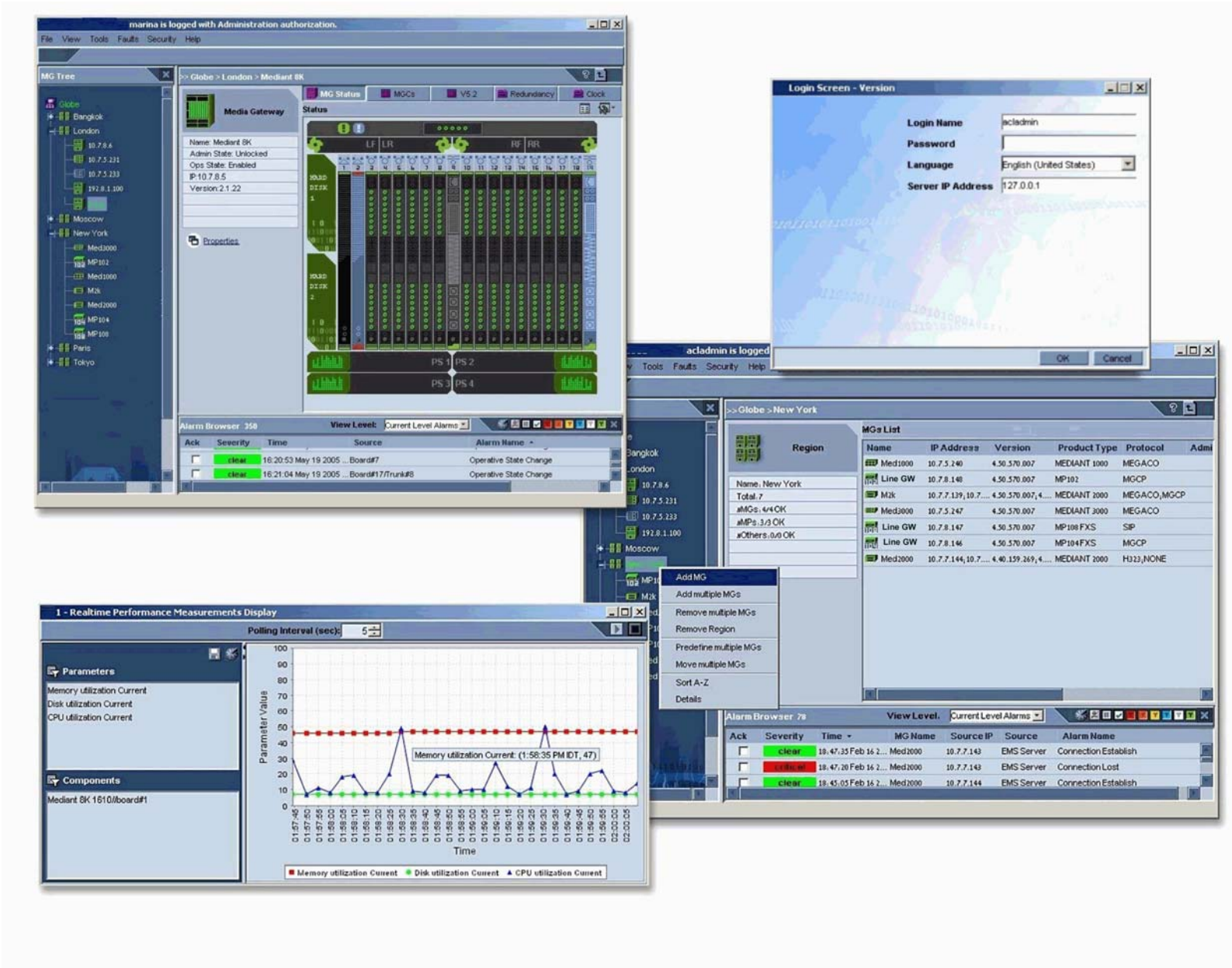
Element Management System (EMS)
Product Description

Version 3.0

Document #: LTRT-94005 Rev 002



Notice

This Product Description describes and illustrates the Element Management System (EMS), available from Nortel. 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 and downloaded by registered Technical Support customers at www.nortel.com.

© 2005 Nortel Ltd. All rights reserved
This document is subject to change without notice.
Refer to the current release notes that may be included with your documentation or hardware delivery.

Date Published: Jun-22-2005 Date Printed: Jun-23-2005

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 Alt + ← .

Note: The Element Management System supports the following products:

1. Media Gateway 3500

Trademarks

All products or trademarks are property of their respective owners.

Customer Support

Customer technical support and service are provided by Nortel. 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. The $ symbol indicates hexadecimal notation.

Related Documentation

Manual Name
Media Gateway 3500 Installation, Operation & Maintenance Manual
Media Gateway 3500 Product Description
Element Management System (EMS) User's Manual
Element Management System (EMS) Server Installation & Maintenance Manual
Element Management System (EMS) Product Description
Element Management System (EMS) Online Help
EMS Parameter Guide for the Media Gateway 3500

Table of Contents

1 Introducing the Nortel Element Management System (EMS) 7
1.1 Characteristics 7
1.2 Architecture Overview 9
1.3 Specifications 9
1.4 Supported VoIP Equipment 11
1.5 EMS System Requirements 12
2 Fault Management 13
3 Configuration Management 17
3.1 Monitoring Media Gateway Status 17
3.2 Media Gateway Provisioning 19
3.3 Media Gateways Maintenance Actions 22
3.3.1 Media Gateway 3500 Maintenance Actions 22
4 Performance Management 24
5 Security Management 26
5.1 Network Communication Security 27
5.2 EMS Application Security 29
6 Northbound Interface 31

List of Figures

Figure 2-1: Alarm Browser in EMS Main Screen 13
Figure 2-2: Alarms History....16
Figure 3-1: Media Gateway 3500 Status Pane 18
Figure 3-2: Media Gateway Parameters Provisioning Screen 19
Figure 3-3: Maintenance Actions (MG 3500) 22
Figure 5-1: Firewall Configuration 27

List of Tables

Table 1-1: Element Management System (EMS) Specifications 9
Table 1-2: Supported VoIP Equipment....11
Table 1-3: User Interface and External Interfaces Specifications 11
Table 1-4: Minimal Platform Requirements....12
Table 1-5: Software Requirements....12
Table 1-6: OS Patches Required for EMS Server....12
Table 3-1: Board Actions (for Media Gateways version 3.0) 17

1 Introducing the Nortel Element Management System (EMS)

The Nortel 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 the Nortel Media Gateway 3500.
The Nortel EMS enables Service Providers the capability of 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 multiple Media Gateway 3500 systems and their modules.

1.1 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 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 and hierarchical organization and Microsoft™ Explorer™ paradigm increase productivity and minimize the learning curve.

- **Versatile System**

  The EMS can simultaneously manage up to 100 Nortel Media Gateway 3500 systems even while having different software versions running on them.

- **FCAPS**

  The EMS supports **FCAPS** functionality:

  Fault management - refer to Section 1 on page 7

  Configuration management - refer to Section 3 on page 17

  Accounting (managed by a higher-level management system such as an NMS)

  Performance management (Planned for future version)

  Security management - refer to Section 5 on page 26

- **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). The EMS is ready to include files to support left-to-right languages.

- **Customizable Features**

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

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

1.2 Architecture Overview

The EMS is an open, standard-based, scalable management tool. Typically, the EMS manages the functions and capabilities within each gateway but doesn't manage the connectivity between different gateways within the network. To support management of the connectivity between itself and other network elements, the EMS communicates upward to higher-level Network Management Systems (NMSs), according to ITU.T (International Telecommunication Union -Telecommunication Standardization Sector) M3.100 standards on the Telecommunications Management Network (TMN) layered model. This TMN-defined architecture for a layered Operations Support System (OSS) enables Service Providers to meet customer needs for rapid deployment of new services, as well as to meet stringent quality of service (QoS) requirements.

1.3 Specifications

- Software Version Number: 3.0
- Release Date: Q3 2005
- Package and Upgrade Distribution: CD-ROM

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

Subject	Description
TMN Standards	ITU-T Recommendation M.3010 series FCAPS functionality support
Fault Management	▪ Alarm fields and actions, according to ITU-T Recommendation X.733, 3GPP Recommendation 3G TS 32.111-1. ▪ Alarm processing: 30 traps per second, continuously ▪ Alarm archiving: at least a one-month history for up to 1100 media gateways (depending on disk size available). ▪ Graphical, context-sensitive Alarm History with filtering options. ▪ Application includes context-sensitive Alarm Browser with various filtering and search options, detailed alarm description, Acknowledge and Delete actions processing, audio indication on receipt of alarms. ▪ Automatic Alarm Clearing ▪ Traps Forwarding to Northbound Interface ▪ Save alarms in a *csv* file
Media Gateways Monitoring	Summary of all managed gateways' statuses in one screen with 'drill down' hierarchy. Color scheme shows element severity, redundant and switchover states.

Subject	Description
Media Gateways Provisioning	▪ Adapts rapidly to changes in new media gateway software releases ▪ Based on hierarchy of managed objects concepts ▪ Online parameter provisioning support, with icons indicating provisioning type ▪ Profile-based provisioning, including Master Profile for all VoIP gateways as well as for the TP-1610 boards. ▪ Search provisioning parameter ▪ Configuration database of MG 3500 gateways is kept inside the media gateways
Security Management	Complies with T1M1.5/2003-007R4 and covers two aspects: Network communication security and EMS application security. **Network Communications Security** ▪ EMS server's network is configured and its ports opened during installation. ▪ EMS client-server communication is secured using RMI (Remote Method Invocation) protocol over SSL (Secure Sockets Layer). ▪ Media Gateway 3500: SNMPv2c, Telnet and FTP over IPSec. **Application Security** ▪ User Management: Using an LDAP server for centralized user authentication, or in the EMS application. ▪ EMS application: Users List. Authentication-based operator access according to user name, password, security level, login machine IP. Modification of user details and access rights, user removal, forced logout, user suspension, releasing users from suspension, user password change, ▪ EMS application: Actions Journal of operators' activities, various filtering and search options.
Performance Management	▪ Real-Time Graphics ▪ Historical Data Collection and Analysis
Media Gateways Maintenance Actions	Media Gateway 3500 ▪ Online software upgrade via a Wizard ▪ Gateway installation, startup and shutdown ▪ All maintenance actions (lock, unlock, add / remove board, etc.) for each media gateway entity, via a convenient Graphical User Interface.

1.4 Supported VoIP Equipment

Table 1-2: Supported VoIP Equipment

Supported VoIP Equipment	Description
 Media Gateway 3500	The Media Gateway 3500 is the medium-sized member of the family of market-ready, standards-compliant, media gateway systems. Main features: Redundant common equipment (Power, Controller, Ethernet Switch) ; N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SIGTRAN Interworking (PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant Applications: VoP Trunking Gateways, IP-Centrex Gateways, VoP Access Gateways Selected specifications: Up to 2,400 independent VoIP to PSTN voice calls; VoiceCoders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fall-back to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP (Refer to the product documentation for detailed information).

Table 1-3: 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

1.5 EMS System Requirements

This section lists the platform and software required to run the EMS application.

Table 1-4: Minimal Platform Requirements

Resource	EMS Server	EMS Client
Operating System	Solaris™ 64-bit, version 5.9	Windows™ 2000 / XP
Memory	1 GB RAM	512 MB RAM
Disk space	40 GB	300 MB
Processor	1 GHz UltraSPARC IIIi	600 MHz Pentium III
Swap space	2 GB	1 GB

Table 1-5: Software Requirements

#	EMS Server	EMS Client
1	JDK 1.4.2 for Solaris™	JDK 1.4.2 for Windows™
2	X Server and Window Manager	
3	Executable tcsh	

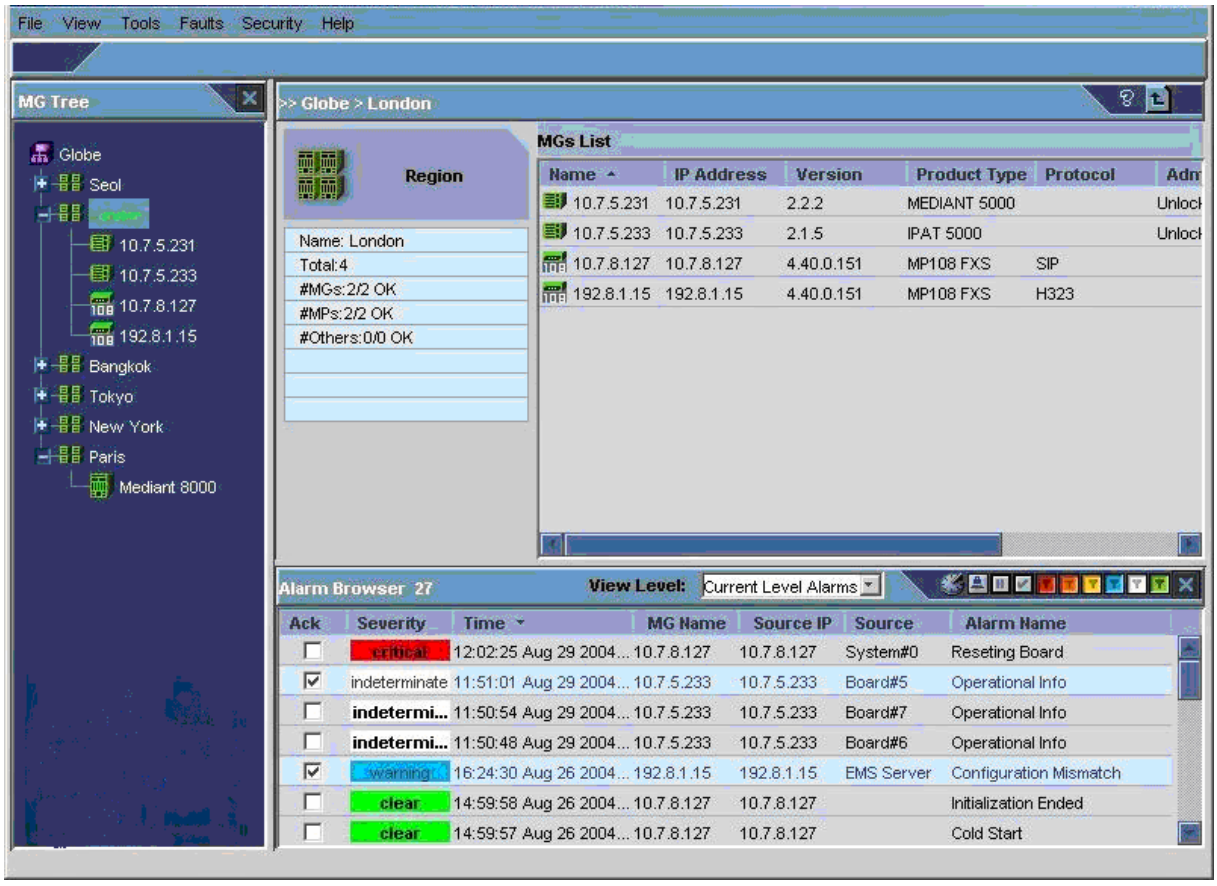
Table 1-6: OS Patches Required for EMS Server

#	Patch Name	Required by Application
1	SUNWarc	Oracle 9i DB
2	SUNWbtool	Oracle 9i DB
3	SUNWhea	Oracle 9i DB
4	SUNWlibm	Oracle 9i DB
5	SUNWlibms	Oracle 9i DB
6	SUNWsprot	Oracle 9i DB
7	SUNWtoo	Oracle 9i DB
8	SUNWi1of	Oracle 9i DB
9	SUNWxwfnt	Oracle 9i DB
10	SUNWxwkey	Oracle 9i DB
11	UPDATE5	Oracle 9i DB (recommended)

2 Fault Management

The EMS's high-level 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 Alarms History.

Figure 2-1: Alarm Browser in EMS Main Screen



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.

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.

Alarm Priorities

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

Automatic Alarms Clearing

Critical, Major, Minor, Warning or Info alarms are automatically cleared from the Alarms Browser (and transferred to Alarms History) by *the same entity (source) and same Media Gateway* that originally generated the Critical, Major, Minor, Warning or Info alarms. This feature is available for system debug purposes. Operators view the list of *only the currently active alarms*.

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.

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.

Alarm Types

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

1. *Communications Alarm*: an alarm of this type is principally associated with the procedures and/or processes required to convey information from one point to another.

2. *QoS alarm*: alarms notifying operators of Quality of Service degradation

3. *Processing Error Alarm*: software or processing fault

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

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

Alarms Actions

Operators can perform the following actions regarding the displayed alarms:

- Acknowledge: informs the other 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.

Detailed Information

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

Searching and 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).

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

Change Alarm Browser View and Level

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). Each user can select the alarms filtering level s/he wishes to apply in his/her Alarm Browser.

The following options are supported: Current Level Alarms (default), Node Level Alarms, Region Level Alarms, All Alarms - globe level.

Audio Indication on Receipt of Alarms

Users can choose whether to enable/disable an audio indication (a bell) when new alarms arrive.

Security

The actions that an operator is authorized to perform on alarms depends on the operator's security level, previously allocated to them by the administrator. Permission *to view* alarms is separate from permission *to respond* to alarms. All operator actions, such as alarm acknowledgement and clearing, are logged in the EMS's Actions Journal (refer to Section 5 on page 26).

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 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, of 1000 alarms per day for up to 100 digital 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 2-2: Alarms History

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

3 Configuration Management

3.1 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 is represented by an icon. Each icon is color-coded to enable operators to quickly determine their status, and sized/shaped to enable operators to immediately identify Media Gateway type. One glance at the EMS Status pane provides operators with the specified Media Gateway's status as well as with the overall network status for all 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, ES, TP/SB, Alarm Card) and trunk status for TP/SB boards. All hardware entities' alarm statuses are graphically represented: power suppliers, fans, and hard disks.

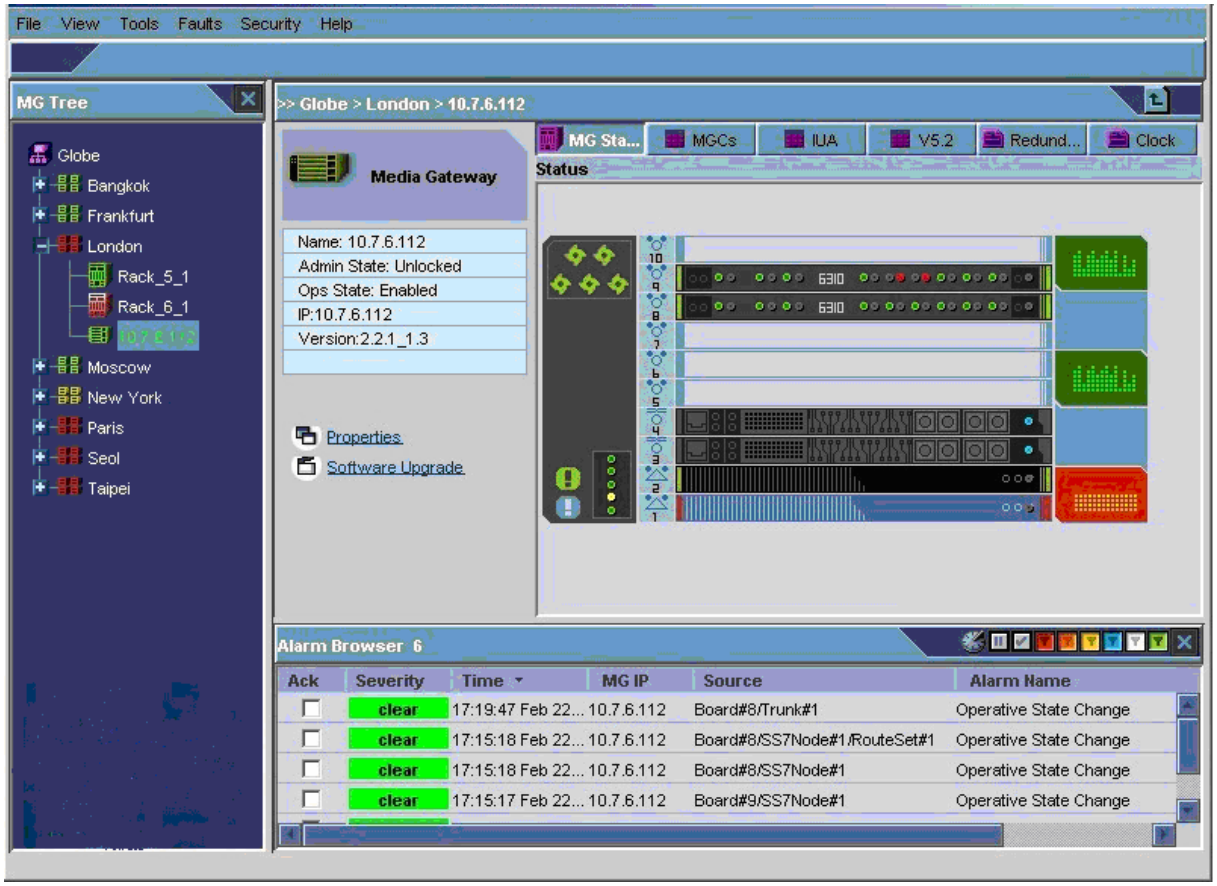
  The color of each entity indicates its status. Special color-coding indicates various fault states of the entities (Critical, Major, Minor, Warning, OK) as well as High Availability status (which board is active, redundant standby, redundant active).

- **One-Click Access to Element Provisioning & Actions**

Table 3-1: Board Actions (for Media Gateways version 3.0)

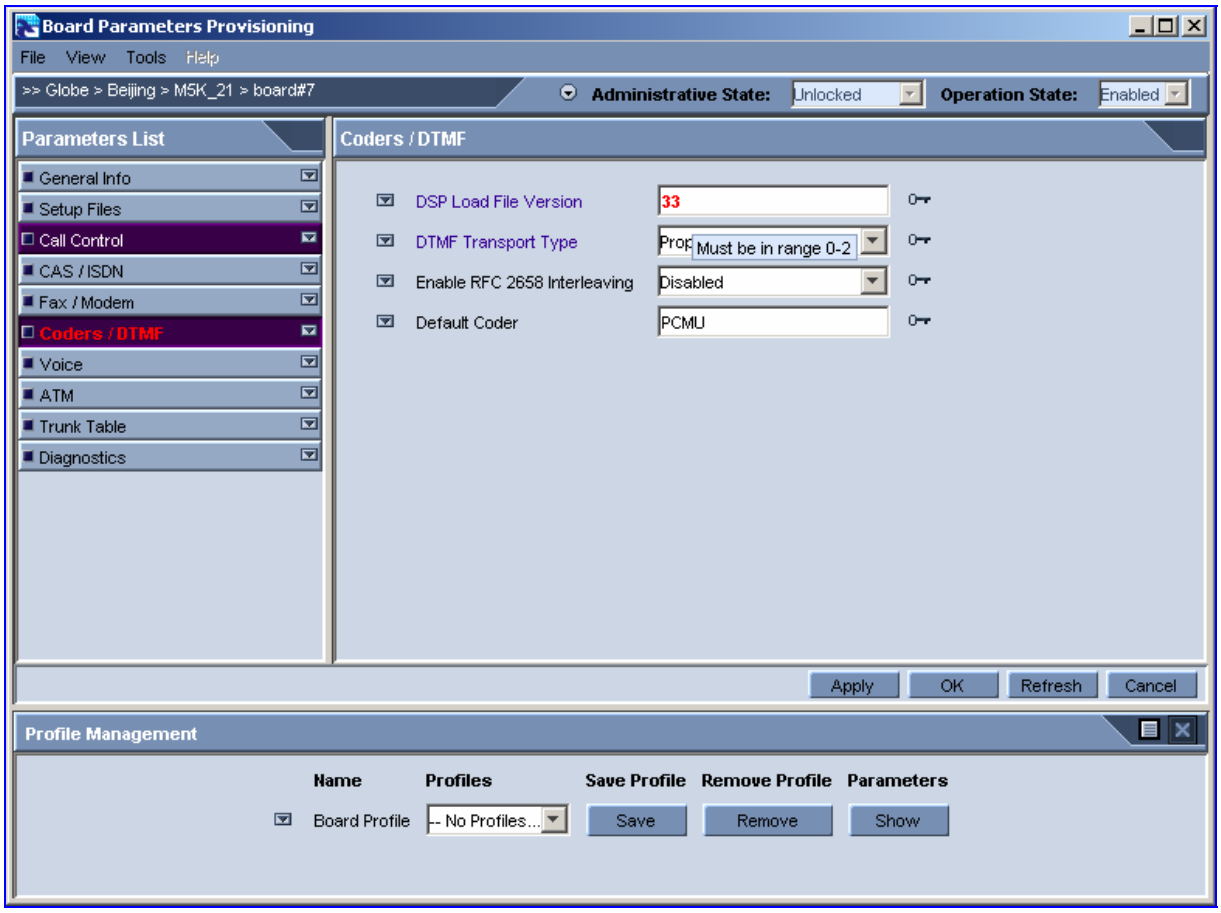
Board Icon	Board Type	Action	Supported Maintenance Actions	Action Description
	SC Board	Switch Over	When a redundant SC board is present	
	TP-1610 Board	Switch Over	Board is **unlocked** and **active**	
		Switch Back	**Board is switched-over**	
		Lock	Always	Caution: This action resets the board and 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 TP-1610 Board		

Figure 3-1: Media Gateway 3500 Status Pane



3.2 Media Gateway Provisioning

Figure 3-2: Media Gateway Parameters Provisioning Screen



Provisioning

Provisioning gateway entities is straightforward and operator-friendly via the EMS. Gateway entities such as boards, trunks, call control protocols, etc., are provisioned using the EMS's Parameters Provisioning screens. Parameter values are loaded to the 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) and the Administrative / Operational State of the Media Gateway 3500. After provisioning, operators perform an Unlock to enable the gateway to start operating with the new parameter values.

Regional files are loaded in the Software Manager (refer to Section 3.3 on page 22).

Provisioning Types

Three provisioning parameter types are supported in provisioning screens, adjacent to modifiable parameters: Instant (changes are applied to the 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.

Color-Coding

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 combos 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”.

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.

Master Profile

- TP-1610 Master Profile for MG 3500 gateways

After finishing configuring the profiles parameters of a TP-1610 board, operators can save the configuration as a master profile. The master profile comprises following *entity* profiles:

- Board Provisioning Frame
- Trunks Provisioning Frame (for all trunks)

After saving the configuration as a master profile, operators can attach it to the TP-1610 board or to multiple TP-1610 boards.

Configuration Verification, Upload and Download

Configuration Verification is a process of verifying that the configuration saved in the EMS database tallies with the actual gateway configuration. In the event of inconsistencies, operators are notified of the mismatch, which they can then correct by working with the EMS's parameter provisioning screens. To perform an overall parameters sync, you can choose to perform Configuration Upload (when all the gateway parameters values are saved in the EMS database), or Configuration Download (when all parameter values, previously saved in EMS, are downloaded to the gateway)

These actions can be performed for a set of gateways.

Capability to Save and Restore Gateway Configuration

The configurations of the small gateways are saved in the EMS database. If a gateway is replaced, this capability enables customers to quickly restore the original gateway's configuration.

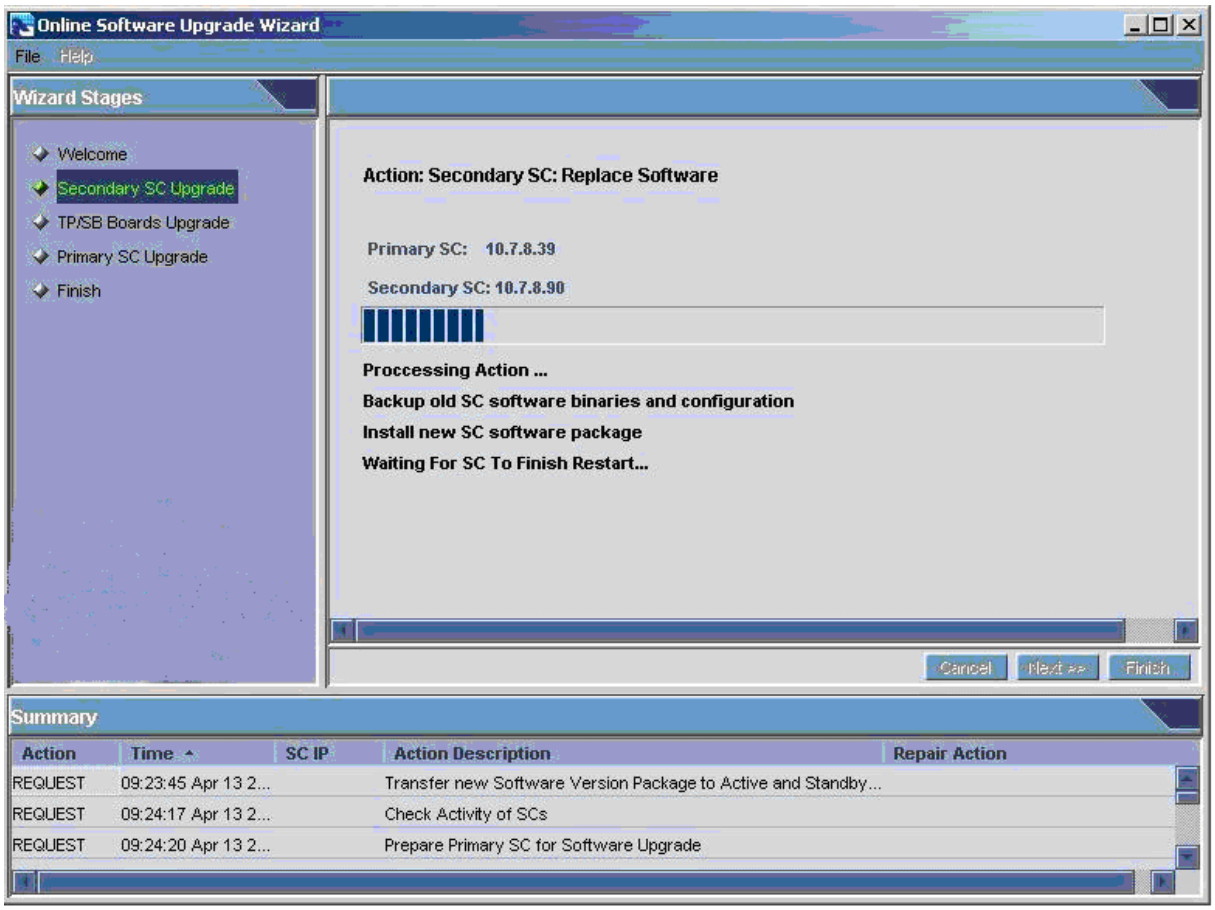
Security

The EMS's security management feature enables the operator who holds the Administrator security level to exert control over other operators' access to system resources. Thus, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexpert operators. Security management is carried out in the Users List screen and in the Actions Journal screen. 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. Refer to Section 5, Security Management, on page 26.

3.3 Media Gateways Maintenance Actions

3.3.1 Media Gateway 3500 Maintenance Actions

Figure 3-3: Maintenance Actions (MG 3500)



- One Click to Element Provisioning and Actions (Boards, Trunks, etc.)
  - Refer to Table 3-1, Board Actions (for Media Gateways version 3.0) on page 17.
- Online Software Upgrade Wizard

  An online software upgrade is performed when both System Controllers are up and running. The software upgrade process upgrades both Self Controller and TP boards' software. An upgrade is best performed at night when traffic volume is low. If an upgrade process fails, users can perform a rollback to previous software and the previous configuration.

  The Online Software Upgrade Wizard GUI includes a 'Wizard Stages' screen section and a 'Summary Table' screen section.

  An offline software upgrade is performed when one System Controller is up and running. The main difference between an offline software upgrade and reinstallation is that during the offline software upgrade process, the media gateway configuration is saved.

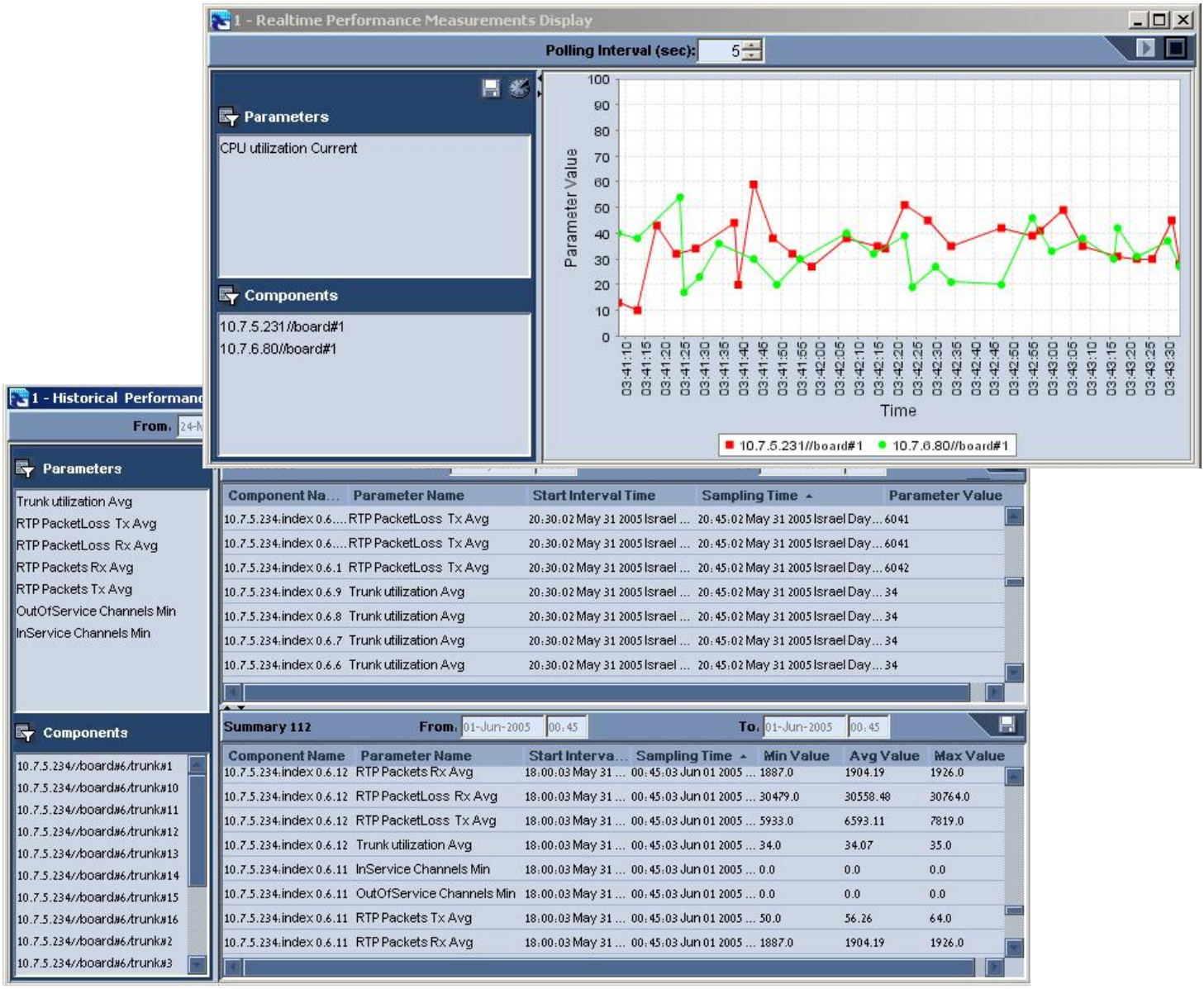
Note that the software upgrade process can be performed starting with version 2.1 of the media gateway and only to a higher version. Any other software version changes should be performed via a reinstallation process.

- Gateway Start Up, Shut Down is possible from the Maintenance Toolbar.

4 Performance Management

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

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



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

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

to another.

- Performance Monitoring actions on multiple gateways. Users can attach a master profile and start / stop background monitoring a single command for the entire set of gateways.

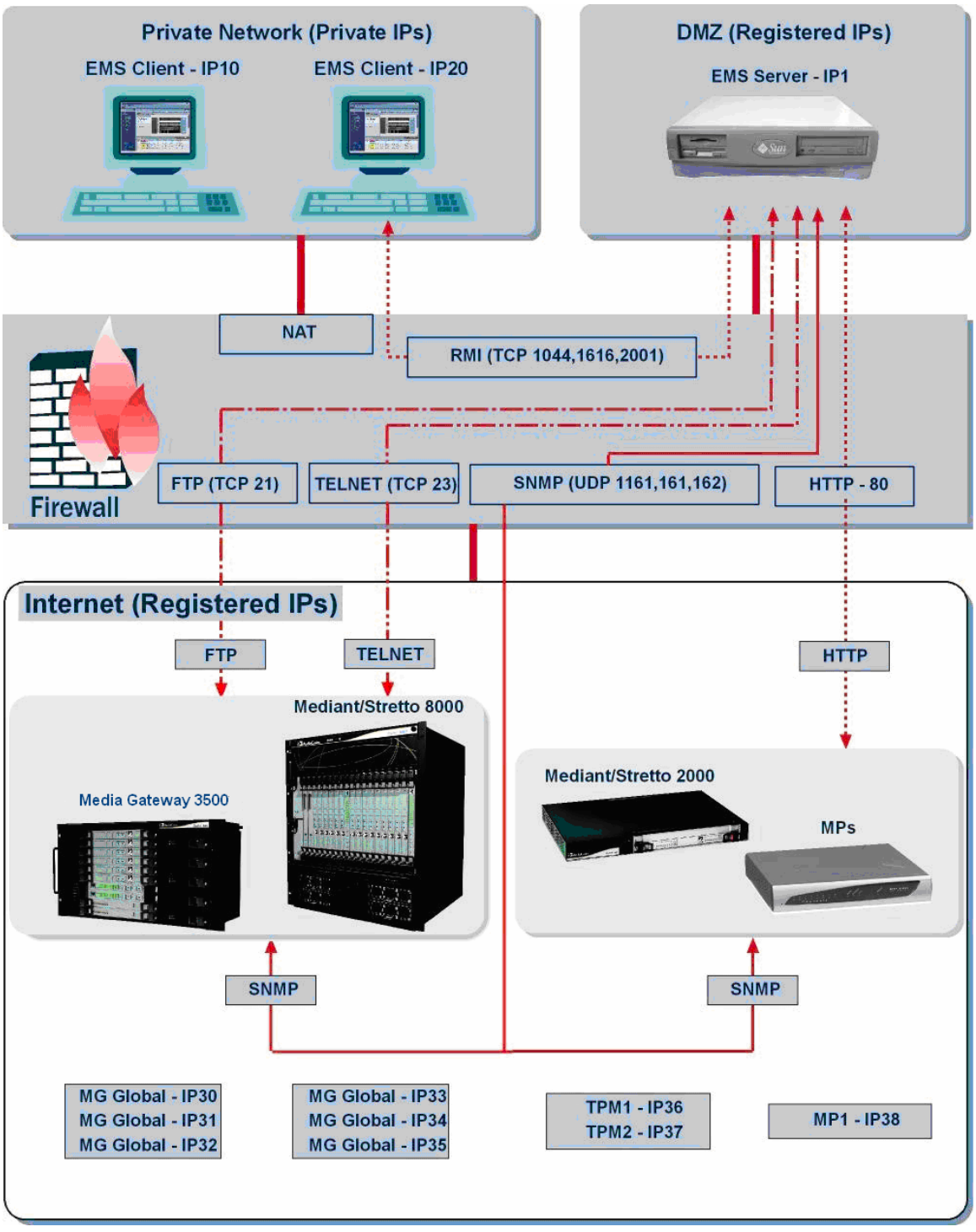
5 Security Management

EMS Security Management features two aspects:

- Network Communication Security
- EMS Application Security.

5.1 Network Communication Security

Figure 5-1: Firewall Configuration



The EMS interoperates with firewalls, protecting against unauthorized access by crackers and hackers, thereby securing regular communications. Define rules in your firewall to enable communications between EMS client, server and managed media gateways (refer to the figure below).

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

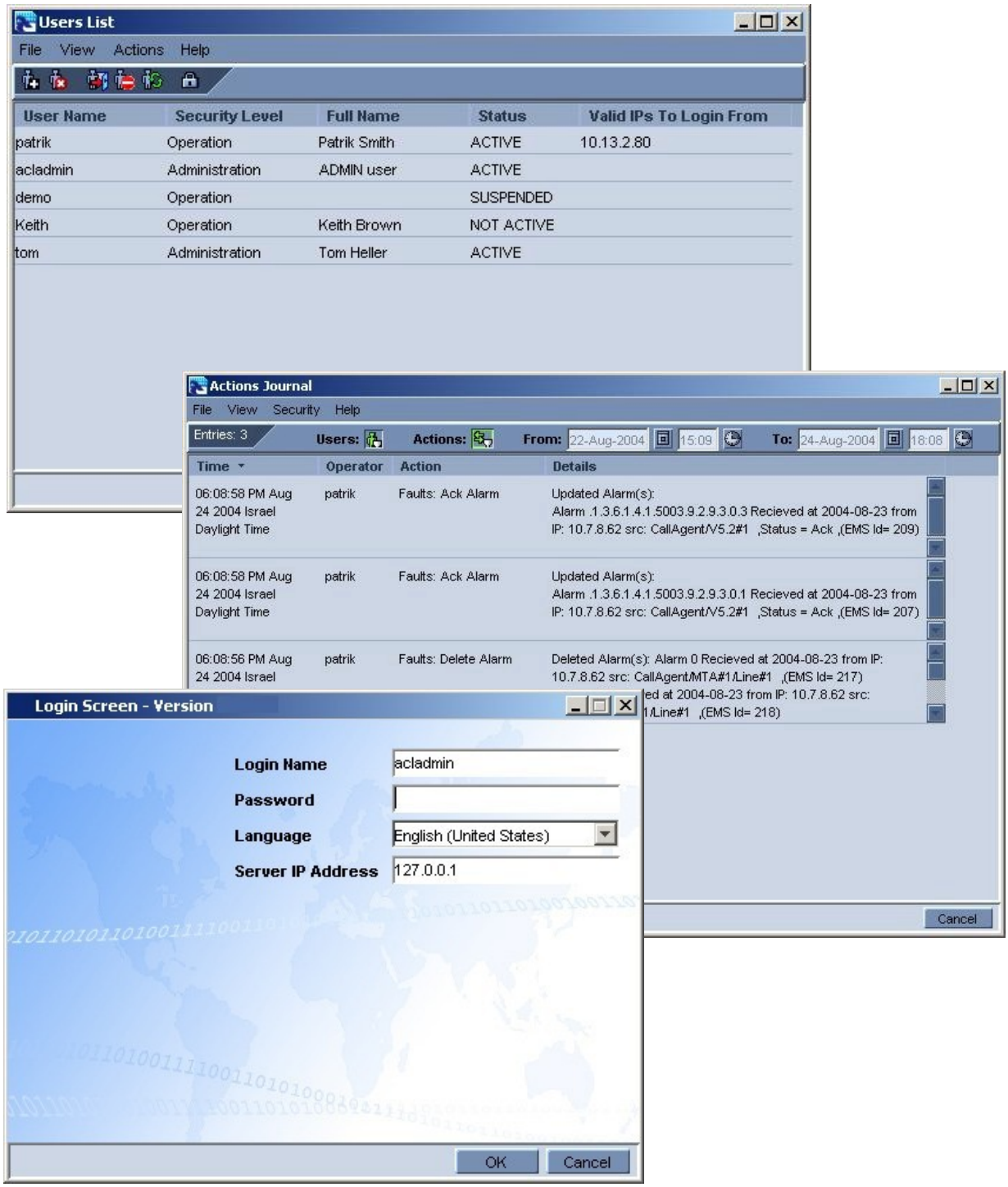
EMS server communications with gateways is performed over the following protocols:

- SNMPv2c for provisioning, maintenance actions and fault management. SNMPv2c security is achieved by running SNMP communication over IPSec protocol.
- Telnet and FTP for installation and upgrading software. Telnet and FTP communications are secured by running them over IPSec protocol.

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

5.2 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.



Users Management in the EMS Application

Management of users can be performed using one of two applications:

1. Centralized LDAP server
2. EMS application

User Security Levels

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.

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/modify user details, remove a user from the Users List, perform the forced logout of an active user and/or suspend a user (as well as release an operator from suspension). The status of each user can be viewed in the Users List screen: ACTIVE, NOT ACTIVE, SUSPENDED or AUTOMATICALLY SUSPENDED.

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. The Actions Journal supports the following filters facilitating easy access to required information: User's Filter, Action Type Filter and the Date and Time Filter.

Changing User Passwords

Operators must change password once at the end of every predefined period of time (by default, every 90 days). Operators are not allowed to reuse their five previously used passwords. The password must include between 8-15 characters. The password must answer at least 3 out of 4 requirements: It must be combined of small and capital letters, digits and signs. The password must not be a repetition of the User Name.

6 Northbound Interface

The EMS features a Command Line Interface (CLI) 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 the 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

Reader's Notes