Media Gateway 3500
Product Description

Version 3.0

Document #: LTRT-92504 Rev 004

Contents

List of Figures

List of Tables

Introductory Matter

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **alt** and ⇦ keys.

Notice

This manual describes the product features and components of the Media Gateway 3500.

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, Nortel cannot guarantee the 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 Technical Support customers at 'www.nortel.com' under Support / Product Documentation.

Date Published: June 30, 2005 Date Printed: July 12, 2005

Trademarks

All products or trademarks are property of their respective owners.

Customer Support

For Customer support contact support@nortel.com

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

- ***Media Gateway 3500 Product Description*** (this manual) - contains the description of the product features, components, standard control protocols and management protocols.
- ***Media Gateway 3500*** *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-907xx.*
- ***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 Media Gateway 3500 to send all alarms set as they are to be handled according to manual or automatic 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).*
- ***EMS Alarm Guide*** - *LTRT-946xx*

1 Introduction to the Media Gateway 3500 Media Gateway

The **Media Gateway 3500** is a high channel density, medium-sized market-ready, standards-compliant, VoIP gateway. It incorporates leading Voice over Packet technology to enable Service Providers rapid time-to-market and reliable cost-effective deployment of next-generation networks.

The Media Gateway 3500 is a robust, scalable and modular solution, designed for the carrier environment, matching the density requirements for medium deployments, while meeting Network Service Providers' demands for high availability, reliable new voice infrastructure networks. For maximum reliability, the Media Gateway 3500 features protection switching and full redundancy of all common equipment.

The chassis platform is supplied in a Redundant (with High Availability) configuration.

1.1 General Features

The Media Gateway 3500 offers a comprehensive system containing the following General Networking Functionality features:

- Up to 96 E1/T1 Interfaces
- MEGACO (H.248) media gateway control protocol
- Vocoder configuration options: PCM, G.711, G.723, G.729A, G.729E, G.728, G.727, G.726
- Integral Announcement support towards PSTN/TDM, and IP
- 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)
- 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)
- On-board, dual redundant Ethernet Switches, each with up to 3 Gigabit aggregated GbE optical interfaces (Ethernet redundancy)
- 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.
- Media (RTP/RTCP) Security - AES - 128 (Rijndael) cipher algorithm.
- Complete gateway solution, designed for the carrier environment
- Remote Online Software Upgrade.

1.2 PSTN Signaling Features

The Media Gateway 3500 offers a comprehensive system containing the following PSTN Signaling features:

- PSTN protocol termination support
- PSTN Signaling: CAS, ISUP, and ISDN PRI
- SIGTRAN IUA
- MFC-R2 and Call Progress Tone detection and generation

1.3 Shelf Management Functionality

The Media Gateway 3500 offers a comprehensive system containing the following Shelf Management features:

- Complete gateway solution, designed for the carrier environment
- High-availability implementation consisting of redundant modules, common modules and load-sharing 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 The Nortel 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 transmitted 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.
- Automatic and Manual Hardware and Software Diagnostic, BIT (Built in Test) fault detection, heart beat, chassis sub-systems monitoring.
- Comprehensive EMS with NMS Northbound interface to operate and manage the media gateway.

1.4 Hardware Platform Functionality

The Media Gateway 3500 offers a comprehensive system containing the following Hardware Platform features:

- Optimal, cost-effective channel density
- Small footprint

- Open platform, designed for the carrier environment, that utilizes industry standard PICMG (PCI Industrial Computer Manufacturers' Group) chassis with the latest cPSB (cPCI Packet-Switching Backplane) technology
- Standard CompactPCI specification (PICMG 2.0, R3.0)
- Hot swap removal and insertion of all system elements - Hot Swap specification for CompactPCI (per PICMG 2.1 R1.0)
- CompactPCI Packet Switched Backplane (cPSB) (per PICMG 2.16)
- Standard connector keying for CompactPCI boards (per PICMG 2.10, R1.0)
- NEBS Level 3-compliance[1]
- Modular hardware expandability “pay-as-you-grow” system
  - Redundant power supply modules (AC or DC)

1.5 Performance Highlights

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

  The Media Gateway 3500 has a wide coverage of applications when it comes to support for wireline and cable networks. The Media Gateway 3500 supports IP and PSTN interfaces, voice coder options, signaling and control protocols for the above applications.

- **Deploy Right-Sized Systems**

  The Media Gateway 3500 VoIP media gateway matches the density requirements for medium-sized deployments, while meeting Network Service Providers' demands for reliable new voice infrastructure networks.

- **Deliver New Solutions Faster**

  Immediately address new opportunities in emerging markets with the most flexible, large mid-size customizable solution available. The Media Gateway 3500 VoIP Gateway system's standards-based control interfaces, protocols, and open architecture ensure easy integration with new products and services.

- **Create Flexible Products and Services**

  The Media Gateway 3500 VoIP Gateway system enables operators to immediately address opportunities that utilize a myriad of legacy circuit-switched infrastructure features and functionality. The Media Gateway 3500 has a wide coverage when it comes to support for regional PSTN interfaces, voice coder options, signaling and control protocols.

- **Smooth Migration**

  The Media Gateway 3500 Media Gateway has been designed to enable smooth migration from a circuit-switched network to a next generation packet-switched networks.

The Media Gateway 3500 is part of Nortel’s complete family of VoIP gateway system solutions for new voice infrastructure networks.

[1] Designed to meet - Formal approval pending.

2 Media Gateway 3500 Basic Feature Highlights

The Media Gateway 3500 Media Gateway offers a comprehensive system complete with the Voice Packet Processing, High Availability, and PSTN Signaling features essential for the wireline communications environment. Beside the PSTN Signaling features 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 Media Gateway 3500 can be summarized in the following areas:

- Voice Packet Processing
- Gateway Management
- Performance Management
- High Availability
- Security
- Remote Online Software Upgrade

2.1 Voice Packet Processing

The Media Gateway 3500 provides a feature-rich set of voice-processing services required for its functionality as a media gateway. These services include:

- Echo Cancellation
- Voice and tone signaling discrimination
- Capacity and Voice compression
- Voice activity detection (VAD)
- Comfort noise generation (CNG)
- Voice, data and fax discrimination
- Fax and data processing
- Tone processing

2.1.1 Echo Cancellation

The Media Gateway 3500 supports Echo Cancellation (32, 64, 128 msec tail adaptive) on each voice channel per G.165 and G.168-2000. The echo cancellation algorithm reduces degradation originating from PSTN interfaces and improves the perceived voice quality.

2.1.2 Voice and Tone Signaling Discrimination

The Media Gateway 3500 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 Media Gateway 3500 + TP-1610 configuration, the chassis accommodates up to 6 TP-1610 media gateway boards per chassis, supports up to 2,400 (5+1 boards) simultaneous calls for the redundant configuration. 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 Media Gateway 3500 can support up to 80 E1 / T1 links in the Redundant configuration.

The Media Gateway 3500 currently supports the following voice compression Vocoder algorithms: G.729A, G.728, G.729E, G.723.1, G.727, G.726, G.711.

The Media Gateway 3500 supports independent dynamic vocoder selection per channel.

2.1.4 Voice Activity Detection and Comfort Noise Generation

The Media Gateway 3500 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 Media Gateway 3500 currently handles fax and modem transmissions according to standard IETF fax over IP (FoIP) protocols. 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 Media Gateway 3500 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.

2.1.6 Tone Processing

The Media Gateway 3500 supports tone processing for VoIP networks. Voice band tones are used in the PSTN for various functions such as dialing, indicating the call progress status, etc. The Media Gateway 3500 detects In Band Signaling (IBS) tones like DTMF, MFC-R2 and PSTN 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.

2.2 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 dependent and hence ensures easier integration with other systems.

Some of the main management tasks performed on the Media Gateway 3500 chassis are:

- **OAM Single point of access via the System Controller** - Providing easy management and provisioning for all Media Gateway 3500 blades via standard SNMP Interface.
- **SNMP v2 Based Provisioning API** - While Media Gateway 3500 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 Media Gateway 3500 '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 data base. 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.
- **Online Software Upgrade** - Software Upgrade of all Media Gateway 3500 components without ongoing service interruption. The SC software upgraded is online. The Media Gateway blades are gracefully shutdown one by one, while other blades operation is uninterrupted. In case of problems, rolling back is supported, but service lost may occur, depending on the stage in which rolling back was issued.
- **Health Monitoring** - 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.
- **SNMP 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) The SNMP alarm traps can be utilized via Telnet/SSH for emergency management.
- **Performance Measurements for Monitoring System** - Performance Measurements are available for a 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. (See "Performance Management" below.)

  The Media Gateway 3500 provides performance measurements in the form of two types:

  - **Gauges** - Gauges represent the current state of activities on the media server. Gauges unlike counters can decrease in value and like counters, can increase. The value of a gauge is the current value or a snapshot of the current activity on the media server at that moment.
  - **Counters** - Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset and then the counters are zeroed.

  The Media Gateway 3500 performance measurements are provided by several proprietary MIBs located under the "performance sub tree".

2.3 Performance Management

Performance Monitoring is an essential feature of any element / network management system. The Media Gateway 3500 supports Performance Measurements (PM) utilization data for Shelf Controllers (Active and Standby) and for all the Media Gateway blades and Interfaces. PMs are maintained on the Media Gateway 3500 Shelf 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, a **real-time view** and an **historic view**:

- A 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.
- An 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 in version 3.0 is fixed, 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.
- An historic report saves all “Time Interval” parameters over a configurable certain period of time. For version 3.0 all the PMs are available in 15 min buckets starting/ending at a configurable date and time. The Historic report is exported by the EMS to Comma Separated Value (CSV) files for use by network management systems. Files history storage is 30 days (for 15 min 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 Media Gateway 3500 performance measurements are provided by several proprietary MIBs located under the "performance sub tree”.

2.3.1 EMS Data Collector and Reduction Functions

- **Real Time Data Collector (RTDC)** resides on the EMS server, collects user requested Real Time PM Values from the SC on a periodic basis and stores the values in a database. The RTDC collects the current value of that PM every configurable N seconds and display them via the EMS Real time view. N is referred to a configurable collection interval.
- **Time Intervals Data Collector (TIDC)** resides on the EMS server, collects Time Interval PM Values from the SC on a periodic basis and stores the values in a database. This data is used by the EMS to present a historic view of performance management data. 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.

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

The Nortel 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 Media Gateway 3500 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 and thoroughly tested system, the Media Gateway 3500 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 56.

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

Each of the two System Controllers are provide with a SA RTM boards, which provide redundant Alarm card function to the system. Each of the SA is controlled by its attached SC for monitoring and controlling the fans' rotational speed, system temperature and power supplies. 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' on page 58.

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 shelf 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 shelf 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 60.

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 43.

2.4.4 Ethernet Uplinks Redundancy

The Media Gateway 3500 provides redundancy between '1+1' Ethernet Switches (ES). With ES version 4411, the Media Gateway 3500 provides redundancy between the two Gigabit Ethernet Media uplinks on the Ethernet Switch boards. If one uplink fails, the traffic continues through the other Ethernet Switch 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 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 shelf 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 to handle E1/T1 CAS (MFC R2), active calls are dropped when Media Gateway board switchover takes place, because the redundant board is started from cold reboot. However, the Media Gateway 3500 Gateway regains original capacity automatically without the need of operator intervention.
- **Hot Redundancy** - Uninterrupted call redundancy. For Media Gateway boards configured to handle SS7 Transparent (ISUP trunks) or ISDN PRI with IUA, active calls are not dropped when the PSTN Redundancy is activated. 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 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 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. For more information on the Media Gateway boards, refer to 'TP-1610 Media Gateway Board' on page 53.

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

The Media Gateway 3500 contains 3 power supply modules. 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 PS-2 Modules' on page 62.

2.4.7 Cooling Fans (Load sharing N:1 Configuration)

The Fan Tray unit contains five fans. Four of them are sufficient to cool the entire system if necessary. The Fan Tray Unit and associated air filter are hot-swappable and efficient replacement can be accomplished without affecting the Media Gateway 3500's operation. For more information on the cooling system, refer to 'Cooling System' on page 47.

2.4.8 Clock and Synchronization Redundancy

The Media Gateway 3500 Media Gateway is able to operate in two synchronization modes. When working in the synchronized mode (non-default mode), the Media Gateway 3500 Media Gateway provides redundant clock synchronization mechanism. It allows the system to continuously operate in synchronization with the PSTN equipment, while synchronizing all the PSTN interfaces to the same clock source. The redundancy is provided in the following levels:

Clock Signals - all the gateway elements provide a double clock synchronization signal path for the case that one of the signals fails. It relates to the back plane and the Media Gateway boards.

Clock Source Level - Allows configuring of two Media Gateway boards (redundant) to provide synchronized clock for the entire gateway. When the current clock master (primary or secondary) board fails, the redundant, standby board becomes the gateway's clock master, providing the clock settings to all of the other boards in the gateway.

Line Clock Reference Level - allows redundancy of the PSTN clock synchronization reference interface. When the current clock reference fails the gateway synchronizeS to alternative clock reference signal according to predefined plan. Any E1/T1 link might serve s a clock synchronization candidate when working at the Line Timing mode.

External Clock Reference Level - (is to be implemented in the next applicable release) allows redundancy of the BITS interfaces on 2 redundant Timing Modules for synchronization reference when working in External Timing mode.

2.4.9 Redundancy Group Procedures

Redundancy Group represents the group of all Media Gateway boards in the shelf. One board in the group has a Redundant GTER behind 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 in a shelf, to which all boards automatically belong.

When defining the redundant board with "make board redundant" action, the administrator also locks a regular Media Gateway board from which its configuration is copied to the redundant board.

The EMS presents each of the boards, current Redundancy status - either redundant or regular "normal" board.

From the EMS, the administrator can manually switch back to the failed board, either after failed board recovery or replacement, or in as a forced switch back in the event that the redundant board is to be saved for an additional board failure.

For SS7, there are two Media Gateway board configuration sets:

- SS7 Transparent and ISDN PRI with IUA
- E1/T1 CAS

From version 3.0 onwards, the Media Gateway 3500 supports both “Warm” and “Hot” redundancy for the TP-1610 boards (refer to 'Media Gateway Boards (N+1 Configuration)' on page 20) that are configured to handle SS7 Transparent. For TP-1610 boards configured for ISDN PRI with IUA "Hot redundancy" is supported (provided the same board's type is selected for the redundant board). In this mode, all of the network elements connected to the board (either IP or PSTN interfaces) treats the switchover process as a minor traffic interruption, but not as a failure. When IUA is configured, the SCTP association between the MGC and the Signaling GW is aborted and the MGC reestablishes it as a SCTP client, while the failed board's IUA configuration, automatically downloads to the redundant board.

Boards that handle E1/T1 CAS (MFC R2) perform a switchover with "Warm redundancy" and all active calls are dropped.

Note: A redundant board can not provide the synchronized clock for the entire gateway even when the failed board was configured to do so.

2.5 Security

The Media Gateway 3500 provides the capability to deliver Quality-of-Service (QoS) enhanced secure communications services using packetized data transmission technology to consumers. The purpose of any security technology is to protect items of value, whether a revenue stream, or a purchasable information asset of some type.

Threats to this revenue stream exist when a user of the network uses a technique to avoid the necessary payments. The addition of security technology to protect value has an associated cost, such that the level of increased security is dependent upon the amount of investment of capital and effort. In order to protect the revenue stream, the Media Gateway 3500 provides a built in security technology that protect the system from users with the intent to steal or disrupt network services.

The Media Gateway 3500 security implementations 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.

2.5.1 Media Gateway Threats

Media Gateway's general threats are:

1. 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.
2. 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 Cryptoanalysis** - 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.

3. 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:

   1. Simple snooping
   2. Call Agent clones
   3. Protocol manipulation
   4. Off-line cryptoanalysis
   5. Service disruption

2.5.2 Media Gateway 3500 Security Features

In order to protect the Media Gateway against those threats, the Media Gateway 3500 supports the following security mechanisms over all external interfaces and 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 then 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 2-1: Media Gateway 3500 Interfaces Security profiles

Interface	Confidentiality	Authentication
EMS Server- Client	SSL	Application level - UserID + Password
EMS/NMS - Media Gateway 3500	IPSec (ESP)	IKE pre-shared key
Call Control (Megaco)	IPSec (ESP)	IKE pre-shared key
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

Apart from that, the Media Gateway 3500 is protected against malicious **denial-of-service** (DoS) attacks which part of them are:

- 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.

2.5.3 Media Gateway 3500 Security Technology

2.5.3.1 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 Media Gateway 3500 to assure confidentiality, authentication and integrity for the following media types:

- Control traffic, such as H.248.
- Sigtran over SCTP traffic, such as IUA.
- Management traffic to EMS/ NMS/ OSS, such as SNMP, FTP and Telnet.

2.5.3.1.1 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 and 3DES.
- Hash types for IKE SA are SHA1 and MD5.

2.5.3.1.2 IPSec

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

IPSec specifications:

- Transport mode only.
- 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 and 3DES.
- Hash types for IPSec SA are SHA1 and MD5.

2.5.3.2 SSH

SSH (Secure Shell) provides secure encrypted communication between two distrusted hosts over an insecure network. SSH is the method used to secure the Media Gateway 3500 's Shelf 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

2.5.3.3 SSL/TLS

SSL (the Secure Socket Layer), also known as TLS (Transport Layer Security), is the method used to secure the Media Gateway 3500 '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 Remote Online Software Upgrade

The Media Gateway 3500 Online software upgrade feature provides an efficient way to upgrade software versions on live systems running at remote field sites. The gateway continues its operation uninterruptedly, however calls are dropped on the Media Gateway board being upgraded, while traffic continues on other boards. Media Gateway boards are upgraded one at a time, so the media gateway's capacity is never reduced by more than a single Media Gateway board's capacity. During the upgrade process, certain Media Gateway 3500 features may not be available.

Software upgrade includes the following:

- The ability to upgrade between the last three recent stable software versions.
- The ability to upgrade a system "patch" (some limitations may be applicable)
- The operator can control the upgrade time duration - short time may affect the grade of service (graceful shut down)
- The ability to "rollback" to the previous software version in the event that the upgrade is not functioning correctly
- The ability to "Downgrade" to the previous software in emergency cases (all calls may be dropped in this event)
- Automatic Upgrade process with minimal user interaction (one user controls the entire process).
- "Breakpoints" are provided in which the operator may perform sanity tests and decide whether to proceed with the upgrade or to rollback
- Online detailed progress status during Upgrade process are displayed to allow the operator to monitor progress

Online Software Upgrade covers the following system components:

- System Controller software
- Media Gateway Boards' software
- Ethernet Switch software

Reader's Notes

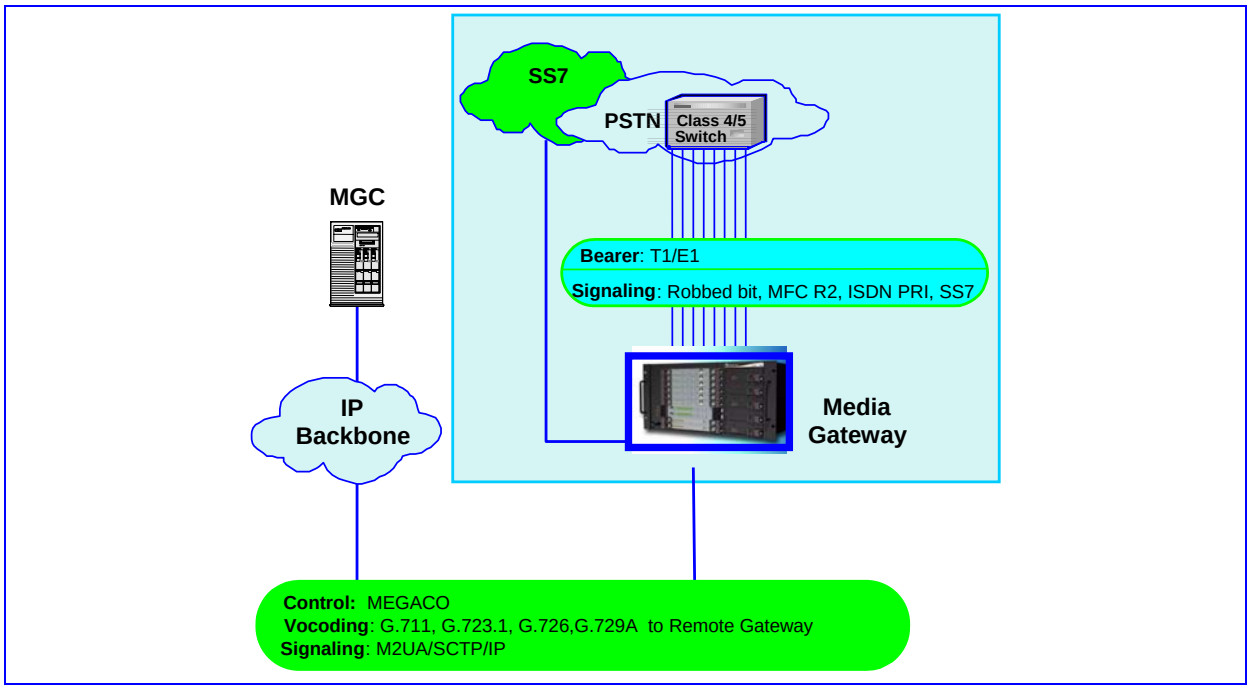
3 Media Gateway 3500 Network Interfaces

The Media Gateway 3500 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 Interface

The Media Gateway 3500 containing TP-1610 blades provides PSTN interconnection via TDM trunks (refer to the figure, "TP-1610 PSTN Interface" below).

Figure 3-1: TP-1610 PSTN Interface



3.1.1 PSTN Protocols

Channel Associated Signaling (CAS) protocols, such as: MFC-R2 can be terminated by the Media Gateway 3500 containing TP-1610 boards. Signaling events terminated by the Media Gateway 3500 are reported through special MEGACO messages, as defined in CAS packages for these protocols. The Soft switch or MSC Server receives the event and can create a new call in response to that event.

The Media Gateway 3500 containing TP-1610 boards supports the following PSTN protocols:

- CAS Protocols
  - Common E1 MFC-R2 CAS protocols
- ISDN Protocols
  - PRI Pan-European (CTR-4)
  - National ISDN 2 PRI
  - ISDN PRI protocol for the Japan - Nippon Telegraph Telephone
  - ISDN PRI protocol for the Australian Telecom
  - ISDN PRI protocol for Hong Kong - HKT
  - ISDN PRI protocol for Korean operator
- Specific ISDN versions are also supported:
  - ISDN PRI protocol for the Lucent/AT&T 5ESS-10 switch
  - ISDN PRI protocol for the Nortel DMS switch
- In Band Tones
  - DTMF detection & generation per TIA 464B
  - DTMF Relay according RFC 2833
  - Real-time Fax over IP/T.38 with superior performance (round trip delay up to 9 sec)
  - Call Progress Tone

Voice calls originating from the PSTN interface, are transported to the Media Gateway 3500's voice-processing mechanism for interconnection to the IP backbones or back to the PSTN backbones.

3.1.2 Clock Synchronization for PSTN Interfaces

When connecting the gateway to PSTN network, the clock synchronization methods that should be applied for the PSTN trunks must be reviewed. Typically, the gateway can receive the synchronization clock from several sources as BITS (Building Integrated Timing Source), SETS (SDH Equipment Timing Source) or from regular E1/T1 trunks. To accomplish this, the clock sources must be prioritized in order to achieve optimal synchronization switches.

The Media Gateway 3500 can operate in either Non-Synchronized or Synchronized mode.

3.1.2.1 Connections for the Non Synchronized Mode

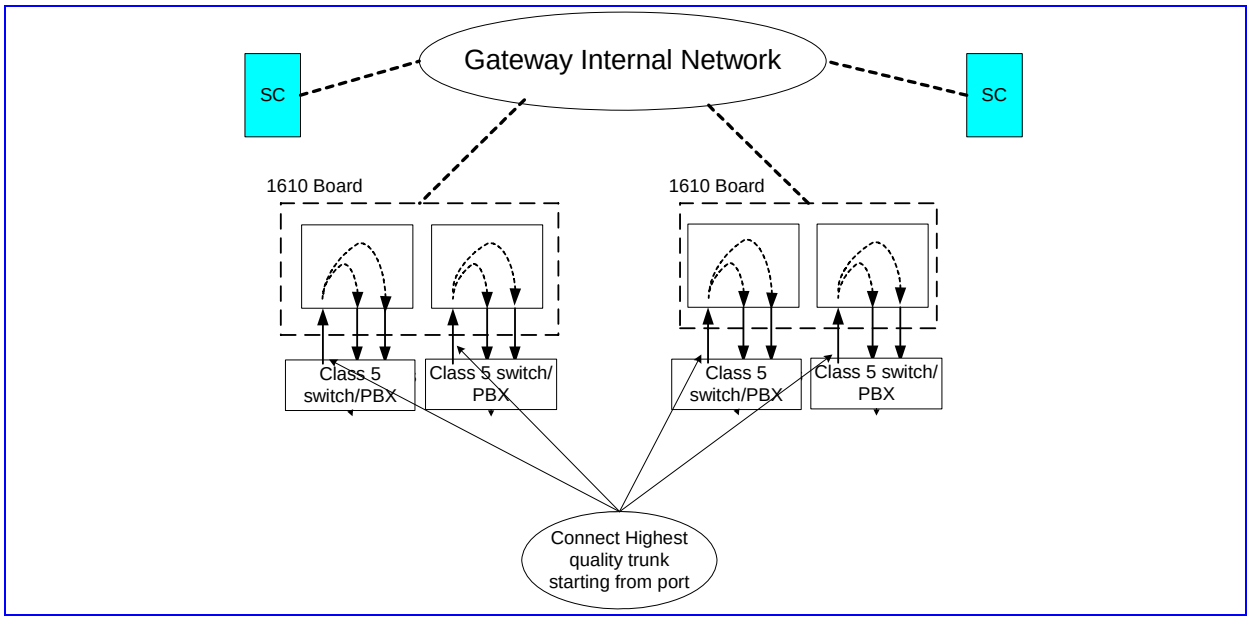
In non-synchronized mode, the gateway is not synchronized to a centralized unique clock. Instead, each 8-trunk group (1-8, 9-16) of every Media Gateway board is internally synchronized, deriving the clock from one of its active trunks.

This mode is the default mode that is used when the gateway terminates the synchronization chain and there is no need for a centralized clock inside the gateway, to synchronize all trunks to that clock.

Some guidelines for connection are:

- When clock quality of the group of 8 trunks is the same, the trunks may be connected arbitrarily.
- When a group includes trunks with different clock qualities, connect the most accurate and stable clock trunks to the Media Gateway board's trunk 9 to 16 (trunk 9 is the highest quality and 16 is the lowest quality.)

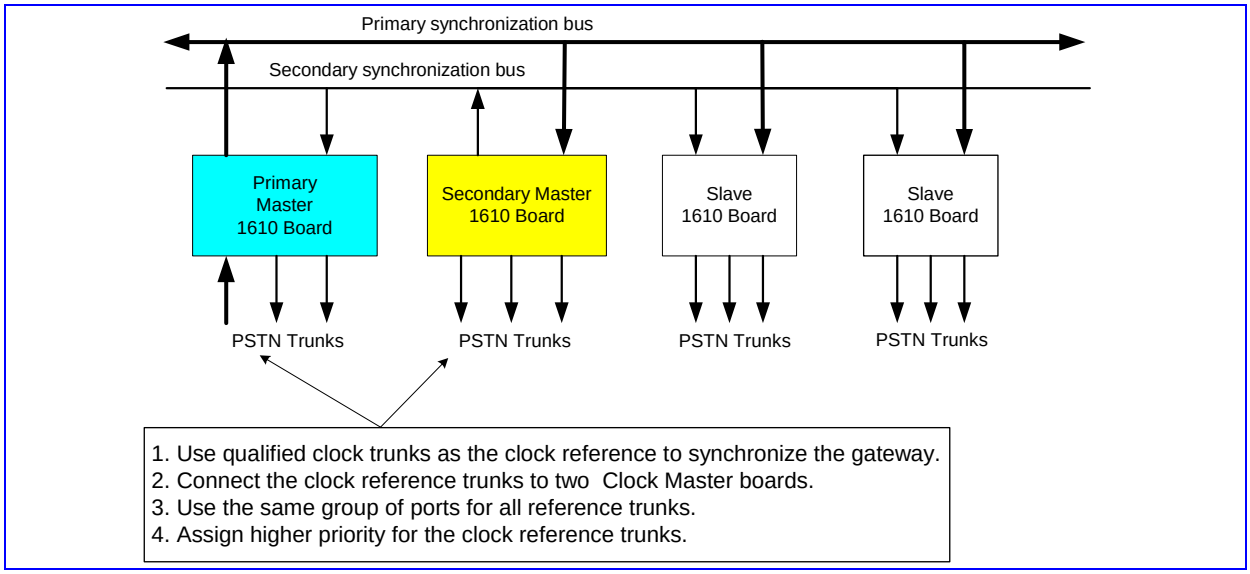
Figure 3-2: Non-Synchronized Mode Connections Diagram



3.1.2.2 Connections for the Synchronized Mode

In synchronized mode, the Media Gateway 3500 operates in synchronization with the PSTN equipment attached to the PSTN interfaces. It derives the synchronization timing from one of the E1 / T1 trunks and distributes the timing to all other synchronous interfaces in the system according to Bellcore GR-1244-CORE line-timing scheme.

Figure 3-3: Synchronized Mode Connections Diagram



3.2 IP Interface

The Media Gateway 3500 supports VoIP services over Ethernet networks. VoIP may be used for transporting PSTN calls over an IP backbone. The Media Gateway 3500 complies with the RTP/RTCP standard (RFC 3550/3551).

The following features are supported on the Media Gateway 3500 IP Interface

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

The media gateway intra-shelf 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.

3.2.1 Connecting to the IP Network

The Media Gateway is connected to the IP backbone via '1+1' Ethernet Switches (ES). Each of the ES can be configured with up to 5 uplinks (see Interface Separation section).

The ES is a cPSB Layer-2 switches that reside within the chassis. These redundant switches allow high available IP connectivity for all boards in the chassis. In order to maintain redundant IP path to ensure high availability, it is important that Media gateway's 1+1 Aggregation Group Uplink would be connected appropriately to the IP backbone.

Generally, two redundant uplinks of the media gateway should be connected to two different L-2 networks. However, these two different L-2 networks should be connected to the same default gateway (IP).

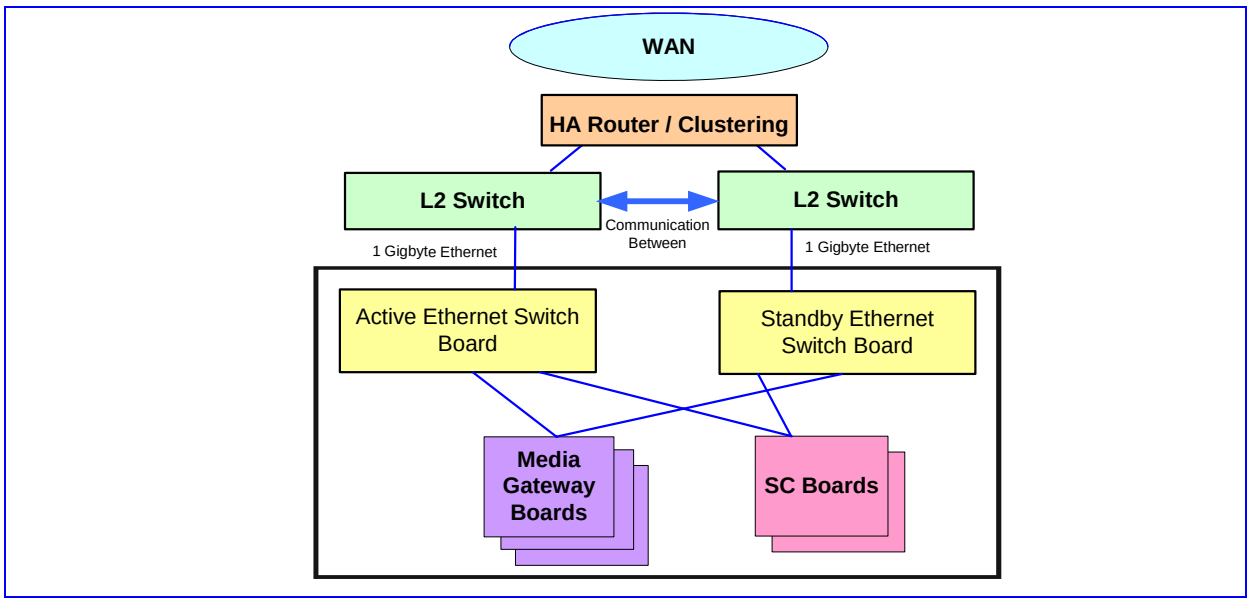
The Media Gateway 3500 can be connected to the IP network in a number of ways to ensure full redundancy. These methods reflect the inherent flexibility of the Media Gateway 3500 to integrate in a number of configurations for back-up purposes. The following are some typical examples:

- **Clustering of Two L-2 Redundant Switches**

In a configuration with the clustering of two L-2 switches, the media gateway's uplink is connected directly to the L2 redundant switches.

This configuration is more economical when more than one Media Gateway 3500 is deployed at a single site. The local communication between multiple Media Gateway 3500 boards passes through the two Ethernet switch boards.

Figure 3-4: Clustering of Two L-2 Redundant Switches



- **One L-2 Switch Network**

In a configuration utilizing a single L-2 switch, the two Aggregation Group Uplinks from both of the ES boards are connected to the same switch.

This is a slight modification of method 1. Because in this method the Switch is subjected to Single Point of Failure, it is not recommend.

3.2.2 Interface Separation

Interface separation provides the Media Gateway 3500 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 Media Gateway 3500 supports between 1 to 3 separate Physical Interfaces as uplinks to the IP cloud. These Interfaces are differentiated according to system protocols mapping.

All Media Gateway 3500 protocols are mapped into the following groups:

- Operation Administration & Maintenance protocols like SNMP, Telnet, FTP, HTTP, etc' are mapped into the OAM group.
- H.248 is mapped into the Control group.
- Media protocols like RTP, RTCP, etc' are mapped into the Media group.

According to the above protocols mapping, the Media Gateway 3500 could be configured to any of the following 4 Interface scenarios:

Table 3-1: 4 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

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

3.2.3 Subnets Separation

When installing the Media Gateway 3500 the user can assign all system IP addresses within a single Local Subnet or alternatively, define the OAM, Control and Media on different Local Subnets. In this case the Media Gateway 3500 could be connected to 3 different LANs and OAM, Control and Media are allocated with different Local IP addresses.

The Subnet Separation feature is partially orthogonal to the Interface Separation feature, as we can define 1 or 2 Interfaces with 3 Subnets, but anyhow the number of the Subnets must be greater or equal than the number of Interfaces.

3.2.4 Static Route Table

Apart from the Subnet Separation, the Media Gateway 3500 holds a Static Route table. Route that are explicitly configured and entered into the routing table take precedence over the Default Gateway. The Static Route capabilities improve the traffic capacity over the IP network and prevent inefficient RTP and other packets routing between routers.

3.2.5 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, Media Gateway 3500 supports the following techniques:

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

Media Gateway 3500 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
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 Media Gateway 3500 supports IEEE 802.1p egress packets marking as well as assignment of packets in ingress and egress queues.

Following QoS service classes' packets are programmable marked by the Media Gateway 3500:

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

Apart from the 802.1p assignment, Media Gateway 3500 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

3.3 Signaling Gateway Interfaces

The Media Gateway 3500 Media Gateway provides SigTran Interworking functionality based on the Internet Engineering Task Force (IETF) Signaling Transport (SigTran) standards. The Media Gateway 3500 is able to provide transport of narrowband ISDN messages received from the circuit-switched PSTN over DS-0s (over E1/T1 links and transport of these messages over IP to a Media Gateway Controller (MGC).

For SigTran Interworking functionality, Media Gateway 3500 supports the following modes of operation:

- ISDN SigTran IUA Signaling Functionality

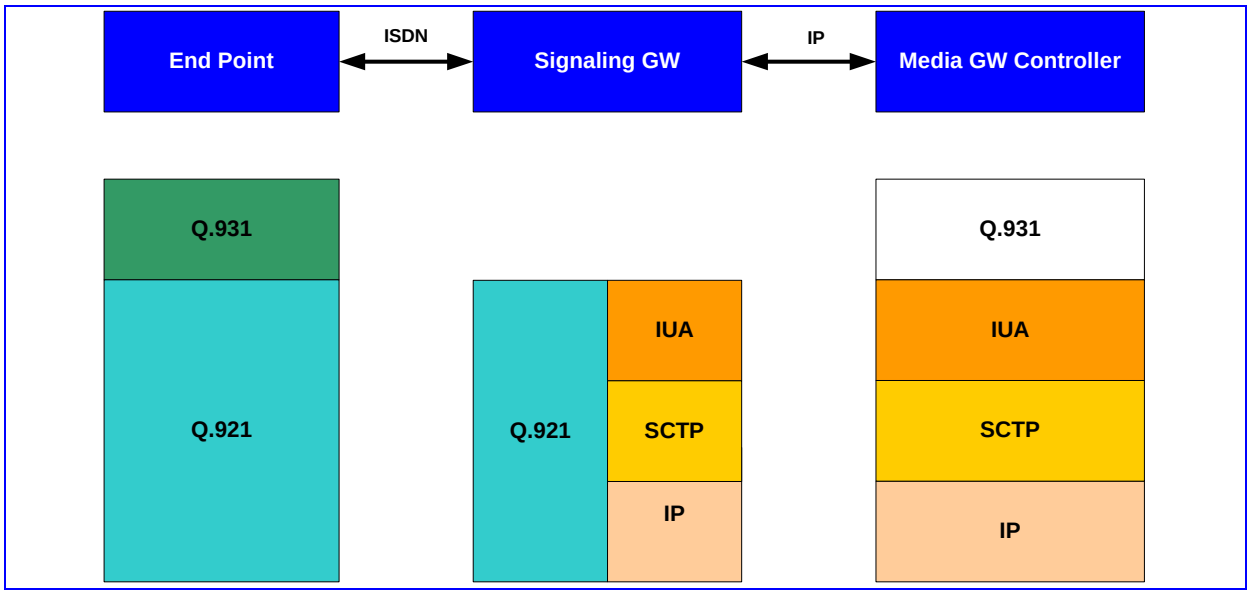
3.3.1 ISDN SigTran IUA Signaling Gateway

The Media Gateway provides IUA/SigTran Interworking functionality based on the Internet Engineering Task Force (IETF) Signaling Transport (SigTran) standards. The Media Gateway 3500 is able to provide transport of ISDN Q.931 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).

3.3.1.1 IUA/SigTran Interworking, Mode of Operations

In an IUA Signaling Gateway, the Media Gateway 3500 terminates the ISDM 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.

Figure 3-5: ISDN SigTran IUA Signaling Gateway Functionality



A signaling message coming into the Media Gateway 3500 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 Control Interface

3.4.1 General

The Media Gateway is a 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 Media Gateway 3500 can be controlled from a Media Gateway Controller (MGC) using standard MEGACO (Media Gateway Control) protocol.

3.4.2 MEGACO Control Protocol

3.4.2.1 MEGACO Overview

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).

3.4.2.2 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 Media Gateway 3500 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

4 Media Gateway 3500 Hardware Elements

4.1 Media Gateway 3500 Hardware Versions

The Media Gateway 3500 is offered with the following hardware configurations:

Media Gateway 3500 + TP-1610 boards - Redundant configuration

4.1.1 Media Gateway 3500 + TP-1610 Board Configuration

The table below details the components of the Media Gateway 3500 + TP-1610 board configuration.

Table 4-1: Components of the Media Gateway 3500 + TP-1610 Board Configuration

Component	Redundant Configuration
Chassis	1
Synchronization and Alarm Rear Transition Module(SA)	2
Ethernet Switch Board - 24 100 Mbps Ports with 2 GbE uplinks (ES/4411)	2
Ethernet Switch 5 I/O Rear Module - (LIM/4411)	2
System Controller (SC)	2
TP-1610 Media Gateway Boards	Up To 6
TP-1610 I/O Rear Transition Module (RTM/1610/Normal)	Up To 5
TP-1610 I/O Rear Transition Module – Redundant (RTM/1610/Redundant)	1
AC or DC Power Supply Modules (PS-1)	3
AC or DC Power Entry Modules (PEM)	1 AC/2 DC
Fan Tray Module (FM)	2
AC or DC Fan Tray Power Supply Module (APM)	2

Figure 4-1: Media Gateway 3500 + TP-1610 Board Configuration

4.1.2 Media Gateway 3500 Accessories Kit

Each Media Gateway 3500 is accompanied by an accessories kit, which includes:

- RS-232 Straight Cable for Console Terminal (not crossed-over)
- RS-232 Straight Cable for Ethernet Switch Console Terminal (not crossed-over)
- AC Power Cable (for AC configurations)
- CD containing Media Gateway 3500 system software
- CDs containing the EMS software (Optional)

For more details about Media Gateway 3500 hardware, see the Media Gateway 3500 Installation, Operation & Maintenance Manual, document # LTRT-907xx.

4.2 Platform Configuration Options

4.2.1 The Media Gateway 3500 + TP-1610 Version Chassis Platform Basic Configurations

The Media Gateway 3500 + TP-1610 version chassis platform can be supplied with the following basic configurations:

- Redundant - all the gateway modules are redundant. The redundant configuration enhances the availability of the system by using redundant units to backup failed units.

Channels can be configured for one of the following:

- Protected - backup capability for the media gateway boards in which voice and signaling trunks are guaranteed constant service
- Non-Protected - no backup capability provided

Beyond the above, configurations may vary according to the precise needs of the customer. The table below summarizes maximum capacities for each configuration given a fully populated chassis.

Table 4-2: Media Gateway 3500 + TP-1610 Version - Maximum Capacities for Simplex and Redundant Configurations

	Redundant
Maximum Number of Voice Channels	
Non-Protected	2,880
Protected	2,400
E1/T1 Trunks	
Non-Protected	96
Protected	80
Time Slots	
E1 - DS-0	
Non-Protected	2,976
Protected	2,480
T1 - DS-0	
Non-Protected	2,208
Protected	1,840

4.3 The Chassis

The Media Gateway 3500 chassis complies with NEBS Level 3 requirements, and conforms to CompactPCI PICMG 2.0 standards. It contains a 10-slot card cage. All component boards have a sturdy, hot-swap cPCI 6U form factor. Boards are inserted from the front and the back and engage the midplane on either side inside the card cage. Slots for the boards are numbered from one to ten on the left of the card cage in the front, for identifying board placement. The midplane contains slot keys to match the appropriate board. This prevents insertion of a board in an wrong location.

The chassis also houses a fan tray unit to the left of the card cage and three Power Supply modules to the right of the card cage and an extractable air filter to the left of the card cage.

Table 4-3: Chassis Dimensions

Dimension	Value
Width	48.3 cm (19 inches)
Height	22.2 cm (8.75 inches)
Depth	
With projections	36.5 cm (13.7 inch)
Without projections	30 cm (11.8 inch)
Weight (Fully loaded)	22.6 kg (49.8 lb)

4.3.1 Chassis Elements Constraints and Dependencies

There are some constraints and dependencies of which the installer should be aware. They relate to the unit's location inside the chassis, or function compatibility between the different units. These are summarized in the following table.

Table 4-4: Chassis Elements Constraints and Dependencies

Element	Dependencies	Constraints	Comments
SC System Controllers		Must be located in slots 1 or 2. Must use SA RTMs.	
SC Satellite Controllers		Uses Network or on-board hard disk	Optional In duplex configuration can be located in slots 8 or 9 instead of Media Gateway board(s)
Ethernet Switch ES/4411	Use in configuration with TP-1610 boards	Gigabit interlink connection must not be connected. Must be located in slots 3 and 4 Slot 3 –1st Ethernet switch board (only slot used in Simplex configuration) Slot 4 – 2nd Ethernet Switch board in redundant	Optical interface solution Includes an RTM (LIM)

Table 4-4: Chassis Elements Constraints and Dependencies

Element	Dependencies	Constraints	Comments
		configurations	
Power Supply Modules	AC or DC Must match the PEM type	3 PS per system	
APM Modules		2 APM per system	
Power Entry Modules (PEM)	AC or DC Must match the Power Supply type		
Fan Tray Unit			A single module contains 5 fans for optimal cooling
SA Synchronization and Alarm Module	Depends on the number of SC boards in chassis	Must be inserted in the rear behind slot 1 or 2 of the SC boards	The current version supports Alarm module only.
TP-1610 board(s) designated as Clock Master	Combined with ES/4411 boards	In the current version each board is self timed from one of the PSTN interfaces in Non-Synchronization mode	

4.3.2 Power Requirements

The Media Gateway 3500 chassis can be powered from either AC or DC sources.

Table 4-5: Power Requirements

Type	Power Requirements	Connection Provisions
AC	100 to 240 V AC, nominal 50/60 Hz	PEMs (Power Entry Modules) with Standard 3-prong quick connect socket (Future Version)
DC	-40.5 to -60 V DC	PEMs with Input terminals

4.3.2.1 Power Consumption

DC Input Power

The average power consumption for a full complement of boards is approximately 460 watts (4 A at 115 VAC, 2 A at 230 VAC and 9.5 A at 48 VDC).

Two Power Entry Modules (PEM), each containing two input terminals, are provided for DC connections on the rear of the chassis. Power is required to be between -40.5 and -60 VDC. Each of the DC input terminal is reverse current protected. The pair of J1 input terminals and the pair of J2 input terminals provide redundancy protection of the power entry circuitry.

Recommendations for DC Power input:

- When using DC power as the primary input, ensure that the power supply complies with the safety requirements of Call Agent CAN/CSA-C22.2 No. 60950-00 and UL 60950, and EN 60950.
- For High Availability, connect two separate DC power sources to avoid total power failure if one of the DC power sources fails.

A standard, properly earthed, quick connect socket (IEC 60320 C20) and associated filtering and circuit breaker are located on the rear panel. The appropriate power cable is provided according to the customer's local standards. Power requirements are 100 to 240 V AC at a nominal 50/60 Hz line frequency.

WARNING

For AC, only one PEM is to be installed in the system.

Recommendations for AC Power input:

- It is recommended to connect the AC power source to a UPS to avoid total power failure if the AC power source fails. This is mandatory for high availability (i.e., on redundant system configurations).
- Connect AC-powered systems only to earthed power outlets.
- Connect the chassis to the facility's earth, using the earthing terminal(s) provided.

4.3.2.2 Cooling System

The Media Gateway 3500 components are cooled by a Fan Tray unit, located at the left of the card cage. The Fan Tray Unit draws air in through a perforated grill at the right side of the chassis.

The incoming air passes through a removable filter (located within the fan assembly, immediately inside the perforated grill), whose honeycombed design prevents RF interference.

The clean air is drawn 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 Media Gateway 3500 via perforated vents of 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 panels are especially constructed to allow optimal air flow within the chassis.

4.3.2.3 Electro Magnetic Compatibility (EMC) Features

The chassis is designed to comply with known EMC/RFI standards, including FCC Part 15, Class B; ICES-003, Class B; EN 55022, Class B; EN 300 386.

Compliance measures include:

- Venting holes - for air intake and exhaust, sized to provide for blockage of frequencies within the specified range
- Blank panels with contact fingers - used for covering empty slots when a configuration requires such
- RFI filters - built-in to the DC power inputs, assuring that conductive interference does not reach the Power Supply Modules, or that switching signals generated by the Power Supply Modules do not propagate over the main feed
- Air filters - integrates a honeycomb EMI shield in its assembly. The honeycomb structure consists of "cells" that are engineered to trap and absorb EMI noise while maintaining 95% to 99% aperture for minimal airflow impedance. A gasket installed around the frame makes sure there is conductivity of the frame to the enclosure.

4.3.3 NEBs Environmental Requirements

The Media Gateway 3500 chassis mechanical envelope complies with the requirements of NEBS GR-63-CORE, Issue 1.

The table below provides a list of the mechanical requirements which were imposed on the chassis design.

Table 4-6: NEBS Requirements

Physical Protection Requirements	Test level	Reference (GR-63 para.)
Humidity	5 to 90%	4.1.2
Altitude	-60 to 4000 m	4.1.3
Fire Resistance		4.2.3

Table 4-6: NEBS Requirements

Physical Protection Requirements	Test level	Reference (GR-63 para.)
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/minute; 100-500 Hz, 0.25 oct/minute	4.4.4
Airborne Contaminants	------	4.5
Thermal Shock	-40° C to +25° C / -40° F to 77° F within 5 minutes +70° C to +25° C / -158° F to 77° F within 5 minutes	5.1.1.1 5.1.1.2

Presently, the system operation is guaranteed under the following conditions:

4.3.3.1 Temperature

Table 4-7: Temperature Range

Temperature Range for Operation	0° C to +55° C
Recommended Ambient Temperature	+5° C to +30° C

4.3.3.2 Humidity

Table 4-8: Humidity Range

Relative Humidity Range for Operation	5 to 90%
Nominal Relative Humidity	70% (wet bulb)

4.3.3.3 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.

4.3.3.4 Altitude

Table 4-9: Altitude Range

Altitude	Up to 3048 m (10,000 ft)

4.3.3.5 Earthquake

Table 4-10: Earthquake Requirements

Earthquake	Zone 4

4.3.3.6 Rack Requirements

Table 4-11: Rack Requirements

Telco Rack	19-inch
Space	As per GR-63-CORE Maintenance access 762 mm (2’ 6”) Wiring access 610 mm (2’)

4.3.4 Electrical Aspects

4.3.4.1 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.

4.3.4.2 Main Midplane Characteristics

The Media Gateway 3500 midplane is designed in accordance with PICMG CompactPCI™ specifications, which include the following features:

- Hot-swapping of boards
- Packet-switching
- Power interface and distribution
- Keying

Hot-swap support allows maintenance of the gateway components during regular gateway operation.

The chassis midplane complies with Packet Switching Backplane (cPSB) standards, supporting up to two PICMG 2.16-compliant Extended Fabric Boards (Ethernet Switch board). This standards compliance enables the use of embedded, fault-tolerant, switched network architecture for higher system performance and reliability. Every board in this architecture is connected by redundant links to each of the Ethernet Switch boards. Accordingly, the Node slots in the chassis are interconnected through Ethernet Switch slots. Nodes operate as standalone "systems in a slot", interfacing each other through an internal IP network.

4.3.4.3 Midplane Keying

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

Note: While the slot keys on the midplane are designed to prevent the insertion of a board in an incorrect location, be sure NOT to force a board into a slot to avoid damaging either the board or the midplane.

4.3.5 Alarm Indicators

The fan module panel contains the alarm indicators (LEDs) Alarm Cutoff and Reset buttons.

The alarm indicators are connected to the fault detection and alarm system provided with the Media Gateway 3500. As needed, LEDs indicate critical, major or minor system faults as well as system and shelf alarms.

Figure 4-2: Fan Tray Unit Panel and Alarm Indicators

Note: Each section describing one of the system component types provides a brief functional specification for the component described. For the functional specifications, refer to 'Media Gateway 3500 + TP-1610 Configuration Selected Functional Specifications' on page 89.

Applicable specifications for the design and construction of the midplane are:

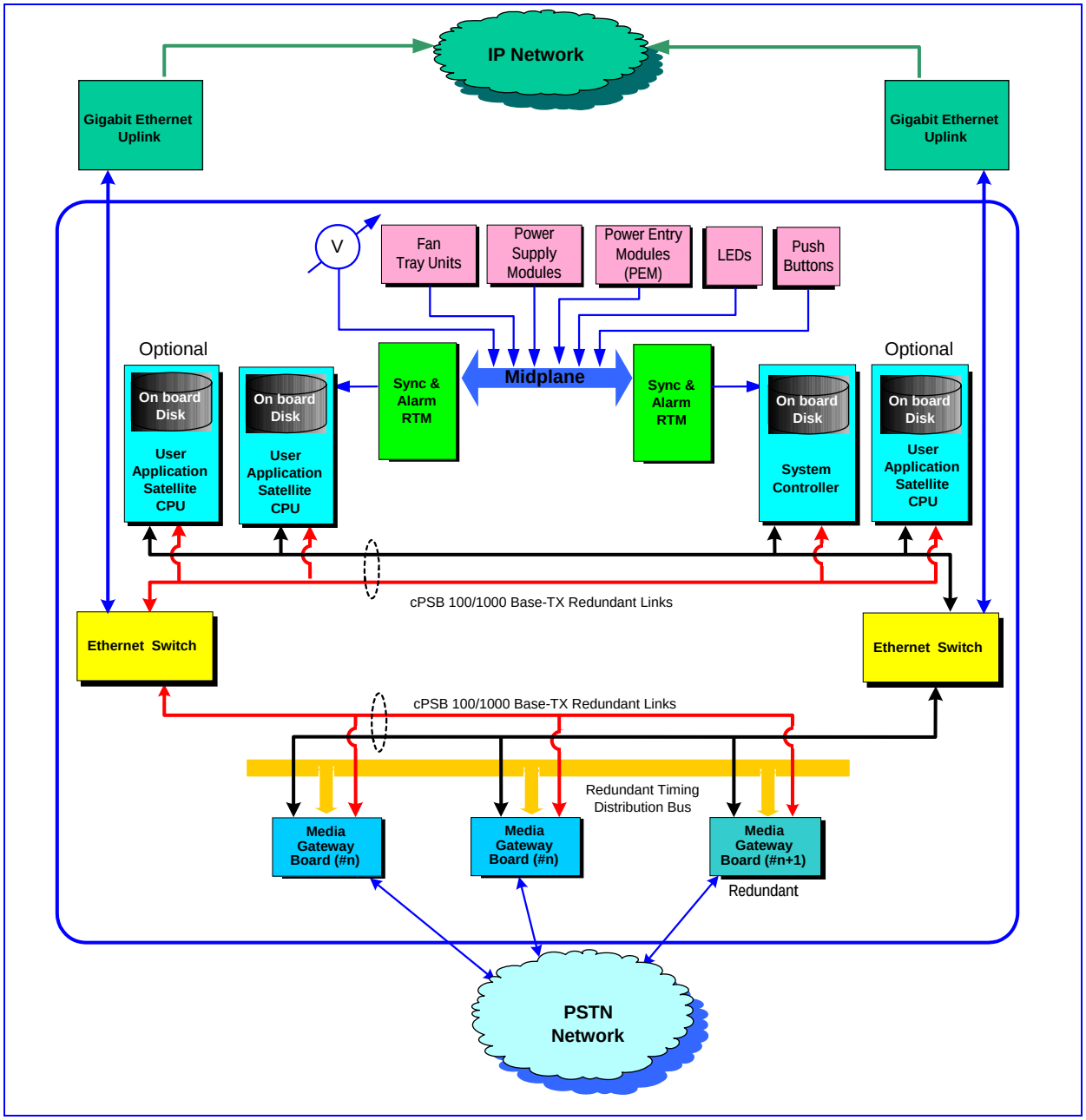
- PICMG 2.0 R3.0, “CompactPCI™ Specification”, October 1, 1999.
- PICMG 2.1 R1.0, “CompactPCI™ Hot Swap Specification”, August 3, 1998.
- PICMG 2.5 R1.0, “CompactPCI™ Computer Telephony Specification”, April 3, 1998.
- PICMG 2.9 R1.0, “CompactPCI™ System Management specification”, February 2, 2000.
- PICMG 2.10 R1.0, “Keying of CompactPCI™ Boards and Backplanes”, October 1, 1999
- PICMG 2.11 R1.0, “CompactPCI™ Power Interface Specification”, October 1, 1999.
- PICMG 2.16 R1.0, “CompactPCI™ Packet Switching Backplane (PSB)”, July 3, 2001.

4.4 Boards and Module Architecture

4.4.1 Gateway Block Diagram

The block diagram of the Media Gateway options are illustrated in the figures below and depicts its functional internal engineering mechanisms.

Figure 4-3: Media Gateway Block Diagram



4.5 TP-1610 & SB-1610 Media Gateway Boards

The TP-1610 VoIP media gateway boards are high-density, hot-swappable, CompactPCI™ resource boards with a capacity of 480 ports supporting all necessary functions for voice, data and fax streaming over IP networks. The board is powered by Voice over Packet processors, and supports 480 independent and concurrent channels with the most demanding algorithms, such as G.168-compliant Echo Cancellation, and a wide set of voice compression algorithms, such as G.723.1 and G.729A.

- The TP-1610 board is appropriate for wireline and cable systems

Each TP-1610 board contains two Voice over Packet (VoP) processor modules, which handle packet-streaming functions through two redundant, on-board 100 Base-TX interfaces. Each processor implements the industry-standard RTP/RTCP packet-streaming protocol for IP transmission, including advanced adaptive jitter buffer management.

The TP-1610 board and RTMs are shown below.

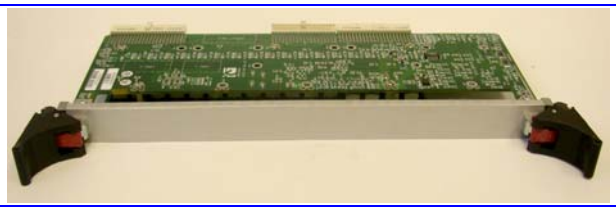
The front panel provides status LEDs for the 16 trunks, both cPSB Ethernet links, board activities LEDs and a standard cPCI blue LED.

The TP-1610 board is accompanied by a Rear Transition Module (RTM) board. There are two types of RTM boards provided, the TP-1610 board providing the standby function for the N+1 redundant configuration is different from the type used for the other TP-1610 boards (i.e. “N” boards in a N+1 configuration). The regular RTM type provides an interface for 16 TDM trunks (E1 / T1 / J1, while the redundant RTM does not have any connections to the PSTN. The PSTN interfaces are internally connected to the RTM module. Thus the TP-1610 board serving as the redundant backup board is identified by a specific RTM board designed for this purpose.

Figure 4-4: TP-1610 Board

Figure 4-5: TP-1610 RTM (RTA-1)

Figure 4-6: TP-1610 RTM (RTA-2 Redundant)



4.5.1 TP-1610 Features

The TP-1610 board has the following features:

- 480 voice/fax/data ports with 16 E1, or 16 T1 integral interfaces
- VoIP packet streaming (RTP/ RTCP) per RFC 3550/3551
- MEGACO (H.248)
- Simultaneous Support for G.711, G.726, G.727, G.723.1, G.729A voice compression Independent vocoder selection per channel
- Silence Suppression supporting VAD (Voice Activity Detection) and CNG (Comfort Noise Generation)
- Automatic Fax Bypass modem
- G.168-2000 compliant Echo Cancellation
- DTMF Detection and Generation to TIA 464B
- PSTN Signaling: CAS, ISDN PRI (11 variants)
- MFC-R2 and Call Progress Tone Detection and Generation
- TDM switching from H.110 bus or from trunk interfaces
- Hot swappable
- Redundant 100 Base-TX packet interface
- Single-slot compactPCI™ (cPCI) 6U board
- Physical connectio nto the E1.T1 via the Rear Transition Module
- PICMG 2.1 for Hot-swap support
- PICMG 2.5 for H.110 support
- cPSB (PICMG 2.16) support
- Management Interfaces: SNMP V2, Embedded Web Server, Syslog

4.5.2 TP-1610 Functional Specifications

Table 4-12: TP-1610 Functional Specifications

Function	Specification
Capabilities	
Capacity	480 independent digital voice, fax or data ports
Silence Suppression	Voice Activity Detection (VAD) & Comfort Noise Generation (CNG)
Echo Cancellation	G.165 and G.168 2000, with 32, 64 or 128* msec echo tail (* 128 with reduced channel capacity)
Trunk-side Gain Control	Controlled via MGCP or MEGACO. Programmable Default gains.
Gain Control	Programmable
Signaling	
DTMF & Tone Signaling	DTMF detection and generation per TIA 464B MFC-R2, detection and generation Call progress Tone detection and generation
PSTN	MFC-R2, ISDN-PRI (11 variants)
Media Gateway Control & Management	
Control Protocols	MEGACO (H.248)
Operations Management	Board is internally managed by the System Controller using proprietary protocol (TPNCP)
Interfaces & Transport	
IP	Dual-redundant 10/100 Base-TX Ethernet ports, via PICMG 2.16 cPSB backplane
Backplane	PICMG 2.1; ; PICMG 2.16 cPSB; PICMG 2.5; PICMG 2.9
Media Gateway Board Control	Via Ethernet
Ethernet	Dual redundant 100 Base-T ports, RJ-45 connectors off rear I/O, cPSB PICMG 2.16 on the backplane
PSTN (TDM)	Up to 16 E1 or 16 T1 ports, rear panel I/O module using two 50-pin Telco connectors (DDK 57AE-40500-21D) each handling 8 E1 / T1 ports.
TDM Interfaces	H.110 CT Bus interface PICMG 2.5, double loaded
HotSwap	Full hot swap supported PICMG 2.1
Power Consumption	38 watt typical

Table 4-12: TP-1610 Functional Specifications

Function	Specification
Power Supply	3.3 V, 5 V
Host Interface	Ethernet
Mechanical	6U single cPCI slot PICMG 2.0, R3.0 CompactPCI™ board

4.6 System Controller (SC) Board

The System Controller (SC) SBC (Single Board Computer) board, shown below, controls and monitors the Media Gateway 3500 operation. The SC 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.

The Media Gateway 3500 contains two SC boards, which are installed into their 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 CompactPCI standards for high-availability systems. It supports hot-swap operation, system management and environmental monitoring. The SC board has two PCI Mezzanine Connectors (PMC), one is occupied by the SC board with on-board hard disk and the second is reserved for future expansion of board functionality.

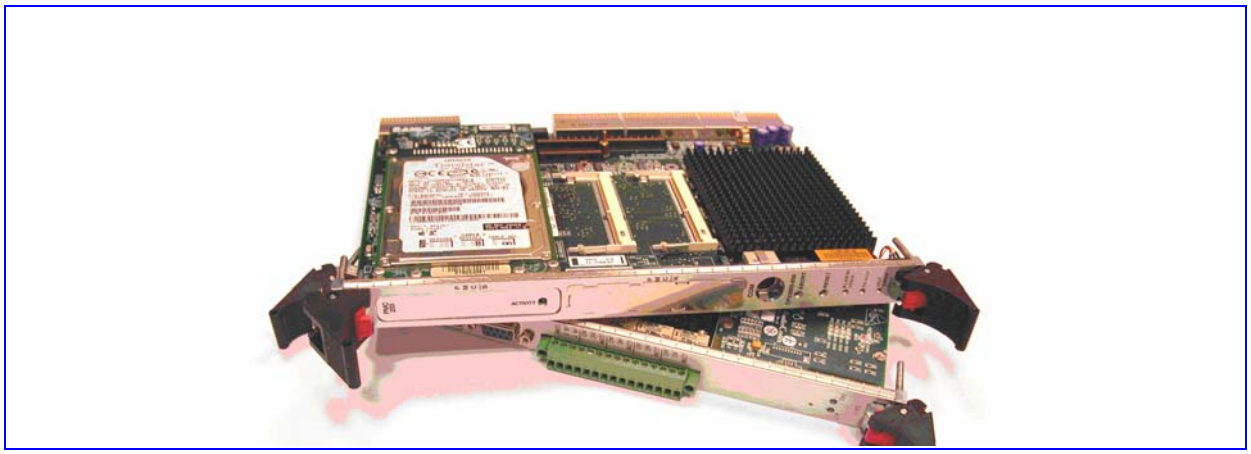
The two 10/100 Base-TX redundant Ethernet ports connect the SC board with the two Ethernet Switch boards via cPSB dedicated links in the midplane. The front panel PS2 COM serial port provides RS-232 console connection.

Note: The RS-232 console connection can be made via the SC front panel PS2 Com serial port or via the RS-232 serial port on the SA RTM.

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. A future version of the SA Rear Transition Module is to assist the System Controller(s) to provide Stratum 3/3E synchronized clock functionality for gateway synchronization. For more information on the SA board, refer to "SA RTM" on page 58.

Figure 4-7: System Controller (SC) Board and Synchronization & Alarm (SA) RTM



4.6.1 SC Major Features

- Modular platform
- Carrier grade
- PIGMG cPCI compatible
- UltraSPARC™ IIi 650 MHz processor with on-chip secondary cache
- Solaris™ operating environment
- 512 Mbyte on-board EEC memory (1.5 Gbyte expandable memory)
- Integrated dual-redundant channel Fast Ethernet interface
- On-board carrier grade 7/24 60 Gbyte hard disk
- 2-level watchdog timer
- 8 Kbyte NVRAM
- 8 Mbyte on-board Flash memory
- 7 Mbyte on-board User flash
- NEBS compliant
- 1 PS2 serial RS232 port
- 1 USB port
- 2 PMC modules support to expand boards functionality
- Upgradeability support

4.6.2 SC Functional Specifications

Table 4-13: SC Board Functional Specifications

Function	Specification
Capabilities	
Processor	650 MHz UltraSparc™ VIS instruction set, binary compatible with SPARC application software
OS Software	Solaris 8/9 Operating Environment
Cache	L2: integrated 4-way, 512 KB cache
Memory	512 Mbyte on-board EDC (Error Detection and Correction) memory Expandable memory: up to 1.5 Gbyte using SO-DIMM memory module)
Mass Memory	60 Gbyte on-board hard disk
Flash Memory	8 MB on-board flash 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)
PMC	PMC (PCI Mezzanine Card) slots One slot is occupied with on-board PMC 60 GB hard disk
IP	Dual-redundant 10/100 Base-TX Ethernet ports; PICMG 2.16 R1.0 CompactPCI Packet Switching Backplane compliant
Front Panel controls/ indicators	Reset (POR) and Abort (XIR) pushbuttons Hot Swap Blue LED, Alarm LED, Power LED

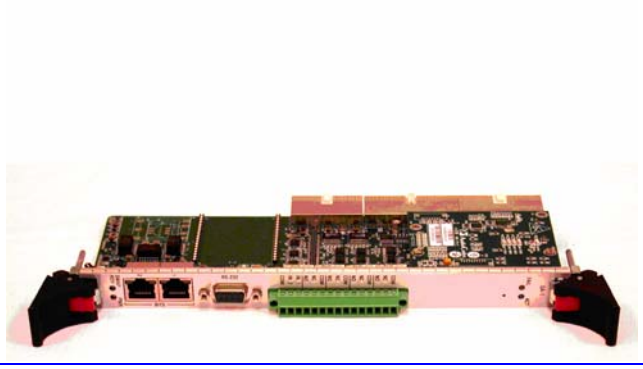
4.7 Synchronization and Alarm (SA) RTM

The Synchronization and Alarm Module (SA) is a rear alarm 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, by controlling the fans' operation, monitoring the proper operation of the power supply modules, monitoring the midplane voltages, to control 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.

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.

A future version or the SA board is to include a clock synchronization functionality according to SONET/SDH synchronization requirement. This can synchronize the gateway to external reference interfaces or supply an internal clock when all the external references are unavailable. The quality of the internal clock is according to SONET Stratum 3/3E / SDH slave equipment (SEC) as per ITU G.813.

Figure 4-8: Synchronization & Alarm (SA) RTM



The gateway software uses the Synchronization and Alarm module to monitor and to control the chassis operation. The gateway reports any abnormal conditions as they occur in the form of managed alarms. Each alarm includes an indicator to correspond to the severity. In addition, 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. When the reported alarm is resolved, the gateway detects that the alarm has been cleared and reports as appropriate. The connection is done using terminal block connector on the front of the SAT (gateway's rear side).

The 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.

The system status can be monitored via the Element Management System (EMS) for, or via the gateway SNMP interface. For more information refer to the *EMS User's Manual* (Document # LTRT-963xx).

The following list summarizes the SA 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

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 and improves the MTBF of the cooling fans.

Table 4-14: SA Functional Specifications

Function	Specification
Power Consumption	150 mA at 5V 450 mA at 3.3V 110 mA at 12V 50 mA at -12V

4.8 Ethernet Switch

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.

The ES/4411 boards have 1 GbE optical Uplink for connecting to external equipment. The fiber-optic Gigabit ports (1000 Base-SX) are located on the front panel of the Ethernet Switch board.

The Ethernet Switch optical interface board, shown below, is capable of sending all Ethernet signals through the midplane. It complies with cPCI Extended Fabric Board standards, utilizing a PICMG 2.16-compliant packet switching matrix onto a cPCI midplane, enabling the use of embedded, fault-tolerant, switched network architecture for higher system performance and reliability.

The ES/4411 Ethernet Switch board provides the following:

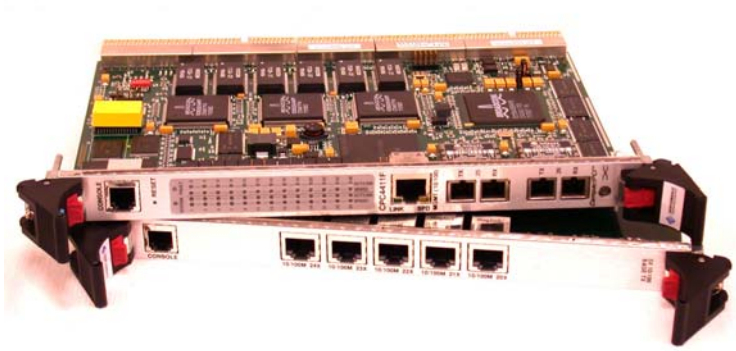
- 24 10/100 Mbps cPSB-compliant and 2 1000Base-SX ports Ethernet ports, where 9 are connected to the Media Gateway 3500 midplane slots and one GbE 1000Base-SX for connecting to external equipment
  - 8K MAC addresses
  - 802.1p priority queuing (4 classes of service per egress port)
  - 802.3-2000 Link Aggregation (up to 6 groups, 8 ports per group)

- Front or rear panel console port (RS-232)
- Front panel LEDs indicating system status, link, speed, and activity
- Power-On diagnostics
- Support for hardware connection layer of PICMG 2.1 Hot Swap

■ Single-slot Rear Transition Module provides 5 100Base-T ports, plus console

The ES/4411 RTM provides five 100 Base-T ports of the 24 ports.

Figure 4-9: ES/4411 Ethernet Switch Board and RTM



The Media Gateway 3500 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.

4.8.1.1 ES/4411 Ethernet Switch Optical Interface Functional Specifications

Table 4-15: ES/4411 Ethernet Switch Board Functional Specifications

Function	Specification
Switching Capacity	Dual 44 Gbps, non-blocking wire speed switching fabrics
Latency	Wire speed
Configuration	Up to 5 10/100/1000 Base-T Uplink ports 19 ports 10/100/1000 Base-T midplane-switched ports
Breakout Options	10/100/1000 Base-T links over the mid plane, plus 1000 Base-TX via the rear panel (Copper version)
Frame Processing	Store and forward, Layers 4-7 filtering
MAC Addresses	16,000

4.9 Power Supply PS-2 Modules

4.9.1 Power Supply Features

- AC or DC input (AC is to be implemented in an up-coming version)
- Universal 100 to 240 V AC input (Future version)
- Power factor correction (AC input) (Future version)
- Class B EMI input filter (AC input) (Future version)
- Wide range -36 to -72 V DC input
- Active current load sharing on positive outputs (V1, V2 & V3)
- DC input, reverse-polarity protected
- Integral LED status indicators
- Hot-pluggable connector, with staged pin lengths
- Hot swappable
- Optimized thermal management
- No minimum load, any output
- Control & monitoring features

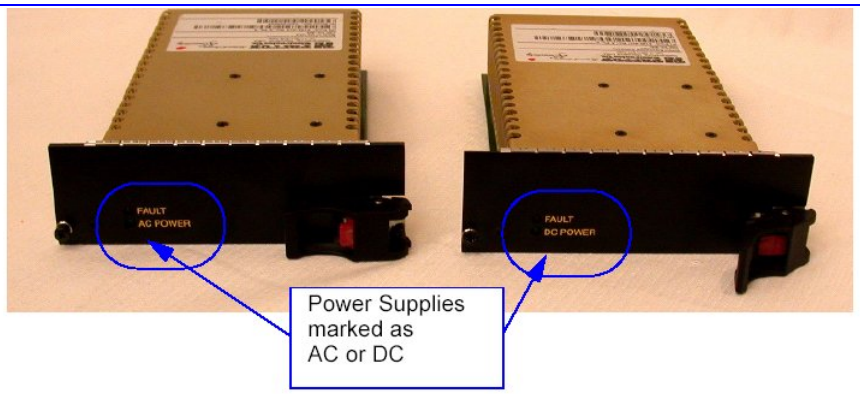
Power for the Media Gateway 3500 is typically provided from redundant DC power feeds, whose input voltage ranges from -36 to -72 V DC to accommodate nominal -48 and -60 V DC mains. Optionally, the Media Gateway 3500 can be powered by an AC power source, operating from 100 to 240 V AC. Power supply units function in a load-shared configuration to provide necessary voltages and failsafe operation.

ThePS-2 power supply, shown in in the figure below, is an advanced-design, multi-output switching power supply, which can be provided in either AC or DC primary input power configurations. This power supply can provide, on a continuous basis, four separate outputs: +3.3 V, +5 V, +12 V and -12 V for a total of 250 watts.

AC power cables are provided as per the customer's local standards.

The power supply comes in an ultra-compact design measuring 4 x 12.7 x 28 cm (1.6 x 5 x 11 inch), for a 6.8 watt/inch^3 power density output. The unit has a handle for easy removal and re-insertion, under power (hot-swap capable).

Figure 4-10: PS-2 Power Supply



Note: The Power Supply and the PEM must be of the same type, either AC or DC.

4.9.2 Power Supply Functional Specifications

Table 4-16: PS-2 Functional Specifications

Function	Specification
Output	
Output Power	250 watts maximum, continuous
Outputs (V1-V5)	+3.3 V at 40 A; +5 V at 40 A; +12 V at 5.5 A; -12 V at 1.5A
Temperature Coefficient	+/- 0.02% / ºC
Controls & Signaling	TTL

Table 4-16: PS-2 Functional Specifications

Function	Specification
AC Input	
PEM/AC	Power Entry Module for AC
Input	100 to 240 V AC
DC Input	
PEM/DC	Power Entry Module for DC
Input	-40.5 to -60 V DC
Frequency	47 to 63 Hz
General Characteristics	
Efficiency	75% at full load
Safety Standards	EN 60950, UL 1950, CSA 22.2 No. 950

Reader's Notes

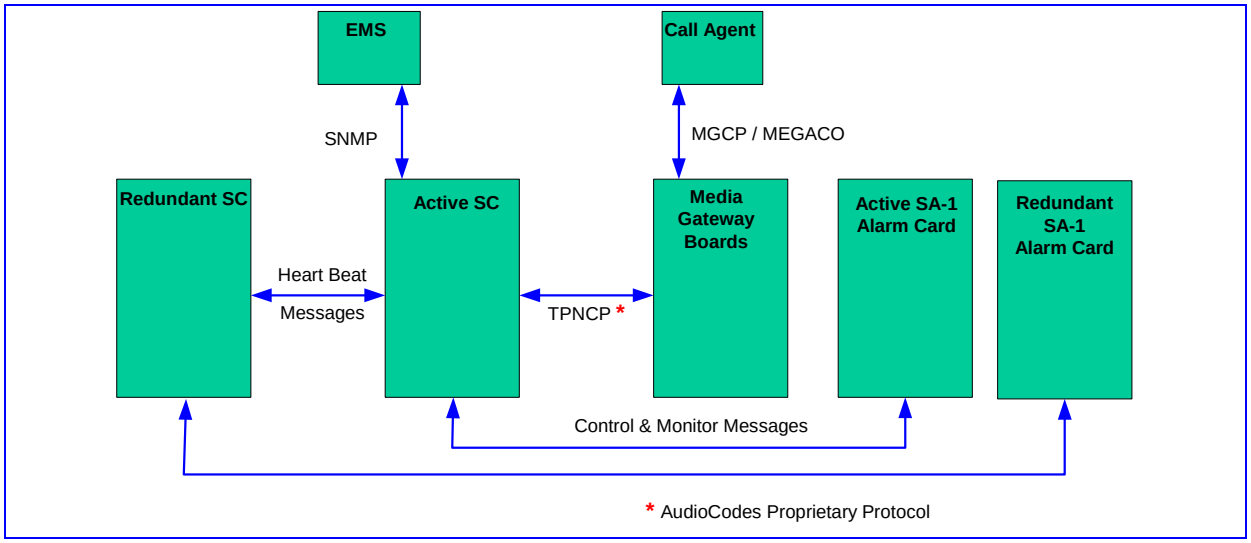
5 Media Gateway 3500 Software Architecture

5.1 Media Gateway 3500 System 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 figure below illustrates the Media Gateway 3500 System protocol architecture.

Figure 5-1: System Protocol Architecture



Single Management Entity

The management API provides a single point of management for the EMS, NMS or any other management system in the network. OAM Tasks are directed from the EMS through SNMP and carried out by the SC board.

Chassis Management

Through the SA RTM residing behind the SC board, the SC board monitors the various hardware elements in the chassis. It also controls the fan speed to insure sufficient cooling. Any hardware failure is detected and reported to the EMS.

Control and Media Protocols

The Media Gateway Controller is directly connected with the Media Gateway boards. In this mode, the Media Gateway Controller controls each of the boards as a stand alone media gateway.

Active/Standby Switchover

The System Controller software monitors the work of the system and handles the switchover of redundant hardware components from standby to active mode in case of a failure (redundant SC, Media Gateway boards, redundant clock sources, etc.).

SC Switchover

Active / Standby redundancy modes are implemented using “heart beat” messages from the SC board that is in active mode to the SC board that is in standby mode, which keeps the standby board constantly ready should it have to assume the current state of the active board. A “Global IP address” (in addition to the individual IP addresses of each of the two SC boards) is attached to the current active SC board and is used by external entities for communicating with the system.

Media Gateway Board Switchover

Media Gateway boards are constantly monitored by the active SC. If the Media Gateway 3500 is equipped with the optional PSTN Redundancy feature and a Media Gateway board fails, the software redirects the trunks connected to the faulty board toward the redundant board and assigns the IP address of the failed board to the redundant board.

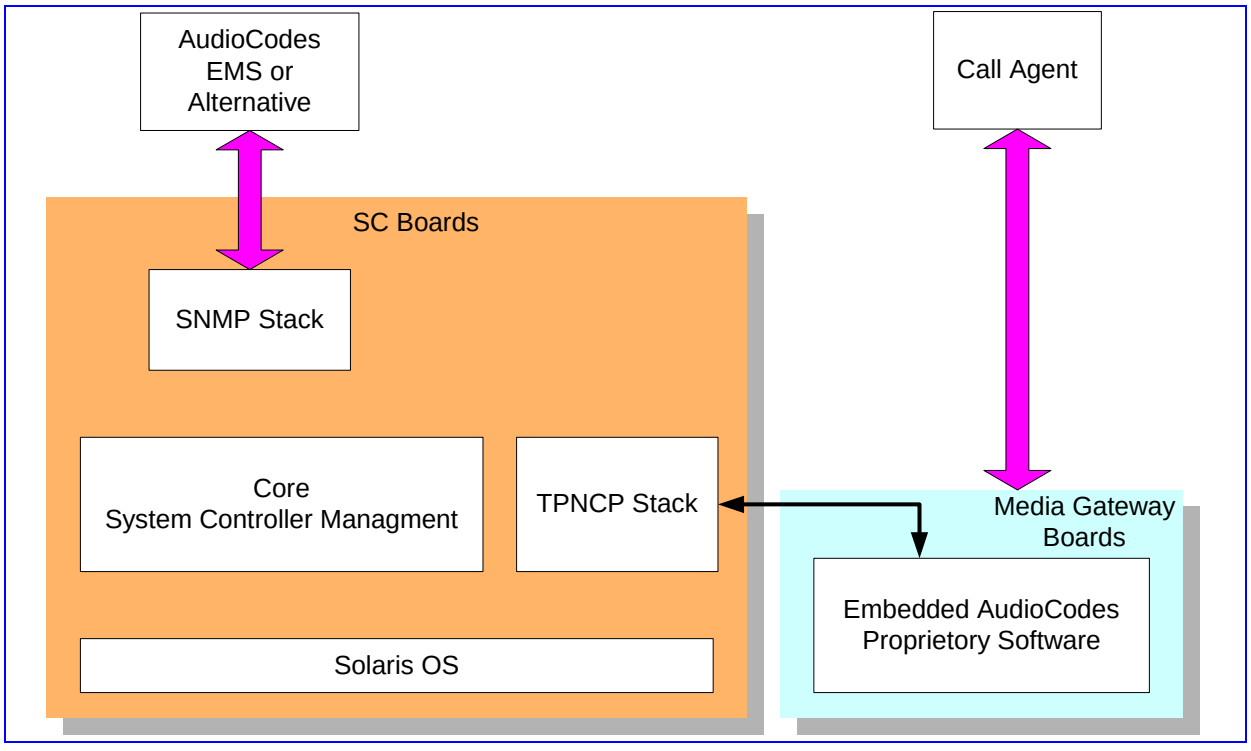
5.2 The SC and Software Architecture

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 Media Gateway 3500.

Figure 5-2: Software Architecture



5.2.1 SC Software Modules

- **Core Process**

  The Core process is the main management process in the System software. It communicates with all other processes and receives events, requests and issues commands from/to all interfaces: SNMP, board management etc. Core processes maintain an internal database, which models both the configuration and the states of each element in the system. This database is the infrastructure for all management tasks done by the core process. The Configuration database is an hierarchical database in which every physical / logical entity in the system is represented by an Managed Object (MO). This MO holds all attributes of the entity as well as its management logic.

- **Watchdog**

  This process is responsible for bringing up all processes in the system and monitoring them. If one of the processes fails, it brings down the SC and switches over to the redundant module.

- **BootP**

  The BootP server is included for downloading software to the Media Gateway boards

- **SNMP**

  The System Controller Software includes an SNMP agent, which processes the SNMP messages originating from the EMS. The System Controller Software allows the user to utilize SNMP to read configurations, update them, monitor the state of the system and control its operation.

- **CLI for Debugging Tasks**

  - Out-of-band management to the Media Gateway
  - Various log files for debugging purposes
  - Various ad-hoc traces

5.2.2 Media Gateway Board's Software

The embedded proprietary software of the Media Gateway boards performs necessary Gateway Voice over Packet Functions and Call Control processes, such as Megaco, 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 proprietary media gateway control protocol (TPNCP).

5.3 Management API

A comprehensive management API enables efficient management interfaces between the Media Gateway 3500 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.

6 EMS for Media Gateway 3500

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 Service Providers 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).

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 10 concurrent clients connected to the server).

EMS Server, running on a Sun™ Microsystems' Solaris™. All management data is stored in the server, using Oracle *9i* relational database software.

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 (Media Gateway 3500 and other gateways), even while having different software versions running on these Media Gateways.

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

  1. "**F**ault Management" on page 77
  2. "**C**onfiguration Management" on page 80
  3. "**A**ccounting Management" - not applicable
  4. "**P**erformance Management" on page 82
  5. "**S**ecurity Management" on page 85

- 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.

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

6.2 EMS Specifications

- Software Version Number: 3.xx
- Release Date: Qxx 20xx
- Package and Upgrade Distribution: CD-ROM

The EMS controls one or more Media Gateways. One EMS can simultaneously manage up to 100 different digital Media Gateways.

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 ▪ Alarm processing: 30 traps per second, continuously ▪ Alarm archiving: at least a one-month history for up to 1100 Media Gateways (depending on disk size available) ▪ Application includes context-sensitive Alarm Browser with filtering and sorting options, detailed alarm description, actions processing and Alarms History ▪ Automatic Alarm Clearing ▪ Traps Forwarding to Northbound Interface ▪ Save alarms in *.csv file
Configuration Management - Monitoring	Summary of all the managed Media Gateways' statuses in one screen with "drill down" hierarchy. Color scheme shows element alarm severity, redundant and switchover states.
Configuration Management – 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 ▪ Configuration database of small Media Gateways is kept inside the EMS ▪ Configuration database of large Media Gateways is kept inside the Media Gateways
Configuration Management – Software Distribution (for small Media Gateways)	Media Gateway software files and Regional properties files (such as Voice Prompts, CAS and other files) can be downloaded to the set of Media Gateways.
Security Management	Authentication-based operator access according to operator security level group. Actions Journal of all operators' activities.

Table 6-2: User Interface and External Interfaces Specifications

Subject	Description
User Access Control	Login + Password to EMS application
Northbound Interface	SNMP v2c traps
Southbound Interface	SNMPv2c, HTTP (MD5 encrypted)
Multi-Platform	Java-based, JDK version 1.4.2
Relational Database	Oracle 9i relational database is used for data storage
Internationalization	Multi-language support ready application

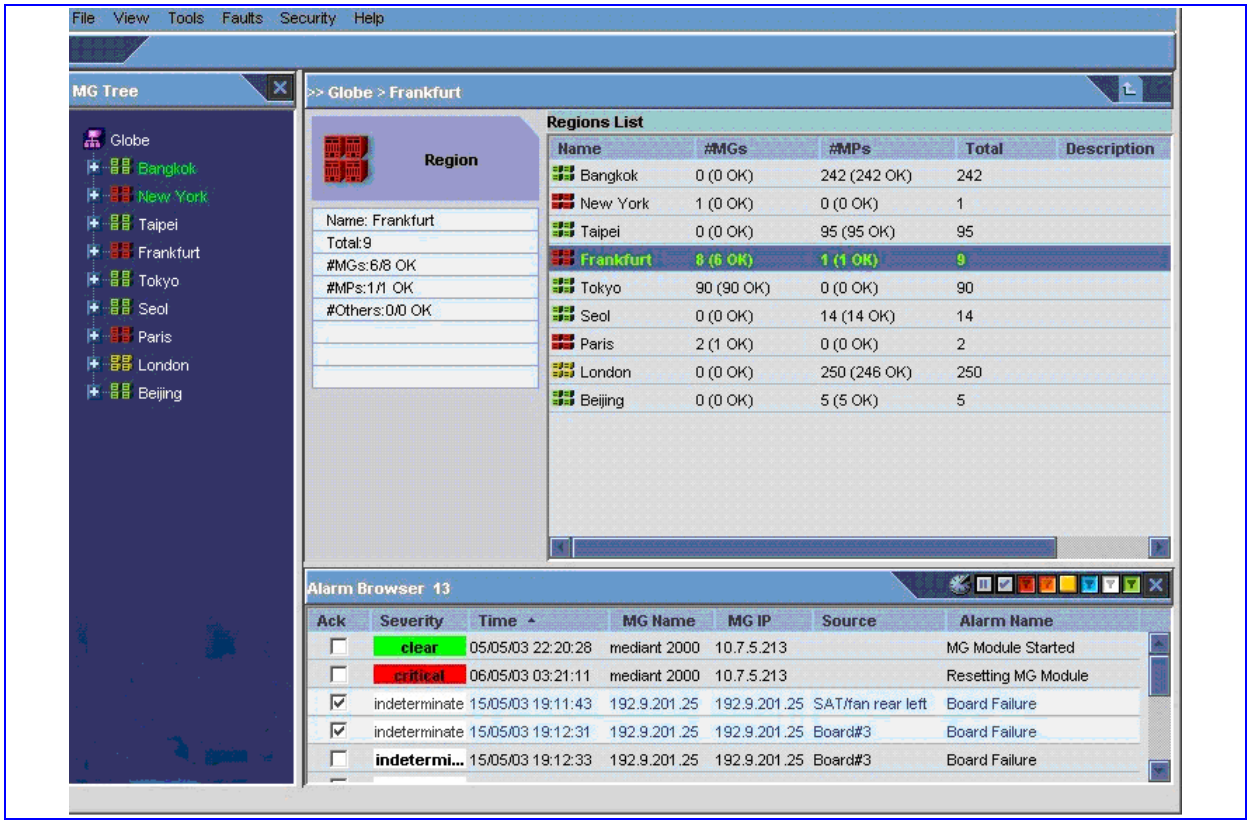
6.3 System Requirements

Refer to the EMS Product Description for the hardware and software requirements necessary to run the EMS.

6.4 Fault Management

The EMS's fault management functionality manages and presents all alarms 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 6-1: Alarm Browser in EMS Main Screen



6.4.1 Alarm Processing

The EMS can typically process 30 alarms 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.

6.4.2 Alarm Context-Based View

The EMS Alarm Browser displays alarms 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.

6.4.3 Alarm Priorities

According to industry-standard management and communication protocols (ITU-T Recommendation X.733, 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.

6.4.4 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)*.

6.4.5 Traps Forwarding to the NMS

All traps received by the EMS from managed Media Gateways can be forwarded to the NMS (Network Management System) as SNMPv2 traps.

6.4.6 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.

6.4.7 Alarm Types

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

a. **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.

b. **QoS Alarm:** alarms notifying operators of Quality of Service degradation

c. Processing Error Alarm: software or processing fault

d. **Equipment Alarm:** alarms associated with an equipment fault, such as board or power supplier failures.

e. Environmental Alarm: alarms such as temperature, power, fire, etc., associated with the physical environment in which the equipment is located.

6.4.8 Alarm Actions

Operators can perform the following actions regarding the displayed alarms:

- Acknowledge: informs operators that a problem diagnosis is underway.
- 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.

6.4.9 Detailed Information

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

6.4.10 Filtering Options

In addition to alarms displayed according to their context (entity) selected, alarms can be filtered according to their severity level, acknowledge status, and Date and Time (in Alarms History).

6.4.11 Change Alarm Browser View

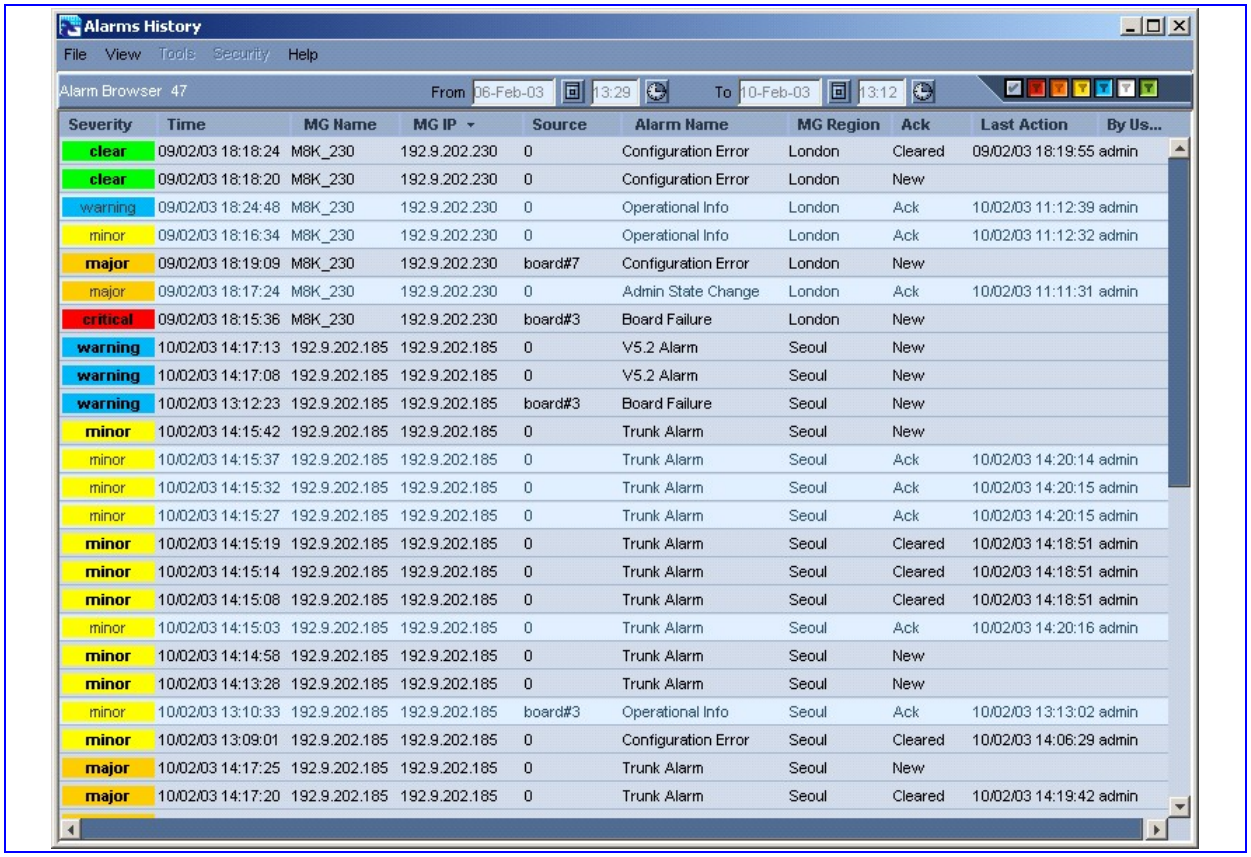
Operators can modify the Alarm Browser's column order according to their preference. In addition, alarms can be sorted by any column (default sorting is according to time).

6.4.12 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 6-2: Alarm History Screen



Severity	Time	MG Name	MG IP	Source	Alarm Name	MG Region	Ack	Last Action	By Us...
clear	09/02/03 18:18:24	M8K_230	192.9.202.230	0	Configuration Error	London	Cleared	09/02/03 18:19:55	admin
clear	09/02/03 18:18:20	M8K_230	192.9.202.230	0	Configuration Error	London	New		
warning	09/02/03 18:24:48	M8K_230	192.9.202.230	0	Operational Info	London	Ack	10/02/03 11:12:39	admin
minor	09/02/03 18:16:34	M8K_230	192.9.202.230	0	Operational Info	London	Ack	10/02/03 11:12:32	admin
major	09/02/03 18:19:09	M8K_230	192.9.202.230	board#7	Configuration Error	London	New		
major	09/02/03 18:17:24	M8K_230	192.9.202.230	0	Admin State Change	London	Ack	10/02/03 11:11:31	admin
critical	09/02/03 18:15:36	M8K_230	192.9.202.230	board#3	Board Failure	London	New		
warning	10/02/03 14:17:13	192.9.202.185	192.9.202.185	0	V5.2 Alarm	Seoul	New		
warning	10/02/03 14:17:08	192.9.202.185	192.9.202.185	0	V5.2 Alarm	Seoul	New		
warning	10/02/03 13:12:23	192.9.202.185	192.9.202.185	board#3	Board Failure	Seoul	New		
minor	10/02/03 14:15:42	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	New		
minor	10/02/03 14:15:37	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Ack	10/02/03 14:20:14	admin
minor	10/02/03 14:15:32	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Ack	10/02/03 14:20:15	admin
minor	10/02/03 14:15:27	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Ack	10/02/03 14:20:15	admin
minor	10/02/03 14:15:19	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Cleared	10/02/03 14:18:51	admin
minor	10/02/03 14:15:14	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Cleared	10/02/03 14:18:51	admin
minor	10/02/03 14:15:08	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Cleared	10/02/03 14:18:51	admin
minor	10/02/03 14:15:03	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Ack	10/02/03 14:20:16	admin
minor	10/02/03 14:14:58	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	New		
minor	10/02/03 14:13:28	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	New		
minor	10/02/03 13:10:33	192.9.202.185	192.9.202.185	board#3	Operational Info	Seoul	Ack	10/02/03 13:13:02	admin
minor	10/02/03 13:09:01	192.9.202.185	192.9.202.185	0	Configuration Error	Seoul	Cleared	10/02/03 14:06:29	admin
major	10/02/03 14:17:25	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	New		
major	10/02/03 14:17:20	192.9.202.185	192.9.202.185	0	Trunk Alarm	Seoul	Cleared	10/02/03 14:19:42	admin

6.5 Configuration Management

6.5.1 Monitoring Media Gateway Status

- Media Gateway 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 element is represented by an icon, each icon being 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 Gateway's status as well as with the overall network status for all Media Gateways managed by the EMS.

- 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, Ethernet Switch, TP, Alarm Card) and trunk status for TP boards. All hardware entities' alarm statuses are graphically represented: power supplies, fans, and hard disks.

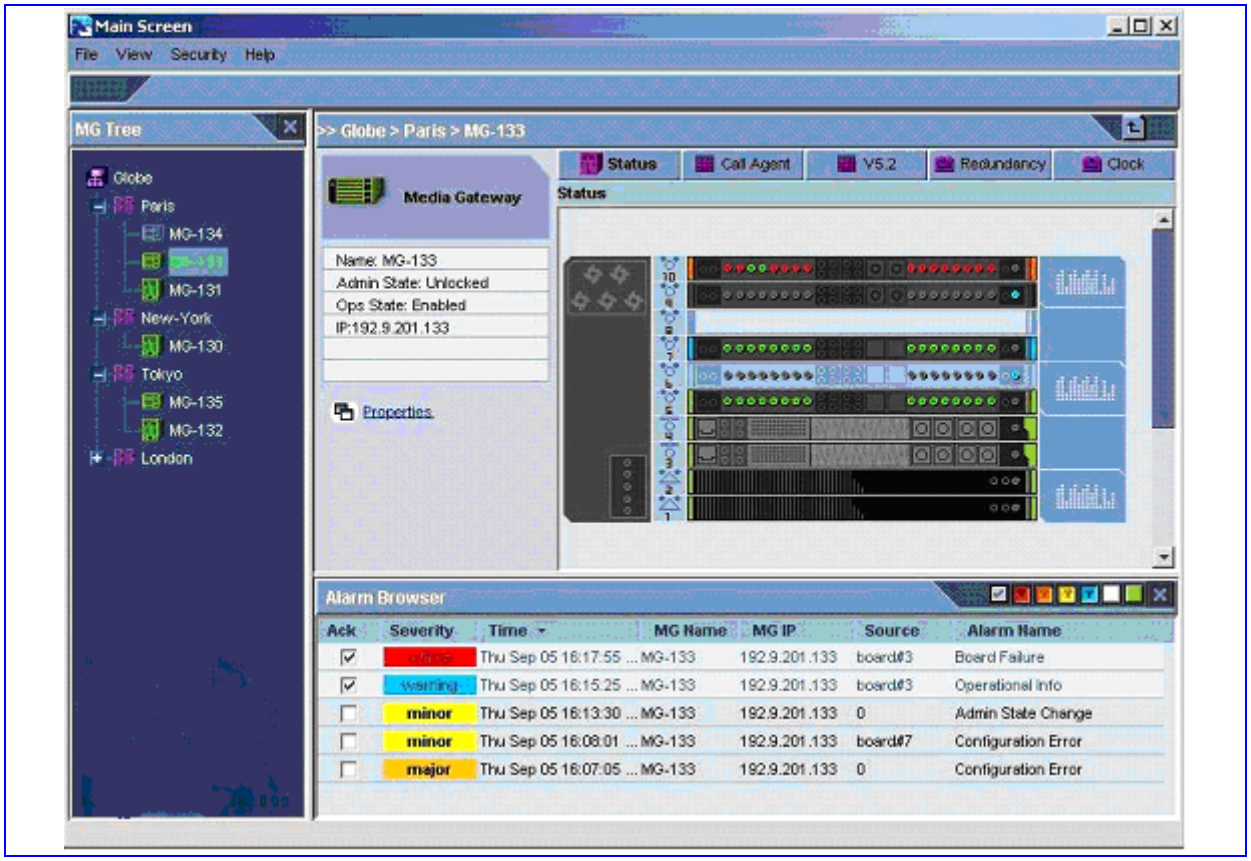
The color of each entity indicates its status. Special color coding indicates various fault states of the entities (Critical, Major, Minor, Warning, OK) as well as High Availability status (which board is active, redundant standby, redundant active).

- One-Click Access to Element Provisioning & Actions

Table 6-3: Board Actions (for Media Gateways version 3.0)

Board Icon	Board Type	Action		Action Availability
	SC Board	Switch Over	When a redundant SC board is present	
	Ethernet Switch Board	Lock	Always	
		Unlock	Always	
	Media Gateway Board	Switch Over	Board is unlocked and active	
		Switch Back	Board is switched-over	
		Lock	Always	Caution: This action resets the board and drops all active calls on it.
		Unlock	Always	
		Remove	Board is Locked	
		Make Board Redundant	Board is Locked	
		Make Board Active	Board is Locked & redundant	
	Empty Board	Add Media Gateway Board		

Figure 6-3: Media Gateway 3500 Status Pane



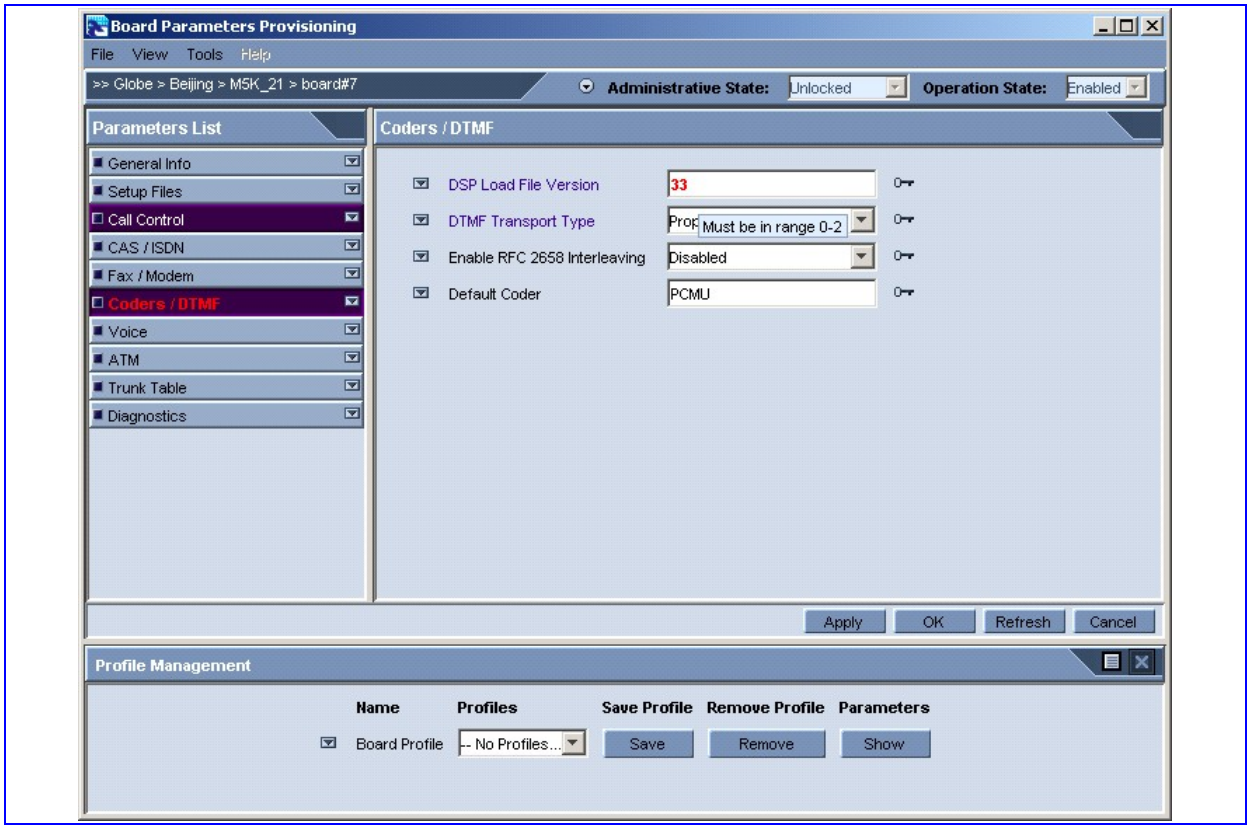
6.6 Performance Monitoring

The EMS offers two view types of Performance Monitoring:

- Real-Time View - used to perform high frequency polling of various system parameters
- Historic View - used to view Historical data of previously created performance Monitoring data collection from data that is stored for up to 30 days

6.7 Media Gateway 3500 Provisioning

Figure 6-4: Media Gateway Parameters Provisioning Screen



6.7.1 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.

The Parameter Provisioning screens are easily and intuitively reached by navigating down the system hierarchy to the entity to be provisioned.

When provisioning, operators always view a location-level indicator (the path of the EMS-managed entity), the Administrative / Operational State (for Media Gateway 3500) and the Reset State (for other gateways) of the entity being provisioned. After provisioning, operators perform the following actions: Unlock (for Media Gateway 3500) and Reset (for other gateways) to enable the Media Gateway to start operating with the new parameter values.

6.7.2 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.

6.7.3 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”.

6.7.4 Configuration Profiles for Quick Provisioning

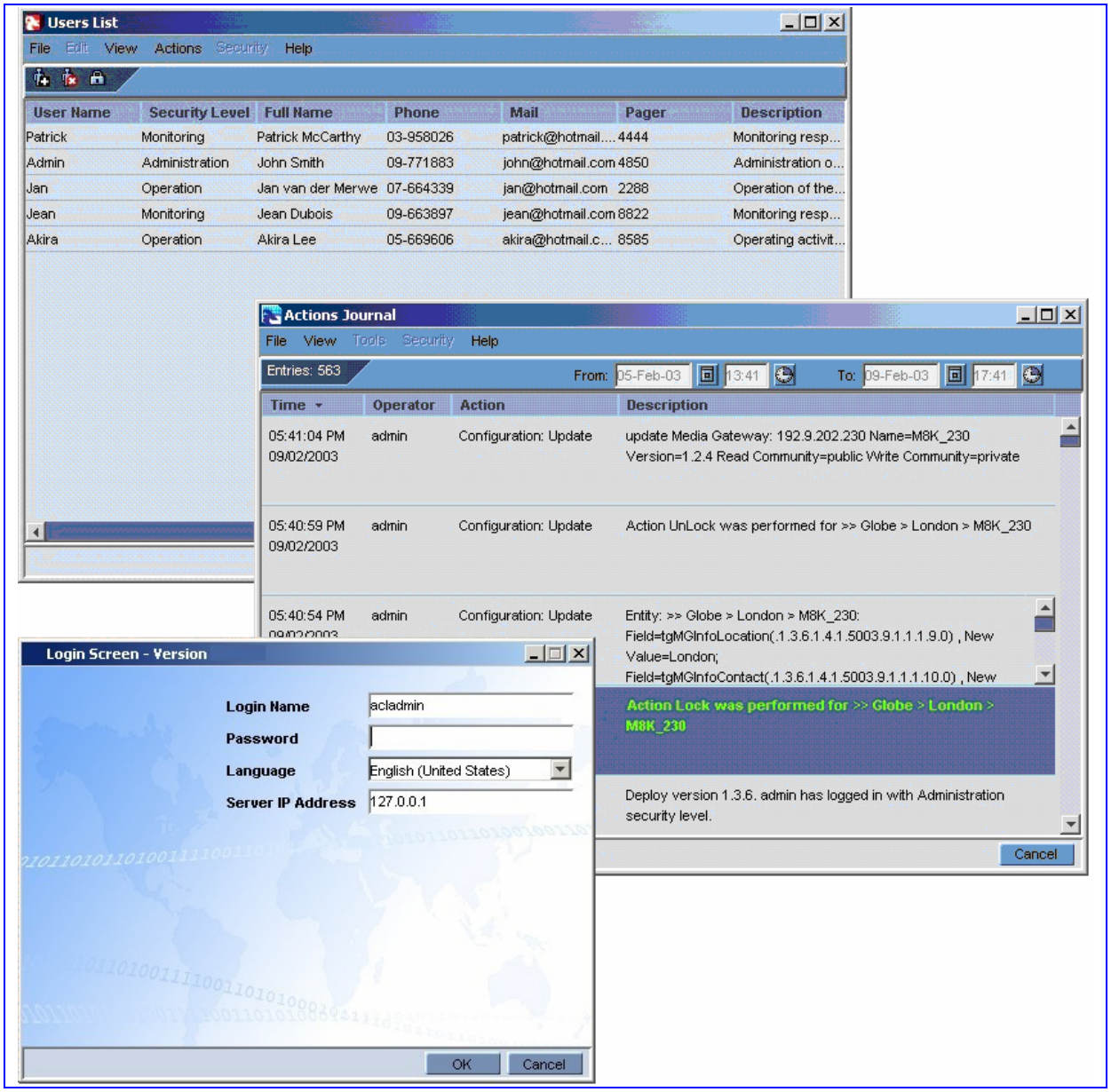
The EMS’s Profile Management enables operators to rapidly provision values to entity parameters by loading a profile. The Profile Manager feature is located in the lowermost pane of the Parameters Provisioning screen.

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.

6.8 Security Management

Security management is carried out in the Users List screen and in the Actions Journal screen, while the Login Screen secures initial access to the EMS.

Figure 6-5: Security Management Screens



6.8.1 EMS Application Security

Initial access to the EMS application is secured via the Login Screen: it includes authentication and authorization with User Name and Password.

6.8.2 User Security Levels

The EMS operators can be allocated one of 3 security levels:

1. Monitoring Level (viewing only)
2. Operation Level (viewing and all system provisioning operations)
3. Administration Level (viewing, all system provisioning operations, and user security management).

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

An operator is assigned administrator security level to exert control over users' access to system resources so that sensitive system information cannot be accessed without appropriate authorization and managed system elements cannot be sabotaged. The Administrator can define new users, change user security level, update user information or remove a user from the Users List.

6.8.3 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.

6.8.4 SNMP Community Strings

Each Media Gateway can have different Read-Write SNMP Community Strings. The Community Strings can be assigned when adding a Media Gateway to the EMS and changed later.

6.8.5 Firewall Support

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.

6.9 Northbound Interface

The EMS now features a CLI (Command Line Interface) and a Java™ API Northbound Interface (for a login command), enabling operators to perform a single log-in process from an NMS client to an EMS client. After the EMS client is installed, operators can access a folder named "Nbif" under the client directory. The folder "Nbif" includes nbif.jar and nbif.html files. The CLI is run from an executable cli.exe file located in the root of the EMS client installation directory.

The following commands are supported:

- nmsLogin - used to open an EMS client focused on a specific (required) Media Gateway
- changeStatusToNodeIP - used to change focus from one Media Gateway to another while a client session is open

Other Northbound Interfaces are provided directly from the Media Gateway using SNMP.

- Faults - SNMP traps can be sent to an NMS, as well as to the EMS simultaneously.
- Configuration - An OSS can modify parameters in the Media Gateway via SNMP. However, it is important to designate which parameters are to be configured via the EMS (handling the bulk of the parameters) and which via the OSS. Having a parameter controlled by more than one management system can be confusing to the user.

7 Media Gateway 3500 Selected Functional Specifications

Table 7-1: Media Gateway 3500 Functional Specifications

Function	Specification
Capacity	
Network Ports/DSP Calls **(independent digital voice, fax or data ports)**	Up to 80 E1/T1 Links; Redundant*, 5+1 Media Gateway Boards configuration, or 96 E1/T1 Links for simplex** 6 Media Gateway Boards configuration *Redundant configuration with protected channels Wireline/Cable: 2,400 simultaneous VoIP voice calls for 5+1 TP-1610 Media Gateway Boards Independent dynamic vocoder, fax or modem selection per channel Capacity is transcoding and voice coder type dependent
Voice Coders	G.711, G.723.1, G.726, G.727, G.728, G.729E, G.729A Independent dynamic vocoder selection per channel
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
Echo Cancellation	G.165 and G.168 2000 compliant
Gain Control	Configurable Input/Output Gain Control: -31 dB to +31 dB in steps of 1 dB
Silence Suppression	G.723.1 Annex A
	G.729 Annex B

Table 7-1: Media Gateway 3500 Functional Specifications

Function	Specification
Voice Activity Detection (VAD), **Comfort Noise Generation (CNG)**	PCM and ADPCM - Per RFC 3389
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
	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	
Local Subnets	Different Local IP Addresses and Subnet masks for Operation Administration & Maintenance (OAM), Control and Media Protocols
Static Routes	Configurable Static Routes tables
DiffServ RFC2474	Configurable, marking capabilities for Network, Premium Control, Premium Media, Gold and Bronze DiffServ classes
Control Protocols	
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
Security	
IPSec (ESP) with IKE pre-shared key	IPSec is supported for the management traffic to EMS/ NMS/ OSS and for control interfaces to MGC (with reduced channel capacity). Encryption algorithms - DES and 3DES Hash types - SHA1 and MD5
Access Control Lists	The control interfaces can be protected by access control lists.
SSH (Secure Shell)	To secure the Telnet and SFTP Server

Table 7-1: Media Gateway 3500 Functional Specifications

Function	Specification
	SSH Protocol Version 2 Supported encryption algorithms: AES-128, BLOWFISH, 3DES Supported authentication algorithms: SHA1, MD5 User/password authentication on each login
SSL (the Secure Socket Layer)	To secure 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,
	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 – only THRH is supported)
PSTN Protocols	MFC/R2 numerous country variants Unique script for each county variant, enabling maximum flexibility of the entire state machine of each CAS protocol Note: Currently supported on Media Gateway blade TP-1610 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 Note: Currently supported on Media Gateway blade TP-1610 only
SIGTRAN	IUA (RFC 3057) over SCTP (RFC 2960)
Maintenance	
Management	Element Management System, SNMP v2 OAM Single point of access via the System Controller; easy management and provisioning with standard SNMP v2 interface
Maintainability	All shelf 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 HW and SW Diagnostic, BIT (Built in Test) fault detection, heart beat, chassis sub-systems monitoring
Physical Interfaces	

Table 7-1: Media Gateway 3500 Functional Specifications

<table>
<tr><th>Function</th><th>Specification</th></tr>
<tr><td>E1/T1 Interfaces</td><td>Two 50-Pin Telco connectors (DDK 57AE-40500-21D) via RTM rear panel I/O module, each handling 8 E1/T1 ports</td></tr>
<tr><td>IP Interfaces</td><td>Up to 3 different IP Uplinks, depending on Ethernet Switch type:
<table><tr><th></th><th>ES/4411</th></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>1 Gigabit optical</td></tr></table>100/1000 Base-TX: RJ-45 Connector Interface (CAT5 Twisted pair)
1 Gigabit optical: Multimode, SC-duplex 1000 Base-SX for the Gigabit Ethernet ports</td></tr>
<tr><td colspan="2">Hardware Specifications</td></tr>
<tr><td>Dimensions
(h x w x d)</td><td>222 x 483 x 311 mm (8.7 in. x 19 in. x 12.3 in.)</td></tr>
<tr><td>Enclosure</td><td>10 -slot 5 U cPCI chassis</td></tr>
<tr><td>Weight</td><td>Approx. 27 lbs. (12.3 kg) unloaded.
Approx. 50 lbs. (22.6 kg), fully loaded</td></tr>
<tr><td>Mounting</td><td>Per EIA Standard RS-310-C in 19-inch rack</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>-48 V DC Dual Feed, with up to 3 DC Power modules OR
100 - 240 V AC with up to 3 AC Power modules</td></tr>
<tr><td>Cooling</td><td>Easily replaceable fan tray& 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
FCC part 15 Class A
CE Mark (EN 55022 Class A, EN 60950, 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>
</table>

Specifications subject to change without notice.

8 Special Information

Notice

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, Nortel cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions.

Date Published: Feb-11-2005

Safety Notices

The protective earth terminal on the back of the MG 3500 must be permanently connected to protective earth.

Industry Canada Notice

This equipment meets the applicable Industry Canada Terminal Equipment technical specifications. This is confirmed by the registration numbers. The abbreviation, IC, before the registration number signifies that registration was performed based on a declaration of conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Caution Laser

The device may contain a Class I Laser/LED emitting device, as defined by 21CFR 1040 and IEC825.

Do NOT stare directly into the beam or fiber optic terminations as this can damage your eyesight.

Digital Device Warnings

This equipment complies with Part 68 of the FCC rules and the requirements adopted by ACTA. On the interface card module of this equipment is a label that contains a product identifier in the format US: AC1ISNANTP1610. If requested this number must be provided to the telephone company.

The Telephone company may make changes in the facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. Should you experience trouble with this telephone equipment, contact: Nortel. **Do not attempt to repair this equipment!**

Facility Interface Code: 04DU9.BN, 04DU9.DN, 04DU9.1KN, 4DU9.ISN

Service Order Code: 6.0N

USOC Jack Type: RJ21X or RJ48C

It this gateway causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also you will be advised of your right to file complaint with the FCC if you believe it is necessary.

Network Information and Intent of Use

The products are for access to ISDN at 2048 kb/s and for access to G.703 Leased lines at 2048 kb/s.

Network Compatibility

The products support the Telecom networks in EU that comply with TBR4 and TBR13.

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
E1 or T1	TNV-1
Ethernet (100 Base-T)	SELV
DC Input Power Port	SELV

TNV-1: Telecommunication network voltage circuits whose normal operating voltages do not exceed the limits for SELV under normal operating conditions and on which over voltages from telecommunication networks are possible.

SELV: Safety extra low voltage circuit.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Reader’s Notes

Index

Product Description