Reference Guide

AudioCodes Media Gateways & Session Border Controllers (SBC)

SNMP Reference Guide

Version 7.2

HD VoIP Sounds Better

AudioCodes

Table of Contents

List of Tables

Notice

This document describes SNMP support for AudioCodes SIP-based Voice over IP (VoIP) devices.

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.

Some features mentioned in this document may not be supported for every product in this software version. You must consult the Release Notes for this version to verify whether your product is supported and/or if specific features are supported for your product. In cases where there are discrepancies between this Reference Guide and the Release Notes, the information in the Release Notes supersedes that in this Reference Guide.

Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/support.

Date Published: September-11-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 are trademarks or registered trademarks of AudioCodes Limited All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
52374	Initial document release for Version 7.2.
52378	Typos.

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 Web site at http://www.audiocodes.com/downloads.

1 Introduction

This document provides you with supplementary information on Simple Network Management Protocol (SNMP) based management for 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:

- **Refer to the *Release Notes 7.2* for products released in Version 7.2**.
- The SNMP MIB manual is supplied in the Software Release Package delivered with your product.
- Using AudioCodes' Element Management System (EMS) 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 is not included in the device's supplied package. Contact AudioCodes for detailed information on AudioCodes' EMS solution for large VoIP deployments.

1.1 Document Convention for Product Names

Throughout this guide, 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
Analog Series	Analog interfaces (FXS and FXO): ▪ MediaPack ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC
Digital Series	Digital PSTN interfaces: ▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC
SBC Series	SBC application support: ▪ Mediant 500 E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 9000 SBC ▪ Mediant SE SBC ▪ Mediant VE SBC

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.
- **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.
- **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 Series):
  - 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
- **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**

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 Series)
- **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
- **acSysModuleTable**
- **acIPMediaChannelsresourcesTable** - IPMedia channels information such as Module ID and DSP Channels Reserved (Applicable only to Mediant 1000)
- **acPSTN MIB** (Applicable only to Digital Series)
- **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 Series: 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 19 characters that can include only the following:

- Upper- and lower-case letters (a to z, and A to Z)
- Numbers (0 to 9)
- Hyphen (-)
- Underline (_)

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 26)
- SNMP (see "Configuring Trap Managers via SNMP" on page 27)

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.

➢ **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 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: 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
- **ds1(18):** DS1-MIB
- **voiceFXO(101):** Voice Foreign Exchange Office. (Applicable only to Mediant 1000.)
- **voiceFXS(102):** Voice Foreign Exchange Station. (Applicable only to Mediant 1000.)

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

For each interface type, the following objects are supported:

4.2.1 Ethernet Interface

Table 4-1: Ethernet Interface

ifTable & ifXTable	Value
ifIndex	Constructed as defined in the device's Index format.
ifDescr	Ethernet interface.
ifType	ethernetCsmacd(6)
ifMtu	1500
ifSpeed	acSysEthernetFirstPortSpeed in bits per second (applicable only to Mediant 1000) 0 since it's GBE - refer to ifHighSpeed (applicable only to Mediant 3000 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

ifTable & ifXTable	Value
	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 Mediant 3000) 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.
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	▪ 1000 (Mediant 3000 / Mediant 4000) ▪ 10 or 100 according to acSysEthernetFirstPortSpeed (Mediant 1000)
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.

4.2.2 DS1 Interface

Note: Applicable only to to Digital PSTN.

Table 4-2: DS1 Digital Interface

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.
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.

4.2.3 BRI Interface

Note: Applicable to the Mediant 1000.

Table 4-3: BRI Interface

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

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.

This page is intentionally left blank.

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 Series.)
- **acPMPSTN:** PSTN-related monitoring such as channel use, trunk utilization. (Applicable only to Digital Series.)
- **acPMSystem:** general (system-related) monitoring.

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. To enable this functionality, set the ini file parameter, PM_EnableThresholdAlarms to 1.

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

6.2 SNMP Performance Monitoring MIBs

The following sections show the performance monitoring SNMP MIBs.

Note: The tables in this section use check marks "√" and crosses "x" to indicate whether the MIB property is supported or not supported, respectively.

6.2.1 IP Network Interface

The SNMP MIBs below provide performance monitoring for the IP network interface.

Table 6-1: Performance Monitoring MIBs for IP Network Interface

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMNetUtilKBytesTable											
Indicates the number of Kbytes (1000 bytes) received and transmitted on the interface (Index 0 is transmit; Index 1 is receive), including those received in error, from the beginning of the current collection interval as indicated by the time interval. EMS parameter name: Number of Incoming / Outgoing Kbytes ▪ High threshold: acPMNetUtilsAttributesKBytesHighThreshold (1.3.6.1.4.1.5003.10.11.1.33.1) ▪ Low threshold: acPMNetUtilsAttributesKBytesLowThreshold (1.3.6.1.4.1.5003.10.11.1.33.2)	G	15	✓	✓	✓	✓	✓	✓	✓	x	x

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMNetUtilPacketsTable											
Indicates the number of incoming and outgoing packets from the interface (Index 0 is transmit; Index 1 is receive), from the beginning of the current collection interval as indicated by time Interval. EMS parameter name: Number of Outgoing / Incoming Pkts. ▪ High threshold: acPMNetUtilsAttributesPacketsHighThreshold (1.3.6.1.4.1.5003.10.11.1.33.3) ▪ Low threshold: acPMNetUtilsAttributesPacketsLowThreshold (1.3.6.1.4.1.5003.10.11.1.33.4)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMNetUtilDiscardedPacketsTable											
Indicates the 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.	C	15	✓	×	×	×	×	×	×	×	×

6.2.2 Media Realm

The SNMP MIBs below provide performance monitoring statistics for Media Realms.

Table 6-2: Performance Monitoring MIBs for Media Realms

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
AcPMMediaRealmPacketLossRxTable											
Indicates the received RTP packet loss (reported by RTCP) per Media Realm.	G	15	×	✓	✓	✓	✓	✓	✓	50	30
AcPMMediaRealmPacketLossTxTable											
Indicates the transmitted RTP packet loss (reported by RTCP) per Media Realm.	G	15	×	✓	✓	✓	✓	✓	✓	50	30
AcPMMediaRealmBytesTxTable											
Indicates the number of bytes received in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmBytesTxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.1) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmBytesTxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.2)	G	15	×	✓	✓	✓	✓	✓	✓	1500000	1000000
AcPMMediaRealmBytesRxTable											
Indicates the number of bytes received in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmBytesRxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.3) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmBytesRxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.4)	G	15	×	✓	✓	✓	✓	✓	✓	1500000	1000000
acPMMediaRealmPacketsTxTable											
Indicates the number of media packets sent in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmPacketsTxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.5) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmPacketsTxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.6)	G	15	×	✓	✓	✓	✓	✓	✓	7500	6000
acPMMediaRealmPacketsRxTable											
Indicates the number of media packets received in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmPacketsRxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.7) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmPacketsRxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.8)	G	15	×	✓	✓	✓	✓	✓	✓	7500	6000

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
AcPMMediaRealmVERealmPacketDelayTable											
Indicates the packet delay in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesVERealmPacketDelayHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.9) ▪ Low threshold: acPMMediaRealmAttributesVERealmPacketDelayLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.10)	G	15	×	✓	✓	✓	×	×	×	150	120
AcPMMediaRealmVERealmPacketJitterTable											
Indicates the packet jitter in RTCP data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesVERealmPacketJitterHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.11) ▪ Low threshold: acPMMediaRealmAttributesVERealmPacketJitterLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.12)	G	15	✓	✓	✓	✓	×	×	×	150	120
acPMMediaRealmRealmMOSTable											
Indicates the MOS quality in RTCP-XR data, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesRealmMOSHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.13) ▪ Low threshold: acPMMediaRealmAttributesRealmMOSLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.14)	G	15	✓	✓	✓	✓	×	×	×	50	10
acPMMediaRealmBwRxTable											
Indicates the average bandwidth for Rx bytes, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmBwRxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.15) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmBwRxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.16)	G	15	✓	✓	✓	✓	×	×	×	1500000	0
acPMMediaRealmBwTxTable											
Indicates the average bandwidth for Tx bytes, per Media Realm. ▪ High threshold: acPMMediaRealmAttributesMediaRealmBwTxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.17) ▪ Low threshold: acPMMediaRealmAttributesMediaRealmBwTxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.18)	G	15	✓	✓	✓	✓	×	×	×	1500000	0

6.2.3 VoIP Calls

The SNMP MIBs below provide performance monitoring statistics for VoIP calls.

Note: The MIBs are not applicable to the MediaPack Series.

Table 6-3: Performance Monitoring MIBs for VoIP Calls

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMChannelsPerCoderTable											
Indicates the number of active channels per coder, where Index denotes the coder (Index: 0=G711, 1=G723, 2=G728, 3=G729a, 4=G729e, 5=AMR etc.). ▪ High threshold: acPMCodersAttributesChannelsPerCoderHighThreshold (1.3.6.1.4.1.5003.10.7.1.32.1) ▪ Low threshold: acPMCodersAttributesChannelsPerCoderLowThreshold (1.3.6.1.4.1.5003.10.7.1.32.2)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModuleRTPPacketLossRxTable											
Indicates the Rx RTP packet loss (reported by RTCP), during the time Interval. EMS parameter name: Rx RTP Packet Loss. ▪ High threshold: acPMNetworkingAttributesModuleRTPPacketLossRxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.17) ▪ Low threshold: acPMNetworkingAttributesModuleRTPPacketLossRxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.18)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModuleRTPPacketLossTxTable											
Indicates the Tx RTP packet loss (reported by RTCP), during the time Interval. EMS parameter name: Tx RTP Packet Loss. ▪ High threshold: acPMNetworkingAttributesModuleRTPPacketLossTxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.19) ▪ Low threshold: acPMNetworkingAttributesModuleRTPPacketLossTxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.20)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMModulePacketDelayTable											
Indicates the RTP packet delay during the collection time interval. EMS parameter name: RTP delay. ▪ High threshold: acPMNetworkingAttributesPacketDelayHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.1) ▪ Low threshold: acPMNetworkingAttributesPacketDelayLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.2)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModulePacketJitterTable											
Indicates the RTP packet jitter during the collection time interval. EMS parameter name: RTP jitter. ▪ High threshold: acPMNetworkingAttributesPacketJitterHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.3) ▪ Low threshold: acPMNetworkingAttributesPacketJitterLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.4)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModuleRTPBytesRxTable											
Indicates the Tx RTP bytes during the collection time interval. EMS parameter name: Rx RTP Bytes. ▪ High threshold: acPMNetworkingAttributesRTPBytesRxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.7) ▪ Low threshold: acPMNetworkingAttributesRTPBytesRxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.8)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModuleRTPBytesTxTable											
Indicates the Rx RTP bytes during the collection time interval. EMS parameter name: Tx RTP Bytes. ▪ High threshold: acPMNetworkingAttributesRTPBytesTxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.5) ▪ Low threshold: acPMNetworkingAttributesRTPBytesTxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.6)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMModuleRTPPacketsRxTable											
Indicates the Rx RTP packets during the collection time interval. EMS parameter name: Rx RTP Packets. ▪ High threshold: acPMNetworkingAttributesRTPPacketsRxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.11) ▪ Low threshold: acPMNetworkingAttributesRTPPacketsRxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.12)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMModuleRTPPacketsTxTable											
Indicates the Tx RTP Packets during the collection time interval. EMS parameter name: Tx RTP Packets. ▪ High threshold: acPMNetworkingAttributesRTPPacketsTxHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.9) ▪ Low threshold: acPMNetworkingAttributesRTPPacketsTxLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.10)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

6.2.4 SIP Messages

The SNMP MIB below provides performance monitoring for SIP messages.

Table 6-4: Performance Monitoring MIBs for SIP Messages

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPActiveSIPTransactionsPerSecondTable											
Indicates the number of active incoming and outgoing SIP transactions (e.g., INVITE message) per second. ▪ High threshold: acPMSipAttributesActiveSIPTransactionsPerSecondHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.35) ▪ Low threshold: acPMSipAttributesActiveSIPTransactionsPerSecondLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.36)	G	15	✓	×	×	×	×	×	×	0	0
acPMSIPIPGroupInviteDialogsTable											
Indicates the number of INVITE dialogs per IP Group. ▪ High threshold: acPMSipAttributesIPGroupINVITEDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.25) ▪ Low threshold: acPMSipAttributesIPGroupINVITEDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.26)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

6.2.5 Gateway Application

Note: The section is applicable only to products supporting Tel (PSTN) interfaces.

6.2.5.1 SIP IP-to-Tel and Tel-to-IP Calls

The SNMP MIBs below provide performance monitoring for SIP IP-to-Tel and Tel-to-IP calls.

Note: In MIB tables, Index 0 indicates Tel-to-IP calls and Index 1 indicates IP-to-Tel calls.

Table 6-5: Performance Monitoring MIBs for SIP IP-to-Tel and Tel-to-IP Calls

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPAttemptedCallsTable											
Indicates the number of attempted calls (Index 1) during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Call Attempts	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPCallDurationTable											
Indicates the call duration of established calls during last interval. EMS parameter name: IP to Tel / Tel to IP Average Call Duration [sec]calls. ▪ High threshold: acPMSipAttributesCallDurationHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.1) ▪ Low threshold: acPMSipAttributesCallDurationLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.2)	G/ C	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
acPMSIPNoMatchCallsTable											
Indicates the number of calls that failed due to mismatched media server capabilities for calls, during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Matched Capabilities.	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPBusyCallsTable											
Indicates the number of calls that failed as a result of a busy line, during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Calls Terminated due to a Busy Line.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPNoAnswerCallsTable											
Indicates the number of calls that weren't answered during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Calls Terminated due to No Answer.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPNoRouteCallsTable											
Indicates the number of calls whose destinations weren't found during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Route.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPFailCallsTable											
This counter is incremented as a result of calls that fail due to reasons not covered by the other counters during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Failed Calls due to Other reasons.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPEstablishedCallsTable											
Indicates the number of established calls during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Established Calls.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPFaxAttemptedCallsTable											
Indicates the number of attempted fax calls.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPFaxSuccessCallsTable											
Indicates the number of successfully established fax calls.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPForwardedCallsEntry											
Indicates the number of calls that were terminated due to a call forward during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Calls Terminated due to Forward.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPNoResourcesCallsTable											
Indicates the number of calls that failed due to unavailable resources or a media server lock during last interval. EMS parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Resources.	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPTel2IPTrunkEstablishedCallsTable											
Indicates the current number of established calls pertaining to a trunk for Tel-to-IP calls.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIP2TelTrunkEstablishedCallsTable											
Indicates the current number of established calls pertaining to a trunk for IP-to-Tel calls.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPTel2IPTrunkGroupEstablishedCallsTable											
Indicates the current number of established calls pertaining to a Trunk Group for Tel-to-IP calls.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIP2TelTrunkGroupEstablishedCallsTable											
Indicates the current number of established calls pertaining to a Trunk Group for IP-to-Tel calls.	G	15	✓	×	×	×	×	×	×	×	×

6.2.5.2 Trunks

The SNMP MIBs below provide performance monitoring for trunks.

Note: The MIBs apply only to the Digital Series.

Table 6-6: Performance Monitoring MIBs for Trunks

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
dsx1IntervalTable											
The DS1 Interval Table contains various statistics collected by each DS1 Interface over the previous 24 hours. The past 24 hours are broken into 96 completed 15 minute intervals. Each row in this table represents one such interval (identified by dsx1IntervalNumber) for one specific instance (identified by dsx1IntervalIndex: ▪ dsx1IntervalESs: Number of Errored Seconds (EMS parameter name: Trunk Errored Seconds) ▪ dsx1IntervalCSSs: Number of Controlled Slip Seconds (EMS parameter name: Trunk Controlled Slip Seconds) ▪ dsx1IntervalPCVs: Number of Path Coding Violations (EMS parameter name: Trunk Path Coding Violations) ▪ dsx1IntervalBESs: Number of Bursty Errored Seconds (EMS parameter name: Trunk Bursty Errored Seconds) ▪ dsx1TotalESs: Call duration per timeslot and E1 since last clear (EMS parameter name: Trunk Calls Duration) ▪ dsx1TotalCSSs: Number of Controlled Slip Seconds encountered by a DS1 interface in the previous 24 hour interval (EMS parameter name: Trunk Controlled Slip Seconds) ▪ dsx1TotalPCVs: Number of Path Coding Violations encountered by a DS1 interface in the previous 24 hour interval (EMS parameter name: Trunk Path Coding Violations) ▪ dsx1TotalBESs: Number of Bursty Errored Seconds encountered by a DS1 interface in the previous 24 hour interval (EMS parameter name: Trunk Bursty Errored Seconds)	G	15	✓	×	×	×	×	×	×	×	×

6.2.5.3 Trunk Groups

The SNMP MIBs below provide performance monitoring for trunk groups.

Note: The MIBs are applicable only to the Digital Series.

Table 6-7: Performance Monitoring MIBs for Trunk Groups

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
AcPMSIPTrunkGroupNoResourcesCallsTable											
Indicates the number of calls that could not be established due to unavailable device resources (e.g., no free channels) per Trunk Group. ▪ High threshold: acPMSipAttributesTrunkGroupNoResourcesCallsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.7) ▪ Low threshold: acPMSipAttributesTrunkGroupNoResourcesCallsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.8)	C	15	✓	×	×	×	×	×	×	0	0
acPMSIPTrunkGroupCallDurationTable											
Indicates the average call duration (in seconds) of calls per trunk group. ▪ High threshold: acPMSipAttributesCallDurationHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.1) ▪ Low threshold: acPMSipAttributesCallDurationLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.2	G	15	✓	✓	✓	✓	×	×	×	0	0
acPMSIPTrunkGroupUtilizationTable											
Indicates the number of channels 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 that if a trunk is in LOF state, this MIB counts only the channels that are used. ▪ High threshold: acPMSipAttributesTrunkGroupUtilizationHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.3) ▪ Low threshold: acPMSipAttributesTrunkGroupUtilizationLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.4)	G	15	✓	✓	✓	✓	✓	✓	✓	2016	0

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMSIPTrunkGroupPercentageUtilizationTable											
Indicates the percentage (%) of channels currently in use (busy) per trunk group. The device supports configuration of a busy channel threshold per trunk group, which when exceeded, sends an SNMP alarm. For example, if a device has 200 voice channels and the threshold is set to 90%, if the number of concurrent busy channels exceeds 90% (i.e., 180 channels), this threshold alarm is sent. ▪ High threshold: acPMSipAttributesTrunkGroupPercentageUtilization HighThreshold (1.3.6.1.4.1.5003.10.8.1.34.5) ▪ Low threshold: acPMSipAttributesTrunkGroupPercentageUtilization LowThreshold (1.3.6.1.4.1.5003.10.8.1.34.6)	G	15	✓	✓	✓	✓	✓	✓	✓	95	85
acPMSIPTrunkGroupAllTrunksBusyTable											
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 that trunks that are out of service or not configured (set to **NONE**) are considered "busy" in this calculation.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPTrunkGroupAllTrunksBusyPercentageTable											
Indicates the percentage (%) of time within a 15-minute polling interval, that all channels in a specific trunk group were busy simultaneously. This measurement is sent only at the end of the interval (beginning of the current interval), so each measurement reflects the previous interval. For example, assume that all trunks of a trunk group were busy for 6 minutes during an interval. The MIB will send a measurement of 40% (i.e., 6 minutes / 15 minutes * 100). In other words, all trunks of the trunk group were simultaneously busy for 40% of the time during this 15-minute interval. ▪ High threshold: acPMSipAttributesTrunkGroupAllTrunksBusyPercentageHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.33) ▪ Low threshold: acPMSipAttributesTrunkGroupAllTrunksBusyPercentageLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.34)	G	15	✓	×	×	×	×	×	×	0	0
acPMTrunkUtilizationTable											
Indicates the number of busy channels on a specific E1 / T1 trunk. A busy channel is when the Physical DS0 Termination isn't in Null context or OOS. ▪ High threshold: acPMTrunkUtilizationAttributesHighThreshold (1.3.6.1.4.1.5003.10.10.1.31.1) ▪ Low threshold: acPMTrunkUtilizationAttributesLowThreshold (1.3.6.1.4.1.5003.10.10.1.31.2)	G	15	✓	✓	✓	✓	✓	✓	✓	30	25

6.2.6 SBC Application

6.2.6.1 SBC Sessions

The SNMP MIBs below provide performance monitoring for SBC (Session Border Controllers) sessions. For MIBs that have low and high thresholds, if a threshold is crossed the device sends the acPerformanceMonitoringThresholdCrossing trap (see Section 7.5.5 on page 109).

Table 6-8: Performance Monitoring MIBs for SBC Sessions

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPSBCAttemptedCallsTable											
Indicates the number of attempted SBC calls. ▪ High threshold: acPMSipAttributesSBCAttemptedCallsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.37) ▪ Low threshold: acPMSipAttributesSBCAttemptedCallsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.38)	C	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPSBCEstablishedCallsTable											
Indicate the number of established SBC calls. ▪ High threshold: acPMSipAttributesSBCEstablishedCallsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.39) ▪ Low threshold: acPMSipAttributesSBCEstablishedCallsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.40)	C	15	✓	×	×	×	×	×	×	0	0
acPMSBCMediaLegsTable											
Indicates the number of media (RTP) session resources currently utilized. ▪ High threshold: acPMSbcMediaLegsHighThreshold (1.3.6.1.4.1.5003.10.8.1.36.50) ▪ Low threshold: acPMSbcMediaLegsLowThreshold (1.3.6.1.4.1.5003.10.8.1.36.51)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSBCTranscodingSessionsTable											
Indicates the number of transcoding sessions. ▪ High threshold: acPMSbcSBCTranscodingSessionsHighThreshold (1.3.6.1.4.1.5003.10.8.1.36.52) ▪ Low threshold: acPMSbcSBCTranscodingSessionsLowThreshold (1.3.6.1.4.1.5003.10.8.1.36.53)	C	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

6.2.6.2 SBC Calls per IP Group

The SNMP MIB below provides performance monitoring for SBC calls per IP Group.

Table 6-9: Performance Monitoring MIBs for SBC Sessions per IP Group

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSIPGroupInCallEstablishedDurationTable											
Indicates the call duration of the last incoming established SBC call per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutCallEstablishedDurationTable											
Indicates the call duration of the last outgoing established SBC call per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAttemptedCallsTable											
Indicates the number of attempted incoming SBC calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAttemptedSubscribeDialogsTable											
Indicates the number of attempted incoming SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAttemptedOtherDialogsTable											
Indicates the number of attempted incoming dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAttemptedCallsTable											
Indicates the number of attempted outgoing SBC calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAttemptedSubscribeDialogsTable											
Indicates the number of attempted outgoing SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAttemptedOtherDialogsTable											
Indicates the number of attempted outgoing dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupRoutingFailedCallsTable											
Indicates the number of failed call routing per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupRoutingFailedSubscribeDialogsTable											
Indicates the number of failed call routing of SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupRoutingFailedOtherDialogsTable											
Indicates the number of failed call routing of all dialogs other than SUBSCRIBE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAdmissionFailedCallsTable											
Indicates the number of failed incoming dialogs due to Admission Control rules per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSBCIPGroupInAdmissionFailedSubscribeDialogsTable											
Indicates the number of failed incoming SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAdmissionFailedOtherDialogsTable											
Indicates the number of failed incoming dialogs other than SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAdmissionFailedCallsTable											
Indicates the number of failed outgoing dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAdmissionFailedSubscribeDialogsTable											
Indicates the number of failed outgoing SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAdmissionFailedOtherDialogsTable											
Indicates the number of failed outgoing dialogs other than SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInNoResourcesCallsTable											
Indicates the number of incoming call resource allocation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutNoResourcesCallsTable											
Indicates the number of outgoing call resource allocation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInNoMatchCallsTable											
Indicates the number of incoming call media negotiation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutNoMatchCallsTable											
Indicates the number of outgoing call media negotiation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInBusyCallsTable											
Indicates the number of incoming busy calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutBusyCallsTable											
Indicates the number of outgoing busy calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInNoAnswerCallsTable											
Indicates the number of incoming no-answer calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutNoAnswerCallsTable											
Indicates the number of outgoing no-answer calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSBCIPGroupInForwardedCallsTable											
Indicates the number of incoming forwarded calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInForwardedSubscribeDialogsTable											
Indicates the number of incoming forwarded SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInForwardedOtherDialogsTable											
Indicates the number of incoming forwarded dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutForwardedCallsTable											
Indicates the number of outgoing forwarded calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutForwardedSubscribeDialogsTable											
Indicates the number of outgoing forwarded SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutForwardedOtherDialogsTable											
Indicates the number of outgoing forwarded dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInGeneralFailedCallsTable											
Indicates the number of incoming calls that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInGeneralFailedSubscribeDialogsTable											
Indicates the number of incoming SUBSCRIBE dialogs that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInGeneralFailedOtherDialogsTable											
Indicates the number of incoming dialogs other than SUBSCRIBE and INVITE that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutGeneralFailedCallsTable											
Indicates the number of outgoing calls that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutGeneralFailedSubscribeDialogsTable											
Indicates the number of outgoing SUBSCRIBE dialogs that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutGeneralFailedOtherDialogsTable											
Indicates the number of outgoing dialogs other than SUBSCRIBE and INVITE that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInEstablishedCallsTable											
Indicates the number of incoming established calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold	LowThreshold
acPMSBCIPGroupInEstablishedSubscribeDialogsTable											
Indicates the number of incoming established SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInEstablishedOtherDialogsTable											
Indicates the number of incoming established dialogs other than SUBSCRIBE and INVITE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutEstablishedCallsTable											
Indicates the number of outgoing established calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutEstablishedSubscribeDialogsTable											
Indicates the number of outgoing established SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutEstablishedOtherDialogsTable											
Indicates the number of outgoing established dialogs other than SUBSCRIBE and INVITE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupInAbnormallyTerminatedCallsTable											
Indicates the number of incoming calls that were abnormally terminated per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAbnormallyTerminatedCallsTable											
Indicates the number of outgoing calls that were abnormally terminated per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSBCIPGroupOutAbnormallyTerminatedCallsTable											
Indicates the number of outgoing calls that were abnormally terminated per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

6.2.6.3 SBC Admission Control

The SNMP MIBs below provide performance monitoring statistics for SBC Admission Control. Performance monitoring is performed per:

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

Performance monitoring is provided by the acGateway MIB.

For MIBs that have low and high thresholds, if a threshold is crossed the device sends the acPerformanceMonitoringThresholdCrossing trap (see Section 7.5.5 on page 109).

Note: This section applies only to the SBC Series.

Table 6-10: Performance Monitoring MIBs for SBC Call Admission

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMSIPSRDDialogsTable											
Indicates the number of all dialogs currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPSRDInviteDialogsTable											
Indicates the number of all calls (initiated by SIP:INVITE) currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPSRDSubscribeDialogsTable											
Indicates the number of all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPSRDOtherDialogsTable											
Indicates the number of all dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIPGroupDialogsTable											
Indicates the number of all dialogs currently being handled by the SBC per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIPGroupSubscribeDialogsTable											
Indicates the number of all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC, per IP Group. ▪ High threshold: acPMSipAttributesIPGroupSubscribeDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.27) ▪ Low threshold: acPMSipAttributesIPGroupSubscribeDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.28)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPIPGroupOtherDialogsTable											
Indicates the number of all other dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIPGroupInOtherDialogsTable											
Indicates the number of all incoming dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
acPMSIPIPGroupOutOtherDialogsTable											
Indicates the number of all outgoing dialogs other than INVITE and SUBSCRIBE (initiated by SIP:REGISTER) currently being handled by the SBC per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMSIPIPGroupInInviteDialogsTable											
Indicates the number of incoming calls (SIP INVITE) per IP Group. ▪ High threshold: acPMSipAttributesIPGroupInInviteDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.13) ▪ Low threshold: acPMSipAttributesIPGroupInInviteDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.14)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPIPGroupInSubscribeDialogsTable											
Indicates the number of incoming SUBSCRIBE dialogs per IP Group. ▪ High threshold: acPMSipAttributesIPGroupInSubscribeDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.15) ▪ Low threshold: acPMSipAttributesIPGroupInSubscribeDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.16)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPIPGroupOutInviteDialogsTable											
Indicates the number of outgoing calls (SIP INVITE) per IP Group. ▪ High threshold: acPMSipAttributesIPGroupOutInviteDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.19) ▪ Low threshold: acPMSipAttributesIPGroupOutInviteDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.20)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPIPGroupOutSubscribeDialogsTable											
Indicates the number of outgoing SUBSCRIBE dialogs per IP Group. ▪ High threshold: acPMSipAttributesIPGroupOutSubscribeDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.21) ▪ Low threshold: acPMSipAttributesIPGroupOutSubscribeDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.22)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSIPIPGroupOutDialogsTable											
Indicates the number of outgoing dialogs per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
acPMSIPInvitedDialogsTable											
Indicates the number of currently active INVITE dialogs. Note that the count considers each leg (not sessions, which consist of two legs). ▪ High threshold: acPMSipAttributesInvitedDialogsHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.29) ▪ Low threshold: acPMSipAttributesInvitedDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.30)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMSIPSubscribeDialogTable											
Indicates the number of SUBSCRIBE dialogs. ▪ High threshold: acPMSipAttributesInvitedSubscribeDialogHighThreshold (1.3.6.1.4.1.5003.10.8.1.34.31) ▪ Low threshold: acPMSipAttributesInvitedSubscribeDialogLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.32)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
acPMSBCRegisteredUsersTable											
Indicates the number of registered users. Increments for each registered user and decrements when they deregister. ▪ High threshold: acPMSbcRegisteredUsersHighThreshold (1.3.6.1.4.1.5003.10.8.1.36.48) ▪ Low threshold: acPMSbcRegisteredUsersLowThreshold (1.3.6.1.4.1.5003.10.8.1.36.49)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

6.2.6.4 Call Quality of Service

The SNMP MIBs below provide performance monitoring statistics for SBC Quality of Service. Performance monitoring is performed per SRD, IP Group or global (all). Major and Minor thresholds can be configured for each performance monitoring metric through the Web interface (only). If the thresholds are crossed, an SNMP alarm is raised (see acASRThresholdAlarm, AcNERThresholdAlarm, and acACDThresholdAlarm).

Note: This section applies only to the SBC Series.

Table 6-11: Performance Monitoring MIBs for SBC Call Quality of Service

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
PM_gwSBCASR											
Indicates the Answer-seizure Ratio (ASR) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCIPGroupASR											
Indicates ASR per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCSRDASR											
Indicates ASR per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCNER											
Indicates the Network Effectiveness Ratio (NER) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCIPGroupNER											
Indicates NER per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCSRDNER											
Indicates NER per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCACD											
Indicates the Average Call Duration (ACD) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCIPGroupACD											
Indicates ACD per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
PM_gwSBCSRDACD											
Indicates ACD per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
acPMSBCInCapsTable											
Indicates the number of incoming calls per second.	G	15	✓	✓	✓	✓	×	×	×	×	×

6.2.7 High Availability

The SNMP MIBs below provide performance monitoring for High Availability (HA) mode.

Table 6-12: Performance Monitoring MIBs for High-Availability

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
AcPMHALinkRedundantToActivePacketLossPercentageTable											
Indicates packet loss (in %) on the HA Maintenance interface from Redundant to Active device, where 0% indicates no packet loss. ▪ High threshold: acPMHAAttributesHALinkRedundantToActivePacketLossPercentageHighThreshold (1.3.6.1.4.1.5003.10.11.1.38.1) ▪ Low threshold: acPMHAAttributesHALinkRedundantToActivePacketLossPercentageLowThreshold (1.3.6.1.4.1.5003.10.11.1.38.2)	G	15	✓	✓	✓	✓	✓	✓	✓	✓ (30)	5
AcPMHALinkActiveToRedundantPacketLossPercentageTable											
Indicates packet loss (in %) on the HA Maintenance interface from Active to Redundant device, where 0% indicates no packet loss. ▪ High threshold: acPMHAAttributesHALinkActiveToRedundantPacketLossPercentageHighThreshold (1.3.6.1.4.1.5003.10.11.1.38.3) ▪ Low threshold: acPMHAAttributesHALinkActiveToRedundantPacketLossPercentageLowThreshold (1.3.6.1.4.1.5003.10.11.1.38.4)	G	15	✓	✓	✓	✓	✓	✓	✓	30	5

6.2.8 DSP Resource Utilization

The SNMP MIB below reports the percentage of DSP resources utilized by the device. Low and high thresholds can also be defined, which if crossed, the SNMP trap event, acPerformanceMonitoringThresholdCrossing is sent by the device.

Note: The MIB is applicable only to Mediant 5xx, Mediant 8xx, Mediant 2600, Mediant 4000, and Mediant 9000.

Table 6-13: Performance Monitoring MIB for DSP Utilization

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
acPMDSPUsage											
Indicates the percentage (%) of DSP resources utilized by the device. A value of 0% indicates that no DSP resources have been used; a value of 100% indicates that all DSP resources have been used. ▪ High threshold: acPMMediaDSPUsageAttrDSPUsageHighThreshold (1.3.6.1.4.1.5003.10.7.1.35.1) ▪ Low threshold: acPMMediaDSPUsageAttrDSPUsageLowThreshold (1.3.6.1.4.1.5003.10.7.1.35.2)	G	15	✓	✓	✓	✓	✓	✓	✓	✓ (101)	✓ (101)

6.2.9 Media Transcoding Cluster

The following SNMP MIBs provides performance monitoring of the Media Transcoding Cluster feature.

Note:

- The section is applicable only to products supporting the Media Transcoding Cluster feature.
- The MIBs are currently not supported and will be supported in the next applicable software release.

Table 6-14: Performance Monitoring MIBs for Media Transcoding Cluster

Performance Monitoring MIB	Properties (Objects)										
	Gauge (G) / Counter (C)	Reporting Interval	Val	Min	Max	Avg	TimeBelowLowThreshold	TimeBetweenThresholds	TimeAboveHighThreshold	HighThreshold (Default)	LowThreshold (Default)
mtcClusterUtilization											
Average utilization (in %) of DSP resources of the entire Media Transcoding Cluster. When utilization exceeds 95%, an alarm is raised. When it drops below 90%, the alarm is cleared. The MIB is raised by the Cluster Manager.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
mtcMtceUtilization											
Average utilization (in %) of DSP resources of the Media Transcoder.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
mtcMtceDspUtilization											
Number of active channels on the Media Transcoder.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
MtcCmToMtcePacketLossPercentage											
Average packet loss (in %) according to UDP heartbeat calculated from the Cluster Manager to the Media Transcoder. When packet loss exceeds 30%, an alarm is raised. When it drops below 5%, the alarm is cleared.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓
MtcMtceToCmPacketLossPercentage											
Average packet loss (in %) according to UDP heartbeat calculated from the Media Transcoder to the Cluster Manager. When packet loss exceeds 30%, an alarm is raised. When it drops below 5%, the alarm is cleared.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

6.2.10 Survivable Branch Appliance (SBA)

The SNMP MIBs below provide performance monitoring statistics for the SBA Skype for Business services status.

Note: Applicable only to the Mediant 800B SBA and Mediant 1000B SBA products.

Table 6-15: Performance Monitoring MIBs for SBA Skype for Business Services Status

MIB Name	Description
acSBAFrontEndServerStatus	Displays the status of the SBA Front End Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.
acSBAMediationServerStatus	Displays the status of the SBA Mediation Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.
acSBAReplicaServerStatus	Displays the status of the SBA Replica Server: ▪ service_continue_pending: The service is about to continue. ▪ service_pause_pending: The service is pausing. ▪ service_paused: The service has paused. ▪ service_running: The service is running. ▪ service_start_pending: The service is starting. ▪ service_stop_pending: The service is stopping. ▪ service_stopped: The service has stopped. ▪ service_not_installed: The service is not installed or has installation errors.

MIB Name	Description
AcSBACentLoggingAgentStatus	Displays the status of the SBA Central Logging agent: ▪ Skype for Business: ✓ service_continue_pending: The service is about to continue. ✓ service_pause_pending: The service is pausing. ✓ service_paused: The service has paused. ✓ service_running: The service is running. ✓ service_start_pending: The service is starting. ✓ service_stop_pending: The service is stopping. ✓ service_stopped: The service has stopped. ✓ service_not_installed: The service is not installed or has installation errors. ▪ Lync 2010: ✓ service_non_available: The service is not supported by Lync 2010.
acSBASetupStatus	Displays the SBA setup status: ▪ setup_not_done: No step has been done. ▪ setup_done: All steps have been successful. ▪ setup_partial: At least one step is successful, not completed or returns an error.

7 SNMP Traps

This section 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 Series)
- **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 12 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 119.

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:
    - noAlarm(0)
    - indeterminate(1)
    - warning(2)
    - minor(3)
    - major(4)
    - critical(5)
- acBoardTrapGlobalsSystemSeverity (OID:1.3.6.1.4.1.5003.9.10.1.21.1.12): Reflects the highest alarm severity (and current alarm) raised by the device:
  - 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:

7.3 Device Alarms

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

7.3.1 Chassis Alarms

7.3.1.1 Fan Tray Alarm

Note: The alarms are applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.

Table 7-2: acFanTrayAlarm

Alarm	acFanTrayAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29		
Description	Sent when a fault occurs in the fan tray or a fan tray is missing.		
Source Varbind Text	Chassis#0/FanTray#0		
Alarm Text	Fan-Tray Alarm <text>		
Event Type	equipmentAlarm		
Probable Cause	▪ One or more fans on the Fan Tray module stopped working. ▪ One or more fans on the Fan Tray module works slower than expected (heatingVentCoolingSystemProblem)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Fan-Tray is missing.	Fan-Tray is missing	1. Check if the Fan Tray module is inserted in the chassis. 2. If the Fan Tray module was removed from the chassis, re-insert it. 3. If the Fan Tray module has already been inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes. **Warning:** When removing the Fan Tray module while the power is on (or after it has recently been switched off), the blades may still be rotating at high speeds. Therefore, to avoid bodily harm, make sure that you don't touch the fan blades.
Major	When one or more fans in the Fan Tray are faulty.	Fan-Tray is faulty	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module is in place and fans are working.	-	-

7.3.1.2 Power Supply Alarm

Note: Applicable only to MP-1288, Mediant 1000, Mediant 2600, and Mediant 4000.

Table 7-3: acPowerSupplyAlarm

Alarm	acPowerSupplyAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30		
Description	Sent when a fault occurs in one of the power supply (PS) modules or a PS module is missing. **Note:** For Mediant 1000 series, to enable the sending of this SNMP trap, set the ini file parameter, Mediant1000DualPowerSupplySupported to 2.		
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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	The HA (High Availability) feature is active and one of the power supply units is faulty or missing.	Power-Supply Alarm. Power-Supply is missing.	1. Check if the unit is inserted in the chassis. 2. If it was removed from the chassis, re-insert it. 3. If it's inserted in the chassis and the alarm is active, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	PS unit is placed and working.	-	-

7.3.1.3 User Input Alarm

Note: The alarms are applicable to Mediant 1000.

Table 7-4: acUserInputAlarm

Alarm	acUserInputAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.36		
Description	Sent when the input dry contact is short circuited; cleared when the circuit is reopened.		
Default Severity	Critical		
Source Varbind Text	Chassis#0		
Event Type	equipmentAlarm		
Probable Cause	inputDeviceError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Input dry contact is short circuited.	User input Alarm. User's Input-Alarm turn on.	Reopen the input dry contact.
Cleared	Input dry contact circuit is reopened.	-	

7.3.1.4 Hardware Failure Alarm (Mediant 1000)

Note: The alarms are applicable only to Mediant 1000.

Table 7-5: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Critical	The module is faulty or has been removed incorrectly.	Module Alarm: Faulty IF-Module	Restart the device to clear this alarm. The alarm is not cleared.
Major	Module mismatch - module and CPU board mismatch.	IF-Module Mismatch	Restart the device to clear this alarm. The alarm is not cleared.

7.3.2 Trunk Alarms

Note: The alarms are applicable only to the Digital Series.

7.3.2.1 Trunk Near-End LOS Alarm

Table 7-6: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Near-end LOS	Trunk LOS Alarm	Los of Signal (LOS) indicates a physical problem. 1. Check that the cable is connected on the board. 2. Check that the correct cable type is being used (crossed/straight). 3. Contact AudioCodes' Support Center at support@audiocodes.com.
Cleared	End of LOS	-	-

7.3.2.2 Trunk Near-End LOF Alarm

Table 7-7: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Near end LOF	Trunk LOF Alarm	1. Make sure that the trunk is connected to a proper follow-up device. 2. Make sure that both sides are configured with the same (E1 / T1) link type. 3. Make sure that both sides are configured with the same framing method. 4. Make sure that both sides are configured with the same line code. 5. Make sure that the clocking setup is correct. 6. Contact AudioCodes' Support Center at support@audiocodes.com.
Cleared	End of LOF	-	-

7.3.2.3 Trunk AIS Alarm

Table 7-8: acTrunksAlarmRcvAIS

Alarm	acTrunksAlarmRcvAIS		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.51		
Source Varbind Text	Interfaces#0/Trunk#<m>, where m is the trunk interface number, 1 being the first trunk		
Alarm Text	communicationsAlarm		
Event Type	PSTN provider has stopped the trunk (receiveFailure)		
Probable Cause	communicationsAlarm		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Receive AIS	Trunk AIS Alarm	1. Contact your PSTN provider to activate the trunk. 2. If the alarm persists, contact the AudioCodes Support Center at support@audiocodes.com
Cleared	End of AIS	-	-

7.3.2.4 Trunk Far-End LOF Alarm

Table 7-9: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Critical	RAI	Trunk RAI Alarm	Make sure that transmission is correct.
Cleared	End of RAI	-	-

7.3.2.5 DS1 Line Status Alarm

Table 7-10: 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 Severity	**<text>**	**Additional Info1,2,3**
-	DS1 Line Status	Updated DS1 Line Status. This variable indicates the Line Status of the interface. It contains loopback, failure, received 'alarm' and transmitted 'alarms' information. dsx1LineStatus is a bitmap represented as a sum, so 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

7.3.2.6 B-Channel Alarm

Table 7-11: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised when B-channel service state changes to 'Out of Service' or 'Maintenance'	B-Channel Alarm. %s	Corrective action is not necessary
Clear	B-channel status changes to 'In Service'	%s – additional information	-

7.3.2.7 NFAS Group Alarm

Table 7-12: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised when an NFAS group goes out-of-service	NFAS Group Alarm. %s	▪ The alarm is sent only when the backup Non-Facility Associated Signaling (NFAS) D-channel also falls, i.e., when *both* D-channels are down. ▪ When at least one of the D-channels (primary or backup) returns to service, the alarm is cleared. ▪ Corrective action is not necessary.
Clear	NFAS group state goes to in- service	%s– Additional information	-

7.3.3 High-Availability (HA) Alarms

Note: The alarms are applicable to HA supporting devices.

7.3.3.1 HA System Fault Alarm

Table 7-13: acHASystemFaultAlarm

Trap	acHASystemFaultAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33		
Description	Sent when the High Availability (HA) system is faulty (i.e., no HA functionality).		
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		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	HA feature is active but the system is not working in HA mode	Fatal exception error	High Availability (HA) was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		TCPIP exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		SW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		HW WD exception error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		DSP error (applicable only to Mediant 4000)	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		BIT tests error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Keep Alive error	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Software upgrade	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.
		Manual switch over	HA was lost due to *switchover* and should return automatically after a few minutes. Corrective action is not required.

Trap	acHASystemFaultAlarm		
		Manual reset	HA was lost due to a *system reset* and should return automatically after few minutes. Corrective action is not required.
		Redundant is not reconnecting after deliberate restart	Reset / replace the redundant module.
		No Ethernet Link in redundant module	Connect Ethernet links to the redundant module
		Eth link error	HA was lost due to switchover, Connect the Eth link back.
		Network watchdog error	HA was lost due to switchover or redundant unit failure. Fix the network connectivity from failed unit
Minor	HA feature is active and the redundant module is in startup mode and hasn't connected yet	Waiting for redundant to connect	Corrective action is not required.
Cleared	HA system is active	-	-

7.3.3.2 HA System Configuration Mismatch Alarm

Table 7-14: acHASystemConfigMismatchAlarm

Trap	acHASystemConfigMismatchAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34		
Description	Sent when the configuration of the modules in the HA system is not identical, causing instability.		
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		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	HA feature is active:	Configuration mismatch in the system:	The actions for the conditions are described below.
	License Keys of Active and Redundant modules are different.	Active and Redundant modules have different feature keys.	Update the Feature Keys of the Active and Redundant modules.
	The Active module was unable to pass on to the Redundant module the License Key.	Fail to update the redundant with feature key.	Replace the Feature Key of the Redundant module – it may be invalid.
	License key of the Redundant module is invalid.	Feature key did not update in redundant module.	Replace the Feature Key of the Redundant module – it may be invalid.
Cleared	Successful License Key update	The feature key was successfully updated in the redundant module	-

7.3.3.3 HA System Switch Over Alarm

Table 7-15: acHASystemSwitchOverAlarm

Trap	acHASystemSwitchOverAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35		
Description	Sent when a switchover from the active to the redundant module has occurred.		
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		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	A switchover from the active to the redundant unit has occurred	Switch-over: See the acHASystemFaultAlarm table above	See Section 7.3.3.2 on page 76 above for details.
Cleared	10 seconds have passed since the switchover	-	-

7.3.4 Board Alarms

The source varbind text for all the alarms under this component is: **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.

7.3.4.1 Fatal Error Alarm

Table 7-16: acBoardFatalError

Alarm	acBoardFatalError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1		
Description	Sent whenever a fatal device error occurs.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Any fatal error	Board Fatal Error: A run-time specific string describing the fatal error	1. Capture the alarm information and the Syslog clause, if active. 2. Contact AudioCodes' Support Center at support@audiocodes.com which will want to collect additional data from the device and perform a reset.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After fatal error	-	

7.3.4.2 Configuration Error Alarm

Table 7-17: acBoardConfigurationError

Alarm	acBoardConfigurationError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Description	Sent when the device's settings are invalid. The trap contains a message stating/detailing/explaining the invalid setting.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	A configuration error was detected	Board Config Error: A run-time specific string describing the configuration error	1. Check the run-time specific string to determine the nature of the configuration error. 2. Fix the configuration error using the appropriate tool: Web interface, EMS, or *ini* file. 3. Save the configuration and if necessary reset the device.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After configuration error	-	

7.3.4.3 Temperature Alarm

Note: The alarm is applicable only to Mediant 1000 Series, Mediant 2600, and Mediant 4000.

Table 7-18: acBoardTemperatureAlarm

Alarm	acBoardTemperatureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3		
Description	Sent when the device exceeds its temperature limits.		
Source Varbind Text	System#0		
Event Type	equipmentAlarm		
Probable Cause	▪ The air filter is saturated. ▪ One of the fans work slower than expected. temperatureUnacceptable (50)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Internal temperature is too high for normal operation	Board temperature too high	1. Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels. 2. Check the chassis ventilation outlet and make sure that they are not obstructed for air flow. Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Temperature returns to normal operating values	-	-

7.3.4.4 Software Reset Alarm

Table 7-19: acBoardEvResettingBoard

Alarm	acBoardEvResettingBoard		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5		
Description	Sent after the device resets.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	When a soft reset is triggered via the Web interface or SNMP	User resetting board	A network administrator has taken action to reset the device. Corrective action is not required.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After raise		

7.3.4.5 Software Upgrade Alarm

Table 7-20: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70		
Description	Sent for software upgrade process errors.		
Default Severity	Major		
Alarms Source	System#0		
Event Type	processingErrorAlarm		
Probable Cause	softwareProgramError		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Raised upon software upgrade errors	SW upgrade error: Firmware burning failed. Startup system from BootP/TFTP.	Start up the system from BootP/TFTP.

7.3.4.6 Call Resources Alarm

Note: The alarms are applicable to SBC Series.

Table 7-21: acBoardCallResourcesAlarm

Alarm	acBoardCallResourcesAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8		
Description	Sent when no free channels are available.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Percentage of busy channels exceeds the predefined RAI high threshold	Call resources alarm	▪ Expand system capacity by adding more channels (trunks) -OR- ▪ Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	Note that to enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated (EnableRAI = **1**).

7.3.4.7 All SIP Proxies Connection Lost Trap per Proxy Set

Table 7-22: acProxyConnectionLost

Alarm	acProxyConnectionLost
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94
Description	Sent when all connections in a specific Proxy Set are down. The trap is cleared when one of the Proxy Set connections is up.
Source Varbind Text	System#0
Alarm Text	Proxy Set Alarm <text>
Event Type	communicationsAlarm
Probable Cause	▪ Network issue (connection fail due to network/routing failure). ▪ Proxy issue (proxy is down). ▪ AudioCodes device issue.

Alarm Severity

Severity	Condition	<text>	Corrective Action
Major	When connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table.	Proxy Set %d: Proxy not found. Use internal routing	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. 3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. 4. Check that routing using the device's (internal) routing table is functioning correctly. 5. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Major	When Proxy Set includes more than one proxy IP with redundancy and connection to one of them is lost.	Proxy Set %d: Proxy lost. looking for another proxy	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. 3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same Alarm. If this is the case, this could confirm that this is not AudioCodes device issue. 4. Check if routing via the redundant proxy is operating correctly. If it is, then this could mean that it's not a network issue. 5. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to proxy is available again	Proxy found. ip:<IP address>:<port #> Proxy Set ID %d	-

7.3.4.8 Controller Failure Alarm

Note: The alarms are applicable to the Analog Series and Digital Series.

Table 7-23: acBoardControllerFailureAlarm

Alarm	acBoardControllerFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.9		
Description	The alarm is sent in the following scenarios: ▪ Physical FXO port is up or down (Out-of-Service or OOS). The FXO line can be down due to, for example, port disconnected or insufficient current and voltage. (Syslog message event is ANALOG_IF_LINE_DISCONNECTED.) ▪ Physical BRI or PRI (E1/T1) port is up or down (OOS). ▪ Proxy is not found or registration fails. In such a case, the device's routing table may be used for routing instead of the Proxy. ▪ Connection to the Proxy is up or down. ▪ Failure in TDM-over-IP call - transparent E1/T1 without signalling. ▪ Connection to the Proxy Set associated with the trunk/line is up/down. ▪ Failure in server registration for the trunk/line. ▪ Failure in a Serving IP Group for the trunk. ▪ Failure in a Proxy Set.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**Text**	**Additional Information**
Major	FXO physical port is down	"BusyOut Line *n* Link failure" Where *n* represents the FXO port number (0 for the first port).	▪ Verify that the FXO line is securely cabled to the device's FXO port.
	BRI or PRI physical port is down	"BusyOut Trunk *n* Link failure" Where *n* represents the BRI or PRI port number (0 for the first port).	Verify that the digital trunk is securely cabled to the device's digital port.
	Proxy has not been found or registration failure	"Proxy not found. Use internal routing" -OR- "Proxy lost. Looking for another Proxy"	▪ Check the network layer ▪ Make sure that the proxy IP and port are configured correctly.
	Connection to Proxy is down	"BusyOut Trunk/Line *n* Connectivity Proxy failure"	-
	Connection to the Proxy Set associated with the trunk or line is down	"BusyOut Trunk/Line *n* Proxy Set Failure" Where *n* represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Proxy Set	"Proxy Set ID *n*" Where *n* represents the Proxy Set ID.	-
	Failure in TDM-over-IP call	"BusyOut Trunk *n* TDM over IP failure (Active calls x Min y)" Where *n* represents the BRI/ PRI trunk.	-

Alarm	acBoardControllerFailureAlarm		
	Failure in server registration for the trunk/line	"BusyOut Trunk/Line *n* Registration Failure" Where *n* represents the BRI/ PRI trunk or FXO line.	-
	Failure in a Serving IP Group for the trunk	"BusyOut Trunk *n* Serving IP Group Failure" Where *n* represents the BRI or PRI trunk ID.	-
Cleared	Proxy is found. The 'Cleared' message includes the IP address of this Proxy.	-	**-**

7.3.4.9 Board Overload Alarm

Table 7-24: acBoardOverloadAlarm

Alarm	acBoardOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Description	Sent when there is an overload in one or some of the system's components.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	An overload condition exists in one or more of the system components	"System CPU overload condition - IdleUtilization percentage=%d" Where *%d* is the percentage of available CPU resources remaining	**1.** Make sure that the syslog level is 0 (or not high). **2.** Make sure that DebugRecording is not running. **3.** If the system is configured correctly, reduce traffic.
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	**-**

7.3.4.10 Feature Key Error Alarm

Table 7-25: acFeatureKeyError

Alarm	acFeatureKeyError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6
Description	Sent to relay Feature Key errors etc.
Default Severity	Critical
Event Type	processingErrorAlarm
Probable Cause	configurationOrCustomizationError (7)
Alarm Text	Feature key error
Status Changes	
Note	Support for this alarm is pending.

7.3.4.11 Administration Status Change Alarm

Table 7-26: acgwAdminStateChange

Alarm	acgwAdminStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7		
Description	Sent when Graceful Shutdown commences and ends.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Admin state changed to shutting down	Network element admin state change alarm: Gateway is shutting down. No time limit.	▪ No corrective action is required. ▪ A network administrator took an action *to gracefully lock the device*.
Major	Admin state changed to locked	Locked	▪ No corrective action is required. ▪ A network administrator took an action *to lock the device, or a graceful lock timeout occured*.
Cleared	Admin state changed to unlocked	-	▪ No corrective action is required. ▪ A network administrator has taken an action *to unlock the device*.

7.3.4.12 Operational Status Change Alarm

Table 7-27: acOperationalStateChange

Alarm	acOperationalStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15		
Description	Sent if the operational state of the node goes to disabled; cleared when the operational state of the node goes to enabled.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Operational state changed to disabled	Network element operational state change alarm. Operational state is disabled.	▪ The alarm is cleared when the operational state of the node goes to enabled. ▪ In IP systems, check for initialization errors - in IP systems the operational state of the node is disabled if the device fails to properly initialize. ▪ Look for other alarms and Syslogs that might provide additional information about the error.
Cleared	Operational state changed to enabled	-	-

7.3.5 License Pool Alarms

7.3.5.1 License Pool Infrastructure Alarm

Table 7-28: acLicensePoolInfraAlarm

Alarm	acLicensePoolInfraAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.106		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Minor	SBC License key received from License Pool Manager Server and reset required.	"New license pool allocations received. Reset device to apply new allocations"	Reset the device.
Major	Device unable to access the License Pool Manager Server	"Device was unable to access the License Server"	Restore connectivity with the License Pool Manager Server (EMS) to clear the alarm.

Alarm	acLicensePoolInfraAlarm		
Critical	No connection with the License Pool Manager Server for approx. 3.5 days	"License-pool is about to expire (12 or less hours before)."	Alarm is cleared when the device requests a new License from the License Pool Manager Server

7.3.5.2 License Pool Application Alarm

Table 7-29: acLicensePoolApplicationAlarm

Alarm	acLicensePoolApplicationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.107		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Warning	The SBC license received from the License Pool Manager Server causes a total capacity that exceeds the maximum supported by the device	"Some of the license pool allocations will not be used because of over-allocation"	Alarm is cleared when a new SBC license whose values are within the maximum are received from the License Pool Manager Server.
Minor	The SBC license received from the License Pool Manager Server causes a total capacity that exceeds the maximum supported by the device, and the device has subsequently reset to apply the license.	"Some of the license pool allocations exceed maximum capability and will not be applied"	Once reset, the device sets its SBC capacity to maximum (and not more). The alarm is cleared only if the device receives a new SBC license from the License Pool Manager Server whose addition does not exceed maximum supported sessions, and the device is subsequently reset.

7.3.6 Network Alarms

7.3.6.1 Ethernet Link Alarm

Table 7-30: acBoardEthernetLinkAlarm

Alarm	acBoardEthernetLinkAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10		
Description	Sent when the Ethernet link(s) is down.		
Default Severity	Critical		
Source Varbind Text	Board#<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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	Fault on single interface	Ethernet link alarm: Redundant link is down	1. Ensure that both Ethernet cables are plugged into the back of the system. 2. Observe the system's Ethernet link lights to determine which interface is failing. 3. Reconnect the cable or fix the network problem
Critical	Fault on both interfaces	No Ethernet link	
Cleared	Both interfaces are operational	-	Note that the alarm behaves differently when coming from the redundant or the active modules of a High Availability (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.

7.3.6.2 Ethernet Group Alarm

Note: The alarms are applicable only to Mediant 500 E-SBC, Mediant 800B Gateway & E-SBC, Mediant 1000B Gateway & E-SBC, Mediant 2600 E-SBC, Mediant 4000 SBC, Mediant 9000 SBC, and Mediant Software SBC.

Table 7-31: acEthernetGroupAlarm

Alarm	acEthernetGroupAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86
Description	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.
Default Severity	Major
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable
Alarm Text	Ethernet Group alarm. %s
Status Changes	
1. Condition	Raised when both ports in a group are down
2. Condition	Cleared when at least one port is up

7.3.6.3 NTP Server Status Alarm

Table 7-32: acNTPServerStatusAlarm

Alarm	acNTPServerStatusAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71		
Description	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. If the <device> receives no response from the NTP server, it polls the NTP server for 10 minutes for a response. If there is still no response after this duration, the <device> declares the NTP server as unavailable, by sending this alarm. The failed response could be due to incorrect configuration.		
Default Severity	Major		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	No initial communication to Network Time Protocol (NTP) server.	NTP server alarm. No connection to NTP server.	Repair NTP communication (the NTP server is down or its IP address is configured incorrectly in the device).
Minor	No communication to NTP server after the time was already set once.	-	-

7.3.6.4 NAT Traversal Alarm

Table 7-33: acNATTraversalAlarm

Alarm	acNATTraversalAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.17
Description	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.
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	See http://tools.ietf.org/html/rfc5389

7.3.6.5 LDAP Lost Connection Alarm

Note: The alarms are applicable to all products except MediaPack Series.

Table 7-34: 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	

7.3.6.6 OCSP Server Status Alarm

Table 7-35: 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	▪ Repair the Online Certificate Status Protocol (OCSP) server -OR- ▪ Correct the network configuration

7.3.6.7 IPv6 Error Alarm

Note: The alarms are applicable only to SBC Series.

Table 7-36: acIPv6ErrorAlarm

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 Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Bad IPv6 address (already exists)	IP interface alarm: IPv6 configuration failed, IPv6 will be disabled.	▪ Find a new IPV6 address. ▪ Reboot the device.
Stays 'Critical' until reboot. A 'Clear' trap is not sent.	After the alarm is raised.	-	-

7.3.6.8 HTTP Proxy Service Alarm

Table 7-37: acHTTPProxyServiceAlarm

Alarm	acHTTPProxyServiceAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.108
Description	Sent when all HTTP hosts in a specific HTTP proxy service are down. The trap is cleared when one of the hosts is back up. The keep-alive with the HTTP host is enabled by the HTTPProxyService_KeepAliveMode parameter.
Source Varbind Text	System#0/HTTPProxyService#<num> System#0/EMSService#<num>
Alarm Text	"Http Proxy Service %d is DOWN" "EMS Service %d is DOWN"
Event Type	communicationsAlarm
Probable Cause	▪ Network issue (connection fail due to network/routing failure). ▪ Host issue (host is down). ▪ Device issue.

Alarm Severity

Severity	Condition	<text>	Corrective Action
Major	When connection to the service is lost and this service is configured with keep-alive.	"Http Proxy Service %d is DOWN" "EMS Service %d is DOWN"	**1** Ping the host. If there is no ping, contact your provider. The probable reason is the host is down. **2** Ping between the host and the device. If there is no ping, the problem could be a network/router issue. **3** If you have more than one device connected to the same host, check if there are more devices with the same alarm. If this is the case, this could confirm that this is not a device issue. **4** Check that routing using the device's (internal) routing table is functioning correctly. **5** Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to service is available again.	-	-

7.3.7 Active Alarm Table Alarm

Table 7-38: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow		
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12		
Description	Sent when an active alarm cannot be entered into the Active Alarm table because the table is full.		
Default Severity	Major		
Source Varbind Text	*System#0*<n>*/AlarmManager#0*		
Event Type	processingErrorAlarm		
Probable Cause	resourceAtOrNearingCapacity (43)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Too many alarms to fit in the active alarm table	Active alarm table overflow	▪ Some alarm information may be lost but the ability of the device to perform its basic operations is not impacted. ▪ A reboot is the only way to completely clear a problem with the active alarm table. ▪ Contact AudioCodes' Support Center at support@audiocodes.com
Remains 'Major' until reboot. A 'Clear' trap is not sent.	After the alarm is raised	-	Note that 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.

7.3.8 Audio Staging from APS Server Alarm

Note: The alarms are applicable only to Mediant 1000B series.

Table 7-39: acAudioProvisioningAlarm

Alarm	acAudioProvisioningAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.14		
Description	Sent if the device is unable to provision its audio.		
Default Severity	Critical		
Source Varbind Text	System#0/AudioStaging#0		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError (7)		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Media server times out waiting for a successful audio distribution from the APS (Audio Provisioning Server)	Unable to provision audio	1. From the Audio Provisioning Server (APS) GUI, ensure that the device is properly configured with audio and that the device has been enabled. 2. Ensure that the IP address for the APS has been properly specified on the device. 3. Ensure that both the APS server and application are in-service. 4. For more information regarding the problem, view the Syslogs from the device as well as the APS manager logs.
Cleared	After the alarm is raised, the media server is successfully provisioned with audio from the APS	-	

7.3.9 Analog Port Alarms

Note: The alarms are applicable only to the Analog Series.

7.3.9.1 Analog Port SPI Out-of-Service Alarm

Table 7-40: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	Analog port has gone out of service	Analog Port SPI out of service	▪ No corrective action is required. ▪ The device shuts down the port and activates it again when the Serial Peripheral Interface (SPI) connection returns.
Cleared	Analog port is back in service	-	-

7.3.9.2 Analog Port High Temperature Alarm

Table 7-41: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	Analog device has reached critical temperature. Device is automatically disconnected.	Analog Port High Temperature	▪ No corrective action is required. ▪ The device shuts down the analog port and tries to activate it again later when the device's temperature drops.
Cleared	Temperature is back to normal - analog port is back in service.	-	-

7.3.9.3 Analog Port Ground Fault Out-of-Service Alarm

Table 7-42: 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	▪ No corrective action is required. ▪ The device shuts down the port and tries to activate it again when the relevant alarm is over.
Note	Relevant to FXS only.

7.3.10 Media Alarms

7.3.10.1 Media Process Overload Alarm

Note: The alarm is applicable only to Mediant 1000B GW & SBC, Mediant 2600, and Mediant 4000.

Table 7-43: acMediaProcessOverloadAlarm

Alarm	acMediaProcessOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.81		
Description	Sent when there is an overload of media (RTP) processing on the device. This can occur, for example, as a result of malicious attacks (such as denial of service or DoS) on a specific port, or as a result of processing SRTP packets.		
Default Severity	Major		
Event Type	environmentalAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	Overload of media processing.	Media Process Overload Alarm	If not due to malicious attacks, reconfigure your device so that it can process the required media sessions per SIP entity according to media characteristics (e.g., SRTP, RTP and coder types). If due to malicious attacks, you should contact your network administrator.
Cleared	Resources are available for media processing.	-	-

7.3.10.2 Media Realm Bandwidth Threshold Alarm

Note: The alarms are applicable only to the Digital Series and SBC Series.

Table 7-44: 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 Severity	**Condition**	**<text>**	**Corrective Action**
Major	-	Media Realm BW Threshold Alarm	Cleared when bandwidth threshold returns to normal range

7.3.11 Call Quality Alarms

7.3.11.1 Answer-Seizure Ratio Threshold Alarm

Table 7-45: acASRThresholdAlarm

Alarm	acASRThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.111		
Description	The Answer-Seizure Ratio (ASR) measures the percentage of answered calls relative to the total number of attempted calls (seizures). The alarm is raised when the configured ASR minor and major thresholds are crossed (configured in the *Performance Profile* table).		
Source Varbind Text	The object for which the threshold is crossed can be any of the following: ▪ PM_gwSBCASR ▪ PM_gwSBCIPGroupASR ▪ PM_gwSBCSRDASR		
Alarm Text			
Event Type	QualityOfServiceAlarm		
Probable Cause	ThresholdCrossed		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	ASR is equal or less than the configured Major threshold.	"ASR threshold crossed."	
Minor	ASR is equal or less than the configured Minor threshold (but greater than the Major threshold).	"ASR threshold crossed."	
Cleared	ASR is above the configured Minor threshold plus the hysteresis.		

7.3.11.2 Average Call Duration Threshold Alarm

Table 7-46: acACDThresholdAlarm

Alarm	acACDThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.112		
Description	The Average Call Duration (ACD) plus the SDD (Session Disconnect time) measures the average call duration from the time from when the sip Bye is sent to the time when the 200 OK is received. The alarm is raised when the configured ACD minor and major thresholds are crossed (configured in the Performance Profile table).		
Source Varbind Text	The object for which the threshold is crossed can be any one of the following: ▪ PM_gwSBCACD ▪ PM_gwSBCIPGroupACD ▪ PM_gwSBCSRDACD		
Alarm Text			
Event Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	ACD is equal or less than the configured Major threshold.	"ACD threshold crossed."	
Minor	ACD is equal or less than the configured Minor threshold (but greater than the Major threshold).		
Cleared	ACD is above the configured Minor threshold plus the hysteresis.		

7.3.11.3 Network Effectiveness Ratio Threshold Alarm

Table 7-47: acNERThresholdAlarm

Alarm	acNERThresholdAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.113		
Description	The NER (Network Effectiveness Ratio) measures the percentage of successfully connected calls relative to the total number of seizures. The alarm is raised when the configured NER minor and major thresholds are crossed (configured in the Performance Profile table).		
Source Varbind Text	The object for which the threshold is crossed, which can be one of the following: ▪ PM_gwSBCNER ▪ PM_gwSBCIPGroupNER ▪ PM_gwSBCSRDNER		
Alarm Text			
Event Type	Quality Of Service Alarm		
Probable Cause	The threshold has been crossed.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	NER is equal or less than the configured Major threshold.	"NER threshold crossed."	

Alarm	acNERThresholdAlarm		
Minor	NER is equal or less than the configured Minor threshold (but greater than the Major threshold).		
Cleared	NER is above the configured Minor threshold plus the hysteresis.		

7.3.12 No Route to IP Group Alarm

Table 7-48: acIpGroupNoRouteAlarm

Alarm	acIpGroupNoRouteAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.114		
Description	The alarm is raised when the device rejects calls to an IP Group due to the following reasons: ▪ IP Group keep-alive failure (Gateway and SBC) ▪ Poor Voice Quality - MOS (SBC only) ▪ Bandwidth threshold has been crossed (SBC only) ▪ ASR threshold has been crossed (SBC only) ▪ ACD threshold has been crossed (SBC only) ▪ NER threshold has been crossed (SBC only)		
Source Varbind Text	The object for which the threshold is crossed according to one of the above mentioned reasons: ▪ IP Group keep alive failure (acProxyConnectivity trap is raised) ▪ Poor Quality of Experience ▪ Bandwidth ▪ ASR (see acASRThresholdAlarm) ▪ ACD (see acACDThresholdAlarm) ▪ NER (see acNERThresholdAlarm)		
Alarm Text	<Alarm Description Reason> as described above.		
Event Type	Quality Of Service Alarm		
Probable Cause	One of the reasons described above.		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Major	When calls rejected to IP Group due to any of the above-mentioned reasons.	"IP Group is temporarily blocked."	-
Cleared	When calls are no longer rejected due to the above mentioned reasons (i.e. when none of the above reasons prevent a route to the IP Group from being established).		-

7.3.13 Intrusion Detection Alarms

7.3.13.1 IDS Policy Alarm

Table 7-49: 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	1. Identify additional traps (acIDSThresholdCrossNotification) that were sent alongside this Intrusion Detection System (IDS) alarm. 2. Locate the remote hosts (IP addresses) that are specified in the traps. 3. Examine the behavior of those hosts (with regard to the reason specified in the alarm), and attempt to fix incorrect operation. 4. If necessary, change the configured thresholds in the IDS Rule table under the IDS Policy table.

7.3.14 Media Transcoding Cluster Alarms

This section describes the alarms of the Media Transcoding Cluster feature.

Note: The alarms are applicable only to products supporting the Media Transcoding Cluster feature.

7.3.14.1 Cluster HA Usage Alarm

Table 7-50: acMtcmClusterHaAlarm

Alarm	acMtcmClusterHaAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.115		
Description	The alarm is raised by the Cluster Manager when the cluster HA usage exceeds 100%. HA usage of 100% means that if a failure occurs in a Media Transcoder, sufficient DSP resources are available on the other Media Transcoders in the cluster to take over the transcoding sessions of the failed Media Transcoder. HA usage exceeding 100% means that insufficient DSP resources are available on the other Media Transcoders to take over the transcoding sessions of the failed Media Transcoder.		
Default Severity	Major		
Alarm Source	device/clusterManager		
Event Type	equipmentAlarm		
Probable Cause	Other		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Cluster HA usage exceeds 100%.	"At least one of the MTCEs is inactive, MTC will now provide only partial HA"	▪ Make sure all Media Transcoders are properly connected to the Cluster Manager. ▪ Make sure all Media Transcoders in the Media Transcoders table are in Admin State “Unlocked” and Status “Connected”.
Cleared	HA usage drops to below 95%	-	-

7.3.14.2 Media Transcoder Network Failure

Table 7-51: acMtceNetworkFailureAlarm

Alarm	acMtceNetworkFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.116		
Description	The alarm is raised when the Cluster Manager fails to connect to the Media Transcoder.		
Default Severity	Major		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Event Type	communicationsAlarm		
Probable Cause	Other		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**

Alarm	acMtceNetworkFailureAlarm		
Major	Connection failure with Media Transcoder	"No Connection with MTCE: <MTCE-name>"	Make sure a physical connection exists between the Media Transcoder and the Cluster Manager.
Cleared	Connection established / re-established with Media Transcoder	-	-

7.3.14.3 Media Transcoder Software Upgrade Failure

Table 7-52: acMtceSwUpgradeFailureAlarm

Alarm	acMtceSwUpgradeFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.117		
Description	The alarm is raised upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Transcoder.		
Default Severity	Major		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Event Type	processingErrorAlarm		
Probable Cause	other		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Major	Software upgrade (.cmp) or Auxiliary file load failure in Media Transcoder	""Reset of the MTCE is required"	Reset the Media Transcoder and perform the upgrade process again. If the upgrade fails again, contact your AudioCodes support representative.
Cleared	Upon reset of Media Transcoder	-	-

7.3.14.4 Media Transcoder High Temperature Failure

Table 7-53: acMtceHwTemperatureFailureAlarm

Alarm	acMtceHwTemperatureFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.118		
Description	The alarm is raised when the temperature of the Media Transcoder chassis reaches a critical threshold.		
Default Severity	Major		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Event Type			
Probable Cause			
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**

Alarm	acMtceHwTemperatureFailureAlarm		
Major	Temperature of Media Transcoder reaches critical threshold	"MTCE reached high temperature threshold"	1. Check that the ambient environment around the chassis was not changed (room temperature, air-conditioner, and location of the chassis on the site). If the ambient environment is the same, make sure that all unoccupied module slots are covered with blank panels. 2. Check the chassis ventilation outlet and make sure that they are not obstructed for air flow. 3. Check if you also received a Fan Tray alarm, which indicates that one or more fans in the Fan Tray are faulty (major). If this is the case, send the faulty Fan Tray to AudioCodes as RMA. Send an RMA request to AudioCodes for the Fan Tray.
Cleared	Connectivity with Media Transcoder is re-established and temperature is reduced	-	-

7.3.14.5 Media Transcoder Fan Tray Module Failure

Table 7-54: acMtceHwFanTrayFailureAlarm

Alarm	acMtceHwFanTrayFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.119		
Description	The alarm is raised upon a failure in the Fan Tray module of the Media Transcoder.		
Default Severity	Minor		
Alarm Source	…./MTCE#1/fanTray#1		
Event Type	equipmentAlarm		
Probable Cause	heatingVentCoolingSystemProblem		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Minor	Failure in Fan Tray module of Media Transcoder	"MTCE fan tray fault"	Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Fan Tray module status returns to normal	-	-

7.3.14.6 Media Transcoder Power Supply Module Failure

Table 7-55: acMtcePsuFailureAlarm

Alarm	acMtcePsuFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.120		
Description	The alarm is raised upon a failure in the Power Supply module of the Media Transcoder.		
Default Severity	Minor		
Alarm Source	…./MTCE#1/powerSupply#1		
Event Type	equipmentAlarm		
Probable Cause	powerProblem		
Alarm Severity	**Condition**	**Alarm Text**	**Corrective Action**
Minor	Failure in Power Supply module of Media Transcoder	"MTCE power supply unit fault"	1. Check if the Power Supply module is inserted in the chassis. 2. If it was removed from the chassis, re-insert it. 3. If the Power Supply module is inserted in the chassis and the alarm is still raised, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Power Supply module status returns to normal	-	-

7.4 Survivable Branch Appliance (SBA) Traps

7.4.1 SBA Services Status Alarm

Note: The alarms are applicable only to the Mediant 800B SBA and Mediant 1000B SBA devices.

Table 7-56: acSBAServicesStatusAlarm

Alarm	acSBAServicesStatusAlarm		
OID	1.3.6.1.4.1.5003.9.30.2.2.0.1		
Description	Services status alarm. The services are Front End Server, Mediation Server, Replica Server, and Centralized Logging Service for Microsoft Skype for Business (Centralized Logging is not available for Lync 2010).		
Source Varbind Text	SBA Server		
Alarm Text	Indicates which of the above mentioned services is down.		
Event Type	Other		
Probable Cause	Other		
Alarm Severity	**Condition**	**<text>**	**Corrective Action**
Critical	Service is down	SERVICE_STOPPED	Start the service and check why the service stopped, using the event viewer.
Major	Service is paused	SERVICE_PAUSED	Start the service and check why the service paused, using the event viewer.
Cleared	Service is running	SERVICE_RUNNING	-
Indeterminate	Service in indeterminate state	SERVICE_CONTINUE_PENDING SERVICE_PAUSE_PENDING SERVICE_START_PENDING SERVICE_STOP_PENDING	Start the service and check why the service is in indeterminate state, using the event viewer.

7.5 SNMP 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).

7.5.1 Intrusion Detection System (IDS)

Note: These trap events are applicable to all products except MediaPack Series.

7.5.1.1 IDS Threshold Cross Notification Trap

Table 7-57: acIDSThresholdCrossNotification

Alarm	acIDSThresholdCrossNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Description	Sent for each scope (IP or IP+Port) crossing a threshold of an active alarm.
Description	The trap is sent for each scope (IP or IPport) 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	1. Identify the remote host (IP address / port) on the network which the Intrusion Detection System (IDS) has indicated is malicious. Note that the IDS determines a host to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). 2. Block the malicious activity.

7.5.1.2 IDS Blacklist Notification Trap

Table 7-58: acIDSBlacklistNotification

Alarm	acIDSBlacklistNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Description	
Default Severity	
Event Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	Added IP * to blacklist Removed IP * from blacklist
Status Changes	
Corrective Action	Identify the malicious remote host (IP address / port) that the Intrusion Detection System (IDS) has automatically blacklisted or removed from the blacklist. Note that a host is determined to be malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). The malicious source is automatically blacklisted for a user-defined period, after which it is removed from the blacklist.

7.5.2 Web User Access Denied due to Inactivity Trap

Table 7-59: acWebUserAccessDisabled

Alarm	acWebUserAccessDisabled
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	Contact your Web security administrator. Only the Web security administrator can unblock a user whose access to the Web interface was denied (for example, because the user made 3 unsuccessful attempts at access). The Web security administrator must: 1. In the Web interface, access the Accounts page (**Configuration** > **System** > **Management** > **Web User Accounts**). 2. Identify in the list of users table that user whose access has been denied. 3. Change the status of that user from **Blocked** to **Valid** or **New**.

7.5.3 Web User Activity Log Trap

Table 7-60: acActivityLog

Alarm	acActivityLog
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.105
Description	Sent upon log (Syslog) generated by device indicating a Web user action (configured by ActivityListToLog). The SNMP trap notification functionality is enabled by the EnableActivityTrap parameter (refer to the *User's Manual*).
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	[description of activity].User:<username>. Session: <session type>[IP address of client (user)]. For example: "Auxiliary file loading was changed from '0' to '1', User:Admin. Session: WEB [172.17.125.12]
Note	Activity log event is applicable to the following OAMP interfaces: SNMP, Web, CLI and REST. For SNMP activity, the username refers to the SNMP community string.

7.5.4 Keep-Alive Trap

Table 7-61: acKeepAlive

Trap	acKeepAlive
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Description	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.
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.

7.5.5 Performance Monitoring Threshold-Crossing Trap

Table 7-62: acPerformanceMonitoringThresholdCrossing

Trap	acPerformanceMonitoringThresholdCrossing
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Description	Sent every time the threshold of a Performance Monitored object ('Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') 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. **Note:** To enable this trap functionality, set the ini file parameter, PM_EnableThresholdAlarms to 1.
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	"Performance: Threshold trap was set", with source = name of performance counter or gauge which caused the trap
Status Changes	
Condition	A performance counter or gauge (for the attributes 'Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') has crossed the high threshold.
Trap Status	Indeterminate
Condition	A performance counter or gauge has returned to under the threshold
Trap Status	Cleared

7.5.6 HTTP Download Result Trap

Table 7-63: acHTTPDownloadResult

Trap	acHTTPDownloadResult
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Description	Sent upon success or failure of the HTTP Download action.
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.

7.5.7 Dial Plan File Replaced Trap

Note: These trap events are applicable only to the Analog Series and Digital Series.

Table 7-64: 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.

7.5.8 High-Availability (HA)

Note: These SNMP events are applicable only to devices that support the High-Availability (HA) feature.

7.5.8.1 Redundant Board Trap

Table 7-65: acRedundantBoardAlarm

Trap	acRedundantBoardAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.97
Description	Active board sends notification when an alarm or notification is raised in the redundant board.
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Condition	Alarm or notification is raised in the redundant board
Trap Text	

7.5.8.2 HA Network Watchdog Status Alarm

Note: This SNMP event is applicable to all HA-supporting devices.

Table 7-66: acHANetworkWatchdogStatusAlarm

Trap	acHANetworkWatchdogStatusAlarm	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.98	
Description	This alarm indicates that the device's HA Network Reachability (network watchdog) feature is configured, but is not functioning correctly due to, for example, the Ethernet Group being down from where the ping is sent to the network entity. The device's HA Network Reachability feature is used to configure a network IP address to test reachability using pings. When the tested peer stops replying to the Active unit, a switchover is made to the Redundant unit. For configuring the HA Network Reachability feature, refer to the *User's Manual*.	
Default Severity	Major	
Source Varbind Text	System#0/Module#<m>, where *m* is the blade module's slot number	
Event Type	alarmTrap	
Probable Cause	outOfService	
Trap Text	**Condition**	**Corrective Action**
Failed sending ping	Some network configuration error	-
Network watchdog is disabled while HA priority is in use	When HA Priority is in use, the network watchdog module is disabled	-
Network watchdog is disabled while Redundant units has less Eth groups available	One or more of the Redundant unit's Ethernet Groups are down	-
Disabling network watchdog due to network interface error in Redundant unit	One or more of the Redundant unit's Ethernet Groups are down	-

7.5.8.3 Hitless Software Upgrade Status Trap

Note: These trap events are applicable only to HA supporting devices.

Table 7-67: acHitlessUpdateStatus

Alarm	acHitlessUpdateStatus	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48	
Description	A notification trap sent at the beginning and end of a Hitless Software Upgrade. Failure during the software upgrade also activates the trap.	
Default Severity	Indeterminate	
Event Type	Other (0)	
Probable Cause	Other (0)	
Source	Automatic Update	
Trap Text	**Condition**	**Corrective Action**
"Hitless: Start software upgrade."	Hitless Upgrade has begun.	Corrective action is not required
"Hitless: SW upgrade ended successfully."	Successful Hitless Upgrade.	Corrective action is not required
"Hitless: Invalid cmp file - missing Ver parameter."	Hitless Upgrade failed because the cmp file is invalid. The cmp file's version parameter is incorrect.	Replace the cmp file with a valid one.
"Hitless fail: SW ver stream name too long."	Hitless Upgrade failed because the cmp file is invalid. The number of characters defining the software version stream name in the cmp file has been exceeded.	Replace the cmp file with a valid one
"Hitless fail: Invalid cmp file - missing UPG parameter."	Hitless Upgrade failed because the cmp file is invalid. An upgrade parameter is missing from the file.	Replace the cmp file with a valid one.
"Hitless fail: Hitless SW upgrade not supported."	Hitless Upgrade failed because the cmp file is invalid. The cmp file does not support Hitless Upgrade of the current software version to the new software version.	Replace the cmp file with a valid one that supports hitless upgrade of the software from the current version to the new one.

7.5.9 Secure Shell (SSH) Connection Status Trap

Table 7-68: 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

7.5.10 SIP Proxy Connection Lost per Proxy Set Trap

Table 7-69: acProxyConnectivity

Alarm	acProxyConnectivity
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.102
Description	Sent when a connection to a specific proxy in a specific Proxy Set is down. The trap is cleared when the proxy connections is up.
Source Varbind Text	System#0
Alarm Text	Proxy Set Alarm <text>
Event Type	communicationsAlarm
Probable Cause	▪ Network issue (connection fail due to network/routing failure). ▪ Proxy issue (proxy is down). ▪ AudioCodes device issue.

Alarm Severity

Severity	Condition	<text>	Corrective Action
Indeterminate	When connection to the proxy server is lost.	Proxy Server <IP address>:<port> is now OUT OF SERVICE	1. Ping the proxy server. If there is no ping, contact your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and AudioCodes device. If there is no ping, the problem could be a network/router issue. 3. If you have more than one device connected to this same proxy, check if there are more AudioCodes devices with the same trap event. If this is the case, this could confirm that this is not AudioCodes device issue. 4. Contact AudioCodes support center (support@audiocodes.com) and send a syslog and network capture for this issue.
Cleared	When connection to the proxy is available again	Proxy Server <IP address>:<port> is now IN SERVICE	-

7.5.11 TLS Certificate Expiry Trap

Table 7-70: acCertificateExpiryNotification Trap

Alarm		acCertificateExpiryNotification	
OID		1.3.6.1.4.1.5003.9.10.1.21.2.0.92	
Description		Sent before (in days) the expiration of the installed certificate credentials, which cannot be renewed automatically.	
Source Varbind Text		tls#<num>	
Alarm Text		Device's TLS certificate of security context #%d will expire in %d days	
Event Type		environmentalAlarm	
Probable Cause		The certificate key expired (keyExpired)	
Alarm Severity			
Severity	**Condition**	**<text>**	**Corrective Action**
Indeterminate	The certificate key is about to expire.	Either: ▪ The device certificate has expired %d days ago ▪ The device certificate will expire in %d days ▪ The device certificate will expire in less than 1 day %d – number of days %d – TLS Context to which certificate belongs	Load a new certificate to the device before the expiration of the installed certificate (which cannot be renewed automatically). To replace certificates, refer to the *User's Manual*.

7.5.12 Cold Start Trap

Table 7-71: coldStart

Trap Name	ColdStart
OID	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Description	Sent if the device reinitializes, following (for example) a power failure, crash, or CLI reload command. Categorized by the RFC as a "generic trap".
Note	This is a trap from the standard SNMP MIB.

7.5.13 Authentication Failure Trap

Table 7-72: authenticationFailure

Trap Name	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB
Description	Sent if a device is sampled with an incorrect community name, access permission or incorrectly authenticated protocol message. Categorized by the RFC as an "enterprise-specific trap".

7.5.14 Board Initialization Completed Trap

Table 7-73: acBoardEvBoardStarted

Trap Name	acBoardEvBoardStarted
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Description	Sent after the device is successfully restored and initialized following reset.
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.

7.5.15 Configuration Change Trap

Table 7-74: entConfigChange

Trap Name	entConfigChange
OID	1.3.6.1.2.1.4.7.2
MIB	ENTITY-MIB
Description	Sent if a change in device configuration is detected, providing users enhanced change management capability and the option to roll-back the change if necessary. Can include the name of the device, its IP address, etc.

7.5.16 Link Up Trap

Table 7-75: linkUp

Trap Name	linkUp
OID	1.3.6.1.6.3.1.1.5.4
MIB	IF-MIB
Description	Sent if the operational status of a communication link changes from “down”. Categorized by the RFC as an “enterprise-specific trap”.

7.5.17 Link Down Trap

Table 7-76: linkDown

Trap Name	linkDown
OID	1.3.6.1.6.3.1.1.5.3
MIB	IF-MIB
Description	Sent if a communication link failure is detected. Categorized by the RFC as an “enterprise-specific trap”.

7.5.18 D-Channel Status Trap

Note: These trap events are applicable only to the Digital Series.

Table 7-77: AcDChannelStatus

Trap Name	acDChannelStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.37
Description	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
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'.

7.5.19 Enhanced BIT Status Trap

Table 7-78: acEnhancedBITStatus

Alarm	acEnhancedBITStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Description	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.
Default Severity	Indeterminate
Source Varbind Text	BIT
Event Type	Other
Probable Cause	other (0)
Alarm Text	Notification on the board hardware elements being tested and their status.
Status Changes	
Additional Info-1	BIT Type: Offline, startup, periodic
Additional Info-2	BIT Results: BIT_RESULT_PASSED BIT_RESULT_FAILED
Additional Info-3	Buffer: Number of bit elements reports
Corrective Action	Not relevant

8 Advanced SNMP Features

8.1 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.

8.2 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 modifications.

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

8.3 Systems

For the management of a system (a chassis with more than 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 modules in the system. In addition, the table can be used to reset an entire system, reset a redundant module or perform switchover when for devices supporting 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. (Applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.)
- **acSysPowerSupplyTable**: A status-only table with the states of the two power supplies. (Applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.)

The above tables are complemented by the following alarm traps (as defined in the acBoard MIB). For more details, see "SNMP Traps" on page 121):

- **acFanTrayAlarm**: fault in the fan tray or fan tray missing. (Applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.)
- **acPowerSupplyAlarm**: fault in one of the power supply modules or PS module missing. (Applicable only to Mediant 1000, Mediant 2600, and Mediant 4000.)
- **acPEMAlarm**: fault in the one of the PEM modules or PEM module missing. (Applicable only to Mediant 3000.)

8.4 High Availability Systems

Note: Applicable only to devices supporting High-Availability (HA).

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.

8.5 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.

This page is intentionally left blank.

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

- **ini file:**

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

- **CLI:**

```
(config-system)# snmp settings
(snmp)# port
```

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.

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.

- **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.

- **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".
- **Web Interface:** SNMP Trap Destinations table (**Setup menu > Administration tab > SNMP folder > 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 Users table configures trap users.
  - To add a trap user: Click **New**, and then configure the user. 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**.

- **CLI:**

```
(config-system)# snmp trap-destination
```

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.

- **ini file:** SNMPTRUSTEDMGR_x = <IP address>, where *x* is the entry index 0 to 4.
- **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.

- **Web interface:** SNMP Trusted Managers table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Trusted Managers)**. Click the **Apply** button for applying your configuration. Use the check boxes for deleting.
- **CLI:**

```
(config-system)# snmp settings
(snmp)# trusted-managers
```

9.2 Getting Acquainted 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'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.
  - **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.
  - **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 applicable to Analog Series only.
  - **acPSTN MIB:** configuration and status of trunk related objects only. Most of the MIB objects are trunk specific. This MIB is applicable to Digital Series 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.
- **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:

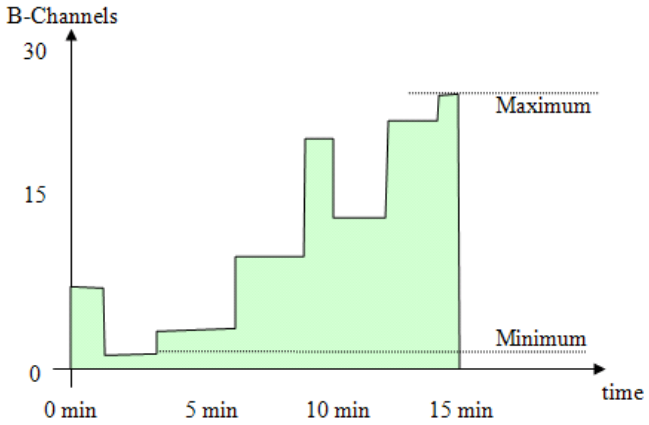
- **Configuration subtree:** allows configuration of general attributes of the MIB and specific attributes of the monitored objects.
- **Data subtree:** this is where the monitored information is found.

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 ('Minimum', 'Average', 'Maximum', 'Distribution below/above/between thresholds', and 'Low and high thresholds') 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)
- 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 on page 123)
- Trap Community String: The default Trap Community String is 'trapuser'. There is only 1 for the entire device.
  - **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:** SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**). Use the **Apply** button to apply your configuration. You can't delete the Trap Community String, only modify its value.
  - **CLI:**

```
(config-system)# snmp trap
(snmp-trap)# community-string
```

- 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
  - This page is intentionally left blank.

This page is intentionally left blank.

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

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info
Website: www.audiocodes.com

Document #: LTRT-52378