Reference Guide

AudioCodes Media Gateways and Session Border Controllers

Simple Network Management Protocol (SNMP)

Version 6.6

audiocodes

Table of Contents

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, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: February-11-2020

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Manual Name
MP-11x & MP-124 SIP User's Manual
Mediant 600 & Mediant 1000 SIP User's Manual
Mediant 500 MSBR User’s Manual
Mediant 800 MSBR User’s Manual
Mediant 800 Gateway & E-SBC User’s Manual
Mediant 850 MSBR User’s Manual

Manual Name
Mediant 1000B MSBR User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
MSBR Series CLI Reference Guide for Data Functionality
MSBR Series CLI Reference Guide for System & VoIP Functionality
Mediant 2000 SIP User's Manual
Mediant 3000 SIP User's Manual
Mediant 4000 E-SBC User's Manual
Mediant Software E-SBC User's Manual

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document provides you with supplementary information on AudioCodes SIP-based, Voice-over-IP (VoIP) devices. This information is complementary to the information provided by the device's *User's Manual* and includes.

Note: The SNMP MIB manual is supplied in the Software Release Package delivered with your product.

Note: Using AudioCodes' Element Management System (EMS) or One Voice Operations Center (OVOC) is recommended for customers with large deployments (for example, multiple devices in globally distributed enterprise offices) that need to be managed by central personnel. The EMS/OVOC is not included in the device's supplied package. Contact AudioCodes for detailed information on AudioCodes' EMS/OVOC solution for large VoIP deployments.

1.1 Product Naming Convention

Throughout this manual, unless otherwise specified, the following terms are used to refer to the different AudioCodes products to indicate applicability:

Table 1-1: Product Naming Convention

Term	Product
Device	All products
MediaPack Series	▪ MP-112 ▪ MP-114 ▪ MP-118 ▪ MP-124
MSBR Series	▪ Mediant 500 MSBR ▪ Mediant 800 MSBR ▪ Mediant 850 MSBR ▪ Mediant 1000B MSBR
Analog Series	Analog interfaces (FXS and FXO): ▪ MediaPack ▪ Mediant 600 ▪ MSBR Series ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000 ▪ Mediant 1000B Gateway & E-SBC

Term	Product
Digital PSTN Series	Digital PSTN interfaces: ▪ Mediant 600 ▪ MSBR Series ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000 ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2000 ▪ Mediant 3000
E-SBC Series	SBC application support: ▪ MSBR Series ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 ▪ Mediant 4000

2 SNMP Overview

Simple Network Management Protocol (SNMP) is a standards-based network control protocol for managing elements in a network. The SNMP Manager (usually implemented by a network Management System (NMS) or an Element Management System (EMS) connects to an SNMP Agent (embedded on a remote Network Element (NE)) to perform network element Operation, Administration, Maintenance, and Provisioning (OAMP).

Both the SNMP Manager and the NE refer to the same database to retrieve information or configure parameters. This database is referred to as the Management Information Base (MIB), and is a set of statistical and control values. Apart from the standard MIBs documented in IETF RFCs, SNMP additionally enables the use of proprietary MIBs, containing non-standard information set (specific functionality provided by the Network Element).

Directives, issued by the SNMP Manager to an SNMP Agent, consist of the identifiers of SNMP variables (referred to as MIB object identifiers or MIB variables) along with instructions to either get the value for that identifier, or set the identifier to a new value (configuration). The SNMP Agent can also send unsolicited events towards the EMS, called SNMP traps.

The definitions of MIB variables supported by a particular agent are incorporated in descriptor files, written in Abstract Syntax Notation (ASN.1) format, made available to EMS client programs so that they can become aware of MIB variables and their usage.

The device contains an embedded SNMP Agent supporting both general network MIBs (such as the IP MIB), VoP-specific MIBs (such as RTP) and proprietary MIBs (acGateway, acAlarm, acMedia, acControl, and acAnalog MIBs) enabling a deeper probe into the interworking of the device. All supported MIB files are supplied to customers as part of the release.

2.1 SNMP Standards and Objects

This section discusses the SNMP standards and SNMP objects.

2.1.1 SNMP Message Standard

Four types of SNMP messages are defined:

- **Get:** A request that returns the value of a named object.
- **Get-Next:** A request that returns the next name (and value) of the "next" object supported by a network device given a valid SNMP name.
- **Set:** A request that sets a named object to a specific value.
- **Trap:** A message generated asynchronously by network devices. It notifies the network manager of a problem apart from the polling of the device.

Each of these message types fulfills a particular requirement of network managers:

- **Get Request:** Specific values can be fetched via the "get" request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device.
- **Get Next Request:** Enables the SNMP standard network managers to "walk" through all SNMP values of a device (via the "get-next" request) to determine all names and values that a device supports.

- **Get-Bulk:** Extends the functionality of GETNEXT by allowing multiple values to be returned for selected items in the request.
- This is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a "get-next", and repeating this operation.
- **Set Request:** The SNMP standard provides a action method for a device (via the "set" request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. This provides a way of configuring and controlling network devices via SNMP.
- **Trap Message:** The SNMP standard furnishes a mechanism for a device to "reach out" to a network manager on their own (via the “trap" message) to notify or alert the manager of a problem with the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

The above message types are all encoded into messages referred to as "Protocol Data Units" (PDUs) that are interchanged between SNMP devices.

2.1.2 SNMP MIB Objects

The SNMP MIB is arranged in a tree-structure, similar to a disk directory structure of files. The top level SNMP branch begins with the ISO "internet" directory, which contains four main branches:

- **"mgmt" SNMP branch:** Contains the standard SNMP objects usually supported (at least in part) by all network devices.
- **“private" SNMP branch:** Contains those "extended" SNMP objects defined by network equipment vendors.
- **"experimental" and "directory" SNMP branches:** Also defined within the "internet" root directory, are usually devoid of any meaningful data or objects.

The "tree" structure described above is an integral part of the SNMP standard, though the most pertinent parts of the tree are the "leaf" objects of the tree that provide actual management data regarding the device. Generally, SNMP leaf objects can be partitioned into two similar but slightly different types that reflect the organization of the tree structure:

- **Discrete MIB Objects:** Contain one precise piece of management data. These objects are often distinguished from "Table" items (below) by adding a “.0" (dot-zero) extension to their names. The operator must merely know the name of the object and no other information.
- **Table MIB Objects:** Contain multiple pieces of management data. These objects are distinguished from "Discrete" items (above) by requiring a "." (dot) extension to their names that uniquely distinguishes the particular value being referenced. The "." (dot) extension is the "instance" number of an SNMP object. For "Discrete" objects, this instance number is zero. For "Table" objects, this instance number is the index into the SNMP table. SNMP tables are special types of SNMP objects, which allow parallel arrays of information to be supported. Tables are distinguished from scalar objects, such that tables can grow without bounds. For example, SNMP defines the "ifDescr" object (as a standard SNMP object) that indicates the text description of each interface supported by a particular device. Since network devices can be configured with more than one interface, this object can only be represented as an array.

By convention, SNMP objects are always grouped in an "Entry" directory, within an object with a "Table" suffix. (The "ifDescr" object described above resides in the "ifEntry" directory contained in the "ifTable" directory).

2.1.3 SNMP Extensibility Feature

One of the principal components of an SNMP manager is a MIB Compiler, which allows new MIB objects to be added to the management system. When a MIB is compiled into an SNMP manager, the manager is made "aware" of new objects that are supported by agents on the network. The concept is similar to adding a new schema to a database.

Typically, when a MIB is compiled into the system, the manager creates new folders or directories that correspond to the objects. These folders or directories can typically be viewed with a "MIB Browser", which is a traditional SNMP management tool incorporated into virtually all network management systems.

The act of compiling the MIB allows the manager to know about the special objects supported by the agent and access these objects as part of the standard object set.

2.2 TrunkPack-VoP Series Supported MIBs

The device contains an embedded SNMP agent supporting the listed MIBs below. A description in HTML format for all supported MIBs can be found in the MIBs directory in the release package.

- **The Standard MIB (MIB-2):** The various SNMP values in the standard MIB are defined in RFC 1213. The standard MIB includes various objects to measure and monitor IP activity, TCP activity, UDP activity, IP routes, TCP connections, interfaces, and general system description.
    - The standard icmpStatsTable and icmpMsgStatsTable under MIB-2 support ICMP statistics for both IPv4 and IPv6.
    - The inetCidrRouteTable (from the standard IP-FORWARD-MIB) supports both IPv4 and IPv6.

Note: For Mediant 3000/TP-6310 and Mediant 2000: In the ipCidrRouteIfIndex, the IF MIB indices are not referenced. Instead, the index used is related to one of the IP interfaces in the blade: (1) OAMP, (2) Media, and (3) Control. When there is only one interface, the only index is OAMP (1). Refer to the device's *User's Manual*.

- **System MIB (under MIB-2):** The standard system group: sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices. You can replace the value of sysObjectID.0 with variable value using the *ini* file parameter that calls SNMPSysOid. This parameter is polled during the startup and overwrites the standard sysObjectID. SNMPSysName is an administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
- **Host Resources MIB (RFC 2790):** The Host Resources MIB is used for managing host systems. The term host is any computer that communicates with other similar computers connected to the Internet and that is directly used by one or more human beings. The following are the Host Resources MIB objects:
    - hrSystem group
    - hrStorage group (basic only)
    - hrDevice group (CPU, RAM, Flash - basic only)

  - hrSWRunPerf (basic only)
  - hrSWInstalled (OS only)

  Applicable Products: All devices.

- **RTP MIB:** The RTP MIB is supported according to RFC 2959. It contains objects relevant to the RTP streams generated and terminated by the device and to the RTCP information related to these streams.

> **Note:** The inverse tables are not supported.

- **Notification Log MIB:** Standard MIB (RFC 3014 - iso.org.dod.internet.mgmt.mib-2) supported for implementation of Carrier Grade Alarms.
- **Alarm MIB:** IETF MIB (RFC 3877) supported as part of the implementation of Carrier Grade Alarms.
- **SNMP Target MIB**: (RFC 2273) allows for configuration of trap destinations and trusted managers.
- **SNMP MIB:** (RFC 3418) allows support for the coldStart and authenticationFailure traps.
- **SNMP Framework MIB:** (RFC 3411).
- **SNMP Usm MIB:** (RFC 3414) implements the user-based Security Model.
- **SNMP Vacm MIB:** (RFC 3415) implements the view-based Access Control Model.
- **SNMP Community MIB:** (RFC 3584) implements community string management.
- **ipForward MIB:** (RFC 2096) - fully supported.
- **RTCP-XR:** (RFC) implements the following partial support (applicable to all except MP):
  - The rtcpXrCallQualityTable is fully supported.
  - In the rtcpXrHistoryTable, support of the RCQ objects is provided only with no more than 3 intervals, 15 minutes long each.
  - Supports the rtcpXrVoipThresholdViolation trap.
- **ds1 MIB:** supports the following (Applicable only to Digital PSTN devices):
  - dsx1ConfigTable: partially supports the following objects with SET and GET applied:
    - dsx1LineCoding
    - dsx1LoopbackConfig
    - dsx1LineStatusChangeTrapEnable
    - dsx1CircuitIdentifier

  All other objects in this table support GET only.

  - dsx1CurrentTable
  - dsx1IntervalTable
  - dsx1TotalTable

    - dsx1LineStatusChange trap

- **ds3 MIB:** (RFC 3896) supports the following (Applicable only to the Mediant 3000):
    - dsx3ConfigTable: refer to the supplied MIB version for limits on specific objects. The table includes the following objects:
        - TimerElapsed
        - ValidIntervals
        - dsx3LoopbackConfig
    - dsx3LineStatusChange: The following tables (RFC 2496) are supported:
        - dsx3CurrentTable
        - dsx3IntervalTable
        - dsx3TotalTable

Proprietary MIB objects that are related to the SONET/SDH configuration (applicable only to Mediant 3000 with TP-6310):

- **In the acSystem MIB**:
        - acSysTransmissionType: sets the transmission type to optical or DS3 (T3).
- **SONET MIB:** (RFC 3592) implements the following partial support:
    - In the SonetMediumTable, the following objects are supported:
        - SonetMediumType
        - SonetMediumLineCoding
        - SonetMediumLineType
        - SonetMediumCircuitIdentifier
        - sonetMediumLoopbackConfig
    - In the SonetSectionCurrentTable, the following objects are supported:
        - IsonetSectionCurrentStatus
        - sonetSectionCurrentESs
        - sonetSectionCurrentSESs
        - sonetSectionCurrentSEFSs
        - sonetSectionCurrentCVs
    - In the SonetLineCurrentTable, the following objects are supported:
        - sonetLineCurrentStatus
        - sonetLineCurrentESs
        - sonetLineCurrentSESs
        - sonetLineCurrentCVs
        - sonetLineCurrentUASs
    - sonetSectionIntervalTable
    - sonetLineIntervalTable
    - sonetPathCurrentTable
    - sonetPathIntervalTable

- **Traps (refer AcBoard MIB for additional details):**
  - SONET (applicable only to Mediant 3000 with TP-6310):
    - acSonetSectionLOFAlarm
    - acSonetSectionLOSAlarm
    - acSonetLineAISAlarm
    - acSonetLineRDIAlarm
    - acSonetPathSTSLOPAlarm
    - acSonetPathSTSAISAlarm
    - acSonetPathSTSRDIAlarm
    - acSonetPathUnequippedAlarm
    - acSonetPathSignalLabelMismatchAlarm
  - DS3 (applicable only to Mediant 3000 with TP-6310):
    - acDS3RAIAlarm - DS3 RAI alarm
    - acDS3AISAlarm - DS3 AIS alarm
    - acDS3LOFAlarm - DS3 LOF alarm
    - acDS3LOSAlarm - DS3 LOS alarm
  - acSonetIfHwFailureAlarm
- **In the acPSTN MIB:**
  - acSonetSDHTable: currently has one entry (acSonetSDHFbrGrpMappingType) for selecting a low path mapping type. Relevant only for PSTN applications. (Refer to the MIB for more details.)
- **In the acSystem MIB:**
  - acSysTransmissionType: sets the transmission type to optical or DS3 (T3).

In addition to the standard MIBs, the complete product series contains proprietary MIBs:

- **AC-TYPES MIB:** lists the known types defined by the complete product series. This is referred to by the sysObjectID object in the MIB-II.
- The AcBoard MIB includes the following group: **acTrap**

Note: The AcBoard MIB is being phased out.

Each proprietary MIB contains a Configuration subtree for configuring the related parameters. In some, there also are Status and Action subtrees.

- **AcAnalog MIB** (Applicable only to Analog devices)
- **acControl MIB**
- **acMedia MIB**
- **acSystem MIB**

- **acSysInterfaceStatusTable:** supports the networking multiple interfaces feature status. This table reflects all the device's active interfaces. The lines indices consist of both the Entry Index and the Type Index. The table contains the following columns:
    - Entry Index - related Interface index in the interface configuration table (if the table is empty,i.e., there is only single IP address, the index appears with 0)
    - Type Index - 1 for IP Address and 2 for IPv6 Link-Local Address
    - Application Types - type assigned to the interface
    - Status Mode - interface configuration mode
    - IP Address - IP address (either IPv4 or IPv6) for this interface
    - Prefix Length - number of ‘1’ bits in this interface’s net mask
    - Gateway - default gateway
    - Vlan ID - VLAN ID of this interface
    - Name - interface’s name
    - Primary DNS Server IP Address - IP address of primary DNS server for this interface
    - Secondary DNS Server IP Address - IP address of secondary DNS server for this interface
- **acSysEthernetStatusTable** - Ethernet relevant information. (Applicable only to Mediant 3000 with TP-8410 Blade)
- **acSysModuleTable** (Applicable only to 8410 Blade Series)
- **acIPMediaChannelsresourcesTable** - IPMedia channels information such as Module ID and DSP Channels Reserved (Applicable only to Mediant 1000)
- **acPSTN MIB** (Applicable only to Digital PSTN devices)
- **acGateway MIB:** This proprietary MIB contains objects related to configuration of the SIP device. This MIB complements the other proprietary MIBs.

  The acGateway MIB includes the following groups:
    - **Common**: parameters common to both SIP and H.323.
    - **SIP**: SIP only parameters.
- **AcAlarm:** This is a proprietary carrier-grade alarm MIB. It is a simpler implementation of the notificationLogMIB and the IETF suggested alarmMIB (both also supported in all devices).

  The acAlarm MIB has the following groups:
    - **ActiveAlarm**: straight forward (single indexed) table listing all currently active Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).
    - **acAlarmHistory**: straight forward (single indexed) table listing all recently raised Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).

The table size can be altered via:

- notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigGlobalEntryLimit
  - or -
- notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigLogTable.nlmConfigLogEntry.nlmConfigLogEntryLimit.

The table size (i.e., number of contained alarms) can be as follows:

- Digital devices: Any value between 10 and 1,000 (default is 500)
- MediaPack devices: Any value between 10 and 100 (default is 100)

Notes:

- A detailed explanation of each parameter can be viewed in the MIB Description field.
- A detailed description in HTML format of all MIBs can be found in the MIBs directory (included in the Release package).
- Not all groups in the MIB are implemented.
- MIB Objects that are marked as 'obsolete' are not implemented.
- When a parameter is Set to a new value via SNMP, the change may affect device functionality immediately or may require that the device be soft reset for the change to take effect. This depends on the parameter type.
- The current (updated) device configuration parameters are configured on the device provided the user doesn't load an *ini* file to the device after reset. Loading an *ini* file after reset overrides the updated parameters.

2.3 SNMP Interface Details

This subsection describes details of the SNMP interface needed when developing an Element Management System (EMS) for any of the TrunkPack-VoP Series products, or to manage a device with a MIB browser.

There are several alternatives for SNMP security:

- SNMPv2c community strings
- SNMPv3 User-based Security Model (USM) users
- SNMP encoded over IPSec
- Various combinations of the above

Currently, both SNMP and *ini* file commands and downloads are not encrypted. For *ini* file encoding, refer to the device's *User's Manual*.

2.3.1 SNMP Community Names

By default, the device uses a single, read-only community string of "public" and a single read-write community string of "private". Up to five read-only community strings and up to five read-write community strings, and a single trap community string can be configured. Each community string must be associated with one of the following predefined groups:

Table 2-1: SNMP Predefined Groups

Group	Get Access	Set Access	Sends Traps
ReadGroup	Yes	No	Yes
ReadWriteGroup	Yes	Yes	Yes
TrapGroup	No	No	Yes

2.3.1.1 Configuring Community Strings via the Web

For detailed information on configuring community strings via the Web interface, refer to the device's *User's Manual*.

2.3.1.2 Configuring Community Strings via the ini File

The following *ini* file parameters are used to configure community strings:

- SNMPREADONLYCOMMUNITYSTRING_<x> = '#######'
- SNMPREADWRITECOMMUNITYSTRING_<x> = '#######'

Where <x> is a number from 0 through 4. Note that the '#' character represents any alphanumeric character. The maximum length of the string is 20 characters.

2.3.1.3 Configuring Community Strings via SNMP

To configure community strings, the EMS must use the standard snmpCommunityMIB. To configure the trap community string, the EMS must also use the snmpTargetMIB.

➢ **To add a read-only v2user community string:**

1. Add a new row to the snmpCommunityTable with CommunityName v2user.
2. Add a row to the vacmSecurityToGroupTable for SecurityName v2user, GroupName ReadGroup and SecurityModel snmpv2c.

➢ **To delete the read-only v2user community string:**

1. If v2user is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
2. Delete the snmpCommunityTable row with CommunityName v2user.
3. Delete the vacmSecurityToGroupTable row for SecurityName v2user, GroupName ReadGroup and SecurityModel snmpv2c.

➢ **To add a read-write v2admin community string:**

1. Add a new row to the snmpCommunityTable with CommunityName v2admin.
2. Add a row to the vacmSecurityToGroupTable for SecurityName v2admin, GroupName ReadWriteGroup and SecurityModel snmpv2c.

➢ **To delete the read-write v2admin community string:**

1. If v2admin is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
2. Delete the snmpCommunityTable row with a CommunityName of v2admin and GroupName of ReadWriteGroup.

➢ **To change the only read-write community string from v2admin to v2mgr:**

1. Follow the procedure above to add a read-write community string to a row for v2mgr.
2. Set up the EM such that subsequent set requests use the new community string, v2mgr.
3. If v2admin is being used as the trap community string, follow the procedure to change the trap community string. (See below.)
4. Follow the procedure above to delete a read-write community name in the row for v2admin.

The following procedure assumes that a row already exists in the snmpCommunityTable for the new trap community string. The trap community string can be part of the TrapGroup, ReadGroup, or ReadWriteGroup. If the trap community string is used solely for sending traps (recommended), then it should be made part of the TrapGroup.

➢ **To change the trap community string:**

1. Add a row to the vacmSecurityToGroupTable with these values: SecurityModel=2, SecurityName=the new trap community string, GroupName=TrapGroup, ReadGroup or ReadWriteGroup. The SecurityModel and SecurityName objects are row indices.

Note: You must add GroupName and RowStatus on the same set.

2. Modify the SecurityName field in the appropriate row of the snmpTargetParamsTable.
3. Remove the row from the vacmSecurityToGroupTable with SecurityName=the old trap community string.

2.3.2 SNMPv3 USM Users

You can configure up to 10 User-based Security Model (USM) users (referred to as *SNMPv3* user). Each SNMPv3 user can be configured for one of the following security levels:

Table 2-2: SNMPv3 Security Levels

Security Levels	Authentication	Privacy
noAuthNoPriv(1)	none	none
authNoPriv(2)	MD5 or SHA-1	none
authPriv(3)	MD5 or SHA-1	DES, 3DES, AES128, AES192, or AES256

Each SNMPv3 user must be associated with one of the predefined groups listed in the following table:

Table 2-3: SNMPv3 Predefined Groups

Group	Get Access	Set Access	Sends Traps	Security Level
ReadGroup1	Yes	No	Yes	noAuthNoPriv(1)
ReadWriteGroup1	Yes	Yes	Yes	noAuthNoPriv(1)
TrapGroup1	No	No	Yes	noAuthNoPriv(1)
ReadGroup2	Yes	No	Yes	authNoPriv(2)
ReadWriteGroup2	Yes	Yes	Yes	authNoPriv(2)
TrapGroup2	No	No	Yes	authNoPriv(2)
ReadGroup3	Yes	No	Yes	authPriv(3)
ReadWriteGroup3	Yes	Yes	Yes	authPriv(3)
TrapGroup3	No	No	Yes	authPriv(3)

⚠ **Note:** The first (initial) SNMPv3 user can only be configured through a management interface other than SNMP (i.e., Web interface, configuration ini file, or CLI). Once configured, additional users can be configured through the SNMP interface as well.

2.3.2.1 Configuring SNMPv3 Users via the ini File

Use the SNMPUsers *ini* file table parameter to add, modify, and delete SNMPv3 users. The SNMPUsers *ini* table is a hidden parameter. Therefore, when you load the *ini* file to the device using the Web interface, the table is not included in the generated file.

Table 2-4: SNMPv3 Table Columns Description

Parameter	Description	Default
Row number	Table index. Its valid range is 0 to 9.	N/A
SNMPUsers_Username	Name of the v3 user. Must be unique. The maximum length is 32 characters.	N/A
SNMPUsers_AuthProtocol	Authentication protocol to be used for this user. Possible values are 0 (none), 1 (MD5), 2 (SHA-1)	0
SNMPUsers_PrivProtocol	Privacy protocol to be used for this user. Possible values are 0 (none), 1 (DES), 2 (3DES), 3 (AES128), 4 (AES192), 5 (AES256)	0
SNMPUsers_AuthKey	Authentication key.	""
SNMPUsers_PrivKey	Privacy key.	""
SNMPUsers_Group	The group that this user is associated with. Possible values are 0 (read-only group), 1 (read-write group), and 2 (trap group). The actual group will be ReadGroup<sl>, ReadWriteGroup<sl> or TrapGroup<sl> where <sl> is the SecurityLevel (1=noAuthNoPriv, 2=authNoPriv, 3=authPriv)	0

Keys can be entered in the form of a text password or in the form of a localized key in hex format. If using a text password, then it should be at least 8 characters in length. Below is an example showing the format of a localized key:

```
26:60:d8:7d:0d:4a:d6:8c:02:73:dd:22:96:a2:69:df
```

The following sample configuration creates three SNMPv3 USM users.

```
[ SNMPUsers ]
FORMAT SNMPUsers_Index = SNMPUsers_Username,
SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey,
SNMPUsers_PrivKey, SNMPUsers_Group;
SNMPUsers 0 = v3user, 0, 0, -, -, 0;
SNMPUsers 1 = v3admin1, 1, 0, myauthkey, -, 1;
SNMPUsers 2 = v3admin2, 2, 1, myauthkey, myprivkey, 1;
[ \SNMPUsers ]
```

The example above creates three SNMPv3 users:

- The user v3user is set up for a security level of noAuthNoPriv(1) and is associated with ReadGroup1.
- The user v3admin1 is setup for a security level of authNoPriv(2), with authentication protocol MD5. The authentication text password is “myauthkey” and the user is associated with ReadWriteGroup2.
- The user v3admin2 is setup for a security level of authPriv(3), with authentication protocol SHA-1 and privacy protocol DES. The authentication text password is “myauthkey”, the privacy text password is “myprivkey”, and the user is associated with ReadWriteGroup3.

2.3.2.2 Configuring SNMPv3 Users via SNMP

To configure SNMPv3 users, the EMS must use the standard snmpUsmMIB and the snmpVacmMIB.

➢ **To add a read-only, noAuthNoPriv SNMPv3 user, v3user:**

1. Clone the row with the same security level. After the clone step, the status of the row will be notReady(3).
2. Activate the row. That is, set the row status to active(1).
3. Add a row to the vacmSecurityToGroupTable for SecurityName v3user, GroupName ReadGroup1 and SecurityModel usm(3).

Note: A row with the same security level (noAuthNoPriv) must already exist in the usmUserTable. (see the usmUserTable for details).

➢ **To delete the read-only, noAuthNoPriv SNMPv3 user, v3user:**

1. If v3user is associated with a trap destination, follow the procedure for associating a different user to that trap destination. (See below.)
2. Delete the vacmSecurityToGroupTable row for SecurityName v3user, GroupName ReadGroup1 and SecurityModel usm.
3. Delete the row in the usmUserTable for v3user.

➢ To add a read-write, authPriv SNMPv3 user, v3admin1:

1. Clone the row with the same security level.
2. Change the authentication key and privacy key.
3. Activate the row. That is, set the row status to active(1).
4. Add a row to the vacmSecurityToGroupTable for SecurityName v3admin1, GroupName ReadWriteGroup3 and SecurityModel usm(3).

Note: A row with the same security level (authPriv) must already exist in the usmUserTable (see the usmUserTable for details).

➢ To delete the read-write, authPriv SNMPv3 user, v3admin1:

1. If v3admin1 is associated with a trap destination, follow the procedure for associating a different user to that trap destination. (See below.)
2. Delete the vacmSecurityToGroupTable row for SecurityName v3admin1, GroupName ReadWriteGroup1 and SecurityModel usm.
3. Delete the row in the usmUserTable for v3admin1.

2.3.3 Trusted Managers

By default, the SNMP agent accepts Get and Set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced implementing *Trusted Managers*. A Trusted Manager is an IP address from which the SNMP agent accepts and processes Get and Set requests. An element management can be used to configure up to five Trusted Manager.

The concept of Trusted Managers is considered to be a weak form of security and therefore is not a required part of SNMPv3 security, which uses authentication and privacy. Trusted Managers for the devices' SNMP agent are applicable only for SNMPv2c users. An exception to this is when the community string is not the default string (‘public’/’private’), at which time Trusted Managers are applicable for SNMPV2c users alongside SNMPv3 users.

Note: If trusted managers are defined, then all community strings works from all trusted managers, i.e.,there is no way to associate a community string with specific trusted managers.

2.3.3.1 Configuring Trusted Managers via ini File

To set the Trusted Managers table from start up, write the following in the *ini* file:

```
SNMPTRUSTEDMGR_X = D.D.D.D
```

Where *X* is any integer between 0 and 4 (0 sets the first table entry, 1 sets the second and so on), and *D* is an integer between 0 and 255.

2.3.3.2 Configuring Trusted Managers via SNMP

To configure Trusted Managers, the Element Management System (EMS) must use the SNMP-COMMUNITY-MIB and snmpCommunityMIB and the snmpTargetMIB.

The procedure below assumes the following: at least one configured read-write community; currently no Trusted Managers; TransportTag for columns for all snmpCommunityTable rows are currently empty.

➢ **To add the first Trusted Manager:**

1. Add a row to the snmpTargetAddrTable with these values: Name=mgr0, TagList=MGR, Params=v2cparams.
2. Add a row to the snmpTargetAddrExtTable table with these values: Name=mgr0, snmpTargetAddrTMask=255.255.255.255:0. The agent does not allow creation of a row in this table unless a corresponding row exists in the snmpTargetAddrTable.
3. Set the value of the TransportTag field on each non-TrapGroup row in the snmpCommunityTable to MGR.

The procedure below assumes the following: at least one configured read-write community; currently one or more Trusted Managers; TransportTag for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from one of the existing Trusted Managers.

➢ **To add a subsequent Trusted Manager:**

1. Add a row to the snmpTargetAddrTable with these values: Name=mgrN, TagList=MGR, Params=v2cparams, where N is an unused number between 0 and 4.
2. Add a row to the snmpTargetAddrExtTable table with these values: Name=mgrN, snmpTargetAddrTMask=255.255.255.255:0.

An alternative to the above procedure is to set the snmpTargetAddrTMask column while you are creating other rows in the table.

The procedure below assumes the following: at least one configured read-write community; currently two or more Trusted Managers; taglist for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from one of the existing trusted managers, but not the one that is being deleted.

➢ **To delete a Trusted Manager (not the last one):**

- Remove the appropriate row from the snmpTargetAddrTable.

The change takes affect immediately. The deleted trusted manager cannot access the device. The agent automatically removes the row in the snmpTargetAddrExtTable.

The procedure below assumes the following: at least one configured read-write community; currently only one Trusted Manager; taglist for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from the final Trusted Manager.

➢ **To delete the last Trusted Manager:**

1. Set the value of the TransportTag field on each row in the snmpCommunityTable to the empty string.
2. Remove the appropriate row from the snmpTargetAddrTable.

The change takes effect immediately. All managers can now access the device. The agent automatically removes the row in the snmpTargetAddrExtTable.

2.3.4 SNMP Ports

The SNMP Request Port is 161 and Trap Port is 162. These port numbers for SNMP requests and responses can be changed by using the following *ini* file parameter:

```
SNMPPort = <port_number>
```

The valid value is any valid UDP port number; the default is 161 (recommended).

2.3.5 Multiple SNMP Trap Destinations

An agent can send traps to up to five managers. For each manager you need to define the manager IP address and trap receiving port along with enabling the sending to that manager. You can also associate a trap destination with a specific SNMPv3 USM user. Traps are sent to this trap destination using the SNMPv3 format and the authentication and privacy protocol configured for that user.

To configure the Trap Managers table, use one of the following methods:

- Web interface (refer to the device's *User's Manual*)
- *ini* file (see "Configuring Trap Managers via the ini File" on page 24)
- SNMP (see "Configuring Trap Managers via SNMP" on page 25)

2.3.5.1 Configuring Trap Managers via Host Name

One of the five available SNMP managers can be defined using the manager's host name (i.e., FQDN). This is currently supported using an *ini* file only (SNMPTrapManagerHostName).

When this parameter value is defined for this trap, the device at start up tries to resolve the host name. Once the name is resolved (i.e., the IP address is found), the resolved IP address replaces the last entry of the trap manager table (defined by the parameter SNMPManagerTableIP_x) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. The port is 162 (unless specified otherwise). The row is marked as 'used' and the sending is 'enabled'.

When using 'host name' resolution, any changes made by the user to this row in either MIBs are overwritten by the device when a resolving is redone (once an hour).

Note: Some traps may be lost until the name resolving is complete.

2.3.5.2 Configuring Trap Managers via ini File

In the *ini* file, parameters below can be set to enable or disable the sending of SNMP traps. Multiple trap destinations can be supported on the device by setting multiple trap destinations in the ini file.

- **SNMPManagerTrapSendingEnable_<x>:** indicates whether or not traps are to be sent to the specified SNMP trap manager. A value of ‘1’ means that it is enabled, while a value of ‘0’ means disabled. The <x> represents a number 0, 1, or 2, which is the array element index. Currently, up to five SNMP trap managers is supported.

- **SNMPManagerTrapUser_<x>:** indicates to send an SNMPv2 trap using the trap user community string configured with the SNMPTrapCommunityString parameter. You may instead specify an SNMPv3 user name.

Below is an example of entries in the *ini* file regarding SNMP. The device can be configured to send to multiple trap destinations.

```
; SNMP trap destinations
; The device maintains a table of trap destinations containing 5
; rows. The rows are numbered 0..4. Each block of 5 items below
; applies to a row in the table.
;
; To configure one of the rows, uncomment all 5 lines in that
; block. Supply an IP address and if necessary, change the port
; number.
;
; To delete a trap destination, set ISUSED to 0.
;
;SNMPManagerTableIP_0=
;SNMPManagerTrapPort_0=162
;SNMPManagerIsUsed_0=1
;SNMPManagerTrapSendingEnable_0=1
;SNMPManagerTrapUser_0=’’
;
;SNMPManagerTableIP_1=
;SNMPManagerTrapPort_1=162
;SNMPManagerIsUsed_1=1
;SNMPManagerTrapSendingEnable_1=1
;SNMPMANAGERTRAPUSER_1=’’
;
;SNMPManagerTableIP_2=
;SNMPManagerTrapPort_2=162
;SNMPManagerIsUsed_2=1
;SNMPManagerTrapSendingEnable_2=1
;SNMPManagerTrapUser_2=’’
;
;SNMPManagerTableIP_3=
;SNMPManagerTrapPort_3=162
;SNMPManagerIsUsed_3=1
;SNMPManagerTrapSendingEnable_3=1
```

```
;SNMPManagerTrapUser_3=''
;
;SNMPMANAGERTABLEIP_4=
;SNMPManagerTrapPort_4=162
;SNMPManagerIsUsed_4=1
;SNMPManagerTrapSendingEnable_4=1
;SNMPManagerTrapUser_4=''
```

The ‘trap manager host name’ is configured via SNMPTrapManagerHostName. For example:

```
;SNMPTrapManagerHostName = 'myMananger.corp.MyCompany.com'
```

Note: The same information that is configurable in the *ini* file can also be configured via the acBoardMIB.

2.3.5.3 Configuring SNMP Engine ID

The SNMPEngineIDString *ini* file parameter configures the SNMP engine ID. The ID can be a string of up to 36 characters. Once defined, the device must be reset for the parameter to take effect.

The default value is 00:00:00:00:00:00:00:00:00:00:00:00 (12 Hex characters). The provided key must be set with 12 Hex values delimited by ‘:’.

If the supplied key does not pass validation of the 12 Hex values input or it is set with the default value, the engine ID is then generated, according to RFC 3411.

Before setting this parameter, all SNMPv3 users must be deleted, otherwise the configuration is ignored.

2.3.5.4 Configuring Trap Managers via SNMP

The snmpTargetMIB interface is available for configuring trap managers.

Note: The acBoard MIB is planned to become obsolete. The only relevant section in this MIB is the trap subtree acTRap.

➢ **To add an SNMPv2 trap destination:**

- Add a row to the snmpTargetAddrTable with these values: Name=trapN, TagList=AC_TRAP, Params=v2cparams, where N is an unused number between 0 and 4

All changes to the trap destination configuration take effect immediately.

➢ **To add an SNMPv3 trap destination:**

1. Add a row to the snmpTargetAddrTable with these values: Name=trapN, TagList=AC_TRAP, Params=usm<user>, where N is an unused number between 0 and 4, and <user> is the name of the SNMPv3 that this user is associated with.

2. If a row does not already exist for this combination of user and SecurityLevel, add a row to the snmpTargetParamsTable with these values: Name=usm<user>, MPModel=3(SNMPv3), SecurityModel=3 (usm), SecurityName=<user>, SecurityLevel=M, where M is either 1(noAuthNoPriv), 2(authNoPriv) or 3(authPriv).

All changes to the trap destination configuration take effect immediately.

➢ To delete a trap destination:

- Remove the appropriate row from the snmpTargetAddrTable.
- If this is the last trap destination associated with this user and security level, you could also delete the appropriate row from the snmpTargetParamsTable.

➢ To modify a trap destination:

You can change the IP address and or port number for an existing trap destination. The same effect can be achieved by removing a row and adding a new row.

- Modify the IP address and/or port number for the appropriate row in the snmpTargetAddrTable.

➢ To disable a trap destination:

- Change TagList on the appropriate row in the snmpTargetAddrTable to the empty string.

➢ To enable a trap destination:

- Change TagList on the appropriate row in the snmpTargetAddrTable to ‘AC_TRAP’.
- Change TagList on the appropriate row in the snmpTargetAddrTable to "AC_TRAP".

3 Carrier-Grade Alarm System

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

A carrier-grade alarm system is characterized by the following:

- The device allows an EMS to determine which alarms are currently active in the device. That is, the device maintains an active alarm table.
- The device allows an EMS to detect lost alarms and clear notifications [sequence number in trap, current sequence number MIB object]
- The device allows an EMS to recover lost alarm raise and clear notifications [maintains a log history]
- The device sends a cold start trap to indicate that it is starting. This allows the EMS to synchronize its view of the device's active alarms.

When the SNMP alarm traps are sent, the carrier-grade alarm system does not add or delete alarm traps as part of the feature. This system provides the mechanism for viewing of history and current active alarm information.

3.1 Active Alarm Table

The device maintains an active alarm table to allow an EMS to determine which alarms are currently active in the device. Two views of the active alarm table are supported by the agent:

- acActiveAlarmTable in the enterprise AcAlarm
- alarmActiveTable and alarmActiveVariableTable in the IETF standard AcAlarm MIB (rooted in the MIB tree)

The acActiveAlarmTable is a simple, one-row per alarm table that is easy to view with a MIB browser.

3.2 Alarm History

The device maintains a history of alarms that have been raised and traps that have been cleared to allow an EMS to recover any lost raise or clear traps. Two views of the alarm history table are supported by the agent:

- acAlarmHistoryTable in the enterprise AcAlarm - a simple, one-row per alarm table, that is easy to view with a MIB browser.
- nlmLogTable and nlmLogVariableTable in the standard NOTIFICATION-LOG-MIB

3.3 SONET Alarm Consolidation

You can enable the device to send trunk alarms only on the DS3 level (instead of trunk level). When the DS3AlarmConsolidation parameter is set to 1, the PSTN alarms are consolidated. In such a setup, only SDH alarms are raised and no alarms are raised for trunks (even if they exist). When the SDH alarm is cleared, trunk alarms are raised (if they exist.

Note: This section is applicable only to Mediant 3000/TP-6310.

3.4 ISDN Alarm Consolidation

The device consolidates trunk alarms pertaining to an NFAS group. When a trunk alarm is raised, the D-channel and B-channel alarms are automatically cleared. When the trunk alarm is cleared, the D-channel and B-channel alarms are restored (raised again).

Note: This section is applicable only to Mediant 3000.

4 Topology MIB Objects

4.1 Physical Entity (RFC 2737)

The following groups are supported:

- **entityPhysical group:** Describes the physical entities managed by a single agent.
- **entityMapping group:** Describes the associations between the physical entities, logical entities, interfaces, and non-interface ports managed by a single agent.
- **entityGeneral group:** Describes general system attributes shared by potentially all types of entities managed by a single agent.
- **entityNotifications group:** Contains status indication notifications.

4.2 IF-MIB (RFC 2863)

The following interface types are presented in the ifTable:

- **ethernetCsmacd(6):** for all Ethernet-like interfaces, regardless of speed, as per RFC 3635 (Gigabit Ethernet for 3000 Series devices)
- **ds1(18):** DS1-MIB
- **voiceFXO(101):** Voice Foreign Exchange Office. (Applicable only to MP-118 and Mediant 1000.)
- **voiceFXS(102):** Voice Foreign Exchange Station. (Applicable only to MP-118 and Mediant 1000.)
- **sonet(39):** SONET-MIB. (Applicable only to the 3000 Series.)
- **ds3(30):** DS3-MIB. (Applicable only to the 3000 Series.)

The numbers in the brackets above refer to the IANA's interface-number.

For each interface type, the following objects are supported:

Table 4-1: DS1 Digital Interfaces (Digital PSTN)

ifTable	Value
ifDescr	Digital DS1 interface.
ifType	ds1(18).
ifMtu	Constant zero.
ifSpeed	DS1 = 1544000, or E1 = 2048000, according to dsx1LineType
ifPhysAddress	The value of the Circuit Identifier [dsx1CircuitIdentifier]. If no Circuit Identifier has been assigned this object should have an octet string with zero length.
ifAdminStatus	Trunk's Lock & Unlock during run time. In initialization process we need to refer the Admin-Status parameter.
ifOperStatus	Up or Down, according to the operation status.
ifLastChange	The value of sysUpTime at the time the interface entered its current operational state.

ifTable	Value
ifDescr	Digital DS1 interface.
ifXTable	**Value**
ifName	Digital# acTrunkIndex
ifLinkUpDownTrapEnable	Set to enabled(1)
ifHighSpeed	Speed of line in Megabits per second: 2
ifConnectorPresent	Set to true(1) normally, except for cases such as DS1/E1 over AAL1/ATM where false(2) is appropriate
ifCounterDiscontinuityTime	Always zero.

Table 4-2: BRI Interfaces (Applicable to MSBR Series, Mediant 1000 & Mediant 600)

ifTable	Value
ifDescr	BRI interface
ifType	isdns(75)
ifMtu	Constant zero
ifSpeed	144000
ifPhysAddress	Octet string with zero length
ifAdminStatus	Trunk’s Lock & Unlock during run time. In initialization process, refer to the Admin-Status parameter.
ifOperStatus	Up or Down according to the operation status.
ifLastChange	The value of sysUpTime at the time the interface entered its current operational state.
ifXTable	**Value**
ifName	BRI port no. #
ifLinkUpDownTrapEnable	Set to enabled (1)
ifHighSpeed	Speed of line in megabits per second.
ifPromiscuousMode	Non promiscuous mode (1)
ifConnectorPresent	Set to true (1) normally
ifCounterDiscontinuityTime	Always zero

Table 4-3: Ethernet (Gigabit for 3000 Series) Interface

ifTable & ifXTable	Value
ifIndex	Constructed as defined in the device's Index format.
ifDescr	Ethernet interface.
ifType	ethernetCsmacd(6)
ifMtu	1500

ifTable & ifXTable	Value
ifSpeed	acSysEthernetFirstPortSpeed in bits per second (Applicable only to Mediant 1000) 0 since it's GBE - refer to ifHighSpeed (Applicable only to 3000 Series and Mediant 4000).
ifPhysAddress	00-90-8F plus acSysIdSerialNumber in hex.Will be same for both dual ports.
ifAdminStatus	Always UP. [Read Only] - Write access is not required by the standard. Support for 'testing' is not required.
ifOperStatus	Up or Down corresponding to acAnalogFxsFxoType where Unknown is equal to Down.
ifLastChange	The value of sysUpTime at the time the interface entered its current operational state.
ifInOctets	The number of octets in valid MAC frames received on this interface, including the MAC header and FCS. This does include the number of octets in valid MAC Control frames received on this interface.
ifInUcastPkts	As defined in IfMIB.
ifInDiscards	As defined in IfMIB.
ifInErrors	The sum for this interface of dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, and dot3StatsInternalMacReceiveErrors.
ifInUnknownProtos	As defined in IfMIB.
ifOutOctets	The number of octets transmitted in valid MAC frames on this interface, including the MAC header and FCS. This does include the number of octets in valid MAC Control frames transmitted on this interface.
ifOutUcastPkts	As defined in IfMIB.
ifOutDiscards	As defined in IfMIB.
ifOutErrors	The sum for this interface of: dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors and dot3StatsCarrierSenseErrors.
ifName	Ethernet (Gigabit for 3000 Series) port #1 or# 2 Gb Ethernet Port 5/n, where *n* is the port number (applicable only to Mediant 4000)
ifInMulticastPkts	As defined in IfMIB.
ifInBroadcastPkts	As defined in IfMIB.
ifOutMulticastPkts	As defined in IfMIB.
ifOutBroadcastPkts	As defined in IfMIB.
ifHCInOctets **ifHCOutOctets**	64-bit versions of counters. Required for ethernet-like interfaces that are capable of operating at 20 Mb/s or faster, even if the interface is currently operating at less than 20 Mb/s.

ifTable & ifXTable	Value
ifHCInUcastPkts **ifHCInMulticastPkts** **ifHCInBroadcastPkts** **ifHCOutUcastPkts** **ifHCOutMulticastPkts** **ifHCOutBroadcastPkts**	64-bit versions of packet counters. Required for ethernet-like interfaces that are capable of operating at 640 Mb/s or faster, even if the interface is currently operating at less than 640 Mb/s. Therefore, will be constant zero.
ifLinkUpDownTrapEnable	Refer to [RFC 2863]. Default is 'enabled'
ifHighSpeed	**3000 Series/Mediant 4000:** 1000 **Mediant 1000:** 10 or 100 according to acSysEthernetFirstPortSpeed
ifPromiscuousMode	Constant False. [R/O]
ifConnectorPresent	Constant True.
ifAlias	An 'alias' name for the interface as specified by a network manager (NVM)
ifCounterDiscontinuityTime	As defined in IfMIB.

Table 4-4: SONET /SDH Interfaces (Mediant 3000)

ifTable & ifXTable	Value
ifDescr	SONET/SDH interface. Module #n Port #n
ifType	sonet(39).
ifMtu	Constant zero.
ifSpeed	155520000
ifPhysAddress	The value of the Circuit Identifier. If no Circuit Identifier has been assigned this object should have an octet string with zero length.
ifAdminStatus	Read-only access -- Always UP.
ifOperStatus	The value testing(3) is not used. This object assumes the value down(2), if the objects sonetSectionCurrentStatus and sonetLineCurrentStatus have any other value than sonetSectionNoDefect(1) and sonetLineNoDefect(1), respectively.
ifLastChange	The value of sysUpTime at the time the interface entered its current operational state.
ifName	SONET /SDH port no. n
ifLinkUpDownTrapEnable	Set to enabled(1)
ifHighSpeed	Speed of line in Megabits per second: 155
ifConnectorPresent	Set to true(1) normally, except for cases such as DS1/E1 over AAL1/ATM where false(2) is appropriate
ifCounterDiscontinuityTime	Always zero.

Table 4-5: DS3 Interfaces (Mediant 3000)

ifTable & ifXTable	Value
ifDescr	DS3 interface, Module no.#d, Port no.#d
ifType	Ds3(30).
ifMtu	Constant zero.
ifSpeed	44736000
ifPhysAddress	The value of the Circuit Identifier. If no Circuit Identifier has been assigned this object should have an octet string with zero length.
ifAdminStatus	Read-only access -- Always UP.
ifOperStatus	The value testing(3) is not used. This object assumes the value down(2), if the objects dsx3LineStatus has any other value than dsx3NoAlarm(1).
ifLastChange	The value of sysUpTime at the time the interface entered its current operational state.
ifName	DS3 port no. n
ifLinkUpDownTrapEnable	Set to enabled(1)
ifHighSpeed	Speed of line in Megabits per second: 45
ifConnectorPresent	Set to true(1)
ifCounterDiscontinuityTime	Always zero.

4.3 MIB-II Counters

Note: This section is applicable only to the MSBR series.

- TCP (1.3.6.1.2.1.6):
    - tcpRtoAlgorithm
    - tcpRtoMin
    - tcpRtoMax
    - tcpMaxConn
    - tcpActiveOpens
    - tcpPassiveOpens
    - tcpAttemptFails
    - tcpEstabResets
    - tcpCurrEstab
    - tcpInSegs

  - tcpOutSegs
  - tcpRetransSegs
  - tcpInErrs
  - tcpOutRsts
  - tcpHCInSegs
  - tcpHCOutSegs
- UDP (1.3.6.1.2.1.7):
  - udpInDatagrams
  - udpNoPorts
  - udpInErrors
  - udpOutDatagrams
  - udpHCInDatagrams
  - udpHCOutDatagrams
- IP (1.3.6.1.2.1.4):
  - ipForwarding
  - ipDefaultTTL
  - ipInReceives
  - ipInHdrErrors
  - ipInAddrErrors
  - ipForwDatagrams
  - ipInUnknownProtos
  - ipInDiscards
  - ipInDelivers
  - ipOutRequests
  - ipOutDiscards
  - ipOutNoRoutes
  - ipReasmTimeout
  - ipReasmReqds
  - ipReasmOKs
  - ipReasmFails
  - ipFragCreate
- ICMP (1.3.6.1.2.1.5):
  - icmpInMsgs
  - icmpInErrors
  - icmpInDestUnreachs
  - icmpInTimeExcds
  - icmpInParmProbs
  - icmpInSrcQuenchs

- icmpInRedirects
- icmpInEchos
- icmpInEchoReps
- icmpInTimestamps
- icmpInTimestampReps
- icmpInAddrMasks
- icmpInAddrMaskReps
- icmpOutMsgs
- icmpOutErrors
- icmpOutDestUnreachs
- icmpOutTimeExcds
- icmpOutParmProbs
- icmpOutSrcQuenchs
- icmpOutRedirects
- icmpOutEchos
- icmpOutEchoReps
- icmpOutTimestamps
- icmpOutTimestampReps
- icmpOutAddrMasks
- icmpOutAddrMaskReps

- IF (1.3.6.1.2.1.2.2):
  - ifInOctets
  - ifInUcastPkts
  - ifInDiscards
  - ifInErrors
  - ifOutOctets
  - ifOutUcastPkts
  - ifOutErrors
  - ifInMulticastPkts
  - ifInBroadcastPkts
  - ifOutMulticastPkts
  - ifOutBroadcastPkts

Reader's Notes

5 File Management

SNMP supports file download, upload, and removal.

5.1 Downloading a File to the Device

The file URL is set in the appropriate MIB object under the acSysHTTPClient subtree (refer to the subtree objects description for the URL form). The download can be scheduled using the acSysHTTPClientAutoUpdatePredefinedTime and acSysHTTPClientAutoUpdateFrequency objects. It can also be a manual process using acSysActionSetAutoUpdate. In this case (only) and as long as one URL is set at a time, the result can be viewed in acSysActionSetAutoUpdateActionResult. In both cases, the acHTTPDownloadResult trap is sent, indicating the success or failure of the process.

acSysActionSetActionId can be set to any value and can be used to indicate an action performed by a certain manager.

A successful process also ends with the file name in the appropriate object under the acSysFile subtree or in the acCASFileTable or the acAuxiliaryFiles subtree, along with the URL being erased from the object under the acSysHTTPClient subtree.

Notes:

- The action result (both in the acSysActionSetAutoUpdateActionResult object and acHTTPDownloadResult trap) for the Voice Prompt and XML indicates only that the file reached the device and has no indication on the application’s ability to parse the file.
- The action result in acSysActionSetAutoUpdateActionResult is reliable as long as only one file is downloaded at a time.

5.2 Uploading and Deleting a File

File upload is the procedure of sending a file from the device to the manager. Deleting a file is erasing it from the device, an offline action that requires a reset for it to be applied. The acSysUpload subtree holds all relevant objects.

- **acSysUploadFileURI** indicates the file name and location along with the file transfer protocol (HTTP or NFS), for example, “http:\\server\filename.txt”.
- **acSysUploadFileType** and **acSysUploadFileNumber** are used to determine the file to be uploaded along with its instance when relevant (for CAS or Video Font).
- **acSysUploadActionID** is at the disposal of the manager and can be used to indicate that a certain manager has performed the action.
- **acSysUploadActionType** determines the action that occurs and triggers it off at the same time.

Note: File upload using SNMP is supported only for ini files; file removal using SNMP is supported for all files except ini files.

Reader's Notes

6 Performance Measurements

Performance measurements are available for a third-party performance monitoring system through an SNMP interface. These can be polled at scheduled intervals by an external poller or utility in the management server or other off-board systems.

The device provides performance measurements in the form of two types:

- **Gauges:** Gauges represent the current state of activities on the device. 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 device 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 device performance measurements are provided by several proprietary MIBs (located under the acPerformance subtree):

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).AudioCodes(5003).acPerformance(10).

The performance monitoring MIBs all have an identical structure, which includes two major subtrees:

- **Configuration**: allows configuration of general attributes of the MIB and specific attributes of the monitored objects
- **Data**

The monitoring results are presented in tables. There are one or two indices in each table. If there are two indices, the first is a sub-set in the table (e.g., trunk number) and the second (or a single where there is only one) index represents the interval number (present - 0, previous - 1, and the one before - 2).

The MIBs include:

- **acPMMedia**: media-related (voice) monitoring such as RTP and DSP.
- **acPMControl**: Control Protocol-related monitoring such as connections, commands.
- **acPMAnalog:** Analog channels off-hook state. (Applicable only to Analog devices.)
- **acPMPSTN:** PSTN-related monitoring such as channel use, trunk utilization. (Applicable only to Digital PSTN devices.)
- **acPMSystem:** general (system-related) monitoring.
- **acPMMediaServer:** for Media Server specific monitoring. (Applicable only to 3000 Series.)

The log trap acPerformanceMonitoringThresholdCrossing (non-alarm) is sent every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

6.1 Total Counters

The counter’s attribute 'total' accumulates counter values since the device's most recent restart. The user can reset the total’s value by setting the Reset-Total object.

Each MIB module has its own Reset Total object, as follows:

- **PM-Analog:** acPMAnalogConfigurationResetTotalCounters (Applicable only to Analog devices)
- **PM-Control:** acPMControlConfigurationResetTotalCounters
- **PM-Media:** acPMMediaConfigurationResetTotalCounters
- **PM-PSTN:** acPMPSTNConfigurationResetTotalCounters (Applicable only to Digital PSTN devices)
- **PM-System:** acPMSystemConfigurationResetTotalCounters

6.2 Performance Monitoring Parameters

The device’s SNMP MIB PM parameters are listed in the subsequent subsections.

6.2.1 DS3 Performance Monitoring

Note: These PM parameters are applicable only to Mediant 3000 with the TP-6310 blade.

DS3 Performance Monitoring

MIB Name	Gauge/Counter	Description
dsx3IntervalPESs	Gauge	The counter associated with the number of P-bit Errored Seconds. EMS Parameter Name: DS3 PESs
dsx3IntervalPSESs	Gauge	The counter associated with the number of P-bit Severely Errored Seconds. EMS Parameter Name: DS3 PSESs
dsx3IntervalUASs	Gauge	The counter associated with the number of Unavailable Seconds. This object may decrease if the occurrence of unavailable seconds occurs across an interval boundary. EMS Parameter Name: DS3 UASs
dsx3IntervalLCVs	Gauge	The counter associated with the number of Line Coding Violations. EMS Parameter Name: DS3 LCVs
DS3 PCVs	Gauge	The counter associated with the number of P-bit Coding Violations. EMS Parameter Name: dsx3IntervalPCVs
dsx3IntervalLESs	Gauge	The number of Line Errored Seconds (BPVs or illegal zero sequences). EMS Parameter Name: DS3 LESs

MIB Name	Gauge/Counter	Description
dsx3IntervalCCVs	Gauge	The number of C-bit Coding Violations. EMS Parameter Name: DS3 CCVs
dsx3IntervalCESs	Gauge	The number of C-bit Errored Seconds. EMS Parameter Name: DS3 CESs
dsx3IntervalCSESs	Gauge	The number of C-bit Severely Errored Seconds. EMS Parameter Name: DS3 CSESs
dsx3CurrentPESs	-	The counter associated with the number of P-bit Errored Seconds.
dsx3CurrentPSESs	-	The counter associated with the number of P-bit Severely Errored Seconds.
dsx3CurrentUASs	-	The counter associated with the number of Unavailable Seconds.
dsx3CurrentLCVs	-	The counter associated with the number of Line Coding Violations.
dsx3CurrentPCVs	-	The counter associated with the number of P-bit Coding Violations.
dsx3CurrentLESs	-	The number of Line Errored Seconds.
dsx3CurrentCCVs	-	The number of C-bit Coding Violations.
dsx3CurrentCESs	-	The number of C-bit Errored Seconds.
dsx3CurrentCSESs	-	The number of C-bit Severely Errored Seconds.

6.2.2 Fiber Group Performance Monitoring

Note: These PM parameters are applicable only to Mediant 3000 with the TP-6310 blade.

Fiber Group Performance Monitoring

MIB Name	Gauge/Counter	Description
sonetSectionCurrentESs	Gauge	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Section in the current 15 minute interval. EMS Parameter Name: Section ESs
sonetSectionCurrentSESs	Gauge	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Section in the current 15 minute interval. EMS Parameter Name: Section SESs
sonetSectionCurrentCVs	Gauge	The counter associated with the number of Coding Violations encountered by a SONET/SDH Section in the current 15 minute interval. EMS Parameter Name: Section CVs

MIB Name	Gauge/Counter	Description
sonetLineCurrentESs	Gauge	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Line in the current 15 minute interval. EMS Parameter Name: Line ESs
sonetLineCurrentSESs	Gauge	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Line in the current 15 minute interval. EMS Parameter Name: Line SESs
sonetLineCurrentCVs	Gauge	The counter associated with the number of Coding Violations encountered by a SONET/SDH Line in the current 15 minute interval. EMS Parameter Name: Line CVs
sonetLineCurrentUASs	Gauge	The counter associated with the number of Unavailable Seconds encountered by a SONET/SDH Line in the current 15 minute interval. EMS Parameter Name: Line UASs
sonetPathCurrentESs	Gauge	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Path in the current 15 minute interval. EMS Parameter Name: Path ESs
sonetPathCurrentSESs	Gauge	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Path in the current 15 minute interval. EMS Parameter Name: Path SESs
sonetPathCurrentCVs	Gauge	The counter associated with the number of Coding Violations encountered by a SONET/SDH Path in the current 15 minute interval. EMS Parameter Name: Path CVs
sonetPathCurrentUASs	Gauge	The counter associated with the number of Unavailable Seconds encountered by a Path in the current 15 minute interval. EMS Parameter Name: Path UASs

6.2.3 System IP Performance Monitoring

System IP Performance Monitoring

MIB Name	Gauge/Counter	Description
acPMNetUtilKBytesVolumeTx	Counter	Counts the total number of outgoing Kbytes (1000 bytes) from the interface during the last interval. EMS Parameter Name: Number of Outgoing KBytes
acPMNetUtilKBytesVolumeRx	Counter	Counts the total number of Kbytes (1000 bytes) received on the interface, including those received in error, during the last interval. EMS Parameter Name: Number of Incoming KBytes

MIB Name	Gauge/Counter	Description
acPMNetUtilPacketsVolumeTx	Counter	Counts the total number of outgoing Packets from the interface during the last interval. EMS Parameter Name: Number of Outgoing Pkts
acPMNetUtilPacketsVolumeRx	Counter	Counts the total number of Packets received on the interface, including those received in error, during the last interval. EMS Parameter Name: Number of Incoming Pkts
acPMNetUtilDiscardedPacketsVal	Counter	Counts the total number of malformed IP Packets received on the interface during the last interval. These are packets which are corrupted or discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc. EMS Parameter Name: Number of Incoming Discarded Pkts
acPMNetUtilKBytesTotalTx	Gauge	This attribute counts the Current total number of outgoing Kbytes (1000 bytes) from the interface, so far from the beginning of the current collection interval as indicated by time Interval. EMS Parameter Name: Number of Outgoing KBytes
acPMNetUtilKBytesTotalRx	Gauge	This attribute counts the total number of Kbytes (1000 bytes) received on the interface, including those received in error, so far from the beginning of the current collection interval as indicated by time Interval. EMS Parameter Name: Number of Incoming KBytes
acPMNetUtilPacketsTotalTx	Gauge	This attribute counts the Current total number of outgoing Packets from the interface, so far from the beginning of the current collection interval as indicated by time Interval. EMS Parameter Name: Number of Outgoing Pkts
acPMNetUtilPacketsTotalRx	Gauge	This attribute counts the Current total number of Packets received on the interface, including those received in error, so far from the beginning of the current collection interval as indicated by time Interval. EMS Parameter Name: Number of Incoming Pkts

MIB Name	Gauge/Counter	Description
acPMNetUtilDiscardedPacketsTotal	Gauge	This attribute counts the Current total number of malformed IP Packets received on the interface from the beginning of the current collection interval. These are packets which are corrupted or discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc. EMS Parameter Name: Number of Incoming Discarded Pkts

6.2.4 VoP Call Statistics Performance Monitoring

Note: These PM parameters are not applicable to the MediaPack series.

VoP Call Statistics Performance Monitoring

MIB Name	Gauge / Counter	Description
acPMActiveContextCountAverage	Gauge	Indicates the average number of voice calls connected on the gateway since the last clear. EMS Parameter Name: Num of Active Contexts Avg
acPMActiveContextCountMin	Gauge	Indicates the minimum number of voice calls connected on the gateway since the last clear. EMS Parameter Name: Num of Active Contexts Min
acPMActiveContextCountMax	Gauge	Indicates the maximum number of voice calls connected on the gateway since the last clear. EMS Parameter Name: Num of Active Contexts Max
acPMChannelsPerCoderAverageG711	Gauge	Indicates the average number of G.711 calls present on the TPM. EMS Parameter Name: G711 Active Calls Avg
acPMChannelsPerCoderAverageG723	Gauge	Indicates the average number of G.723 calls present on the TPM. This attribute is only displayed if the G.723 Codec is provisioned on the DSP template. EMS Parameter Name: G723 Active Calls Avg
acPMChannelsPerCoderAverageG728	Gauge	Indicates the average number of G.728 calls present on the TPM. This attribute is only displayed if the G.728 Codec is provisioned on the DSP template. EMS Parameter Name: G728 Active Calls Avg

MIB Name	Gauge / Counter	Description
acPMChannelsPerCoderAverageG729a	Gauge	Indicates the average number of G.729a calls present on the TPM. This attribute is only displayed if the G.729a Codec is provisioned on the DSP. EMS Parameter Name: G729a Active Calls Avg
acPMChannelsPerCoderAverageG729e	Gauge	Indicates the average number of G.729e calls present on the TPM. This attribute is only displayed if the G.729e Codec is provisioned on the DSP template. EMS Parameter Name: G729e Active Calls Avg
acPMChannelsPerCoderAverageAMR	Gauge	Indicates the average number of AMR calls present on the TPM. This attribute is only displayed if the AMR Codec is provisioned on the DSP template. EMS Parameter Name: AMR Active Calls Avg
acPMModuleRTPPacketLossRxMax	Gauge	Indicates the Max Rx RTP Packet loss (reported by RTCP) per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Rx RTP Packet Loss Max
acPMModuleRTPPacketLossTxMax	Gauge	Indicates the Max Tx RTP Packet loss (reported by RTCP) per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Tx RTP Packet Loss Max
acPMModulePacketDelayAverage	Gauge	Indicates the average RTP packets delay per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP delay Average
acPMModulePacketDelayMax	Gauge	Indicates the maximum RTP packets delay per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP delay Max
acPMModulePacketDelayMin	Gauge	Indicates the minimum RTP packets delay per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP delay Min
acPMModulePacketJitterAverage	Gauge	Indicates the average RTP packets jitter per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP jitter Average

MIB Name	Gauge / Counter	Description
acPMModulePacketJitterMin	Gauge	Indicates the minimum RTP packets jitter per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP jitter Min
acPMModulePacketJitterMax	Gauge	Indicates the maximum RTP packets jitter per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: RTP jitter Max
acPMModuleRTPBytesRxMax	Gauge	Indicates the Max Tx RTP Bytes per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Rx RTP Bytes Max
acPMModuleRTPBytesTxMax	Gauge	Indicates the Max Rx RTP Bytes per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Tx RTP Bytes Max
acPMModuleRTPPacketsRxMax	Gauge	Indicates the Max Rx RTP Packets per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Rx RTP Packets Max
acPMModuleRTPPacketsTxMax	Gauge	Indicates the Max Tx RTP Packets per TPM, up to this point in time during the collection interval, as indicated by the time Interval. EMS Parameter Name: Tx RTP Packets Max
acPMActiveContextCountVal	Gauge	Indicates the current number of voice calls connected on the box since last clear. EMS Parameter Name: Num of Active Contexts
acPMChannelsPerCoderValG711	Gauge	This attribute indicates the current number of G711 calls present on the TPM. EMS Parameter Name: G711 Active Calls
acPMChannelsPerCoderValG723	Gauge	This attribute indicates the current number of G723 calls present on the TPM.This attribute is only displayed if the G723 Codec is provisioned on the DSP template. EMS Parameter Name: G723 Active Calls
acPMChannelsPerCoderValG728	Gauge	This attribute indicates the current number of G728 calls present on the TPM.This attribute is only displayed if the G728 Codec is provisioned on the DSP template. EMS Parameter Name: G728 Active Calls
acPMChannelsPerCoderValG729a	Gauge	This attribute indicates the current number of G729a calls present on the TPM.This attribute is only displayed if the G729a Codec is provisioned on the DSP. EMS Parameter Name: G729a Active Calls

MIB Name	Gauge / Counter	Description
acPMChannelsPerCoderValG729e	Gauge	This attribute indicates the current number of G729e calls present on the TPM.This attribute is only displayed if the G729e Codec is provisioned on the DSP template. EMS Parameter Name: G729e Active Calls
acPMChannelsPerCoderValAMR	Gauge	This attribute indicates the current number of AMR calls present on the TPM.This attribute is only displayed if the AMR Codec is provisioned on the DSP template. EMS Parameter Name: AMR Active Calls
acPMModuleRTPPacketLossRxTotal	Gauge	The total number of RTP packet loss reported by RTCP since last reset. EMS Parameter Name: Rx Packet Loss current
acPMModuleRTPPacketLossTxTotal	Gauge	The total number of RTP packet loss reported by RTCP since last reset. EMS Parameter Name: Tx Packets Loss current
acPMModuleRTPPacketsRxTotal	Gauge	The total number of packets recieved since last reset. EMS Parameter Name: Rx Packets Current
acPMModuleRTPPacketsTxTotal	Gauge	The total number of RTP packets transmited since last reset. EMS Parameter Name: Rx Packets Current

6.2.5 Common Control Performance Monitoring

Note: These PM parameters are not applicable to the MediaPack series.

Common Control Performance Monitoring

MIB Name	Gauge/Counter	Description
acPMCPConnectionLifetimeAverage	Counter	Indicates the Connection lifetime, in seconds. EMS Parameter Name: Lifetime in seconds Avg
acPMCPConnectionLifetimeMin	Counter	Indicates the Connection lifetime, in seconds. EMS Parameter Name: Lifetime in seconds Min
acPMCPConnectionLifetimeMax	Counter	Indicates the Connection lifetime, in seconds. EMS Parameter Name: Lifetime in seconds Max

MIB Name	Gauge/Counter	Description
acPMCPCommandCounterValRx	Counter	Indicates the MGC response counters. EMS Parameter Name: MGC response counters
acPMCPCommandCounterValTx	Counter	Indicates the MGC command counters. EMS Parameter Name: MGC command counters
acPMCPRetransmissionCountValRx	Counter	Counts the number of incoming retransmissions. EMS Parameter Name: MGC Rx retransmissions
acPMCPRetransmissionCountValTx	Counter	Counts the number of transactions retransmissions sent from the board. EMS Parameter Name: MGC Tx retransmissions
acPMCPCallAttemptsPerSecAverage	Counter	Average of call attempts (successful and unsuccessful) per second, during last interval. EMS Parameter Name: Call Attempts Per Sec Average
acPMCPCallAttemptsPerSecMax	Counter	Maximum of call attempts (successful and unsuccessful) per second, during last interval. EMS Parameter Name: Call Attempts Per Sec Max
acPMCPCallAttemptsPerSecMin	Counter	Minimum of call attempts (successful and unsuccessful) per second, during last interval. EMS Parameter Name: Call Attempts Per Sec Min
acPMCPConnectionLifetimeVolume	Counter	The Connection lifetime in seconds. EMS Parameter Name: Lifetime in seconds
acPMCPCommandCounterTotalTx	Gauge	MGC command counters. EMS Parameter Name: MGC Tx command counters
acPMCPCommandCounterTotalRx	Gauge	MGC response counters. EMS Parameter Name: MGC Rx command counters
acPMCPRetransmissionCountTotalTx	Gauge	Number of transactions retransmissions sent from the board. EMS Parameter Name: MGC Tx retransmissions
acPMCPRetransmissionCountTotalRx	Gauge	Number of incoming retransmissions. EMS Parameter Name: MGC Rx retransmissions
acPMCPCallAttemptsPerSecVal	Gauge	Number of Call attempts (successful and unsuccessful) per second, during current interval. EMS Parameter Name: Call Attempts Per Sec

6.2.6 SIP IP-to-Tel Performance Monitoring

Note: These PM parameters are not applicable to Mediant 4000.

SIP IP-to-Tel Performance Monitoring

MIB Name	Gauge/Counter	Description
acPMSIPAttemptedCallsVal	Counter	Indicates the number of attempted calls for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Call Attempts
acPMSIPEstablishedCallsVal	Counter	Indicates the number of established calls for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Established Calls
acPMSIPBusyCallsVal	Counter	Indicates the number of calls that failed as a result of a busy line for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Calls Terminated due to a Busy Line
acPMSIPNoAnswerCallsVal	Counter	Indicates the number of calls that weren't answered for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Calls Terminated due to No Answer
acPMSIPForwardedCallsVal	Counter	Indicates the number of calls that were terminated due to a call forward for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Calls Terminated due to Forward
acPMSIPNoRouteCallsVal	Counter	Indicates the number of calls whose destinations weren't found for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Failed Calls due to No Route
acPMSIPNoMatchCallsVal	Counter	Indicates the number of calls that failed due to mismatched media server capabilities for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Failed Calls due to No Matched Capabilities
acPMSIPNoResourcesCallsVal	Counter	Indicates the number of calls that failed due to unavailable resources or a media server lock for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Failed Calls due to No Resources

MIB Name	Gauge/Counter	Description
acPMSIPFailCallsVal	Counter	This counter is incremented as a result of calls that fail due to reasons not covered by the other counters for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Number of Failed Calls due to Other reasons
acPMSIPCallDurationAverage	Gauge	Indicates the average call duration of established calls for IP to Tel direction, during last interval. EMS Parameter Name: IP to Tel Average Call Duration [sec]
IP2TelTrunkGroupEstablishedCalls	Gauge	Indicates the current number of established calls pertaining to a Trunk Group for IP to Tel direction.
IP2TelTrunkEstablishedCalls	Gauge	Indicates the current number of established calls pertaining to a trunk for IP to Tel direction.

6.2.7 SIP Tel-to-IP Performance Monitoring

Note: These PM parameters are not applicable to Mediant 4000.

SIP Tel-to-IP Performance Monitoring

MIB Name	Gauge/Counter	Description
acPMSIPAttemptedCallsVal	Counter	Indicates the number of attempted calls for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Call Attempts
acPMSIPEstablishedCallsVal	Counter	Indicates the number of established calls for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Established Calls
acPMSIPBusyCallsVal	Counter	Indicates the number of calls that failed as a result of a busy line for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Calls Terminated due to a Busy Line
acPMSIPNoAnswerCallsVal	Counter	Indicates the number of calls that weren't answered for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Calls Terminated due to No Answer

MIB Name	Gauge/Counter	Description
acPMSIPForwardedCallsVal	Counter	Indicates the number of calls that were terminated due to a call forward for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Calls Terminated due to Forward
acPMSIPNoRouteCallsVal	Counter	Indicates the number of calls whose destinations weren't found for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Failed Calls due to No Route
acPMSIPNoMatchCallsVal	Counter	Indicates the number of calls that failed due to mismatched media server capabilities for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Failed Calls due to No Matched Capabilities
acPMSIPNoResourcesCallsVal	Counter	Indicates the number of calls that failed due to unavailable resources or a media server lock for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Failed Calls due to No Resources
acPMSIPFailCallsVal	Counter	This counter is incremented as a result of calls that fail due to reasons not covered by the other counters for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Number of Failed Calls due to Other reasons
acPMSIPCallDurationAverage	Gauge	Indicates the average call duration of established calls for Tel to IP direction, during last interval. EMS Parameter Name: Tel to IP Average Call Duration [sec]
Tel2IPTrunkEstablishedCalls	Gauge	Indicates the current number of established calls pertaining to a trunk for Tel to IP direction.
Tel2IPTrunkGroupEstablishedCalls	Gauge	Indicates the current number of established calls pertaining to a Trunk Group for Tel to IP direction.

6.2.8 Media Realms Statistics Performance Monitoring

Media Realm Statistics Performance Monitoring

MIB Name	Gauge/Counter	Description
PM_RTPRealmPacketLossRx	Gauge	RTP packet loss reported in outgoing RTCP data, per realm
PM_RTPRealmPacketLossTx	Gauge	RTP packet loss reported in incoming RTCP data, per realm

MIB Name	Gauge/Counter	Description
acPMMediaRealmBytesTx	Gauge	Media bytes received in RTCP data, per realm
acPMMediaRealmBytesRx	Gauge	Media bytes received in RTCP data, per realm
acPMMediaRealmPacketsTx	Gauge	Media packets sent in RTCP data, per realm
acPMMediaRealmPacketsRx	Gauge	Media packets received in RTCP data, per realm
acPMMediaRealmVERealmPacketDelay	Gauge	Packet delay in RTCP data, per realm
acPMMediaRealmVERealmPacketJitter	Gauge	Packet jitter in RTCP data, per realm
PM_RealmMOS	Gauge	MOS quality in RTCP-XR data, per realm
PM_MediaRealmBwRx	Gauge	Average bandwidth for Rx bytes, per realm
PM_MediaRealmBwTx	Gauge	Average bandwidth for Tx bytes, per realm
acPMMediaRealmRealmMOS	Gauge	MOS quality in RTCP-XR data, per realm
acPMMediaRealmBwRx	Gauge	Bandwidth of Rx media bytes in RTCP data, per realm.
acPMMediaRealmBwTx	Gauge	Bandwidth of Tx media bytes in RTCP data, per realm.
acPMMediaRealmPacketLossRx	Gauge	RTP bytes received in RTCP data, per realm.
acPMMediaRealmPacketLossTx	Gauge	RTP packets sent in RTCP data, per realm

6.2.9 SBC Admission Control Performance Monitoring

The device now provides SNMP performance monitoring for the SBC Admission Control feature. The performance monitoring is performed per the following:

- SRD/IP Group
- Incoming, outgoing, or both
- SIP request types - INVITE, SUBSCRIBE, OTHER, or ALL

The performance monitoring is provided by the acGateway MIB.

Note: This section is applicable only to the E-SBC series.

SBC Call Admission Control Performance Monitoring

MIB Name	Gauge / Counter	Description
acPMSIPSRDDialogsTable	Counter	Counter for all dialogs currently being handled by the SBC per SRD

MIB Name	Gauge / Counter	Description
acPMSIPSRDInviteDialogsTable	Counter	Counter of all calls (initiated by SIP:INVITE) currently being handled by the SBC per SRD
acPMSIPSRDSubscribeDialogsTable	Counter	Counter of all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per SRD
acPMSIPSRDOtherDialogsTable	Counter	Counter of all dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per SRD
acPMSIPIPGroupDialogsTable	Counter	Counter for all dialogs currently being handled by the SBC per IP Group
acPMSIPIPGroupInviteDialogsTable	Counter	Counter of all calls (initiated by SIP:INVITE) currently being handled by the SBC per IP Group
acPMSIPIPGroupSubscribeDialogsTable	Counter	Counter of all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per IP Group
acPMSIPIPGroupOtherDialogsTable	Counter	Counter of all other dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per IP Group

6.2.10 Trunk Statistics Performance Monitoring

Note: These PM parameters are applicable only to Digital PSTN devices.

Trunk Statistics Performance Monitoring

MIB Name	Gauge/Counter	Description
gwTrunkGroupUtilization	Gauge	Indicates Trunk Group utilization. It shows the number of channels that are currently in use (busy) per Trunk Group. For example, if the device has 240 channels and the threshold is set to 106, if the number of concurrent busy channels exceeds 106, this threshold alarm is sent. **Note:** If a trunk is in LOF state, this MIB counts only the channels that are used.

MIB Name	Gauge/Counter	Description
GwTrunkGroupAllTrunksBusy	Counter	Indicates the duration (in seconds) that all channels of a specific Trunk Group were concurrently busy, if this scenario occurs. For example, if Trunk Group #3 has 200 channels and all these were concurrently busy for 60 seconds, then this MIB will display 60 for this Trunk Group. **Note:** Trunks that are out of service or not configured (set to NONE) are considered "busy" in this calculation.
acPMTrunkUtilizationAverage	Gauge	Indicates the Average of simultaneously busy DS0 channels on this Trunk up to this point in time during the collection interval, as indicated by the Time Interval. A busy channel is when the Physical DS0 Termination isn't in Null context or OOS. A Trunk is either E1 or T1. EMS Parameter Name: Trunk utilization Avg
acPMTrunkUtilizationMin	Gauge	Indicates the Minimum of simultaneously busy DS0 channels on this Trunk up to this point in time during the collection interval, as indicated by the Time Interval. A busy channel is when the Physical DS0 Termination isn't in Null context or OOS. A Trunk is either E1 or T1. EMS Parameter Name: Trunk utilization Min
acPMTrunkUtilizationMax	Gauge	Indicates the Maximum of simultaneously busy DS0 channels on this Trunk up to this point in time during the collection interval, as indicated by the Time Interval. A busy channel is when the Physical DS0 Termination isn't in Null context or OOS. A Trunk is either E1 or T1. EMS Parameter Name: Trunk utilization Max
dsx1IntervalESs	Gauge	Indicates the number of Errored Seconds. EMS Parameter Name: Trunk Errored Seconds
dsx1IntervalCSSs	Gauge	Indicates the number of Controlled Slip Seconds. EMS Parameter Name: Trunk Controlled Slip Seconds
dsx1IntervalPCVs	Gauge	Indicates the number of Path Coding Violations. EMS Parameter Name: Trunk Path Coding Violations
dsx1IntervalBESs	Gauge	Indicates the number of Bursty Errored Seconds. EMS Parameter Name: Trunk Bursty Errored Seconds

MIB Name	Gauge/Counter	Description
acPMTrunkUtilizationVal	Gauge	This attribute indicates the Current simultaneous busy DS0 channels on this Trunk. A busy channel is when the Physical DS0 Termination isn't in Null context or OOS. A Trunk is either E1 or T1. EMS Parameter Name: Trunk utilization
acPMPSTNTrunkActivitySecondsTotal	Gauge	This attribute amount of call duration per timeslot and E1 since last clear. EMS Parameter Name: Trunk Calls Duration
dsx1TotalESs	Gauge	This attribute indicates amount of Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0. EMS Parameter Name: Trunk Errored Seconds
dsx1TotalCSSs	Gauge	This attribute indicates amount of Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0. EMS Parameter Name: Trunk Controlled Slip Seconds
dsx1TotalPCVs	Gauge	This attribute indicates amount of Path Coding Violations encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0. EMS Parameter Name: Trunk Path Coding Violations
dsx1TotalBESs	Gauge	This attribute indicates amount of Bursty Errored Seconds encountered by a DS1 interface in the previous 24 hour interval. Invalid 15 minute intervals count as 0. EMS Parameter Name: Trunk Bursty Errored Seconds

6.2.11 Data Networking Statistics Performance Monitoring

Note: These PM parameters are applicable only to MSBR devices.

acSysDataInterfaceStatusTable OID 1.3.6.1.4.1.5003.9.10.10.2.6.4.22. This table contains a summary of the IP status and configuration of the data interfaces. The interface types are: VLAN, loopback, sub interface, physical port, bridge, Dot11, GRE, IPIP, PPPoE, L2tp, PPTP, ATM, ATM VLAN, cellular, serial, multilink. Every entry in the table represents a data/logic interface and contains the following fields:

Data Networking Statistics Performance Monitoring Counters

MIB Name	Description
Name	Interface name
IPAddress	IPv4 address for this interface
Netmask	Netmask for this interface
Info	Status of interface can be one of the following: Unknown, Disabled, Enabled, Connected or Disconnected
Description	Description of the interface
OperationalState	Protocol is Up or Down
StateTime	State Time (hh:mm:ss)
Uptime	Uptime (hh:mm:ss)
MtuMode	Maximum Transmission Unit (MTU) on the specified interface. Can be: automatically, DHCP or value (in bytes)
DnsStatus	The primary and secondary IP addresses
RxPackets	Total packets received
RxBytes	Total bytes received
RxDropped	No space in Linux buffers
RxErrors	Bad packets received
TxPackets	Total packets transmitted
TxBytes	Total bytes transmitted
TxDropped	No space available in Linux
TxErrors	Packet transmit problem
Minutes	Determines the time interval (minutes) in which the rate sampling is done. The value is relevant to the columns MinuteInputRate and MinuteOutputRate. The value is 5 minutes.
MinuteInputRate	Average value of packets and bits transmitted (per second units) in the last *x* minutes.
MinuteOutputRate	Average value of packets and bits received (per second units) in the last *x* minutes. The output rate is exponentially weighted averages with a time of x minutes.
Seconds	Determines the time interval (seconds) in which the rate sampling is done. The value is relevant to the columns SecondInputRate and SecondOutputRate. The value is 15 seconds.
SecondInputRate	Average value of packets and bits transmitted (per second units) in the last *x* seconds.
SecondOutputRate	Average value of packets and bits received (per second units) in the last *x* seconds. The output rate is exponentially weighted averages with a time of x seconds.

7 SNMP Traps

This chapter describes the SNMP traps.

7.1 Standard Traps

The device also supports the following standard traps:

- **authenticationFailure**
- **coldStart:** The device supports a cold start trap to indicate that the device is starting up. This allows the EMS to synchronize its view of the device's active alarms. In fact, two different traps are sent at start-up:
  - **Standard coldStart trap:** iso(1).org(3).dod(6).internet(1). snmpV2(6). snmpModules(3). snmpMIB(1). snmpMIBObjects(1). snmpTraps(5). coldStart(1) sent at system initialization.
  - **Enterprise acBoardEvBoardStarted:** generated at the end of system initialization. This is more of an "application-level" cold start sent after all the initializing process is over and all the modules are ready
- **linkDown**
- **linkup**
- **entConfigChange**
- **dsx1LineStatusChange** (Applicable only to Digital PSTN devices)
- **dsx3LineStatusChange** (Applicable only to Mediant 3000)

7.2 Proprietary Traps

This subsection provides information on proprietary SNMP traps supported by the device. There is a separation between traps that are alarms and traps that are not (i.e., logs). All the traps have the same structure made up of the same 11 varbinds (Variable Binding), i.e., 1.3.6.1.4.1.5003.9.10.1.21.1. For a list of the varbinds, see "Trap Varbinds" on page 108.

The source varbind is composed of a string that details the device component from which the trap is being sent (forwarded by the hierarchy in which it resides). For example, an alarm from an SS7 link has the following string in its source varbind: acBoard#1/SS7#0/SS7Link#6.

In this example, the SS7 link number is specified as 6 and is part of the only SS7 module in the device that is placed in slot number 1 (in a chassis) and is the module to which this trap relates. For devices where there are no chassis options the slot number of the device is always 1.

Full proprietary trap definitions and trap Varbinds are found in AcBoard MIB and AcAlarm MIB.

Note: All traps are sent from the SNMP port (default 161).

7.2.1 Trap Varbinds

Each trap described above provides the following fields (known as *varbinds*). Refer to the AcBoard MIB for additional details on these varbinds.

- acBoardTrapGlobalsName
- acBoardTrapGlobalsTextualDescription
- acBoardTrapGlobalsSource
- acBoardTrapGlobalsSeverity:
    - The acSysStateGWSeverity parameter reflects the highest active alarm severity on the device. The options include the following:
        - noAlarm(0)
        - indeterminate(1)
        - warning(2)
        - minor(3)
        - major(4)
        - critical(5)
- acBoardTrapGlobalsUniqID
- acBoardTrapGlobalsType
- acBoardTrapGlobalsProbableCause
- acBoardTrapGlobalsDateAndTime
- acBoardTrapGlobalsAdditionalInfo1
- acBoardTrapGlobalsAdditionalInfo2
- acBoardTrapGlobalsAdditionalInfo3

Note: 'acBoardTrapGlobalsName' is actually a number. The value of this varbind is 'X' minus 1, where 'X' is the last number in the trap's OID. For example, the 'name' of 'acBoardEthernetLinkAlarm' is '9'. The OID for 'acBoardEthernetLinkAlarm' is 1.3.6.1.4.1.5003. 9.10.1.21.2.0.10.

7.2.2 Customizing Trap's Enterprise OID

You can change the enterprise value in the device's SNMP Traps to a variable value using the *ini* parameter SNMPTrapEnterpriseOid. This parameter replaces the Traps' OID prefix from 'AcTrap' (1.3.6.1.4.1.5003.9.10.1.21) to user-defined root. All other OIDs remain the same.

For example, the current acBoardEvBoardStarted parameter's OID is '1.3.6.1.4.1.5003.9.10.1.21.2.0.4'. Its prefix ('1.3.6.1.4.1.5003.9.10.1.21') can be changed, and all other OIDs remain the same.

7.2.3 SNMP Alarms in Syslog

All SNMP alarms are sent to the Syslog server using the following format.

- **Raised alarms:** RAISE-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >.

  If additional information exists in the alarm, then these are also added: Additional Info1:/ Additional Info2:/ Additional Info3

  The Messages' Severity is as follows:

Table 7-1: Message Severity

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
Critical	RecoverableMsg
Major	RecoverableMsg
Minor	RecoverableMsg
Warning	Notice
Indeterminate	Notice
Cleared	Notice

- **Cleared alarm:**

  CLEAR-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >; If exists Additional Info1:/ Additional Info2:/ Additional Info3:

7.2.4 Proprietary Trap Summary List

The following proprietary traps are supported by the device:

Table 7-2: Proprietary Traps

Trap	Description
acBoardFatalError	Sent whenever a fatal device error occurs.
acBoardConfigurationError	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.
acBoardTemperatureAlarm	Sent when the device exceeds its temperature limits. **Note:** Applicable only to 2000 and 3000 Series devices.
acBoardEvResettingBoard	Sent after the device resets.
acBoardEvBoardstarted	Sent after the device is successfully restored and initialized following reset.
acCertificateExpiryNotifiaction	Sent before (in days) the expiration of the installed certificate credentials, which cannot be renewed automatically.
acFeatureKeyError	Sent to relay Feature Key errors etc.

Trap	Description
acgwAdminStateChange	Sent when Graceful Shutdown commences and ends.
acBoardEthernetLinkAlarm	Sent when the Ethernet link(s) is down.
acBoardWanLinkAlarm	This alarm is raised when the WAN Link is down (and cleared when link is up again). **Note:** This alarm is applicable only to MSBR devices.
acEthernetGroupAlarm	This alarm is raised when both ports in an Ethernet port-pair group (1+1) are down, and cleared when at least one port is up. **Note:** This alarm is applicable only to Mediant 800 GW & E-SBC and Mediant 1000B GW & E-SBC.
acWirelessCellularModemAlarm	This alarm is raised when either the wireless modem is down or in backup mode, and cleared when modem is up. **Note:** This alarm is applicable only to Mediant 800 MSBR.
acActiveAlarmTableOverflow	Sent when an active alarm cannot be entered into the Active Alarm table because the table is full.
acAudioProvisioningAlarm	Sent if the device is unable to provision its audio. **Note:** Not applicable to MSBR.
acOperationalStateChange	Sent if the operational state of the node goes to disabled; cleared when the operational state of the node goes to enabled.
acNATTraversalAlarm	Sent when the NAT is placed in front of a device and is identified as a symmetric NAT. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one. **Note:** Not applicable to MSBR.
acEnhancedBITStatus	Sent for the status of the BIT (Built In Test). The information in the trap contains blade hardware elements being tested and their status. The information is presented in the additional info fields. **Note:** Not applicable to MSBR.
acTMInconsistentRemoteAndLocalPLLStatus	Inconsistent Remote and Local PLL status. **Note:** Applicable only to Mediant 3000.
acTMReferenceStatus	Timing manager reference status. **Note:** Applicable only to Mediant 3000.
acTMReferenceChange	Timing manager reference change. **Note:** Applicable only to Mediant 3000.
acFanTrayAlarm	Sent when a fault occurs in the fan tray or a fan tray is missing. **Note:** Applicable only to Mediant 1000 and 3000 Series devices.
acPowerSupplyAlarm	Sent when a fault occurs in one of the power supply (PS) modules or a PS module is missing. **Note:** Applicable only to the Mediant 1000 Series and Mediant 3000 devices.
acPEMAlarm	Sent when a fault occurs in one of the PEM modules or a PEM module is missing. **Note:** Applicable only to the 3000 Series devices.

Trap	Description
acSAMissingAlarm	Sent when the SA module is missing or non operational. **Note:** Applicable only to the 3000 Series devices.
acUserInputAlarm	Sent when the input dry contact is short circuited; cleared when the circuit is reopened. **Note:** Applicable only to the 3000 Series devices.
acPerformanceMonitoringThresholdCrossing	Sent every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.
acNTPServerStatusAlarm	NTP server status alarm. Raised when the connection to the NTP server is lost. Cleared when the connection is reestablished. Unset time (as a result of no connection to NTP server) may result with functionality degradation and failure in device.
acDChannelStatus	Non-alarm trap sent at the establishment, re-establishment or release of LAPD link with its peer connection occurs. The trap is sent with one of the following textual descriptions: ▪ D-channel synchronized ▪ D-channel not-synchronized **Note:** Applicable only to the Digital PSTN devices.
acHTTPDownloadResult	Sent upon success or failure of the HTTP Download action.
acKeepAlive	Part of the NAT traversal mechanism. If the STUN application in the device detects a NAT, this trap is sent on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the device.
acPowerOverEthernetStatus	This trap is sent when Power over Ethernet (PoE) for a specific port is disabled.
acMediaProcessOverloadAlarm	This alarm is raised upon overload of the device’s media processing and interfaces.
acIDSThresholdCrossNotification	This trap is sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
SIP Traps	
acBoardCallResourcesAlarm	Sent when no free channels are available.
acBoardControllerFailureAlarm	▪ Sent when the Proxy is not found or registration fails. Internal routing table may be used for routing. ▪ Sent when the physical network link is up or down ("BusyOut Trunk/Line n Link failure"). ▪ GWAPP_TRAP_BUSYOUT_CONNECTIVITY: Sent when the connection to the Proxy is up or down ("BusyOut Trunk/Line n Connectivity Proxy failure"). ▪ GWAPP_TRAP_BUSYOUT_TDM_OVER_IP: Sent when a failure occurs in TDM over IP (transparent T1/E1 without signaling) - "BusyOut Trunk n TDM over IP failure (Active calls x Min y)". (**Note:** Applicable only to Digital PSTN devices.)

Trap	Description
	▪ GWAPP_TRAP_BUSYOUT_PROXY_SET: Sent when the connection to the Proxy Set associated with this trunk/line is up/down ("BusyOut Trunk/Line n Proxy Set Failure"). ▪ GWAPP_TRAP_BUSYOUT_REGISTRATION: Sent when a failure occurs in server registration for this trunk/line ("BusyOut Trunk/Line n Registration Failure"). ▪ GWAPP_TRAP_BUSYOUT_SERVING_IPGROUP: Sent when a failure occurs in a Serving IP Group for this trunk ("BusyOut Trunk n Serving IP Group Failure"). (**Note:** Applicable only to Digital PSTN devices.) ▪ GWAPP_TRAP_PROXY_SET: Sent when a failure occurs in a Proxy Set (not per trunk/line, but per Proxy Set) - "Proxy Set ID n".
acProxyConnectionLost	Sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.
acBoardOverloadAlarm	Sent when there is an overload in one or some of the system's components.
acGWSASEmergencyModeAlarm	Sent by the Stand-Alone Survivability (SAS) application when switching from “Normal" mode to “Emergency" mode. This alarm is cleared once the SAS returns to “Normal" mode. **Note:** Applicable only to MediaPack, Mediant 800, Mediant 1000, and Mediant 2000.
High Availability Traps **Note:** Applicable only to Mediant 3000 HA what about M4K and SW E-SBC.	
acHASystemFaultAlarm	Sent when the High Availability (HA) system is faulty (i.e., no HA functionality).
acHASystemConfigMismatchAlarm	Sent when the configuration of the modules in the HA system is not identical, causing instability.
acHASystemSwitchOverAlarm	Sent when a switchover from the active to the redundant module has occurred.
acSWUpgradeAlarm	Sent for SW upgrade process errors.
PSTN - SONET Traps **Note:** Applicable only to Mediant 3000 with TP-6310.	
acSonetSectionLOFAlarm	SONET section Loss of Frame alarm.
acSonetSectionLOSAlarm	SONET section Loss of Signal alarm.
acSonetLineAISAlarm	SONET Line AIS alarm.
acSonetLineRDIAlarm	SONET Line RDI alarm.

7.2.5 Alarms

The tables in the following subsections provide information on alarms that are raised as a result of a generated SNMP trap. The component name (described in each of the following headings) refers to the string that is provided in the acBoardTrapGlobalsSource trap varbind. To clear a generated alarm, the same notification type is sent but with the severity set to 'cleared'.

7.2.5.1 Chassis Alarms

7.2.5.1.1 Fan Tray Alarm

Note: Applicable only to Mediant 3000 and Mediant 1000.

Table 7-3: acFanTrayAlarm (Applicable Only to 3000 Series and Mediant 1000)

Alarm:	acFanTrayAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.29
Default Severity:	Critical
Source Varbind Text	Chassis#0/FanTray#0
Event Type:	equipmentAlarm
Probable Cause:	heatingVentCoolingSystemProblem
Alarm Text:	Fan-Tray Alarm
Status Changes:	
1. Condition:	Fan-Tray is missing
Alarm Status:	Critical
<text> Value:	Fan-Tray Alarm. Fan-Tray is missing
2. Condition:	One or more fans in the Fan-Tray are faulty.
Alarm Status:	Major
Corrective Action:	Fan is faulty
3. Condition:	Fan tray is in place and fans are working.
Alarm Status:	Cleared

7.2.5.1.2 Power Supply Alarm

Note: Applicable only to Mediant 3000 and Mediant 1000.

Table 7-4: acPowerSupplyAlarm

Alarm:	acPowerSupplyAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.30
Default Severity:	Critical
Source Varbind Text	Chassis#0/PowerSupply#<m>, where *m* is the power supply's slot number
Event Type:	equipmentAlarm
Probable Cause:	powerProblem
Alarm Text:	Power-Supply Alarm. Power-Supply is missing.
Status Changes:	
1. Condition:	The HA (High Availability) feature is active (applicable only to Mediant 3000) and one of the power supply units is faulty or missing.
Alarm Status:	Major
2. Condition:	PS unit is placed and working.
Alarm Status:	Cleared

7.2.5.1.3 User Input Alarm

Note: Applicable only to Mediant 3000, Mediant 1000, and Mediant 600.

Table 7-5: acUserInputAlarm

Alarm:	acUserInputAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.36
Default Severity:	Critical
Source Varbind Text	Chassis#0
Event Type:	equipmentAlarm
Probable Cause:	inputDeviceError
Alarm Text:	User input Alarm. User's Input-Alarm turn on.
Status Changes:	
1. Condition:	Input dry contact is short circuited.
Alarm Status:	Critical
2. Condition:	Input dry contact circuit is reopened.
Alarm Status:	Cleared

7.2.5.1.4 PEM Alarm

Note: Applicable only to Mediant 3000.

Table 7-6: acPEMAlarm

Alarm:	acPEMAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.31
Default Severity:	Critical
Source Varbind Text	hassis#0/PemCard#<m>, where *m* is the power entry module's (PEM) slot number
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	PEM Module Alarm.
Status Changes:	
1. Condition:	The HA (High Availability) feature is active (applicable only to Mediant 3000) and one of the PEM units is missing (PEM – Power Entry Module)
Alarm status:	Critical
<text> Value:	PEM card is missing.
2. Condition:	PEM card is placed and both DC wires are in.
Alarm Status:	Cleared

7.2.5.1.5 Hardware Failure Alarm

Note: Applicable only to Mediant 1000.

Table 7-7: acHwFailureAlarm

Alarm:	acHwFailureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.43
Default Severity:	Critical
Source Varbind Text	Chassis#0/module#<m>, where *m* is the module's number
Event Type:	equipmentAlarm
Probable Cause:	equipmentMalfunction
Alarm Text:	Module Alarm: <text>
Status Changes:	
1. Condition:	The module is faulty or has been removed incorrectly.
Alarm Status:	Critical
<text> Value:	Faulty IF-Module
Note:	This alarm is not cleared. The device must be restarted to clear this alarm.
2. Condition:	Module mismatch - module and CPU board mismatch.
Alarm Status:	Major
<text> Value:	IF-Module Mismatch
Note:	This alarm is not cleared. The device must be restarted to clear this alarm.

7.2.5.2 Timing Module Alarms

Note: These alarms are applicable only to Mediant 3000.

7.2.5.2.1 TM Inconsistent Remote and Local PLL Status Alarm

Table 7-8: acTMInconsistentRemoteAndLocalPLLStatus Alarm

Alarm:	acTMInconsistentRemoteAndLocalPLLStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.56
Default Severity:	Major
Source Varbind Text	Chassis#0/TimingManager#0
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	Timing Manager Alarm <text>
1. Condition:	The alarm is triggered when the system is in 1+1 status and redundant board PLL status is deferent than active board PLL status
Alarm Status:	Major
<text> Value:	Timing Manager Alarm. Local and Remote PLLs status is different.
2. Condition:	
Alarm Status:	Status remains major until a reboot. A clear trap is not sent.
Corrective Action:	Synchronize the timing module.

7.2.5.2.2 TM Reference Status Alarm

Table 7-9: acTMReferenceStatus Alarm

Alarm:	acTMReferenceStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.57
Default Severity:	Major
Source Varbind Text	Chassis#0/TimingManager#0
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	Timing Manager Alarm <text>
Status Changes:	While primary and secondary clock references are down for more than 24 hours, the alarm will be escalated to critical.
1. Condition:	The alarm is triggered when the primary reference or secondary reference or both are down.
Alarm Status:	Major
<text> Value:	Timing Manager Alarm. PRIMARY REFERENCE DOWN/SECONDARY REFERENCE DOWN/ALL REFERENCES ARE DOWN
2. Condition:	
Alarm Status:	Status remains major until a reboot. A clear trap is not sent.
Corrective Action:	Synchronize the timing module.

7.2.5.2.3 TM Reference Change Alarm

Table 7-10: acTMReferenceChange Alarm

Alarm:	acTMReferenceChange
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.58
Default Severity:	Indeterminate
Source Varbind Text	Chassis#0/TimingManager#0
Event Type:	
Probable Cause:	
Alarm Text:	Timing Manager
Status Changes:	
1. Condition:	Log is sent on PLL status change.

7.2.5.3 Trunk Alarms

Note: Applicable only to Digital PSTN devices.

7.2.5.3.1 Trunk Near-End LOS Alarm

Table 7-11: acTrunksAlarmNearEndLOS

Alarm:	acTrunksAlarmNearEndLOS
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.49
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	lossOfSignal
Alarm Text:	Trunk LOS Alarm.
Status Changes:	
Condition:	Near-end LOS
Alarm Status:	Critical
Condition:	End of LOS
Alarm Status:	Cleared
Corrective Action:	Ensure the trunk is properly connected.

7.2.5.3.2 Trunk Near-End LOF Alarm

Table 7-12: acTrunksAlarmNearEndLOF

Alarm:	acTrunksAlarmNearEndLOF
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.50
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	lossOfFrame
Alarm Text:	Trunk LOF Alarm.
Status Changes:	
Condition:	Near end LOF
Alarm Status:	Critical
Condition:	End of LOF
Alarm Status:	Cleared
Corrective Action:	Ensure the trunk is connected to a proper follow up device. Ensure correct clocking setup.

7.2.5.3.3 Trunk AIS Alarm

Table 7-13: acTrunksAlarmRcvAIS

Alarm:	acTrunksAlarmRcvAIS
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.51
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	Trunk AIS Alarm
Status Changes:	
Condition:	Receive AIS
Alarm Status:	Critical
Condition:	End of AIS
Alarm Status:	Cleared
Corrective Action:	None

7.2.5.3.4 Trunk Fare-End LOF Alarm

Table 7-14: acTrunksAlarmFarEndLOF

Alarm:	acTrunksAlarmFarEndLOF
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.52
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm

Probable Cause:	transmitFailure
Alarm Text:	Trunk RAI Alarm.
Status Changes:	
Condition:	RAI
Alarm Status:	Critical
Condition:	End of RAI
Alarm Status:	Cleared
Corrective Action:	Ensure correct transmission.

7.2.5.3.5 DS1 Line Status Alarm

Table 7-15: dsx1LineStatusChange

Alarm:	dsx1LineStatusChange
OID:	1.3.6.1.2.1.10.18.15.0.1
Default Severity:	Major on raise; Clear on clear
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	
Alarm Text:	DS1 Line Status
Status Changes:	
Additional Info1,2,3:	Updated DS1 Line Status. This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information. The dsx1LineStatus is a bit map represented as a sum, therefore, it can represent multiple failures (alarms) and a LoopbackState simultaneously. dsx1NoAlarm must be set if and only if no other flag is set. If the dsx1loopbackState bit is set, the loopback in effect can be determined from the dsx1loopbackConfig object. The various bit positions are: 1 dsx1NoAlarm No alarm present 2 dsx1RcvFarEndLOF Far end LOF (a.k.a., Yellow Alarm) 4 dsx1XmtFarEndLOF Near end sending LOF Indication 8 dsx1RcvAIS Far end sending AIS 16 dsx1XmtAIS Near end sending AIS 32 dsx1LossOfFrame Near end LOF (a.k.a., Red Alarm) 64 dsx1LossOfSignal Near end Loss Of Signal 128 dsx1LoopbackState Near end is looped 256 dsx1T16AIS E1 TS16 AIS 512 dsx1RcvFarEndLOMF Far End Sending TS16 LOMF 1024 dsx1XmtFarEndLOMF Near End Sending TS16 LOMF 2048 dsx1RcvTestCode Near End detects a test code 4096 dsx1OtherFailure Any line status not defined here 8192 dsx1UnavailSigState Near End in Unavailable Signal State 16384 dsx1NetEquipOOS Carrier Equipment Out of Service 32768 dsx1RcvPayloadAIS DS2 Payload AIS 65536 dsx1Ds2PerfThreshold DS2 Performance Threshold Exceeded

7.2.5.3.6 B-Channel Alarm

Table 7-16: acBChannelAlarm

Alarm:	acBChannelAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.85
Default Severity:	Minor
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	degradedSignal
Alarm Text:	B-Channel Alarm. %s
Status Changes:	
Condition:	Raised when B-channel service state changes to out of service or maintenance
Alarm Status:	Major
Text <value>:	%s – additional information
Condition:	B-channel status changes to In Service
Alarm Status:	Clear
Corrective Action:	

7.2.5.3.7 NFAS Group Alarm

Table 7-17: acNFASGroupAlarm

Alarm:	acNFASGroupAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.84
Default Severity:	Major
Source Varbind Text	Interfaces#0/Trunk#<m>, where *m* is the trunk interface number, 1 being the first trunk
Event Type:	communicationsAlarm
Probable Cause:	degradedSignal
Alarm Text:	NFAS Group Alarm. %s
Status Changes:	
Condition:	Raised when an NFAS group goes out-of-service
Alarm Status:	Major
text <value>:	%s– Additional information
Condition:	NFAS group state goes to in service
Alarm Status:	Clear
Corrective Action:	

7.2.5.4 SONET Alarms

⚠ **Note:** These alarms are applicable only to Mediant 3000 with TP-6310 blade.

The source varbind text for the alarms under this component is Interfaces#0/Sonet#<m>, where *m* is the SONET interface number.

7.2.5.4.1 SONET Section LOF Alarm

Table 7-18: AcSonetSectionLOFAlarm

Alarm:	acSonetSectionLOFAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.38
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	lossOfFrame
Alarm Text:	SONET-Section LOF.
Status Changes:	
1. Condition:	LOF condition is present on SONET no.n
Alarm Status:	Critical
<text> Value:	LOF
Note:	The sonetSectionCurrentStatus field in the sonetSectionCurrentTable will have a value sonetSectionLOF (4).
2. Condition:	LOF condition is not present.
Alarm Status:	Cleared

7.2.5.4.2 SONET Section LOS Alarm

Table 7-19: AcSonetSectionLOSAlarm

Alarm:	acSonetSectionLOSAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.39
Default Severity:	critical
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	lossOfSignal
Alarm Text:	SONET-Section LOS.
Status Changes:	
1. Condition:	LOS condition is present on SONET no #n
Alarm Status:	Critical
<text> Value:	LOS
Note:	The sonetSectionCurrentStatus field in the sonetSectionCurrentTable will have a value sonetSectionLOS (2).
2. Condition:	AIS condition is present (LOS condition is not present)
Alarm Status:	Critical
3. Condition:	LOS condition is not present.
Alarm Status:	Cleared

7.2.5.4.3 SONET Section AIS Alarm

Table 7-20: AcSonetLineAISAlarm

Alarm:	acSonetLineAISAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.40
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	SONET-Line AIS.
Status Changes:	
1. Condition:	AIS condition is present on SONET-Line #n.
Alarm Status:	Critical
<text> Value:	AIS
Note:	The sonetLineCurrentStatus field in the sonetLineCurrentTable will have a value sonetLineAIS (2).
2. Condition:	AIS condition is not present.
Alarm Status:	Cleared

7.2.5.4.4 SONET Line RDI Alarm

Table 7-21: AcSonetLineRDIAlarm

Alarm:	acSonetLineRDIAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.41
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Sonet#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	transmitFailure
Alarm Text:	SONET-Line RDI.
Status Changes:	
1. Condition:	RDI condition is present on SONET-Line #n.
Alarm Status:	Critical
<text> Value:	RDI
Note:	The sonetLineCurrentStatus field in the sonetLineCurrentTable will have a value sonetLineRDI (4).
2. Condition:	RDI condition is not present.
Alarm Status:	Cleared

7.2.5.4.5 SONET Path STS LOP Alarm

Table 7-22: acSonetPathSTSLOPAlarm

Alarm:	acSonetPathSTSLOPAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.61
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	SONET Path STS AIS alarm.
Status Changes:	
1. Condition:	LOP condition is present on Path #n.
Alarm Status:	Critical
<text> Value:	LOP
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSLOP (2).
2. Condition:	LOP condition is not present.
Alarm Status:	Cleared

7.2.5.4.6 SONET Path STS AIS Alarm

Table 7-23: acSonetPathSTSAISAlarm

Alarm:	acSonetPathSTSAISAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.62
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	SONET Path STS AIS alarm.
Status Changes:	
1. Condition:	AIS condition is present on Path #n.
Alarm Status:	Critical
<text> Value:	AIS
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSAIS(4).
2. Condition:	AIS condition is not present.
Alarm Status:	Cleared

7.2.5.4.7 SONET Path STS RDI Alarm

Table 7-24: acSonetPathSTSRDIAlarm

Alarm:	acSonetPathSTSRDIAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.63
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	transmitFailure
Alarm Text:	SONET Path STS RDI alarm.
Status Changes:	
1. Condition:	RDI condition is present on Path #n.
Alarm Status:	Critical
<text> Value:	RDI
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSTSRDI(8).
2. Condition:	RDI condition is not present.
Alarm Status:	Cleared

7.2.5.4.8 SONET Path Unequipped Alarm

Table 7-25: acSonetPathUnequippedAlarm

Alarm:	acSonetPathUnequippedAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.64
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	SONET Path Unequipped alarm.
Status Changes:	
1. Condition:	Unequipped condition is present on Path #n.
Alarm Status:	Critical
<text> Value:	Unequipped
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathUnequipped(16).
2. Condition:	Unequipped condition is not present.
Alarm Status:	Cleared

7.2.5.4.9 SONET Path Signal Label Mismatch Alarm

Table 7-26: acSonetPathSignalLabelMismatchAlarm

Alarm:	acSonetPathSignalLabelMismatchAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.65
Default Severity:	Critical
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	SONET Path Signal Label Mismatch alarm.
Status Changes:	
1. Condition:	Signal Label Mismatch condition is present on Path #n.
Alarm Status:	Critical
<text> Value:	SignalLabelMismatch
Note:	The sonetPathCurrentStatus in the sonetPathCurrentTable has a value of sonetPathSignalLabelMismatch(32).
2. Condition:	Signal Label Mismatch condition is not present.
Alarm Status:	Cleared

7.2.5.4.10 SONET Hardware Failure Alarm

Table 7-27: acSonetIfHwFailureAlarm

Alarm:	acSonetIfHwFailureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.42
Default Severity:	Critical on raise; Clear on clear
Source Varbind Text	Interfaces#0/Path#<m>, where *m* is the SONET interface number
Event Type:	communicationsAlarm
Probable Cause:	Transmit failure
Alarm Text:	SONET/SDH interface Failure Alarm

7.2.5.5 DS3 Alarms

Note: These alarms are applicable only to Mediant 3000 with TP-6310 blade.

7.2.5.5.1 DS3 RAI Alarm

Table 7-28: acDS3RAIAlarm

Alarm:	acDS3RAIAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.66
Default Severity:	Critical
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type:	communicationsAlarm
Probable Cause:	transmitFailure
Alarm Text:	DS3 RAI alarm.
Status Changes:	
1. Condition:	RAI condition is present on DS3-Line #n.
Alarm Status:	Critical
<text> Value:	RAI
Note:	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3RcvRAIFailure(2).
2. Condition:	RIA condition is not present.
Alarm Status:	Cleared

7.2.5.5.2 DS3 AIS Alarm

Table 7-29: acDS3AISAlarm

Alarm:	acDS3AISAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.67
Default Severity:	Critical
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type:	communicationsAlarm
Probable Cause:	receiveFailure
Alarm Text:	DS3 AIS alarm.
Status Changes:	
1. Condition:	AIS condition is present on DS3-Line #n.
Alarm Status:	Critical
<text> Value:	AIS
Note:	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3RcvAIS(8).
2. Condition:	AIS condition is not present.
Alarm Status:	Cleared

7.2.5.5.3 DS3 LOF Alarm

Table 7-30: acDS3LOFAlarm

Alarm:	acDS3LOFAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.68
Default Severity:	Critical
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type:	communicationsAlarm
Probable Cause:	lossOfFrame
Alarm Text:	DS3 LOF alarm.
Status Changes:	
1. Condition:	LOF condition is present on DS3-Line #n.
Alarm Status:	Critical
<text> Value:	LOF
Note:	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3LOF (32).
2. Condition:	LOF condition is not present.
Alarm Status:	Cleared

7.2.5.5.4 DS3 LOS Alarm

Table 7-31: acDS3LOSAlarm

Alarm:	acDS3LOSAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.69
Default Severity:	Critical
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type:	communicationsAlarm
Probable Cause:	lossOfSignal
Alarm Text:	DS3 LOS alarm.
Status Changes:	
1. Condition:	LOS condition is present on DS3-Line #n.
Alarm Status:	Critical
<text> Value:	LOS
Note:	The dsx3LineStatusfield in the dsx3ConfigTablewill have a value dsx3LOS (64).
2. Condition:	LOS condition is not present.
Alarm Status:	Cleared

7.2.5.5.5 DS3 Line Status Change Alarm

Table 7-32: dsx3LineStatusChangeTrap

Alarm:	dsx3LineStatusChange
OID:	1.3.6.1.2.1.10.30.15.0.1
Default Severity:	Major on raise; Clear on clear
Source Varbind Text	Interfaces#0/DS3#<m>, where *m* is the DS3 interface number.
Event Type:	communicationsAlarm
Probable Cause:	A dsx3LineStatusChange trap is sent when the value of an instance of dsx3LineStatus changes. It can be utilized by an NMS to trigger polls. When the line status change results in a lower level line status change (i.e., ds1), then no traps for the lower level are sent.
Alarm Text:	DS3 Line Status
Additional Info1,2,3:	Updated DS3 Line Status. This variable indicates the Line Status of the interface. It contains loopback state information and failure state information. The dsx3LineStatus is a bit map represented as a sum, therefore it can represent multiple failures and a loopback (see dsx3LoopbackConfig object for the type of loopback) simultaneously. The dsx3NoAlarm must be set if and only if no other flag is set. If the dsx3loopbackState bit is set, the loopback in effect can be determined from the dsx3loopbackConfig object. The various bit positions are: 1 dsx3NoAlarm No alarm present 2 dsx3RcvRAIFailure Receiving Yellow/Remote Alarm Indication 4 dsx3XmitRAIAlarm Transmitting Yellow/Remote Alarm Indication 8 dsx3RcvAIS Receiving AIS failure state 16 dsx3XmitAIS Transmitting AIS 32 dsx3LOF Receiving LOF failure state 64 dsx3LOS Receiving LOS failure state 128 dsx3LoopbackState Looping the received signal 256 dsx3RcvTestCode Receiving a Test Pattern 512 dsx3OtherFailure Any line status not defined here 1024 dsx3UnavailSigState Near End in Unavailable Signal State 2048 dsx3NetEquipOOS Carrier Equipment Out of Service

7.2.5.6 Hitless Software Upgrade Alarm

Note: This alarm is applicable only to Mediant 3000.

Table 7-33: acHitlessUpdateStatus

Alarm:	acHitlessUpdateStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.48
Default Severity:	-
Event Type:	Other
Probable Cause:	Other
Alarm Text:	Hitless Update Event
Status Changes:	
Condition:	A Notification trap that is sent out at the beginning and the end of a Hitless SW update. Failure during the process will also instigate the trap. May include the following information: Hitless: start SW upgrade. Hitless: Stream read error, aborting CMP file processing. Hitless: Invalid cmp file - missing Ver parameter. Hitless fail: Hitless SW upgrade is not supported under version 5.2. Hitless fail: SW ver stream name too long. Hitless fail: Invalid cmp file - missing UPG parameter. Hitless fail: Hitless SW upgrade not supported. Hitless fail: Communication with redundant module failed. Hitless: SW upgrade ended successfully.
Alarm Status:	Indeterminate
Corrective Action:	

7.2.5.7 High Availability Alarms

Note: These alarms are applicable only to Mediant 3000 HA.

7.2.5.7.1 HA System Fault Alarm

Table 7-34: acHASystemFaultAlarm

Trap:	acHASystemFaultAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.33
Default Severity:	critical
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number
Event Type:	qualityOfServiceAlarm
Probable Cause:	outOfService
Trap Text:	No HA! <text>
Status Changes:	
1. Condition:	HA feature is active but the system is not working in HA mode.
Trap Status:	Critical
<text> Value:	There are many possible values for the text: Fatal exception error TCPIP exception error Network processor exception error SW WD exception error HW WD exception error SAT device is missing SAT device error DSP error BIT tests error PSTN stack error Keep Alive error Software upgrade Manual switch over Manual reset Board removal Can't read slot number TER misplaced HW fault. TER in slot 2 or 3 is missing HW fault. TER has old version or is not functional HW fault. invalid TER Type HW fault. invalid TER active/redundant state HW fault. Error reading GbE state Redundant module is missing Unable to sync SW versions Redundant is not connecting Redundant is not reconnecting after deliberate restart No Ethernet Link in redundant module SA module faulty or missing
2. Condition:	HA feature is active and the redundant module is in start up mode and hasn't connected yet.
Trap Status:	Minor
<text> Value:	Waiting for redundant to connect
3. Condition:	HA system is active.
Trap Status:	Cleared

7.2.5.7.2 HA System Configuration Mismatch Alarm

Table 7-35: acHASystemConfigMismatchAlarm

Trap:	acHASystemConfigMismatchAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.34
Default Severity:	major
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number
Event Type:	processingErrorAlarm
Probable Cause:	configurationOrCustomizationError
Trap Text:	Configuration mismatch in the system.
Status Changes:	
1. Condition:	HA feature is active: ▪ License Keys of Active and Redundant modules are different. ▪ The Active module was unable to pass on to the Redundant module the License Key. ▪ License key of the Redundant module is invalid.
Trap Status:	Major
<text> Value:	▪ Active and Redundant modules have different feature keys. ▪ Fail to update the redundant with feature key. ▪ Feature key did not update in redundant module.
2. Condition:	Successful License Key update.
Trap Status:	Cleared
<text> Value:	The feature key was successfully updated in the redundant module

7.2.5.7.3 HA System Switch Over Alarm

Table 7-36: acHASystemSwitchOverAlarm

Trap:	acHASystemSwitchOverAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.35
Default Severity:	Critical
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number
Event Type:	qualityOfServiceAlarm
Probable Cause:	outOfService
Trap Text:	Switch-over: <text>
Status Changes:	
1. Condition:	A switch over from the active to the redundant blade has occurred.
Trap Status:	Critical
<text> Value:	See the acHASystemFaultAlarm table above.
2. Condition:	10 seconds have passed since the switch over.
Trap Status:	cleared

7.2.5.7.4 Ethernet Link Alarm

Table 7-37: acBoardEthernetLinkAlarm

Trap:	acBoardEthernetLinkAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Default Severity:	Critical
Source Varbind Text	Chassis#0/Module#<m>/EthernetLink#0, where *m* is the blade's slot number
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Trap Text:	Ethernet link alarm: <text>
Status Changes:	
1. Condition:	Fault on single interface of the Active module.
Trap Status:	Major
<text> Value:	Redundant link (physical link n) is down
2. Condition:	Fault on both interfaces
Trap Status:	Critical
<text> Value:	No Ethernet link
3. Condition:	Fault on single interface of the Redundant module.
Trap Status:	Major
<text> Value:	Redundant link in the redundant module (physical link n) is down
4. Condition:	Both interfaces are operational
Trap Status:	Cleared
Corrective Action:	Ensure that both Ethernet cables are plugged into the back of the system. Inspect the system's Ethernet link lights to determine which interface is failing. Reconnect the cable or fix the network problem
Note:	The alarm behaves differently when coming from the redundant or the active modules of an HA system. The alarm from the redundant is raised when there is an operational HA configuration in the system. There is no critical severity for the redundant module losing both its Ethernet links as that is conveyed in the no HA alarm that follows such a case.

7.2.5.8 Device (Board) Alarms

The source varbind text for all the alarms under this component depends on the device:

- 3000 Series: **Board#0<n>**
- All other devices: **System#0<n>**

Where *n* is the slot number in which the blade resides in the chassis. For Mediant 1000 and MediaPack, *n* always equals to 1.

7.2.5.8.1 Fatal Error Alarm

Table 7-38: acBoardFatalError

Alarm:	acBoardFatalError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Default Severity:	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Board Fatal Error: <text>
Status Changes:	
1. Condition:	Any fatal error
Alarm Status:	Critical
<text> Value:	A run-time specific string describing the fatal error
2. Condition:	After fatal error
Alarm Status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	Capture the alarm information and the Syslog clause, if active. Contact your first-level support group. The support group will likely want to collect additional data from the device and perform a reset.

7.2.5.8.2 Configuration Error Alarm

Table 7-39: acBoardConfigurationError

Alarm:	acBoardConfigurationError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.2
Default Severity:	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Board Config Error: <text>
Status Changes:	
1. Condition:	A configuration error was detected
Alarm Status:	critical
<text> Value:	A run-time specific string describing the configuration error.
2. Condition:	After configuration error
Alarm Status:	Status stays critical until reboot. A clear trap is not sent.

Alarm:	acBoardConfigurationError
Corrective Action:	Inspect the run-time specific string to determine the nature of the configuration error. Fix the configuration error using the appropriate tool: Web interface, EMS, or *ini* file. Save the configuration and if necessary reset the device.

7.2.5.8.3 Temperature Alarm

Table 7-40: acBoardTemperatureAlarm

Alarm:	acBoardTemperatureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.3
Default Severity:	Critical
Event Type:	equipmentAlarm
Probable Cause:	temperatureUnacceptable (50)
Alarm Text:	Board temperature too high
Status Changes:	
1. Condition:	Temperature is above 60°C (140°F)
Alarm Status:	Critical
2. Condition:	After raise, temperature falls below 55°C (131°F)
Alarm Status:	Cleared
Corrective Action:	Inspect the system. Determine if all fans in the system are properly operating.

7.2.5.8.4 Software Reset Alarm

Table 7-41: acBoardEvResettingBoard

Alarm:	acBoardEvResettingBoard
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.5
Default Severity:	Critical
Event Type:	equipmentAlarm
Probable Cause:	outOfService (71)
Alarm Text:	User resetting board
Status Changes:	
1. Condition:	When a soft reset is triggered via the Web interface or SNMP.
Alarm Status:	Critical
2. Condition:	After raise
Alarm Status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	A network administrator has taken action to reset the device. No corrective action is required.

7.2.5.8.5 Software Upgrade Alarm

Table 7-42: acSWUpgradeAlarm

Alarm:	acSWUpgradeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.70
Default Severity:	Major
Alarms Source:	System#0
Event Type:	processingErrorAlarm
Probable Cause:	softwareProgramError
Alarm Text:	SW upgrade error. <text>
Note:	
Condition:	Raised upon software upgrade errors.
Alarm Status:	major
<text> value:	Firmware burning failed. Startup system from Bootp/tftp.
Corrective Action:	Start up system from BootP/TFTP.

7.2.5.8.6 Call Resources Alarm

Table 7-43: acBoardCallResourcesAlarm

Alarm:	acBoardCallResourcesAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.8
Default Severity:	Major
Event Type:	processingErrorAlarm
Probable Cause:	softwareError (46)
Alarm Text:	Call resources alarm
Status Changes:	
1. Condition:	Percentage of busy channels exceeds the predefined RAI high threshold.
Alarm Status:	Major
Note:	To enable this alarm the RAI mechanism must be activated (EnableRAI = 1).
2. Condition:	Percentage of busy channels falls below the predefined RAI low threshold.
Alarm Status:	Cleared

7.2.5.8.7 Controller Failure Alarm

Table 7-44: acBoardControllerFailureAlarm

Alarm:	acBoardControllerFailureAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.9
Default Severity:	Major
Event Type:	processingErrorAlarm
Probable Cause:	softwareError (46)
Alarm Text:	Controller failure alarm
Status Changes:	
1. Condition:	Proxy has not been found or physical network link is up or down ("BusyOut Trunk/Line n Link failure").
Alarm Status:	Major
Additional Info:	Proxy not found. Use internal routing or Proxy lost. looking for another Proxy
2. Condition:	Proxy is found. The clear message includes the IP address of this Proxy.
Alarm Status:	Cleared

7.2.5.8.8 Board Overload Alarm

Table 7-45: acBoardOverloadAlarm

Alarm:	acBoardOverloadAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.11
Default Severity:	Major
Event Type:	processingErrorAlarm
Probable Cause:	softwareError (46)
Alarm Text:	Board overload alarm
Status Changes:	
1. Condition:	An overload condition exists in one or more of the system components.
Alarm Status:	Major
2. Condition:	The overload condition passed
Alarm Status:	Cleared

7.2.5.8.9 Feature Key Error Alarm

Table 7-46: acFeatureKeyError

Alarm:	acFeatureKeyError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Default Severity:	Critical
Event Type:	processingErrorAlarm
Probable Cause:	configurationOrCustomizationError (7)
Alarm Text:	Feature key error
Status Changes:	
Note:	Support for this alarm is pending.

7.2.5.8.10Missing SA/M3K Blade (Alarm, Status and Synchronization) Alarm

⚠ **Note:** Applicable only to Mediant 3000.

Table 7-47: acSAMissingAlarm

Alarm:	acSAMissingAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.32
Default Severity:	Critical
Source Varbind Text	Chassis#0/SA#<m>, where *m* is the shelf Alarm module's slot number
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	SA Module Alarm. SA-Module from slot #n is missing.
Status Changes:	
1. Condition:	SA module removed or missing
Alarm Status:	Critical
2. Condition:	SA module is in slot 2 or 4 and working.
Alarm Status:	Cleared

7.2.5.8.11 Administration Status Change Alarm

Table 7-48: acgwAdminStateChange

Alarm:	acgwAdminStateChange
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.7
Default Severity:	Major
Event Type:	processingErrorAlarm
Probable Cause:	outOfService (71)
Alarm Text:	Network element admin state change alarm Gateway is <text>
Status Changes:	
1. Condition:	Admin state changed to shutting down
Alarm Status:	Major
<text> Value:	shutting down. No time limit.
2. Condition:	Admin state changed to locked
Alarm Status:	Major
<text> Value:	locked
1. Condition:	Admin state changed to unlocked
Alarm Status:	cleared
Corrective Action:	A network administrator has taken an action to lock the device. No corrective action is required.

7.2.5.8.12 Operational Status Change Alarm

Table 7-49: acOperationalStateChange

Alarm:	acOperationalStateChange
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.15
Default Severity:	Major
Event Type:	processingErrorAlarm
Probable Cause:	outOfService (71)
Alarm Text:	Network element operational state change alarm. Operational state is disabled.
Note:	This alarm is raised if the operational state of the node goes to disabled. The alarm is cleared when the operational state of the node goes to enabled.
Status Changes:	
1. Condition:	Operational state changed to disabled
Alarm Status:	Major
2. Condition:	Operational state changed to enabled
Alarm Status:	cleared
Note:	In IP systems, the operational state of the node is disabled if the device fails to properly initialize.
Corrective Action:	In IP systems, check for initialization errors. Look for other alarms and Syslogs that might provide additional information about the error.

7.2.5.9 Network Alarms

7.2.5.9.1 Ethernet Link Alarm

Table 7-50: acBoardEthernetLinkAlarm

Alarm:	acBoardEthernetLinkAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Default Severity:	Critical
Source Varbind Text	All except 3000 Series: Board#<n>/EthernetLink#0 (where n is the slot number) 3000 Series: Module#<n>/EthernetLink#0 (where n is the slot number) This trap relates to the Ethernet Link Module (the #0 numbering doesn't apply to the physical Ethernet link).
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Ethernet link alarm: <text>
Status Changes:	
1. Condition:	Fault on single interface
Alarm Status:	Major
<text> Value:	Redundant link is down
2. Condition:	Fault on both interfaces
Alarm Status:	critical
<text> Value:	No Ethernet link
3. Condition:	Both interfaces are operational
Alarm Status:	cleared
Corrective Action:	Ensure that both Ethernet cables are plugged into the back of the system. Inspect the system's Ethernet link lights to determine which interface is failing. Reconnect the cable or fix the network problem

7.2.5.9.2 Ethernet Group Alarm

Note: Applicable only to Mediant 800 GW & E-SBC and Mediant 1000B GW & E-SBC.

Table 7-51: acEthernetGroupAlarm

Alarm:	acEthernetGroupAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.86
Default Severity:	Major
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	Ethernet Group alarm. %s

Alarm:	acEthernetGroupAlarm
Status Changes:	
1. Condition:	Raised when both ports in a group are down
2. Condition:	Cleared when at least one port is up

7.2.5.9.3 WAN Link Alarm

Table 7-52: acBoardWanLinkAlarm (Only for MSBR Devices)

Alarm:	acBoardWanLinkAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.79
Default Severity:	Major / Clear
Event Type:	equipmentAlarm
Source Varbind Text	Board#x/WanLink#y
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	
Status Changes:	
1. Condition:	WAN link down
Alarm Status:	Major
<text> Value:	
2. Condition:	WAN link up
Alarm Status:	Clear
<text> Value:	
Corrective Action:	Connect WAN port

7.2.5.9.4 Data Interface Status Alarm

Note: Applicable only to MSBR series.

Table 7-53: acDataInterfaceStatus

Alarm:	acDataInterfaceStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.83
Default Severity:	indeterminate
Event Type:	communicationsAlarm
Probable Cause:	
Alarm Text:	
Status Changes:	
1. Condition:	
Alarm Status:	
<text> Value:	
Corrective Action:	

7.2.5.9.5 Wireless Cellular Modem Alarm

Note: Applicable only to Mediant 800 MSBR.

Table 7-54: acWirelessCellularModemAlarm

Alarm:	acWirelessCellularModemAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.82
Default Severity:	Major / Clear
Source Varbind Text	Board#x/WanLink#y
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	WAN wireless cellular modem alarm.
Status Changes:	
1. Condition:	Raised when either the wireless modem is down or in backup mode, and cleared when modem is up.
Alarm Status:	Major
2. Condition:	WAN link up
Alarm Status:	Clear

7.2.5.9.6 NTP Server Status Alarm

Table 7-55: acNTPServerStatusAlarm

Alarm:	acNTPServerStatusAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.71
Default Severity:	Major
Event Type:	communicationsAlarm
Probable Cause:	communicationsSubsystemFailure
Alarm Text:	NTP server alarm. No connection to NTP server.
Status Changes:	
1. Condition:	No initial communication to Network Time Protocol (NTP) server.
Alarm Status:	Major
2. Condition:	No communication to NTP server after the time was already set once.
Alarm Status:	Minor
Corrective Action:	Repair NTP communication. (The NTP server is down or its IP address is configured incorrectly in the device.)

7.2.5.9.7 NAT Traversal Alarm

Table 7-56: acNATTraversalAlarm

Alarm:	acNATTraversalAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.17
Default Severity:	Indeterminate
Event Type:	-
Probable Cause:	other (0)
Alarm Text:	NAT Traversal Alarm
Status Changes:	The STUN client in the device is enabled and has either identified a NAT or is not finding the STUN server. Keep-alive is sent out every 9/10 of the time defined in the NatBindingDefaultTimeout parameter.
Corrective Action:	-

7.2.5.9.8 LDAP Lost Connection Alarm

Table 7-57: acLDAPLostConnection

Alarm:	acLDAPLostConnection
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.75
Default Severity:	Minor
Event Type:	communicationsAlarm
Probable Cause:	communicationsSubsystemFailure If a connection is idle for more than the maximum configured time in seconds that the client can be idle before the LDAP server closes the connection, the LDAP server returns an LDAP disconnect notification and this alarm is raised.
Alarm Text:	LDAP Lost Connection
Status Changes:	This alarm is raised when there is no connection to the LDAP server
1. Condition:	
Alarm Status:	

7.2.5.9.9 OCSP Server Status Alarm

Table 7-58: acOCSPServerStatusAlarm

Alarm:	acOCSPServerStatusAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.78
Default Severity:	Major / Clear
Event Type:	communicationsAlarm
Probable Cause:	communicationsSubsystemFailure
Alarm Text:	OCSP server alarm
Corrective Action	-

7.2.5.9.10IPv6 Error Alarm

Table 7-59: acIPv6ErrorAlarm (Applicable only to Mediant 800 E-SBC/3000 Series)

Alarm:	acIPv6ErrorAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.53
Default Severity:	Critical
Source Varbind Text	System#0/Interfaces#<n>.
Event Type:	operationalViolation
Probable Cause:	communicationsProtocolError
Alarm Text:	IP interface alarm. <text>
Status Changes:	
1. Condition:	Bad IPv6 address (already exists)
Alarm Status:	Critical
<text> Value:	IPv6 Configuration failed, IPv6 will be disabled.
2. Condition:	After alarm raise
Alarm Status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	Find new IPV6 address and reboot.

7.2.5.10 Active Alarm Table Alarm

Table 7-60: acActiveAlarmTableOverflow

Alarm:	acActiveAlarmTableOverflow
OID:	1.3.6.1.4.15003.9.10.1.21.2.0.12
Default Severity:	Major
Source Varbind Text	*System#0*<n>*/AlarmManager#0*
Event Type:	processingErrorAlarm
Probable Cause:	resourceAtOrNearingCapacity (43)
Alarm Text:	Active alarm table overflow
Status Changes:	
1. Condition:	Too many alarms to fit in the active alarm table
Alarm Status:	Major
2. Condition:	After raise
Alarm Status:	Status remains Major until reboot. A Clear trap is not sent.
Note:	The status remains Major until reboot as it denotes a possible loss of information until the next reboot. If an alarm is raised when the table is full, it is possible that the alarm is active, but does not appear in the active alarm table.
Corrective Action:	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

7.2.5.11 Audio Staging from APS Server Alarm

⚠ **Note:** Applicable only to Mediant 1000 series.

Table 7-61: acAudioProvisioningAlarm

Alarm:	acAudioProvisioningAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.14
Default Severity:	Critical
Source Varbind Text	System#0/AudioStaging#0
Event Type:	processingErrorAlarm
Probable Cause:	configurationOrCustomizationError (7)
Alarm Text:	Unable to provision audio
Status Changes:	
1. Condition:	Media server times out waiting for a successful audio distribution from the APS (Audio Provisioning Server)
Alarm Status:	Critical
2. Condition:	After raise, media server is successfully provisioned with audio from the APS
Alarm Status:	Cleared
Corrective Action:	From the APS (Audio Provisioning Server) GUI ensure that the device is properly configured with audio and that the device has been enabled. Ensure that the IP address for the APS has been properly specified on the device. Ensure that both the APS server and application are in-service. For more information regarding the problem, view the Syslogs from the device as well as the APS manager logs.

7.2.5.12 Analog Port Alarms

⚠ **Note:** These alarms are applicable only to Analog devices.

7.2.5.12.1 Analog Port SPI Out-of-Service Alarm

Table 7-62: acAnalogPortSPIOutOfService

Alarm:	acAnalogPortSPIOutOfService
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.46
Default Severity:	Major
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number
Event Type:	physicalViolation
Probable Cause:	equipmentMalfunction
Alarm Text:	Analog Port SPI out of service
Status Changes:	

Alarm:	acAnalogPortSPIOutOfService
1. Condition:	Analog port has gone out of service
Alarm Status:	Major
2. Condition:	Analog port is back in service.
Alarm Status:	Cleared
Corrective Action:	None

7.2.5.12.2 Analog Port High Temperature Alarm

Table 7-63: acAnalogPortHighTemperature

Alarm:	acAnalogPortHighTemperature
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.47
Default Severity:	Major
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number
Event Type:	physicalViolation
Probable Cause:	equipmentMalfunction
Alarm Text:	Analog Port High Temperature
Status Changes:	
1. Condition:	Analog device has reached critical temperature. Device is automatically disconnected.
Alarm Status:	Major
2. Condition:	Temperature is back to normal - analog port is back in service.
Alarm Status:	Cleared
Corrective Action:	None
Note:	Relevant to FXS only.

7.2.5.12.3 Analog Port Ground Fault Out-of-Service Alarm

Table 7-64: acAnalogPortGroundFaultOutOfService

Alarm:	acAnalogPortGroundFaultOutOfService
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.76
Default Severity:	Major / Clear
Source Varbind Text	System#0/analogports#<n>, where *n* is the port number
Event Type:	physicalViolation
Probable Cause:	equipmentMalfunction (This alarm is raised when the FXS port is inactive due to a ground fault)
Alarm Text:	Analog Port Ground Fault Out Of Service
Corrective Action:	-
Note:	Relevant to FXS only.

7.2.5.13 Media Alarms

7.2.5.13.1 Media Process Overload Alarm

> **Note:** This alarm is applicable only to MSBR series, Mediant 1000B GW & SBC, Mediant 2000, and Mediant 3000.

Table 7-65: acMediaProcessOverloadAlarm

Alarm:	acMediaProcessOverloadAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.81
Default Severity:	Major
Event Type:	environmentalAlarm
Probable Cause:	underlyingResourceUnavailable
Alarm Text:	Media Process Overload Alarm. %s
Status Changes:	
1. Condition:	
Alarm Status:	Major
2. Condition:	
Alarm Status:	Cleared
Corrective Action:	None

7.2.5.13.2 Media Realm Bandwidth Threshold Alarm

> **Note:** This alarm is applicable only to Mediant 1000B GW & SBC and Mediant 800 GW & E-SBC.

Table 7-66: acMediaRealmBWThresholdAlarm

Alarm:	acMediaRealmBWThresholdAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.87
Default Severity:	
Event Type:	ProcessingErrorAlarm
Probable Cause:	Raised when a bandwidth threshold is crossed
Alarm Text:	Media Realm BW Threshold Alarm.
Status Changes:	
1. Condition:	
Alarm Status:	Major
Corrective Action:	Cleared when bandwidth threshold returns to normal range

7.2.5.14 Network Monitoring (Probe) between Devices

Note: This alarm is applicable only to Mediant 800 MSBR and Mediant 850 MSBR.

7.2.5.14.1NQM Connectivity Alarm

Table 7-67: acNqmConnectivityAlarm

Alarm:	acNqmConnectivityAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.88
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsSubsystemFailure
Probable Cause:	Raised when Connectivity with NQM probe destination is lost
Alarm Text:	Connectivity with NQM probe destination is lost
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	Cleared when Connectivity with NQM probe destination is re-established

7.2.5.14.2NQM High RTT Alarm

Table 7-68: acNqmRttAlarm

Alarm:	acNqmRttAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.89
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsSubsystemFailure
Probable Cause:	Raised when Detected high RTT towards NQM probe destination
Alarm Text:	Detected high RTT towards NQM probe destination
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	

7.2.5.14.3NQM High Jitter Alarm

Table 7-69: acNqmJitterAlarm

Alarm:	acNqmJitterAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.90
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsAlarm
Probable Cause:	Raised when Detected high Jitter towards NQM probe destination - thresholdCrossed
Alarm Text:	Detected high Jitter towards NQM probe destination
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	

7.2.5.14.4NQM High Packet Loss Alarm

Table 7-70: acNqmPacketLossAlarm

Alarm:	acNqmPacketLossAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.91
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsAlarm
Probable Cause:	Raised when Detected high Packet Loss towards NQM probe destination
Alarm Text:	Detected high PL towards NQM probe destination
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	

7.2.5.14.5NQM Low Conversational MOS Alarm

Table 7-71: acNqmCqMosAlarm

Alarm:	acNqmCqMosAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.95
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsAlarm
Probable Cause:	Raised when Detected low conversational voice quality towards NQM probe destination
Alarm Text:	Detected low conversational voice quality towards NQM probe destination

Alarm:	acNqmCqMosAlarm
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	

7.2.5.14.6NQM Low Listening MOS Alarm

Table 7-72: acNqmLqMosAlarm

Alarm:	acNqmLqMosAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.96
Default Severity:	
Alarm Source:	Board#%d/NqmSender#%d
Event Type:	communicationsAlarm
Probable Cause:	Raised when Detected low listening voice quality towards NQM probe destination
Alarm Text:	Detected low listening voice quality towards NQM probe destination
Status Changes:	
1. Condition:	
Alarm Status:	Minor
Corrective Action:	

7.2.5.15 Intrusion Detection Alarms

7.2.5.15.1 IDS Policy Alarm

Table 7-73: acIDSPolicyAlarm

Alarm:	acIDSPolicyAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Description:	The alarm is raised whenever a threshold is crossed in the IDS system. The alarm is associated with the MO pair IDSMatch & IDSRule.
Default Severity:	
Event Type:	Other
Probable Cause:	
Alarm Text:	“Policy NUM (NAME): minor/major/critical threshold (NUM) of REASON cross in global/ip/ip+port scope (triggered by IP)”
Status Changes:	
Corrective Action:	

7.2.5.16 SAS Alarms

7.2.5.16.1 Emergency Mode Alarm

Table 7-74: acGWSASEmergencyModeAlarm

Alarm:	acGWSASEmergencyModeAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.59
Default Severity:	
Event Type:	Other
Probable Cause:	Other
Alarm Text:	-
Status Changes:	Sent by the Stand-Alone Survivability (SAS) application when switching from “Normal" mode to “Emergency" mode. This alarm is cleared once the SAS returns to “Normal" mode.
Corrective Action:	-

7.2.6 Event Traps (Notifications)

This subsection details traps that are not alarms. These traps are sent with the severity varbind value of ‘indeterminate’. These traps don’t ‘clear’ and they don’t appear in the alarm history or active tables. (The only log trap that does send clear is acPerformanceMonitoringThresholdCrossing.)

7.2.6.1 IDS Threshold Cross Notification

Table 7-75: acIDSThresholdCrossNotification

Alarm:	acIDSThresholdCrossNotification
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Description:	The trap is sent for each scope (IP or IP:port) crossing a threshold of an active alarm.
Default Severity:	
Event Type:	Other
Probable Cause:	
Alarm Text:	“Threshold cross for scope value IP. Severity=minor/major/critical. Current value=NUM"
Status Changes:	
Corrective Action:	

7.2.6.2 Web User Access Denied due to Inactivity Trap

Table 7-76: acWebUserAccessDisabled

Alarm:	
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Default Severity:	indeterminate
Event Type:	
Probable Cause:	Sent when Web user was disabled due to inactivity
Alarm Text:	
Status Changes:	
Corrective Action:	

7.2.6.3 Power-Over-Ethernet Status Trap

Note: This alarm is applicable only to Mediant 800 MSBR.

Table 7-77: acPowerOverEthernetStatus

Trap:	acPowerOverEthernetStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.80
Default Severity:	Indeterminate
Event Type:	environmentalAlarm
Probable Cause:	underlyingResourceUnavailable
Trap Text:	"POE Port %d Was Not Powered Due To Power Management" Where, %d is the Ethernet port number.
Condition:	This trap is sent when insufficient power is available for a plugged-in PoE client in a PoE-enabled LAN port.
Trap Status:	Trap is sent

7.2.6.4 Keep-Alive Trap

Table 7-78: acKeepAlive

Trap:	acKeepAlive
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Default Severity:	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Trap Text:	Keep alive trap
Status Changes:	
Condition:	The STUN client is enabled and identified as a NAT device or doesn't locate the STUN server. The *ini* file contains the following line: 'SendKeepAliveTrap=1'
Trap Status:	Trap is sent
Note:	Keep-alive is sent every 9/10 of the time defined in the parameter NatBindingDefaultTimeout.

7.2.6.5 Performance Monitoring Threshold-Crossing Trap

Table 7-79: acPerformanceMonitoringThresholdCrossing

Trap:	acPerformanceMonitoringThresholdCrossing
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Default Severity:	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Trap Text:	"Performance: Threshold trap was set", with source = name of performance counter which caused the trap
Status Changes:	
Condition:	A performance counter has crossed the high threshold
Trap Status:	Indeterminate
Condition:	A performance counter has returned to under the threshold
Trap Status:	Cleared

7.2.6.6 HTTP Download Result Trap

Table 7-80: acHTTPDownloadResult

Trap:	acHTTPDownloadResult
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Default Severity:	Indeterminate
Event Type:	processingErrorAlarm (3) for failures and other (0) for success.
Probable Cause:	other (0)
Status Changes:	
Condition:	Successful HTTP download.
Trap Text:	HTTP Download successful
Condition:	Failed download.
Trap Text:	HTTP download failed, a network error occurred.
Note:	There are other possible textual messages describing NFS failures or success, FTP failure or success.

7.2.6.7 Dial Plan File Replaced Trap

Note: This alarm is applicable only to Digital PSTN devices.

Table 7-81: acDialPlanFileReplaced

Alarm:	acDialPlanFileReplaced
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.45
Default Severity:	Indeterminate
Event Type:	Other (0)
Probable Cause:	Other (0)
Status Change:	
Condition:	Successful dial plan file replacement
Trap Text:	Dial plan file replacement complete.

7.2.6.8 Hitless Software Upgrade Status Trap

⚠ **Note:** This alarm is applicable only to Mediant 3000.

Table 7-82: acHitlessUpdateStatus

Alarm:	acHitlessUpdateStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.48
Default Severity:	Indeterminate
Event Type:	Other (0)
Probable Cause:	Other (0)
Source:	Automatic Update
Status Changes:	
Condition:	Successful SW upgrade
Trap Text:	Hitless: SW upgrade ended successfully
Condition:	Failed SW upgrade
Trap Text:	Hitless fail: Waiting for module in slot <n> to burn new SW and reboot Timed out. (n – slot number).

7.2.6.9 Secure Shell (SSH) Connection Status Trap

Table 7-83: acSSHConnectionStatus

Alarm:	acSSHConnectionStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.77
Default Severity:	indeterminate
Event Type:	environmentalAlarm
Probable Cause:	other
Alarm Text:	"SSH logout from IP address <IP>, user <user>" "SSH successful login from IP address <IP>, user <user> at: <IP>:<port>" "SSH unsuccessful login attempt from IP address <IP>, user <user> at: <IP>:<port>. <reason>" "WEB: Unsuccessful login attempt from <IP> at <IP>:<port>. <reason>"
Status Changes:	
Condition:	SSH connection attempt
<text> Value:	%s – remote IP %s – user name
Condition:	SSH connection attempt – success of failure

7.2.6.10 SIP Proxy Connection Lost Trap

Table 7-84: acProxyConnectionLost

Alarm:	acProxyConnectionLost
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.94
Default Severity:	
Event Type:	
Probable Cause:	Raised when all connections in the Proxy Set are down
Alarm Text:	
Status Changes:	
Condition:	
<text> Value:	
Condition:	

7.2.6.11 TLS Certificate Expiry Trap

Table 7-85: acCertificateExpiryNotifiaction Trap

Alarm:	acCertificateExpiryNotifiaction
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.92
Default Severity:	Intermediate
Event Type:	environmentalAlarm
Probable Cause:	keyExpired
Alarm Text:	The device TLS server certificate will expire in %d days
Status Changes:	
Condition:	Send before the expiration of the installed credentials, which cannot be renewed automatically
Alarm Status:	Intermediate
<text> value	%d – Number of days

7.2.6.12 Cold Start Trap

Table 7-86: coldStart

Trap Name:	coldStart
OID:	1.3.6.1.6.3.1.1.5.1
MIB:	SNMPv2-MIB
Note:	This is a trap from the standard SNMP MIB.

7.2.6.13 Authentication Failure Trap

Table 7-87: authenticationFailure

Trap Name:	authenticationFailure
OID:	1.3.6.1.6.3.1.1.5.5
MIB:	SNMPv2-MIB

7.2.6.14 Board Initialization Completed Trap

Table 7-88: acBoardEvBoardStarted

Trap Name:	acBoardEvBoardStarted
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
MIB:	AcBoard
Severity:	cleared
Event Type:	equipmentAlarm
Probable Cause:	Other(0)
Alarm Text:	Initialization Ended
Note:	This is the AudioCodes Enterprise application cold start trap.

7.2.6.15 Configuration Change Trap

Table 7-89: entConfigChange

Trap Name:	entConfigChange
OID:	1.3.6.1.2.1.4.7.2
MIB:	ENTITY-MIB

7.2.6.16 Link Up Trap

Table 7-90: linkUp

Trap Name:	linkUp
OID:	1.3.6.1.6.3.1.1.5.4
MIB:	IF-MIB

7.2.6.17 Link Down Trap

Table 7-91: linkDown

Trap Name:	linkDown
OID:	1.3.6.1.6.3.1.1.5.3
MIB:	IF-MIB

7.2.6.18 D-Channel Status Trap

Note: This alarm is applicable only to Digital PSTN devices.

Table 7-92: AcDChannelStatus

Trap Name:	acDChannelStatus
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
MIB	AcBoard
Severity:	Minor
Event Type:	communicationsAlarm
Probable Cause:	communicationsProtocolError
Alarm Text:	D-Channel Trap.
Source:	Trunk <m> where m is the trunk number (starts from 0).
Status Changes:	
Condition:	D-Channel un-established.
Trap Status:	Trap is sent with the severity of Minor.
Condition:	D-Channel established.
Trap Status:	Trap is sent with the severity of Cleared.

8 Advanced SNMP Features

8.1 Dual Module Interface

Note: This subsection is applicable only to 2000 Series devices.

Dual module blades have a first and second module (the first is on the right side of the blade -- TP-1610 and IPM-1610 -- when looking at it from the front). Differentiation is based on the modules' serial numbers.

MIB object acSysIdSerialNumber always returns the serial number of the module on which the GET is performed. MIB object acSysIdFirstSerialNumber always returns the serial number of the first module.

If the module on which the GET is performed is the second module, the values in these two are different. If, on the other hand, the module is the first module, the value in the two objects is the same.

8.2 SNMP NAT Traversal

A NAT placed between the device and the element manager calls for traversal solutions:

- **Trap source port:** all traps are sent from the SNMP port (default is 161). A manager receiving these traps can use the binding information (in the UDP layer) to traverse the NAT back to the device.
  The trap destination address (port and IP) are as configured in the snmpTargetMIB.

- **acKeepAliveTrap:** this trap is designed to be a constant life signal from the device to the manager, allowing the manager NAT traversal at all times. The acBoardTrapGlobalsAdditionalInfo1 varbind has the device’s serial number.

  The destination port (i.e., the manager port for this trap), can be set to be different than the port to which all other traps are sent. To do this, use the **acSysSNMPKeepAliveTrapPort** object in the acSystem MIB or the KeepAliveTrapPort *ini* file parameter.

  The Trap is instigated in three ways:

  - Via an *ini* file parameter (SendKeepAliveTrap = 1). This ensures that the trap is continuously sent. The frequency is set via the 9/10 of the NATBindingDefaultTimeout (or MIB object acSysSTUNBindingLifeTime) parameter.
  - After the STUN client has discovered a NAT (any NAT).
  - If the STUN client can not contact a STUN server.

Note: The two latter options require the STUN client be enabled (*ini* file parameter EnableSTUN). In addition, once the acKeepAlive trap is instigated it does not stop.

- The manager can view the NAT type in the MIB: audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemStatus(2).acSysNetwork(6).acSysNAT(2).acSysNATType(1)
- The manager also has access to the STUN client configuration: audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemConfiguration(1).acSysNetworkConfig(3).acSysNATTraversal(6).acSysSTUN(21)
- **acNATTraversalAlarm**: When the NAT is placed in front of a device that is identified as a symmetric NAT, this alarm is raised. It is cleared when a non-symmetric NAT or no NAT replaces the symmetric one.

8.3 Media Server Configuration

Note: This subsection is applicable only to IPmedia Series and Mediant 1000.

Configuration for the device can be performed by using the SNMP interfaces in the acBoardMIB or setting of configuration parameters in the *ini* file. Access to the configuration parameters is also provided through the Web interface.

A default *ini* (or initialization) template has been defined, which configures the configuration parameters to settings that typically, do not require later modificatons.

Configuration parameters in the acBoardMIB specific to services on the device include:

- **amsApsIpAddress:** IP address of the audio provisioning server
- **amsApsPort**: port number to use for the audio provisioning server
- **amsPrimaryLanguage:** primary language used for audio variables
- **amsSecondaryLanguage:** secondary language used for audio variables

8.4 Systems

Note: This subsection is applicable only to 3000 Series.

For the management of a system (a chassis with more then one type of module running), the acSystem/acSystemChassis subtree in the acSystem MIB should be used:

- The first few objects are scalars that are read-only objects for the dry-contacts' state.
- **acSysModuleTable:** A table containing mostly status information that describes the blade modules in the system. In addition, the table can be used to reset an entire system, reset a redundant module or perform switchover when the system is HA.
- **acSysFanTrayTable**: A status-only table with the fan tray's state. Objects in the table indicate the specific state of the individual fans within the fan tray.
- **acSysPowerSupplyTable**: A status-only table with the states of the two power supplies.

- **acSysPEMTable**: A status-only table with the states of the two PEMs (Power Entry Modules).

The above tables are complemented by the following alarm traps (as defined in the acBoard MIB. For more details, see "SNMP Traps" on page 112):

- **acFanTrayAlarm**: fault in the fan tray or fan tray missing.
- **acPowerSupplyAlarm**: fault in one of the power supply modules or PS module missing.
- **acPEMAlarm**: fault in the one of the PEM modules or PEM module missing.
- **acSAMissingAlarm**: SA module missing or non operational.
- **acUserInputAlarm**: the alarm is raised when the input dry contact is short circuited and cleared when the circuit is reopened.

8.5 High Availability Systems

Note: This subsection is applicable only to Mediant 3000.

For the management of the High Availability (HA) systems, use the acSysChassis MIB subtree (as in the above section). The acSysModuleTable gives the HA state of the system. This includes defining which modules are active and which are in standby mode (redundant). The table also enables to read some of the statuses of the redundant modules (such as SW version, HW version, temperature, license key list, etc.). Resetting the system, resetting the redundant module, and performing switchover are performed done using this table.

Complementing the above are the following alarm traps (as defined in the acBoard MIB):

- **acHASystemFaultAlarm:** the HA is faulty and therefore, there is no HA.
- **acHASystemConfigMismatchAlarm**: configuration to the modules in the HA system us uneven causing instability.
- **acHASystemSwitchOverAlarm**: a switchover from the active to the redundant module has occurred.

8.6 Configuring Clock Synchronization

Note: This subsection is applicable only to Mediant 3000.

The procedures below describe how to configure clock synchronization modes.

➢ **To configure line synchronization, perform the following steps:**

1. Set acSysTimingMode to lineSync.
2. Set acSysTDMClockSource to the interface (according to the hardware you are using) from which you wish to derive the clock.

3. Set TDMBusLocalReference to the reference trunk number.
4. Set acSysTDMClockPLLOutOfRange to the requested value.
5. Set acSysActionSetOnLineChangesApply to 1 in order to apply all changes.

➢ **To configure BITS Synchronization mode through SNMP:**

1. Set acSysTimingMode to external.
2. Set acSysTDMClockBitsReference (1 – Primary Clock Reference is BITs A. (Default) 2 – Primary Clock Reference is BITs B).
3. Set acSysTDMClockEnableFallBack (manual(0), autoNon-Revertive(1), auto-Revertive(2) TDMBusEnableFallback sets the fallback clock method between primary to secondary BITS clock references.)
4. Set acSysTimingExternalIFType to define the external BITS reference transmission type for both primary and secondary interfaces.
5. Set acSysTimingT1LineBuildOut / acSysTimingE1LineBuildOut.
6. Set acSysTimingValidationTime to the requested time range: 0-15 minutes.
7. Set acSysActionSetOnLineChangesApply to 1 in order to apply all changes.

8.7 SNMP Administrative State Control

Node maintenance for the device is provided via an SNMP interface. The acBoardMIB provides two parameters for graceful and forced shutdowns of the device. These parameters are in the acBoardMIB as follows:

- acSysActionAdminState - read-write MIB object. When a GET request is sent for this object, the agent returns the current device administrative state - determines the device's desired operational state:
  - **locked (0):** Shutdown the device in the time frame set by acSysActionAdminStateLockTimeout.
  - **shuttingDown (1):** (read-only) Graceful shutdown is being performed - existing calls are allowed to complete, but no new calls are allowed.
  - **unlocked (2):** The device is in service.

  On a SET request, the manager supplies the required administrative state, either locked(0) or unlocked(2). When the device changes to either shuttingDown or locked state, an adminStateChange alarm is raised. When the device changes to an unlocked state, the adminStateChange alarm is cleared.
- acSysActionAdminStateLockTimeout - defines the time remaining (in seconds) for the shutdown to complete:
  - **0:** immediate shutdown and calls are terminated (forced lock)
  - **1:** waits until all calls are terminated (i.e., perform a Graceful shutdown)
  - **> 0:** the number of seconds to wait before the graceful shutdown turns into a force lock

Note: The acSysActionAdminStateLockTimeout must be set before the acSysActionAdminState.

9 Getting Started with SNMP

This section provides a getting started for quickly setting up the device for management using AudioCodes SNMP MIBs.

9.1 Basic SNMP Configuration Setup

This subsection provides a description of the required SNMP configuration when first accessing the SNMP agent running on the device.

To access the device's SNMP agent, there are a few parameters that can be configured if you wish not to use default settings. The SNMP agent default settings include the following:

- SNMP agent is enabled.
- Port 161 in the agent is used for SNMP GET/SET commands.
- No default trap managers are defined, therefore, the device does not send traps.
- The Trap destination port is 162.
- The SNMP agent is accessible to all SNMP managers (i.e., no trusted managers).
- SNMP Protocol version - SNMPv2c with 'public' and 'private' as the read-only and read-write community strings respectively.

Configuring these SNMP attributes is described in the following subsections:

9.1.1 Configuring SNMP Port

To configure the agent's SNMP port in the ini file, set the following

```
SNMPPort = <x>
; where 'x' is the port number
```

9.1.2 Configuring Trap Managers (Trap Destination)

Configuring Trap Managers (i.e., trap destinations) includes defining IP address and port. This configuration corresponds to the snmpTargetAddrTable. The agent supports up to five separate trap destinations. For each manager, you need to set the manager IP address and trap-receiving port along with enabling the sending to that manager. Trap managers can be configured using ini file, SNMP, or Web interface.

In addition, you can associate a trap destination with a specific SNMPv3 USM user. Traps will be sent to that trap destination using the SNMPv3 format and the authentication and privacy protocol configured for that user.

- **Using ini File:** two options that can be used separately or together:
  - Explicit IP address:

    ```
    SNMPMANAGERTABLEIP_x=<IP address>
    SNMPMANAGERISUSED_x=1
    SNMPMANAGERTRAPSENDINGENABLE_x=1
    SNMPMANAGERTRAPPORT_x=162 ;(optional)
    Where x is the entry index from 0 to 4
    ```

  - Manager host name:

```
SNMPTrapManagerHostName = <'host name on network'>
```

For example: 'myMananger.corp.MyCompany.com'

The host name is translated into the IP address using DNS resolution and is then defined as the fifth (last) trap manager. Until the address is resolved, some traps are expected to be lost.

Notes:

- This option also requires you to configure the DNS server IP address (in the Multiple Interface table).
- This option results in the fifth manager being overrun by the resolved IP address. Online changes to the Manager table will also be overrun.

- **Using SNMP:** The trap managers are SET using the SNMPTargetMIB MIB onbject.
  - To add an SNMPv2 trap destination: Add a row to the snmpTargetAddrTable with these values:
    - Name=trapN, where *N* is an unused number between 0 and 4.
    - TagList=AC_TRAP
    - Params=v2cparamsm

    All changes to the trap destination configuration take effect immediately.
  - To add an SNMPv3 trap destination:
    1. Add a row to the snmpTargetAddrTable with these values: Name=trapN, >, where *N* is an unused number between 0 and 4, and <*user*> is the name of the SNMPv3 that this user is associated with:
       - ✓ TagList=AC_TRAP
       - ✓ Params=usm<user>
    2. If a row does not already exist for this combination of user and SecurityLevel, add a row to the snmpTargetParamsTable with this values:
       - ✓ Name=usm<user>
       - ✓ MPModel=3(SNMPv3)
       - ✓ SecurityModel=3 (usm)
       - ✓ SecurityName=<user>
       - ✓ SecurityLevel=M, where *M* is either 1(noAuthNoPriv), 2(authNoPriv) or 3(authPriv)
  - To delete a trap destination:
    1. Remove the appropriate row from the snmpTargetAddrTable.
    2. If this is the last trap destination associated with this user and security level, you can also delete the appropriate row from the snmpTargetParamsTable.
  - To modify a trap destination, change the IP address and or port number for the appropriate row in the snmpTargetAddrTable for an existing trap destination. The same effect can be achieved by removing a row and adding a new row.
  - To disable a trap destination, change TagList on the appropriate row in the snmpTargetAddrTable to the empty string.
  - To enable a trap destination, change TagList on the appropriate row in the snmpTargetAddrTable to "AC_TRAP".
- **Using Web Interface:** The Trap Destination table appears in the 'SNMP Trap

Destinations' page (**Configuration** tab > **System** menu > **Management** > **SNMP** > **SNMP Trap Destinations**). The check box on the left indicates if the row is used. The three columns are used to set IP address, port and enable trap sending. The SNMPv3 Settings table, also accessed from the 'Management Setting' page is used for setting trap users.

- To add a trap user: In the field near the **Add Index** button, enter the index of the row you want to add (0 to 9), and then click the button. The row is now available for configuration. The five columns include name, authentication protocol, privacy protocol, authentication key and privacy key. After configuring the columns, click **Apply**.
- To delete a row: Select the corresponding index field, and then click **Delete**.

9.1.3 Configuring Trap Destination Port

For configuring the trap destination port, see trap managers, above.

9.1.4 Configuring Trusted Managers

The configuration of trusted managers determines which managers can access the device. You can define up to five trusted managers.

Notes:

- The concept of trusted managers is considered to be a weak form of security and is therefore, not a required part of SNMPv3 security, which uses authentication and privacy.
- Trusted managers are therefore, not supported in SNMPv3 – thus they apply only when the device is set to use SNMPv2c.
- If trusted managers are defined, then all community strings work from all trusted managers. That is, there is no way to associate a community string with particular trusted managers.

The configuration can be done via ini file, SNMP and Web.

- **Using ini file:** SNMPTRUSTEDMGR_x = <IP address>, where *x* is the entry index 0 to 4.
- **Using SNMP:** To configure Trusted Managers, the EM must use the SNMP-COMMUNITY-MIB, snmpCommunityMIB, and snmpTargetMIB.
  - To add the first Trusted Manager: This procedure assumes that there is at least one configured read-write community. There are currently no Trusted Managers. The TransportTag for columns for all snmpCommunityTable rows are currently empty.
    1. Add a row to the snmpTargetAddrTable with these values:
       - ✓ Name=mgr0
       - ✓ TagList=MGR
       - ✓ Params=v2cparams.
    2. Add a row to the snmpTargetAddrExtTable table with these values:
       - ✓ Name=mgr0
       - ✓ snmpTargetAddrTMask=255.255.255.255:0.

The agent does not allow creation of a row in this table unless a corresponding row exists in the snmpTargetAddrTable.

3. Set the value of the TransportTag field on each non-TrapGroup row in the snmpCommunityTable to MGR.

- To add a subsequent Trusted Manager: This procedure assumes that there is at least one configured read-write community. There are currently one or more Trusted Managers. The TransportTag for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from one of the existing Trusted Managers.

  1. Add a row to the snmpTargetAddrTable with these values:
     - ✓ Name=mgrN, where N is an unused number between 0 and 4.
     - ✓ TagList=MGR
     - ✓ Params=v2cparams
  2. Add a row to the snmpTargetAddrExtTable table with these values:
     - ✓ Name=mgrN
     - ✓ snmpTargetAddrTMask=255.255.255.255:0.

  An alternative to the above procedure is to set the snmpTargetAddrTMask column while you are creating other rows in the table.

- To delete a Trusted Manager (not the final one): This procedure assumes that there is at least one configured read-write community. There are currently two or more Trusted Managers. The taglist for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from one of the existing trusted managers, but not the one that is being deleted. Remove the appropriate row from the snmpTargetAddrTable; The change takes effect immediately. The deleted trusted manager cannot access the device. The agent automatically removes the row in the snmpTargetAddrExtTable.

- To delete the final Trusted Manager: This procedure assumes that there is at least one configured read-write community. There is currently only one Trusted Manager. The taglist for columns for all rows in the snmpCommunityTable are currently set to MGR. This procedure must be done from the final Trusted Manager.

  1. Set the value of the TransportTag field on each row in the snmpCommunityTable to the empty string.
  2. Remove the appropriate row from the snmpTargetAddrTable; The change takes effect immediately. All managers can now access the device. The agent automatically removes the row in the snmpTargetAddrExtTable.

- Using Web interface: Under the **Configuration** tab, choose **System**, **Management**, **SNMP**, and then click **SNMP Trusted Managers**. The Web now displays the table. Use the **Submit** button for applying your configuration. Use the check boxes for deleting.

9.2 Familiarizing yourself with AudioCodes MIBs

AudioCodes proprietary MIBs are located in the AudioCodes subtree (OID 1.3.6.1.4.1.5003). A classification within the subtree separates the MIBs according to the following:

- Configuration and status MIBs – in the acBoardMibs subtree
- Performance monitoring MIBs – in the acPerformance subtree
- Proprietary Carrier Grade Alarm MIB – in the acFault subtree

In the acBoardsMibs and acPerformance subtrees, the different MIB modules are grouped according to different virtual modules of AudioCodes' devices. In general, the division is as follows (a more detailed breakdown of the MIBs is discussed below):

- **acBoardMibs subtrees:**
  - **acBoard MIB:** proprietary traps.
  - **acGateway MIB:** SIP control protocol specific objects. This MIB is supported only in SIP devices. This MIB's structure is unlike the other configuration and status MIBs.
  - **acMedia MIB:** DSP and media related objects. This MIB includes the configuration and status of DSP, voice, modem, fax, RTP/RTCP related objects. This MIB is relevant to all devices.
  - **acControl MIB:** mostly MEGACO and MGCP CP related objects. A number of objects are also related to SIP. The MIB is divided into subtrees that are common to both MEGACO and MGCP (amongst these are also the SIP relevant objects) and subtrees that are specific to the different CPs. This MIB is relevant to all devices.
  - **acAnalog MIB:** all objects in this MIB are related only to the configuration, status and line testing or resetting of analog interfaces. This MIB is relevant to devices with analog interfaces only.
  - **acPSTN MIB:** configuration and status of trunk related objects only. Most of the MIB objects are trunk specific. This MIB is relevant to devices with digital PSTN interfaces only.
  - **acSystem MIB:** configuration and status of a wide range of general objects along with chassis related objects and a variety of actions that can be instigated. The MIB is relevant to all devices.
  - **acV5 MIB:** configuration and status of v5.2 related objects only. This MIB is relevant to Mediant 3000/TP-6310.
- **acPerformance subtrees:**
  - acPMMedia, acPMControl, acPMAnalog, acPMPSTN, acPMSystem: module specific parameters performance monitoring MIBs
  - acPMMediaServer MIB: performance monitoring specifically for MediaServer related parameters (IVR, BCT, Conference and Trunk-Testing)
  - acPerfH323SIPGateway MIB: performance specific for SIP CP devices. This MIB's structure is unlike the other performance monitoring MIBs.
- **acFault subtree:** only one MIB exists – the acAlarm which is a proprietary simplification of the standard notificationLogMIB and alarmMIB (both are also supported).

The structure of the different MIBs is similar, depending on the subtree in which they reside. The MIBs in the acBoardMibs subtree have a very similar structure (except the acBoard and acGateway MIBs). Each MIB can be made up of four major subtrees:

- **Configuration subtree:** mostly read-write objects, tables and scalars. The relevant module's configuration is done via these objects.
- **Status subtree:** read-only objects, tables and scalars. Module status is collected by these objects.
- **Action subtree:** read-write objects that are used to instigate actions on the device (such as reset, save configuration, and so on) and read-only objects used to receive the actions' results.

- **Chassis subtree (in acSystem MIB only):** read-write and read-only objects related to chassis control and management (this includes, fan trays, power supply modules, PSTN IF modules, etc').

The acBoard MIB contains some deprecated objects and current proprietary trap definitions.

The acGateway MIB contains only the configuration subtree which in return is divided into common, SIP and H323 subtrees. The H323 subtree is mostly deprecated or obsolete.

9.3 Performance Monitoring Overview

Performance monitoring (PM) are available for a Third-Party Performance Monitoring System through an SNMP interface and can be polled at any interval by an external poller or utility in the management server or other off device system.

This section describes AudioCodes proprietary performance measurements (PM) MIB.

The device's performance measurements are provided by several proprietary MIBs (located under the "acPerformance" subtree (see below for more detail on each of the MIBs):

- **acPMMedia:** for media (voice) related monitoring such as RTP and DSP.
- **acPMControl:** for Control Protocol related monitoring such as connections, commands.
- **acPMAnalog:** Analog channels off-hook state (applicable to devices with analog interfaces only)
- **acPMPSTN:** for PSTN related monitoring such as channel use, trunk utilization.
- **cPMSystem:** for general (system related) monitoring.
- **acPMMediaServer:** for Media Server specific monitoring. (Applicable to the 3000/6310/8410 devices)

Performance Monitoring MIBs have a fixed format. They all have an identical structure consisting of two major subtrees:

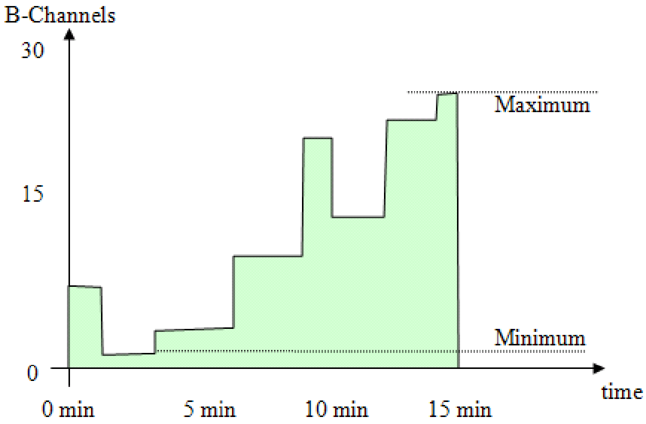
- **Configuration subtree:** allows configuration of general attributes of the MIB and specific attributes of the monitored objects.
- **Data subtree:** this is where the monitored information is found.

The information supplied by the device is divided into time intervals (default is 15 minutes). These intervals are used as a key in the tables. Thus, the monitoring results are presented in tables. There are one or two indices in each table. If there are two, the first is a sub-set in the table (e.g., trunk number) and the second (or the single where there is only one) index represents the interval number (present - 0, previous - 1 and the one before - 2).

Some of the PM parameters support a history with more than two intervals. These include the MEGACO parameters, IVR requests, IVR-play-collect, IVR-play-record, BCT contexts, conference calls, trunk-test calls and digit-collect requests.

Note: The interval's start time is synchronized with the device's clock so that they begin on the hour. If you are using NTP, then it is likely that the last interval within the first hour after device startup will be cut short to accommodate for this synchronization.

Following is a graphic example of one monitored parameter, in this case the number of utilized B-channels in a single trunk:



The x-axis is the time within the interval. The y-axis is the number of used channels. The parameter's value is a gauge. While the interval index is 0 (thus it is the current interval, any GET on the parameter value will return y-axis value for the graph at that moment in time. When the interval is over (index 1 or 2) the value is no longer relevant but there are other attributes such as the average – in this case the area in green divided by the interval length in seconds.

The configuration subtree includes:

- **Reset Total Counters:** resets the 'total' (see below) objects in all the MIB's tables if they are defined.
- **Attributes subtrees:** a number of subtrees in which scalars are used to configure the high and low thresholds for relevant tables.

The Data subtree consists of monitored data and statistics:

- **Time From Start Of Interval object:** GETs the time in seconds from the beginning of the current interval.
- **Data tables:** all have similar structure. Not all possible columns appear in all of them. The specific structure of a table (i.e. what columns are defined) is parameter specific. The only column that always appears is the interval column. The information in each column is a statistical attribute of the parameter being looked at.

Note: When an attribute value is -1, it means that the attribute isn't relevant at that point of time.

The columns are:

- Table specific index – table key.
- Interval – index, 0,1,2 – table key.
- Val – value of gauge or counter. This is the snapshot view of current device activity.
    - Counter – cumulative, only increases in value.
    - Gauge – fluctuates in value, value increases and decreases.
- Average – within the period length.
- Max – gauge high water mark.
- Min - gauge low water mark.
- Volume – number of times gauge or counter was updated, indicating the volume of change. For example:
    - For a trunk utilization element, the volume indicates how many calls were made and released.
    - For the Ethernet connection status element, the volume indicates how many network connections and disconnections occurred.
- TimeBelowLowThreshod – Percent of interval time for which the gauge is below the determined low threshold.
- TimeAboveHighThreshod – Percent of interval time for which the gauge is above the determined high threshold.
- TimeBetweenThresholds – Percent of interval time for which the gauge is between thresholds.
- FullDayAverage – 24 hour average.
- Total – relevant when using counters. Sums all counter values so far. It resets only once every 24 hours.
- StateChanges – the number of times a state (mostly active/non-active) was toggled.

The log trap, acPerformanceMonitoringThresholdCrossing (non-alarm) is sent out every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it returns to under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

Expansions for the different MIBs.

- **acPMMedia:** Consists of data related to voice, DSPs coders etc. This MIB includes the following parameters:
    - Number of active DSP channels
    - Channels used for each coder
    - Discarded packets in robust RTP filter
    - Media Networking subtree - an array of packet behavior parameters such as delay, jitter, transmitted/received and lost RTP bytes and packets.
    - Media Networking Aggregated subtree - displays similar data only for the entire device and includes TDM-IP and IP-IP calls.
    - Channel Utilization subtree - parameters regarding channel use by fax, modem, TDM-IP calls, RTP, SRTP, multicast source and modem relay.

- Streaming Cache subtree - hit count, miss count and server request count.

- **acPMControl:** Control Protocol related monitoring is divided into three groups – MEGACO, MGCP and SIP. The MIB includes the following parameters:
  - CP Connection subtree – general for all three control protocols. Its parameters include connection lifetime/state, counters for commands, retransmissions, active contexts, command success/failure and process time, transaction processing time and call attempts.
  - The remaining three subtrees are self-explanatory and are CP specific.
- **acPMAnalog:** Analog channels statistics - one table only (offhook state).
- **acPMPSTN:** All statistics in this MIB are per trunk:
  - Number of active channels.
  - Trunk activity.
  - Number of channels that are in/out of service and in maintenance.
- **acPMSystem:** This detailed MIB is for general (system related) monitoring:
  - IP connection.
  - Discarded UDP packets due to unknown port.
  - System Net Utils subtree – transmitted/received bytes/packets, discarded packets.
  - System Network subtree – DHCP response time/request count. STUN related statistics.
  - IPsec security associations. (Applicable only to MP, Mediant 1000, Mediant 2000, Mediant 3000)
  - System Multicast subtree – multicast IP packets received, multicast IP packets conveying UDP payload packets received/rejected, IGMP packets/general-queries/specific-queries received, IGMP membership-report/leave-group sent messages.
  - System Congestion subtree – congestion state for general resources, DSP resources, IP resources, conference resources. (ATM resources table is obsolete).
  - System NFS subtree – NFS related parameters.
  - System MSBG subtree – includes received good/bad octets, received undersized/oversized/discarded packets, received MAC errors, received FSC error packets, transmitted octets/packets/collisions/late-packets.
- **acPMMediaServer:** (Applicable to the 3000/6310/8410 devices) The Media Server related data is divided into four subtrees:
  - IVR subtree – play requests, play progress/duration/collect/collect-in-progress/collect-duration/record/record-in-progress/record-duration, digit-collect requests, digit-collect in-progress/duration.
  - BCT subtree – BCT contexts, BCT in-progress/duration.
  - Conference subtree – conference calls, conference in-progress/duration.
  - Trunk Test subtree – trunk test requested, trunk tests in-progress/duration.

9.4 Traps and Alarms

AudioCodes supports standard traps and proprietary traps. Most of the proprietary traps are alarm traps, that is, they can be raised and cleared. Thus, they are referred to as *alarm traps*. All the standard traps are non-alarm traps, referred to as *log traps*. The complete list of all supported traps is mentioned in previous subsections.

The proprietary traps are defined under the acBoardTrapDefinitions subtree.

The standard MIB traps supported include the following:

- coldStart
- authenticationFailure
- linkDown
- linkup
- dsx1LineStatusChange
- rtcpXrVoipThresholdViolation
- dsx3LineStatusChange
- entConfigChange

This subsection describes the device's configuration so that traps are sent out to user-defined managers under SNMPv2c or SNMPv3. It continues with an explanation on the 'carrier grade alarm' abilities and usage.

9.4.1 Device Configuration

For a device to send out traps to specified managers the most basic configuration are the trap targets. More advanced configuration includes the Trap Community String or traps over SNMPv3.

- Destination IP address and port (see Basic SNMP Configuration Setup)
- Trap Community String: The default Trap Community String is 'trapuser'. There is only 1 for the entire device. It can be configured via ini file, SNMP or Web:
    - INI file: SNMPTRAPCOMMUNITYSTRING = <your community string here>.
    - SNMP: add a new community string to the snmpCommunityTable. To associate the traps to the new Community String change the snmpTargetParamsSecurityName in the snmpTargetParamsTable so it coincides with the snmpCommunitySecurityName object. If you wish, you can remove the older Trap Community String from snmpCommunityTable (however, it is not mandatory).
    - Web: under the 'Management' tab, choose 'Management Settings' in the 'Management Settings' menu. On the page, click the **SNMP Community String** arrow to display the table. Use the **Submit** button to apply your configuration. You can't delete the Trap Community String, only modify its value.

- SNMPv3 Settings: When using SNMPv3 settings it is important to note that by default the trap configuration remains such that the traps are sent out in SNMPv2c mode. To have traps sent out in SNMPv3, you can use either ini file or SNMP:

  - INI file: amongst the SNMPv3 users ensure that you also define a trap user (the value of 2 in the SNMPUsers_Group indicates the trap user). For example: you can have the SNMP users table defined with a read-write user, ‘rwmd5des’ with MD5 authentication and DES privacy, along with a trap user, ‘tmd5no’ with SHA authentication and DES privacy:

    ```
    [ SNMPUsers ]
    FORMAT SNMPUsers_Index = SNMPUsers_Username,
    SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol,
    SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group;
    SNMPUsers 1 = rwmd5des, 1, 1, myauthkey, myprivkey, 1;
    SNMPUsers 2 = tshades, 2, 1, myauthkey, myprivkey, 2
    [ \SNMPUsers ]
    ```

Notes:

- If you define a trap user only, the device runs in SNMPv3 mode but will not be accessible as there are no defined read-write or even read-only users.
- If you define non-default community strings (SNMPv2c), you need to access the device via SNMPv2c.

Along with this configuration, you also need to associate the trap targets (managers) with the user:

```
SNMPMANAGERTRAPUSER_x=tshades
```

where *x* is the target index and can be between 0 and 4.

Any targets that are defined in the ini file where this last parameter isn’t defined, receives SNMPv2c traps.

  - SNMP: change snmpTargetAddrParams object to the user of your choice adding the letters ‘usm’ as prefix (ensure it’s a trap user). For example, the ‘tshades’ user should be added as ‘usmtshades’.

9.4.2 Carrier Grade Alarm (CGA)

A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element management system outages, network outages, and transport mechanism such as SNMP over UDP.

A carrier-grade alarm system is characterized by the following:

- The device allows a manager to determine which alarms are currently active in the device. That is, the device maintains an active alarm table.
- The device allows a manager to detect lost alarms and clear notifications (sequence number in trap, current sequence number MIB object).
- The device allows a manager to recover lost alarm raise and clear notifications (maintains a log history).
- The device sends a cold start trap to indicate that it is starting. This allows the manager to synchronize its view of the device's active alarms.

When the SNMP alarm traps are sent, the carrier-grade alarm system does not add or delete alarm traps as part of the feature. This system provides the mechanism for viewing history and current active alarm information.

As part of CGA, the device supports the following:

- **Active Alarm Table:** The device maintains an active alarm table to allow an EMS to determine which alarms are currently active in the device. Two views of the active alarm table are supported by the agent:
    - acActiveAlarmTable in the proprietary AcAlarm MIB (this is a simple, one-row per alarm table that is easy to view with a MIB browser)
    - alarmActiveTable and alarmActiveVariableTable in the IETF standard AcAlarm MIB (rooted in the MIB tree)
- **Alarm History:** The device maintains a history of alarms that have been raised and traps that have been cleared to allow an EMS to recover any lost raised or cleared traps. Two views of the alarm history table are supported by the agent:
    - acAlarmHistoryTable in the proprietary AcAlarm MIB (this is a simple, one-row per alarm table that is easy to view with a MIB browser)
    - nlmLogTable and nlmLogVariableTable in the standard NOTIFICATION-LOG-MIB

Reader's Notes

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Document #: LTRT-52418