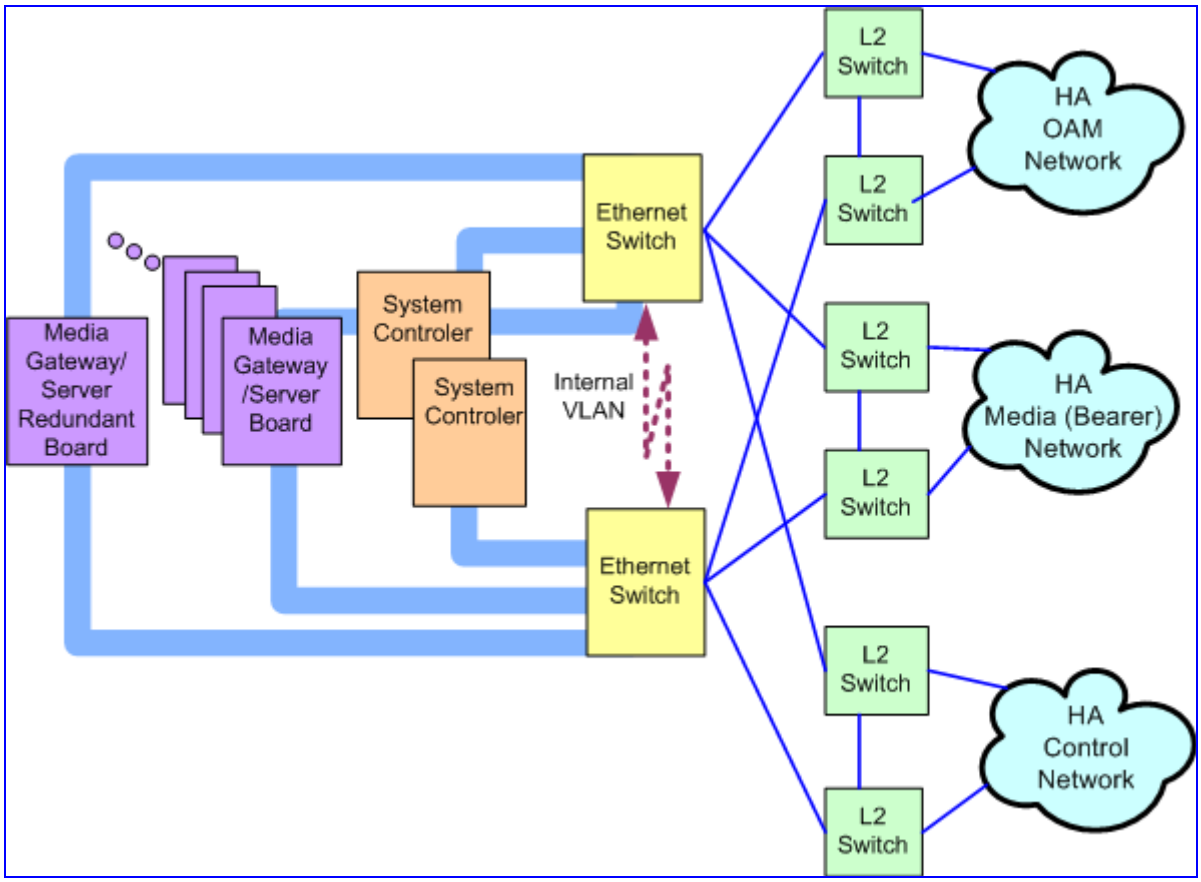
- The L3 switches are clustered using the VRRP / HSRP protocol. Since this connection does not support High Availability, it is recommended to add an extra link to the aggregation.

Note: For ES/6600, the interconnection between the Mediant 5000 and external equipment can be aggregated for media traffic to achieve a maximum 3 Gigabit Ethernet bandwidth.

- **Multiple Networks**

The figure below illustrates the connection method with three separate network configurations. In this case, there are three separate networks for the Media, OAM and Control traffic types (same configuration with OAM, WAN and LAN).

Figure 3-2: Multiple IP Networks



Note: Media Ethernet links can be aggregated into a group of up to three links.

3.3.3 Interface Separation

Interface separation gives the Mediant 5000 the ability to protect each of the Interfaces independently against malicious attacks, by assigning a Firewall or any other Server for protecting the applications running behind these specific Interfaces.

The Mediant 5000 supports between 1 to 3 separate Physical Interfaces as uplinks to the IP cloud. These Interfaces are differentiated according to system protocols mapping.

All protocols supported by the Mediant 5000 can be mapped into one of the following groups:

- Operation Administration and Maintenance protocols like SNMP, Telnet, FTP, HTTP, etc. are mapped into the OAM group.
- Control protocols like H.248, MGCP, TGCP, and SIP are mapped into the Control group.
- Media protocols like RTP, RTCP, etc. are mapped into the Media group.

According to the above protocols mapping, the Mediant 5000 could be configured to any of the following 6 Interface scenarios:

Table 3-1: Four Interface Scenarios

Interface Scenario	Configuration	Details
1	1 Physical Interface	Carries all OAM, Control and Media packets
2	2 Physical Interfaces	1 Uplink for OAM and Control packets 1 Uplink for Media packets
3	2 Physical Interfaces	1 Uplink for OAM packets 1 Uplink for Control and Media packets
4	3 Physical Interfaces	1 Uplink for OAM packets 1 Uplink for Control packets 1 Uplink for Media packets
5	2 Physical Interfaces	1 Uplink for OAM Control and Media packets on LAN Interface. 1 Uplink for Control and Media packets on WAN Interface.
6	3 Physical Interfaces	1 Uplink for OAM packets on OAM Interface 1 Uplink for Control and Media packets on LAN Interface 1 Uplink for Control and Media packets on WAN Interface

Apart from the above Interfaces, there is an additional mirror port for debugging and maintenance.

3.3.4 Subnets Separation

Media, Control, and Management (OAM) traffic in the Mediant 5000 can be assigned one of the following IP addressing schemes:

- **Single IP address for all traffic** (i.e., for Media, Control, and OAMP).
- **Separate IP address for each of the three traffic types**: The different traffic types are separated into three or more dedicated networks. Instead of a single IP address, the system is assigned with couple of IP addresses subnet masks and Default GWs (complying RFC 1122 - Strong End System Model), each relating to a different traffic type. This architecture enables you to integrate the device into different-networks environment with a focus on security and segregation. Each entity in the system (e.g., SNMP and RTP) is mapped to a single traffic type.
- **Dual IP mode**: One IP addresses is assigned to a combination of two traffic types (Media and Control or OAM and Control), while the other IP addresses are assigned to whichever traffic type is not included in this combination. For example, a typical scenario using this mode, includes one IP address assigned to Control and OAM, and another IP address assigned to Media.

Multi Subnets capacity:

- Up to 3 OAM Subnets.
- Up to 10 Media and/or Control Subnets (e.g. 4 Media and 4 Control Subnets, or 4 Media and 4 Control + Media Subnets).

Note: The number of the Subnets must be greater or equal than the number of Interfaces.

3.3.5 Static Route Table

Apart from the Subnet Separation, the Mediant 5000 maintains a Static Route table. Routes that are explicitly configured and entered into the routing table take precedence over the Default gateway supporting RFC 1122 - Strong End System Model. In the “Strong End System Model”, the routing decision is based also on the source IP Address (Subnet). This allows the user to configure routing rules (static routing rules as well as default gateway) based on the source Subnet/VLAN (or source IP Address).

The Static Route capabilities improve the traffic capacity over the IP network and prevent inefficient routing of RTP and other packets between routers.

3.3.6 Virtual LAN (VLAN) Configuration

Virtual LAN (VLAN) technology, which is defined under the IEEE 802.1q specifications, has allowed enterprises to extend the reach of their corporate networks across the WAN. VLANs enable a LAN to be partitioned based on functional requirements, while maintaining connectivity across all devices on the network. VLAN groups network devices and enables them to behave as if they are in one single network. Data security is ensured by preventing access to the data exchanged between devices of a particular VLAN (within the same network) to non-authorized VLAN users.

Apart from the Interfaces, each of the Subnets indicated above, could be assigned to either a specific VLAN identifier based upon the above protocol mapping, the OAM, Control and Media protocol groups or it can be left untagged.

The OAM can be assigned with up to 3 VLAN tags, Control and/or Media can be assigned with up to 10 VLAN tags. Given the above, the Mediant 5000 could be configured with different VLAN tags with the following limitation:

1. The number of VLANs should be equal or greater than the number of interfaces.
2. The same VLAN tag is not allowed on different physical interfaces.
3. The number of Networks' VLAN tags should equal to the number of subnets.

3.3.7 Quality of Service (QoS) Capabilities

QoS is a necessary strategy in multi-service networks to guarantee the best service to all the applications. As shown in the following sections, Mediant 5000 supports the following techniques:

- RFC 2474, DiffServ in routed networks.
- IEEE 802.1p in switched layer 2 networks

Mediant 5000 has created the following standardized default QoS behavior options in the form of end-to-end network service classes (SC):

Table 3-2: Standardized Default QoS Behavior Options

SC	Target Applications and Services	Tolerance to:		
		Loss	Delay	Jitter
Critical	network-to-network device communications within an administrative domain like heartbeats between routers/switches	Very Low	Very Low	N/A
Network	communications between network devices within one administrative domain like ICMP, COPS, RSVP, DNS, DHCP, BootP, high priority OAM	Low	Low	N/A
Premium	telephony service like RTP media, T.38 Fax over IP, Lawful Intercept or Control protocols	Very Low	Very Low	Very Low
Platinum	Used for Video Conferencing, Interactive Gaming	Low	Low	Low

SC	Target Applications and Services	Tolerance to:		
		Loss	Delay	Jitter
Gold	Used for Voice Streaming, Video on demand Broadcast TV, Video surveillance	Med-Low	Med-High	High
Silver	Used for fast response for TCP and HTTP short lived flows like Credit card transactions.	Low	Low-Med	N/A
Bronze	Used for long-lived TCP, and HTTP flows like Non time-critical OAM&P, Email, Instant Messaging.	Low	Med-High	N/A
Standard	Used for all traffic that has not been characterized into one of the other service classes and for Best effort applications.	Med	High	N/A

The Mediant 5000 supports IEEE 802.1p egress packets marking as well as assignment of packets in ingress and egress queues.

Frames either arrive tagged, or are tagged at the ingress port, with a particular priority placed on the queue, which corresponds to the tagged-priority value. ES6600 maps tagged-frame priority values (0-7) to one of 8 COS queues. The queues provide different levels of frame-priority in the switch. The queues priority cannot be changed.

The following QoS service classes' packets are supported by the Mediant 5000 :

- Network IEEE 802.1p Priority
- Premium Control IEEE 802.1p Priority
- Premium Media IEEE 802.1p Priority
- Gold IEEE 802.1p Priority
- Bronze IEEE 802.1p Priority

Apart from the IEEE 802.1p assignment, Mediant 5000 provides marking capabilities for the following DiffServ (RFC 2474) QoS service classes:

- Network IP DiffServ
- Premium Control DiffServ
- Premium Media DiffServ
- Gold DiffServ
- Bronze DiffServ

3.4 Signaling Gateway Interfaces

The Mediant 5000 Media Gateway provides SS7/SigTran Interworking functionality based on the Internet Engineering Task Force (IETF) Signaling Transport (SigTran) standards. The Mediant 5000 is able to provide transport of narrow-band SS7 messages received from the circuit-switched PSTN over DS-0s (over E1/T1 links) and transport of these messages over IP to a Gateway Controller (MGC).

For SS7/SigTran Interworking functionality, the Mediant 5000 supports the following modes of operation:

- Narrow-band SS7 / SigTran Signaling Functionality.
- ISDN SigTran IUA/DUA Signaling Functionality.
- SS7/MTP2 Tunneling.

3.4.1 Narrow-band SS7 / SigTran Signaling Functionality

For SS7/SigTran Interworking functionality, there are two modes of operations:

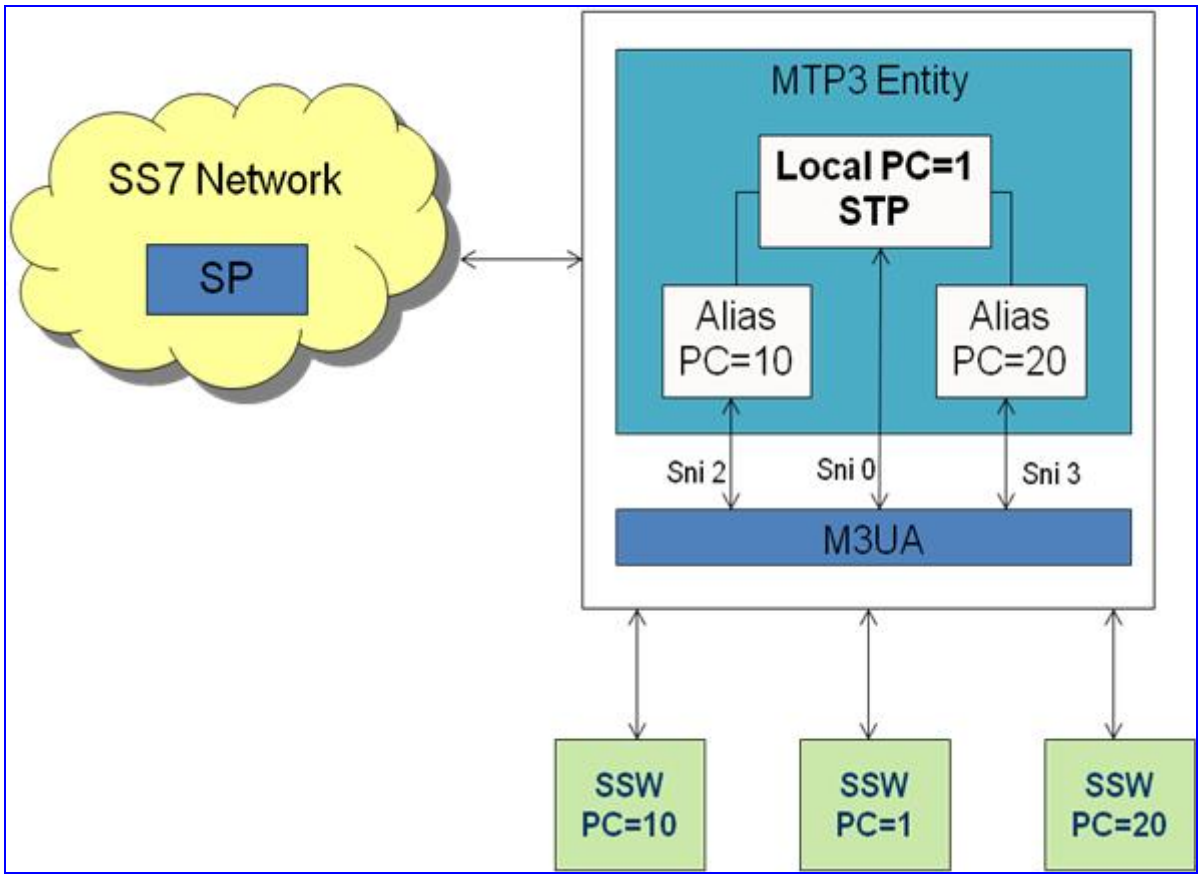
- Mediant 5000 terminates MTP-1/MTP-2 SS7 layers received from the PSTN and transports the SS7 MTP-3 and higher layers (e.g., ISUP, TCAP, MAP, etc.), using the M2UA over SCTP/IP IETF SigTran protocols, to a centrally-located MSC Server. Transferring the MTP-3 layer to a centralized MSC Server or Signaling Gateway reduces the number of SS7 Point Codes required in a network. This is especially useful when taking advantage of the ability to distribute switching using Media Gateways.
- The Mediant 5000 Media Gateway acts as a signaling Gateway for the delivery of SS7 messages over M3UA. All layers of the SS7 Transport protocols, MTP-1, MTP-2 up to MTP-3 are terminated on the Mediant 5000 Media Gateway , and the SS7 ISUP/ SCCP messages are delivered over M3UA/SCTP/IP to the MSC Server. When the Mediant 5000 terminates the MTP-3 layer, an SS7 Point Code is required for the Media Gateway blade and the Higher layers (e.g., ISUP, SCCP/TCAP, etc.) are transferred to a centrally-located MSC Server using the M3UA over SCTP/IP IETF SigTran protocols.

3.4.2 SS7 Alias Point Code Functionality

An SS7 Alias Point Code is an SS7 address that is shared by several systems supporting the same functions. It allows other SS7 systems to address the function instead of maintaining the status of multiple point codes [see T1.711-1999].

The Mediant SS7 Alias Point Code feature provides the capability to route signaling messages with a Destination Point Code (DPC) that is different to the Local Point Code (PC), from the TDM network to the IP network. See diagram below.

Figure 3-3: SS7 Point Code Alias



3.4.3 ISDN SigTran IUA/DUA Signaling Gateway

The Media Gateway provides IUA/DUA Interworking functionality based on the Internet Engineering Task Force (IETF) Signaling Transport (SigTran) standards. The Mediant 5000 is able to provide transport of ISDN Q.931 or DPNSS-L3 messages received from the ISDN PRI, over the Data Link and transport of these messages over IP to the Soft switch or to a Media Gateway Controller (MGC).

3.4.3.1 IUA/SigTran Interworking, Mode of Operations

In an IUA Signaling Gateway , the Mediant 5000 terminates the ISDN layer 2 (Q.921) and transports the ISDN layer 3 messages (Q.931), using the IUA over SCTP/IP IETF SigTran protocols to a centrally-located MGC.

An incoming signaling message coming into the Mediant 5000 from the ISDN network goes through the PRI Data Link and Q.921 Layer 2 protocol. The Q.931 Protocol messages are then relayed to the Media Gateway Controller (MGC), using IUA over SCTP/IP. The MGC initiates SCTP and IUA layers on its side and then completes the upper signaling layers. The reverse direction is applied similarly.

3.4.4 SS7/MTP2 Tunneling

The Mediant 5000 Media Gateways can be used to deploy MTP2 tunneling over IP backbone between the SS7 Legacy network and the Signaling Gateway.

MTP2 tunneling means transferring SS7 MTP2 link data over IP, while both sides of the link are pure TDM sources and are unaware of the IP tandem that is used between them.

In the figure below, each SS7 TDM switch 'feels' that the SS7 link is a point-to-point connection and that each SS7 message sent from one side arrives to the other side without any intervention.

Our solution is composed of two Mediant 5000 systems: one at the "remote" SS7 TDM switch, and one at the "Central" SS7 TDM switch. The figure below illustrates the general concept of MTP2 Tunneling.

Nodal Tunneling Endpoint comprises of the following features:

- MTP2 towards the SS7 TDM switch
- M2UA SG towards IP network
- SCTP is used to increase reliability of transmission over IP toward the remote side
- Several links from several remote Endpoints may be concentrated on one central Endpoint
- No proprietary protocol elements are required on this Endpoint

Remote Tunneling Endpoint comprises of the following features:

- MTP2 towards the SS7 TDM switch
- M2UA MGC side toward IP Network
- SCTP is used to increase reliability of transmission over IP toward the central side
- Proprietary application:
  - Transmits traffic from MTP2 to M2UA MGC and vice versa
  - Controls the maintenance operation of both sides according to network and internal events

3.5 Control Interface

The Media Gateway is part of the VoIP solution in the network. The Softswitch sends various control messages to the different sub-systems connected to the network. As a result, many scenarios can be generated. The Mediant 5000 can be controlled from a Media Gateway Controller (MGC) using standard MGCP (Media Gateway Control Protocol), TGCP (Trunking Gateway Control Protocol), MEGACO (Media Gateway Control) protocol, or SIP (Session Initiation Protocol).

3.5.1 MGCP Control Protocol

MGCP (Media Gateway Control Protocol) is a standard-based network control protocol (based on the IETF RFC 3435 and RFC 3660 located on the IETF web site). MGCP assumes a call control architecture where the call control intelligence is outside the device and handled by an external Call Agent. MGCP is a master/slave protocol, where the device is expected to execute commands sent by the Call Agent(another name for MGC).

3.5.1.1 Supported MGCP Packages

Events and signals are grouped in packages within which they share the same namespace, which we refer to as event names in the following. A package is a collection of events and signals supported by a particular endpoint-type. Among the MGCP client packages supported by the Mediant 5000 are:

- DTMF
- RTP Package
- CAS Packages
- Fax Package Definition
- Media Format Parameter Package
- Extended line Package
- Announcement Package
- Trunk Package
- Generic Package
- Signal List Package
- Support for RFC3264 (caller/called)

Note: For more information, refer to the Programmer's User Manual, document # *LTRT-962xx*.

3.5.2 TGCP Control Protocol

TGCP (Trunking Gateway Control Protocol) is a standards-based PacketCable's network control protocol based on the PacketCable Network-Based Call Signaling (NCS) specification and Media Gateway Control Protocol (MGCP) IETF RFC 3435 and input generated by the PacketCable PSTN Gateway focus team. TGCP assumes a call control architecture where the call control intelligence is outside the device and handled by an external Call Agent. TGCP is a master/slave protocol, where the device is expected to execute commands sent by the MGC.

3.5.2.1 Supported TGCP Packages

Events and signals are grouped in packages within which they share the same namespace, which we will refer to as event names in the following. A package is a collection of events and signals supported by a particular endpoint-type. The Mediant 5000 TGCP client supports PacketCable ISUP Trunk (IT) Package as well as other proprietary TGCP packages.

The Mediant 5000 TGCP client supports the following PacketCable Event Packages:

- ISUP Trunk Package (IT)
- MF FGD Operator Services Package (MO)
- MF Terminating Protocol Package (MT)

Note: For more information, refer to the Programmer's User Manual, document # *LTRT-962xx*.

3.5.3 MEGACO Control Protocol

MEGACO (Media Gateway Control) Protocol is a standards-based network control protocol (based on IETF RFC 3015 and ITU-T H.248). MEGACO assumes a call control architecture where the call control intelligence is outside the device and handled by an external Media Gateway Controller (MGC). MEGACO is a master/slave protocol, where the device is expected to execute commands sent by the Call Agent (another name for MGC).

3.5.3.1 Support for Megaco Virtual Gateways

The nameMediant 5000 offers Virtual gateway functionality for MEGACO Media Gateway boards (according to the H.248.1 spec, section 11.1 "Multiple Virtual MGs"). Each VoIP board can be represented to the IP cloud as up to 3 different gateways, when each Virtual gateway autonomously registers and operates against its controlling MGC. This way, the user can see a single VoIP board as a number of Gateways or Media Servers.

Each Virtual Gateway has individual MGC lists (one Active and several Redundant) and maintains its own connectivity state. Each Virtual Gateway may be connected on different control networks/VLAN and run over different transport layers (UDP/TCP/SCTP).

3.5.3.2 Supported MEGACO Packages

Events and signals are grouped in packages within which they share the same namespace, which we will refer to as event names in the following. A package is a collection of events and signals supported by a particular endpoint-type. Among the MEGACO client packages supported by the Mediant 5000 are:

- Generic Media Package
- Base Root Package
- Tone Generator Package
- Tone Detection Package
- DTMF Generator Package
- DTMF Detection Package
- Call Progress Tones Generator Package
- Call Progress Tones Detection Package
- Basic Continuity Package
- Network Package
- RTP Package
- TDM Circuit Package
- Generic Announcement Package
- Expanded Call Progress Tones Generator Package
- Basic Service Tones Generation Package
- Expanded Services Tones Generation Package
- Basic CAS Package
- R2 CAS Package
- MF Generator Package
- MF Detection Package
- Inactivity Timer Package
- Basic Call Progress Tones Generator with Directionality Package
- Call Type Discrimination Package
- IP Fax Package
- Basic CAS addressing package
- Robbed bit signaling package
- Operator services and emergency services package
- Application Data Inactivity Detection Package (H.248.40)

Note: For more information, refer to the Programmer's User Manual, document # *LTRT-962xx*.

3.5.3.3 E911 (H.248-25) Support

E911 is the North American emergency phone service. A 911 call is routed to the PSAP - Public Safety Answering Point. A 911 call must carry the caller ID with it, to enable locating the caller. Also, typically a 911 call can be released only by the 911 operator. This function is called "operator hold".

The USA government requires E911 support from all telephone companies.

In order to support E911, the Mediant 5000 supports the following H.248-25 packages:

- bcas - Basic CAS packages.
- bcasaddr - Basic CAS addressing package.
- rbs - Robbed bit signalling package.
- oses - Operator services and emergency services package

3.5.3.4 H.248 CALEA as defined in PacketCabe

Supporting H.248 Electronic Surveillance Package for implementing CALEA according to PacketCabe PKT-SP-ESP-I01-991230. The CALEA Electronic surveillance capability enables valid media packets sent and received on specific calls, to be replicated and forwarded to the Electronic Surveillance Delivery function.

This replication is done on the network level, in which the original packet is wrapped into a new envelope, including in it the CCCID. The CCCID identifies the call by the receiving surveillance authority. This property is a part of the Local Control descriptor.

3.5.4 3GPP IMS Control Protocols

In the IMS Architecture (TS 23.228), media requests are handled by Media Gateway Control Function (MGCF) – IM Media Gateway (IM-MGW) Mn interface. The MGCF acts as a control layer which coordinates operations between the S-CSCF, or BGCF and the IM-MGW. When the S-CSCF requires media processing it sends a request to the MGCF which in turn manages the IM-MGW to invoke the media processing required for media transcoding, anchoring and streaming.

Since the Mediant 5000 is an IMS; IM-Media Gateway , its H.248 includes the Mn interfaces (3GPP TS 29.332).

The following termination types are supported:

- Regular VoIP on IPv4.
- PSTN (TDM)

3.5.5 SIP Application-Layer Control Interface

The Mediant 5000 includes the Session Initialization Protocol (SIP) as an application-layer control protocol for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, media announcements and conferences.

The Mediant 5000 is a part of the distributed VoP solution in the network. It provides end-to-end client-server functionality enabling session setup termination and changes.

The Mediant 5000 operates together with the SIP workhorses as Proxy Servers, Redirect Server, Registrar, as well as SIP end devices as User Agents (Clients and Servers).

SIP invitations are used to create sessions and carry session descriptions that enable participants to agree on a set of compatible media types. SIP uses elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies and provide features to users. SIP also provides a registration function that enables users to upload their current locations for use by proxy servers. SIP, on the Mediant 5000 , complies with the IETF (Internet Engineering Task Force) RFC 3261 (refer to www.ietf.org/rfc/rfc3261.txt?number=3261

3.5.5.1 Mediant SIP Features

- Compliant with SIP (RFC 3261)
- Reliable User Datagram Protocol (UDP) transport, with retransmissions
- Transmission Control Protocol (TCP) Transport layer
- SIPS using TLS
- T.38 fax with superior performance (handling a round-trip delay of up to nine seconds)
- Works with Proxy or without Proxy, using an internal routing table
- Fallback to internal routing table if Proxy is not responding
- Proxy or Registrar Registration
- Single Gateway Registration or multiple Registration of all Gateway endpoints
- Proxy and Registrar Authentication (handling 401 and 407 responses) using Basic or Digest methods, Proxy or Registrar Registration
- Supports domain name resolving using DNS NAPTR and SRV records for Proxy, Registrar and domain names that appear in the Contact and Record-Route headers
- Supported methods: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, UPDATE, NOTIFY, PRACK and SUBSCRIBE
- Modifying connection parameters for an already established call (re-INVITE)
- Working with a Redirect server and handling 3xx responses
- Early Media (supporting 183 Session Progress)
- PRACK reliable provisional responses (RFC 3262)
- Supports RFC 3327, Adding 'Path' to Supported header
- Supports RFC 3711, Secured RTP and Key Exchange according to <draft-ietf-mmusic-sdescriptions-12>
- Supports RFC 3581, Symmetric Response Routing
- Supports RFC 3605, RTCP Attribute in SDP
- Supports RFC 3326, Reason header
- Supports RFC 4028, Session Timers in SIP
- Supports network asserted identity and privacy (RFC 3325 and RFC 3323)
- Support RFC 3911, The SIP Join Header

- Support RFC 3903, SIP Extension for Event State Publication
- Support RFC 3953, The Early Disposition Type for SIP
- Support RFC 4244, An Extension to SIP for Request History Information
- Supports Tel URI (Uniform Resource Identifier) according to RFC 2806 bis
- Supports ITU V.152 - Procedures for supporting Voice-Band Data over IP Networks
- Remote party ID <draft-ietf-sip-privacy-04.txt>
- Supports obtaining Proxy Domain Name(s) from DHCP (Dynamic Host Control Protocol) according to RFC 3361
- RFC 2833 Relay for Dual Tone Multi Frequency (DTMF) digits, including payload type negotiation
- DTMF out-of-band transfer using:
  - INFO method <draft-choudhuri-sip-info-digit-00.txt>
  - INFO method, compatible with Cisco Gateways
  - NOTIFY method <draft-mahy-sipping-signaled-digits-01.txt>
- Supports "IP address" or "domain name" URL
- Supports RFC 4040, RTP payload format for a 64 kbit/s transparent data
- Can negotiate coder from a list of given coders
- Supports negotiation of dynamic payload types
- Supports multiple ptime values per coder
- Supports RFC 3389, RTP Payload for Comfort Noise
- Supports reception and DNS resolution of FQDNs received in SDP
- Supports RTCP-XR reports publishing according to RFC 3611
- Responds to OPTIONS messages both outside a SIP dialog and in mid-call. Generates SIP OPTIONS messages as Proxy keep-alive mechanism
- Representing trunk groups in tel/sip Uniform Resource Identifiers (URIs) according to <draft-ietf-iptel-trunk-group-04>
- Publishes the total number of free Tel channels in a 200 OK response to an OPTIONS request
- Support for RFC 3310 HTTP Digest Authentication Using (Authentication and Key Agreement (AKA)
- Support for RFC 4458 (Service information URIs for Applications such as Voicemail and Interactive Voice Response)
- Support for RFC 3608 (SIP Extension Header Field for Service Route Discovery During Registration)
- Support RFC 4412 (Communications Resource Priority for the Session Initiation Protocol)
- Support RFC 4411 (Extending the Session Initiation Protocol reason header for Preemption Events)

3.5.5.2 PSTN-to-SIP Interworking

The Mediant 5000 simultaneously supports different variants of CAS and PRI protocols on different E1/T1 spans, PSTN to SIP and SIP to PSTN Called and Calling numbers can be optionally modified.

Supported Interworking Features:

- Definition and use of Trunk Groups for routing IP PSTN calls
- B-channel negotiation for PRI spans
- ISDN Non Facility Associated Signaling (NFAS)
- Configuration of Numbering Plan and Type for IP ->ISDN calls
- PRI to SIP interworking according to <draft-ietf-sipping-qsig2sip-04.txt>
- PRI to SIP Interworking of Q.931 Display (Calling name) information element
- PRI (NI-2, 5-ESS) to SIP interworking of Calling Name using Facility IE in Setup and Facility messages
- Interworking and flexible mapping of PSTN to SIP release causes
- Interworking of ISDN redirect number to SIP diversion header (according to IETF <draft-levysip-diversion-05.txt>)
- Optional change of redirect number to called number for ISDN IP calls
- Interworking of ISDN calling line Presentation & Screening indicators using RPID header <draft-ietf-sip-privacy-04.txt>
- Interworking of Q.931 Called and Calling Number Type and Number Plan values using the RPID header
- Supports ISDN en-block or overlap dialing for incoming Tel IP calls
- Supports routing of IP Tel calls to predefined trunk groups
- Supports a configurable channel select mode per trunk group
- Supports various number manipulation rules for IP ->Tel and Tel-> IP, called and calling numbers
- Supports ISDN PRI Setup and Facility messages tunneling over SIP INVITE and INFO messages
- Supports ISDN PRI messages tunneling over SIP messages according to RFC 3372 - SIP-T
- Interworking of Redirect Number for QSIG to SIP calls
- Interworking of ISDN Connected number to SIP P-Asserted-Identity header
- Interworking of Calling and Called Subaddress values for SIP'ISDN and ISDN'SIP calls
- Supports QSIG Call Re-Route
- Supports QSIG MWI Notifications
- Supports QSIG messages tunneling over SIP according to <draft-elwell-sipping-qsig-tunnel-03>

Note: For more information, refer to the Programmer's User Manual, document # *LTRT-962xx*.

3.5.6 V5.2 LE Access Gateway

The Mediant V5.2 Access application aggregates legacy circuit-switched voice from the subscriber side, converts V5.2 protocol messages to the H.248 IP protocol and then sends them to a Soft switch and vice versa (The Soft switch replaces the traditional Class 5 switch).

V5.2 System Capabilities:

- Mediant 5000 - <CAP138410M5K> Blades: TP-8410 blades, running as N+1 redundancy mode.
- V5 Links: Each TP-8410 blade may have on its TDM side, up to 42 E1 trunks configured as V5 links.
- V5 Interfaces: These E1 trunks (or V5 links) are divided into groups or V5.2 interfaces of 2-16 E1s each. There may be up to 30 V5 interfaces per board.
- Signaling Channels: A V5 interface uses 2 timeslots for signaling (active and standby) in different V5 links called Primary and Secondary links. In both signaling links, the timeslot 16 is dedicated to the V5 signaling.
- Voice Channels: The number of simultaneous calls in a V5 application is derived from the number of timeslots available for voice, after subtracting the signaling channels.
- User Ports: A V5 Application supports around 14,800 PSTN user ports per board, distributed among the V5 interfaces so that each interface may have up to 4,800 user ports.

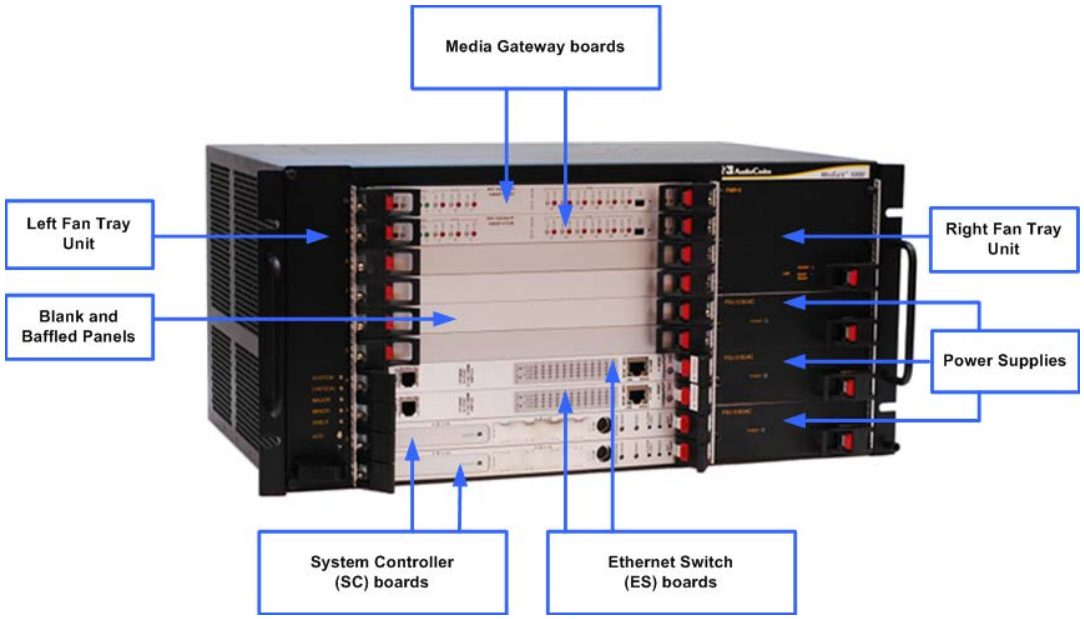
Reader's Notes

4 Mediant 5000 Hardware Elements

The Mediant 5000 is offered with the following hardware configuration:

- Mediant 5000+ TP-6310 boards - Redundant configuration
- Mediant 5000 + TP-8410boards - Redundant configuration

Figure 4-1: Mediant 5000 Front View



4.1 Mediant 8000 + TP-6310 Board Configuration

The table below details the components of the Mediant 5000 + TP-6310 Boards configuration.

Table 4-1: Components of the Mediant 5000 + Mediant 5000 Boards Configuration

Component	Redundant Configuration
Chassis	1
SC (System Controller)	2
SA/RTM (Synchronization and Alarm Rear Transition Module)	2
ES/6600 (Ethernet Switch Board - 24 Gigabit Ethernet)	2
ES/6600/RTM (Ethernet Switch 7 I/O Rear Transition Module)	2
@@BOARDNAME Media Gateway Boards	3+1 or 2+2 = 4*
6310/RTM (TP-6310 I/O Rear Transition Module)	3 or 2*
6310/RTM/Redundant (TP-6310 I/O Rear Transition Module – Redundant)	2 or 1*
PS/AC/5K or PS/DC/5K Power Supply Modules	3
PEM/DC/5K or PEM/AC/5K Power Entry Modules	2
FML/5K and FMR/5K Fan Tray Modules	2
AF/5K Air Filter	1
FPM-5/52/DC or FPM-5/52/AC Fan Power Modules	2

* up to 2 redundancy groups can be configured in the Mediant 5000(each group with a designated 6310/RTM/Redundant board).

4.2 Mediant 8000 + TP-8410 Board Configuration

The table below details the components of the Mediant 5000 + TP-8410 Boards configuration.

Table 4-2: Components of the Mediant 5000 + Mediant 5000 Boards Configuration

Component	Redundant Configuration
Chassis	1
SC (System Controller)	2
SA/RTM (Synchronization and Alarm Rear Transition Module)	2
ES/6600 (Ethernet Switch Board - 24 Gigabit Ethernet)	2
ES/6600/RTM (Ethernet Switch 7 I/O Rear Transition Module)	2
Media Gateway Boards	3+1 or 2+2 = 4*
6310/RTM (TP-6310 I/O Rear Transition Module)	3 or 2*
6310/RTM/Redundant (TP-6310 I/O Rear Transition Module – Redundant)	2 or 1*
PS/AC/5K or PS/DC/5K Power Supply Modules	3
PEM/DC/5K or PEM/AC/5K Power Entry Modules	2
FML/5K and FMR/5K Fan Tray Modules	2
AF/5K Air Filter	1
FPM-5/52/DC or FPM-5/52/AC Fan Power Modules	2

* up to 2 redundancy groups can be configured in the Mediant 5000(each group with a designated 6310/RTM/Redundant board).

For more details about Mediant 5000 hardware, see the Mediant 5000 Installation, Operation and Maintenance Manual, document # *LTRT-923xx*.

4.3 The Chassis

The Mediant 5000 chassis conforms to the CompactPCI PICMG 2.0 standards and has a 6U form factor. It features 10 cPCI slots, occupied by System Controller boards, Ethernet Switch boards, Media Gateway boards and corresponding Rear Transition Modules. The boards are inserted from the front and the back and engage the midplane on either side inside the chassis.

Board slots are numbered from one to ten on the left of the card cage in the front of the chassis for identifying board placement. The midplane contains slot keys to match the appropriate board; there are separate slot keys for the ES, SC and TP/IPM boards. This prevents insertion of a board in an incorrect slot.

In addition to the cPCI boards, the Mediant 5000 chassis houses two Fan Tray units facing the front panel of the chassis, one is to the left of the cPCI slots and another to the right. The left fan tray unit houses an extractable air filter and is used for cooling all of the boards in the chassis. The right fan tray is used for cooling the power supply modules. The chassis also holds three Power Supply modules to the right of the cPCI slots (under the right Fan Tray unit).

Table 4-3: Mediant 5000 Version Chassis Dimensions

Dimension	Value
Width	48.3 cm (19 inches)
Height	22.2 cm (8.75 inches)
Depth **With projections** **Without projections**	 36.5 cm (13.7 inch) 30 cm (11.8 inch)
Weight (Fully loaded)	20.45 kg (45.1 lb)

4.3.1 Cooling System

The cooling system of the Mediant 5000 consists of the following hardware components:

- FML-5 Left Fan Tray Module- Fan Tray Unit
- FMR-5 Right -Fan Tray Module Unit

Both of the above components can be easily removed and are hot-swappable.

4.3.1.1 FML-5 Left Fan Tray

The FML-5 Left Fan Tray module is located on the left side of the chassis. It contains five fans (two big and three smaller ones) and a removable filter (located within the fan assembly, immediately inside the perforated grill). The filter features a honeycombed design that prevents RF interference. The left fan tray is used to cool all of the Mediant 8000 boards in the chassis.

Figure 4-2: FML-5 Left Fan Tray Module

4.3.1.2 FMR-5 Right Fan Tray

The FMR-5 Right Fan Tray Module is located on the right side of the chassis. It contains 2 fans and serves as a complementary to the Left Fan Tray Module. The right fan tray is used to cool the power supplies in the chassis.

Figure 4-3: FMR-5 Right Fan Tray Module

4.3.1.2.1 Air Flow

Clean air is drawn in by the fans and passes through the entire set of plug-in front and rear boards residing in the slots, cooling each one. The air exits the Mediant 5000 via perforated vents in the chassis.

Blank panels are used to cover all unoccupied slots (as per the customer's configuration) on both sides of the chassis. The front blank baffled panels are specially constructed to allow optimal air flow within the chassis.

Power is supplied using Power Supplies and Power Entry Modules.

The AC or DC Power System powers the Mediant 5000 from the AC or DC power sources. It consists of the following hardware components:

- PEM/AC/5K or PEM/DC/5K Power Entry Module
- PS/AC/5K or PS/DC/5K Power Supply Module
- FPM-5/52/AC or FPM-5/52/DC Fan Power Module

Power for the Mediant 5000 is typically provided from either AC or DC redundant power feeds.

4.3.2 Power Supply Features

- DC input

  The unit is required to be powered from a -48 V DC grounded DC power systems.

  - Reverse-polarity protected
- AC input
  - Universal 100 to 240 V AC input
  - Power factor correction (AC input)
  - Class B EMI input filter (AC input)
- Active current load sharing on positive outputs (V1 and V2)

4.3.3 Power Entry Modules

The PEM-5/AC and PEM-5/DC Power Entry Modules are used for connecting the Mediant 5000 chassis to the AC or DC power sources. Two PEM modules are installed in the back of the chassis and enable chassis connection to two independent AC or DC power sources. Such connection provides chassis power high-availability in case of AC power source failure.

4.3.4 Power Supplies

The PSU-5/30/AC Power Supply Modules convert wide-range AC input voltage into DC used for local power inside the chassis. The PSU-5/30/DC Power Supply modules convert DC input voltage into DC used for local power inside the chassis.

Power supply units function in a load-sharing configuration to provide necessary voltages and failsafe operation.

Three Power Supply Modules are installed in the front of the chassis – to the right of the cPCI board slots. The AC and DC Power Supply Modules are hot-swappable.

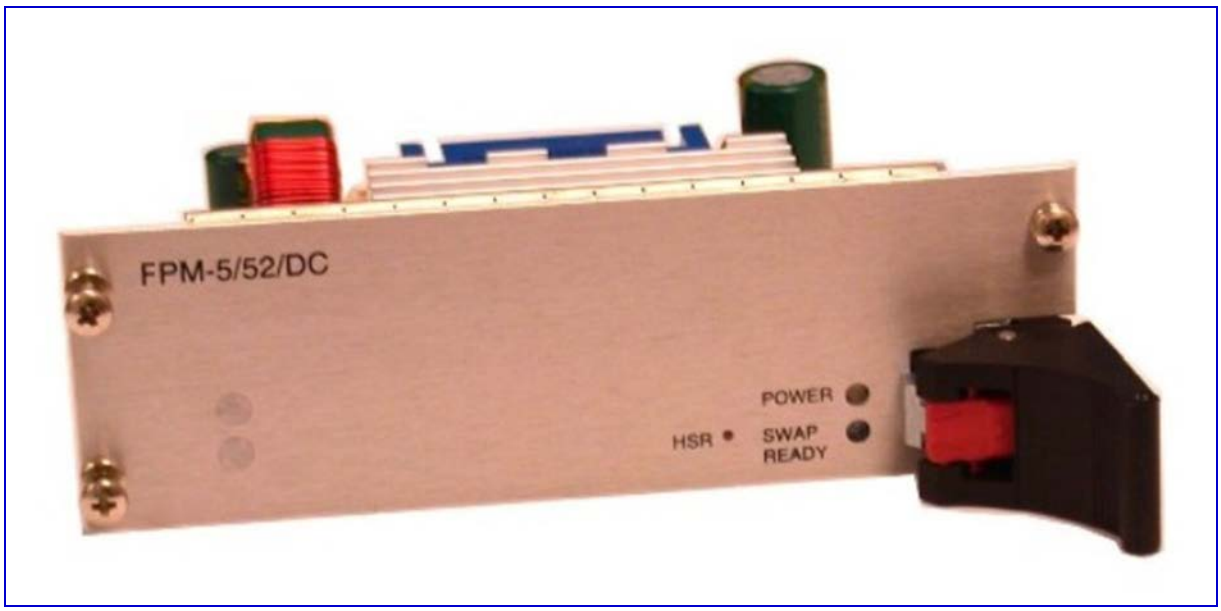
The power supplies shown in the figures below are an advanced-design, multi-output switching power unit, which is provided in AC and DC primary input power configurations.

Table 4-4: PS/ PEM Technical Specifications

Function	Specification
Output	
Output Power	300 watts maximum, continuous
Outputs (V1-V4)	+3.3 V at 40 A; +5 V at 40 A; +12 V at 5.5 A; -12 V at 1.5A
Controls & Signaling	TTL
General Characteristics	
Efficiency	75% at full load
Safety Standards	EN 60950-1, UL 6050-1
AC Input	
PEM/AC	Power Entry Module for AC
Input	100 to 240 V AC 50/60 Hz 8A MAX
DC Input	
PEM/DC	Power Entry Module for DC
Input	-40.5 to -60 V DC

4.3.5 Fan Power Module DC (FPM-5/52/DC) and Fan Power Module AC (FPM-5/52/AC) -for Mediant 5000 System Configurations

The Fan Power Module DC (FPM-5/52/DC) and Fan Power Module AC (FPM-5/52/AC) are DC and AC power supply for the fan tray unit respectively. Two FPM-5/52/DC or FPM-5/52/AC units are provided for redundant protection. These units are hot-swappable.



4.3.6 Environmental Requirements

The site must satisfy the following environment requirements:

The Mediant 5000 complies with the requirements of GR-63-CORE Issue 2 for network switching systems (NEBS) standard . The system operation is guaranteed under the following conditions.

Table 4-5: NEBS Requirements

Item	Requirement	GR-63 Reference
Extended Short-term Temperature Range for Operation	-5° C to +55°C / 23º F to +131°F	4.1.2
Recommended Ambient Temperature for Operation	+5° C to +40° C / 41ºF to +104ºF	4.1.2
Thermal Shock	-40° C to +25º C / -158° F to 77º F within 5 minutes	4.1.1.1 4.1.1.2
Normal Range Humidity	5 to 90%	4.1.2
Nominal Relative Humidity	70% (wet bulb)	4.1.2
Altitude	-60 to 3048 m (10,000 ft)	4.1.3
Fire Resistance		4.2.3
Drop Test, Packaged	Drop height: 600 mm	4.3.1 (10-25 kg, one person carrying)
Drop Test, Unpackaged	Drop height: 75 mm	4.3.2 (10-25 kg, one person carrying)
Earthquake	Zone 4	4.4.1
Office Vibration	5-100-5 Hz/0.1g, 0.1 oct/minute; 3 axes	4.4.3
Transportation Vibration	5-100 Hz, 0.1 oct/min; 100-500 Hz, 0.25 oct/min	4.4.4
Airborne Contaminants		4.5
Rack Requirements	Telco 19-Inch	
	Space	As per GR-63-CORE Maintenance access 762 mm (2’ 6”) Wiring access 610 mm (2’)

Lightning Protection

In addition to correct earthing, sufficient lightning protection must be included at the site in order to prevent damage to the equipment. Damage to the equipment can result either from a direct strike of lightning or from propagated high voltage surges.

In order to avoid damage caused by lightning surges, installation of equipment should be compatible with Class 3 classification as defined by EN61000-4-5 Annex B, where the surge level may not exceed 2kV.

4.3.7 Main Midplane Characteristics

The main midplane routes all signals and power to and from the plug-in boards residing in the slots, in both the front and rear sections of the chassis.

4.3.7.1 Midplane Keying

Each slot is equipped with a key on the midplane to match the appropriate board type in order to prevent inserting anincorrect board type into the slot.

4.3.8 Alarm Indicators

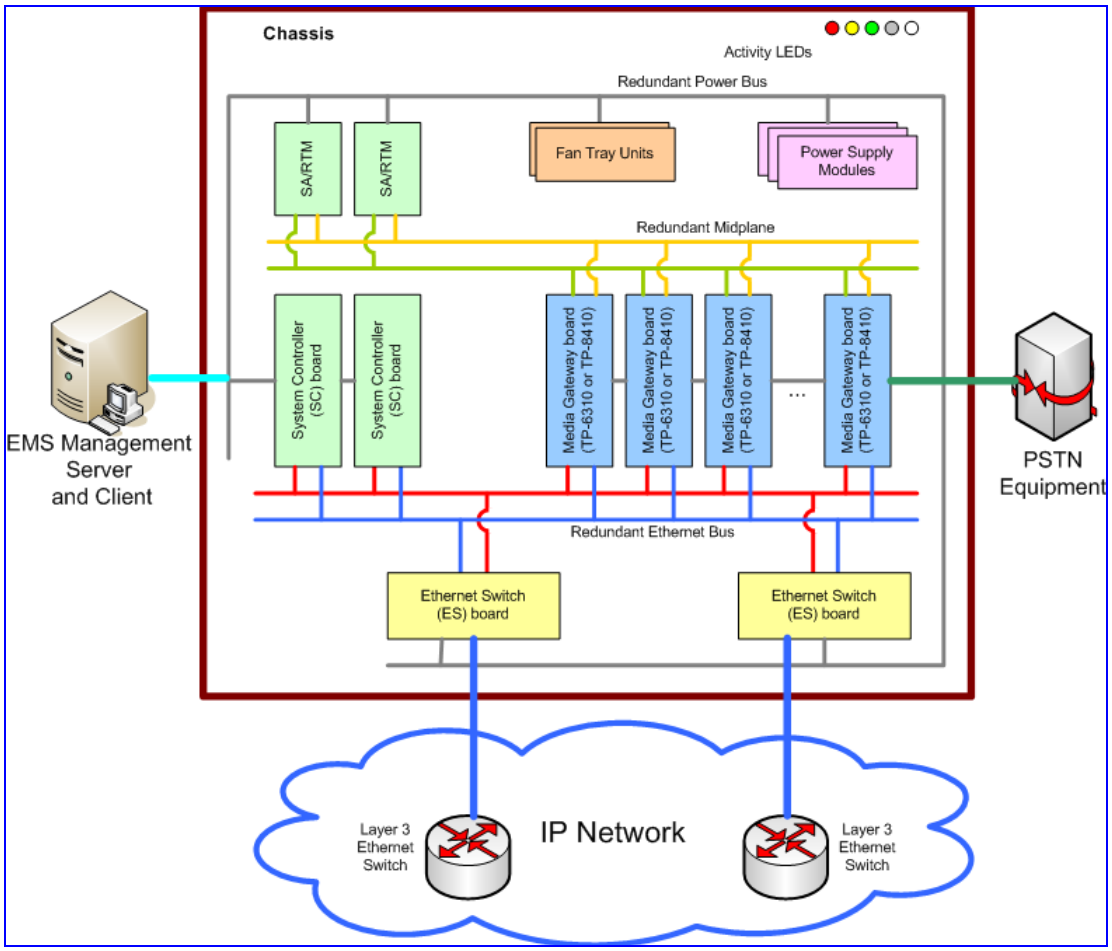
Chassis Alarm Indicators are located on the FML/5K Left Fan Tray Module's front panel. They are used to indicate failure conditions on hardware components – e.g. malfunction of the Fan Tray Module or lack of the power input in a Power Supply.

Indication provided via Chassis Alarm Indicators is very brief and high-level. The EMS management interface is used for obtaining detailed information about the status of each hardware module.

4.4 Boards and Module Architecture

The block diagram of the Mediant 5000 is shown below.

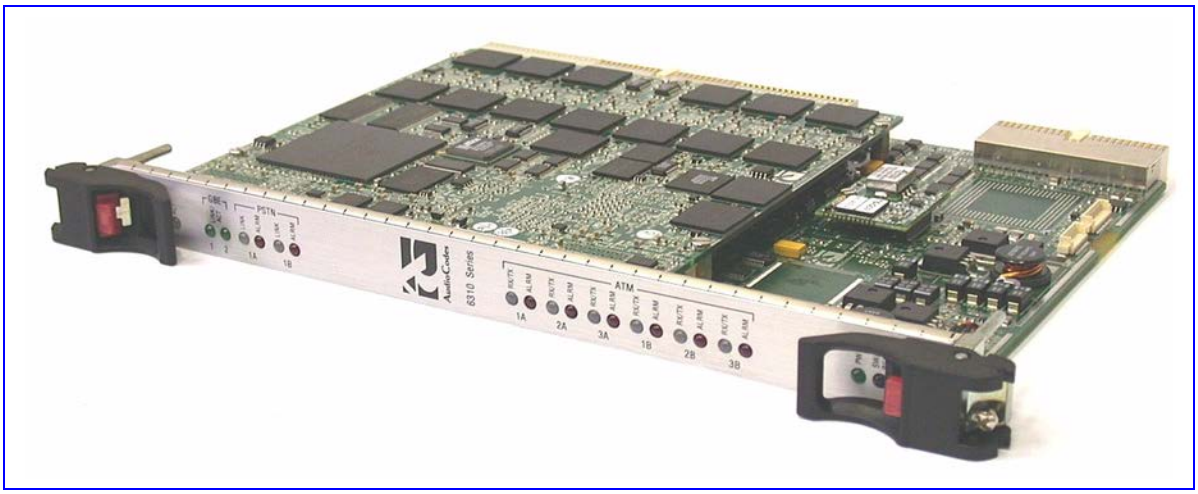
Figure 4-4: Mediant 5000 Block Diagram



4.5 TP-6310 Media Gateway Boards

The TP-6310 board is a member of the 6310 series - TrunkPack VoP communication platform family. The board is a high-density, hot-swappable, resource board with a capacity of 2016 DS0 channels, supporting all necessary functions for voice, data and fax streaming over IP networks. The TP-6310 board provides STM-1/OC-3, PSTN and T3 interfaces via its Rear Transition Module (RTM).

Figure 4-5: TP-6310 Board



4.5.1 6310/RTM Rear Transition Module

The 6310/RTM panel contains Tx and Rx transceivers for the following:

- 1+1 (total 2) PSTN STM-1/OC-3 interfaces
- 3 T3 (DS-3) PSTN interfaces (6 connectors – 3 RX and 3 TX)

Each OC-3 PSTN connection is a cage provided with a slim form pluggable SFP 155 Mbps optical module to connect to an optical fiber with an STM-1/Dual-LC optical connector. The SFP module complies with the INF-8074i - Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA).

To ensure full integrated Automatic Protection Switching (APS) for the PSTN interface, the fiber optic cables must be connected to corresponding PSTN connectors on the 6310/RTM. The PSTN interface is provided with 1+1 protection.

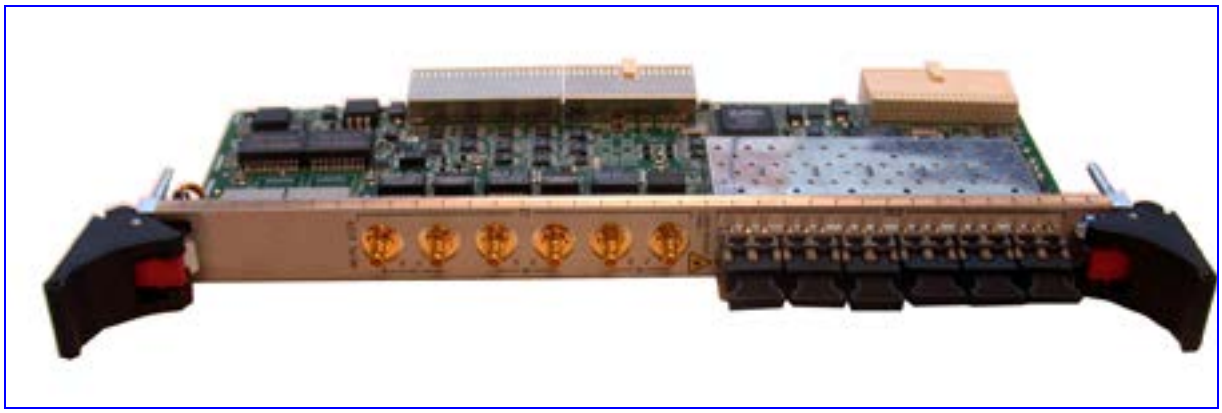
- Each STM-1/ OC-3 PSTN I/O connection is a cage provided with a slim form pluggable SFP 155 Mbps optical module with Tx and Rx transceivers to connect to an optical fiber with an Dual-LC optical connector.

Each T3 PSTN interface port is a mini-SMB connector with Tx and Rx transceivers.The 6310/RTM is designed for protection capabilities and provides a unique Redundant protection functionality. The 6310/RTM/Redundant itself does not provide any PSTN ports. The same redundant RTM should be used for both STM-1 and T3 versions.

Slots 7 to 8 and 11 to 17 are used for up to 9 TP-6310 boards (including the redundant TP-6310 board) according to the customer's requirements. The appropriate rear RTMs are located in the rear cage of the Mediant 8000 Media Gateway in the corresponding slot. The figures below display the panels of the TP-6310 board and 6310/RTM.

For redundant N+1 protection, the 6310/RTM/Redundant Standby board is provided. It contains no port connections and occupies slot 17.

Figure 4-6: 6310/RTM Module



4.6 TP-8410 Media Gateway Board

The TP-8410 board is a high-density, hot-swappable resource board with a capacity of up to 2016 VoP channels, supporting all necessary functions for voice, data and fax streaming over IP networks. It provides the following PSTN interfaces:

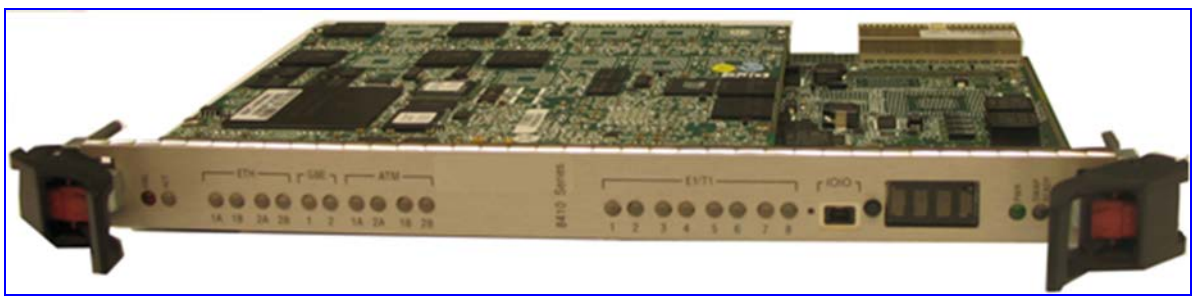
- 42 E1 interfaces with up to 31 channels per trunk (1302 DS0 channels)
- 42 T1 interfaces with up to 24 channels per trunk (1008 DS0 channels)

TP-8410 Media Gateway boards feature N+1 redundant protection which ensures that when specific TP-8410 board fails, all traffic and signaling processed by it is recovered on a designated “redundant” TP-8410 board. The Redundant TP-8410 board must be equipped with a special Redundant RTM that has no PSTN interfaces on it.

The TP-8410 is a member of AudioCodes’ TrunkPack VoP communication platform family. The board providing integrated voice and signaling gateway functionality.

The TP-8410 has a capacity of 2016 VoIP channels and supports 42 PSTN E1 interfaces with up to 31 channels per trunk (1302 DS0 channels in a 7 (6+1) configuration) or 42 PSTN T1 interfaces with up to 24 channels per trunk (1008 DS0 channels in a 7 (6+1) configuration).

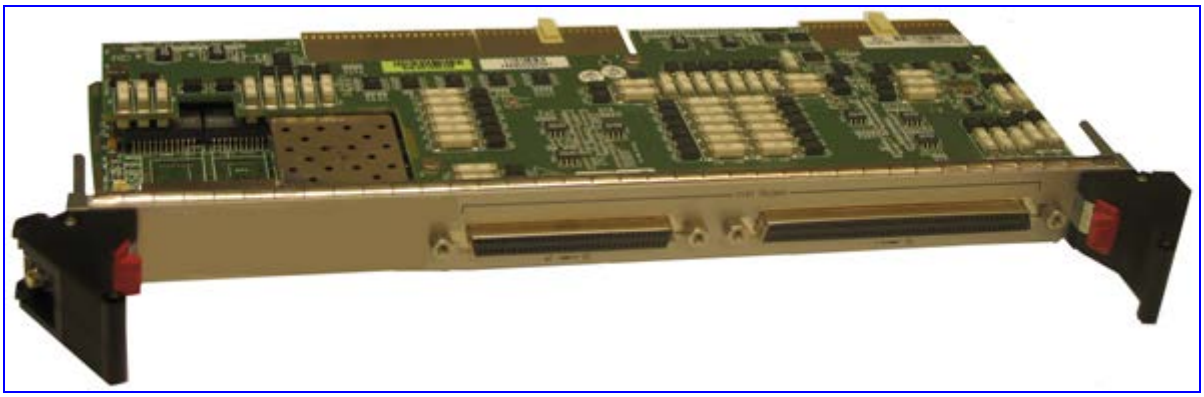
Figure 4-7: TP-8410 Board



4.6.1 8410/RTM Rear Transition Module

The 8410 blade is supplied with rear input/output (I/O) Rear Transition Modules (RTM-8410). The RTM-8410 provides and routes DS1 (E1/T1) PSTN interfaces to the active 8410 blade (in the front panel). The PSTN interfaces are provided by two SCSI connectors per RTM-8410 (100-Pin female SCSI connector and 68-Pin female SCSI connector), supporting up to 42 DS1 (E1/T1) trunks per RTM-8410.

For redundant N+1 protection, the 8410/RTM/Redundant Standby board is provided (occupies slot 17). It contains no port connections and is used for routing PSTN E1/T1 trunks from the failed TP-8410 board to the redundant board.



4.7 System Controller Board

The System Controller (SC) board controls and monitors the Mediant 5000 operation.

Two SC Board types are available, depending on software version and Operating System:

- System Controller - 1 (SC-1) Board
- System Controller - 2 (SC-2) Board

The SC-1 board has equipped the Mediant systems since the first software version. The phase-out process of the replacement of SC-1 with SC-2 has commenced in version 5.8. In version 5.8 and future versions both SC boards will be supported.

The Mediant 5000 contains two SC boards, which are installed into their respective dedicated slots. Each controller contains an on-board hard disk, which stores the system controller software and configuration and performance database.

The SC board is designed according to PICMG standards for high-availability systems. It supports hot-swap operation, system management and environmental monitoring.

The SC's two 10/100 Base-TX redundant Ethernet ports connect the SC board with the two Ethernet Switch boards via cPSB dedicated links in the midplane. The SC's front panel PS2 COM serial port provides an RS-232 console connection.

The SC board is accompanied by an SA (Synchronization and Alarm) Rear Transition Module (RTM) board. The SA board is inserted into the midplane directly behind the main SC board and contains an RS-232 port for connecting to a console terminal.

The SC board provides the hot-swap operation and system management activities required as the result of the alarm reports sent to it by the SA board. The SA Rear

Transition Module assists the System Controller(s) to provide Stratum 3 synchronized clock functionality for gateway synchronization. For more information on the SA/RTM board, refer to 'SA/RTM Synchronization and Alarm Rear Transition Module' on page 99.

4.7.1 System Controller (SC-1) Board

The SC-1 board incorporates a 650 MHz UltraSparc™ processor with 512 MB memory and uses the robust Solaris™ operating system environment enhanced for advanced high-availability features.

Figure 4-8: System Controller (SC) Board and Synchronization & Alarm (SA) RTM

4.7.2 SC-1 Board Major Features

- UltraSparc™ III 650 MHz processor with an on-chip secondary cache
- Solaris™ operating environment
- Integrated dual-redundant channel Fast Ethernet interface
- On-board carrier grade 7/24 40 Gbyte hard disk or a Solid State 32 Gbyte Disk
- 8 kbyte NVRAM
- NEBS compliant
- 2 PMC modules support to expand boards functionality
- Upgradeability support

Table 4-6: SC-1 Board Technical Specifications

Function	Specification
Capabilities	
Processor	650 MHz UltraSparc™ VIS instruction set, binary compatible with SPARC application software
OS Software	Solaris 9 Operating Environment
Cache	L2: integrated 4-way, 512 KB cache
Memory	512 Mbyte on-board EDC (Error Detection and Correction) memory
NVRAM	8 kbyte to save OpenBoot configuration
Interfaces & Transport	
Ancillary ports	PS2 serial RS232 port – for front connection (RS232 serial port on SA - for rear connection) Two 32 MHz x 32-bit
PMC	PMC (PCI Mezzanine Card) slots One slot is occupied with an on-board PMC 40 GB hard disk
IP	Dual-redundant 10/100 Base-TX Ethernet ports
Front Panel controls/ indicators	Reset (POR) and Abort (XIR) pushbuttons Hot Swap Blue LED, Alarm LED, Power LED

4.8 System Controller - 2 (SC-2) Board

The SC-2 board incorporates a Pentium M 1400MHz processor with 2GB cache memory and uses the Linux™ operating system environment supporting full high-availability.

Figure 4-9: SC-2 Board

4.8.1 SC-2 Major Features

- Pentium M 1400MHz with an on-chip 2MB cache
- Linux™ operating environment
- Integrated dual-redundant channel Fast Ethernet interface
- On-board carrier grade 64 GB SSD.
- NEBS compliant
- Upgradeability support

Table 4-7: SC-2 Board Technical Specifications

Function	Specification
Capabilities	
Processor	Pentium M 1400MHz
OS Software	Linux Operating Environment
Cache	2MB
Memory	2GB DDR SDRAM. On-board 64 GB SSD.
Interfaces and Transport	
Auxiliary ports	2xUSB, RS-232, VGA connectors.
IP	Dual-redundant 1GBE Ethernet ports
Front Panel controls/ indicators	Reset Switch. LED indications: Hot Swap Blue LED, Alarm LED, Power LED

4.9 SA/RTM Synchronization and Alarm Rear Transition Module

The SA/RTM Synchronization and Alarm Rear Transition Module is a hot-swappable rear module that is used to complement the SC board. It provides chassis management functionality, utilized by the SC board management software, such as control over the fan trays, monitoring of the chassis voltages etc.

The SA/RTM board may be optionally equipped with a Timing Module that is used to provide clock synchronization on the Media Gateway PSTN interfaces.

Note: To order the SA/RTM board with a resident Timing Module (SA-1/RTM board), refer to the AudioCodes price list.

4.9.1 SA/RTM Overview

Two SA/RTM boards are provided for high-availability and installed in the chassis' rear slots 1 and 2, behind the corresponding SC boards.

The Synchronization and Alarm (SA) is a rear transition module (RTM) designed to be plugged into the rear slots 1 or 2, behind the SC boards. This module provides the chassis management capabilities for the SC boards and the system synchronization to the BITS (Building Integrated Timing Supply) of the CO infrastructure.

The chassis management capabilities are as follows: controlling the fans' operation, monitoring the proper operation of the power supply modules, monitoring the midplane voltages, controlling the chassis temperature, chassis LEDs, pushbutton and the alarm dry contact relay functions. As an I/O extension of the SC functionality, it receives indications regarding the functioning of the chassis elements and reacts with appropriate controlling commands.

The synchronization capabilities are as follows: Sync the IO cards in the chassis to BITS equipment, any of the trunks line clock, Stratum-3 performance, full redundancy in the timing path, synchronization alarms etc.

Each SA board is hot swappable, allowing replacement while the system is active. In addition to the chassis control functionality, it provides an RS-232 and terminal block connectors for connecting to a Telco alarm unit and support two T1/E1 line interface for the BITS interface on each SA/RTM module.

The Synchronization and Alarm module is able to control three dry-contact relays to replicate the gateway's status for minor, major and critical alarms. The connections are made using terminal block connector on the front of the SA/RTM (gateway's rear side).

Three alarm LEDs on the chassis label panel function in a similar way. In the event of a fault condition or an alarm condition, the appropriate chassis LED is activated and the alarm trap is sent over the SNMP protocol.

4.9.1.1 Chassis Management

The following summarizes the SA/RTM chassis management functionality:

- Monitoring all midplane voltages
- Monitoring proper operation of all power supplies
- Monitoring and controlling chassis temperature by changing the fans' speed as a function of chassis temperature
- Monitoring the speed of all chassis fans
- Monitoring the temperature of boards
- Controlling the state of alarm relays
- Controlling the front panel chassis LEDs
- Detecting the state of front chassis push-buttons

4.9.1.2 Chassis Temperature Control

One of the important chassis management functions facilitated by the SA/RTM is to control the gateway temperature. This temperature control is accomplished by adjusting the rotational speed of the fans, thereby keeping the internal temperature at acceptable levels for proper gateway operation. In addition, reducing the fan rotational speed significantly reduces the level of generated acoustic noise.

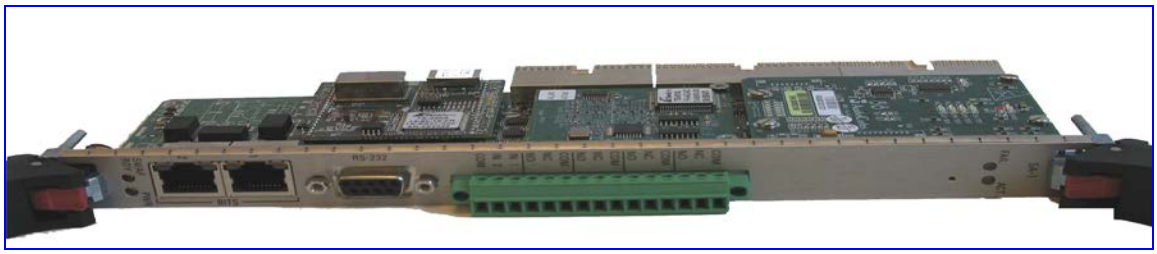
4.9.1.3 Synchronization

The following summarizes the Synchronization functionality that is provided by SA/RTM with the optional Timing Module:

- Integrates two SA/RTM cards to support 1+1 redundancy capability
- Provides Stratum 3 synchronization clock to all Media Gateway synchronous interfaces.
  - Complying with Telecordia GR-1244-CORE and GR-253-CORE Stratum 3.
  - Complying with ITU-T G.813.
  - Free Run accuracy of 4.6ppm.
  - Fully HA with no single point of failure.
- External Clock Synchronization (for TP-8410-1+1 T1/E1/T12 redundancy with no single point of failure):
  - Supporting ITU G.813 options 1 and 2, ETSI EN 300-462-5-1, ANSI SMC T1.105.09 and Bellcore GR-1244-core stratum 3.
  - Supporting the following External Reference input:
    - G.703 E1/T1 External Clock Port (SSM isn't supported);
    - 2048 kHz synchronization signal according to clause 13/G.703 (T12).
    - Output synchronization signals on STM-1/OC3 PSTN lines.

The following figure illustrates the SA/RTM board including the optional Timing Module:

Figure 4-10: SA/RTM board



4.10 Ethernet Switch--ES/6600

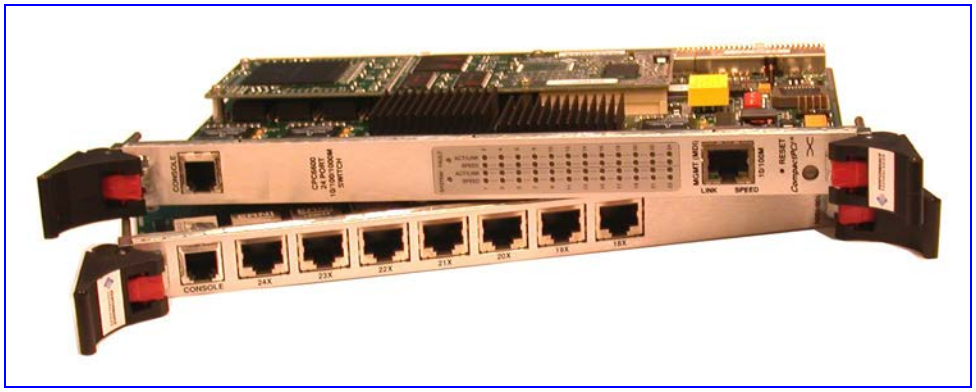
The Mediant 5000 utilizes two Ethernet Switch boards in an active/standby configuration, in which one Ethernet Switch board functions in active mode while the other Ethernet Switch board remains in standby mode. Designed for reliability, the Ethernet Switch maximizes network uptime by continuously checking its status. If a problem is detected, the switch de-asserts all links, signaling the attached devices to use another route. The replacement unit can obtain all of its operational and configuration information from the Ethernet Switch board that has taken over the active mode or from an external manager, making change-out of failed modules a simple matter of sliding one board out and replacing it with a new one.

All of the VoP traffic (media and signaling) is routed between the Gateway (to and from the Media Gateway boards) and the IP network via the Ethernet Switch (ES). Each Media Gateway board communicates with both Ethernet Switches, each via two redundant 100/1000 Mbps cPSB links.

The SC boards communicate with both Ethernet Switches, each via two redundant 100 Mbps cPSB links. This configuration ensures redundant operation protection upon failure of any of the communication elements.

Both ES boards are interconnected according to the PICMG 2.16 cPSB standard in a dual-star configuration, with one ES board in active mode and the other in standby mode. This configuration provides full redundant Ethernet routes to all boards in the chassis. Failure of the active ES board automatically switches the second ES board from standby to active mode. Each of the ES boards has two fiber optic or copper Gigabit uplink interfaces (according to customer preference) for connection to the IP backbone network.

Figure 4-11: ES/6600 Ethernet Switch Board and RTM



The Mediant 5000 utilizes two Ethernet Switch boards in an active/standby configuration, in which one Ethernet Switch board functions in active mode while the other Ethernet Switch board remains in standby mode. Designed for reliability, the Ethernet Switch maximizes network uptime by continuously checking its status. If a problem is detected, the switch de-asserts all links, signaling the attached devices to use another route. The replacement unit can obtain all of its operational and configuration information from the Ethernet Switch board that has taken over the active mode or from an external manager, making change-out of failed modules a simple matter of sliding one board out and replacing it with a new one.

The ES/6600 Ethernet Switch board provides the following features:

- 24 10/100/1000 Mbps cPSB-compliant Ethernet ports (18 are connected to the Mediant 5000 midplane slots, the remainder are for future use)
- Dual 44Gbs switched fabrics
- Advanced Fast Filter Processor for wire speed Layer 2-7 packet classification and filtering
- Support for hardware connection layer of PICMG 2.1 Hot Swap
- Full duplex IEEE 802.3x Flow Control
- 16K MAC addresses (Layer2)
- Managed learning of attached devices on a per-port basis for enhanced network security
- IEEE 802.3ac tagged packet support
- Jumbo packet (9KB) support
- IEEE 802.1p priority queuing (8 classes of service).
- IEEE 802.1q VLAN support (16 VLANs)
- IEEE 802.3-2000 Link Aggregation (up to 12 groups, 8 ports per group)
- Broadcast storm detection and suppression
- Multi-Port Mirroring
- Power-On diagnostics

- Front or rear panel console port (RS-232)
- Single-slot Rear Transition Module provides seven 1000BaseT ports, plus console.

4.10.1 Ethernet Switch-ES/6600 Port Allocation

4.10.1.1 Port Allocation

The ES/6600/RTM provides seven 1000 Base-T ports of the 24 ports for external connection, one of which is configured for connection with the second ES board.

- The OAM and Control Networks uses 100MbE, WAN uses GbE, LAN uses up to 2 GbE copper aggregated links and the Media Network uses up to 3 GbE copper aggregated links.

Table 4-8: Port allocation, Aggregation and Number of Interfaces

Interfaces	One interface: OCM	Two interfaces: OC – M	Two interfaces: O – CM	Two interfaces: WAN – LAN	Three Interfaces O – C– M	Three Interfaces O – WAN – LAN
ES/6600	OCM – 20*	OC – 18 CM – 20*	O - 18 CM - 20*	O + LAN -20* WAN -22	O - 18 C - 19 M -20*	O - 18 WAN - 22 LAN - 20*

Legend;

O – OAM

C – Control

M – Media

4.10.1.2 Port Aggregation

On OCM, OC-M, O-CM and O-C-M Interface Modes:

Up to three port for Media enabled for aggregation fully compliant with IEEE-802.3ad. Allocated ports 20, 21, 22: three options (no aggregation, 20+21, and 20+21+22).

On WAN-LAN and O-WAN-LAN Interface modes:

Up to 2 ports for LAN 20 and 21 enabled for aggregation, fully compliant with IEEE-802.3ad.

20*-If aggregation is enabled (including 21/22)

4.11 Ethernet Switch – ES-2

The Mediant 8000 utilizes two Ethernet Switch boards in an active/standby configuration, where one Ethernet Switch board functions in active mode while the other Ethernet Switch board remains in standby mode. Designed for reliability, the Ethernet Switch maximizes network uptime by continuously checking its status. If a problem is detected, the switch de-asserts all links, signaling the attached devices to use another route. The replacement unit can obtain all of its operational and configuration information from the Ethernet Switch board that has taken over the active mode or from an external manager. This ensures that the replacement of failed modules simply involves sliding one board out and replacing it with the new one.

All of the VoP traffic (media and signaling) is routed between the gateway (to and from the Media Gateway boards) and the IP network via the Ethernet Switch (ES). Each Media Gateway board communicates with both Ethernet Switches, each via two redundant 100/1000 Mbps cPSB links.

The SC boards communicate with both Ethernet Switches, each via two redundant 100 Mbps cPSB links. This configuration ensures redundant operation protection upon failure of any of the communication elements.

Both ES boards are interconnected according to the PICMG 2.16 cPSB standard in a dual-star configuration, with one ES board in active mode and the other in standby mode. This configuration provides full redundant Ethernet routes to all boards in the chassis. Failure of the active ES board automatically switches the second ES board from standby to active mode.

Figure 4-12: ES-2 Ethernet Switch Board and RTM

The ES-2 Ethernet Switch board provides the following features:

- 22 10/100/1000 Mbps cPSB-compliant Ethernet ports (12 are connected to the Mediant 8000 midplane slots, 10 for uplink)
- Support for hardware connection layer of PICMG 2.1 Hot Swap
- Full duplex IEEE 802.3x Flow Control
- IEEE 802.3ac tagged packet support
- Jumbo packet support

- IEEE 802.1p priority queuing (8 classes of service).
- IEEE 802.1q VLAN support (16 VLANs)
- IEEE 802.3ad Link Aggregation (up to 3 GbE copper ports Aggregation)
- Broadcast storm detection and suppression
- Multi-Port Mirroring
- Power-On diagnostics
- Front panel console port (RS-232)
- Single-slot Rear Transition Module provides ten 1000BaseT ports.

4.11.1 Ethernet Switch Port Allocation – ES-2

The ES/ ES-2 /RTM provides seven 1000 Base-T ports of the 22 ports for external connection, one of which is configured for connection with the second ES board.

- The OAM and Control Networks uses GbE, WAN uses GbE, LAN uses up to 2 GbE copper aggregated links and the Media Network uses up to 3 GbE copper aggregated links.

Table 4-9: Port allocation, Aggregation and Number of Interfaces

Interface	Slot Number									
Interface separation	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ONE_O_C_M	OCM	OCM	OCM							Mirror
TWO_O_CAND_M	OC		M	M	M					Mirror
TWO_OAND_C_M	O		CM	CM	CM					Mirror
THREE_OAND_CAND_M	O	C	M	M	M					Mirror
TWO_O_LAN_AND_WAN	OLAN	OLAN			WAN					Mirror
THREE_OAND_LAN_AND_WAN	O	LAN	LAN		WAN					Mirror

Reader's Notes

5 Mediant 5000 Software Architecture

The System Controller (SC) management software performs the system's "housekeeping" tasks, including monitoring the system's components and handling the switchover processes as needed. The SC board contains the software and configuration for the entire chassis components, including booting up the boards and configuring them.

The Mediant 5000 software runs on both of the SC boards (System Controllers) in the system. In the Active SC, the software attaches a 'global IP address' to the SC board. All external entities (Call Agent and Element Management System) communicate with this 'global IP address'.

The two SC boards exchange 'heartbeat' messages at all times. When the Active SC stops sending the 'heartbeat' to the Redundant/Standby SC, it is assumed that the Active SC has failed and the Redundant/Standby SC's software switches or takes over operation. It commences SC functionality by assuming the 'global IP address' of the SC. This way all communication is addressed through the now Active SC and not through the failed SC.

The active SC board controls the Media Gateway boards using a proprietary protocol. It configures the boards and manages the high availability features of the system.

In addition, the active SC board uses SNMP with the Media Gateway boards for polling of Performance Measurement information collected by these boards.

5.1 SC Software Modules

The SC operating system is responsible for the status of all of the boards in the system and the "health" of the system. Its responsibilities include:

- Maintaining the basic software infrastructures
- Maintaining the internal logic of physical and logical objects in the system
- Holding all basic configuration and parameter information about the system
- Providing High Availability (HA) detection and recovery functions
- Supporting data replication for switchover

The figure below illustrates the general software architecture of the Mediant 5000.

Note: For the sake of clarity, several system processes are not included in the figure above.

- **Core Process**

  The 'Core' process is the system's main process, maintaining the system's managed objects (MOs). The 'Core' process contains all configuration parameters and logic of the MOs, and provides these services for the MOs:

  - Access to SNMP

- Persistence (the MOs are saved on disk)
- Replication (the MOs are also replicated to the redundant SC)

- **HBG / HBM**

  The HBG (Heartbeat Generator) generates messages to other SC boards. HBM (Heartbeat Monitor) monitors Heartbeat messages from other SCs as well as from each Media Gateway board.

- **SNMP Agent**

  The SNMP Agent handles SNMP messages from the external EMS using the services of the 'Core' process for handling the messages.

- **SNMP Manager**

  The SNMP Manager manages the Media gateway resident Ethernet Switches. In addition, it extracts Performance Monitor information collected by the Media Gateway boards (for both real-time and history view).

- **TPNCP**

  The TPNCP process runs several threads. Each thread is responsible for TPNCP communication (proprietary protocol) between the SC and one Media Gateway board. In addition, there is a high-priority thread for Media Gateway board switch-over handling. Starting from version 3.0, the internal TPNCP runs on a reliable TCP stack. The TPNCP process is also responsible for handling different error conditions in TPNCP over TCP communication between the active SC and the boards.

- **Watchdog**

  The "Watchdog" process ensures that all processes are running. It shuts down the SC-resident software if one of the processes crashes and causes SC switch-over.

- **BootP**

  The BootP process handles BootP requests. It is used to boot Gateway resident Media Gateway boards. It also communicates with the 'core' process to get configuration information.

5.1.1 Media Gateway Board's Software

The embedded proprietary software of the Media Gateway boards performs necessary Gateway /Server Voice over Packet Functions and Call Control processes, such as Megaco, MGCP, SIP, voice compression, jitter buffering, echo cancellation, voice activation detection (VAD) and comfort noise generation (CNG), tone detection and generation, and announcements. The Media Gateway boards are managed by the SC software using the AudioCodes proprietary media Gateway control protocol (TPNCP).

5.2 Mediant 5000 Hardware and Software Configuration

The configuration concept for the Mediant 5000 is a combination of Media Gateway board Hardware types and Software configuration. Each of the Hardware types provides different channels capacity and numbers of DSPs and PSTN interfaces, while the Software application type run on the Media Gateway board defines the application configuration.

Table 5-1: Media Gateway Board Software Application Types

Application Name *	Description	Media Gateway /Server Board Type
General GW	The regular Gateway application for supporting H.248/ MGCP/ TGCP, PSTN, SS7 etc. This application also provides simple announcements (with simple indexes, constructed by the AC "TrunkPack Downloadable conversion utility").	▪ TP-8410 Hardware Platform to support E1/T1 Trunks ▪ TP-6310 OC-3/STM-1 Hardware Platform to support OC-3 or STM-1 Links ▪ TP-6310 T3 Hardware Platform to support 3 T3 links
SIP GW	The General GW with the addition of the SIP call control protocol.	
General IPM**	The Server application that Supports Audio online provisioning by an APS, to support complex announcement functionality and Interactive Voice Response (IVR), as well as conferencing, Bearer Channel Tandeming (BCT) and Trunks Testing using the H.248/MGCP/TGCP call control protocols.	▪ IPM-6310 OC-3/STM-1 Hardware Platform - a TP-6310-based board with additional DSPs to support OC-3 or STM-1 Links ▪ IPM-6310 T3 Hardware Platform - a TP-6310-based board with additional DSPs to support 3 T3 links
SIP IPM**	The General IPM with the addition of the SIP call control protocol.	

* Application Name as it appears in the EMS.

** For more information on the IPM applications and IPmedia Server functionality, refer to AudioCodes IPmedia related documents.

A mixture of Media Gateway /Server board types on the same Mediant 5000 system is currently not supported.

5.3 Management Interfaces

The Mediant 5000 provides two interfaces for the operation, configuration, maintenance and support tasks of its carrier class Media Gateway:

- Command Line Interface (CLI)
- Element Management System (EMS) GUI

5.3.1 Mediant 5000 Provisioning

The Command Line Interface (CLI) is available via the following management interfaces:

- Telnet
- SSH (Secure Shell)
- RS-232 console

CLI provides a predefined set of commands with a choice of options that comprehensively cover the maintenance tasks required on the media Gateway , including:

- Show status & configuration
- Modify configuration
- Scripting capabilities
- Debugging

All CLI commands are fully documented and are provided with a versatile auto-completion system, activated by pressing the Tab key at any stage while typing the command.

In addition to Gateway -specific commands, complete UNIX shell functionality and standard UNIX command-line utilities are available for use. These utilities can be combined with Gateway -specific commands to accomplish complicated maintenance tasks.

5.3.2 Element Management System (EMS) GUI

The EMS configures and monitors the media gateway using SNMP. It can change the configuration, read status, get real-time or history Performance Monitoring values, and get events through traps.

A comprehensive management API enables efficient management interfaces between the Mediant 5000 components and Element Management System, as well as parallel management systems (such as NMS or OSS). Full feature management and alarm handling are accomplished via this API. As such, the EMS provides full media gateway provisioning and management in contrast to the higher level NMS that can manage, for example, related resources for the Media Gateway Controller and Media gateway.

This level of integration is possible because the configuration of the media gateway is kept in the database within the media gateway. It also allows several managers to change the configuration in parallel. When a configuration is changed, all managers are notified regarding this particular change, thereby being synchronized with the current configuration of the media gateway.

This SNMP agent functioning in the SC board software allows full provisioning of the system (including all boards) and sends traps for alarms that occur in the system. The SNMP API is based on proprietary MIBs that support all VoIP engine functionality. For more information, see 'EMS for Mediant 5000' on page 113.

Reader's Notes

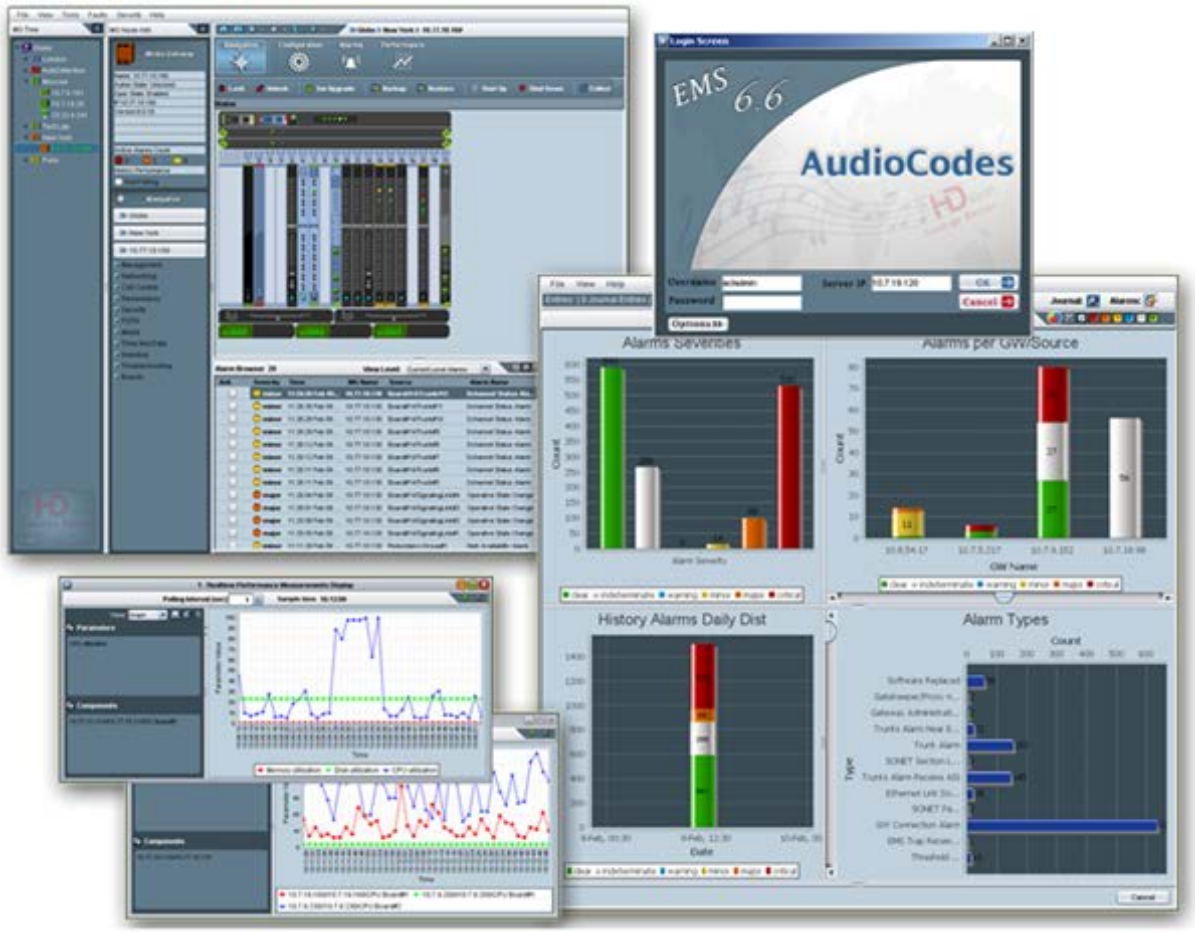
6 EMS for Mediant 5000

The Element Management System (EMS) is an advanced solution for standards-based management of Media Gateways within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of Media Gateways.

The EMS enables System Integrators (SI) the capability to offer customers rapid time-to-market and inclusive, cost effective management of next-generation networks.

The standards-compliant EMS for Media Gateways uses distributed SNMP based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a feature-rich management framework. It supports fault management, configuration and security. The EMS simultaneously manages the full line of multiple digital Media Gateway systems and their modules, as well as the analog VoIP Media Gateway Customer Premises Equipment (CPE).

Figure 6-1: EMS Screens



6.1 EMS Characteristics

- EMS System Characteristics

  The EMS features a Client/Server architecture, enabling customers to access the EMS from multiple, remotely located work centers and workstations.

  The entire system is designed in Java™, based on a consistent, vendor-neutral framework, and following recognized design patterns. Client - Server communication is implemented with Java™ RMI (Remote Method Invocation) protocol over TCP (Transmission Control Protocol).

  The EMS enables multiple work centers and workstations to simultaneously access the EMS server(up to 25 concurrent clients connected to the server).

  EMS Server, running on a Sun™ Microsystems' machine running Solaris™ version 10 or on CentOS Linux (kernel version 5.3). All management data is stored in the server, using Oracle 11g relational database software. EMS Server High Availability is available for EMS Server Applications running on the Linux platform.

  EMS Client, running on Microsoft™ Windows™, displays the EMS GUI screens that provide operators access to system entities. The operator-friendly GUI hierarchical organization and Microsoft™ Explorer™ paradigm increase productivity and minimize the learning curve.

- Versatile System

  The EMS can simultaneously manage all Media Gateway platforms (Mediant 5000 and other Gateways/servers), even while having different software versions running on these Media Gateways.

- Provisioning

  The EMS provides a straightforward provisioning interface to enable smooth equipment setup.

- FCAPS

  FCAPS, is an acronym, of the five key areas defined by the ITU for general management systems functionality, described as follows

  - 'Fault Management' on page 129
  - Configuration Management (see 'Entity Management and Configuration' on page 122)
  - Accounting Management - not applicable
  - 'Performance Management' on page 34
  - 'Security' on page 34

- Open Standard Design

  The open standard design of the EMS allows for a seamless flow of information within and between the layers of the Telecommunications Management Network (TMN) model, in accordance with the International Telecommunications Union (ITU) M.3010. It also enables smooth integration with existing and future network and service (NMS/Network Management System, OSS/Operation Support System) management solutions.

- Multi-Language Support

  The EMS is a globally ready application. It can be adapted to various regions and languages without requiring engineering changes. Locale-dependent data such as dates and currencies appear in formats that conform to the customer's region and language. With the addition of localized (language) data, the same application can be used worldwide. A different locale can be selected per client application.

  The default locale language is English (USA).

- Customizable Features

  The features listed in this subsection can be modified to suit the customer's request, and following customization, a new Client installation disk is provided to that customer.

  - All texts in the application are customizable.
  - Menu bar and popup menu modifications (items can be reordered, separated with separators, or removed from menus).
  - Parameter Provisioning screen modifications (tabs can be reordered or removed from the screen).
  - Status pane navigation buttons can be removed or reordered.

6.2 EMS Specifications

Table 6-1: Element Management System (EMS) Specifications

Subject	Description
TMN Standards	ITU-T Recommendation M.3010 series FCAPS functionality support
Fault Management	▪ Alarm fields and actions, according to ITU-T Recommendation X.733, 3GPP Recommendation 3G TS 32.111-1. ▪ Alarm processing: 30 traps per second, continuously ▪ Alarm archiving: up to six-month history for all Media Gateways (depending on disk size available). ▪ Application includes context-sensitive Alarm Browser and Alarm History with various filtering and search options, detailed alarm description, Acknowledge and Delete actions processing and audio indication on receipt of alarms. ▪ Automatic and Manual Alarm Clearing ▪ Carrier-Grade alarms system performing constant re-synchronization of EMS and managed gateways to ensure that all the alarms are synchronized and up to date. ▪ Combined alarms and journal allow users to correlate possible influence of user actions on systems behavior and alarms. ▪ Alarms reports graphical representation. ▪ Traps Forwarding to the Northbound Interface via SNMP, Mail, SMS or Syslog protocols. ▪ Save alarms in a *csv* file
Media Gateways Automatic Detection and Monitoring	When the MediaPack is connected to the network for the first time, it is automatically detected by the EMS and added to the managed gateways. A Summary of all managed gateways' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.
Media Gateways Provisioning	▪ Adapts rapidly to changes in new Media Gateway software releases. ▪ Based on hierarchy of managed objects concepts. ▪ Online parameter provisioning support, with icons indicating provisioning type. ▪ Profile-based provisioning, including Master Profile for all VoIP gateways and media servers, as well as for the TP-1610, TP-6310 and TP-8410 boards. ▪ Search provisioning parameter ▪ Configuration database of small gateways is kept inside the EMS. ▪ Configuration database of large gateways is kept inside the Media Gateways.

Subject	Description
Security Management	Complies with T1M1.5/2003-007R4 and covers two aspects: Network communication security and EMS application security. The EMS application complies with the USA Department of Defense standard-FIPS 140-2 (FIPS-Federal Information Processing Standards-US Government Security Standards for Cryptography modules) and the JITC (Joint Interoperability Test Command) lab. Encryption and authentication related software are now implemented using FIPS compliant third party software, Therefore, all encryption modules used by the EMS application are FIPS 140-2 certified. **Network Communications Security** EMS server's network is configured and its ports opened during installation. Interoperation with firewalls, protecting against unauthorized access by crackers and hackers. MediaPack, Mediant 1000, Mediant 2000, Mediant 3000 can be managed behind the NAT. EMS client-server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). EMS server - Media Gateway communication is secured using SNMPv2c/SNMPv3, HTTP/HTTPS, Telnet and FTP over IPSec / SSH and SCP. **Application Security** User Management using a Radius server for centralized user authentication and Authorization or in the EMS application. EMS application: Users List. Authentication-based operator access according to user name, password, security level, login machine IP. Modification of user details and access rights, user removal, forced logout, user suspension, releasing users from suspension and user password change EMS application: Actions Journal of operators' activities, various filtering and search options. **EMS Server Hardening** EMS server hardening enables you to harden the Solaris 10 and Linux platforms for enhanced security performance. The hardening protects the EMS server from unauthorized access and hostile attack.
Performance Management	▪ Real-Time Graphics ▪ Historical Data Collection and Analysis

Subject	Description
Session Experience Management	▪ Modular tool with separate views for Network, Statistics, Calls, Alarms and Reports. ▪ Graphic representation of managed devices/links in a Table, Map and Regions view with a popup summary of critical metrics. ▪ Voice quality diagnostics for devices/links and users in the VoIP network. ▪ Real-time, as well as historical monitoring of VoIP network traffic health. ▪ Call quality rating metrics (MOS, jitter, packet loss, delay (or latency) and echo). ▪ Call trend statistics according to key metrics, traffic load, average call duration and call success. ▪ SEM alerts based on user defined call success rate and quality thresholds. ▪ Active alarms and history alarms display. ▪ Monitoring of links quality between AudioCodes and non-AudioCodes devices such as Microsoft Lync 2010 Server. ▪ Filtering according to time range, devicesand links.
Media Gateways Maintenance Actions	Mediant 8000 Media Gateway and Mediant 5000 Media Gateway: ▪ Online software upgrade via a Wizard ▪ Gateway installation, startup and shutdown ▪ All maintenance actions (lock, unlock, switchover, add / remove board, etc.) for each media gateway entity, via a convenient Graphical User Interface. ▪ Various Debug tools allowing collection of the data during the troubleshooting process. Mediant 600, Mediant 800, Mediant 1000, Mediant 2000, Mediant 3000, and MediaPack: ▪ Software files and Regional properties files (such as Voice Prompts, CAS and other files) can be loaded to the set of gateways. ▪ Actions (such as Lock / Unlock, Reset, Configuration Download, Upload, etc.) can be performed to the set of gateways.

Table 6-2: User Interface and External Interfaces Specifications

Subject	Description
User Access Control	Local EMS application or centralized RADIUS / TACACS+ users authentication and authorization.
Northbound Interface	Topology as CSV file, Alarms as SNMP v2c / SNMPv3 traps, PMs as CSV / XML files.
Southbound Interface	SNMPv2c / SNMPv3 , HTTP/HTTPS, SSH, SCP, NTP (possible over IPSec).
Multi-Platform	Java-based, JDK version 1.6.
Relational Database	Oracle *11g* relational database is used for data storage.

6.3 EMS Server Features

This section describes selected features of the EMS server.

6.3.1 Connecting to the EMS Server

The EMS server can be configured with up to four network interfaces (connected to different subnets). You can connect to any one of these four interfaces directly from the EMS client login dialog.

When EMS server High Availability (HA) is implemented, the EMS client login dialog enables you to specify up to two EMS server IP addresses. For more information, see EMS Server High Availability on page 120.

6.3.2 EMS Server High Availability

EMS servers High Availability (HA) is supported for EMS server applications running on the Linux platform.

Two EMS server machines are required to support High Availability. One machine serving as the Primary machine, and the other serving as the Secondary machine. When the EMS application is active and running, all data stored in the EMS server machine and Database is replicated from the Primary machine to the Secondary machine. Upon Primary machine failure recognition (either on the EMS application or on the Network), activity is automatically transferred from the Primary server machine to the Secondary server machine.

Two models of High Availability are supported:

- Regular: both servers are located in the same subnet. A Single EMS server IP address - Global (Virtual) IP address is used for all the Network components (EMS clients and Managed Gateways).
- Geographic: each server is located in a different network subnet and has its own IP address. The user provisions both these IP addresses in the Client login dialog. The EMS client application constantly searches for the currently active EMS server machine.

6.3.3 Virtualized EMS Server

The EMS server, in addition to the regular installation, is delivered as virtual appliance (VMware vSphere Hypervisor™ (ESXi) on the VMware Virtual Servers. The virtual environment allows the IT manager, carriers and all EMS customers to minimize dedicated hardware per application usage, and consequently lead to IT maintenance cost savings.

6.3.4 Disk Mirroring (RAID 1) on Netra T5220

The EMS server machine (Netra T5220 server's on-board SAS controller) can perform disk mirroring for up to two configured RAID volumes. Disk mirroring (RAID 1) is a technique that uses data redundancy; two complete copies of all data stored on two separate disks, to protect against loss of data due to disk failure.

6.3.5 Syslog and Debug Recording

Syslog and Debug recordings from all managed machines can be logged directly to the EMS server without the need for a 3rd party server in the same local network.

6.3.6 EMS Server Management Utility

The EMS server Management tool is a command line utility which enables the user to view information on the EMS server and configure its various components. The utility enables you to perform the following tasks:

- Collect information and logs
- Perform networking actions such as changing the EMS server's IP address and configuring network Interfaces
- Performs security actions such as basic and advanced hardening
- Performs maintenance actions such as backup, restore and reboot

The available menu options differ according to the respective permissions of the EMS server OS users. For more information, see EMS Server OS Users.

The EMS server configuration information is also displayed in the EMS GUI under the Help menu.

6.4 Entity Management and Configuration

6.4.1 Media Gateway /Server Status Summary

The EMS enables operators to navigate down the system's hierarchical layers from the MG Tree and the Status pane to each Trunk, and back up. Regions listed under Globe in the MG Tree expand to display the Media Gateways under them. These same Media Gateways are also displayed in the MGs List pane. Each is represented by an icon. Each icon is color-coded to enable operators to quickly determine their status, and sized/shaped to enable operators to immediately identify Media Gateway type. One glance at the EMS Status pane provides operators with the specified Media Gateways status as well as with the overall network status for all gateways managed by the EMS.

Figure 6-2: Mediant 5000 Status Pane

6.4.2 Navigation Buttons

Navigation buttons are located on the upper right side of the EMS status screen; including Home, Favorites, Back, Forward, Up and Online Help buttons.

6.4.3 Inventory Management

Inventory information can be accessed from the media gateway status screen. Inventory information includes: Chassis Info (incorporating chassis hardware and software information), Boards Table (summarizing the high-level status of all boards defined in the chassis (all boards' hardware/application/redundancy types, administrative and operative statuses), TP Boards Table, SC Boards Table and ES Boards Table.

Users can easily export all screen information to a text format file using the option 'Print Frame'.

6.4.4 Real-Time, Color-Coded Media Gateway View

The EMS graphically represents the Media Gateway's status, as well as enabling intuitive, hierarchical navigation to physical and logical entities within each Media Gateway. It shows every board's status (SC, ES, TP/SB, Alarm Card) and trunk status for TP/SB boards. All hardware entities' alarm statuses are graphically represented: power suppliers, fans, and hard disks

The color of each entity indicates its status. Special color-coding indicates various fault states of the entities (Critical, Major, Minor, Warning, OK) as well as High Availability status (which board is active, redundant standby, redundant active).

6.4.5 One-Click Access to Element Provisioning and Actions

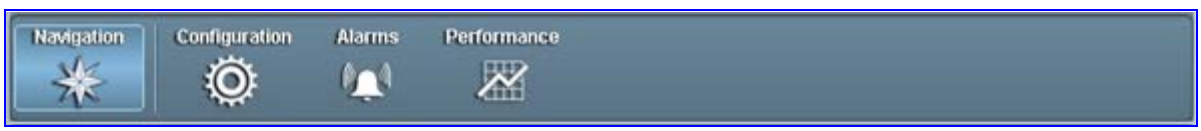
Board actions can be performed using either the right-click menu or by selecting the appropriate action in the Actions bar. The right-click menu consists of the following sub-menus: Configuration, Maintenance and Performance. The items displayed in the Actions bar are context sensitive and therefore reflect the selected entity. For more information, see 'Context Sensitive Elements' on page 125.

For a full list of supported actions, see the EMS User's Manual.

6.4.6 Modular Workflow Process

EMS entities are provisioned through an intuitive workflow process consisting of navigation desktops. You can easily navigate between these modes by clicking on the relevant button in a quick access Toolbar e.g. 'Configuration.

Figure 6-3: EMS Toolbar



The management modes are as follows:

6.4.6.1 Navigation Desktop

When you select a gateway in the MG Tree, the EMS displays the Media Gateway Status screen. A hierarchy tree of provisioning options representing the selected gateway are displayed in the Navigation pane. The options displayed in the hierarchy tree changes according to selected entity. For example, if you select the Media Gateway board, then all relevant provisioning options for the Media Gateway board are displayed.

An MG Tree (displayed in the Navigation pane) enables the user to easily view and navigate up/down the provisioning hierarchy tree. For example, *Globle* > *Region* > *Gateway* > *Board* > *Networking*.

6.4.6.2 Configuration Desktop

Once you have selected the desired provisioning option in the Navigation pane, you can quickly access the provisioning screens in the Configuration pane (located below the Navigation pane).

An option to lock/unlock the relevant entity is displayed in the Provisioning screens. At any time, you can return to the Navigation mode view by clicking the 'Navigation' button in the Toolbar.

When provisioning, operators always view in the provisioning screen a location-level indicator (the path of the EMS-managed entity), the Administrative / Operational State (for Mediant 8000) and the Reset State (for other gateways) of the entity being provisioned.

Unlock (for Mediant 5000) and Reset (for other gateways) to enable the Media Gateway to start operating with the new parameter values can be performed from the provisioning screens.

6.4.6.3 Alarms Desktop

You can display the Alarms browser for the relevant entity by selecting the relevant entity in the Navigation mode and then clicking the 'Alarms' button in the Toolbar. In the Alarms pane, you can choose to view either the Current or History Alarms browser. In the Alarms browser Actions bar, you can click the pie-chart to view different graphical statistical representations of the alarms for the selected entity. For more information, see 'Alarm Reports Graphical Display' on page 132.

6.4.6.4 Performance Desktop

You can run Performance Monitoring for the relevant entity by selecting the relevant entity in the Navigation mode and then clicking the 'Performance' button in the Toolbar. In the Performance pane, you can choose to view either History or Real-time performance monitoring. The respective Performance Monitoring provisioning screens are displayed. Starting and Stopping of Polling can be performed from the Main Actions bar or from the Actions bar in the respective Performance Monitoring provisioning screens. For more information, see 'Performance Monitoring' on page 135.

6.4.7 Context Sensitive Elements

The Status pane as well as the navigation bar allows operators to move up and down the provisioning hierarchy. Operators can always determine their exact location/level in the provisioning hierarchy from the location/level indication at the top of the screen. The Information pane always displays details regarding the current location/level.

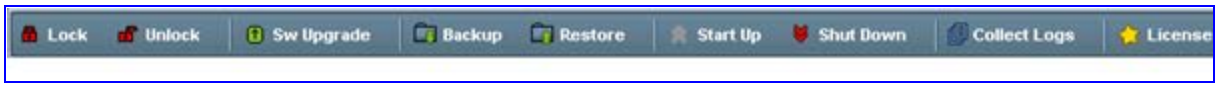
The entire EMS's GUI is context-based, affected by any change in location/level:

- The MG Node Info pane shows details of the selected MOs at the current location/level

- MG Tree shows the current region / media gateway, as selected

- Alarms displayed in the Alarm Browser are contextualized; only alarms associated with the entity selected in the MG Tree/Status pane/Board are displayed.
- The Actions bar always reflects the current provisioning location. For example, when you view the Gateway status screen, you see the most commonly used actions for the Gateway displayed in the Actions bar i.e. Lock, Unlock, Backup, Restore. Alternatively, when a Trunk is selected in the Trunk List at the TP board level, you see the most commonly used actions for the trunk i.e. 'Lock,' 'Unlock', 'Activate', 'Deactivate', 'Create Loopback' And 'Remove Loopback'.

Figure 6-4: EMS Actions Bar-Media Gateway Context



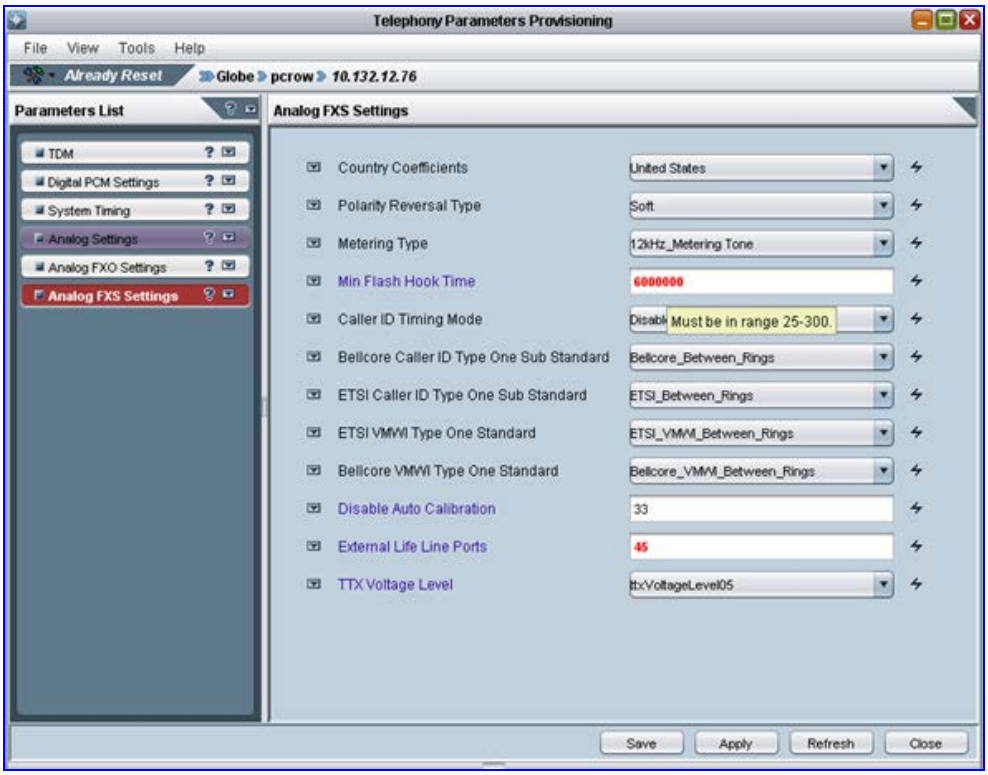
6.4.8 Virtual Directories

The EMS includes Virtual directories, which contain similar objects, frames and tabs. For example, the VoIP virtual directory contains network, media and other VoIP related folders.

6.5 Provisioning

Provisioning Media Gateway entities is straightforward and operator-friendly via the EMS. Media Gateway entities such as boards, trunks, call control protocols, etc. are provisioned using the EMS's Parameters Provisioning screens. Parameter values are downloaded to the Media Gateway via SNMPv2c or SNMPv3.

Figure 6-5: Board Parameters Provisioning Screen



6.5.1 Provisioning Types

Three icons representing three provisioning parameter types are displayed in provisioning screens adjacent to modifiable parameters: Instant (changes are applied to the Media Gateway after pressing Apply/OK), Online (the modified entity must be locked prior to applying the changes) and Offline / Reset (the modified entity must be locked prior to applying the changes and the physical component (board or Media Gateway) and unlocked (or reset) after applying the changes). This feature considerably facilitates the parameter provisioning/modifying process for operators.

6.5.2 Color-Coded for Quick Operator Assessment

The Parameters List pane in the Parameters Provisioning screens categorizes all provisioning parameters under category tabs. The tabs are color-coded for quick operator assessment. For example, if a parameter is provisioned illegally, the invalid parameter is colored in red and a tool tip with the corrective instructions appears. The category tab name is colored in red as well. Drop-down lists adjacent to each category tab and to each parameter field in that category, list two actions that operators can optionally perform (for each individual parameter and for each category): “Undo modification/s” and “Factory default value”.

6.5.3 Configuration Profiles for Quick Provisioning

The EMS’s Profile Management enables operators to rapidly provision values to entity parameters by loading a profile. The Profile Manager feature is located in the lowermost pane of the Parameters Provisioning screen.

Operators can view all currently available profile types, select a profile type best suited to customer application requirements, attach the profile, view a visual representation of the parameter values modified and save it as a new profile.

6.5.4 Parameters Search

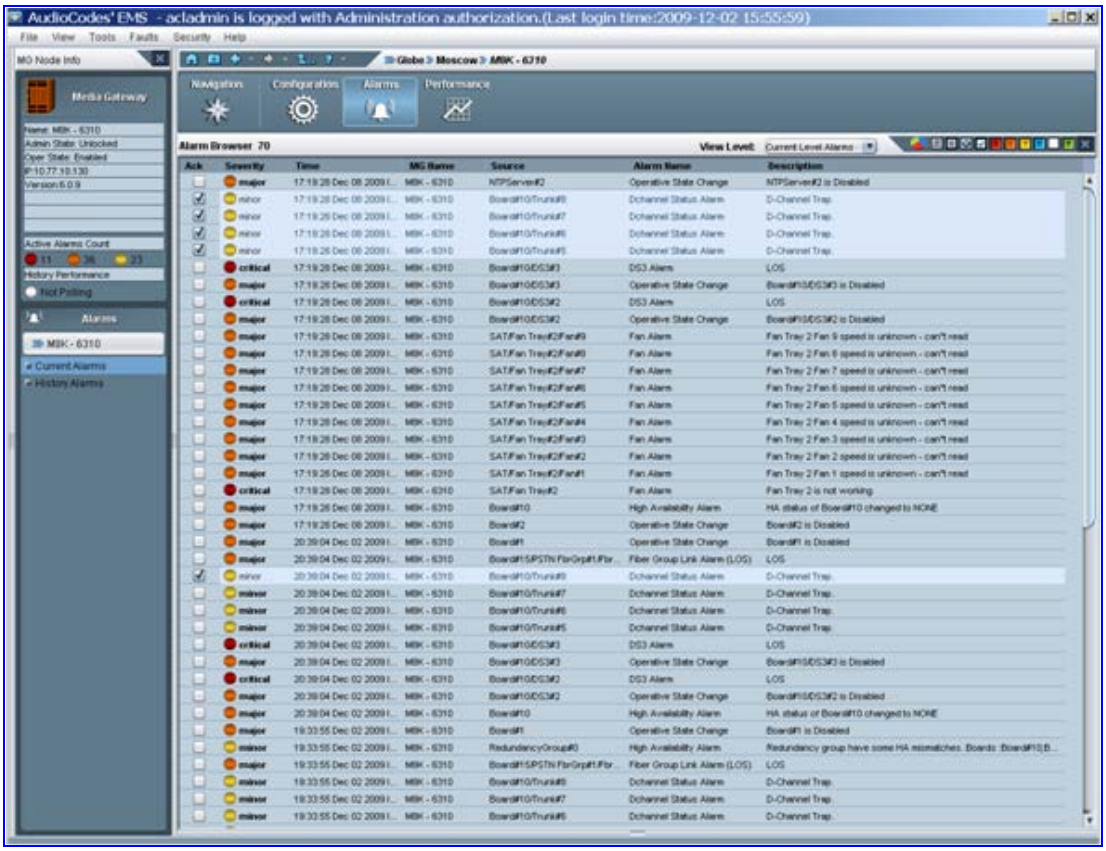
The context sensitive parameter search option enables the user to search for configuration parameters in the gateways provisioning frames. The basic search option enables you to perform a random search for a 'contains' string. Advanced search options enables you to match an exact/any word and to search for a MIB parameter.

The configuration frames containing the results parameters can be opened directly after selecting the desired parameter path.

6.6 Fault Management

The EMS's fault management functionality manages and presents all alarms and events from managed elements (received via SNMP traps) and displays them in an Alarm Browser, thereby notifying operators of problems in the system. The EMS's fault management comprises the Alarm Browser and Alarm History.

Figure 6-6: Alarm Browser in EMS Main Screen



6.6.1 Alarm Processing

The EMS can typically process 30 SNMP traps per second continuously. When an alarm is received, it is parsed, stored in the database and immediately displayed in the Alarm Browser. The Alarm Browser displays current system faults at the top of the alarms list, allowing operators to identify the entity generating the alarm.

Operators can pause automatic updating of the displayed alarms in order to take a system snapshot.

6.6.2 Alarm Context-Based View

The EMS Alarm Browser displays alarms and events according to an operator-selected context: Region, Media Gateway or Board. This capability (of being able to view the faults of an operator-specified system entity) enables operators to quickly and efficiently isolate and pinpoint a problem's precise location.

6.6.3 Current and History Alarms View

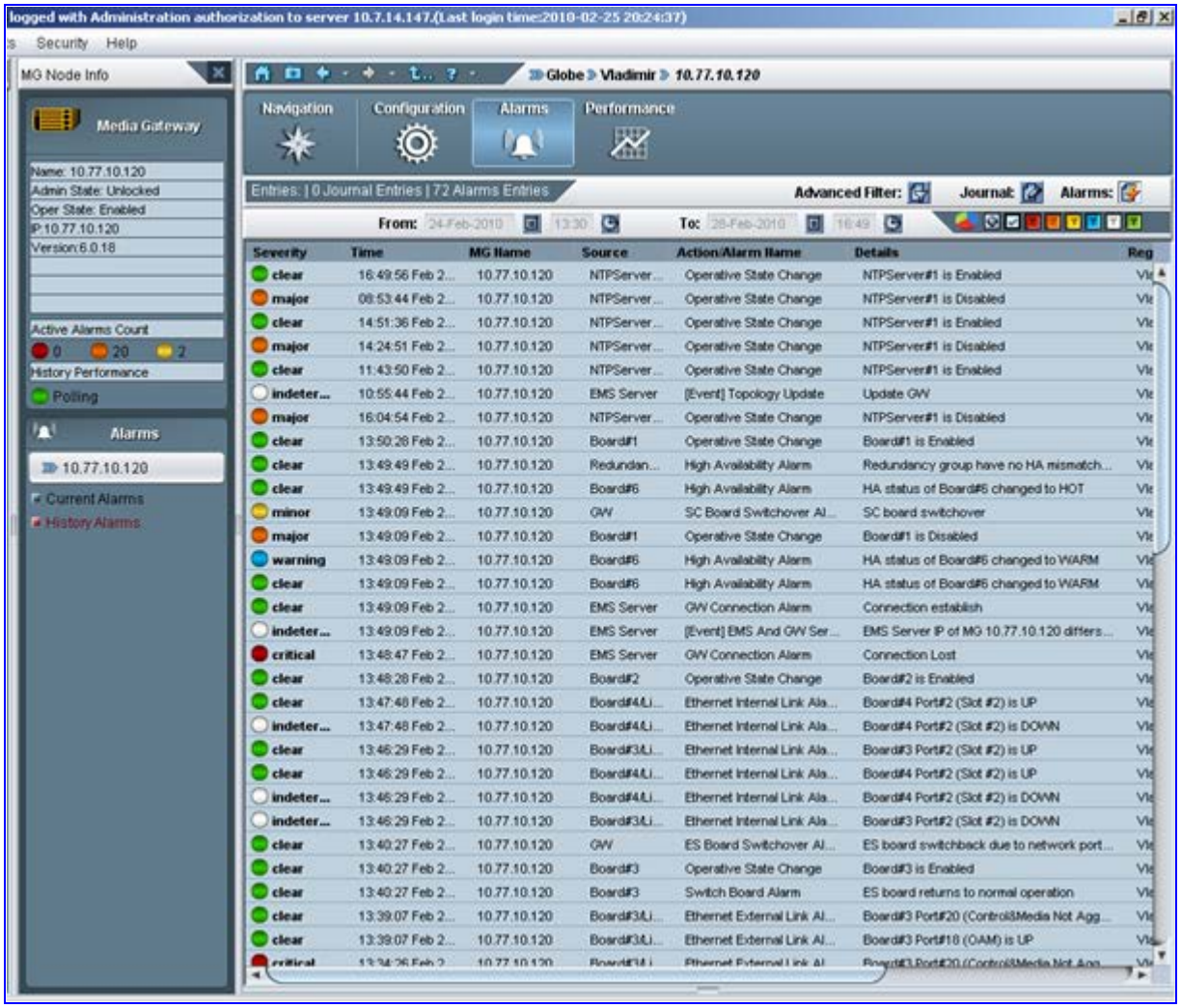
You can display both current and history (archived alarms) for the selected entity.

6.6.4 Alarm Archiving (History)

All alarms received by the EMS are archived in the database. Extensive information related to the alarm is saved, together with the alarm itself: Region and Media Gateway placement and the failed entity's physical attributes.

The Alarms History screen provides the EMS operators with a view of the alarms' history over an extended period of time (a history of at least a one month is provided, depending on disk space available - 1000 alarms per day for up to 250 Media Gateways). The Alarms History screen informs operators of the actions performed on each alarm, including the alarm's current state, the last action performed on the alarm and the name of the operator who performed the last action on this alarm.

Figure 6-7: History Alarms



6.6.5 Alarm Priorities

Based upon industry-standard management and communication protocols (ITU-T Recommendation X.733, 3GPP Recommendation 3G TS 32.111-1), the EMS supports 6 prioritized alarm levels (Critical, Major, Minor, Warning, Info and Clear). Each is color-coded so that operators can quickly and easily comprehend severity level and prioritize corrective actions.

6.6.6 Automatic Alarm Clearing

Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) when a Clear alarm is generated by the same entity (Media Gateway) that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature prevents irrelevant alarms from congesting the Alarms Browser. Operators view only alarms that are relevant (active).

Events are automatically cleared from the Alarm Browser after a predefined period of time (default – 3 days).

You can easily sort between alarms and events or filter events from the Alarm Browser and Alarm History windows.

6.6.7 Traps Forwarding to the NMS

All traps (alarms and events) received by the EMS from a managed Media Gateway, including both proprietary and standard traps as well as those issued by the EMS application itself can be forwarded to the NMS (Network Management System) as SNMP traps.

User can choose either to forward EMS Alarms only, or perform forwarding of both EMS and gateway alarms. Users can also choose whether to filter the forwarding of alarms and events for both the EMS and the managed Media Gateways. Both SNMPv2c and SNMPv3 are supported.

Traps can be forwarded to an NMS destination host from the EMS to a mail server host in e-mail or SMS format; to a Syslog server in Syslog format or to an NMS destination host as an SNMP trap.

In addition, an option is provided in the EMS to forward traps to an NMS destination host directly from a managed Media Gateway. In this case, traps are always forwarded to the NMS as SNMP traps.

6.6.8 Save Alarms into .csv File

Viewed alarms can be saved in a **.csv* file from the Alarm Browser and Alarms History screens. The alarms in a **.csv* file include all alarm fields viewed in the Alarm Details screen. The saved **.csv* file can be viewed in Microsoft™ Excel™, enabling all Excel features (statistics, graphs) on it.

6.6.9 Alarm Types

The EMS classifies alarms under 5 basic types, as required by network management standards:

1. **Communications Alarm:** an alarm of this type is principally associated with the procedures and/or processes required to convey information from one point to another
2. **QoS Alarm:** alarms notifying operators of Quality of Service degradation
3. **Processing Error Alarm:** software or processing fault
4. **Equipment Alarm:** alarms associated with an equipment fault, such as board or power supplier failures
5. **Environmental Alarm:** alarms such as temperature, power, fire, etc., associated with the physical environment in which the equipment is located

6.6.10 Alarm Actions

Operators can perform the following actions regarding the displayed alarms:

- Acknowledge: informs operators that a problem diagnosis is under way
- Manual clearing: removes inactive alarms from the operator's view
- Last operator action performed on alarms, including User Name and Action Time, can be viewed in the Alarms History pane.

6.6.11 Detailed Information

Quick access to detailed information on each alarm, including alarm type, probable cause and trap-specific information, facilitates diagnosis and troubleshooting.

6.6.12 Searching and Filtering Options

In addition to alarms displayed according to their context (entity) selected, alarms and events can be filtered according to their severity level, acknowledge status, and date and time.

In addition to severity, event, ack state and date and time filters, users can perform a string search in the Alarms History screen.

6.6.13 Alarm Reports Graphical Display

In addition to displaying tables of data, EMS also provides the user with the option to generate graphical reports.The active and history alarms can be displayed as a set of predefined graphical reports upon a user request. Reports are generated according to the data that is displayed in the Active or History Alarm Browser and according to the user filters applied on this data.

The following graphs are displayed:

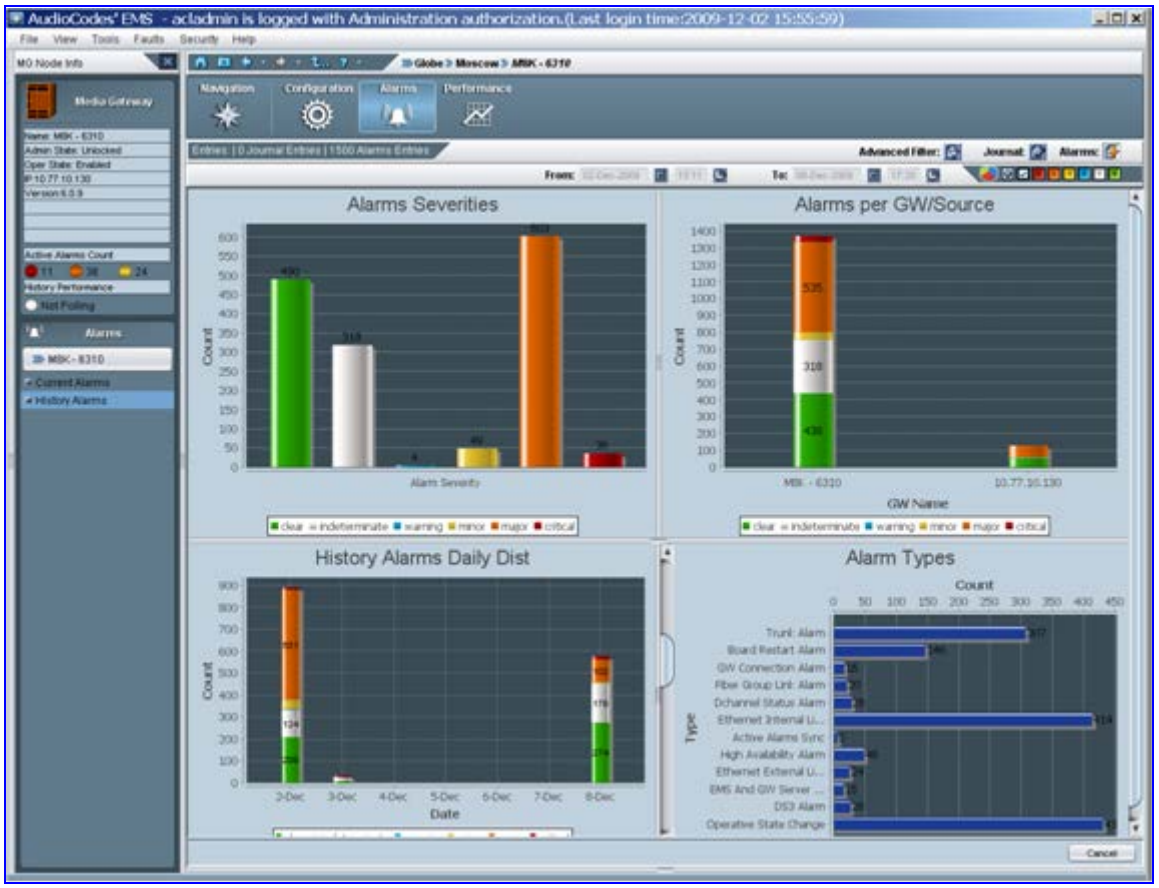
- Alarms Severity distribution: displays the number of Critical, Major, Minor, Warning, Indeterminate and Clear alarms.
- Alarms Severities distribution over time: for Active alarms hourly – during the last 24 hours; for History alarms daily – during the time that the history data was viewed.
- Alarms Severities distribution per Gateway (when in the Region view) or in the selected context.
- Alarm Types distribution for the selected context. For example, the number of Security alarms, Power Supply alarms or Ethernet Switch alarms is displayed.

The following figure illustrates an example of a user generated graphical report for current alarms.

Figure 6-8: Graphical Report-Current Alarms

The following figure illustrates an example of a user generated graphical report for history alarms.

Figure 6-9: Graphical Report-History Alarms



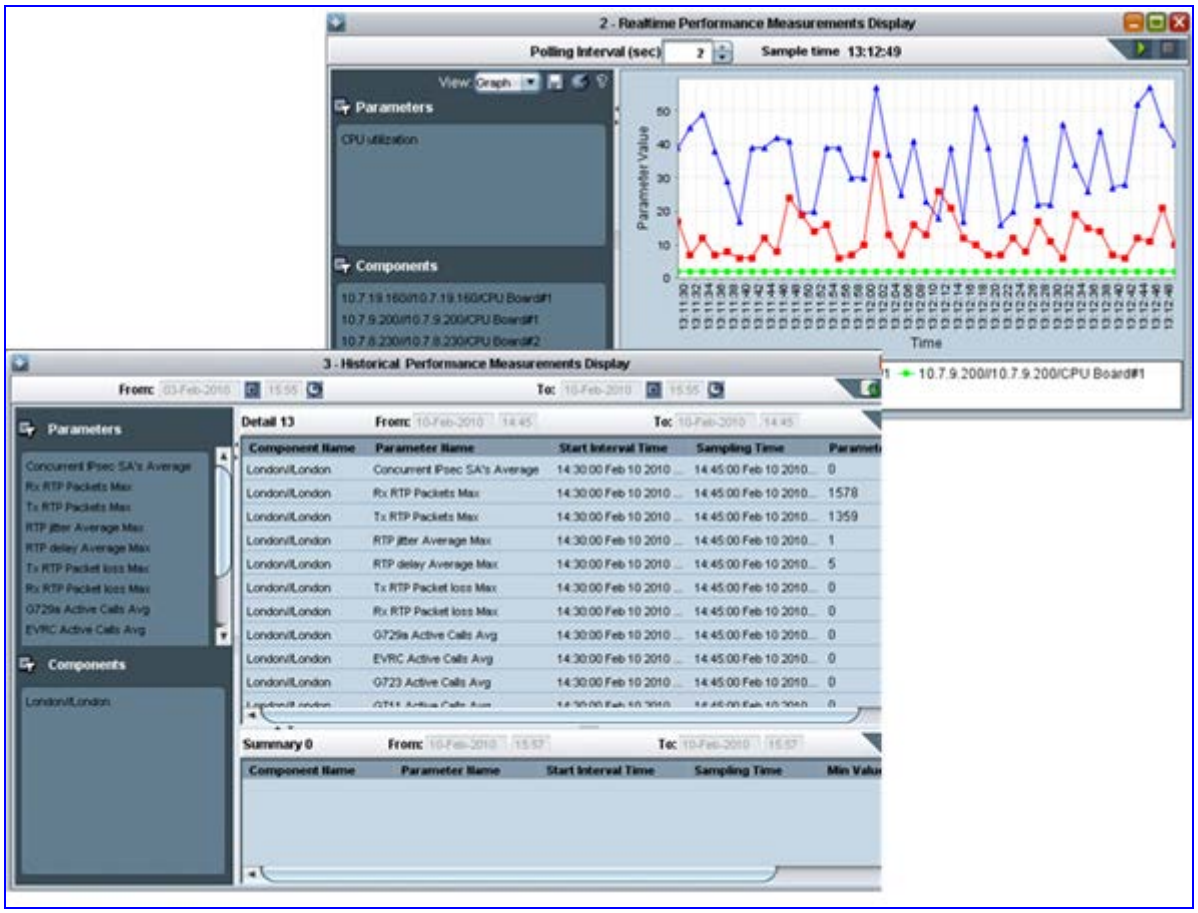
6.6.14 Change Alarm Browser View

Operators can modify the Alarm Browser's column order according to their preference. In addition, alarms can be sorted by any column (default sorting is according to time).

6.7 Performance Monitoring

After service is provisioned for a subscriber under a given QoS level, the Service Provider must ensure that the purchased level of service is delivered. In the domain of EMSs, this process involves high-level fault and performance management of the managed entities.

Figure 6-10: Performance Monitoring



The EMS's Performance Management is composed of real-time and historical data monitoring.

- **Real-Time Graphs** - Real-time data monitoring can be used to troubleshoot network or system problems and to isolate a problem after it is detected by the fault management system. In a single graph, users can compare different parameters of the same gateway, or same parameter over different gateways.

  Users can use two graph types to analyze their performance data: Table View and Line Graph. A Line Graph is generally used when only a few parameters are compared. Table View is used when extensive data is displayed and analyzed.

- **Background (History) Monitoring** - Historical data can be used for long-term network analysis and planning. PM profile, specifying those parameters that users want to collect from EMS background monitoring, can be easily transferred from one gateway to another.

In addition to storing PM background monitoring data in the EMS server database, an xml or csv file can be created per time interval The file is created at the end of the PM polling interval in accordance with a user-defined PM profile, and stored in the EMS server under directory 'Pmfiles'. Users can choose whether or not to receive a trap when each file is created. The trap contains information as to the file name and the time it was created.

- **Aggregated PMs**- Performance monitoring parameters can be aggregated for all the VoP board statistics. These parameters are defined at the Media Gateway level.
- **Configuring High and Low History PM Threshold values** - history PM thresholds can be used to raise appropriate alarms when a predefined High threshold value is exceeded. For example: once 'Lifetime in Seconds (Max)' has exceeded the user defined 'Lifetime High Threshold', a Threshold exceed alarm is issued by the Gateway and displayed in the EMS. The alarm is cleared when the PMs value drops below the predefined Low Threshold value.

6.8 Session Experience Manager (SEM)

The SEM is a valuable new tool that delivers important technical and business statistics, based on AudioCodes methodologies, developed over years of VoIP experience.

Figure 6-11: The Session Experience Manager

The tool enables VoIP network managers to do the following:

- Rapidly identify the metric or metrics responsible for degradation in the quality of any VoIP call made over the network.
- Accurately diagnose and troubleshoot quality problems in response to VoIP user criticism.
- Proactively prevent VoIP quality degradation and optimize quality of experience for VoIP users.

The following describes examples of key issues addressed by the SEM module:

- Identifies overall Voice Quality in the network.
- Identifies on which device or link 'Failed' calls of 'Poor' Quality calls were reported.
- Identifies which metrics caused a deteriation in voice quality.
- Identifies whether performance deteriorates as the numbers of calls increases.
- Identifies which users have the most call time.
- Identifies which metric most affected a specific users call's quality.
- Identifies how much bandwidth the network is utilizing.

The SEM provides a real-time, as well as historical monitoring and VoIP network health model.

- Examples of critical call quality metrics that are calculated by the SEM include: the Mean Opinion Score (MOS) Jitter; Delay (or latency); Packet Loss and Echo.

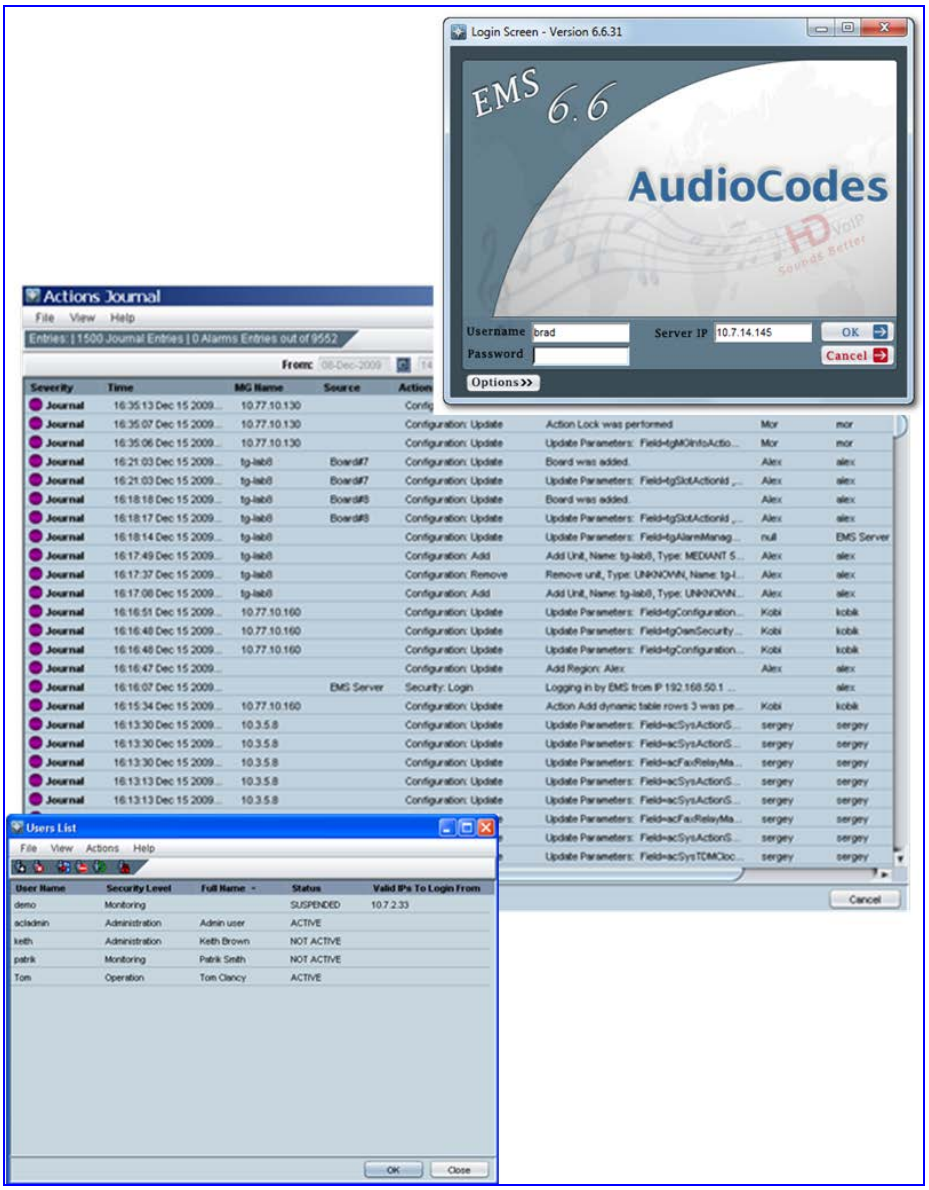
6.9 Security Management

EMS Security Management features covers following areas:

- Network Communication Security
- EMS Users Authentication and Authorization
  - Using Centralized Radius Server
  - Local Users Management
- EMS Users Actions Journal

- EMS Server Machine Hardening (including UNIX and Oracle related items, for more details refer to the EMS Server IOM Guide)

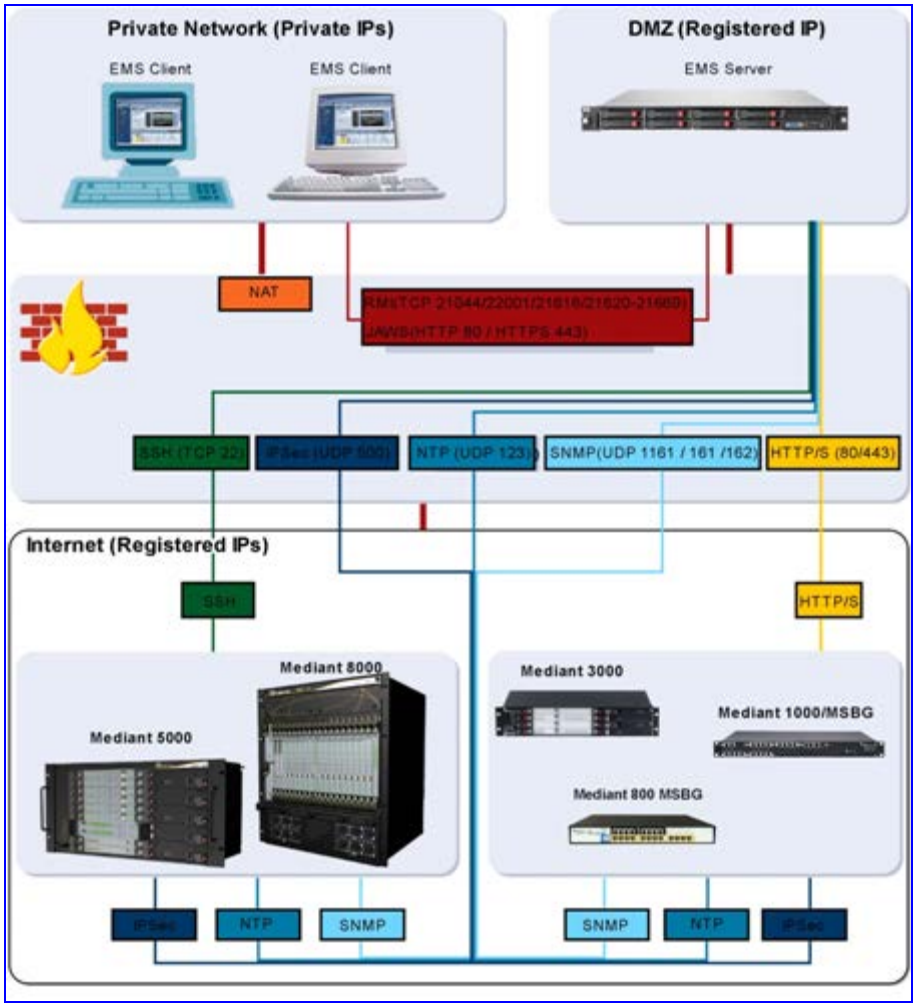
Figure 6-12: Security Management Screens



6.9.1 Network Communication Security

The EMS interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. Customers need to define rules in their firewall to enable communications between EMS client, server and managed Media Gateways.

Figure 6-13: Firewall Configuration



- EMS Client <-> EMS Server:

  The EMS comprises EMS client and server machines, intercommunicating via RMI protocol over TCP. To secure EMS client-server communications, RMI protocol runs over Secure Socket Layer (RMI over SSL).

- EMS Server <-> Mediant 5000, 8000 Media Gateways

  SNMPv3 or SNMPv2c over IPSec for provisioning, maintenance actions, fault and performance management.

- SSH and SCP for installation, upgrading software, auxiliary files management.
- Media Gateways Access Control

All user names and passwords used by EMS application to access gateways, including SNMP, HTTP, and SSH are stored in the EMS database encrypted.

6.9.2 EMS Users Authentication & Authorization

Initial access to the EMS application is secured via the Login screen, where access control consists of authentication and authorization with a user name and password.

An EMS operator is authenticated and authorized to the EMS application using either the local EMS users management tools or a centralized Radius or TACACS+ server. By default, the EMS application manages its users in the local EMS server.

EMS can be configured to authenticate and authorize users in one of the following ways:

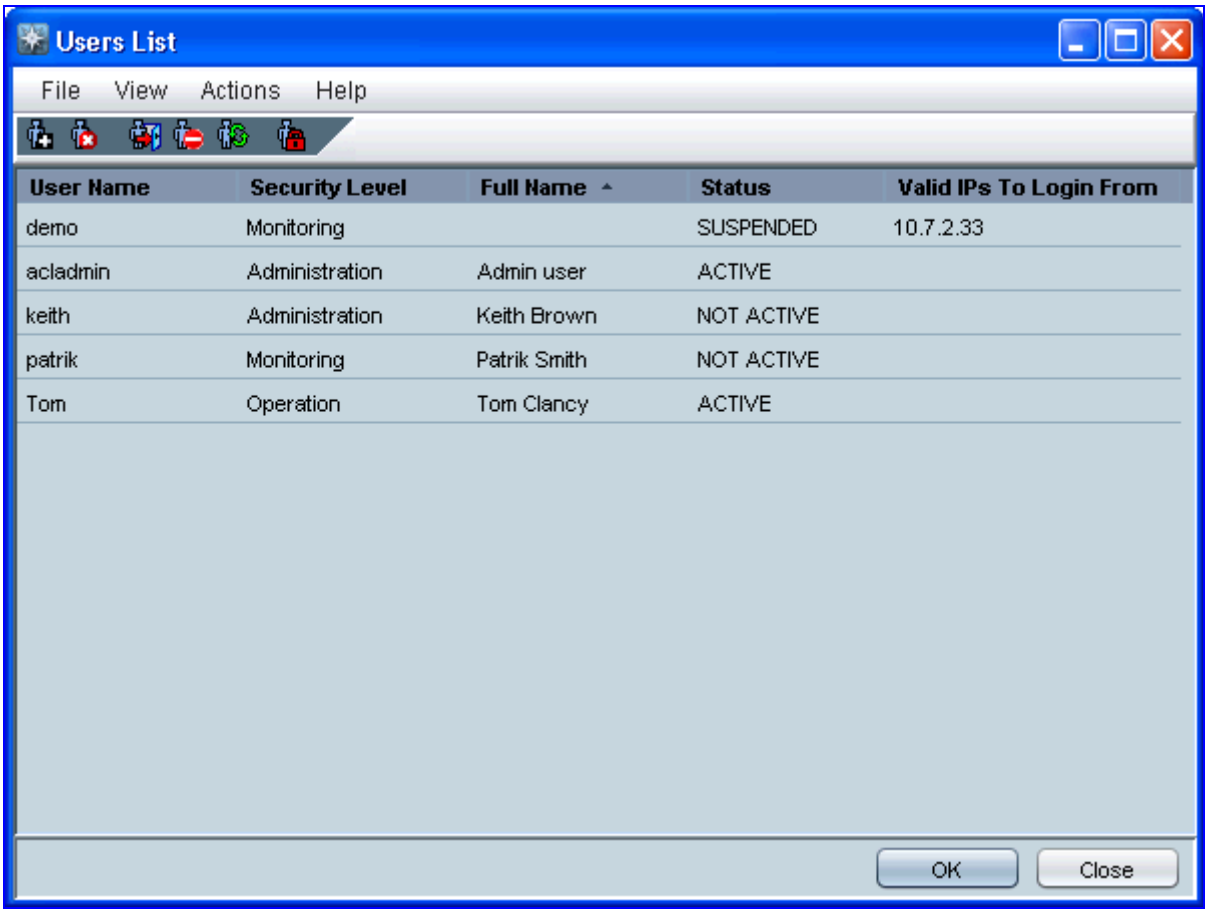
- Centralized Radius or TACACS+ Servers User Profile

  Customers may enhance the security and capabilities of logging to the EMS application by using a Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to store numerous usernames, passwords and access level attributes. This enables multiple user management on a centralized platform. The EMS server doesn't store the username and password (these users are not displayed in the EMS users list); however, forwards them to the pre-configured RADIUS or TACACS+) server. The local EMS users and passwords defined in Users' List can be used as a fallback mechanism in case the RADIUS servers does not respond.

- EMS Application User Profile

  In this case, all EMS users are defined in the EMS application using the User's List. This menu enables you to perform various user management actions such as adding or removing a user.

Figure 6-14: Users List



- Password complexity and maintenance rules, such as password length and character mix, ensure that strong and secure EMS user passwords are maintained.
- A session inactivity timer, ensures that a malicious intruder cannot use the EMS application's active session after no action has been performed for a configured period of time. The user must enter their password to unlock the session.
- A user account is blocked when the user does not enter the EMS application for a configured period of time. The blocking of inactive user accounts is intended to prevent usage of these accounts by potential intruders.

6.9.2.1 User Security Levels

The EMS operators can be allocated one of the following security levels:

- Monitoring Level (viewing only)
- Operation Level (viewing and all system provisioning operations)
- Administration Level (viewing, all system provisioning operations, and user security management).
- Super User (adding, removing and manipulating other low level users, including Administrators).

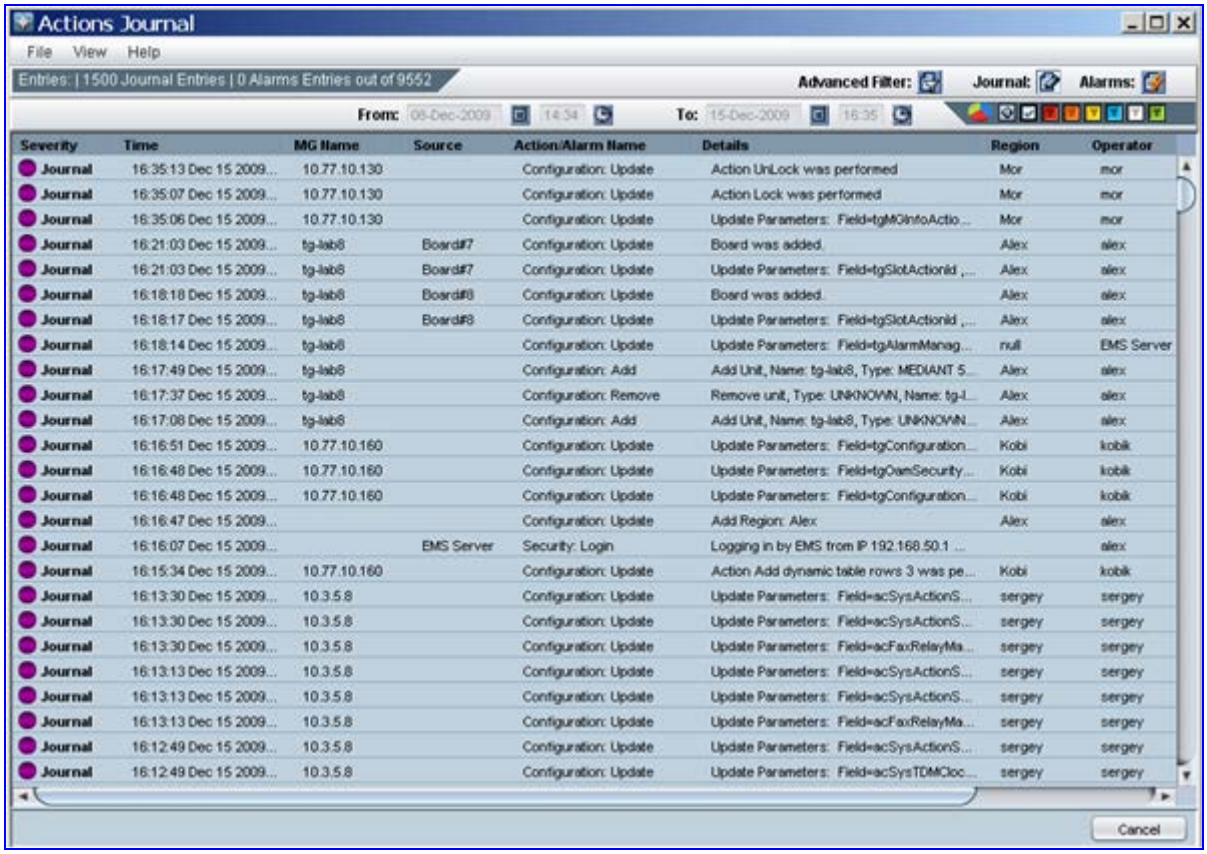
User Name and security level are displayed in the title bar of the main screen, adjacent to “EMS”.

Figure 6-15: User Details

6.9.2.2 User Actions Journal

The Actions Journal displays all logged user actions, enabling the Administrator to verify appropriate user access to system resources and providing the Administrator with the means to retroactively analyze actions previously carried out by users. Every action performed by any user is listed in the Actions Journal with information about the operator, action classification and the exact time the action was taken.

Figure 6-16: Users Action Journal



6.10 NMS Integration (Northbound Interface)

The EMS integrates easily with higher level management systems allowing the NMS to focus on network level management only.

The EMS support integration with higher management systems in the following areas:

- Remote Single Sign-On login from an NMS application to the EMS client via the EMS CLI.
- Support for Radius and TACACS+ server for centralized users Authentication and Authorization
- Fault management (alarms and events forwarding via SNMP protocol).
- Performance Management (performance monitoring collection enable using XML or CSV files format).
- Managed Gateways Topology file using CSV file format.
- Mediant 5000 / 8000 backup files.
- EMS server backup files.

For more information, refer to the EMS OAM Integration Guide document.

7 Mediant 8000 Selected Technical Specifications

Table 7-1: Mediant 5000 Technical Specifications

Function	Specification
Capacity	
Network Ports/DSP Calls (independent digital voice, fax or data ports)	**For Mediant 5000 + TP-8410 Configuration**: Up to 126 E1/T1 Links; Redundant*, 3+1 Media Gateway Boards configuration. Wireline/Wireless/Cable: 3,780 simultaneous VoIP voice calls for 3+1 TP-8410 Media Gateway Boards **For Mediant 5000 + TP-6310 Configuration**: Up to 3 Dual STM-1/OC-3 SDH /SONET Ports; APS protected; Redundant, 3+1 Media Gateway Boards configuration Up to 9 T3; Redundant, 3+1 Media Gateway Boards configuration Wireline/Cable: Up to 6048 simultaneous VoIP voice calls for 3+1 TP-6310 Media Gateway Boards GSM/CDMA: Up to 6048independent simultaneous VoIP voice calls **For all Mediant 5000 configurations**: Independent dynamic vocoder, fax or modem selection per channel Capacity is transcoding and voice coder type dependent
Media Processing	
IP Transport	VoIP (RTP/ RTCP) per IETF RFC 3550 and RFC 3551
DTMF/MF Transport	DTMF/MF RTP Relay per RFC 2833, Mute, Transparent (transfer in coder as voice)
Voice Processing	All voice processing features are supported simultaneously on all ports
	Dynamic Network Jitter Buffer with reordered RTP packets correction
	Call Progress Tones generation and detection
	Integral Announcement support towards PSTN/TDM and IP
	Transcoding of a G.711 RTP stream to any Low Bit-Rate Coder RTP stream using one DSP channel resource
	Mediation between two IP endpoints of the same coder without using any DSP channel resource
	Media duplication (one source to many destinations) using the same coder without using additional DSP channel resources

Function	Specification
Voice Coders	Wireline: G.711, G.723.1, G.729A,B, G.727, G.726, NetCoder Cables: G.711, G.726 and iLBC UMTS/GSM: AMR (8 variants/rates), AMR-WB, GSM-FR, GSM-EFR and G.711 (PCM), G.722, MS GSM. CDMA: EVRC, EVRC-B, G.729.1 (up to 12 kbps) Additional coders are supported - contact AudioCodes for further information
Echo Cancelation	G.165 and G.168 2000 compliant 32, 64, 128 msec echo tail (128 may reduce channel capacity)
Gain Control	Configurable Input/Output Gain Control: -31 dB to +31 dB in steps of 1 dB
Silence Suppression **Voice Activity Detection (VAD),** **Comfort Noise Generation (CNG)**	G.723.1 Annex A
	G.729 Annex B
	PCM and ADPCM - Per RFC 3389 or Proprietary, NetCoder.
	3GPP Voice Activity Detection (VAD) 3GPP 26.094 and Comfort Noise Generation (CNG) 3GPP 26.092
	GSM 6.10
Fax and Modem Transport	
Fax Relay and Bypass	Supported on all ports
	Group 3 real-time Fax Relay to 14.4 kbps with auto fallback
	Tolerant of delays of up to 9 seconds
	T.30 (PSTN) and T. 38 (IP) compliant (real-time fax)
	CNG tone detection & Relay per T.38
	Voice-Band Data according to V.152
	Automatic Fax ByPass (pass-through) to G.711 or ADPCM
Modem Bypass	Automatic switching (pass-through) to PCM or ADPCM for modem signals (V.34 or V.90 modem detection)
IP Interface	
IP Subnets	IPv4/ IPv6 Dual stack support. Different Local IP Addresses and Subnet masks for Operation Administration & Maintenance (OAM), Control and Media Protocols
Static Routes	Configurable Static Routes tables
Subnets/VLANs IEEE 802.1q	Multi Subnets/ IEEE 802.1q VLAN tagging capacity: ▪ Up to 3 OAM Subnets

Function	Specification
	▪ Up to 8 Media Subnets ▪ 1 Control Subnet
Link Aggregation	Up to 3 links can be included in the Aggregation group according to IEE 802.3ad
QoS IEEE 802.1p	Configurable IEEE 802.1p routing and marking capabilities for Network, Premium Control, Premium Media, Gold and Bronze QoS classes
DiffServ RFC2474	Configurable, marking capabilities for Network, Premium Control, Premium Media, Gold and Bronze DiffServ classes
Control Protocols	
MGCP (RFC 3435)	Call control, Supporting Trunk package, Generic Media package, Basic announcements package, Conferencing, DTMF and RTP Packages, CAS Packages, Fax Package, Media Format Parameter Package and other packages according to Basic MGCP Packages (RFC 3660)
MEGACO (H.248)	Call control, Supporting Generic Media Package, Base Root, Tone Generator, Tone Detection, DTMF Generator, DTMF Detection, Call Progress Tones Generator, Call Progress Tones Detection, Basic Continuity, Network, RTP, TDM Circuit, Generic Announcement, Expanded Call Progress Tones Generator, Basic Service Tones Generation, Expanded Services Tones Generation, Basic CAS, R2 CAS, MF Generator, MF Detection, Inactivity Timer, Basic Call Progress Tones Generator with Directionality, Call Type Discrimination, IP Fax as well as other more packages, Basic CAS addressing package, Robbed bit signalling package, Operator services and emergency services package, etc.
SIP	**SIP Functions:** User Agent Client (UAC), User Agent Server (UAS) **Operation with SIP Horses:** Third party Proxy, Redirect, Registrar servers **SIP Methods:** INVITE, ACK, BYE, CANCEL, REGISTER, REFER, NOTIFY, INFO, OPTIONS, PRACK, UPDATE **SIP Transport:** UDP, TCP **SIP Security:** TLS 0.1 (Transport Layer Security) Supported SIP RFCs: RFC 3261 - SIP RFC 3262 - Reliability of Provisional Responses RFC 3263 - Locating SIP Servers RFC 3264 - Offer/Answer Model RFC 3265 - (SIP)-Specific Event Notification RFC 2327 - SDP RFC 2782 - A DNS RR for specifying the location of services RFC 3323 - Privacy Mechanism RFC 3325 - Private Extensions to the SIP for Asserted Identity within

Function	Specification
	Trusted Networks RFC 3327 - Extension Header Field for Registering Non-Adjacent Contacts RFC 3515 - Refer Method RFC 3581 - Symmetric Response Routing RFC 3725 - Third Party Call Control RFC 3605 - RTCP attribute in SDP RFC 2833 - Telephone event RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication RFC 3891 - "Replaces" Header RFC 3311 - UPDATE Method *draft-ietf-iptel-trunk-group-02.txt* - Representing trunk groups in tel/sip URIs *draft-burger-sipping-netann-10.txt* - Basic Network Media Services with SIP *draft-ietf-avt-rtp-clearmode-05.txt* - RTP payload format for a 64 kbit/s transparent call *draft-ietf-sip-referredby-04* - The SIP Referred-By Mechanism *draft-ietf-sip-session-timer-15* - Session Timers in the Session Initiation Protocol *draft-levy-sip-diversion-08* - Diversion Indication in SIP *draft-vandyke-mscml-04* - Media Server Control Markup Language (MSCML) *draft-ietf-sipping-qsig2sip-04.txt* - Interworking between SIP and QSIG *draft-ietf-sipping-realtimefax-01.txt* - SIP Support for Real-time Fax: Call Flow Examples *draft-choudhuri-sip-info-digit-00.txt* - SIP INFO method for DTMF digit transport and collection *draft-mahy-sipping-signaled-digits-01.txt* - Signaled Telephony Events in the Session Initiation Protocol
TGCP (PKT-SP-TGCP)	PacketCable's Call control, IT Package as well as other proprietary TGCP packages.
Security	
IPSec (ESP) with IKE pre-shared key or X.509 Certificate	IPSec (in Transport mode) is supported for the management traffic to EMS/ NMS/ OSS and for control interfaces to MGC (MGCP or H.248 with reduced channel capacity). Encryption algorithms - DES and 3DES Hash types - SHA1 and MD5
SNMP v3	Northbound management interface to EMS, NMS and OSS. Providing encryption and authentication of the management traffic. Authentication protocols: HMAC-MD5-96, HMAC-SHA-96. Encryption protocols: CBC-DES (DES-56), 3DES, AES-128.

Function	Specification
Media Gateway Boards-Based Firewalls	Up to 20 Filtering criteria rules according to: Source IP-address and subnet Destination port range Protocol type Packet size Traffic rate in bytes-per-second
Access Control Lists	The control interfaces can be protected by access control lists.
Media Encryption	Media encryption is supported per PacketCable specification (with reduced channel capacity). AES - 128 (Rijndael) cipher algorithm, in CBC mode Optional 2-byte or 4-byte MAC based on MMH algorithm Or, SRTP (RFC 3711)* media encryption limited to AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80 secured suites H.248 Keys negotiation as per RFC 4568: Or, MGCP proprietary Keys negotiation
SSH (Secure Shell)	To secure the Telnet and SFTP Server SSH Protocol Version 2 Supported encryption algorithms: AES-128, BLOWFISH, 3DES Supported authentication algorithms: SHA1, MD5 User/password authentication on each login
SSL/TLS (the Secure Socket Layer)	To secure SIP control interfaces and Media Gateway Boards web server and telnet Supported transports: SSL 2.0, SSL 3.0, TLS 1.0 Supported ciphers: DES, RC4 compatible Authentication: Username & Password, X.509 certificates
PSTN Signaling	
In-band/Out-of-band Signaling (DTMF & Tone Detection/Generation)	DTMF per TIA 464B
	DTMF over RTP per RFC 2833
	MFC-R2, MF-R1, MF-R1 (US) including FG-A/B/D
	Packet side or PSTN side generation/detection of DTMF and User Defined Call Progress Tones (PSTN, IP) & Continuity Test Tones (per ITU-T Q.724)
PSTN Protocols	CAS - T1 robbed bit: WinkStart, delay dial, immediate start, FGB, FGD, etc. MFC/R2 numerous country variants Unique script for each county variant, enabling maximum flexibility of the

Function	Specification
	entire state machine of each CAS protocol Mercury Exchange Limited CAS (MelCAS) signaling protocol. Supported in MEGACO only
	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
CAS Relay	ABCD signaling over RTP per RFC 2833
SS7 Narrow-band Links	MTP-2 (ITU / ANSI) link termination
SIGTRAN	IUA (RFC 3057) over SCTP (RFC 2960) M2UA, (RFC 3331) over SCTP (RFC 2960) M3UA, (RFC 3332) over SCTP (RFC 2960)
SS7 Signaling	
SS7 Signaling Nodes (SN)	SNs per 2 blades in Point Code Sharing configuration;SS7 Broad-band Signaling Nodes or SS7 Narrow-band Signaling Nodes, providing SP or STP* functionality.
SS7 Route Sets	Up to 30 Route Sets per SS7 Node
SS7 Link Sets	Up to 32 SS7 Link Sets per SS7 blade and up to 4 Link Sets per Route Set.
SS7 Links	Up to 32 SS7 Links per blade and up to 8 Links per Link Set.
SIGTRAN Narrow-band Interworking	Termination of MTP-1, MTP-2, layers and delivery of MTP3 messages over M2UA/SCTP/IP Termination of all layers up to MTP3 layer and delivery of SCCP/ISUP messages over M3UA/SCTP/IP
Clock Synchronization	
Clock Specification	ITU G.813 option 1 and 2, ETSI EN 300-462-5-1 and ANSI SMC T1.105.09 and Bellcore GR-1244-core stratum 3. Supporting the following Reference input signals: ▪ G.703 E1/T1 External Clock Port (SSM not supported); ▪ 2048 kHz synchronization signal according to clause 13/G.703 (T12). ▪ Recovers timing from a received E1/T1, STM-1/OC3 or T1 on T3 connected to the PSTN Network. ▪ Distributes clock to the PSTN Network through E1/T1, STM-1/OC3 or T1 on T3 lines.

Function	Specification
3GPP IMS Services	
Media Gateway Control Protocols	IMS Mn - 3GPP TS 29.332 for IPv4 and PSTN termination types.
Cable Services	
PacketCable Vocoders	G.711 (A-law/m-law), 729E, and iLBC supporting PacketCable PKT-SP-Codec Additional coders such as BV16 may be supported - contact AudioCodes for further information
Media Gateway Control Protocols	TGCP, IT, MO and MT Packages according to PacketCable PKT-SP-TGCP
PacketCable Security	Call Control Security, supporting IPSec with pre-shared Key, as per relevant sections of PKT-SP-SEC Media (RTP/RTCP) Security - AES - 128, as per relevant sections of PKT-SP-SEC
PacketCable CALEA	Electronic Surveillance as per relevant sections of PKT-SP-ESP and PKT-SP-TGCP
Maintenance	
Management	Element Management System, SNMPv2 or SNMPv3 OAM Single point of access via the System Controller; easy management and provisioning with standard SNMP v2 or SNMPv3 interface.
Maintainability	All system modules are hot swappable, including boards, Power Supply modules, fans and Alarm modules
Redundancy Scheme	CPUs, Ethernet switches: Active/Standby Power supplies, fans: Load Shared Media Gateway boards: N+1
Diagnostic	Automatic and Manual Hardware and SW Diagnostic, BIT (Built in Test) fault detection, heart beat, chassis sub-systems monitoring
Physical Interfaces	
E1/T1 Interfaces	Per TP-8410 Board: The PSTN interfaces are provided by two SCSI connectors per RTM-8410 (100-Pin female SCSI connector and 68-Pin female SCSI connector), supporting up to 42 DS1 (E1/T1) trunks per RTM-8410.
STM-1/OC3 Interfaces	Per TP-6310 Board: Replaceable Dual-LC connectors; 155 Mbps optical SFP modules

<table>
<tr><th>Function</th><th>Specification</th></tr>
<tr><td></td><td>(complies with the INF-8074i - Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA))
Hot Swappable</td></tr>
<tr><td>T3 Interfaces</td><td>Per TP-6310 Board:
Three T3 (DS-3) ports using unshielded mini-SMB connectors</td></tr>
<tr><td>IP Interfaces</td><td>Per ES Board:
on ES/6600, up to 3 different IP Uplinks:
<table>
<tr><td></td><td>ES/6600</td></tr>
<tr><td>OAM</td><td>100 Base-TX</td></tr>
<tr><td>Control</td><td>100 Base-TX</td></tr>
<tr><td>Media</td><td>3 aggregated 1000 Base-TX</td></tr>
</table>
100/1000 Base-TX: RJ-45 Connector Interface (CAT5 Twisted pair)</td></tr>
<tr><td colspan="2">Hardware Specifications</td></tr>
<tr><td>Midplane</td><td>PICMG 2.16 cPCI Packet Switching Backplane (cPSB)
PICMG 2.1 cPCI hot swap specification
PICMG 2.0 cPCI specification</td></tr>
<tr><td>Power</td><td>The average power consumption for a full complement of boards in a TP-6310 configuration is approximately:
▪ 615 watts - 2.6 A at 230 VAC
▪ 630 watts - 5.6 A at 110 VAC
▪ 640 watts - 13.4 A at -48 VDC
The average power consumption for a full complement of boards in a TP-8410 configuration is approximately:
▪ 650 watts - 2.6 A at 230 VAC
▪ 650 watts - 13.4 A at -48 VDC</td></tr>
<tr><td>Cooling</td><td>Easily replaceable fan trays and filter</td></tr>
<tr><td colspan="2">Regulatory Compliance</td></tr>
<tr><td>Telecommunication Standards</td><td>FCC part 68
TBR4 and TBR13</td></tr>
<tr><td>Safety and EMC Standards</td><td>UL 60950-1
FCC part 15 Class A
CE Mark (EN 55022 Class A, EN 60950-1, EN 55024, EN 300386)</td></tr>
<tr><td>Environmental</td><td>NEBS Level 3: GR - 63-Core, GR -1089-Core Type 1 & 3,
ETS 300 019</td></tr>
<tr><td colspan="2">* Currently not supported, consult AudioCodes release notes for up-to-date availability of this</td></tr>
</table>

Function	Specification
features ** Designed to meet - formal approval pending	
Specifications subject to change without notice.	

Reader's Notes

8 Index

F

G

H

I

M

N

O

P

Q

R

S

T

U

V

X

Reader's Notes

AudioCodes™ Media Gateway

Mediant 5000™

Product Description

Version 6.6

Document # LTRT-92520

AudioCodes

www.audiocodes.com