Reference Guide

AudioCodes Session Border Controller Series

Simple Network Management Protocol

Mediant 9000 SBC (Rev. B/9030/9080)

Version 7.2

audiocodes

Notice

Date Published: October-26-2022

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Related Documentation

Document Name
SBC-Gateway Series Release Notes for Latest Release Versions
SBC-Gateway Series Release Notes for Long Term Support Versions
Mediant 9000 SBC User's Manual

Document Revision Record

LTRT	Description
52374	Initial document release for Ver. 7.2.
52378	Typos.
52380	MP-1288 added; number of trap varbinds (13); acBoardTrapGlobalsSystemSerialNumber (new); acLicensePoolInfraAlarm (updated); acLicensePoolApplicationAlarm (updated); acLicensePoolOverAllocationAlarm (updated); acTrackIdStateChangeAlarm (new); acModuleServiceAlarm; acClusterBandwidthAlarm (new); acSBAServicesStatusAlarm (updated); acKeepAlive (updated); acProxyConnectivity (updated)
52381	SBA-related SNMP removed (added to SBA documents).
52383	Typos; varbinds increased to 16 (new - acBoardTrapGlobalsDeviceName, acBoardTrapGlobalsDeviceInfo, acBoardTrapGlobalsDeviceDescription); acLicensePoolInfraAlarm (description updated); acLicensePoolApplicationAlarm (description updated); acLicenseKeyHitlessUpgradeAlarm (new)
52384	Source names added for PM MIB names; event source added to acPerformanceMonitoringThresholdCrossing; description updated for entConfigChange
52385	Source name for acPMSBCIPGroupInCallEstablishedDurationTable; Media Transcoding Cluster removed
52386	Updated descriptions: acPowerSupplyAlarm; acHwFailureAlarm; acHASystemFaultAlarm; acHASystemSwitchOverAlarm New alarm -acHANetworkMonitorAlarm
52389	Updated to Ver. 7.20A.200.019 New traps: acHAEthernetGroupAlarm; acHANetworkMismatchAlarm; acNGINXConfigurationIsInvalidAlarm; acNGINXPprocessIsNotRunningAlarm Updated traps: acHwFailureAlarm; acHASystemFaultAlarm; acHANetworkMonitorAlarm (OID); acHTTPProxyServiceAlarm
52391	Updated to Ver. 7.20A.202.112 Updated traps: AcPowerSupplyAlarm; acBoardTemperatureAlarm; acCertificateExpiryNotification changed to acCertificateExpiryAlarm; acLicensePoolApplicationAlarm; acIpGroupNoRouteAlarm; acIDSPolicyAlarm; acKeepAlive

LTRT	Description
	New traps: acCloudLicenseManagerAlarm; acFloatingLicenseAlarm Performance Monitoring - updated
52392	Updated to Ver. 7.20A.204.115 acAWSSecurityRoleAlarm
52393	acDataInterfaceStatus removed; acNATTraversalAlarm removed
52394	OIDs of performance monitoring MIBs; acProxyConnectionLost updated (severity); SNMPSysName updated
52395	Updated for Ver. 7.20A.252 Configuring performance monitoring thresholds; coder enums for acPMChannelsPerCoderTable; new acAnalogLineLeftOffhookAlarm; acIpGroupNoRouteAlarm (description updated); new PM MIBs (acPMActiveContextCountTable, acPMSBCInAttemptedCallsTable, acPMSBCOutAttemptedCallsTable, acPMSBCInEstablishedCallsTable, acPMSBCOutEstablishedCallsTable, acPMSBCMediaBrokenConnectionCallsTable, acPMSBCInShortCallsTable, acPMSBCOutShortCallsTable, acPMSBCInAttemptedRegistrationsTable, acPMSBCOutAttemptedRegistrationsTable, acPMSBCInSuccessfulRegistrationsTable, acPMSBCOutSuccessfulRegistrationsTable, acPMSBCIPGroupMediaBrokenConnectionCallsTable, acPMSBCIPGroupInShortCallsTable, acPMSBCIPGroupOutShortCallsTable, acPMSBCIPGroupInAttemptedRegistrationsTable, acPMSBCIPGroupOutAttemptedRegistrationsTable, acPMSBCIPGroupInSuccessfulRegistrationsTable, acPMSBCIPGroupOutSuccessfulRegistrationsTable, acPMSBCSRDInAttemptedCallsTable, acPMSBCSRDOutAttemptedCallsTable, acPMSBCSRDInEstablishedCallsTable, acPMSBCSRDOutEstablishedCallsTable, acPMSBCSRDMediaBrokenConnectionCallsTable, acPMSBCSRDInShortCallsTable, acPMSBCSRDOutShortCallsTable, acPMSBCSRDInAttemptedRegistrationsTable, acPMSBCSRDOutAttemptedRegistrationsTable, acPMSBCSRDInSuccessfulRegistrationsTable, acPMSBCSRDOutSuccessfulRegistrationsTable, acPMSBCInUserDefinedFailures<1-26>Table, acPMSBCOutUserDefinedFailures<1-26>Table, cPMSBCSRDInUserDefinedFailures<1-26>Table, acPMSBCSRDOutUserDefinedFailures<1-26>Table, acPMSBCIPGroupInUserDefinedFailures<1-26>Table, acPMSBCIPGroupOutUserDefinedFailures<1-26>Table, acPMSBCInCapsTable,

LTRT	Description
	acPMSBCOutCapsTable, acPMSBCSrdInCapsTable, acPMSBCSrdOutCapsTable
52396	acCDRServerAlarm alarm added
52397	Updated to Ver. 7.20A.254 AcFanTrayAlarm and acBoardTemperatureAlarm updated for Mediant 90xx; CLI command added to acBoardOverloadAlarm
52398	Typo fixed for acPMSIPSBCEstablishedCallsTable
52399	Updated to Ver. 7.20A.256.024 New PM MIB - acPMChannelsPerCoderG711Table; AcDSPFarmsMismatchAlarm (new); acRemoteMonitoringAlarm (new); acBoardEvResettingBoard (text updated); acMtcmClusterHaAlarm (updated); acMtceNetworkFailureAlarm (updated); acMtceSwUpgradeFailureAlarm (updated); acMediaClusterAlarm (new).
52407	Miscellaneous typos; acBoardEthernetLinkAlarm (description); acEthernetGroupAlarm (description); acFeatureKeyError (not supported note removed).
52416	acFlexLicenseManagerAlarm (new); acMeteringAlarm (new); alarm descriptions updated.
52426	acLicenseKeyHitlessUpgradeAlarm (only Local license); acEthernetGroupAlarm (description).
52430	IF-MIB removed.
52439	ifLinkUpDownTrapEnable (disabled and description); acPMSIPSBCAttemptedCallsTable (description)
52484	acInstallationFailureAlarm note for non-support.

Table of Contents

1 Introduction

This document provides you with supplementary information on Simple Network Management Protocol (SNMP) based management for your AudioCodes device . This information complements the information provided by the device's *User's Manual*, and includes SNMP configuration, SNMP traps (events and alarms), and SNMP performance monitoring MIBs.

- The SNMP MIB manual is supplied in the Software Release Package delivered with the device.
- For large deployments (for example, multiple devices in globally distributed enterprise offices) that need to be managed by central personnel, it is recommended to use AudioCodes One Voice Operations Center (OVOC). OVOC is not included in the device's supplied package. Contact AudioCodes for more information on its OVOC solution for large VoIP deployments.

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 third-party Network Management System (NMS) or AudioCodes One Voice Operations Center (OVOC), 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 an 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.

SNMP Standards and Objects

This section discusses the SNMP standards and SNMP objects.

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.

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 SNMP branches:

- **"mgmt":** Contains the standard SNMP objects usually supported (at least in part) by all network devices.
- **“private":** Contains those "extended" SNMP objects defined by network equipment vendors.
- **"experimental" and "directory":** 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).

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.

Supported MIBs

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

- **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):** Standard system group: sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices. You can replace the value of sysObjectID.0 with a variable value using the ini file parameter SNMPSysOid. This

parameter is polled during 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 (FQDN). If the name is unknown, the value is the zero-length string. If the [HostName] ini file parameter is configured, its' value overwrites the value of SNMPSysName.

- **RTP MIB:** The 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.

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:
  - 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.

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.
- **AcBoard MIB:** includes the acTrap group.

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

- **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**
- **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 supported).

  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 sent 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 by one of the following:
  - notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigGlobalEntryLimit

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

The table size (i.e., number of contained alarms) can be any value between 10 and 1,000 (default is 500)

- 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.

SNMP Interface Details

This subsection describes details of the SNMP interface needed when developing an Element Management System (EMS) for any AudioCodes devices, 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*.

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

Configuring Community Strings via the Web

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

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 (_)

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.

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.

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 to 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)

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.

Configuring SNMPv3 Users via 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.

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).

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.

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 Managers.

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 work from all Trusted Managers. In other words, there is no way to associate a community string with specific Trusted Managers.

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.

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 following procedure 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 following procedure 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 following procedure 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 effect immediately. The deleted trusted manager cannot access the device. The agent automatically removes the row in the snmpTargetAddrExtTable.

The following procedure 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.

SNMP Ports

The SNMP Request Port is 161 and the SNMP Trap Port is 162. These port numbers for SNMP requests and responses can be changed, by using the [SNMPPort] ini file parameter. The valid value is any valid UDP port number. The default is 161 (recommended).

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 ini File on the next page)
- SNMP (see Configuring Trap Managers via SNMP on page 17)

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 can be configured using the ini file parameter [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).

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

Configuring Trap Managers via ini File

In the ini file, the following parameters 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.

The following 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'
```

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

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.

When the device operates in HA mode, the SNMPEngineIDString parameter has the same value for both active and redundant devices (i.e., system identifier). If the devices return to Standalone mode (i.e., non-HA mode), you must configure the parameter to a NULL value (i.e., no value) on both devices. When the devices reset to the standalone mode, each device automatically sets this parameter to a unique value based on its serial number (S/N).

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 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.

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.

Alarm History

The device maintains a history of alarms that have been sent 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

4 Topology MIB Objects

This section describes the topology of the MIB objects.

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.

5 File Management

SNMP supports file download, upload, and removal.

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.

- 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.

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.

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

6 Performance Monitoring

Performance measurements (performance monitoring) are available for third- party performance monitoring systems 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, which causes the counters to reset to zero (0).

The device's performance measurements are provided by the following proprietary MIBs that are located under the acPerformance subtree, iso (1).org (3).dod (6).internet (1).private (4).enterprises(1).AudioCodes(5003).acPerformance(10):

- **acPMMedia:** Media-related (voice) monitoring such as RTP and DSP. The 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 (SIP) monitoring such as connections, commands.
  - CP Connection subtree – parameters include connection lifetime/state, counters for commands, retransmissions, active contexts, command success/failure and process time, transaction processing time and call attempts
  - SIP subtree
- **acPMSystem:** General device 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 and STUN-related statistics
- 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
- System NFS subtree – NFS-related parameters

Performance monitoring MIBs all have an identical, fixed structure, which includes two major subtrees:

- **Configuration subtree:** Allows configuration of general attributes of the MIB and specific attributes of the monitored objects. This subtree includes:
  - Reset Total Counters: Resets the "total" (see below) objects in all the MIB's tables, if they are defined.
  - Attributes subtrees: Number of subtrees in which scalars are used to configure high and low thresholds for relevant tables.
- **Data subtree:** Consists of monitored data and statistics, and includes:
  - 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 measured.

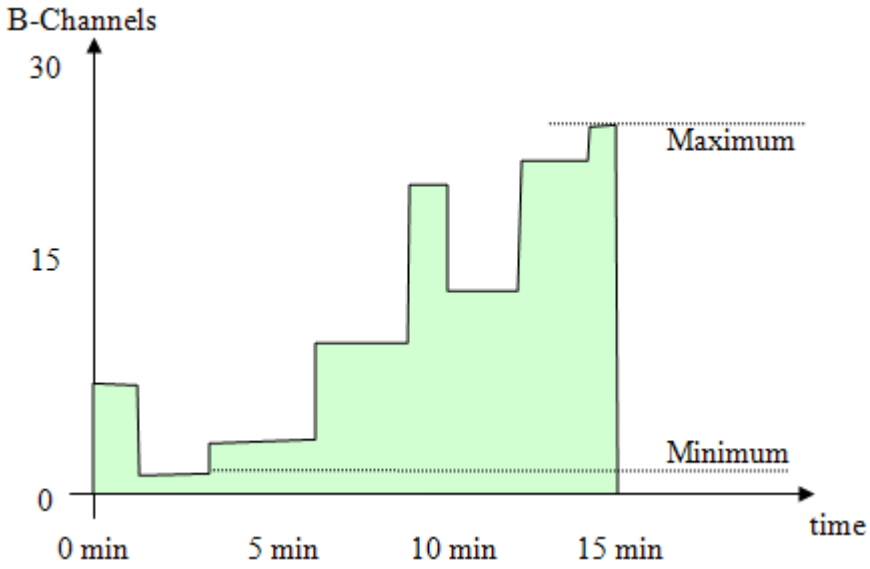
The device measures performance at fixed intervals of 15 minutes. The device keeps a record of the last two completed intervals. These intervals are used as a key in the MIB tables in which the performance monitoring results are presented. There are one or two indices in each table. If there are two, 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:

- **0:** Current interval (not completed)
- **1:** Last completed interval
- **2:** Second last completed interval

When the current interval (Interval 0) completes (reaches 15 minutes), Interval 2 is discarded, Interval 1 becomes Interval 2, Interval 0 becomes Interval 1, and a new Interval 0 is created.

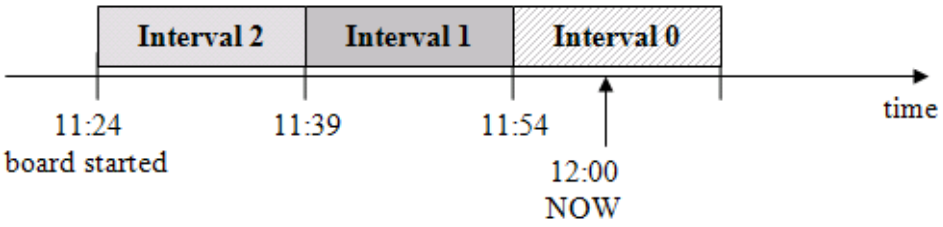
- The interval's start time is synchronized with the device's clock so that the intervals begin on the hour (e.g., 12:00). If you are using NTP, then it is likely that the last interval within the first hour after device startup will be cut short to accommodate for this synchronization.
- Some performance monitoring parameters support a history with more than two intervals. These include conference calls, trunk-test calls and digit-collect requests.
- An attribute whose value is -1 means that the attribute isn't relevant at that point of time.
- If the device has just started up and the first measuring interval has not elapsed, intervals 1 and 2 are not applicable and their data values are typically displayed as "-1" or as empty cells.

The following figure shows an example of a 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 (i.e., current interval), any GET on the parameter value will return a y-axis value at that moment. When the interval is complete (index 1 or 2), the gauge value is no longer relevant and other attributes become relevant such as the average (area in green divided by the interval length in seconds), which is called time-based statistics.

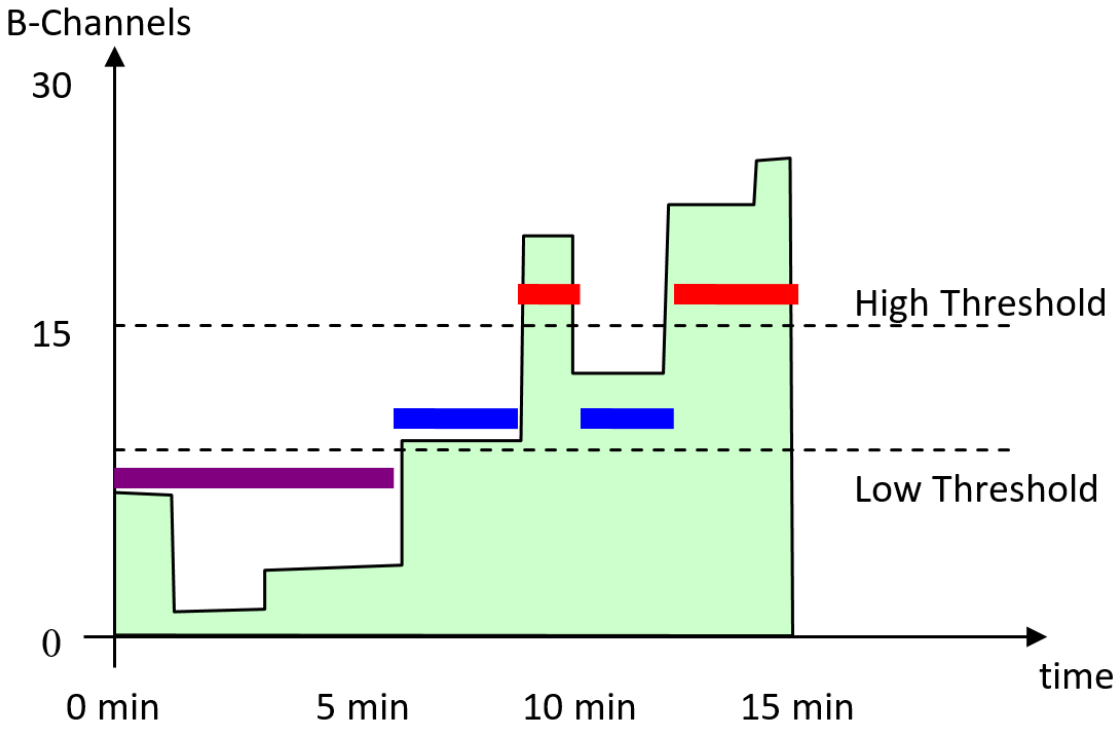
The following figure shows an example of the last three intervals. In this example, the device was powered up at 11:24. The first interval (of 15 minutes) ended at 11:39 and the second interval (of 15 minutes) ended at 11:54. The current interval (Interval 0) has not completed the 15 minutes. Typically, you would want the measured performance of the last completed interval (i.e., Interval 1).



The performance monitoring MIB tables can include the following properties (columns):

- **Table specific index:** This is a table key.
- **Interval:** Indicates the measured interval (0,1, or 2), which is a table key.
- **Val:** Indicates the value of the gauge or counter. This is the snapshot view of the device's current activity.
  - **Counter:** Cumulative value (only increases).
  - **Gauge:** Fluctuates in value (increases and decreases).
- **Average:** Indicates the average value within the interval.
- **Max:** Indicates the maximum gauge value during the interval.
- **Min:** Indicates the minimum gauge value during the interval.
- **Volume:** Indicates the number of times the gauge or counter was updated (i.e., 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.
- **Thresholds:**
  - **TimeBelowLowThreshod:** Indicates the percent (%) of the interval time for which the gauge was below the low threshold (if defined).
  - **TimeAboveHighThreshod:** Indicates the percent (%) of the interval time for which the gauge was above the high threshold (if defined).
  - **TimeBetweenThresholds:** Indicates the percent (%) of the interval time for which the gauge was between the low and high thresholds (if defined).

  The following figure shows an example of how the device calculates thresholds. The purple bar indicates the time when the element was below the low threshold (about 40% of the interval time), the blue bar indicates the time when the element was between the low and high threshold (about 30%), and the red bar indicates the time when the element was above the high threshold (about 30%).



The SNMP trap event acPerformanceMonitoringThresholdCrossing is sent every time the high or low threshold of a Performance Monitored MIB object is crossed (see Performance Monitoring Threshold-Crossing Trap on page 158). The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it returns to below the threshold. The trap's 'source varbind' indicates the object for which the threshold is crossed. To enable this feature, load an ini file to the device with the following parameter setting:

```
PM_EnableThresholdAlarms = 1
```

Once enabled, you can change the low and high threshold values from their default values, through ini file by using the following syntax:

```
PM_<MIB Source Name> = '1,<Low Threshold>,<High Threshold>,15'
```

where:

- *<MIB Source Name>:* The source name of the MIB (e.g., PM_TrunkUtilization, PM_NetUtilKBytes, and PM_gwIPGroupOutINVITEDialogs)
- *<Low Threshold>:* Defines the low-threshold value
- *<High Threshold>:* Defines the high-threshold value

The value "15" in the syntax is the measuring interval, which is always fixed at 15 minutes.

The following is an example of an ini file that configures the acPMSIPIPGroupOutInviteDialogsTable performance monitoring MIB (OID 1.3.6.1.4.1.5003.10.8.2.52.35) with a low threshold of 10 and a high threshold of 18:

```
PM_gwIPGroupOutINVITEDialogs = '1,10,18,15'
```

If you download (save) the device's ini file, it includes all SNMP performance monitoring MIBs whose thresholds (low and/or high) you have changed from default. To apply these same threshold values to other devices, load the file to the other devices.

- **FullDayAverage:** Indicates the 24-hour average.
- **Total:** (Applicable only to Counters) Indicates the summation of all counter values. In other words, it does not reset to zero for each new interval. However, the total does reset after a device reset. In addition, you can reset this property per MIB module, by setting the ResetTotal object to the value 2:
  - PM-Control: acPMControlConfigurationResetTotalCounters
  - PM-Media: acPMMediaConfigurationResetTotalCounters
  - PM-System: acPMSystemConfigurationResetTotalCounters

  For example:

  ```
  acPMMediaConfigurationResetTotalCounters.0 (integer) resetTotalCounters (2)
  ```

- **StateChanges:** Indicates the number of times a state (mostly active/non-active) was toggled.

Not all the properties listed above are applicable to every Performance Monitoring MIB. Properties that are not applicable are displayed as "-1" or as an empty cell.

SNMP Performance Monitoring MIBs

This section describes the Performance Monitoring SNMP MIBs.

The tables in this section use check marks "√" and crosses "x" to indicate support for the specific MIB property:

- "G/C": gauge / counter
- "Int": measured interval
- "Val": value of gauge or counter
- "Min": minimum gauge value
- "Max": maximum gauge value
- "Avg": average within the interval
- "TbLT": percentage of interval time that value was below low threshold
- "TbT": percentage of interval time that value was between low and high thresholds
- "TaHT": percentage of interval time that value was above high threshold
- "HT": configured or default high threshold
- "LT": configured or default low threshold

Performance Monitoring MIBs for IP Network Interfaces

The following table lists the performance monitoring MIBs for IP network interfaces.

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

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMNetUtilKBytesTable ■ OID: 1.3.6.1.4.1.5003.10.11.2.31.1 ■ Source Name: PM_NetUtilKBytes											
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. OVOC parameter name: Number of Incoming / Outgoing Kbytes ■ High threshold: acPMNetUtilsAttributesKBytesHighThreshold	G	15	✓	✓	✓	✓	✓	✓	✓	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
(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)											
■ MIB Name: acPMNetUtilPacketsTable ■ OID: 1.3.6.1.4.1.5003.10.11.2.31.2 ■ Source Name: PM_NetUtilPackets											
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. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMNetUtilDiscardedPacketsTable ■ OID: 1.3.6.1.4.1.5003.10.11.2.31.3 ■ Source Name: PM_NetUtilDiscardedPackets											
Indicates the number of	C	1	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
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. OVOC parameter name: Number of Incoming Discarded Pkts.		5									

Performance Monitoring MIBs for Media Realms

The following table lists the performance monitoring MIBs for Media Realms.

Table 6-2: Performance Monitoring MIBs for Media Realms

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMMediaRealmPacketLossRxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.10 ■ Source Name: PM_MediaRealmPacketLossRx											
Indicates the received RTP packet loss (reported by RTCP) per Media Realm.	G	15	×	✓	✓	✓	✓	✓	✓	50	30
■ MIB Name: acPMMediaRealmPacketLossTxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.11 ■ Source Name: PM_MediaRealmPacketLossTx											
Indicates the transmitted RTP packet loss (reported by RTCP)	G	15	×	✓	✓	✓	✓	✓	✓	50	30

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
per Media Realm.											
■ MIB Name: acPMMediaRealmBytesTxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.1 ■ Source Name: PM_MediaRealmBytesTx											
Indicates the number of bytes received in RTCP data, per Media Realm. ■ High threshold: acPMMediaRealmAttributes MediaRealmBytesTxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.1) ■ Low threshold: acPMMediaRealmAttributes MediaRealmBytesTxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.2)	G	15	×	✓	✓	✓	✓	✓	✓	1500000	1000000
■ MIB Name: acPMMediaRealmBytesRxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.2 ■ Source Name: PM_MediaRealmBytesRx											
Indicates the number of bytes received in RTCP data, per Media Realm. ■ High threshold: acPMMediaRealmAttributes MediaRealmBytesRxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.3) ■ Low threshold: acPMMediaRealmAttributes MediaRealmBytesRxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.4)	G	15	×	✓	✓	✓	✓	✓	✓	1500000	1000000

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMMediaRealmPacketsTxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.3 ■ Source Name: PM_MediaRealmPacketsTx											
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
■ MIB Name: acPMMediaRealmPacketsRxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.4 ■ Source Name: PM_MediaRealmPacketsRx											
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
■ MIB Name: acPMMediaRealmVERealmPacketDelayTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.53.5 ■ Source Name: PM_VERealmPacketDelay											
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
■ MIB Name: acPMMediaRealmVERealmPacketJitterTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.6 ■ Source Name: PM_VERealmPacketJitter											
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
■ MIB Name: acPMMediaRealmRealmMOSTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.53.7 ■ Source Name: PM_RealmMOS											
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
■ MIB Name: acPMMediaRealmBwRxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.8 ■ Source Name: PM_MediaRealmBwRx											
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
■ MIB Name: acPMMediaRealmBwTxTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.53.9											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_MediaRealmBwTx											
Indicates the average bandwidth for Tx bytes, per Media Realm. ■ High threshold: acPMMediaRealmAttributes MediaRealmBwTxHighThreshold (1.3.6.1.4.1.5003.10.8.1.35.17) ■ Low threshold: acPMMediaRealmAttributes MediaRealmBwTxLowThreshold (1.3.6.1.4.1.5003.10.8.1.35.18)	G	15	✓	✓	✓	✓	×	×	×	1500000	0

Performance Monitoring MIBs for VoIP Calls

The following table lists the performance monitoring MIBs for VoIP calls.

Table 6-3: Performance Monitoring MIBs for VoIP Calls

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMChannelsPerCoderTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.22 ■ Source Name: PM_VEChannelsPerCoder											
Indicates the number of active channels per coder, where the Index denotes the coder: 0 (G.711), 1 (G.723), 2 (G.728), 3 (G.729A), 4 (G.729E), 5 (AMR), 6 (G.729EV), 7 (EG.711), 8 (EVRC), 9 (Unknown Coder), 10 (G.726), 11 (RTA), 12 (SILK), 13 (AMR-WB), 14 (G.722), 15	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G / C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
(G.727), 16 (GSM), 17 (QCELP), 18 (VOX ADPCM), 19 (iLBC), 20 (Speex). ■ 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)											
■ MIB Name: acPMChannelsPerCoderG711Table ■ OID: 1.3.6.1.4.1.5003.10.7.2.26 ■ Source Name: PM_VeG711Channels											
Indicates the number of active channels per G.711 A-law or G.711 U-law, where the Index denotes the coder type: 0 (G.711 A-law) and 1 (G.711 U-law). ■ 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMModuleRTPPacketLossRxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.9 ■ Source Name: PM_veModuleRTPPacketLossRx											
Indicates the Rx RTP packet loss (reported by RTCP), during the time Interval. OVOC parameter name: Rx RTP Packet Loss.	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ 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)											
■ MIB Name: acPMModuleRTPPacketLossTxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.10 ■ Source Name: PM_veModuleRTPPacketLossTx											
Indicates the Tx RTP packet loss (reported by RTCP), during the time Interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMModulePacketDelayTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.1 ■ Source Name: PM_veModulePacketDelay											
Indicates the RTP packet delay during the collection time interval. OVOC parameter name: RTP delay. ■ High threshold: acPMNetworkingAttributesPacketDelayHighThreshold (1.3.6.1.4.1.5003.10.7.1.33.1)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Low threshold: acPMNetworkingAttributesPacketDelayLowThreshold (1.3.6.1.4.1.5003.10.7.1.33.2)											
■ MIB Name: acPMModulePacketJitterTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.2 ■ Source Name: PM_veModulePacketJitter											
Indicates the RTP packet jitter during the collection time interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMModuleRTPBytesRxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.4 ■ Source Name: PM_veModuleRTPBytesRx											
Indicates the Tx RTP bytes during the collection time interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMModuleRTPBytesTxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.3 ■ Source Name: PM_veModuleRTPBytesTx											
Indicates the Rx RTP bytes during the collection time interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMModuleRTPPacketsRxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.6 ■ Source Name: PM_RTPModulePacketsRx											
Indicates the Rx RTP packets during the collection time interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMModuleRTPPacketsTxTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.31.21.5 ■ Source Name: PM_RTPModulePacketsTx											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the Tx RTP Packets during the collection time interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIBs for SIP Messages

The following table lists the performance monitoring MIBs for SIP messages.

Table 6-4: Performance Monitoring MIBs for SIP Messages

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSIPActiveSIPTransactionsPerSecondTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.41 ■ Source Name: PM_gwActiveSIPTransacionsPerSecond											
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: acPMSipAttributesActiveSIPTran	G	15	✓	×	×	×	×	×	×	0	0

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
sactionsPerSecondLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.36)											
■ MIB Name: acPMSIPIPGroupInviteDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.22 ■ Source Name: PM_gwIPGroupINVITEDialogs											
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

Performance Monitoring MIBs for Calls per IP Group

The following table lists the performance monitoring MIBs for SBC calls per IP Group.

For additional performance monitoring MIBs for SBC calls per IP Group, see SBC Calls per IP Group on page 58.

Table 6-5: Performance Monitoring MIBs for Call Sessions per IP Group

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCIPGroupInAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.3 ■ Source Name: PM_gwSBCIPGroupInAttemptedCalls											
Indicates the	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
number of attempted incoming calls per IP Group.											
■ MIB Name: acPMSBCIPGroupOutAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.6 ■ Source Name: PM_gwSBCIPGroupOutAttemptedCalls											
Indicates the number of attempted outgoing calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupRoutingFailedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.9 ■ Source Name: PM_gwSBCIPGroupRoutingFailedCalls											
Indicates the number of failed call routing per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInNoResourcesCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.18 ■ Source Name: PM_gwSBCIPGroupInNoResourcesCalls											
Indicates the number of incoming call	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
resource allocation failures per IP Group.											
■ MIB Name: acPMSBCIPGroupOutNoResourcesCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.19 ■ Source Name: PM_gwSBCIPGroupOutNoResourcesCalls											
Indicates the number of outgoing call resource allocation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInNoMatchCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.20 ■ Source Name: PM_gwSBCIPGroupInNoMatchCalls											
Indicates the number of incoming call media negotiation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutNoMatchCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.21 ■ Source Name: PM_gwSBCIPGroupOutNoMatchCalls											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of outgoing call media negotiation failures per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInBusyCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.22 ■ Source Name: PM_gwSBCIPGroupInBusyCalls											
Indicates the number of incoming busy calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutBusyCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.23 ■ Source Name: PM_gwSBCIPGroupOutBusyCalls											
Indicates the number of outgoing busy calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInNoAnswerCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.24 ■ Source Name: PM_gwSBCIPGroupInNoAnswerCalls											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of incoming no-answer calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutNoAnswerCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.25 ■ Source Name: PM_gwSBCIPGroupOutNoAnswerCalls											
Indicates the number of outgoing no-answer calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInForwardedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.26 ■ Source Name: PM_gwSBCIPGroupInForwardedCalls											
Indicates the number of incoming forwarded calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutForwardedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.29 ■ Source Name: PM_gwSBCIPGroupOutForwardedCalls											
Indicates the	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
number of outgoing forwarded calls per IP Group.											
■ MIB Name: acPMSBCIPGroupInGeneralFailedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.32 ■ Source Name: PM_gwSBCIPGroupInGeneralFailedCalls											
Indicates the number of incoming calls that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutGeneralFailedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.35 ■ Source Name: PM_gwSBCIPGroupOutGeneralFailedCalls											
Indicates the number of outgoing calls that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.38											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwSBCIPGroupInEstablishedCalls											
Indicates the number of incoming established calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.41 ■ Source Name: PM_gwSBCIPGroupOutEstablishedCalls											
Indicates the number of outgoing established calls per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

IP-to-Tel and Tel-to-IP Calls

The following table lists the performance monitoring MIBs for IP-to-Tel and Tel-to-IP calls.

> In the MIB tables, Index 0 indicates Tel-to-IP calls and Index 1 indicates IP-to-Tel calls.

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

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSIPAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.1 ■ Source Name: PM_gwAttemptedCalls											

Performance Monitoring MIB	G / C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of attempted calls (Index 1) during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Call Attempts	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMCPCallAttemptsPerSecTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.31.10 ■ Source Name: PM_CPCallAttemptsPerSec											
Indicates the number of attempted calls per second. It counts the number of SIP INVITE messages per second. ■ High threshold: acPMCPConnectionAttributesCallAttemptsPerSecHighThreshold (1.3.6.1.4.1.5003.10.8.1.32.19) ■ Low threshold: acPMCPConnectionAttributesCallAttemptsPerSecLowThreshold (1.3.6.1.4.1.5003.10.8.1.32.20)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0
■ MIB Name: acPMActiveContextCountTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.31.5 ■ Source Name: PM_ActiveContextCount											
Indicates the number of Gateway calls. ■ High threshold: acPMActiveContextCountTimeAboveHighThreshold (1.3.6.1.4.1.5003.10.8.2.31.5.1.9) ■ Low threshold: acPMActiveContextCountTimeBelowLowThreshold (1.3.6.1.4.1.5003.10.8.2.31.5.1.7)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSIPCallDurationTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.2 ■ Source Name: PM_gwCallDuration											
Indicates the call duration of established calls during last interval. OVOC 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
■ MIB Name: acPMSIPNoMatchCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.3 ■ Source Name: PM_gwNoMatchCalls											
Indicates the number of calls that failed due to mismatched media server capabilities for calls, during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Matched Capabilities.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPBusyCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.4 ■ Source Name: PM_gwBusyCalls											
Indicates the number of calls that failed as a result of a busy line, during last interval. OVOC parameter name: IP to Tel /	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Tel to IP Number of Calls Terminated due to a Busy Line.											
■ MIB Name: acPMSIPNoAnswerCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.5 ■ Source Name: PM_gwNoAnswerCalls											
Indicates the number of calls that weren't answered during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Calls Terminated due to No Answer.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPNoRouteCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.6 ■ Source Name: PM_gwNoRouteCalls											
Indicates the number of calls whose destinations weren't found during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Route.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPFailCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.7 ■ Source Name: PM_gwFailCalls											
This counter is incremented as a result of calls that fail due to reasons not covered by the other counters during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Failed Calls due to Other reasons.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.8											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwEstablishedCalls											
Indicates the number of established calls during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Established Calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPFaxAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.9 ■ Source Name: PM_gwFaxAttemptedCalls											
Indicates the number of attempted fax calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPFaxSuccessCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.10 ■ Source Name: PM_gwFaxSuccessCalls											
Indicates the number of successfully established fax calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPForwardedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.11 ■ Source Name: PM_gwForwardedCalls											
Indicates the number of calls that were terminated due to a call forward during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Calls Terminated due to Forward.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPNoResourcesCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.12 ■ Source Name: PM_gwNoResourcesCalls											
Indicates the number of calls that failed due to unavailable resources	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
or a media server lock during last interval. OVOC parameter name: IP to Tel / Tel to IP Number of Failed Calls due to No Resources.											
■ MIB Name: acPMSIPTel2IPTrunkEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.13 ■ Source Name: PM_gwTel2IPTrunkEstablishedCalls											
Indicates the current number of established calls pertaining to a trunk for Tel-to-IP calls.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIP2TelTrunkEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.14 ■ Source Name: PM_gwIP2TelTrunkEstablishedCalls											
Indicates the current number of established calls pertaining to a trunk for IP-to-Tel calls.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPTel2IPTrunkGroupEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.15 ■ Source Name: PM_gwTel2IPTrunkGroupEstablishedCalls											
Indicates the current number of established calls pertaining to a Trunk Group for Tel-to-IP calls.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIP2TelTrunkGroupEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.16 ■ Source Name: PM_gwIP2TelTrunkGroupEstablishedCalls											
Indicates the current number of established calls pertaining to a Trunk Group for IP-to-Tel calls.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIBs for SBC Application

This section describes the performance monitoring MIBs of the SBC application.

SBC Sessions

The following table lists the performance monitoring MIBs for SBC sessions. For MIBs that have low and high thresholds, if a threshold is crossed the device sends the acPerformanceMonitoringThresholdCrossing trap (see Performance Monitoring Threshold-Crossing Trap on page 158).

Table 6-7: Performance Monitoring MIBs for SBC Sessions

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSIPSBCAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.42 ■ Source Name: PM_gwSBCAttemptedCalls											
Indicates the number of attempted SBC calls. It applies only to SIP dialog-initiating INVITE messages and counts both incoming and outgoing legs per call. Therefore, each successful call increments the counter by 2. If the INVITE fails Classification stage, only the incoming side is counted (i.e., counter incremented only by 1). ■ 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
■ MIB Name: acPMSBCInAttemptedCallsTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.54.65 ■ Source Name: PM_gwSBCInAttemptedCalls											
Indicates the total number of attempted incoming SBC calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.67 ■ Source Name: PM_gwSBCOutAttemptedCalls											
Indicates the total number of attempted outgoing SBC calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPSBCEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.43 ■ Source Name: PM_gwSBCEstablishedCalls											
Indicates 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
■ MIB Name: acPMSBCInEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.69 ■ Source Name: PM_gwSBCInEstablishedCalls											
Indicates the total number of incoming established SBC calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutEstablishedCallsTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.54.71 ■ Source Name: PM_gwSBCOutEstablishedCalls											
Indicates the total number of outgoing established SBC calls.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCMediaBrokenConnectionCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.151.1 ■ Source Name: PM_gwSBCMediaBrokenConnectionCalls											
Indicates the total number of established calls that were disconnected because no RTP packets (media) were received for a user-defined period (configured by the BrokenConnectionEventTimeout parameter).	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCInShortCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.1 ■ Source Name: PM_gwSBCInShortCalls											
Indicates the total number of incoming calls whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutShortCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.2 ■ Source Name: PM_gwSBCOutShortCalls											
Indicates the total number of outgoing calls whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCInAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.1 ■ Source Name: PM_gwSBCInAttemptedRegistrations											
Indicates the number of incoming attempted SBC registrations.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.2 ■ Source Name: PM_gwSBCOutAttemptedRegistrations											
Indicates the number of outgoing attempted SBC registrations.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCInSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.1 ■ Source Name: PM_gwSBCInSuccessfulRegistrations											
Indicates the number of incoming successful registrations.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.2 ■ Source Name: PM_gwSBCOutSuccessfulRegistrations											
Indicates the number of outgoing successful registrations.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCMediaLegsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.47 ■ Source Name: PM_gwSBCMediaLegs											
Indicates the number of media (RTP) session resources	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
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)											
■ MIB Name: acPMSBCTranscodingSessionsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.48 ■ Source Name: PM_gwSBCTranscodingSessions											
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)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

SBC Calls per IP Group

The following table lists the performance monitoring MIBs for SBC calls per IP Group.

For additional performance monitoring MIBs for SBC calls per IP Group, see Performance Monitoring MIBs for Calls per IP Group on page 42.

Table 6-8: Performance Monitoring MIBs for SBC Calls per IP Group

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCIPGroupInCallEstablishedDurationTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.1 ■ Source Name: PM_gwSBCIPGroupInCallEstablishedDuration											
Indicates the call duration of the last incoming established SBC call per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutCallEstablishedDurationTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.2 ■ Source Name: PM_gwSBCIPGroupOutCallEstablishedDuration											
Indicates the call duration of the last outgoing established SBC call per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAttemptedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.4 ■ Source Name: PM_gwSBCIPGroupInAttemptedSUBSCRIBEDialogs											
Indicates the number of attempted incoming SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAttemptedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.5 ■ Source Name: PM_gwSBCIPGroupInAttemptedOtherDialogs											
Indicates the number of attempted incoming dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAttemptedSubscribeDialogsTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.54.7 ■ Source Name: PM_gwSBCIPGroupOutAttemptedSUBSCRIBEDialogs											
Indicates the number of attempted outgoing SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAttemptedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.8 ■ Source Name: PM_gwSBCIPGroupOutAttemptedOtherDialogs											
Indicates the number of attempted outgoing dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupRoutingFailedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.10 ■ Source Name: PM_gwSBCIPGroupRoutingFailedSUBSCRIBEDialogs											
Indicates the number of failed call routing of SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupRoutingFailedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.11 ■ Source Name: PM_gwSBCIPGroupRoutingFailedOtherDialogs											
Indicates the number of failed call routing of all dialogs other than SUBSCRIBE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAdmissionFailedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.12											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwSBCIPGroupInAdmissionFailedCalls											
Indicates the number of failed incoming dialogs due to Admission Control rules per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAdmissionFailedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.13 ■ Source Name: PM_gwSBCIPGroupInAdmissionFailedSUBSCRIBEDialogs											
Indicates the number of failed incoming SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAdmissionFailedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.14 ■ Source Name: PM_gwSBCIPGroupInAdmissionFailedOtherDialogs											
Indicates the number of failed incoming dialogs other than SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAdmissionFailedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.15 ■ Source Name: PM_gwSBCIPGroupOutAdmissionFailedCalls											
Indicates the number of failed outgoing dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCIPGroupOutAdmissionFailedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.16 ■ Source Name: PM_gwSBCIPGroupOutAdmissionFailedSUBSCRIBEDialogs											
Indicates the number of failed outgoing SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAdmissionFailedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.17 ■ Source Name: PM_gwSBCIPGroupOutAdmissionFailedOtherDialogs											
Indicates the number of failed outgoing dialogs other than SUBSCRIBE dialogs pertaining to Admission Control per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInForwardedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.27 ■ Source Name: PM_gwSBCIPGroupInForwardedSUBSCRIBEDialogs											
Indicates the number of incoming forwarded SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInForwardedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.28 ■ Source Name: PM_gwSBCIPGroupInForwardedOtherDialogs											
Indicates the number of incoming forwarded dialogs other than SUBSCRIBE	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
and INVITE dialogs per IP Group.											
■ MIB Name: acPMSBCIPGroupOutForwardedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.30 ■ Source Name: PM_gwSBCIPGroupOutForwardedSUBSCRIBEDialogs											
Indicates the number of outgoing forwarded SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutForwardedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.31 ■ Source Name: PM_gwSBCIPGroupOutForwardedOtherDialogs											
Indicates the number of outgoing forwarded dialogs other than SUBSCRIBE and INVITE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInGeneralFailedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.33 ■ Source Name: PM_gwSBCIPGroupInGeneralFailedSUBSCRIBEDialogs											
Indicates the number of incoming SUBSCRIBE dialogs that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInGeneralFailedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.34 ■ Source Name: PM_gwSBCIPGroupInGeneralFailedOtherDialogs											
Indicates the number of incoming dialogs	G	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
other than SUBSCRIBE and INVITE that failed due to general fail reason per IP Group.											
■ MIB Name: acPMSBCIPGroupOutGeneralFailedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.36 ■ Source Name: PM_gwSBCIPGroupOutGeneralFailedSUBSCRIBEDialogs											
Indicates the number of outgoing SUBSCRIBE dialogs that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutGeneralFailedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.37 ■ Source Name: PM_gwSBCIPGroupOutGeneralFailedOtherDialogs											
Indicates the number of outgoing dialogs other than SUBSCRIBE and INVITE that failed due to general fail reason per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInEstablishedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.39 ■ Source Name: PM_gwSBCIPGroupInEstablishedSUBSCRIBEDialogs											
Indicates the number of incoming established SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInEstablishedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.40 ■ Source Name: PM_gwSBCIPGroupInEstablishedOtherDialogs											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of incoming established dialogs other than SUBSCRIBE and INVITE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutEstablishedSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.42 ■ Source Name: PM_gwSBCIPGroupOutEstablishedSUBSCRIBEDialogs											
Indicates the number of outgoing established SUBSCRIBE dialogs per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutEstablishedOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.43 ■ Source Name: PM_gwSBCIPGroupOutEstablishedOtherDialogs											
Indicates the number of outgoing established dialogs other than SUBSCRIBE and INVITE per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAbnormallyTerminatedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.44 ■ Source Name: PM_gwSBCIPGroupInAbnormallyTerminatedCalls											
Indicates the number of incoming calls that were abnormally terminated per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAbnormallyTerminatedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.45											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwSBCIPGroupOutAbnormallyTerminatedCalls											
Indicates the number of outgoing calls that were abnormally terminated per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupMediaBrokenConnectionCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.151.3 ■ Source Name: PM_gwSBCIPGroupMediaBrokenConnectionCalls											
Indicates the number of established calls per IP Group that were disconnected because no RTP packets (media) were received for a user-defined period (configured by the BrokenConnectionEventTimeout parameter).	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInShortCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.5 ■ Source Name: PM_gwSBCIPGroupInShortCalls											
Indicates the number of incoming calls per IP Group, whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutShortCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.6 ■ Source Name: PM_gwSBCIPGroupOutShortCalls											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of outgoing calls per IP Group, whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.5 ■ Source Name: PM_gwSBCIPGroupInAttemptedRegistrations											
Indicates the number of incoming attempted user registrations per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.6 ■ Source Name: PM_gwSBCIPGroupOutAttemptedRegistrations											
Indicates the number of outgoing attempted user registrations per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.5 ■ Source Name: PM_gwSBCIPGroupInSuccessfulRegistrations											
Indicates the number of successful incoming registrations per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.6											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwSBCIPGroupOutSuccessfulRegistrations											
Indicates the number of successful outgoing registrations per IP Group.	C	15	✓	×	×	×	×	×	×	×	×

SBC Calls per SRD

The following table lists the performance monitoring MIBs for SBC calls per SRD.

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

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCSRDInAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.66 ■ Source Name: PM_gwSBCSRDInAttemptedCalls,											
Indicates the number of incoming attempted calls per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDOutAttemptedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.68 ■ Source Name: PM_gwSBCSRDOutAttemptedCalls											
Indicates the number of outgoing attempted calls per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDInEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.70 ■ Source Name: PM_gwSBCSRDInEstablishedCalls											
Indicates the number of incoming calls per SRD that were	C	15	✓	×	×	×	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
established.											
■ MIB Name: acPMSBCSRDOutEstablishedCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.72 ■ Source Name: PM_gwSBCSRDOutEstablishedCalls											
Indicates the number of outgoing calls per SRD that were established.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDMediaBrokenConnectionCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.151.2 ■ Source Name: PM_gwSBCSRDMediaBrokenConnectionCalls											
Indicates the number of established calls per SRD that were disconnected because no RTP packets (media) were received for a user-defined period (configured by the BrokenConnectionEventTimeout parameter).	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDInShortCallsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.3 ■ Source Name: PM_gwSBCSRDInShortCalls											
Indicates the number of incoming calls per SRD, whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDOutShortCallsTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.54.152.4 ■ Source Name: PM_gwSBCSRDOutShortCalls											
Indicates the number of outgoing calls per SRD, whose duration was less than the value configured by the ShortCallSeconds parameter.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDInAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.3 ■ Source Name: PM_gwSBCSRDInAttemptedRegistrations											
Indicates the number of incoming attempted user registrations per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDOutAttemptedRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.153.4 ■ Source Name: PM_gwSBCSRDOutAttemptedRegistrations											
Indicates the number of outgoing attempted user registrations per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDInSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.3 ■ Source Name: PM_gwSBCSRDInSuccessfulRegistrations											
Indicates the number of incoming successful registrations per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDOutSuccessfulRegistrationsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.154.4 ■ Source Name: PM_gwSBCSRDOutSuccessfulRegistrations											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the number of outgoing successful registrations per SRD.	C	15	✓	×	×	×	×	×	×	×	×

SBC Call Admission Control

The following table lists the performance monitoring MIBs for SBC Call 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 with high and low thresholds, if a threshold is crossed the device sends the acPerformanceMonitoringThresholdCrossing trap (see Performance Monitoring Threshold-Crossing Trap on page 158).

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

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSIPSRDDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.17 ■ Source Name: PM_gwSRDDialogs											
Indicates the number of all dialogs currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPSRDInviteDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.18 ■ Source Name: PM_gwSRDINVITEDialogs											
Indicates the number of all calls (initiated by SIP:INVITE) currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPSRDSubscribeDialogsTable											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.52.19 ■ Source Name: PM_gwSRDSUBSCRIBEDialogs											
Indicates the number of all SUBSCRIBE dialogs (initiated by SIP:SUBSCRIBE) currently being handled by the SBC per SRD.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPSRDOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.20 ■ Source Name: PM_gwSRDOtherDialogs											
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	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIPGroupDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.21 ■ Source Name: PM_gwIPGroupDialogs											
Indicates the number of all dialogs currently being handled by the SBC per IP Group.	G	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIPGroupSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.23 ■ Source Name: PM_gwIPGroupSUBSCRIBEDialogs											
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)	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Low threshold: acPMSipAttributesIPGroupSubscribeDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.28)											
■ MIB Name: acPMSIPIPGroupOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.24 ■ Source Name: PM_gwIPGroupOtherDialogs											
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	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIPGroupInOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.34 ■ Source Name: PM_gwIPGroupInOtherDialogs											
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	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIPGroupOutOtherDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.37 ■ Source Name: PM_gwIPGroupOutOtherDialogs											
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	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSIPIPGroupInInviteDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.32 ■ Source Name: PM_gwIPGroupInINVITEDialogs											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
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
■ MIB Name: acPMSIPIPGroupInSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.33 ■ Source Name: PM_gwIPGroupInSUBSCRIBEDialogs											
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
■ MIB Name: acPMSIPIPGroupOutInviteDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.35 ■ Source Name: PM_gwIPGroupOutINVITEDialogs											
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:	G	15	✓	✓	✓	✓	✓	✓	✓	0	0

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
acPMSipAttributesIPGroupOutInviteDialogsLowThreshold (1.3.6.1.4.1.5003.10.8.1.34.20)											
■ MIB Name: acPMSIPIPGroupOutSubscribeDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.36 ■ Source Name: PM_gwIPGroupOutSUBSCRIBEDialogs											
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
■ MIB Name: acPMSIPIPGroupOutDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.31 ■ Source Name: PM_gwIPGroupOutDialogs											
Indicates the number of outgoing dialogs per IP Group.	C	15	✓	×	×	×	×	×	×	×	û
■ MIB Name: acPMSIPInvitedDialogsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.38 ■ Source Name: PM_gwINVITEDialogs											
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	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
(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)											
■ MIB Name: acPMSIPSubscribeDialogTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.52.39 ■ Source Name: PM_gwSUBSCRIBEDialogs											
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
■ MIB Name: acPMSBCRegisteredUsersTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.46 ■ Source Name: PM_gwSBCRegisteredUsers											
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

SBC Call Quality of Service

The following table lists the performance monitoring MIBs 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 sent (see acASRThresholdAlarm, AcNERThresholdAlarm, and acACDThresholdAlarm).

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

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCAsrTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.49 ■ Source Name: PM_gwSBCASR											
Indicates the Answer-seizure Ratio (ASR) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupAsrTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.50 ■ Source Name: PM_gwSBCIPGroupASR											
Indicates ASR per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCSrdAsrTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.51 ■ Source Name: PM_gwSBCSRDASR											
Indicates	G	15	✓	✓	✓	✓	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
ASR per SRD.											
■ MIB Name: acPMSBCNerTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.55 ■ Source Name: PM_gwSBCNER											
Indicates the Network Effectiveness Ratio (NER) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupNerTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.56 ■ Source Name: PM_gwSBCIPGroupNER											
Indicates NER per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCSrdNerTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.57 ■ Source Name: PM_gwSBCSRDNER											
Indicates NER per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCAcdTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.52 ■ Source Name: PM_gwSBCACD											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
Indicates the Average Call Duration (ACD) for all (global) entities (i.e., all IP Groups and SRDs).	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupAcdTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.53 ■ Source Name: PM_gwSBCIPGroupACD											
Indicates ACD per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCSrdAcdTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.54 ■ Source Name: PM_gwSBCSRDACD											
Indicates ACD per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCInCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.59 ■ Source Name: PM_gwSBCInCPS											
Indicates the number of incoming calls per second.	G	15	✓	✓	✓	✓	×	×	×	×	×

SBC User-Defined SIP Failure Responses

You can configure up to 26 user-defined PM groups to count SIP responses that are received (or generated by the device) to indicate call failures. You need to specify the responses that you want counted as well as the associated SIP method (INVITE or REGISTER). User-defined PMs are configured in the Web interface's User Defined Failure PM table (UserDefinedFailurePM). For more information, refer to the *User's Manual*.

Table 6-12: User-defined Performance Monitoring MIBs for SIP Failure Responses

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCInUserDefinedFailures<1-26>Table ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.1 ■ Source Name: PM_gwSBCInUserDefinedFailures<1-26>											
Indicates the total number of incoming failure responses (i.e., all IP Groups and SRDs).	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCOutUserDefinedFailures<1-26>Table ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.2 ■ Source Name: PM_gwSBCOutUserDefinedFailures<1-26>											
Indicates the total number of outgoing failure responses (i.e., all IP Groups and SRDs).	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDInUserDefinedFailures<1-26>Table											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.3 ■ Source Name: PM_gwSBCSRDInUserDefinedFailures<1-26>											
Indicates the number of incoming failure responses per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCSRDOutUserDefinedFailures<1-26>Table ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.4 ■ Source Name: PM_gwSBCSRDOutUserDefinedFailures<1-26>											
Indicates the number of outgoing failure responses per SRD.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInUserDefinedFailures<1-26>Table ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.5 ■ Source Name: PM_gwSBCIPGroupInUserDefinedFailures<1-26>											
Indicates the number of incoming failure responses per IP Group.	C	15	✓	×	×	×	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupOutUserDefinedFailures<1-26>Table ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.155.1.6											

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ Source Name: PM_gwSBCIPGroupOutUserDefinedFailures<1-26>											
Indicates the number of outgoing failure responses per IP Group.	C	15	✓	×	×	×	×	×	×	×	×

SBC Calls Per Second

The following table lists the performance monitoring MIBs for SBC calls per second (CPS).

Table 6-13: Performance Monitoring MIBs for SBC Calls Per Second

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMSBCInCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.59 ■ Source Name: PM_gwSBCInCPS											
Indicates the number of CPS for incoming SBC calls.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCOutCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.60 ■ Source Name: PM_gwSBCOutCPS											
Indicates the number of	G	15	✓	✓	✓	✓	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
CPS for outgoing SBC calls.											
■ MIB Name: acPMSBCSrdInCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.63 ■ Source Name: PM_gwSBCSRDInCPS											
Indicates the number of CPS for incoming SBC calls per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCSrdOutCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.64 ■ Source Name: PM_gwSBCSRDOutCPS											
Indicates the number of CPS for outgoing SBC calls per SRD.	G	15	✓	✓	✓	✓	×	×	×	×	×
■ MIB Name: acPMSBCIPGroupInCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.61 ■ Source Name: PM_gwSBCIPGroupInCPS											
Indicates the number of CPS for incoming SBC calls	G	15	✓	✓	✓	✓	×	×	×	×	×

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
per IP Group.											
■ MIB Name: acPMSBCIPGroupOutCapsTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.62 ■ Source Name: PM_gwSBCIPGroupOutCPS											
Indicates the number of CPS for outgoing SBC calls per IP Group.	G	15	✓	✓	✓	✓	×	×	×	×	×

SBC Call Attempts per Second

The following table lists the performance monitoring MIBs for SBC call attempts per second.

Table 6-14: Performance Monitoring MIBs for SBC Call Attempts Per Second

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acSBCCallAttemptsPerSecTable ■ OID: 1.3.6.1.4.1.5003.10.8.2.54.73 ■ Source Name: PM_SBCCallAttemptsPerSec											
Indicates the number of SBC call attempts (SIP INVITEs) per second. Each leg is included in the count. For example, if the device receives an INVITE on the incoming leg and then sends it on the outgoing leg, it's considered as two call attempts (if within a	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
second). ■ High threshold: acPMSbcCallAttemptsPerSecHighThreshold (1.3.6.1.4.1.5003.10.8.1.36.56) ■ Low threshold: acPMSbcCallAttemptsPerSecLowThreshold (1.3.6.1.4.1.5003.10.8.1.36.57)											

Performance Monitoring MIBs for High Availability

The following table lists the performance monitoring MIBs for the High Availability (HA) mode.

Table 6-15: Performance Monitoring MIBs for High-Availability

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMHALinkRedundantToActivePacketLossPercentageTable ■ OID: 1.3.6.1.4.1.5003.10.11.2.111.1 ■ Source Name: PM_HALinkRedundantToActivePacketLossPercentage											
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	G	15	✓	✓	✓	✓	✓	✓	✓	✓ (30)	5

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
(1.3.6.1.4.1.5003.10.11.1.38.2)											
■ MIB Name: acPMHALinkActiveToRedundantPacketLossPercentageTable ■ OID: 1.3.6.1.4.1.5003.10.11.2.111.2 ■ Source Name: PM_HALinkActiveToRedundantPacketLossPercentage											
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

Performance Monitoring MIB for DSP Resource Utilization

The following table lists the SNMP MIB that 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.

Table 6-16: Performance Monitoring MIB for DSP Utilization

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
■ MIB Name: acPMDSPUsageTable ■ OID: 1.3.6.1.4.1.5003.10.7.2.25 ■ Source Name: PM_VEDSPUsage											
Indicates the percentage (%)	G	15	✓	✓	✓	✓	✓	✓	✓	✓	✓

Performance Monitoring MIB	G/C	Int	Val	Min	Max	Avg	TbLT	TbT	TaHT	HT	LT
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)										(101)	(101)

7 SNMP Traps

This section describes the SNMP traps supported by the device.

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 OVOC 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)

Proprietary Traps

This section 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 traps have the same structure made up of the same 16 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 the next page.

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. 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 is always 1.

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

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

Trap Varbinds

Trap varbinds are sent with each proprietary SNMP trap. Refer to the AcBoard MIB for more information on these varbinds.

Table 7-1: Trap Varbinds for Proprietary SNMP Traps

Trap Varbind	Description
acBoardTrapGlobalsName (1)	Alarm or event number. The number value is obtained from the last digit(s) of the OID of the sent trap, and then subtracted by 1. For example, for the trap acBoardEthernetLinkAlarm, which has an OID of 1.3.6.1.4.1.5003.9.10.1.21.2.0.10, the value of the varbind is 9 (i.e., 10 – 1). The value is an integer from 0 to 1000.
acBoardTrapGlobalsTextualDescription (2)	Description of the reported issue. The value is an octet string of up to 200 characters.
acBoardTrapGlobalsSource (3)	The source of the issue. For example, Trunk#1 or Entity1#x. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsSeverity (4)	Active alarm severity on the device: ■ noAlarm(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5)
AcBoardTrapGlobalsUniqID (5)	Consecutive number count of trap since device was powered on. The number is managed separately for alarms and events. For example, you may have an alarm whose value is 1 and an event whose value is 1. The value is an integer from 0 to 32000.
acBoardTrapGlobalsType (6)	■ other(0)

Trap Varbind	Description
	■ communicationsAlarm(1) ■ qualityOfServiceAlarm(2) ■ processingErrorAlarm(3) ■ equipmentAlarm(4) ■ environmentalAlarm(5) ■ integrityViolation(6) ■ operationalViolation(7) ■ physicalViolation(8) ■ securityServiceOrMechanismViolation(9) ■ timeDomainViolation(10)
acBoardTrapGlobalsProbableCause (7)	■ other(0) ■ adapterError(1) ■ applicationSubsystemFailure(2) ■ bandwidthReduced(3) ■ callEstablishmentError(4) ■ communicationsProtocolError(5) ■ communicationsSubsystemFailure(6) ■ configurationOrCustomizationError(7) ■ congestion(8) ■ corruptData(9) ■ cpuCyclesLimitExceeded(10) ■ dataSetOrModemError(11) ■ degradedSignal(12) ■ dteDceInterfaceError(13) ■ enclosureDoorOpen(14) ■ equipmentMalfunction(15) ■ excessiveVibration(16) ■ fileError(17) ■ fireDetected(18)

Trap Varbind	Description
	■ floodDetected(19) ■ framingError(20) ■ heatingVentCoolingSystemProblem(21) ■ humidityUnacceptable(22) ■ inputOutputDeviceError(23) ■ inputDeviceError(24) ■ lanError(25) ■ leakDetected(26) ■ localNodeTransmissionError(27) ■ lossOfFrame(28) ■ lossOfSignal(29) ■ materialSupplyExhausted(30) ■ multiplexerProblem(31) ■ outOfMemory(32) ■ ouputDeviceError(33) ■ performanceDegraded(34) ■ powerProblem(35) ■ pressureUnacceptable(36) ■ processorProblem(37) ■ pumpFailure(38) ■ queueSizeExceeded(39) ■ receiveFailure(40) ■ receiverFailure(41) ■ remoteNodeTransmissionError(42) ■ resourceAtOrNearingCapacity(43) ■ responseTimeExecessive(44) ■ retransmissionRateExcessive(45) ■ softwareError(46) ■ softwareProgramAbnormallyTerminated (47)

Trap Varbind	Description
	■ softwareProgramError(48) ■ storageCapacityProblem(49) ■ temperatureUnacceptable(50) ■ thresholdCrossed(51) ■ timingProblem(52) ■ toxicLeakDetected(53) ■ transmitFailure(54) ■ transmitterFailure(55) ■ underlyingResourceUnavailable(56) ■ versionMismatch(57) ■ authenticationFailure(58) ■ breachOfConfidentiality(59) ■ cableTamper(60) ■ delayedInformation(61) ■ denialOfService(62) ■ duplicateInformation(63) ■ informationMissing(64) ■ informationModificationDetected(65) ■ informationOutOfSequence(66) ■ intrusionDetection(67) ■ keyExpired(68) ■ nonRepudiationFailure(69) ■ outOfHoursActivity(70) ■ outOfService(71) ■ proceduralError(72) ■ unauthorizedAccessAttempt(73) ■ unexpectedInformation(74)
acBoardTrapGlobalsAdditionalInfo1 (8)	Provides additional information regarding the reported trap. The value is an octet string of up to 100

Trap Varbind	Description
	characters.
acBoardTrapGlobalsAdditionalInfo2 (9)	Provides additional information regarding the reported trap. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsAdditionalInfo3 (10)	Provides additional information regarding the reported trap. The value is an octet string of up to 100 characters.
acBoardTrapGlobalsDateAndTime (11)	Date and time the trap was sent.
acBoardTrapGlobalsSystemSeverity (12)	The highest alarm severity sent by the device when the trap was sent: ■ cleared(0) ■ indeterminate(1) ■ warning(2) ■ minor(3) ■ major(4) ■ critical(5)
acBoardTrapGlobalsDeviceName (13)	Name of the device. The value is an octet string of up to 100 characters. **Note:** The device sends an empty string "\0". AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsDeviceInfo (14)	Device information. The value is an octet string of up to 100 characters. **Note:** The device sends an empty string "\0". AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsDeviceDescription (15)	Device description. The value is an octet string of up to 100 characters.

Trap Varbind	Description
	Note: The device sends an empty string "\0". AudioCodes OVOC provides the proper string value when it sends it northbound.
acBoardTrapGlobalsSystemSerialNumber (16)	The Serial Number of the device that sent the trap. The value is an octet string of up to 255 characters.

Customizing Trap's Enterprise OID

You can change the enterprise value in the device's SNMP Traps to a variable value, using the ini file 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.

SNMP Alarms in Syslog

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

- **Sent 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, the following are also added: Additional Info1:/ Additional Info2:/ Additional Info3

  The message severity is as follows:

Table 7-2: 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:

SNMP 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'.

- You can customize the severity level of SNMP trap alarms using the Alarms Customization table [AlarmSeverity]. This table also lets you suppress alarms.
- Currently, the acInstallationFailureAlarm trap alarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2) is not supported.

Chassis Alarms

This section describes alarms related to the device's chassis.

Fan Tray Alarm

Table 7-3: acFanTrayAlarm

Alarm	acFanTrayAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.29
Description	The alarm is sent when a fault occurs in the fan tray or a fan tray is missing. For Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080: Not only is the alarm sent when the entire Fan Tray module is faulty or missing, but also per fan (faulty or missing). For example, if a failure occurs in fan 3, the alarm is sent ("Fan-Tray Alarm. Fan 3 is faulty"). If a failure then occurs in fan 4 as well, the first alarm is cleared and a new alarm is sent indicating failures in fans 3 and 4 ("Fan-Tray Alarm. Fans 3,4 are faulty"). If fans 3 and 4 return to normal operation, the alarm is cleared.
Source Varbind Text	Chassis#0/FanTray#0
Alarm Text	Fan-Tray Alarm Text
Event Type	equipmentAlarm

<table>
<tr><th>Alarm</th><th colspan="3">acFanTrayAlarm</th></tr>
<tr><td>Probable Cause</td><td colspan="3">■ 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)</td></tr>
<tr><td>Severity</td><td>Condition</td><td>Text</td><td>Corrective Action</td></tr>
<tr><td>Critical</td><td>No Fan Tray module installed in chassis.</td><td>"Fan-Tray is missing"</td><td>a. Check if the Fan Tray module is inserted in the chassis.
b. If the Fan Tray module was removed from the chassis, re-insert it.
c. 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.</td></tr>
<tr><td>Major</td><td>When one or more fans in the Fan Tray module are faulty.</td><td>"Fan-Tray Alarm. Fan <#,#> <is or are> faulty"</td><td>Fan Tray module is faulty. Send a Return Merchandise Authorization (RMA) request to AudioCodes.</td></tr>
<tr><td>Cleared</td><td>Fan Tray module is in place and all fans are working.</td><td>-</td><td>-</td></tr>
</table>

Power Supply Alarm

Table 7-4: acPowerSupplyAlarm

Alarm	acPowerSupplyAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.30		
Description	The alarm is sent when a fault occurs in one of the Power Supply modules or a Power Supply module is not installed in the chassis or not installed properly. **Note:** ■ The alarm is applicable only when the device is installed with dual Power Supply modules and one of them is functioning. ■ To enable the sending of this trap, configure the ini file parameter [DualPowerSupplySupported] 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		
Severity	Condition	Text	Corrective Action
Major	Unable to detect Power Supply module (faulty or missing)	"Power-Supply Alarm. Power-Supply is missing."	1. Check if the Power Supply module is fully inserted into the chassis. 2. If a Power Supply module 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	Power Supply module is functioning.	-	-

High-Availability Alarms

This section describes the alarms concerned with the High Availability (HA) system.

HA System Fault Alarm

Table 7-5: acHASystemFaultAlarm

Alarm	acHASystemFaultAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.33		
Description	The alarm is 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		
Severity	Condition	Text	Corrective Action
Critical	HA feature has failed to initialize due to some configuration error.	"SYS_HA: HA Remote address not configured, No HA system."	Need to configure a valid 'HA Remote Address'.
		"SYS_HA: HA Remote address and Maintenance IF address are not on the same subnet, No HA system."	Need to configure a valid Maintenance network interface and 'HA Remote Address'.
		"SYS_HA: HA Remote address and Maintenance IF address should be different, No HA system."	Need to configure a valid Maintenance network interface and 'HA Remote Address'.
	HA feature is active, but the system is	"Switch-Over: Reason = Fatal	HA was lost due to switchover and should

Alarm	acHASystemFaultAlarm		
	not operating in HA mode.	exception error"	return automatically after a few minutes. Corrective action is not required.
		"Switch-Over: Reason = SW WD exception error"	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.
		"Switch-Over: Reason = System error"	HA was lost due to switchover caused by a general system error and should return automatically after a few minutes. Corrective action is not required.
		"Switch-Over: Reason = Eth link error"	HA was lost due to switchover. Reconnect the Ethernet link.
		"Switch-Over: Reason = Network Monitor error. Failed table rows index: <id 1> … up to <id 10>"	HA was lost due to switchover due to the HA Network Monitor feature as the threshold of unreachable rows (in the HA Network Monitor table) was exceeded. The indices of these unreachable rows are provided in the alarm's text. The HA mode should return automatically after a few minutes. No corrective action is required.
		"Switch-Over: Reason = Keep Alive error"	HA was lost due to switchover and should return automatically after a few minutes.

Alarm	acHASystemFaultAlarm		
			Corrective action is not required.
		"Switch-Over: Reason = DSP error"	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required. Note: Applicable only to Mediant 4000.
		"Switch-Over: Reason = Software upgrade"	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.
		"Switch-Over: Reason = Software upgrade - switch back"	HA was lost due to switchover (Hitless Software Upgrade process switched from the active to redundant device) and should soon return automatically. Corrective action is not required.
		"Switch-Over: Reason = Fk upgrade"	HA was lost due to switchover caused by a Hitless License Upgrade process and should return automatically after a few minutes. Corrective action is not required.
		“Switch-Over: Reason = Manual switch over"	HA was lost due to switchover and should return automatically after a few minutes. Corrective action is not required.

Alarm	acHASystemFaultAlarm		
Major	HA feature is active, but the system is not operating in HA mode.	"Switch-Over: Reason = Higher HA priority"	HA was lost due to switchover to unit with higher HA priority and should return automatically after a few minutes. Corrective action is not required.
		"SYS_HA: Invalid Network configuration, fix it and reboot Redundant unit - no HA system!"	HA synchronization process has failed. Correct invalid network configuration and then restart the Redundant device in order to trigger HA synchronization again.
		“SYS_HA: Offline configuration was changed, HA is not available until next system reboot.”	HA synchronization process has failed. Changing configuration that requires a device reset to apply the new configuration must be done before the standalone system can become HA again.
		“SYS_HA: Redundant is not reconnecting after deliberate restart, No HA system.”	HA synchronization process has failed. Manually reboot the Redundant device.
Minor	HA Network Monitor feature will not be the cause of a switchover as the 'Preempt Mode' parameter is configured to Enable and the 'Preempt Priority' is configured to a level.	"Network Monitor switch-over is blocked when HA Preemptive mode and Priority is configured"	-

Alarm	acHASystemFaultAlarm		
	The HA Network Monitor feature will not be the cause of a switchover as the number of Ethernet Groups (Ethernet links) in the redundant device in "up" status are less than on the active device.	"Network Monitor switch-over is blocked when status of Ethernet links on redundant is worse than on active unit"	-
	The Ethernet Group that is associated with the Maintenance IP interface, used for HA systems, is configured with two ports and one of them goes down (i.e., no 1+1 Ethernet port redundancy)	"SYS_HA: Maintenance redundant link is down - no HA maintenance link redundancy"	■ Make sure that the network cable is firmly plugged into the Ethernet port. ■ Make sure that the other end of the network cable is correctly connected to the network.
Cleared	HA system is active.	-	-

HA System Configuration Mismatch Alarm

Table 7-6: acHASystemConfigMismatchAlarm

Alarm	acHASystemConfigMismatchAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.34
Description	The alarm is sent when the configuration of the modules in the High Availability (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

Alarm	acHASystemConfigMismatchAlarm		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError		
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"	-

HA System Switch Over Alarm

Table 7-7: acHASystemSwitchOverAlarm

Alarm	acHASystemSwitchOverAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.35
Description	The alarm is sent when a switchover occurs from active to redundant device in a High Availability (HA) system.
Default Severity	Critical
Source Varbind Text	System#0/Module#<m>, where m is the blade module's slot

Alarm	acHASystemSwitchOverAlarm		
	number		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Severity	Condition	Text	Corrective Action
Critical	A switchover from the active to the redundant unit has occurred	(See acHASystemFaultAlarm)	See HA System Configuration Mismatch Alarm on page 102 for details.
	A switchover occurred due to the HA Network Monitor feature as the threshold of unreachable rows (in the HA Network Monitor table) was exceeded. The indices of these unreachable rows are provided in the alarm's text.	"Reason = Network Monitor error. Failed table rows index: <id 1> … up to <id 10>"	
Cleared	10 seconds have passed since the switchover	-	-

HA Network Monitor Alarm

Table 7-8: acHANetworkMonitorAlarm

Alarm	acHANetworkMonitorAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.136
Description	The alarm is sent when all previously reachable destinations configured for a specific row in the HA Network Monitor table (for the HA Network Monitor feature) are now unreachable (i.e., none of them reply to the

Alarm	acHANetworkMonitorAlarm		
	device's pings). For configuring the HA Network Monitor feature, refer to the *User's Manual*.		
Default Severity	Major		
Source Varbind Text	Board#1/NetworkMonitor#X		
Event Type	communicationsAlarm		
Probable Cause	connectionEstablishmentError		
Severity	Condition	Text	Corrective Action
Major	All destinations of a specific row in the HA Network Monitor table that replied in the past to the device's pings are now "unreachable"	"Destination/s <peer destination IP address(es)> is/are unreachable"	-
Cleared	At least one of the "unreachable" destinations replies to the device's pings and is now "reachable", or the row in the HA Network Monitor table has been deleted	-	-

HA Ethernet Group Alarm

Table 7-9: acHAEthernetGroupAlarm

Alarm	acHAEthernetGroupAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.137
Description	The alarm is sent when the Ethernet link of at least one port in the Ethernet Group that is associated with the HA Maintenance interface is down.
Default Severity	Minor

Alarm	acHAEthernetGroupAlarm		
Source Varbind Text	system#0		
Event Type	qualityOfServiceAlarm		
Probable Cause	outOfService		
Severity	Condition	Text	Corrective Action
Minor	At least one of the Ethernet port links in the Ethernet Group associated with the HA Maintenance interface is down	"SYS_HA: Maintenance Group - One of the links is down - NO HA of maintenance link redundancy"	Check that the Ethernet cables are connected securely to the ports. Check that the ports at the other end are up (working).
Cleared	All Ethernet ports in the Ethernet Group associated with the HA Maintenance interface become up again	-	-

Board Alarms

The source varbind text for all alarms under this component is System#0<n>, where *n* is the slot number in which the blade resides in the chassis.

Fatal Error Alarm

Table 7-10: acBoardFatalError

Alarm	acBoardFatalError
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Description	The alarm is sent whenever a fatal device error occurs.
Default Severity	Critical
Event Type	equipmentAlarm
Probable Cause	underlyingResourceUnavailable (56)

Alarm	acBoardFatalError		
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, 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	-	

Configuration Error Alarm

Table 7-11: acBoardConfigurationError

Alarm	acBoardConfigurationError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.2		
Description	The alarm is sent when the device's settings are invalid. The trap contains a message stating, detailing, and explaining the invalid setting.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable (56)		
Severity	Condition	Text	Corrective Action
Critical	A configuration error was detected	"Board Config Error: A run-time specific string describing the configuration error"	a. Check the run-time specific string to determine the nature of the configuration error. b. Fix the configuration error using the appropriate tool: Web interface, OVOC, or ini file.

Alarm	acBoardConfigurationError		
			c. Save the configuration and if necessary reset the device. **Note:** The alarm remains in Critical severity until a device reboot. A Clear trap is not sent.
	After configuration error	-	

Temperature Alarm

Table 7-12: acBoardTemperatureAlarm

Alarm	acBoardTemperatureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.3
Description	The alarm is sent when the device exceeds its temperature limits (threshold). For Mediant 9000: The alarm is sent when the temperature of the CPU exceeds a specific threshold, configured by the ini file parameter [HighTemperatureThreshold]. The default is 70°C (158°F). For Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080: The alarm is sent when the temperature at a specific sensor exceeds a specific threshold, configured by the ini file parameter [HighTemperatureThreshold]. For example, if the temperature threshold is exceeded at sensor 1, the alarm is sent ("Board Temperature Alarm: Sensor #1 is 88 degrees Celsius. Exceeded threshold of 70"). If the temperature threshold at sensor 2 is then exceeded as well, the first alarm is cleared and a new alarm is sent indicating exceeded temperature at both sensors ("Board Temperature Alarm: Sensors #1,#2 are 88,90 degrees Celsius. Exceeded threshold of 70").
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	acBoardTemperatureAlarm		
Alarm Severity	Condition	Text	Corrective Action
Critical	Internal temperature is too high for normal operation. Mediant 9000: Temperature threshold of CPU has been exceeded. Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080: Temperature threshold at specific sensor (s) has been exceeded.	"Board temperature too high" Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080: "Board Temperature Alarm: Sensors <#,#> <is or are> <temperature,temperature> degrees Celsius. Exceeded threshold of <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. 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.
Cleared	Temperature	-	-

Alarm	acBoardTemperatureAlarm		
	returns to normal operating values (at all sensors for Mediant 9000 Rev. B, Mediant 9030 and Mediant 9080).		

Software Reset Alarm

Table 7-13: acBoardEvResettingBoard

Alarm	acBoardEvResettingBoard		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.5		
Description	The alarm is sent after the device resets.		
Default Severity	Critical		
Event Type	equipmentAlarm		
Probable Cause	outOfService (71)		
Severity	Condition	Text	Corrective Action
Critical	When the device is reset through the Web interface or SNMP	"Device is resetting"	A network administrator has reset the device. Corrective action is not required. The alarm remains at Critical severity level until the device completes the reboot. A Clear trap is not sent.

Software Upgrade Alarm

Table 7-14: acSWUpgradeAlarm

Alarm	acSWUpgradeAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.70		
Description	The alarm is sent when an error occurs during the software upgrade process.		
Default Severity	Major		
Alarms Source	System#0		
Event Type	processingErrorAlarm		
Probable Cause	softwareProgramError		
Severity	Condition	Text	Corrective Action
Major	Software upgrade errors	"SW upgrade error: Firmware burning failed. Startup system from BootP/TFTP."	Start up the system from BootP/TFTP.

Call Resources Alarm

Table 7-15: acBoardCallResourcesAlarm

Alarm	acBoardCallResourcesAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.8
Description	The alarm is sent when no free channels are available. **Note:** To enable this alarm, the Remote Alarm Indication (RAI) mechanism must be activated, by configuring the [EnableRAI] parameter to [1].
Default Severity	Major
Event Type	processingErrorAlarm
Probable Cause	softwareError (46)

Alarm	acBoardCallResourcesAlarm		
Severity	Condition	Text	Corrective Action
Major	Percentage of busy channels exceeds the predefined RAI high threshold	"Call resources alarm"	Do one of the following: ■ Expand system capacity by adding more channels (trunks) ■ Reduce traffic
Cleared	Percentage of busy channels falls below the predefined RAI low threshold	-	

All SIP Proxies Connection Lost per Proxy Set Alarm

Table 7-16: acProxyConnectionLost

Alarm	acProxyConnectionLost		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.94		
Description	The alarm is sent when all or some proxy servers in a Proxy Set are offline.		
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.		
Severity	Condition	Text	Corrective Action
Major	Connection to all the proxy servers in the Proxy Set are lost (offline) and the 'Proxy Load Balancing Method' parameter is disabled.	"Proxy Set <ID>: Proxy lost. looking for another proxy"	1. Ping the proxy server. If there is no ping, contact your proxy provider. The prob-

Alarm	acProxyConnectionLost		
			able 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 and send a syslog and network capture for this issue.
	The number of online proxy servers in the Proxy Set is less than the number configured for the 'Min. Active Servers for Load Balancing' parameter and the 'Proxy Load Balancing Method' parameter is enabled (Round Robin or Random Weights).	"Proxy Set <ID>: Proxy lost. looking for another proxy"	
Major	Connection to the Proxy Set is lost and this Proxy Set is configured with fallback to routing table (IsFallbackUsed	"Proxy Set <ID>: Proxy not found. Use internal routing"	1. Ping the proxy server. If there is no ping, contact your proxy provider. The prob-

Alarm	acProxyConnectionLost		
	parameter). **Note:** Applicable only to the Gateway application.		able 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 routing table is functioning correctly. 5. Contact AudioCodes support and send a syslog and network capture for this issue.
Minor	All proxy servers were online and now at least one proxy server in the Proxy Set is offline (and at least one proxy server is still online)	"Proxy Set <ID> ("<Name>"): Server <IP address>:<port> is down - one or more servers in the proxy set are offline"	

Alarm	acProxyConnectionLost		
	All proxy servers were offline and now at least one proxy server in the Proxy Set is online (and at least one proxy server is still offline)	"Proxy Set <ID> ("<Name>"): Server <IP address>:<port> is up, one or more servers in the proxy set are still offline"	
Cleared	All proxy servers in the Proxy Set are online	"Proxy found. ip:<IP address>:<port #> Proxy Set ID <ID>"	-

Board Overload Alarm

Table 7-17: acBoardOverloadAlarm

Alarm	acBoardOverloadAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.11		
Description	The alarm is sent when there is an overload in one or some of the system's components. An overload occurs when a specific percentage of CPU resources is available. You can configure the percentage of available resources to trigger the raising of this alarm, by using the CLI command `configure voip > sip-definition settings > overload-sensitivity-level`.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	softwareError (46)		
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	a. Make sure that the syslog level is 0 (or not high). b. Make sure that DebugRecording is

Alarm	acBoardOverloadAlarm		
		available CPU resources remaining.	not running. c. If the system is configured correctly, reduce traffic.
Cleared	The overload condition passed	"System CPU overload condition - IdleUtilization percentage=%"	-

Administration Status Change Alarm

Table 7-18: acgwAdminStateChange

Alarm	acgwAdminStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.7		
Description	The alarm is sent when Graceful Shutdown commences and ends.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
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 occurred.

Alarm	acgwAdminStateChange		
Cleared	Admin state changed to unlocked	-	■ No corrective action is required. ■ A network administrator has taken an action to unlock the device.

Operational Status Change Alarm

Table 7-19: acOperationalStateChange

Alarm	acOperationalStateChange		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.15		
Description	The alarm is sent if the operational state of the node changes to disabled. It is cleared when the operational state of the node changes to enabled.		
Default Severity	Major		
Event Type	processingErrorAlarm		
Probable Cause	outOfService (71)		
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 changes 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.

Alarm	acOperationalStateChange		
Cleared	Operational state changed to enabled	-	-

CDR Server Alarm

Table 7-20: acCDRServerAlarm

Alarm	acCDRServerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.142		
Description	The alarm is sent when the device fails to send a locally stored CDR file to all the remote CDR (SFTP) servers, which is configured in the SBC CDR Remote Servers table.		
Default Severity	Major		
Source Varbind Text	Board#1		
Event Type	equipmentAlarm		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Major	Device failed to send the CDR local storage file to all the configured CDR servers.	"Device failed to send CDR local storage files to all configured SFTP servers"	Check the network connectivity to the remote server.
Cleared	Device successfully sent the CDR file to at least one of the CDR servers.	"Files transfer succeeded to one of the CDR servers"	-

Remote Monitoring Alarm

Table 7-21: acRemoteMonitoringAlarm

Alarm	acRemoteMonitoringAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.145		
Description	The alarm is sent when the device loses connection with the remote monitoring server (configured on the device as a Remote Web Service) for remote monitoring of the device when it is located behind a NAT.		
Default Severity	Warning		
Source Varbind Text	Board#1		
Event Type	communicationsAlarm		
Probable Cause	callEstablishmentError		
Alarm Severity	Condition	Text	Corrective Action
Warning	The device receives an HTTP failure response (4xx/5xx/6xx) when it sends the monitoring report.	"No connection with Remote Monitoring server"	Check that the configuration of the Remote Web Service is correct.
Cleared	The device receives an HTTP successful response (2xx) when it sends the monitoring report.	-	-

TLS Certificate Expiry Alarm

Table 7-22: acCertificateExpiryAlarm

Alarm	acCertificateExpiryAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.128
Description	The alarm is sent to indicate that the installed TLS certificate belonging to a configured TLS Context is about to expire (which cannot be renewed automatically) or has expired.

Alarm	acCertificateExpiryAlarm		
Default Severity	Minor		
Source Varbind Text	Board#1/CertificateExpiry#X		
Event Type	communicationsAlarm		
Probable Cause	communicationsSubsystemFailure		
Severity	Condition	Text	Corrective Action
Minor	The certificate is about to expire. This is sent a user-defined number of days (TLSExpiryCheckStart) before the expiration date.	"The certificate of TLS context %d will expire in %d days"	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.
Major	The certificate is about to expire. This is sent a week as well as a day before the expiration date.	"The certificate of TLS context %d will expire in less than a week" Or "The TLS certificate of TLS context %d will expire in a day" Or "The TLS certificate of TLS context %d will expire in less than a day"	
Critical	The certificate has expired.	"The certificate of TLS context	Load a new certificate to the device before the expiration of the installed

Alarm	acCertificateExpiryAlarm		
		%d has expired %d days ago"	certificate (which cannot be renewed automatically). To replace certificates, refer to the User's Manual.
Cleared	A new certificate is installed.	-	

License Key Alarms

This section describes the alarms concerned with the device's License Key.

Feature Key Error Alarm

The alarm is applicable only to the local License Key.

Table 7-23: acFeatureKeyError

Alarm	acFeatureKeyError		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.6		
Description	The alarm is sent when an error occurs in the local License Key.		
Default Severity	Critical		
Source Varbind Text			
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomizationError (7)		
Alarm Severity	Condition	Text	Corrective Action
Critical	License Key error.	"Feature key error"	-

License Key Hitless Upgrade Alarm

The alarm is applicable only to the local License Key.

Table 7-24: acLicenseKeyHitlessUpgradeAlarm

Alarm	acLicenseKeyHitlessUpgradeAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.129		
Description	The alarm is sent when installing a local License Key using the Hitless Upgrade method when the device operates in High-Availability (HA) mode, and installation fails due to a failure in the HA switchover process.		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	Condition	Text	Corrective Action
Major	License Key Hitless Upgrade failed due to failure in HA switchover process.	"Feature key hitless upgrade failed due to failure of switchover process"	Reload the License Key, and then perform the Hitless Upgrade process.

License Pool Application Alarm

The alarm is applicable only to the Fixed License.

Table 7-25: acLicensePoolApplicationAlarm

Alarm	acLicensePoolApplicationAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.107
Description	The alarm is sent when the device receives new SBC licenses from the OVOC License Pool and any of the following conditions exist: ■ The device needs to reset or perform a Hitless Upgrade to apply the license. ■ The device is currently undergoing a local License Key upgrade.
Default Severity	Major
Source Varbind	system0Mo

Alarm	acLicensePoolApplicationAlarm		
Text			
Event Type	communicationsAlarm		
Probable Cause	New License pool		
Alarm Severity	Condition	Text	Corrective Action
Major	The device has received a new SBC License from the OVOC License Pool, but requires a reset for it to be applied.	"License Pool Alarm. New license pool allocations received"	Perform one of the following actions in the OVOC License Pool to apply the new license: ■ Standalone: Reset the device. ■ HA: Apply a Hitless Upgrade or reset the device.
	The device is configured to be managed by the OVOC License Pool, but it is not listed in the License Pool.	"License pool synchronization failed, Device is not listed in the License Server"	Check if the device is expected to be listed in the OVOC License Pool. If yes, then add it to the OVOC License Pool. If not, then remove the device from the License Pool.
	The device is configured to be managed by the OVOC License Pool and is listed in the License Pool, but not managed by it.	"License pool synchronization failed, Device is not managed by License Server "	Check if the device is expected to be managed by the OVOC License Pool. If yes, then add it to the License Pool. If not, then remove

Alarm	acLicensePoolApplicationAlarm		
			the device from the License Pool.
	The device failed to configure the parameters of the OVOC License Pool.	"Device License pool server configuration failed "	Re-send the License Pool from the OVOC License Pool to the device.
Minor	■ Standalone: The device receives a new SBC License from the License Pool Manager, but the device is undergoing a local License Key upgrade. ■ HA: The device receives a new SBC License from the License Pool Manager, but the devices are currently undergoing a local License Key upgrade.	■ Standalone: "Local License Key was loaded. License Pool requests are ignored until License Key is installed." ■ HA: "Local License Key was loaded. License Pool requests are ignored until License Key is installed.”	Do one of the following in the License Pool Manager to install the local License Key: ■ Standalone: Reset the device. ■ HA: Apply a Hitless Upgrade to the local License Key or reset the device.

License Pool Over-Allocation Alarm

The alarm is applicable only to the Fixed License.

Table 7-26: acLicensePoolOverAllocationAlarm

Alarm	acLicensePoolOverAllocationAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.125		
Description	The alarm is sent when the SBC license received from the OVOC License Pool has exceeded the maximum capacity supported by the device.		
Alarm Source	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	Overallocation		
Severity	Condition	Text	Corrective Action
Warning	The SBC license received from the License Pool has exceeded the maximum capacity supported by the device. (Sent after the configuration has been applied in the License Pool; but prior to a device reset or hitless upgrade.)	"License Pool Alarm. Some of the license pool allocations exceed maximum capability and will not be applied"	In the OVOC License Pool, do one of the following: ■ Apply the new license (reset device or apply hitless upgrade); the device sets its SBC capacity to maximum and disregards the excess configured sessions. ■ Reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).
Warning	The SBC license received from the License Pool has exceeded the maximum capacity supported by the device. (Sent after a device restart.)	"License Pool Alarm. Some of the license pool allocations will not be used because of over-allocation"	In the OVOC License Pool, reconfigure the license sessions with values that fall within the device capacity and then apply the new license (reset device or apply hitless upgrade).

License Pool Infrastructure Alarm

The alarm is applicable only to the Fixed License.

Table 7-27: acLicensePoolInfraAlarm

Alarm	acLicensePoolInfraAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.106		
Description	The alarm is sent if one of the following occurs: ■ The device is unable to communicate with the OVOC License Pool. ■ The device license has expired. ■ The device is no longer managed by the OVOC License Pool.		
Default Severity	Major		
Source Varbind Text	system0Mo		
Event Type	communicationsAlarm		
Probable Cause	keyExpired		
Alarm Severity	Condition	Text	Corrective Action
Critical	Device unable to establish an HTTPS REST connection with OVOC after successive attempts.	"License Pool Alarm. License pool validity is about to expire."	In OVOC, perform the 'MG Update' action to re-establish a REST connection with device and to send the latest license.
	The device's license has expired.	"License Pool Alarm. The device license has expired! Use of this device is strictly prohibited."	
Major	The last attempt to establish an HTTPS REST connection with OVOC was not successful.	"License Pool Alarm. Device was unable to access the License Server."	■ Wait for the next connection attempt. ■ In OVOC,

Alarm	acLicensePoolInfraAlarm		
			perform the 'MG Update' action to re-establish a REST connection with device and to send the current license.
	The device has been configured as Non-Managed in the OVOC License Pool. If there are active licensed sessions for this device, the device automatically performs a reset or hitless upgrade.	"License Pool Alarm. Device is no longer managed by the SBC License Pool."	If you wish, reconfigure the device to be managed by the OVOC License Pool.
Clear	The alarm is cleared when: ■ Connection has been re-established with the OVOC License Pool. An updated license has been loaded to the device and an apply-reset has been performed. ■ The device has been reconfigured to be managed by the OVOC License Pool. A new license has been loaded to the device, and an apply-reset has been performed.	-	-

Flex License Manager Alarm

The alarm is applicable only to the Flex License.

Table 7-28: acFlexLicenseManagerAlarm

Alarm	acFlexLicenseManagerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.144		
Description	The alarm is sent when a change in status occurs in one or more SBC capacity license types that are managed by OVOC Flex License. The status change can be from "ok" to "overlicense" or vice versa. The SBC capacity license types include Signaling Sessions, FEU (Far End Users), Transcoding Sessions, and Media Sessions.		
Default Severity	Warning		
Source Varbind Text	Board#1		
Event Type	processingErrorAlarm		
Probable Cause	communicationsProtocolError		
Alarm Severity	Condition	Text	Corrective Action
Warning	OVOC Flex License pool stops the device's service of an SBC capacity license type(s) due to pool's license capacity reached or exceeded (utilization status changed to "overlicense").	"Service for <service name> license parameter is stopped" Where <service type> can be Signaling sessions, FEU (Far End Users), Transcoding sessions, and Media sessions	-
Cleared	OVOC Flex License pool allows the device's service of an SBC capacity license type(s) when sufficient licenses are restored to the pool (utilization status changed to "ok").	-	-

Cloud License Manager Alarm

The alarm is applicable to the Floating License and Flex License.

Table 7-29: acCloudLicenseManagerAlarm

Alarm	acCloudLicenseManagerAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.132		
Description	The alarm is sent in any of the following scenarios: ■ Disconnection between the device and OVOC. ■ Device fails to send usage reports to OVOC. ■ The Fixed License Pool is enabled and an attempt was made to enable the Floating License or Flex License.		
Source Varbind Text	Board#1		
Event Type	processingErrorAlarm		
Probable Cause	configurationOrCustomisationError		
Severity	Condition	Text	Corrective Action
Major	There is no connection between the device and OVOC either prior to initial handshake or due to long disconnection time (default is 3 months, but it can be overridden by OVOC)	"No connection with OVOC"	■ Check TCP/TLS connectivity. ■ Check that device is registered with OVOC.
	The device did not send usage reports to OVOC for a specified number of days.	"Failed to send usage report to OVOC for X days."	Check TCP/TLS connectivity.
	The Fixed License Pool is enabled and an attempt was made to enable the Floating License or Flex License.	"Floating license cannot be enabled when device is managed by License Pool."	Disable the Floating License or Flex License on the device. Remove the device from the Fixed License Pool in OVOC.
Critical	The device couldn't connect to OVOC (handshake).	"Connection with OVOC failed, response code	■ <Forbidden 403>: Contact AudioCodes support.

Alarm	acCloudLicenseManagerAlarm		
		<XXX>"	■ <unauthorized 401>: Check username and password. Possible HTTP response codes and reasons: ■ 4xx-6xx responses: The device retries the request using the value in the Retry-After header if specified, or immediately following an update of the OVOC Product Key. ■ OVOC response to Register requests: ■ 200: If successful request ■ 400: Request format is not valid or request data is not valid, or if OVOC is in a state of initial registration required ■ 401: username or password are incorrect ■ 403: Customer is blocked, or OVOC maximum capacity has been reached ■ 404: Request URI contains device ID that is not identified by OVOC ■ 500: Server is not able to handle the request due to

Alarm	acCloudLicenseManagerAlarm		
			server-side error (no resources, internal component failure etc.) ■ Server may response with 4xx or 5xx error as defined in HTTP RFC, when appropriate
	The device couldn't connect to OVOC (handshake).	"Connection with OVOC failed. Failed initialize connection"	Check TCP/TLS connectivity.
	The device couldn't initialize connection with OVOC (handshake).	"Device was rejected by OVOC while trying to fetch device id"	<Forbidden 403>: Contact AudioCodes support.
Cleared	■ Connection with OVOC is established. ■ Reports are sent successfully. ■ Floating License or Flex License is disabled on the device or the device is removed from the Fixed License Pool on OVOC. The alarm is cleared upon the next device reset.	-	-

Floating License Alarm

The alarm is applicable only to the Flex License and Floating License.

Table 7-30: acFloatingLicenseAlarm

Alarm	acFloatingLicenseAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.138		
Description	The alarm is sent when insufficient memory resources (physical memory) exist for the capacity of the user-defined (Custom) Allocation Profile configured for the Floating License on the Floating License page.		
Source Varbind Text	Board#1		
Event Type	processingErrorAlarm		
Additional Info	Detailed explanation of the problematic parameter, requested and actual value. For example: "SignalingSessions – requested 10000, allocated 1000"		
Probable Cause	communicationsProtocolError		
Severity	Condition	Text	Corrective Action
Warning	An attempt was made to configure a customized Allocation Profile with values that exceed the device's capacity support based on physical memory.	"Not enough memory to allocate for 'custom' profile."	Configure an Allocation Profile within the bounds of the device's capacity support.

Network Alarms

This section describes alarms concerned with the network.

NTP Server Status Alarm

Table 7-31: acNTPServerStatusAlarm

Alarm	acNTPServerStatusAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.71
Description	The alarm is sent when the connection to the NTP server is lost. Cleared when the connection is reestablished. Unset time (because 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

Alarm	acNTPServerStatusAlarm		
	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		
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.	-	-

Ethernet Link Alarm

Table 7-32: acBoardEthernetLinkAlarm

Alarm	acBoardEthernetLinkAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Description	The alarm is sent when an Ethernet link(s) is down. The alarm is sent regardless of the number of ports configured in an Ethernet Group; as soon as an Ethernet port (link) goes down, the alarm is sent.
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	acBoardEthernetLinkAlarm		
Severity	Condition	Text	Corrective Action
Minor	Ethernet Group with two Ethernet ports and only one is down.	"Ethernet link alarm. LAN port number <n> link is down" (where *n* is the port number)	1. Ensure that the Ethernet cables are plugged into the chassis. 2. Check the device's Ethernet link LEDs to determine which interface is failing. 3. Reconnect the cable or fix the network problem
Minor	Ethernet Group with two Ethernet ports and both are down, or Ethernet Group with a single port and the port is down.	"No Ethernet link"	
Cleared	Ethernet Group with two Ethernet ports and both are up, or Ethernet Group with a single port and the port is up again.	-	**Note:** For High-Availability (HA) systems, the alarm's behavior is different when sent from the redundant or active device. The alarm from the redundant is sent 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

Alarm	acBoardEthernetLinkAlarm		
			conveyed in the no HA alarm that follows such a case.

Ethernet Group Alarm

Table 7-33: acEthernetGroupAlarm

Alarm	acEthernetGroupAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.86		
Description	The alarm is sent when an Ethernet port in an Ethernet Group goes down. **Note:** If an Ethernet Group is configured with two ports and only one port goes down, the alarm is not sent.		
Default Severity	Major		
Event Type	equipmentAlarm		
Probable Cause	underlyingResourceUnavailable		
Alarm Text	Ethernet Group alarm. %s		
Severity	Condition	Text	Corrective Action
Major	Ethernet Group is configured with only one port and the port is down.	"Ethernet Group alarm. Ethernet Group <ID> is Down"	-
Major	Ethernet Group is configured with two ports and both ports are down.	"Ethernet Group alarm. Ethernet Group (ID> is Down"	-
Cleared	Ethernet Group configured with only one port: alarm cleared when the port comes up again. Ethernet Group configured with two ports: alarm is	-	-

Alarm	acEthernetGroupAlarm		
	cleared when at least one port comes up again.		

LDAP Lost Connection Alarm

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 sent.
Alarm Text	LDAP Lost Connection
Status Changes	The alarm is sent when there is no connection to the LDAP server

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	Try any of the following: ■ Repair the Online Certificate Status Protocol (OCSP) server ■ Correct the network configuration

IPv6 Error Alarm

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		
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. **Note:** The alarm remains in Critical severity until the device reboots (a Clear trap is not sent).

HTTP Proxy NGINX Alarms

This section describes the alarms related to HTTP Proxy Services (NGINX).

NGINX Configuration is Invalid

Table 7-37: acNGINXConfigurationIsInvalidAlarm

Alarm	acNGINXConfigurationIsInvalidAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.130		
Description	The alarm is sent when NGINX Directives Sets have been configured with invalid syntax. NGINX continues to run with the previous, valid configuration unless the device is restarted, in which case, the NGINX process is stopped and the NGINX Process is not Running alarm is sent (see below).		
Alarm Title	NGINX configuration is not valid		
Alarm Source	operationalViolation		
Alarm Type	alarmTrap		
Probable Cause	configurationOrCustomizationError		
Severity	Condition	<text>	Corrective Action
Minor	NGINX Directives Sets have been configured with invalid syntax.	"NGINX Configuration file is not valid."	Identify and resolve NGINX Directives Sets syntax errors to ensure an uninterrupted HTTP Proxy service. You can run CLI commands for troubleshooting: ■ show network http-proxy conf new: to display the Directives Set configuration that generated the errors. ■ show network http-proxy conf errors: to display the errors resulting from the invalid Directives Set configuration.

NGINX Process Not Running

Table 7-38: acNGINXPprocessIsNotRunningAlarm

Alarm	acNGINXPprocessIsNotRunningAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.131		
Description	The alarm is sent when the device is restarted with an erroneous NGINX configuration (i.e., after the alarm "NGINX Configuration is not Valid" is sent (see above).		
Alarm Source	communicationsAlarm		
Alarm Title	NGINX process could not be started		
Alarm Type	alarmTrap		
Probable Cause	applicationSubsystemFailure		
Severity	Condition	<text>	Corrective Action
Major	The device is restarted with an erroneous NGINX configuration.	"NGINX process is not running."	Correct the NGINX Directives syntax (the NGINX process will restart automatically).

HTTP Proxy Service Alarm

Table 7-39: acHTTPProxyServiceAlarm

Alarm	acHTTPProxyServiceAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.108
Description	The alarm is sent when an HTTP host specified in the Upstream Groups table is down. The trap is cleared when the host is back up.
Source Varbind Text	System#0/HTTPProxyService#<num> System#0/EMSService#<num>
Event Type	communicationsAlarm
Probable Cause	■ Network issue (connection fail due to network/routing failure). ■ Host issue (host is down). ■ Device issue.

Alarm	acHTTPProxyServiceAlarm		
Severity	Condition	Text	Corrective Action
Major	When connection to the Upstream Host is lost.	"HTTP Proxy Upstream Host IP:Port (Host #n in Upstream Group name) is OFFLINE"	1. Ping the host. If there is no ping, contact your provider. The probable reason is that 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. Check that routing using the device's (internal) routing table is functioning correctly. 4. 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.	-	-

Active Alarm Table Alarm

Table 7-40: acActiveAlarmTableOverflow

Alarm	acActiveAlarmTableOverflow
OID	1.3.6.1.4.15003.9.10.1.21.2.0.12
Description	The alarm is 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

Alarm	acActiveAlarmTableOverflow		
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.
Remains 'Major' until reboot. A 'Clear' trap is not sent.	After the alarm is sent	-	Note that the status remains 'Major' until reboot as it denotes a possible loss of information until the next reboot. If an alarm is sent when the table is full, it is possible that the alarm is active, but does not appear in the active alarm table.

Media Alarms

Media Realm Bandwidth Threshold Alarm

Table 7-41: 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	The alarm is sent when a bandwidth threshold is crossed		
Severity	Condition	Text	Corrective Action
Major	-	"Media Realm BW Threshold Alarm"	Cleared when bandwidth threshold returns to normal range

Call Quality Alarms

This section describes the alarms concerned with call quality.

Answer-Seizure Ratio Threshold Alarm

Table 7-42: 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 sent 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		
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.	-	-

Average Call Duration Threshold Alarm

Table 7-43: 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 sent 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.		
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.	-	-

Network Effectiveness Ratio Threshold Alarm

Table 7-44: 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 sent 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 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.		
Severity	Condition	Text	Corrective Action
Major	NER is equal or less than the configured Major threshold.	"NER threshold crossed."	
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.		

No Route to IP Group Alarm

Table 7-45: acIpGroupNoRouteAlarm

Alarm	acIpGroupNoRouteAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.114		
Description	The alarm is sent when the device rejects calls to the destination IP Group due to any of the following reasons: ■ Server-type IP Group is not associated with a Proxy Set, or it's associated with a Proxy Set that is not configured with any addresses, or the associated Proxy Set experiences a proxy keep-alive failure (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. The text displayed for this alarm can be one of the following: ■ "No Working Proxy" (acProxyConnectivity trap is sent) ■ "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.		
Severity	Condition	Text	Corrective Action
Major	When calls rejected to IP Group due to any of the above-	"IP Group is temporarily	-

Alarm	acIpGroupNoRouteAlarm		
	mentioned reasons.	blocked. IPGroup(<name>) Blocked Reason: <reason – see Source Varbind Text>"	
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).		-

Intrusion Detection Alarms

This section describes the alarms concerned with the device's Intrusion Detection System (IDS) feature.

IDS Policy Alarm

Table 7-46: acIDSPolicyAlarm

Alarm	acIDSPolicyAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.99
Description	The alarm is sent when a threshold of a specific IDS Policy rule is crossed for the Intrusion Detection System (IDS) feature. The alarm displays the crossed severity threshold (Minor or Major), IDS Policy and IDS Rule, and the IDS Policy-Match index. The alarm is associated with the MO pair IDSMatch and IDSRule.
Default Severity	-
Event Type	Other
Probable Cause	
Alarm Text	"<Severity> (enum severity) cross. Policy: <Name> (<Index>), Rule: <Name>, Last event: <Name>, Source: <IP Address:portprotocol>, SIP Interface: <Name> (<Index>)"

Alarm	acIDSPolicyAlarm		
	For example: "Major threshold (3) cross. Policy: My Policy (3), Rule: Malformed messages, Last event: SIP parser error, Source: 10.33.5.111:62990udp, SIP Interface: SIPInterface_0 (0)."		
Severity	Condition	Text	Corrective Action
Minor or Major (depending on crossed threshold)	Threshold of a specific IDS Policy rule is crossed.	(see Alarm Text above)	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.

Media Cluster Alarms

This section describes the alarms for the Media Cluster feature.

Cluster HA Usage Alarm

The alarm is applicable only to the Media Transcoding Cluster feature (Mediant VE SBC).

Table 7-47: acMtcmClusterHaAlarm

Alarm	acMtcmClusterHaAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.115
Description	The alarm is sent by the Cluster Manager when the cluster HA usage exceeds 100%. HA usage of 100% means that if a failure occurs in a Media Component (MC or vMC), sufficient DSP resources are available on the other Media Components in the cluster to take over the transcoding sessions of the failed Media Component. HA usage exceeding 100%

Alarm	acMtcmClusterHaAlarm		
	means that insufficient DSP resources are available on the other Media Components to take over the transcoding sessions of the failed Media Component.		
Default Severity	Major		
Alarm Source	device/clusterManager		
Event Type	equipmentAlarm		
Probable Cause	Other		
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 Components are properly connected to the Cluster Manager. ■ Make sure all Media Components in the Media Components table show "Unlocked" for the Admin State field and "Connected" for the Status field.
Cleared	HA usage drops to below 95%	-	-

Media Component Network Failure Alarm

The alarm is applicable to the Media Transcoding Cluster feature.

Table 7-48: acMtceNetworkFailureAlarm

Alarm	acMtceNetworkFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.116		
Description	The alarm is sent when the Cluster Manager (Media Transcoding Cluster feature) or Signaling Component (Elastic Media Cluster feature) fails to connect to the Media Component.		
Default Severity	Major		
Alarm Source	Board#1/clusterManager#0/MTCE#xxx		
Event Type	communicationsAlarm		
Probable Cause	Other		
Severity	Condition	Alarm Text	Corrective Action
Major	Connection failure with Media Component	"No Connection with MTCE: <MTCE-name>"	For the Media Transcoding Cluster feature, ensure a physical connection exists between the Media Component and the Cluster Manager.
Cleared	Connection established / re-established with Media Component	-	-

Media Component Software Upgrade Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature.

Table 7-49: acMtceSwUpgradeFailureAlarm

Alarm	acMtceSwUpgradeFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.117
Description	The alarm is sent upon a software upgrade (.cmp) or Auxiliary file load failure in the Media Media Component.

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

Media Component High Temperature Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature.

Table 7-50: acMtceHwTemperatureFailureAlarm

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

Alarm	acMtceHwTemperatureFailureAlarm		
Major	Temperature of Media Component 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 Component is re-established and temperature is reduced	-	-

Media Component Fan Tray Module Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature.

Table 7-51: acMtceHwFanTrayFailureAlarm

Alarm	acMtceHwFanTrayFailureAlarm		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.119		
Description	The alarm is sent upon a failure in the Fan Tray module of the Media Component (MC type).		
Default Severity	Minor		
Alarm Source	..../MTCE#1/fanTray#1		
Event Type	equipmentAlarm		
Probable Cause	heatingVentCoolingSystemProblem		
Severity	Condition	Alarm Text	Corrective Action
Minor	Failure in Fan Tray module of Media Component	"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	-	-

Media Component Power Supply Module Failure Alarm

The alarm is applicable only to the Media Transcoding Cluster feature.

Table 7-52: acMtcePsuFailureAlarm

Alarm	acMtcePsuFailureAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.120
Description	The alarm is sent upon a failure in the Power Supply module of the Media Component (MC type).
Default Severity	Minor
Alarm Source	..../MTCE#1/powerSupply#1
Event Type	equipmentAlarm

Alarm	acMtcePsuFailureAlarm		
Probable Cause	powerProblem		
Severity	Condition	Alarm Text	Corrective Action
Minor	Failure in Power Supply module of Media Component	"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 sent, send a Return Merchandise Authorization (RMA) request to AudioCodes.
Cleared	Power Supply module status returns to normal	-	-

Cluster Bandwidth Utilization Alarm

The alarm is applicable to the Media Transcoding Cluster feature.

Table 7-53: acClusterBandwidthAlarm

Alarm	acClusterBandwidthAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.126
Description	The alarm is sent when the bandwidth utilization of a Cluster interface exceeds the configured maximum bandwidth (refer to the MtcClusterNetworkMaxBandwidth parameter).
Default Severity	Minor
Alarm Source	Board#1/EthernetLink#<ehternet port number>
Event Type	Other
Probable	performanceDegraded

Alarm	acClusterBandwidthAlarm		
Cause	■ Too many sessions processed on the specific Cluster interface. ■ Cluster interface is being used by another application (e.g., OAMP).		
Severity	Condition	Text	Corrective Action
Major	Bandwidth utilization is greater than 90%.	"Cluster Bandwidth is above 90% utilization on Interface name: <name>. No more transcoding sessions will be allocated on that Cluster Interface"	Reduce the number of Media Components on the Cluster interface. Alternatively, the overall permitted bandwidth for the Cluster interfaces should be increased, if possible, using the ini file parameter [MtcClusterNetworkMaxBandwidth].
Minor	Bandwidth utilization is between 85 and 90%. Note: If a Major alarm was sent and the bandwidth later declined to between 80 and 85%, the alarm is changed to Minor.	"Cluster Bandwidth is above 85% utilization on Interface name: <name>"	
Cleared	Bandwidth utilization is less than 80%.	-	-

SNMP Event Traps (Notifications)

This subsection details traps (events) 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 table or Active table. The only log trap that does send 'Clear' is acPerformanceMonitoringThresholdCrossing.

Intrusion Detection System (IDS)

This section describes the trap events concerned with the Intrusion Detection System (IDS) feature.

IDS Threshold Cross Notification Trap

Table 7-54: acIDSThresholdCrossNotification

Event	acIDSThresholdCrossNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.100
Description	The alarm is 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 crossed 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 that the Intrusion Detection System (IDS) has indicated as malicious. 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.

IDS Blacklist Notification Trap

Table 7-55: acIDSBlacklistNotification

Event	acIDSBlacklistNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Description	The trap is sent when the Intrusion Detection System (IDS) feature has blacklisted a malicious host or removed it from the blacklist.
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.

Web User Access Denied due to Inactivity Trap

Table 7-56: acWebUserAccessDisabled

Event	acWebUserAccessDisabled
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.93
Default Severity	Indeterminate
Event Type	
Probable Cause	The alarm is sent when Web user was disabled due to inactivity
Alarm Text	

Event	acWebUserAccessDisabled
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 Local Users table (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Local Users**). 2. Identify in the table those users whose access has been denied. 3. Change the status of that user from Blocked to **Valid** or **New**.

Web User Activity Log Trap

Table 7-57: acActivityLog

Event	acActivityLog
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.105
Description	The alarm is 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.

Keep-Alive Trap

Table 7-58: acKeepAlive

Event	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 device's STUN application 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. If the device is configured for SNMPv3, the trap is sent with acBoardTrapGlobalsAdditionalInfo2: SNMPVersion=SNMPv3. If the device is configured for SNMPv2, the trap is sent with acBoardTrapGlobalsAdditionalInfo2: SNMPVersion= SNMPv2c. If the device is also in High-Availability mode (HA) and the active and redundant devices are synchronized with one another, the trap is sent by the active device with the acBoardTrapGlobalsAdditionalInfo3 varbind, which contains the redundant device's serial number (S/N). **Note:** Keep-alive is sent every 9/10 of the time configured by the [NatBindingDefaultTimeout] parameter.
Default Severity	Indeterminate
Event Type	other (0)
Probable Cause	other (0)
Trap Text	Keep alive trap
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

Performance Monitoring Threshold-Crossing Trap

Table 7-59: acPerformanceMonitoringThresholdCrossing

Event	acPerformanceMonitoringThresholdCrossing
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.27

Event	acPerformanceMonitoringThresholdCrossing
Description	The alarm is 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 Source	<Performance Monitoring name> #<Managed Object ID> For example: PM_gwIPGroupINVITEDialogs#7, refers to SIP INVITE messages of IP Group ID 7.
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

HTTP Download Result Trap

Table 7-60: acHTTPDownloadResult

Event	acHTTPDownloadResult
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.28
Description	The alarm is sent upon success or failure of the HTTP Download action.

Event	acHTTPDownloadResult
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.

High-Availability (HA)

This section describes the SNMP trap events concerned with the High-Availability (HA) system.

Redundant Board Trap

Table 7-61: acRedundantBoardAlarm

Event	acRedundantBoardAlarm
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.97
Description	The notification trap is sent by the active device when an alarm or notification is sent by the redundant device: ■ System (1) ✓ acBoardFatalError ✓ acBoardTemperatureAlarm ■ ethernetLink (4) ✓ acBoardEthernetLinkAlarm ■ chassis (16)

Event	acRedundantBoardAlarm
	■ fanTray (17) ✓ acFanTrayAlarm ■ powerSupply (18) ✓ acPowerSupplyAlarm ■ module (21) ✓ acHwFailureAlarm ■ EthGroup (37) ✓ acEthernetGroupAlarm
Default Severity	Indeterminate
Event Type	Other (0)
Probable Cause	Other (0)
Condition	Alarm or notification is sent in the redundant device
Trap Text	

Hitless Software Upgrade Status Trap

Table 7-62: acHitlessUpdateStatus

Event	acHitlessUpdateStatus	
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.48	
Description	The notification trap is sent at the beginning and end of a Hitless Software Upgrade, which is used in the High Availability system. 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

Event	acHitlessUpdateStatus	
"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.

Secure Shell (SSH) Connection Status Trap

Table 7-63: acSSHConnectionStatus

Event	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

Event	acSSHConnectionStatus
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

SIP Proxy Connection Lost per Proxy Set Trap

Table 7-64: acProxyConnectivity

Event	acProxyConnectivity		
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.103		
Description	The alarm is sent when the device loses connectivity with a specific proxy that is configured for a specific Proxy Set. 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.		
Severity	Condition	Text	Corrective Action
Indeterminate	When connection to	"Proxy Server <IP address>:<port> is	1. Ping the proxy server. If there is no ping, contact

Event	acProxyConnectivity		
	the proxy server is lost.	now OUT OF SERVICE"	your proxy provider. The probable reason is the proxy is down. 2. Ping between the proxy and the device. If there is no ping, the problem could be a network or 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 an issue with the device. 4. Contact AudioCodes support 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"	-

Cold Start Trap

Table 7-65: coldStart

Event	ColdStart
OID	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Description	The alarm is 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.

Authentication Failure Trap

Table 7-66: authenticationFailure

Event	authenticationFailure
OID	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB
Description	The alarm is 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”.

Board Initialization Completed Trap

This is the AudioCodes Enterprise application cold start trap.

Table 7-67: acBoardEvBoardStarted

Event	acBoardEvBoardStarted
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
Description	The alarm is 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

Configuration Change Trap

Table 7-68: entConfigChange

Event	entConfigChange
OID	1.3.6.1.2.1.4.7.2

Event	entConfigChange
MIB	ENTITY-MIB
Description	The alarm is sent if a change in the device's hardware is detected, for example, when a module is removed from the chassis.

Enhanced BIT Status Trap

Table 7-69: acEnhancedBITStatus

Event	acEnhancedBITStatus
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.18
Description	The alarm is 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

This section describes advanced SNMP features.

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] parameter or MIB object acSysSTUNBindingLifeTime.
  - After the STUN client has discovered a NAT (any NAT).
  - If the STUN client cannot contact a STUN server.

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 sent. It is cleared when a non-symmetric NAT or no NAT replaces the symmetric one.

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.
- acSysPowerSupplyTable: A status-only table with the states of the two power supplies.

The above tables are complemented by the following alarm traps (as defined in the acBoard MIB). For more details, see Getting Started with SNMP on page 170.

- acFanTrayAlarm: Fault in the fan tray or fan tray missing (see Fan Tray Alarm on page 95).
- acPowerSupplyAlarm: Fault in one of the power supply modules or power supply module is missing (see Power Supply Alarm on page 97).

High-Availability Systems

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.

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 sent. 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

The acSysActionAdminStateLockTimeout must be set before the acSysActionAdminState.

9 Getting Started with SNMP

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

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 don't want 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 and 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 is 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:

Configuring SNMP Port

To configure the agent's SNMP port:

- ini file:

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

- CLI:

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

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.

  - This option also requires you to configure the DNS server IP address (in the IP Interfaces 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:
    i. 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>

ii. 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:

  i. Remove the appropriate row from the snmpTargetAddrTable.

  ii. 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
```

Configuring Trap Destination Port

For configuring the trap destination port, see Configuring Trap Managers (Trap Destination) on page 170.

Configuring Trusted Managers

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

- The concept of trusted managers is 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.
    i. Add a row to the snmpTargetAddrTable with these values:
    Name=mgr0
    TagList=MGR
    Params=v2cparams.
    ii. 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.
    iii. 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.
    i. 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
    ii. 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.

  i. Set the value of the TransportTag field on each row in the snmpCommunityTable to the empty string.

  ii. 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
```

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**. The different MIB modules are grouped according to different virtual modules of the device. In general, the division is as follows (a more detailed breakdown of the MIBs is discussed below):
  - 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.

- 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.

- **Performance monitoring MIBs – in the acPerformance subtree**. The different MIB modules are grouped according to different virtual modules of the device. In general, the division is as follows (a more detailed breakdown of the MIBs is discussed below):
  - 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.
- **Proprietary Carrier Grade Alarm MIB – in the acFault subtree**:
  - acAlarm: 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.

Traps and Alarms

The device supports standard traps and proprietary traps. Most of the proprietary traps are alarm traps, that is, they can be sent and cleared. Thus, they are referred to as alarm traps. All the standard traps are non-alarm traps, referred to as log traps.

The proprietary traps are defined under the acBoardTrapDefinitions subtree.

The supported standard MIB traps 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.

Device Configuration

For a device to send 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 170)
- 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 ]
```

- 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'.

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 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 OVOC 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 sent and traps that have been cleared to allow an OVOC to recover any lost sent 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.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-52484