

Oracle® Communications Unified Session Manager

MIB Reference Guide
Release S-CZ7.3.5

April 2017

Notices

Copyright© 2017, 2013, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Introduction.....	9
About MIBs.....	9
Object Identifiers and Instance IDs.....	9
MIB Tree Structure.....	10
Managed Objects.....	10
SNMP Traps.....	11
MIBs Supported.....	11
Standard MIBS.....	11
Enterprise MIBs.....	12
Traps.....	13
Standard Traps.....	13
Enterprise Traps.....	14
EMS Traps.....	25
SNMPv3 Secure Traps.....	26
Authentication and Privacy.....	26
Enabling SNMPv3.....	26
Consideration for HA Nodes.....	27
Complete SNMPv3 Configuration.....	27
Persistent indexing of SNMP Tables.....	28
Log Levels and syslog Level Severities.....	29
Log Levels.....	29
syslog Level Severities.....	30
Mapping Trap Filter Levels to syslog and Alarm Severities.....	30
2 Standard SNMP GET Requests.....	33
Interfaces Object.....	33
Interface Table.....	33
ifXTable Table.....	36
ip Object.....	39
ipAddrTable Table.....	40
icmp Object.....	41
TCP Object.....	42
tcpConnTable Table.....	44
UDP Object.....	44
System Object.....	45
Object Resource Information Object.....	46
SNMP Object.....	46
Physical Entity Table.....	47
3 Enterprise SNMP GET Requests.....	53
Applications MIB (ap-apps.mib).....	53
apAppsENUMServerStatusTable Table	53
apAppsDnsServerStatusTable.....	53
Codec and Transcoding MIB (ap-codec.mib).....	54
apCodecPairStatsTable.....	57
Transcoding Capacity in System Management MIB (ap-smgmt.mib).....	58
Diameter MIB (ap-diameter.mib).....	59
DNS ALG MIB (ap-dnsalg.mib).....	60

apDNSALGServerStatusTable.....	60
apDNSALGStatsTable.....	61
Environment Monitor MIB (ap-env-monitor.mib).....	62
H.323 MIB (ap-h323.mib).....	67
License MIB (ap-license.mib).....	68
Security MIB (ap-security.mib).....	69
apSecurityCertificateTable.....	70
SIP MIB (ap-sip.mib).....	70
syslog MIB (ap-slog.mib).....	71
System Management MIB (ap-smgmt.mib).....	73
Notes on ENUM Server Names.....	90
Software Inventory MIB (ap-swinventory.mib).....	91
Multicore Monitoring MIB (ap-usbcsys.mib).....	92
4 SNMP-based Application Features.....	97
SNMP Reporting of Message Rate Statistics.....	97
apSIPRateIntfStatsTable.....	97
apSIPRateAgentStatsTable.....	97
apDnsAlgServerRateStatsTable.....	98
apEnumServerRateStatsTable.....	98
FQDN-resolved Session Agent Statistics SNMP Retrieval.....	98
CAC Utilization Statistics via SNMP.....	98
SNMP Get for CAC Utilization.....	99
CAC Utilization Traps.....	100
External Policy Server Connection Status Reporting.....	101
A— System Alarms.....	103
Alarm Severities.....	116
Glossary.....	117

About this Guide

The Oracle Communications MIB Reference Guide provides information about MIBs, traps, and SNMP GET query information.

This guide also describes the correlation between system alarms and the MIBs that support traps, and it provides reference information about log levels, syslog level severities (the protocol used for the network logging of system and network events), and trap receiver filter levels.

Documented Objects and Traps

This MIB Reference Guide only documents the traps and objects supported in the release version S-CZ7.3.5 for the Acme Packet 4500, Acme Packet 6100, and Acme Packet 6300 platforms. Acme Packet enterprise MIBs, however, can contain additional traps and objects not documented here.

Enterprise MIB files are global across all session border controllers. Each MIB contains a superset of objects and traps for all SBC platforms, current releases, and prior releases.

In addition, a MIB might contain objects and traps intended for future releases. For example, the ap-smgmt.mib might contain traps intended for support in release Release S-CZ7.3.5.

To verify what this release supports:

1. Reviewing the list of supported capabilities in MIB README.txt
2. Reading the capability descriptions in the ap-agentcapability.mib to identify which object and/or notification groups they contain and in which MIB those groups are located.
3. Locating the object and/or notification group in its specific MIB to review what individual objects or traps it contains.

Platform sysObjectIDs

Each hardware platform in the Acme Packet family has a designated system object ID (sysObjectID). In addition to the system object ID, each platform includes a descriptive string (sysDescr) comprised of the product name followed by a string identifying the full software version operating on the system.

The table below provides sysObjectID values for all platforms.

Platform	sysObjectID OID Name: Number
Acme Packet 4500	apNetNet4500: 1.3.6.1.4.1.9148.1.1.2
Acme Packet 3820	apNetNet3800: 1.3.6.1.4.1.9148.1.3.3
Acme Packet 3820	apNetNet3820: 1.3.6.1.4.1.9148.1.3.2
Acme Packet 6300	apNetNet6300 1.3.6.1.4.1.9148.1.5.1

Related Documentation

The following table describes the documentation set for this release.

Document Name	Document Description
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.

About this Guide

Document Name	Document Description
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Service Provider Oracle USM.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle USM logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle USM's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the Oracle USM's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle USM's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle USM family of products.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.

Revision History

Date	Description
March 2016	<ul style="list-style-type: none"><li data-bbox="854 268 1049 296">• Initial release
March 2017	<ul style="list-style-type: none"><li data-bbox="854 338 1409 432">• Provides more thorough explanations of the apSysMgmtTacacsDownClearTrap and apSysMgmtTacasDownTrap SNMP traps.
April 2017	<ul style="list-style-type: none"><li data-bbox="854 468 1438 527">• Updates the guide to reflect the deprecation of MGCP.

Introduction

This chapter describes Management Information Bases (MIBs) and the correlation between system alarms and the MIBs that support traps. It also provides reference information about log levels, syslog level severities (the protocol used for the network logging of system and network events), and trap receiver filter levels.

About MIBs

Each network device managed by SNMP must have a MIB that describes its manageable objects. MIBs are collections of objects or definitions that define the properties of the managed objects. Each managed object has specific characteristics.

The manager relies upon the database of definitions and information about the properties of managed resources and the services the agents support. When new agents are added to extend the management domain of a manager, the manager must be provided with a new MIB component that defines the manageable features of the resources managed through that agent.

The data types and the representations of resources within a MIB, as well as the structure of a particular MIB, are defined in a standard called the Structure of Management Information (SMI).

Object Identifiers and Instance IDs

Each managed object/characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (for example, 1.3.6.1.4.1.9148.1); numeric OIDs can also be translated into human-readable form. The MIB associates each OID with a readable label and various other parameters related to the object. The OID identifies the location of a given managed object within the MIB tree hierarchy by listing the numbers in sequence from the top of the tree down to the node, separated by dots.

By specifying a path to the object through the MIB tree, the OID allows the object to be uniquely identified. The digits below the enterprise OID in the tree can be any sequence of user-defined numbers chosen by an organization to represent its private MIB groups and managed objects.

An instance ID identifies developments that have occurred for the managed object. The instance ID values are represented as a combination of the OID and the table index. For example, you can find the following instance ID in the TCP connection table:

```
tcpConnState.127.0.0.1.1024.127.0.0.1.3000
```

- tcpConnState is the OID
- 127.0.0.1 is an IPv4 address

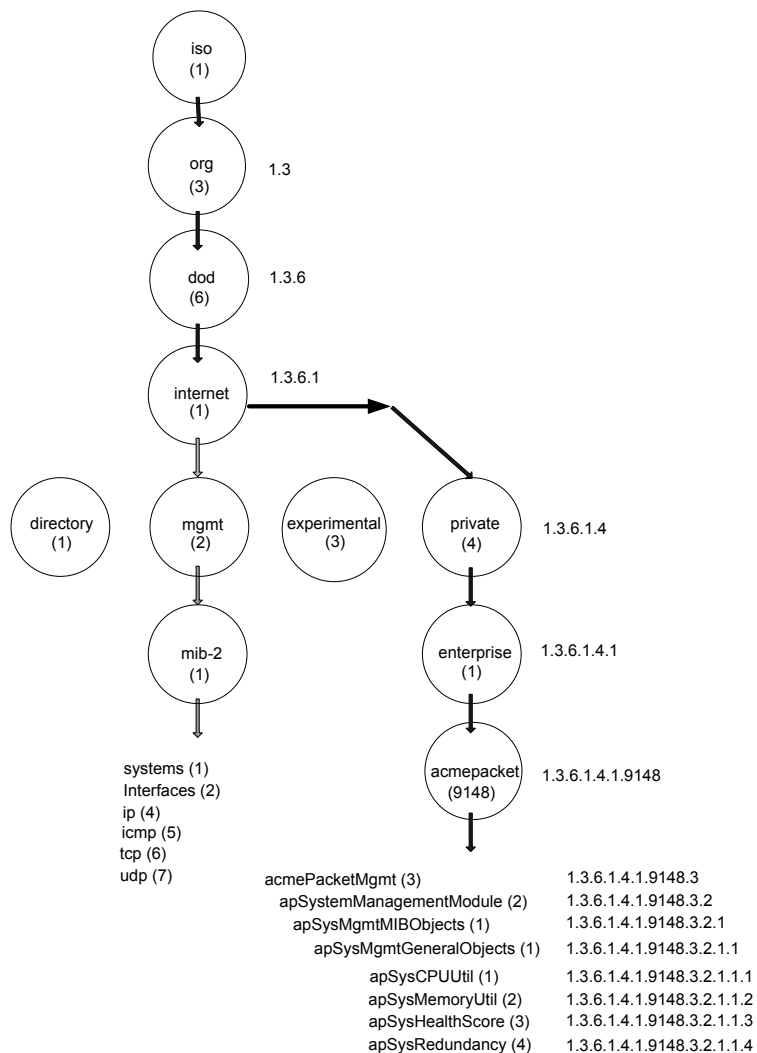
Introduction

- 1024 is the port number
- 127.0.0.1 is another IPv4 address
- 3000 is another port number

MIB Tree Structure

MIBs are arranged in a tree-structured fashion, similar in many ways to a operating system directory structure of files. The following diagram illustrates a MIB tree with a sample of the standard MIBs shown under the mib-2 node and a sample of a system management enterprise MIB under the enterprise node. (The listing is only a partial sample of the MIB contents.)

The diagram shows how the OID is a concatenation of the prior addresses up to that point. For example, the OID for apSysCPUUtil is 1.3.6.1.4.1.9148.3.2.1.1.1.



The diagram shows the Acme Packet node has the value 9148; this is Oracle's vendor-specific number that uniquely identifies an Acme Packet product MIB. This node is the highest level of the private (proprietary) branch containing Acme Packet managed objects. The number 9148 was assigned by the Internet Assigned Numbers Authority (IANA).

Managed Objects

Managed objects are made up of one or more object instances, which are essentially variables. Managed objects can be scalar (defining a single object instance) or tabular (defining multiple, related instances).

Scalar MIB Objects

Scalar MIB objects contain one precise piece of data (also referred to as discrete). These objects are often distinguished from the table objects by adding a .0 (dot-zero) extension to their names. Many SNMP objects are scalar. That is, the operator merely has to know the name of the object and no other information. Discrete objects often represent summary values for a device, particularly useful for scanning information from the network for the purposes of comparing network device performance. If the extension (instance number) of the object is not specified, it can be assumed as .0 (dot-zero). See the Enterprise SNMP Get Requests chapter for examples of scalar MIB objects.

Table MIB Objects

Table MIB objects contain multiple pieces of management data. These objects are distinguished from the scalar objects by requiring a . (dot) extension to their names that uniquely distinguishes the particular value being referenced. The . (dot) extension is also referred as the instance number of an SNMP object. In the case of table objects, this instance number is the index into the SNMP table. (In the case of scalar objects, this instance number is zero.)

SNMP tables allow parallel information to be supported. Tables are distinguished from scalar objects, in that tables can grow without bounds. For example, SNMP defines the ifDescr object as a standard SNMP object, which 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 could 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.) See the Enterprise SNMP Get Requests chapter for examples of table MIB objects.

SNMP Traps

The MIB also contains information about SNMP traps, which enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. When an element sends a TRAP packet, it can include OID and value information (bindings) to clarify the event.

MIBs Supported

The system supports both standard MIBs and Oracle-specific MIBs (enterprise MIBs). The configurable system elements are identified in the MIBs provided by Oracle. Every system maintains a database of values for each of the definitions written in these MIBs.

Standard MIBS

The values in the standard MIBs are defined in RFC-1213, (one of the governing specifications for SNMP). A standard MIB includes objects to measure and monitor IP activity, TCP activity, UDP activity, IP routes, TCP connections, interfaces, and general system description. Each of these values is associated both an official name (such as sysUpTime, which is the elapsed time since the managed device was booted) and a numeric value expressed in dot-notation (such as 1.3.6.1.2.1.1.3.0, which is the OID for sysUpTime).

Oracle provides the following standard MIBs:

- rfc3411-framework.mib
- rfc1907-snmpv2.mib
- rfc2011-ip.mib
- rfc2737-entity.mib
- rfc2863-if.mib (Oracle supports the ifName entry of the ifXTable, which is an extension to the interface table and which replaces ifExtnsTable. See RFC 2863 for details.)
- ianaiftype.mib
- rfc4001-inetAddr.mib
- rfc4022-tcp.mib

Introduction

- rfc4113-udp.mib

Enterprise MIBs

Oracle provides the following enterprise MIBs:

MIB Name	Description
ap-agentcapability.mib	<p>Details the SNMP agent's capabilities that includes support for different modules:</p> <ul style="list-style-type: none">• SNMPv2 capabilities support the SNMPv2 MIB and include the systemGroup, snmpGroup, snmpCommunityGroup, and snmpBasicNotificationsGroup variables.• MIB-II capabilities support MIB-II and include the User Datagram Protocol (UDP)-MIB (udpGroup) variables and some, but not all of the IF-MIB (ifGeneralGroup and ifPacketGroup), IP-MIB (ipGroup and icmpGroup), and TCP-MIB (tcpGroup) variables. For more information about which variables are currently supported, refer to the ap-agentcapability.mib file.• MIB capabilities include support for the contents of the MIBs listed in this table. Refer to the individual MIBs for details.
ap-ami.mib	Management interface on the SBC.
ap-codec.mib	Codec and transcoding information generated by systems.
ap-ems.mib	EMS traps.
ap-entity-vendortype.mib	OID assignments for Acme Packet hardware components.
ap-env-monitor.mib	Fan speed, voltage, temperature, and power supply for the system. It also sends out traps when status changes occur.
ap-license.mib	Status of your licenses.
ap-products.mib	Descriptions of the different SBC versions.
ap-security.mib	Information about the Acme Management Interface running on the SBC.
ap-slog.mib	<p>syslog messages generated by the system via SNMP. Used for the network logging of system and network events, the syslog protocol facilitates the transmission of event notification messages across networks. The syslog MIB can also be used to allow remote log access. The SNMP system manager references syslog to find out about any and all syslog messages.</p> <p>If the following conditions are present, the SNMP agent sends an SNMP trap when a message is sent to the syslog system:</p> <ul style="list-style-type: none">• The system configurations's snmp-enabled parameter is set to enabled.• The system configuration's enable-snmp-syslog-notify parameter is set to enabled.• The actual syslog severity level is of equal or greater severity than the severity level configured in the system config's snmp-syslog-level field. <p>No trap is sent under the following conditions:</p>

MIB Name	Description
	<ul style="list-style-type: none"> A syslog event is generated and the system config's enable-snmp-syslog-notify parameter is set to disabled. The actual syslog severity level is of lesser severity (for example, higher numerical code value) than the severity level configured in the system config's snmp-syslog-level parameter.
ap-smgmt.mib	Status of the system (for example, system memory or system health).
ap-smi.mib	General information about the system's top-level architectural design.
ap-swinventory.mib	Status of the boot images, configuration information, and bootloader images for the system.
ap-tc.mib	Textual conventions used in enterprise MIBs.

Traps

A trap is initiated by tasks to report that an event has happened on the system. SNMP traps enable an SNMP agent to notify the NMS of significant events using an unsolicited SNMP message.

Oracle uses SNMPv2c. These notification definitions are used to send standard and enterprise traps.

Traps are sent according to the criteria established in the following:

- IETF RFC 1907 Management Information Base for Version 2 of the Simple Network Management Protocol
- IETF RFC 2233 The Interfaces Group MIB using SMIV2
- Appropriate enterprise MIB (for example the syslog MIB or the System Management MIB).

Standard Traps

The following table identifies the standard traps that the system supports.

Trap Name	Description
linkUp	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.
linkDown	The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state.
coldStart	The SNMPv2 agent is reinitializing itself and its configuration may have been altered. This trap is not associated with a system alarm.
authenticationFailure	The SNMPv2 agent received a protocol message that was not properly authenticated. If the snmp-enabled and enable-snmp-auth-traps fields in the ACLI's system-config element are set to enabled a snmpEnableAuthenTraps object is generated. This trap is not associated with a system alarm.

Introduction

Enterprise Traps

The following sections list traps available on the Oracle USM. Traps are divided by the mib file they are contained within.

apApps Traps (ap-apps.mib)

The following traps are found in ap-apps.mib.

Trap	Description
apAppsENUMServerStatusChangeTrap 1.3.6.1.4.1.9148.3.16.2.2.1.0.1	Generated if the reachability status of an ENUM server changes.
apAppsDnsServerStatusChangeTrap 1.3.6.1.4.1.9148.3.16.2.2.2.0.1	Generated if the reachability status of a DNS server changes.

apDiameter Traps (ap-diameter.mib)

The following traps are found in ap-diameter.mib.

Trap	Description
apDiameterAcctSrvrUpTrap: .1.3.6.1.4.1.9148.3.13.1.2.2.0.1	Generated when a Diameter Accounting Server goes up.
apDiameterAcctSrvrDownTrap: 1.3.6.1.4.1.9148.3.13.1.2.2.0.2	Generated when a Diameter Accounting Server goes down.
apAcctMsgQueueFullTrap: 1.3.6.1.4.1.9148.3.13.1.2.2.0.3	Generated when the accounting message queue is full and all accounting servers are down.
apAcctMsgQueueFullClearTrap: 1.3.6.1.4.1.9148.3.13.1.2.2.0.4	Generated when the apAcctMsgQueueFullTrap condition clears.
apDiameterSrvrErrorResultTrap: 1.3.6.1.4.1.9148.3.13.1.2.2.0.5	Generated when the Diameter Server returns 3xxx (Protocol Errors), 4xxx (Transient Failures), or 5xxx (Permanent Failure) Result-Code AVP (268).
apDiameterSrvrSuccessResultTrap: 1.3.6.1.4.1.9148.3.13.1.2.2.0.6	After an error result, generated when the Diameter Server returns a 2xxx (Success) Result-Code AVP (268).

apDnsAlg Traps (ap-dnsalg.mib)

The following traps are found in ap-dnsalg.mib.

Trap	Description
apDnsAlgStatusChangeTrap 1.3.6.1.4.1.9148.3.14.2.2.0.1	Generated if the reachability status of a DNS-ALG server changes from In-Service to either Timed out or Out of Service.
apDnsAlgStatusChangeClearTrap 1.3.6.1.4.1.9148.3.14.2.2.0.2	Generated if the reachability status of a DNS-ALG server changes from either Timed out or Out of Service to In-Service.
apDnsAlgConstraintStateChangeTrap 1.3.6.1.4.1.9148.3.14.2.2.0.3	Generated if a DNS-ALG configuration object's constraints state changes from In-Service to Constraints Exceeded.

Trap	Description
apDnsAlgConstraintStateChangeClearTrap 1.3.6.1.4.1.9148.3.14.2.2.0.4	Generated if a DNS-ALG configuration object's constraints state changes from Constraints Exceeded to In-Service.
apDnsAlgSvrConstraintStateChangeTrap 1.3.6.1.4.1.9148.3.14.2.2.0.5	Generated if a DNS Server (i.e. IP-Address) constraints state changes from In-Service to Constraints Exceeded.
apDnsAlgSvrConstraintStateChangeClearTrap 1.3.6.1.4.1.9148.3.14.2.2.0.6	Generated if a DNS Serve (i.e. IP-Address) constraints state changes from Constraints Exceeded to In-Service.

apEnvMon Traps (ap-env-monitor.mib)

The following traps are found in `ap-env-monitor.mib`. They are used generally for reporting on environmental changes.

Trap	Description
apEnvMonI2CFailNotification: 1.3.6.1.4.1.9148.3.3.4.0.1	Sent when the Inter-IC bus (I2C) state changes from normal (1) to not functioning (7).
apEnvMonPortChangeNotification: 1.3.6.1.4.1.9148.3.3.4.0.5	For the AP4500 only. Generated if a physical port is inserted/present or removed/not present.
apEnvMonStatusChangeNotification: 1.3.6.1.4.1.9148.3.3.4.0.2	Sent when any entry of any environment monitor table changes in the state of a device being monitored. To receive this trap, you need to set the system config's enable- env- monitor- table value to enabled.

apLicense Traps (ap-license.mib)

The following traps are found in `ap-license.mib`. They are used generally for reporting on environmental changes.

Trap	Description
apLicenseApproachingCapacityNotification: 1.3.6.1.4.1.9148.3.5.3.0.1	Generated when the total number of active sessions on the system (across all protocols) is within 98 - 100% of the licensed capacity.
apLicenseNotApproachingCapacityNotification: 1.3.6.1.4.1.9148.3.5.3.0.2	Generated when the total number of active sessions on the system (across all protocols) has gone to or below 90% of its licensed capacity (but no sooner than 15 seconds after the original alarm was triggered).
apLicenseExpirationWarningNotification 1.3.6.1.4.1.9148.3.5.3.0.3	This trap is sent when a license is within 7 days of expiration.

apSecurity Traps (ap-security.mib)

The following traps are found in `ap-security.mib`.

Introduction

Trap	Description
apSecurityTunnelFailureNotification: 1.3.6.1.4.1.9148.3.9.3.1.0.1	Generated when an IPSec IKEV2 tunnel cannot be established.
apSecurityTunnelDPDNotification: 1.3.6.1.4.1.9148.3.9.3.2.0.1	Generated when an IPSec IKEV2 tunnel fails because of Dead Peer Detection (DPD).
apSecurityCRLInvalidNotification: 1.3.6.1.4.1.9148.3.9.3.4.0.1	Generated when an invalid CRL is detected.
apSecurityCertExpiredNotification 1.3.6.1.4.1.9148.3.9.3.6.0.1	This trap is generated periodically if a locally installed certificate has expired. The interval of minutes between this trap being generated is configured in the local-cert-exp-trap-int parameter.
apSecurityCertExpireSoonNotification 1.3.6.1.4.1.9148.3.9.3.6.0.2	This trap is generated if a locally installed certificate will soon expire. The number of days before expiration in which this trap is sent is configured in the local-cert-exp-warn-period parameter.
apSecurityTacacsFailureNotification 1.3.6.1.4.1.9148.3.9.3.1.0.4	Generated when TACACS+ authentication request fails due to one of the following reasons: <ul style="list-style-type: none"> • a TACACS+ daemon becomes unreachable • an unreachable TACACS+ daemon becomes reachable • an authentication error occurs • an authorization error occurs

apSip Traps (ap-sip.mib)

The following traps are found in ap-sip.mib.

Trap Name	Description
apSipSecInterfaceRegThresholdExceededTrap: 1.3.6.1.4.1.9148.3.15.2.1.2.0.1	Generated if the total number of registrations on all secondary SIP interfaces exceeds the configured threshold.
apSipSecInterfaceRegThresholdClearTrap: 1.3.6.1.4.1.9148.3.15.2.1.2.0.2	Generated if the total number of registrations on all secondary SIP interfaces falls below the configured threshold.
apSipCACUtilAlertTrap 1.3.6.1.4.1.9148.3.15.2.3.2.0.1	Generated if the apSipCACUtilTrapValue exceeds the monitoring threshold set in the cac-trap-threshold configured in a realm or session agent.
apSipCACUtilClearTrap 1.3.6.1.4.1.9148.3.15.2.3.2.0.2	Generated when the CAC utilization thresholds fall below the cac-trap-threshold configured in a realm or session agent.

apSyslog Traps (ap-slog.mib)

The following traps are found in ap-slog.mib. They are used generally for reporting on environmental changes.

Trap	Description
apSyslogMessageGenerated: 1.3.6.1.4.1.9148.3.1.2.0.1	Generated by a syslog event. For example, this trap is generated if a switchover alarm occurs (for High Availability (HA) system peers only), or if an HA system peer times out or goes out-of-service.

apSysMgmt Traps (ap-smgmt.mib)

The following traps are found in ap-smgmt.mib. These Traps generally are used for system management.

Trap	Description
apSysMgmtAlgdCPULoadTrap: 1.3.6.1.4.1.9148.3.2.6.0.24	Generated if the CPU utilization percentage of application tasks has exceeded the threshold algd-load-limit.
apSysMgmtAlgdCPULoadClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.25	Generated when the CPU utilization percentage of application tasks has fallen below the threshold algd-load-limit.
apSysMgmtRejectedMesagesThresholdExeededTrap 1.3.6.1.4.1.9148.3.2.6.0.57	Generates when the number of rejected messages exceeds the configured threshold within the configured window. This trap is used for both whitelists and HMR rejected messages. The trap does not indicate which feature enabled this trap. To indicate which messages and rules generated the trap, you can consult the matched.log file.
apSysMgmtAdminAuditLogFullTrap: 1.3.6.1.4.1.9148.3.2.6.0.58	Generated when one of the audit logs full threshold is met: <ul style="list-style-type: none"> time interval file size percentage full
apSysMgmtAdminAuditLogFullClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.59	Generated when free audit log storage space becomes available.
apSysMgmtAdminAuditPushFailTrap: 1.3.6.1.4.1.9148.3.2.6.0.60	Generated when the audit file transfer fails.
apSysMgmtAdminAuditPushFailClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.61	Generated when the audit file is successfully transferred.
apSysMgmtAdminAuthLockoutTrap: 1.3.6.1.4.1.9148.3.2.6.0.64	Generated upon system lockout after multiple authentication failures.
apSysMgmtAuthenticationFailedTrap: 1.3.6.1.4.1.9148.3.2.6.0.16	Generated when an attempt to login to the SBC through Telnet, SSH, or by using the console fails for any reason; also sent when if a user fails authentication on the console or over FTP, SSH, or SFTP. The trap sent to all configured trap receivers includes the following information: <ul style="list-style-type: none"> administration and access level (SSH, user, enable)


Introduction

Trap	Description
	<ul style="list-style-type: none"> connection type (Telnet or console) FTP support is new to Release C5.0.
apSysMgmtCallRecordingStateChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.50	Generated when a call recording server changes state.
apSysMgmtCdrFileDeleteTrap	Generated when a CDR file is deleted because of lack of space on the partition or the drive exceeds the number of files specified.
apSysMgmtCDRPushReceiverFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.53	Generated when an enabled CDR push receiver fails. Returns the address, the address type, and the failure reason code.
apSysMgmtCDRPushReceiverFailureClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.54	Generated when an enabled CDR push receiver resumes normal operation after a failure.
apSysMgmtCDRPushAllReceiversFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.55	Generated when all enabled CDR push receivers fail.
apSysMgmtCDRPushAllReceiversFailureClearTrap 1.3.6.1.4.1.9148.3.2.6.0.56	Generated when one or more enabled CDR push receivers return to normal operation after failures were encountered on all push receivers.
apSysMgmtCfgSaveFailTrap: 1.3.6.1.4.1.9148.3.2.6.0.13	Generated if an error occurs while the system is trying to save the configuration to memory.
apSysMgmtCollectorPushSuccessTrap: 1.3.6.1.4.1.9148.3.2.6.0.44	Generated when the collector successfully completes a push operation.
apSysMgmtENUMStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.27	Generated if the reachability status of an ENUM server changes; contains: <ul style="list-style-type: none"> apENUMConfigName apENUMServerIpAddress apENUMServerStatus
apSysMgmtExpDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.2	Generated when a device exceeds configured thresholds and is denied access by the SBC.
apSysMgmtFanTrap: 1.3.6.1.4.1.9148.3.2.6.0.3	Generated if a fan unit speed falls below the monitoring level.
apSysMgmtGatewaySynchronizedTrap: 1.3.6.1.4.1.9148.3.2.6.0.49	Generated when the default gateway is synchronized in the ARP table.
apSysMgmtGatewayUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.10	Generated if the gateway specified becomes unreachable by the system.
apSysMgmtGatewayUnreachableClear: 1.3.6.1.4.1.9148.3.2.6.0.21	Generated when the system determines that the gateway in question is once again reachable.


Trap	Description
apSysMgmtGroupTrap: 1.3.6.1.4.1.9148.3.2.3.0.1	Generated when a significant threshold for a system resource use or health score is exceeded. For example, if Network Address Translation (NAT) table usage, Address Resolution Protocol (ARP) table usage, memory usage, or Central Processing Unit (CPU) usage reaches 90% or greater of its capacity, the apSysMgmtGroupTrap is generated. If the health score (for HA peers only) falls below 60, the apSysMgmtGroupTrap is generated. This trap is sent for sessions only if tiered thresholds for sessions have been configured in system-config>alarm-threshold. If no tiered thresholds have been configured for sessions, then the apSysMgmtLicenseCapacity is sent.
apSysMgmtGroupClearTrap: 1.3.6.1.4.1.9148.3.2.3.0.2	Generated when the SBC's system resource use or its health score returns to levels that are within thresholds. For example, NAT table usage or memory usage could return to acceptable levels, and the systems health score could return to a level above 60.
apSysMgmtHardwareErrorTrap: 1.3.6.1.4.1.9148.3.2.6.0.14	Provides a text string indicating the type of hardware error that has occurred. If the message text exceeds 255 bytes, the message is truncated to 255 bytes.
apSysMgmtInetAddrWithReasonDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.4	Generated when an IP address is placed on a deny list because of denial-of-service attempts. It provides the IP address that has been demoted, the realm ID of that IP address (if available), the URI portion of the SIP From header for the message that caused the demotion, and the reason for the demotion.
apSysMgmtInetAddrTrustedToUntrustedDOSTrap 1.3.6.1.4.1.9148.3.2.8.0.5	Generated when an IP is placed on a untrusted list from trusted list. Contains the ip address that has been demoted, the realm-id of that IP (if available), and the URI portion of the SIP From header of the message that caused the demotion.
apSysMgmtInterfaceStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.26	Generated when there is a change in the status of the SIP interface; either the SIP interface is in service or constraints have been exceeded. <ul style="list-style-type: none"> • apSysMgmtSipInterfaceRealmName—Realm identifier for the SIP interface (OID 1.3.6.1.4.1.9148.3.2.5.24) • apSysMgmtSipInterfaceIP—IP address of the first SIP port in the SIP interface (OID 1.3.6.1.4.1.9148.3.2.5.25) • apSysMgmtSipInterfaceStatus—Code is 0 (OID 1.3.6.1.4.1.9148.3.2.5.26) • apSysMgmtSipInterfaceStatusReason—Status reasons and in-service (3) and

Introduction

Trap	Description
	constraintExceeded (4) (OID 1.3.6.1.4.1.9148.3.2.5.27)
apSysMgmtLDAPStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.42	Generated if the status of whether a LDAP server is reachable changes.
apSysMgmtMediaBandwidthTrap: 1.3.6.1.4.1.9148.3.2.6.0.7	Generated if bandwidth allocation fails at a percentage higher or equal to the system's default threshold rate. Bandwidth allocation failure rates are checked every 30 seconds. The trap is sent when the failure rate is at 50% or higher. After that time, the trap is sent every 30 seconds until the failure rate drops below 35%. The clear trap is sent once the failure rate drops below 5%.
apSysMgmtMediaBandwidthClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.19	Generated when the percentage rate of failure for media bandwidth allocation decreases to the default allowable threshold.
apSysMgmtMediaOutOfMemory: 1.3.6.1.4.1.9148.3.2.6.0.8	Generated if the media process cannot allocate memory.
apSysMgmtMediaOutOfMemoryClearr: 1.3.6.1.4.1.9148.3.2.6.0.20	Generated when the alarm for insufficient memory for media processes is cleared manually.
apSysMgmtMediaPortsTrap: 1.3.6.1.4.1.9148.3.2.6.0.6	Generated if port allocation fails at a percentage higher or equal to the system's default threshold rate. Port allocation failure rates are checked every 30 seconds. The trap is sent when the failure rate is at 50% or higher. After that time, the trap is sent every 30 seconds until the failure rate drops below 35%. The clear trap is sent once the failure rate drops below 5%.
apSysMgmtMediaPortsClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.18	Generated if the port allocation failure rate drops below the system's default acceptable threshold.
apSysMgmtMediaUnknownRealm: 1.3.6.1.4.1.9148.3.2.6.0.9	Generated if the media process cannot find an associated realm for the media flow.
apSysMgmtNTPClockSkewTrap: 1.3.6.1.4.1.9148.3.2.6.0.43	Generated if the NTP has to adjust the clock by more than 1000 seconds.
apSysMgmtNTPServerUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.30	Generated if the specified NTP server becomes unreachable. <ul style="list-style-type: none"> apSysMgmtNTPServer—Server that is or was formerly unreachable (OID 1.3.6.1.4.1.9148.3.2.5.31)

Trap	Description
apSysMgmtNTPServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.31	Generated when an NTP server deemed unreachable subsequently becomes reachable.
apSysMgmtNTPServiceDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.32	Generated if all configured NTP servers are unreachable.
apSysMgmtNTPServiceDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.33	Generated if NTP service again becomes available.
apSysMgmtPhyUtilThresholdTrap	Generated when the media port's utilization crosses a configured threshold. Indicates whether the OverloadProtection feature is active.
apSysMgmtPhyUtilThresholdClearTrap	Generated when a media port's utilization falls below the lowest configured threshold.
apSysMgmtPowerTrap: 1.3.6.1.4.1.9148.3.2.6.0.1	Generated if a power supply is powered down, powered up, inserted/present or removed/not present.
apSysMgmtPushServerUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.28	Generated if the system collector cannot reach a specified server; used with the historical data recording (HDR) feature.
apSysMgmtPushServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.29	Generated if the system collector can again reach a specified server that was unreachable; used with the historical data recording (HDR) feature.
apSysMgmtRadiusDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.11	Generated if all or some configured RADIUS accounting servers have timed out from a RADIUS server.
apSysMgmtRadiusDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.22	Generated when some or all of the previously unreachable RADIUS servers can be again be reached.
apSysMgmtTacacsDownTrap 1.3.6.1.4.1.9148.3.2.6.0.78	<p>Generated when a TACACS+ server becomes unreachable.</p> <p> Note: The SBC searches for a TACACS+ server until it finds an available one and then stops searching. However, in the TACACS+ SNMP implementation, SNMP expects the SBC to make connection attempts to all servers. When there is only one TACACS+ server and that server goes down, the SBC behaves normally, sending a apSysMgmtTacacsDownTrap trap when the server goes down, and a apSysMgmtTacacsDownClearTrap trap when the server comes back up. When there is more than one TACACS+ server and the active server goes down, an apSysMgmtTacacsDownTrap trap is sent, indicating that some servers are down and the next server is tried. If all servers fail, an</p>

Introduction

Trap	Description
	<p>apSysMgmtTacacsDownTrap is sent indicating that all servers are down. If one of the servers comes back up while the rest are still down, an apSysMgmtTacacsDownTrap is sent indicating that some servers are still down.</p>
<p>apSysMgmtTacacsDownClearTrap 1.3.6.1.4.1.9148.3.2.6.0.79</p>	<p>Generated when a TACACS+ server that was unreachable becomes reachable.</p> <p> Note: The SBC searches for a TACACS+ server until it finds an available one and then stops searching. However, in the TACACS+ SNMP implementation, SNMP expects the SBC to make connection attempts to all servers. When there is only one TACACS+ server and that server goes down, the SBC behaves normally, sending a apSysMgmtTacacsDownTrap trap when the server goes down, and a apSysMgmtTacacsDownClearTrap trap when the server comes back up. When there is more than one TACACS+ server and the active server goes down, an apSysMgmtTacacsDownTrap trap is sent, indicating that some servers are down and the next server is tried. If all servers fail, an apSysMgmtTacacsDownTrap is sent indicating that all servers are down. If one of the servers comes back up while the rest are still down, an apSysMgmtTacacsDownTrap is sent indicating that some servers are still down.</p>
<p>apSysMgmtRealmIcmpFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.51</p>	<p>Generated when ICMP heartbeat failure occurs.</p>
<p>apSysMgmtRealmIcmpFailureClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.52</p>	<p>Generated when ICMP heartbeat failure clears.</p>
<p>apSysMgmtRegCacheThresholdTrap: 1.3.6.1.4.1.9148.3.2.6.0.46</p>	<p>Generated when the number of contacts stored in the registration cache exceeds the configured threshold.</p>
<p>apSysMgmtRegCacheThresholdClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.47</p>	<p>Generated when the number of contacts stored in the registration cache falls below the configured threshold.</p>
<p>apSysMgmtRealmMinutesExceedTrap: 1.3.6.1.4.1.9148.3.2.6.0.40</p>	<p>Generated if the monthly minutes for a realm are exceeded.</p>
<p>apSysMgmtRealmMinutesExceedClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.41</p>	<p>Generated if monthly minutes for a realm are reset.</p>

Trap	Description
apSysMgmtRealmStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.45	Generated when there is a change in the status of the realm constraints.
apSysMgmtRedundancyTrap: 1.3.6.1.4.1.9148.3.2.6.0.5	Generated if a state change occurs on either the primary or secondary system in a redundant (HA) pair.
apSysMgmtSAStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.15	Generated when a session agent is declared unreachable or unresponsive for the following reasons: <ul style="list-style-type: none"> • signaling timeout (H.323 and SIP) • session agent does not respond to SIP pings (SIP only) When session agents are declared unreachable or unresponsive, they are placed out-of-service for a configurable period of time.
apSysMgmtSipRejectionTrap: 1.3.6.1.4.1.9148.3.2.10.0.1	Generated when a SIP INVITE or REGISTRATION request fail.
apSysMgmtSpaceAvailThresholdTrap: 1.3.6.1.4.1.9148.3.2.6.0.68	Generated when the space available on a partition crosses a configured space threshold.
apSysMgmtSpaceAvailThresholdClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.69	Generated when the space available on a partition falls below the lowest configured threshold.
apSysMgmtSurrogateRegFailed: 1.3.6.1.4.1.9148.3.2.6.0.39	Generated if a SIP user attempts to register more than the configured, allowable number of times; supports SIP surrogate registration for IMS. <ul style="list-style-type: none"> • apSysMgmtSurrogateRegHost (OID 1.3.6.1.4.1.9148.3.2.5.5.35) • apSysMgmtSurrogateRegAor (OID 1.3.6.1.4.1.9148.3.2.5.5.36)
apSysMgmtSystemStateTrap: 1.3.6.1.4.1.9148.3.2.6.0.17	Generated when the SBC is instructed to change the system-state or the transition from becoming offline to online occurs. This trap contains one field called apSysMgmtSystemState, and that field has three values: <ul style="list-style-type: none"> • online(0) • becoming-offline(1) • offline(2)
apSysMgmtTaskDelete: 1.3.6.1.4.1.9148.3.2.5.24	Generated to described what task was deleted. From Release C4.1.4 and C5.1.0 forward, this trap contains text noting that the time has been reset when the system clock time and remote clock time are too far skewed.
apSysMgmtTaskDeleteTrap:	[Reserved for future use.]

Introduction

Trap	Description
1.3.6.1.4.1.9148.3.2.6.0.23	Generated when a task is deleted; it reads apSysMgmtTaskDelete and includes the test in the trap.
apSysMgmtTaskSuspendTrap: 1.3.6.1.4.1.9148.3.2.6.0.4	Generated if a critical task running on the system enters a suspended state.
apSysMgmtTempTrap: 1.3.6.1.4.1.9148.3.2.6.0.2	Generated if the temperature falls below the monitoring level.
apSysMgmtAdminWriteFailTrap: 1.3.6.1.4.1.9148.3.2.6.0.62	Generated when a write to file fails.
apSysMgmtAdminWriteFailClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.63	Generated when a write to file succeeds.
apSysMgmtExtPolicyServerConnDownTrap 1.3.6.1.4.1.9148.3.2.6.0.74	Generated when the SBC is unable to connect to an external policy server
apSysMgmtExtPolicyServerConnEstTrap 1.3.6.1.4.1.9148.3.2.6.0.75	Generated when the SBC is able to re-establish a connection with an external policy server
apSwCfgActivateNotification: 1.3.6.1.4.1.9148.3.4.3.0.1	Generated when an activate-config command is issued and the configuration has been changed at running time.
apSecurityOCSRDownNotification: 1.3.6.1.4.1.9148.3.9.3.3.0.1	Generated when an OSCR server becomes unreachable.
apSecurityOCSRUpNotification: 1.3.6.1.4.1.9148.3.9.3.3.0.2	Generated when an OSCR server becomes available.
apSysMgmtOCSRDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.80	Generated if all or some of the configured OSCR accounting servers are down.
apSysMgmtOCSRDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.81	Generated if all OSCR accounting servers have resumed communications.
apSysMgmtCPULoadAvgTrap 1.3.6.1.4.1.9148.3.2.6.0.86	The trap will be generated when CPU Load Average Alarm exceeds its minor alarm threshold.
apSysMgmtCPULoadAvgClearTrap 1.3.6.1.4.1.9148.3.2.6.0.87	The clear trap will be sent when the CPU load average recedes to the minor alarm level.

apUSBC Traps (ap-usbcsys.mib)

The following traps are found in ap-usbcsys.mib.

Trap Name	Description
apUsbcSysThreadUsageExceededTrap 1.3.6.1.4.1.9148.3.17.2.2.1.1	The trap is generated when a thread is exceeding pre-defined usage.
apUsbcSysThreadUsageClearTrap 1.3.6.1.4.1.9148.3.17.2.2.1.2	The trap is generated when a thread is dropping back under pre-defined usage.
apUsbcSysThreadUsageOverloadEnableTrap 1.3.6.1.4.1.9148.3.17.2.2.1.3	The trap is generated when a thread cpu overload is activated.
apUsbcSysThreadUsageOverloadDisableTrap 1.3.6.1.4.1.9148.3.17.2.2.1.4	The trap is generated when a thread cpu overload is deactivated.

EMS Traps

This section describes the EMS traps contained in the EMS MIB. EMS generates traps when it detects the following:

- failure to discover or rediscover a SBC configuration
- failure to save a SBC configuration
- failure to activate a SBC configuration
- missing components when validating a SBC configuration
- node status change from reachable to unreachable

You need to configure an external server as the receiver for these traps.

EMS generates the following traps:

Trap Name	Description
apEMSDiscoveryFailure	Generated when EMS fails to discover or rediscover a SBC configuration. The trap is generated from any discovery or rediscovery failure initiated by the SOAP XML API, EMS, or system processing. The trap contains the SBC's node ID, the start and end time of the discovery or rediscovery operation, and the user who initiated the operation.
apEMSSaveFailure	Generated when EMS fails to save a configuration. The trap is generated by a save failure whether initiated by the SOAP XML API or EMS GUI for save/activate, save or offline save operations. The trap contains the SBC node ID, the start and stop time of the save configuration attempt, and the user initiating the save operation.
apEMSActivateFailure	Generated when EMS fails to activate a configuration, whether initiated from the SOAP XML API or EMS GUI for the save/activate or activate operations.
apEMSInvalidConfigDiscoveredNotification	Generated when EMS validates a discovered SBC's configuration (for example confirms each referenced realm is configured) and detects missing components. The trap contains the time and the SBC node ID.

Introduction

Trap Name	Description
apEMSNodeUnreachableNotification	Generated when a node's status changes from reachable to unreachable. The trap contains the SBC's node ID and the time of the event.
apEMSNodeUnreachableClearNotification	Generated when a node's status changes from unreachable to reachable. The trap contains the SBC's node ID and the time of the event.

SNMPv3 Secure Traps

The Oracle USM supports SNMPv3, which provides the SNMP agent and SNMP Network Management System (NMS) with authentication, privacy, and access control during the delivery of secured traps. Currently, SNMPv3 traps are supported on the Oracle USM; SNMPv3 Get/Get-Bulk/Set actions are not supported at this time.

By default, the Oracle USM supports SNMPv1v2. If you want to retain existing SNMPv1v2 behavior, you do not need to update configuration. You can enable SNMPv3 at any time, at which point SNMPv1v2 configurations are ignored, and only SNMPv3 encrypted traps are sent to associated external SNMP managers. **snmp-agent-mode**, an attribute under **system-config**, allows you to select the desired mode.

Authentication and Privacy

SNMPv3 employs a User-Based Security Model (USM). The two protocols used for authentication and privacy are:

- Authentication—HMAC-SHA-96
- Privacy—CBC-DES

Four parameters generate keys under the designated algorithm:

- **SNMPEngineID**—The unique identifier for the SNMP Engine. This value is a specially formatted string for use in the SNMP.
- **User name**—The user's name as defined under **snmp-user-entry**.
- **Authorization password**—The authorization password configured under the **snmp-user-entry** configuration. This parameter is used to derive the authentication key.
- **Privacy password**—You set the privacy password in the **snmp-user-entry** configuration. It is used to derive the password key.

Password-to-Key Conversion

There are two distinct passwords in SNMPv3. The authentication password is manipulated using the HMAC-SHA-96 algorithm to produce a key used to authenticate the trap. Authentication ensures the identity of the user and that the trap has not been tampered with in transit. Likewise, the privacy password is manipulated using the CBC-DES algorithm to ensure message privacy.

One user is associated by a name, an authentication password and a privacy password. These three parameters are always consistent for the user and can be used across multiple Oracle USMs. The key generation differs from one Oracle USM to another due to the varying **SNMPEngineIDs**. This ensures that a compromised key for one Oracle USM does not compromise the keys for other Oracle USMs associated with the same user.

Enabling SNMPv3

The table below gives a brief overview of the SNMPv3 configuration on your SBC. The Caveats column describes the SNMPv1v2 configuration attributes that are ignored if **SECURE-TRAP** mode is enabled.

Configuration	Description	Caveat
snmp-agent-mode	Set this attribute to SECURE-TRAP to enable SNMPv3.	Once SNMPv3 is enabled, the snmp-community and community-name attributes are ignored.
snmp-engine-id-suffix	Set this attribute as a string to customize and uniquely identify the SNMP Engine.	The show snmp-info command has been expanded to include the SNMP Engine Base, the SNMP Engine Suffix, and the SNMP Engine ID.
snmp-user-entry	Enter the user name, authorization password and privacy password.	The user, as defined in this object, must be added to the attribute user-list under trap-receiver in order to receive secured traps.
trap-receiver	Configure a trap-receiver with the IP address of the NMS that receives secured traps.	
user-list	Add users who are authorized to receive secured traps.	If instances of snmp-user-entry are configured, but no users are listed under user-list, a warning message is sent during a verify-config execution.

Consideration for HA Nodes

Key pairs are generated based on the user and SNMPEngineID. In the event of a switchover, the SNMPEngineID will vary. The user's NMS should be updated with the SNMPEngineID of the standby Oracle USM.

Complete SNMPv3 Configuration

Configuring the Oracle USM to use SNMPv3 requires completion of 3 procedures.

1. Enabling SNMPv3
2. Adding SNMPv3 users
3. Adding trap receivers

SNMPv3 Configuration

To enable SNMPv3 on the SBC for sending secured traps:

1. Access the **system-config** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# system-config
ORACLE(system-config)#
```

2. Type **select** to begin editing the **system-config** object.

```
ORACLE(system-config)# select
ACMEPACKET(system-config)#
```

3. **snmp-agent-mode**—To enable support, change this parameter from its default (V1V2) to **SECURE-TRAP**.

```
ORACLE(system-config)# snmp-agent-mode secure-trap
```

4. **snmp-engine-id-suffix**—To set a unique suffix for the SNMPEngineID, enter a string. This attribute is optional.

```
ORACLE(system-config)# snmp-engine-id-suffix Group1Unit3
```

Introduction

5. Type **done** to save your configuration.

Users and Password for SNMPv3 Configuration

To configure users for SNMPv3:

1. Access the **snmp-user-entry** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# snmp-user-entry
ORACLE(snmp-user-entry)
```

2. **user-name**—Enter the name for this user. This value is required and must be unique.

```
ORACLE(snmp-user-entry)# user-name monitor
```

3. **auth-password**—Enter the authorization password for this user. Passwords must be 6-24 characters long. The password will be shown as **** regardless of the length. This value is required.

```
ORACLE(snmp-user-entry)# auth-password ****
```

4. **priv-password**—Enter the privacy password for this user. Passwords must be 6-24 characters long. The password will be shown as **** regardless of the length. This value is required.

```
ORACLE(snmp-user-entry)# priv-password ****
```

5. Type **done** to save your configuration.

Adding Authorized Trap Receivers

To add users as authorized trap-receivers:

1. Access the **trap-receiver** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# trap-receiver
ORACLE(trap-receiver)#
```

2. Select the **trap-receiver** object to edit.

```
ORACLE(trap-receiver)# select
<ip-address>:
```

```
ORACLE(trap-receiver)#
```

3. **ip-address**—Enter the IP address and port for the NMS that supports SNMPv3.

```
ORACLE(trap-receiver)# ip-address 172.30.0.82:1620
```

4. **user-list**—Add or subtract users to the list using (+) and (-) symbols.

```
ORACLE(trap-receiver)# user-list +monitor
```

5. Type **done** to save your configuration.

Persistent indexing of SNMP Tables

Certain Oracle USM proprietary MIB tables support persistent indexing across reboots. The purpose is to maintain the value of that object so that after a reboot or configuration reload, the value that identifies an object remains the same.

Please be aware of the following three limitations:

ObjectID Wrapping

The maximum value of an object that is persistently indexed is 4294967295. In the unlikely event that the Net-Net SBC exhausts all index values, it will wrap beginning with the first, lowest, unused index number.

Consecutive Table Entries

For any two consecutive table entries, the indices from ObjectID are not guaranteed to be consecutive. The value of an ObjectID reflects the order when the object is created.

Persistent Exception

Using the backup-config and the restore-backup-config commands do not impact the index persistency. But, if a configuration file created on one Net-Net SBC is loaded on another Net-Net SBC, the element IDs were assigned by the first Net-Net SBC are likely to be different that the IDs used on the second Net-Net SBC.

If, after a backup is created, an element is deleted from the configuration and then later created again, the element's ID will probably change. Then, if the operator restores an older backup, a change in the MIB ID of the object will result.

Table 1: List of Persistently indexed MIB Tables

MIB Table	in MIB file	Persistent Index
apSigRealmStatsTable 1.3.6.1.4.1.9148.3.2.1.2.4	ap-smgmt.mib	apSigRealmStatsRealmIndex
apCombinedSessionAgentStatsTable 1.3.6.1.4.1.9148.3.2.1.2.1	ap-smgmt.mib	apCombinedStatsSessionAgentIndex
apSipSessionAgentStatsTable 1.3.6.1.4.1.9148.3.2.1.2.2	ap-smgmt.mib	apSipSAStatsSessionAgentIndex
apH323SessionAgentStatsTable 1.3.6.1.4.1.9148.3.2.1.2.3	ap-smgmt.mib	apH323SAStatsSessionAgentIndex

Log Levels and syslog Level Severities

There is a direct correlation between log levels and syslog level severities. This correlation can be used for syslog MIB reference purposes.

Log Levels

The following table defines the log levels by name and number, and provides a description of each level.

Numerical Code	Log Level	Description
1	EMERGENCY	The most severe condition within the system which requires immediate attention. If you do not attend to it immediately, there could be physical, irreparable damage to your system.
2	CRITICAL	A serious condition within the system which requires attention as soon as it is noted. If you do not attend to these conditions immediately, there may be physical damage to your system.
3	MAJOR	Functionality has been seriously compromised. As a result, there may be loss of functionality, hanging

Introduction

Numerical Code	Log Level	Description
		applications, and dropped packets. If you do not attend to this situation, your system will suffer no physical harm, but it will cease to function.
4	MINOR	Functionality has been impaired to a certain degree and, as a result, you may experience compromised functionality. There will be no physical harm to your system. However, you should attend to it as soon as possible in order to keep your system operating properly.
5	WARNING	The system has noted some irregularities in its performance. This condition is used to describe situations that are noteworthy. Nonetheless, you should attend to it in order to keep your system operating properly.
6	NOTICE	All used for Oracle customer support purposes.
7	INFO	
8	TRACE	
9	DEBUG	

syslog Level Severities

The following table defines the syslog levels by severity and number against the University of California Berkeley Software Distribution (BSD) syslog severities (by level and number).

Refer to the Example Log Message column to view example syslog-related content/messages.

syslog Level (Numerical Code)	BSD syslog Severity Level (Number)
EMERGENCY (1)	Emergency - system is unusable (0)
CRITICAL (2)	Alert - action must be taken immediately (1)
MAJOR (3)	Critical - critical conditions (2)
MINOR (4)	Error - error conditions (3)
WARNING (5)	Warning - warning conditions (4)
NOTICE (6)	Notice - normal, but significant condition (5)
INFO (7)	Informational - informational messages (6)
TRACE (8)	Debug - debug level messages (7)
DEBUG (9)	

Mapping Trap Filter Levels to syslog and Alarm Severities

Although there is no direct correlation between system alarms and the generation of SNMP traps, traps can be mapped to syslog and alarm severities through trap filters that are configured in the filter-level field of the trap-receiver configuration element of the ACLI. The following table shows this mapping.

filter-level Field Value	Filter Level Description	syslog Level (Numerical Code)	Alarm Severity Levels
CRITICAL	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to CRITICAL (with a lesser log level numerical code). The corresponding NMS receives only error events.	EMERGENCY (1) CRITICAL (2)	EMERGENCY CRITICAL
MAJOR	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to MAJOR (with a lesser log level numerical code). The corresponding NMS receives warning and error events.	EMERGENCY (1) CRITICAL (2) MAJOR (3)	EMERGENCY CRITICAL MAJOR
MINOR	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to MINOR (i.e., with a lesser log level numerical code) a generate a trap. The corresponding NMS receives informational, warning, and error events.	EMERGENCY (1) CRITICAL (2) MAJOR (3) MINOR (4)	EMERGENCY CRITICAL MAJOR MINOR
ALL	The SNMP agent sends a trap for all alarms, syslogs, and other traps. The corresponding NMS receives informational, warning, and error events.	EMERGENCY (1) CRITICAL (2) MAJOR (3) MINOR (4) WARNING (5) NOTICE (6) INFO (7) TRACE (8) DEBUG (9)	EMERGENCY CRITICAL MAJOR MINOR WARNING

The following table describes the types of events that an NMS can receive.

Event Category	Description
Error	Indicates a catastrophic condition has occurred (e.g., an internal temperature reading exceeds the recommendation).
Warning	Indicates pending failures or unexpected events (e.g., at the console, you typed the wrong password three consecutive times)
Informational	Represents non-critical conditions (e.g., an event can indicate to an administrator that a configuration element has changed).

For more information about the filter-level field specifically or the trap-receiver element in general, refer to the Configuration via the ACLI chapter of the Administration and Configuration Guide for the ACLI.

Standard SNMP GET Requests

This section explains the standard SNMP GET requests supported by the Oracle USM. SNMP uses five basic messages, one of which is the GET request that is used to query for information on or about a network entity.

Interfaces Object

MIB Object	Object ID: 1.3.6.1.2.1.2 +	Description
ifNumber	.1	The number of network interfaces (regardless of their current state) present on this system.
ifTable	.2	A list of interface entries. The number of entries is given by the value of ifNumber.

Interface Table

The following table describes the standard SNMP Get support for the interfaces table, which contains information on the entity's interfaces. Each interface is thought of as being attached to a subnetwork. (Note that this term should not be confused with subnet, which refers to an addressing partitioning scheme used in the Internet suite of protocols.)

MIB Object	Object ID 1.3.6.1.2.1.2.2.1 +	Description
ifIndex	.1	Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization. See for examples of ifIndex values.
ifDescr	.2	Textual string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the hardware interface.
ifType	.3	Information about the type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.

Standard SNMP GET Requests

MIB Object	Object ID 1.3.6.1.2.1.2.2.1 +	Description
ifMtu	.4	Size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface.
ifSpeed	.5	Estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where an accurate estimation cannot be made, it contains the nominal bandwidth.
ifPhysAddress	.6	Address of the interface, at the protocol layer immediately below the network layer in the protocol stack. For interfaces which do not have such an address for example., a serial line), it contains an octet string of zero length.
ifAdminStatus	.7	Current administrative state of the interface. The testing(3) state indicates that operational packets cannot be passed.
ifOperStatus	.8	Current operational state of the interface. The testing(3) state indicates that operational packets cannot be passed.
ifLastChange	.9	Value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value.
ifInOctets	.10	Total number of octets received on the interface, including framing characters.
ifInUcastPkts	.11	Number of subnetwork-unicast packets delivered to a higherlayer protocol.
ifInNUcastPkts	.12	Number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
ifInDiscards	.13	Number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	.14	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	.15	Number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
ifOutOctets	.16	Total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	.17	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
ifOutNUcastPkt	.18	Total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a

MIB Object	Object ID 1.3.6.1.2.1.2.2.1 +	Description
		subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
ifOutDiscards	.19	Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutErrors	.20	Number of outbound packets that could not be transmitted because of errors.
ifOutQLen	.21	Length of the output packet queue (in packets).
ifSpecific	.22	Returns a reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER {0 0}, which is a syntactically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.

Interface Description in MIB

The *ifDescr* object in the *ifEntry* object in *ifTable* is a string of up to 255 characters. It currently contains the name of the interface only. This change adds to the *ifDescr* string, separated from the first part by a space, a keyword that represents the internal interface type. The values can be {ETH, FE, GE, OC, XE, null}.

RFC 3635 supercedes RFC 2665. RFC 2665 recommends, but RFC 3635 requires, that all Ethernet-like interfaces use an *ifType* of ethernetCsmacd (6) regardless of the speed that the interface is running or the link-layer encapsulation in use. Heretofore, Oracle USMs could return values of fastEthernet (62) and gigaEthernet (117), but, in accordance with RFC 3635, will now return ethernetCsmacd (6) for all Ethernet interface types. To let users determine the type of Ethernet interface more readily than by some other method, Oracle has changed the syntax for *ifDescr* to include the interface type.

The current values of *ifDescr* are either the names of physical or network interfaces (for example, "wancom0", "lo", "s1p0", "Access", or "Core"), or, for sub-interfaces, interface names appended with sub-interface numbers (for example, "Access.22" or "Core.33"). This change adds to the *ifDescr* string, separated from the first part by a space, a keyword that represents the internal interface type rather than the actual queried value. The current set of possible values is {ETH, FE, GE, XE, null}.

Examples:

- wancom0 GE
- lo (Second part empty)
- s1p0 GE
- s0p0 XE
- Access GE
- Access.22 (Second part empty)
- Core.33 (Second part empty)

ifXTable Table

The ifXTable is available to support 64-bit counters for interface statistics. Only Gets are supported for this MIB Table, and only media interfaces will be returned in an SNMP query. All other interfaces do not support 64-bit counters.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
ifName	.1	ifName is the textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's console. This might be a text name, such as le0 or a simple port number, such as 1, depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. For an agent that responds to SNMP queries concerning an interface on some other (proxied) device, the value of ifName is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.
ifInMulticastPkts	.2	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifInBroadcastPkts	.3	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutMulticastPkts	.4	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutBroadcastPkts	.5	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
		Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTim
ifHCInOctets	.6	The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCInUcastPkts	.7	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCMulticastPkts	.8	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCInBroadcastPkts	.9	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCOctets	.10	The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of
ifHCOOutUcastPkts	.11	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the

Standard SNMP GET Requests

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
		management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCOutMulticastPkts	.12	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutBroadcastPkts	.13	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifLinkUpDownTrapEnable	.14	Indicates whether linkUp/linkDown traps should be generated for this interface. By default, this object should have the value enabled(1) for interfaces which do not operate on 'top' of any other interface (as defined in the ifStackTable), and disabled(2) otherwise.
ifHighSpeed	.15	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is somewhere in the range of `n-500,000' to `n+499,999'. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero.
ifPromiscuousMode	.16	This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. The value true(1) is only legal on certain types of media. If legal, setting this object to a value of true(1) may require the interface to be reset before becoming effective. The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
ifConnectorPresent	.17	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.

ip Object

The following table describes the standard SNMP Get support for the IP group. Implementation of the IP group is mandatory for all systems. The IP address table contains this entity's IP addressing information

MIB Object	Object ID: 1.3.6.1.2.1.4 +	Description
ipForwarding	.1	Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a badValue response if a management station attempts to change this object to an inappropriate value.
ipDefaultTTL	.2	Default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
ipInReceives	.3	Total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	.4	Number of input datagrams 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, and so on.
ipInAddrErrors	.5	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ...) and addresses of unsupported Classes (for example, Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams	.6	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
ipInUnknownProtos	.7	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	.8	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which

Standard SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.2.1.4 +	Description
		were discarded (e.g., for lack of buffer space). (Note that this counter does not include any datagrams discarded while awaiting re-assembly.)
ipInDelivers	.9	Total number of input datagrams successfully delivered to IP user-protocols including ICMP.
ipOutRequests	.10	Total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. (Note that this counter does not include any datagrams counted in ipForwDatagrams.)
ipOutDiscards	.11	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). (Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.)
ipOutNoRoutes	.12	Number of IP datagrams discarded because a route could not be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this "no-route" criterion. (This includes any datagrams which a host cannot route because all of its default gateways are down.)
ipReasmTimeout	.13	Maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
ipReasmReqds	.14	Number of IP fragments received which needed to be reassembled at this entity.
ipReasmOKs	.15	Number of IP datagrams successfully re-assembled.
ipReasmFails	.16	Number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). (Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.)
ipFragOKs	.17	Number of IP datagrams that have been successfully fragmented at this entity.
ipFragFails	.18	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set).
ipFragCreates	.19	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ipAddrTable	.20	The table of addressing information relevant to this entity's IPv4 addresses.

ipAddrTable Table

The table of addressing information relevant to this entity's IPv4 addresses.

MIB Object	Object ID: 1.3.6.1.2.1.4.20.1 +	Description
ipAdEntAddr	.1	IP address to which this entry's addressing information pertains.
ipAdEntIfIndex	.2	Index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
ipAdEntNetMask	.3	Subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to .
ipAdEntBcastAddr	.4	Value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value is 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
ipAdEntReasmMaxSize	.5	Size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

icmp Object

The following table describes the standard SNMP Get support for the Internet Control Message Protocol (ICMP) group. Implementation of the ICMP group is mandatory for all systems.

MIB Object	Object ID: 1.3.6.1.2.1.5 +	Description
icmpInMsgs	.1	Total number of ICMP messages which the entity received. (Note that this counter includes all those counted by icmpInErrors.)
icmpInErrors	.2	Number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
icmpInDestUnreachs	.3	Number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	.4	Number of ICMP Time Exceeded messages received.
icmpInParmProbs	.5	Number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	.6	Number of ICMP Source Quench messages received.
icmpInRedirects	.7	Number of ICMP Redirect messages received.
icmpInEchos	.8	Number of ICMP Echo (request) messages received.
icmpInEchoReps	.9	Number of ICMP Echo Reply messages received.

Standard SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.2.1.5 +	Description
icmpInTimestamps	.10	Number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	.11	Number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	.12	Number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	.13	Number of ICMP Address Mask Reply messages received.
icmpOutMsgs	.14	Total number of ICMP messages which this entity attempted to send. (This counter includes all those counted by icmpOutErrors.)
icmpOutErrors	.15	Number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
icmpOutDestUnreachs	.16	Number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	.17	Number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	.18	Number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	.19	Number of ICMP Source Quench messages sent.
icmpOutRedirects	.20	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos	.21	Number of ICMP Echo (request) messages sent.
icmpOutEchoReps	.22	Number of ICMP Echo Reply messages sent.
icmpOutTimestamps	.23	Number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	.24	Number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	.25	Number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	.26	Number of ICMP Address Mask Reply messages sent.

TCP Object

The following table describes the standard SNMP Get support for the TCP connection table, which contains information about this entity's existing TCP connections.

MIB Object	Object ID: 1.3.6.1.2.1.6 +	Description
tcpRtoAlgorithm	.1	Algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	.2	Minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	.3	Maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
tcpMaxConn	.4	Total number of TCP connections the entity supports. In entities where the maximum number of connections is dynamic, this object contains the value -1.
tcpActiveOpens	.5	Number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	.6	Number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	.7	Number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state.
tcpEstabResets	.8	Number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
tcpCurrEstab	.9	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
tcpInSegs	.10	Total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	.11	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	.12	Total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	.14	Total number of segments received in error (for example, bad TCP checksums).
tcpConnTable	.13	
tcpOutRsts	.15	Number of TCP segments sent containing the RST flag.

tcpConnTable Table

Per connection, tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.x Refer to the following table for all objects per connection.

MIB Object	Object ID: 1.3.6.1.2.1.6.13.1 +	Description
tcpConnState	.1	State of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a badValue response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, an RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).
tcpConnLocalAddress	.2	Local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value is 0.0.0.0.
tcpConnLocalPort	.3	Local port number for this TCP connection.
tcpConnRemAddress	.4	Remote IP address for this TCP connection.
tcpConnRemPort	.5	Remote port number for this TCP connection.

UDP Object

The following table describes the standard SNMP Get support for the UDP group. Implementation of the UDP group is mandatory for all systems which implement the UDP. The UDP listener table contains information about this entity's UDP end-points on which a local application is currently accepting datagrams.

MIB Object	Object ID: 1.3.6.1.2.1.7 +	Description
udpInDatagrams	.1	Total number of UDP datagrams delivered to UDP users.
udpNoPorts	.2	Total number of received UDP datagrams for which there was no application at the destination port.
udpInErrors	.3	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpOutDatagrams	.4	Total number of UDP datagrams sent from this entity.
udpTable.udpEntry	.5.x	The UDP Listener Table, per entry

UDP Listener Table

MIB Object	Object ID: 1.3.6.1.2.1.7.5 +	Description
udpLocalAddress	.1	Local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.
udpLocalPort	.2	Local port number for this UDP listener.

System Object

The following table describes the standard SNMP Get support for the system group which is a collection of objects common to all managed systems.

MIB Object	Object ID: 1.3.6.1.2.1.1 +	Description
sysDescr	.1	Textual description of the entity. This value includes the full name and version identification of the system's hardware type, software operating-system, and networking software.
sysObjectID	.2	Vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed. For example, if vendor Flintstones, Inc. was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its Fred Router.
sysUpTime	.3	Time (in hundredths of a second) since the network management portion of the system was last re-initialized.
sysContact	.4	Textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.
sysName	.5	Administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
sysLocation	.6	Physical location of this node (for example, telephone closet, 3rd floor). If the location is unknown, the value is the zero-length string.
sysServices	.7	Value which indicates the set of services that this entity may potentially offer. The value is a sum which initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, $2^{(L-1)}$ is added to the sum. For example, a node which performs only routing functions would have a value of 4 ($2^{(3-1)}$). In contrast, a node which is a host offering application services would have a value of 72 ($2^{(4-1)} + 2^{(7-1)}$). See the following table for how this value is calculated.
sysORLastChange	.8	Value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.

Standard SNMP GET Requests

layer	functionality
1	physical (for example, repeaters)
2	datalink/subnetwork (for example, bridges)
3	internet (for example, supports IP)
4	end-to-end (for example, supports TCP)
7	applications (for example., supports SMTP)

For systems including OSI protocols, layers 5 and 6 may also be counted.

Object Resource Information Object

The following table describes the standard SNMP Get support for the object resource information which is a collection of objects which describe the SNMPv2 entity's (statistically and dynamically configurable) support of various MIB modules.

MIB Object	Object ID: 1.3.6.1.2.1.1.9 +	Description
sysORID	.2	Authoritative identification of a capabilities statement with respect to various MIB modules supported by the local SNMPv2 entity acting in an agent role
sysORDescr	.3	Textual description of the capabilities identified by the corresponding instance of sysORID.
sysORUpTime	.4	Value of sysUpTime at the time this conceptual row was last instantiated.

SNMP Object

The following table describes the standard SNMP Get support for the SNMP group which is a collection of objects providing basic instrumentation and control of an SNMP entity.

MIB Object	Object ID: 1.3.6.1.2.1.11 +	Description
snmpInPkts	.1	Total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	.3	Total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	.4	Total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
snmpInBadCommunityUses	.5	Total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
snmpInASNParseErrs	.6	Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.

MIB Object	Object ID: 1.3.6.1.2.1.11 +	Description
snmpEnableAuthenTraps	.30	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. (It is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system.)
snmpSilentDrops	.31	Total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
snmpProxyDrops	.32	Total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a timeout) such that no Response-PDU could be returned.

Physical Entity Table

Oracle USM implements the Physical Entity table from the Entity MIB (RFC 2737). The following table describes the standard SNMP Get support for the Entity group, which is a collection of multiple logical entities supported by a single SNMP agent.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
entPhysicalIndex	.1	The index for this entry.
entPhysicalDescr	.2	Textual description of the physical entity. A string that identifies the manufacturer's name; which should be set to a distinct value for each version or model of the physical entity.
entPhysicalVendorType	.3	Indication of the vendor-specific hardware type of the physical entity. (This is different from the definition of MIB-II's sysObjectID). An agent should set this object to an enterprise-specific registration identifier value indicating the specific equipment type in detail. The associated instance of entPhysicalClass is used to indicate the general type of hardware device. If no vendor-specific registration identifier exists for this physical entity,

Standard SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
		or the value is unknown by this agent, then the value { 0 0 } is returned.
entPhysicalContainedIn	.4	Value of entPhysicalIndex for the physical entity which contains this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. The set of containment relationships define a strict hierarchy; that is, recursion is not allowed. In the event a physical entity is contained by more than one physical entity (for example, double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.
entPhysicalClass	.5	Indication of the general hardware type of the physical entity. An agent should set this object to the standard enumeration value that most accurately indicates the general class of the physical entity, or the primary class if there is more than one. If no appropriate standard registration identifier exists for this physical entity, then the value other(1) is returned. If the value is unknown by this agent, then the value unknown(2) is returned
entPhysicalParentRelPos	.6	<p>An indication of the relative position of this child component among all its sibling components. Sibling components are defined as entPhysicalEntries that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects. An NMS can use this object to identify the relative ordering for all sibling components of a particular parent (identified by the entPhysicalContainedIn instance in each sibling entry).</p> <p>This value should match any external labeling of the physical component if possible. For example, for a container (such as card slot) labeled as slot #3, entPhysicalParentRelPos should have the value 3. The entPhysicalEntry for the module plugged in slot 3 should have an entPhysicalParentRelPos value of 1.</p> <p>If the physical position of this component does not match any external numbering or clearly visible ordering, use external reference material to determine the parent-relative position. If this is not possible, the agent should assign a consistent (but possibly arbitrary) ordering to a given set of sibling components, perhaps based on internal representation of the components.</p> <p>If the agent cannot determine the parent-relative position for some reason, or if the associated value</p>

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
		<p>of entPhysicalContainedIn is 0, then the value -1 is returned. Otherwise a non-negative integer is returned, indicating the parent-relative position of this physical entity. Parent-relative ordering normally starts from 1 and continues to N, where N represents the highest positioned child entity. However, if the physical entities (for example, slots) are labeled from a starting position of zero, the first sibling should be associated with a entPhysicalParentRelPos value of 0.</p> <p>This ordering might be sparse or dense, depending on agent implementation. The actual values returned are not globally meaningful, as each parent component may use different numbering algorithms. The ordering is only meaningful among siblings of the same parent component. The agent should retain parent-relative position values across reboots, either through algorithmic assignment or use of non-volatile storage</p>
entPhysicalName	.7	<p>Textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's console. This might be a text name, such as console or a simple component number (for example, port or module number), such as 1, depending on the physical component naming syntax of the device. If there is no local name, or this object is otherwise not applicable, this object contains a zero-length string. The value of entPhysicalName for two physical entities will be the same in the event that the console interface does not distinguish between them, for example, slot-1 and the card in slot-1.</p>
entPhysicalHardwareRev	.8	<p>Vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier actually printed on the component itself (if present). If revision information is stored internally in a non-printable (for example, binary) format, the agent must convert such information to a printable format, in an implementation-specific manner. If no specific hardware revision string is associated with the physical component, or this information is unknown to the agent, this object contains a zero-length string.</p>
entPhysicalFirmwareRev	.9	<p>Vendor-specific firmware revision string for the physical entity. If revision information is stored internally in a non-printable (for example, binary) format, the agent must convert such information to a printable format, in an implementation-specific</p>

Standard SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
		manner. If no specific firmware programs are associated with the physical component, or this information is unknown to the agent, this object contains a zero-length string.
entPhysicalSoftwareRev	.10	Vendor-specific software revision string for the physical entity. If revision information is stored internally in a non-printable (for example, binary) format, the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software programs are associated with the physical component, or this information is unknown to the agent, this object contains a zero-length string.
entPhysicalSerialNum	.11	<p>Vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present). On the first instantiation of an physical entity, the value of entPhysicalSerialNum associated with that entity is set to the correct vendor-assigned serial number, if this information is available to the agent. If a serial number is unknown or non-existent, the entPhysicalSerialNum will be set to a zero-length string instead.</p> <p>Implementations which can correctly identify the serial numbers of all installed physical entities do not need to provide write access to the entPhysicalSerialNum object.) Agents which cannot provide non-volatile storage for the entPhysicalSerialNum strings are not required to implement write access for this object.</p> <p>Not every physical component will have, or need, a serial number. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to false(2) do not need their own unique serial number. An agent does not have to provide write access for such entities, and might return a zero-length string.</p> <p>If write access is implemented for an instance of entPhysicalSerialNum, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalSerialNum instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re- initializations/reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value.</p>

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
entPhysicalMfgName	.12	<p>Name of the manufacturer of this physical component. The preferred value is the manufacturer name string actually printed on the component itself (if present). (Note that comparisons between instances of the entPhysicalModelName, entPhysicalFirmwareRev, entPhysicalSoftwareRev, and the entPhysicalSerialNum objects, are only meaningful amongst entPhysicalEntries with the same value of entPhysicalMfgName.) If the manufacturer name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</p>
entPhysicalModeName	.13	<p>Vendor-specific model name identifier string associated with this physical component. The preferred value is the customer-visible part number, which may be printed on the component itself. If the model name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.</p>
entPhysicalAlias	.14	<p>Alias name for the physical entity as specified by a network manager, it provides a non-volatile handle for the physical entity.</p> <p>On the first instantiation of an physical entity, the value of entPhysicalAlias associated with that entity is set to the zero-length string. However, an agent might set the value to a locally unique default value, instead of a zero-length string.</p> <p>If write access is implemented for an instance of entPhysicalAlias, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAlias instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re- initializations/reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value.</p>
entPhysicalAssetID	.15	<p>User-assigned asset tracking identifier for the physical entity as specified by a network manager, which provides non-volatile storage of this information. On the first instantiation of an physical entity, the value of entPhysicalAssetID associated with that entity is set to the zero-length string.</p> <p>Not every physical component will have a asset tracking identifier, or even need one. Physical entities for which the associated value of the</p>

Standard SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
		<p>entPhysicalIsFRU object is equal to false(2), do not need their own unique asset tracking identifier.</p> <p>An agent does not have to provide write access for such entities, and might instead return a zero-length string. If write access is implemented for an instance of entPhysicalAssetID, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAssetID instance associated with the same physical entity for as long as that entity remains instantiated. This includes instantiations across all re- initializations/reboots of the network management system, including those which result in a change of the physical entity's entPhysicalIndex value. If no asset tracking information is associated with the physical component, then this object will contain a zero-length string</p>
entPhysicalIsFRU	.16	<p>Whether this physical entity is considered a field replaceable unit by the vendor.</p> <ul style="list-style-type: none"> • true(1) means this is a field replaceable unit. • false(2) means this is not a replaceable unit

Enterprise SNMP GET Requests

This section explains the proprietary enterprise SNMP GET requests supported by the system. The SNMP GET is used to query for information on or about a network entity.

Applications MIB (ap-apps.mib)

The Apps mib (ap-apps.mib) contains tables related ENUM and DNS statistics and states.

apAppsENUMServerStatusTable Table

The following table all configured ENUM servers' status.

MIB Object	Object ID 1.3.6.1.4.1.914 8.3.16.1.2.1.1 +	Description
apAppsENUMServerStatusEntry	.1	Numbered table entry.
apAppsENUMConfigName	.1.1	The name of the enum-config element that contains this ENUM server.
apAppsENUMServerInetAddressType	.1.2	The internet address type of this ENUM server.
apAppsENUMServerInetAddress	.1.3	The IP address of this ENUM server.
apAppsENUMServerStatus	.1.4	The status of this ENUM server.

apAppsDnsServerStatusTable

The following table all configured ENUM servers' status.

Enterprise SNMP GET Requests

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.2.1 +	Description
apAppsDnsServerInterfaceName	.1	The name of the dns interface that contains this dns server.
apAppsDnsServerInetAddressType	.1.2	The internet address type of this DNS server.
apAppsDnsServerInetAddress	.1.3	The IP address of this DNS server.
apAppsDnsServerStatus	.1.4	The status of this DNS server.

Codec and Transcoding MIB (ap-codec.mib)

The following table describes the SNMP GET query names for the Codec and Transcoding MIB (ap-codec.mib).

apCodecMIBObjects

The apCodecMIBObjects object has the OID 1.3.6.1.4.1.9148.3.7.1. The apCodecRealmStatsTable object has the OID 1.3.6.1.4.1.9148.3.7.1.1. The apCodecRealmStatsEntry object has the OID 1.3.6.1.4.1.9148.3.7.1.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.1.1.1 +	Description
apCodecRealmCountOther	.1	Count of the SDP media streams received in the realm which negotiated to a codec not defined in this table.
apCodecRealmCountPCMU	.2	Count of SDP media streams received in the realm which negotiated to the PCMU codec.
apCodecRealmCountPCMA	.3	Count of SDP media streams received in the realm which negotiated to the PCMA codec.
apCodecRealmCountG722	.4	Count of SDP media streams received in the realm which negotiated to the G722 codec.
apCodecRealmCountG723	.5	Count of SDP media streams received in the realm which negotiated to the G723 codec.
apCodecRealmCountG726-16	.6	Count of SDP media streams received in the realm which negotiated to the G726-16 codec.
apCodecRealmCountG726-24	.7	Count of SDP media streams received in the realm which negotiated to the G726-24 codec.
apCodecRealmCountG726-32	.8	Count of SDP media streams received in the realm which negotiated to the G726-32 codec.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.1.1.1 +	Description
apCodecRealmCountG726-40	.9	Count of SDP media streams received in the realm which negotiated to the G726-40 codec.
apCodecRealmCountG728	.10	Count of SDP media streams received in the realm which negotiated to the G728 codec.
apCodecRealmCountG729	.11	Count of SDP media streams received in the realm which negotiated to the G729 codec.
apCodecRealmCountGSM	.12	Count of SDP media streams received in the realm which negotiated to the GSM codec.
apCodecRealmCountILBC	.13	Count of SDP media streams received in the realm which negotiated to the iLBC codec.
apCodecRealmCountAMR	.14	Count of SDP media streams received in the realm which negotiated to the AMR codec.
apCodecRealmCountEVRC	.15	Count of SDP media streams received in the realm which negotiated to the EVRC codec.
apCodecRealmCountH261	.16	Count of SDP media streams received in the realm which negotiated to the H261 codec.
apCodecRealmCountH263	.17	Count of SDP media streams received in the realm which negotiated to the H.263 codec.
apCodecRealmCountT38	.18	Count of SDP media streams received in the realm which negotiated to the T.38 codec.
apCodecRealmCountAMRWB	.19	Count of SDP media streams received in the realm which negotiated to the AMR-WB codec.
apCodecRealmCountEVRC0	.20	Count of SDP media streams received in the realm which negotiated to the EVRC0 codec.
apCodecRealmCountEVRC1	.21	Count of SDP media streams received in the realm which negotiated to the EVRC1 codec.
apCodecRealmCountEVRCB	.22	Count of SDP media streams received in the realm which negotiated to the EVRCB codec.
apCodecRealmCountEVRCB0	.23	Count of SDP media streams received in the realm which negotiated to the EVRCB0 codec.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.1.1.1 +	Description
apCodecRealmCountEVRCB1	.24	Count of SDP media streams received in the realm which negotiated to the EVRCB1 codec.
apCodecRealmCountOpus	.25	Count of SDP media streams received in the realm which negotiated to the Opus codec.
apCodecRealmCountSILK	.26	Count of SDP media streams received in the realm which negotiated to the SILK codec.
apCodecRealmCountT140	.27	Count of SDP media streams received in the realm which negotiated to the T.140 codec.
apCodecRealmCountBAUDOT	.28	Count of SDP media streams received in the realm which negotiated to the BAUDOT codec.
apCodecRealmCountH264	.29	Count of SDP media streams received in the realm which negotiated to the H.264 codec.

apTranscodingMIBObjects

The apTranscodingMIBObjects object has the OID 1.3.6.1.4.1.9148.3.7.2. The apCodecTranscodingRealmStatsTable object has the OID 1.3.6.1.4.1.9148.3.7.2.1. The apTranscodingRealmStatsEntry object has the OID 1.3.6.1.4.1.9148.3.7.2.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.2.1.1 +	Description
apCodecRealmSessionsTransparent	.1	Number of sessions in the realm that did not use any DSP resources for transcoding or transrating.
apCodecRealmSessionsTransrated	.2	Number of sessions in the realm that had a common codec but used DSP resources to modify packetization rate.
apCodecRealmSessionsTranscoded	.3	Number of sessions in the realm that had used DSP resources to transcode between codecs.

apCodecTranscodingResourceMIBObjects

The apCodecTranscodingResourceMIBObjects object has the OID 1.3.6.1.4.1.9148.3.7.2.2. It contains 5 OIDS that return overall system transcoding counts and statistics.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.2.2 +	Description
apCodecTranscodingResourcesTotal	.1	Total number of transcoding sessions available on the system.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.2.2 +	Description
apCodecTranscodingResourcesCurrent	.2	Number of transcoding sessions currently in-use.
apCodecTranscodingResourcesHigh	.3	Highest number of transcoding sessions simultaneously in-use since system reboot or manual statistic reset.
apCodecTranscodingInUsePercentageCurrent	.4	Transcoding sessions currently in-use as a percentage of total available sessions.
apCodecTranscodingInUsePercentageHigh	.5	Transcoding sessions simultaneously in-use since system reboot or manual statistic reset expressed as a percentage of total available sessions.

apCodecPairStatsTable

This table, found in the ap-codec.mib, provides a listing of all unique codec pairs currently being transcoding and the session count of that pair currently in use. It conveys the same information displayed in the **show xcode codecs** command. Use the apCodecTable for correlation between Codec name (apCodecName) and Codec index (apCodecIndex) to define apCodecPairAIndex and apCodecPairBIndex. When Ptimes for call legs in the codec pair differ, they will be included as additional indices. When digit translation is active on the call and digit translation types differ across call legs, indication of which call leg uses which digit translation type is output as well. Use the ApCodecDigitTypes object for digit type value correlation.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.7.2.4 +	Description
apCodecPairStatsEntry	.1	Entry of this table. Note that the end point A is the one with smaller or equal apCodecIndex.
apCodecPairAIndex	.1.1	The index of the first codec in the pair
apCodecPairBIndex	.1.2	The index of the second codec in the pair
apCodecPairAPValue	.1.3	The p value in the end point A. A value of zero indicates the value is not provided.
apCodecPairBPValue	.1.4	The p value in the end point B. A value of zero indicates the value is not provided.
apCodecPairADigitType	.1.5	The digit type index in the end point A.
apCodecPairBDigitType	.1.6	The digit type index in the end point B.

Enterprise SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.7.2.4 +	Description
apCodecPairTranscodingCurrent	.1.7	The current number of transcoding sessions for this codec-pair since system reboot or manual statistic reset.
apCodecPairTranscodingHigh	.1.8	The highest number of transcoding sessions in use for this codec-pair since system reboot or manual statistic reset.

Transcoding Capacity in System Management MIB (ap-smgmt.mib)

The following VARBINDs are used in Transcoding related traps. They may not be polled and retrieved using an SNMP GET.

The apSysMgmtMIBObjects object has the OID 1.3.6.1.4.1.9148.3.2.1. The apSysMgmtGeneralObjects object has the OID 1.3.6.1.4.1.9148.3.2.1.1.

SNMP Object Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
apSysXCodeCapacity	.34	Percentage of transcoding utilization.
apSysXCodeAMRCapacity	.35	Percentage of licensed AMR transcoding sessions.
apSysXCodeAMRWBCapacity	.36	Percentage of licensed AMR-WB transcoding sessions.
apSysXCodeEVRCCapacity	.39	Percentage of licensed EVRC transcoding sessions.
apSysXCodeEVRBCapacity	.40	Percentage of licensed EVRCB transcoding sessions.
apSysAcpTlsEnabled	.41	A value of TRUE indicates ACP over TLS connection is supported and enabled. A FALSE value indicates ACP over TLS connection is not enabled
apSysXCodeG729Capacity	.42	The percentage of licensed G729 transcoding utilization
apSysXCodeOpusCapacity	.46	The percentage of licensed Opus transcoding utilization (non pollable).
apSysXCodeSILKCapacity	.47	The percentage of licensed SILK transcoding utilization (non pollable).

Diameter MIB (ap-diameter.mib)

The Diameter MIB (ap-diameter.mib) contains one table (apDiamClfErrorStatsTable: 1.3.6.1.4.1.9148.3.13.1.1.2.1) and 6 traps. There are numerous objects that are included within the traps, and these objects are not accessible from outside of the traps

The apDiamClfErrorStatsTable lists Diameter Clf error status.

Table 2: apDiamClfErrorStatsTable

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.13.1.1.2.1 +	Description
apDiamClfErrorStatsEntry	.1	
apDiamClfExtPolSvrIndex	.1.1	An integer for the sole purpose of indexing the external policy servers.
apDiamClfExtPolSvrName	.1.2	External policy server name
apDiamClfErrorsRecent	.1.3	Number of diameter errors in recent period received on e2 interface with the CLF.
apDiamClfErrorsTotal	.1.4	Total number of diameter errors in life time received on e2 interface with the CLF.
apDiamClfErrorsPerMax	.1.5	PerMax count of diameter errors in life time received on e2 interface with the CLF.

The following objects in the ap-diameter MIB are only available in the trap notifications:

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.13.1.1.2.1 +	Description
apDiamAcctSvrHostName	.1	The Diameter Accounting Server host name.
apDiamAcctSvrIPPort	.2	The Diameter Accounting Server IP address and port number: XX.XX.XX.XX:P
apDiamAcctSvrOriginRealm	.3	The Diameter Accounting Server Origin Realm.
apDiamAcctSvrOriginHost	.4	The Diameter Accounting Server Origin Host.
apDiamAcctSvrTransportType	.5	The Diameter Accounting Server Transport Type.
apAcctMsgQueueAvailCurrent	.6	The current measured percentage value of space available

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.13.1.2.1 +	Description
apAcctMsgQueueMinorThreshold	.7	The current configured minor threshold value.
apAcctMsgQueueMajorThreshold	.8	The current configured major threshold value.
apAcctMsgQueueCriticalThreshold	.9	The current configured critical threshold value.
apDiameterResultCode	10	The Result-Code AVP (268) value RFC 3588, 7.1. Result-Code AVP

DNS ALG MIB (ap-dnsalg.mib)

The DNS ALG mib (ap-dnsalg.mib) contains tables related to capturing dns-alg constraints and other statistics.

apDNSALGServerStatusTable

This table, found in the ap-dnsalg.mib, provides a listing of DNS ALG status of a the DNS ALG server. It conveys the same information displayed in the **show dnsalg status** command. This table is indexed by the DNS ALG server

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.14.1.2.1 +	Description
apDNSALGServerStatusEntry	.1	An entry designed to hold the status of a single DNSALG server.
apDNSALGConfigIndex	.1.1	An integer for the sole purpose of indexing the DNS-ALG configuration. Only one DNS-ALG configuration is allowed per a realm.
apDNSALGServerIndex	.1.2	An integer for the sole purpose of indexing the Dns Server Attributes in a DNS-ALG config. Each DNS-ALG configuration can have multiple Dns Server Attributes.
apDNSALGConfigName	.1.4	The name of the dns-alg config element that contains this DNS-ALG server.
apDNSALGServerRealm	.1.5	The name of the server realm element that contains this DNS-ALG server.
apDNSALGDomainSuffix	.1.6	The name of the domain suffix element that contains this DNS-ALG server.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.14.1.2.1 +	Description
apDNSALGServerIpAddress	.1.7	The IP address of this DNS-ALG server.
apDNSALGServerStatus	.1.8	The status of this DNS-ALG server. <ul style="list-style-type: none"> • 0 - in service • 1 - lower priority • 2 - out of service, unreachable.

apDNSALGStatsTable

This table, found in the ap-dnsalg.mib, provides a listing of DNS ALG statistics and counts for a specific realm. It conveys the same information displayed in the **show dnsalg stats** command. This table is indexed by the DNS ALG realm.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.14.1.2.2 +	Description
apDnsALGStatsEntry	.1	Entry of this table.
apDnsAlgClientRealmIndex	.1.1	Index of this table.
apDnsAlgClientRealmName	.1.2	The name of the realm that contains this DNS-ALG server.
apDnsAlgCurrentQueries	.1.3	Total number of lifetime queries received on the DNS-ALG server in the given realm.
apDnsAlgTotalQueries	.1.4	Total number of lifetime queries received on the DNS-ALG server in the given realm.
apDnsAlgCurrentSuccess	.1.5	Number of success responses in a recent period received on the DNS-ALG server in the given realm.
apDnsAlgTotalSuccess	.1.6	Total number of lifetime success responses received on the DNS-ALG server in the given realm.
apDnsAlgCurrentNotFound	.1.7	Number of not-found responses in a recent period received on the DNS-ALG server in the given realm.
apDnsAlgTotalNotFound	.1.8	Total number of lifetime not-found responses in received on the DNS-ALG server in the given realm.
apDnsAlgCurrentTimeOut	.1.9	Number of time-out responses in a recent period received on the

Enterprise SNMP GET Requests

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.14.1.2.2 +	Description
		DNS-ALG server in the given realm.
apDnsAlgTotalTimeOut	.1.10	Total number of time-out responses in a life time received on the DNS-ALG server in the given realm.
apDnsAlgCurrentBadStatus	.1.11	Number of bad status responses in a recent period received on the DNS-ALG server in the given realm.
apDnsAlgTotalBadStatus	.1.12	Total number of bad status responses in a lifetime received on the DNS-ALG server in the given realm.
apDnsAlgCurrentOtherFailures	.1.13	Number of other failure responses in a recent period received on the DNS-ALG server in the given realm.
apDnsAlgTotalOtherFailures	.1.14	Total number of other failure responses in a lifetime received on the DNS-ALG server in the given realm.
apDnsAlgAvgLatency	.1.15	Average observed one-way signalling latency during the period in milliseconds.
apDnsAlgMaxLatency	.1.16	Maximum observed one-way signalling latency during the period in milliseconds.
apDnsAlgMaxBurstRate	.1.17	Maximum burst rate of traffic measured during the period (combined inbound and outbound).

Environment Monitor MIB (ap-env-monitor.mib)

The following table describes the SNMP GET query names for the Environment Monitor MIB (ap-env-monitor.mib).

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1 +	Description
apEnvMonI2CState	.1	State of the environmental monitor located in the chassis. Values are: initial (1): environment is at the initial state normal (2): environment is good; for example at low temperature

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1 +	Description
		<p>minor (3): environment is not good; for example fans speed is more than minor alarm threshold but less than major alarm threshold</p> <p>major (4): environment is bad; for example an speed is more than major alarm threshold, but less than critical alarm threshold</p> <p>critical (5): environment is very bad; for example fan speed is more than critical alarm threshold</p> <p>shutdown (6): environment is at its worst, the system should be shutdown immediately</p> <p>notPresent (7): environmental monitor is not present</p> <p>notFunctioning (8): environmental monitor does not function properly; for example, IC2 failure or temperature sensor generates abnormal data</p> <p>unknown (9): no information available because of internal error</p>

The apEnvMonVoltageStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.2.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.2.1.1 +	Description
apEnvMonVoltageStatusType	.2	<p>Entity part type from which the voltage value is from:</p> <p>v2p5- 2.5v sensor: L3 cache core voltage; micro-processor and co-processor I/O voltage; Field-Programmable Gate Array (FPGA) memories I/O voltage.</p> <p>v3p3 - 3.3V sensor: general TTL supply rail; control logic; micro-processor; micro-processor and co-processor; SDRAM</p> <p>v5 - 5V sensor: fans; micro-processor core voltage regulator</p> <p>CPU sensor: CPU voltage; micro-processor core voltage</p>
apEnvMonVoltageStatusDescr	.3	Textual description of the entity being monitored for voltage.
apEnvMonVoltageStatusValue	.4	Current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value.
apEnvMonVoltageState	.5	Current state of the voltage for the device being monitored. Possible values are:

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.2.1.1 +	Description
		<p>Host Processor 7455</p> <p>normal range: 1.55v to 1.65v</p> <p>minor range: 1.4v to 1.55v or 1.65v to 1.8v</p> <p>shutdown range: <1.4v or >1.8v</p> <p>Host Processor 7457</p> <p>Version 1.0</p> <p>normal range: 1.35v to 1.45v</p> <p>minor range: 1.00v to 1.35v or 1.45v to 1.6v</p> <p>shutdown range: <1.0v or >1.6v</p> <p>Version 1.1 and later</p> <p>normal range: 1.25v to 1.35v</p> <p>minor range: 1.00v to 1.25v or 1.35v to 1.6v</p> <p>shutdown range: <1.0v or >1.6v</p>
apEnvMonVoltageSlotID	.6	Slot for this voltage.
apEnvMonSlotType	.7	Type of module found in this slot.

The apEnvMonTemperatureStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.3.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.3.1.1 +	Description
apEnvMonTemperatureStatusType	.2	<p>Indicates the entity being monitored for temperature. Values are:</p> <p>ds1624sMain (1)</p> <p>ds1624sCPU (2)</p> <p>lm84 (3)</p> <p>lm75 (4)</p> <p>lm75Main (5)</p> <p>lm75Cpu (6)</p> <p>lm75Phy (7)</p>
apEnvMonTemperatureStatusDescr	.3	Description of the temperature being monitored. It has the value of the Main Board PROM Temperature (in Celsius).
apEnvMonTemperatureStatusValue	.4	The current temperature of the main board PROM in Celsius.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.3.1.1 +	Description
apEnvMonTemperatureState	.5	<p>Current state of the temperature which can have one of the following values:</p> <p>3800:</p> <p>1: initial. Temperature is at its initial state.</p> <p>2: normal. The temperature is normal.</p> <p>3: minor alarm - the temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius.</p> <p>4: major alarm. The temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius.</p> <p>5: critical alarm. The temperature is greater than 73 degrees Celsius.</p> <p>6: shutdown. The system should be shutdown immediately</p> <p>7: not present: The temperature sensor does not exist.</p> <p>8: not functioning: The temperature sensor is not functioning properly.</p> <p>9: unknown. Cannot obtain information due to an internal error.</p> <p>4500:</p> <p>1: initial. Temperature is at its initial state.</p> <p>2: normal. The temperature is normal.</p> <p>3: minor alarm - the temperature is greater than or equal to 95 degrees Celsius and less than 100 degrees Celsius.</p> <p>4: major alarm. The temperature is greater than or equal to 100 degrees Celsius and less than 105 degrees Celsius.</p> <p>5: critical alarm. The temperature is greater than or equal to 105 degrees Celsius.</p> <p>6: shutdown. The system should be shutdown immediately</p> <p>7: not present: The temperature sensor does not exist.</p>

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.3.1.1 +	Description
		8: not functioning: The temperature sensor is not functioning properly. 9: unknown. Cannot obtain information due to an internal error.
apEnvMonTemperatureSlotID	.6	Slot for which this temperature is found.
apEnvMonTemperatureSlotType	.7	Type of module found in this slot.

The apEnvMonFanStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.4.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.4.1.1 +	Description
apEnvMonFanStatusType	.2	Location of the fan, which can have one of the following values: 11: fan1 12: fan2 13: fan3 14: fan4
apEnvMonFanStatusDescr	.3	Textual description of the fan.
apEnvMonFanStatusValue	.4	Current measurement of fan speed in percentage.
apEnvMonFanState	.5	Current state of the fan speed which can have one of the following values: 1: initial. The temperature is at its initial state. 2: normal. The fan speed is normal. 3: minor. The fan speed is between 75% and 90% of the full fan speed 4: major. The fan speed is between 50% and 75% of the full fan speed 5: critical. The fan speed is less than 50% of the full fan speed. 6: shutdown. The system should be shutdown immediately 7: not present. The fan sensor does not exist. 8: not functioning. The fan sensor is not functioning properly. 9: unknown. Cannot obtain information due to an internal error.
apEnvMonFanState	.6	Current state of the fan being monitored.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.4.1.1 +	Description
apEnvMonFanSlotID	.7	Slot where this fan is found. A zero is returned if this fan is not the type slot.

The apEnvMonPowerSupplyStatusEntr object has the OID 1.3.6.1.4.1.9148.3.3.1.5.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.5.1.1 +	Description
apEnvMonPowerSupplyStatusType	.2	Location of the power supply, which can have one of the following values: 0: left power supply B 1: right power supply A 3: slot
apEnvMonPowerSupplyStatusDescr	.3	Textual description of the power supply.
apEnvMonPowerSupplyState	.4	Current state of the power supply. Values: 2: normal. The power supply is normal. 7: not present: The power supply sensor does not exist.

The apEnvPhyCardStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.6.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.6.1.1 +	Description
apEnvMonPhyCardStatusDescr	.3	Textual description of the phy card.
apEnvMonPhyCardState	.4	The current state of the phy card. Values: 2: normal 7: not present

H.323 MIB (ap-h323.mib)

The following table describes the SNMP GET query names for the H.323 MIB (ap-h323.mib).

The apH323MIBObjects object has the OID 1.3.6.1.4.1.9148.3.10.1, the apH323StackTable object has the OID 1.3.6.1.4.1.9148.3.10.1.1, and the apH323StackEntry object has the OID 1.3.6.1.4.1.9148.3.10.1.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.10.1.1.1 +	Description
apH323StackName	.1	Configured H.323 stack name.
apH323StackCurrentCalls	.2	Number of current calls.

License MIB (ap-license.mib)

The following table describes the SNMP GET query names for the License MIB (ap-license.mib). The apLicenseEntry object has the OID 1.3.6.1.4.1.9148.3.5.1.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.5.1.1.1 +	Description
apLicenseKey	.2	Key, not applicable to the first index, which represents the consolidated license. Displays N/A.
apLicenseCapacity	.3	Maximum number of simultaneous sessions allowed by a system for all combined protocols.
apInstallDate	.4	Installation time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
apLicenseBeginDate	.5	Installation time and date in the following format: hh:mm:ss month day year. Displays N/A if a license is not enabled.
apLicenseExpireDate	.6	Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
apLicenseSIPFeature	.7	Value that indicates whether a Session Initiation Protocol (SIP) license is present. A value of 1 indicates that SIP licensing is enabled. A value of 2 indicates that SIP licensing is not enabled.
apLicenseMGCPFeature	.8	Not Supported.
apLicenseH323Feature	.9	Value that indicates whether a H.323 Protocol license is present. A value of 1 indicates that H.323 licensing is enabled. A value of 2 indicates that H.323 licensing is not enabled.
apLicenseIWFFeature	.10	Value that indicates whether a Interworking Feature (IWF) license is present. A value of 1 indicates that IWF licensing is enabled. A value of 2 indicates that IWF licensing is not enabled.
apLicenseQoSFeature	.11	Value that indicates whether a Quality of Service (QoS) license is present. A value of 1 indicates that QoS licensing is enabled. A value of 2 indicates that QoS licensing is not enabled.
apLicenseACPFfeature	.12	Value that indicates whether a Acme Control Protocol (ACP) license is present. A value of 1 indicates that ACP licensing is enabled. A value of 2 indicates that ACP licensing is not enabled.
apLicenseLPFeature	.13	Value that indicates whether a Local Policy (LP) license is present. A value of 1 indicates that LP licensing is enabled. A value of 2 indicates that LP licensing is not enabled.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.5.1.1.1 +	Description
apLicenseSAGFeature	.14	Value that indicates whether a Session Agent Group (SAG) license is present. A value of 1 indicates that SAG licensing is enabled. A value of 2 indicates that SAG licensing is not enabled. (load balancing feature)
apLicenseACCTFeature	.15	Value that indicates whether a ACCT license is present. An ACCT license allows the system to create connections and send CDRs to one or more RADIUS servers. A value of 1 indicates that ACCT licensing is enabled. A value of 2 indicates that ACCT licensing is not enabled.
apLicenseHAFeature	.16	Value that indicates whether a High Availability (HA) license is present. A value of 1 indicates that HA licensing is enabled. A value of 2 indicates that HA licensing is not enabled.
apLicensePACFeature	.17	Value that indicates whether a PAC license is present. A value of 1 indicates that PAC licensing is enabled. A value of 2 indicates that PAC licensing is not enabled.

Security MIB (ap-security.mib)

The following table describes the SNMP Get query names for the Security MIB (ap-security.mib).

The apSecurityMIBObjects object has the OID 1.3.6.1.4.1.9148.3.9.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.9.1 +	Description
apSecurityOCSRIPAddress	.5	OCSR server IP Address
apSecurityOCSRHostname	.6	OCSR server hostname

The apSecurityTacacsTable object has the OID 1.3.6.1.4.1.9148.3.9.1.4, and the apSecurityTacacsEntry object has the 1.3.6.1.4.1.9148.3.9.1.4.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.9.1.4.1+	Description
apSecurityTacacsCliCommands	.3	Number of CLI commands sent for TACACS+ accounting
apSecurityTacacsSuccessAuthentication	.4	Number of successful TACACS+ authentication requests
apSecurityTacacsFailureAuthentication	.5	Number of failed TACACS+ authentication requests
apSecurityTacacsSuccessAuthorization	.6	Number of successful TACACS+ authorization requests
apSecurityTacacsFailureAuthorization	.7	Number of failed TACACS+ authorization requests

apSecurityCertificateTable

This table, found in the ap-security.mib, provides information about installed security certificates and their expiration. It conveys the same information displayed in the **show security certificates** command.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.9.1.10 +	Description
apSecurityCertificateEntry	.1	The certificate entry.
apSecurityCertificateConfigId	.1.1	The internal configuration ID of the certificate.
apSecurityCertificateIndex	.1.2	The internal index of the certificate. Combined with configuration ID is the unique ID of a certificate.
apSecurityCertificateRecordName	.1.3	The SBC's configuration record name for the certificate.
apSecurityCertificateCertSubject	.1.4	The security certificate subject.
apSecurityCertificateCertStart	.1.5	The start time and date of the security certificate.
apSecurityCertificateCertExpire	.1.6	The expiration time and date of the security certificate.
apSecurityCertificateCertIssuer	.1.7	The issuer of the security certificate.
apSecurityCertificateCertIsCA	.1.8	Boolean value indicating if the certificate is a CA certificate.

SIP MIB (ap-sip.mib)

The following table describes the SNMP Get query names for the SIP MIB (ap-sip.mib).

The apSipMIBGeneralObjects object has the OID 1.3.6.1.4.1.9148.3.15.1.1.1.


SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.1 +	Description
apSipSecInterfaceTotalRegistrations	.1.0	Total number of registrations on all secondary SIP interfaces.
apSipSecInterfaceRegThreshold	.2.0	The maximum threshold for registrations on all secondary SIP interfaces. If this threshold is exceeded, an alarm is raised.
apSipSecInterfaceClearThreshold	.3.0	The threshold for registrations on all secondary SIP interfaces to clear an alarm.

Object group in ap-sip.mib	apSipSecInterfaceRegObjectsGroup Includes:	Object group to monitor registrations for secondary SIP interfaces.
----------------------------	---	---

	apSipSecInterfaceTotalRegistrations apSipSecInterfaceRegThreshold apSipSecInterfaceClearThreshold (apSipObjectGroups 1)	
Object in ap-sip.mib	apSipSecInterfaceTotalRegistrations (apSipSecInterfaceObjects 1)	Total number of registration on all secondary SIP interfaces.
Object in ap-sip.mib	apSipSecInterfaceRegThreshold (apSipSecInterfaceObjects 2)	The max threshold for registrations on all secondary interfaces beyond which a trap is generated.
Object in ap-sip.mib	apSipSecInterfaceClearThreshold (apSipSecInterfaceObjects 3)	The threshold for registrations on all secondary SIP interfaces below which a clear trap is generated.

syslog MIB (ap-slog.mib)


The following table describes the SNMP GET query names for the syslog MIB (ap-slog.mib).

 **Note:** Form the Object Identifier (OID) Number by concatenating the OID of apSyslogBasic (1.3.6.1.4.1.9148.3.1.1.1) with the OID termination number.


SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.1.1.1 +	Description
apSyslogNotificationsSent	.1	Number of apSyslogMessageGenerated notifications sent. This number may include notifications that were prevented from being transmitted due to reasons such as resource limitations and/or non-connectivity. If one is receiving notifications, one can periodically poll this object to determine if any notifications were missed. If so, a poll of the apSyslogHistoryTable might be appropriate.
apSyslogNotificationsEnabled	.2	Information about whether or not apSyslogMessageGenerated notifications will be sent when a syslog message is generated by the device. Disabling notifications does not prevent syslog messages from being added to the apSyslogHistoryTable.
apSyslogMaxLevel	.3	Information about which syslog severity levels will be processed. Any syslog message with a log-level value greater than this value will be ignored by the syslog agent. Note that severity numeric values increase as their severity decreases (for example, major (3) is more severe than debug (9)).

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.1.1.1 +	Description
apSyslogMsgIgnores	.4	Number of syslog messages which were ignored, meaning that there is no need to send an apSyslogMessageGenerated notification. A message will be ignored if it has a log level value greater than the apSyslogMaxLevel value.
apSyslogMsgDrops	.5	Number of syslog messages which could not be processed due to lack of system resources. Most likely, this will occur at the same time that syslog messages are generated to indicate this lack of resources. Increases in this object's value may serve as an indication that system resource levels should be examined via other MIB objects. A message that is dropped will not appear in the history table, and no notification will be sent for this message.

 **Note:** Form the Object Identifier (OID) Number by concatenating the OID of apSyslogHistory (1.3.6.1.4.1.9148.3.1.1.2) with the OID termination number.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.1.1.2 +	Description
apSyslogHistTableMaxLength	.1	Upper limit for the number of entries that the apSyslogHistoryTable may contain. A value of 0 will prevent any history from being retained. When the apSyslogHistoryTable is full, the oldest entry will be deleted and a new one will be created.
apSyslogHistMsgsFlushed	.2	Number of entries that have been removed from the apSyslogHistoryTable in order to make room for new entries. Use this to determine whether the polling frequency on the history table is fast enough and/or if the size of the history table is large enough such that messages are not missed.

 **Note:** Form the Object Identifier (OID) Number by concatenating the OID of apSyslogHistoryEntry (1.3.6.1.4.1.9148.3.1.1.2.3) with the OID termination number.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.1.1.2.3 +	Description
apSyslogHistIndex	.1	Monotonically increasing integer for the sole purpose of indexing messages. When it reaches the maximum value, the agent wraps the value back to 1.
apSyslogHistFrom	.2	Process name and host of the sending client (for example, anyclient@sr.acme.com)
apSyslogHistLevel	.3	Log level of the message.
apSyslogHistType	.4	Textual identification for the log type, which categorizes the log message.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.1.1.2.3 +	Description
apSyslogHistContent	.5	Text of the syslog message. If the text of the message exceeds 255 bytes, it is truncated to 255 bytes.
apSyslogHistTimestamp	.6	Value of sysUpTime when this message was generated.

System Management MIB (ap-smgmt.mib)

The following table describes the SNMP GET query names for the System Management MIB (ap-smgmt.mib).

Note that the apSigRealmStats MIB is populated for realms on which H.323 and SIP are configured; this supports aggregate statistics for H.323 and SIP. A note like this one appears with the OID information shown in the table below.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
apSysCPUUtil	.1	Percentage of CPU utilization. This value reflects the mean CPU utilization for all cores on the system. For a system with 4 cores, the number reported here is (CPU0 + CPU1 + CPU2 + CPU3)/4. This value is updated very second.
apSysMemoryUtil	.2	Percentage of memory utilization.
apSysHealthScore	.3	System health percentage, with a system health percentage value of 100 (100%) being the healthiest.
apSysRedundancy	.4	For HA pairs, information about whether this SBC is active or standby. Possible values are: initial(1): system is at initial stage active(2): system is active standby(3): system is standby outOfService(4): system is out of service For a Standalone system, a value of (2) is returned.
apSysGlobalConSess	.5	Total instant number of global concurrent sessions at the moment.
apSysGlobalCPS	.6	Number of global calls per second. This is an instant value, which is the sum of SIP and H.323 calls.
apSysNATCapacity	.7	Percentage of NAT table in Content Addressable Memory (CAM) utilization.
apSysARPCapacity	.8	Percentage of ARP table (in CAM) utilization.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
apSysState	.9	Current system state. Online denotes regular call processing and offline implies no call processing occurring but other administrative functions are available.
apSysLicenseCapacity	.10	Percentage of licensed sessions currently in progress.
apSysSipStatsActiveLocalContacts	.11	Number of currently cached registered contacts in the SBC.
apSysMgcpGWEndpoints	.12	Not Supported.
apSysH323Registration	.13	Number of H.323 registrations in the SBC.
apSysRegCacheLimit	.14	Maximum number of contacts to be accepted into the registration cache. A value of 0 indicates no limit.
apSysApplicationCPULoadRate	.16	This value reflects the load of the sipd application on the cores where the threads have been scheduled. Thus if there are two sipd threads running on individual cores, a and b, the number reported here is $(CPU_a + CPU_b)/2$.
apSysRejectedMessages	.18	Number of messages rejected by the SBC due to matching criteria.
apSysSipEndptDemTrustToUntrust	.19	Global counter for SIP endpoint demotion from trusted to untrusted.
apSysSipEndptDemUntrustToDeny	.20	Global counter for SIP endpoint demotion from untrusted to deny.
apSysMgcpEndptDemTrustToUntrust	.21	Not Supported.
apSysMgcpEndptDemUntrustToDeny	.22	Not Supported.
apSysSipTotalCallsRejected	.25	Global counter for SIP calls that are rejected by the SBC
apSysSipStatsActiveSubscriptions	.27	An unsigned 32-bit integer that specifies the current global count of active SIP subscriptions.
apSysSipStatsPerMaxSubscriptions	.28	An unsigned 32-bit integer that specifies the maximum global count of SIP subscriptions initiated during any 100 second period since the last SBC re-boot.
apSysSipStatsPerMaximumActiveSubscriptions	.29	An unsigned 32-bit integer that specifies the maximum global count of active SIP subscriptions since the last SBC re-boot.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
apSysSipStatsTotalSubscriptions	.30	An unsigned 32-bit integer that specifies the global count of active SIP subscriptions since the last SBC r e-boot.
apSysMgmtH248MgcName	.31	Not Supported.
apSysMgmtH248Realm	.32	Not Supported.
apSysMgmtH248PortMapUsage	.33	Not Supported.
apSysCPULoadAvgOneMinute	.43	The percentage of CPU Load across all cores measured over 1 minute.
apSysCPULoadAvgFiveMinute	.44	The percentage of CPU Load across all cores measured over 5 minutes.
apSysCPULoadAvgFifteenMinute	.45	The percentage of CPU Load across all cores measured over 15 minutes.

The apSysMgmtCPULoadAvgGroup object has the OID 1.3.6.1.4.1.9148.3.2.4.2.31, and is an object that monitors CPU Load Average across all CPU cores for 1, 5, and 15 minutes.

The apSysStorageSpaceTable object has the OID 1.3.6.1.4.1.9148.3.2.1.1.23, and the apSysStorageSpaceEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.1.23.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1.23.1 +	Description
apSysVolumeIndex	.1	Monotonically increasing integer for the purpose of indexing volumes.
apSysVolumeName	.2	Name of the volume.
apSysVolumeTotalSpace	.3	Total size of the volume in MB.
apSysVolumeAvailSpace	.4	Total space available on the volume in KB.

The apCombinedSessionAgentStatsEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.2.1.1.

This table object reflects statistics found in the **show sipd agents** CLI command.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
apCombinedStatsSessionAgentIndex	.1	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
apCombinedStatsSessionAgentHostname	.2	The hostname of the session agent for which the following statistics are being calculated.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
apCombinedStatsSessionAgentType	.3	The type of the specified session agent, either SIP or H323.
apCombinedStatsCurrentActiveSessionsInbound	.4	Number of current active inbound sessions. This value is found on the ACLI at show sipd agents , "Inbound Active" column.
apCombinedStatsCurrentSessionRateInbound	.5	Current inbound session rate in CPS. This value is found on the ACLI at show sipd agents , "Inbound Rate" column.
apCombinedStatsCurrentActiveSessionsOutbound	.6	Number of current active outbound sessions. This value is found on the ACLI at show sipd agents , "Outbound Active" column.
apCombinedStatsCurrentSessionRateOutbound	.7	Current outbound session rate in CPS. This value is found on the ACLI at show sipd agents , "Outbound Rate" column.
apCombinedStatsTotalSessionsInbound	.8	Total number of inbound sessions during the 100 second sliding window period.
apCombinedStatsTotalSessionsNotAdmittedInbound	.9	Total number of non-bandwidth constraints that exceeded rejections on inbound sessions (for example, max-

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
		sessions, burst rate, etc.).
apCombinedStatsPeriodHighInbound	.10	Highest number of concurrent inbound sessions during the period.
apCombinedStatsAverageRateInbound	.11	Average rate of inbound sessions during the 100 second sliding window period in CPS. This value is found on the ACLI at show sipd agents , "Inbound Rate" column.
apCombinedStatsTotalSessionsOutbound	.12	Total number of outbound sessions during the 100 second sliding window period.
apCombinedStatsTotalSessionsNotAdmittedOutbound	.13	Total number of non-bandwidth constraints that exceeded rejections on outbound sessions (for example, max-sessions, burst rate, etc.).
apCombinedStatsPeriodHighOutbound	.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apCombinedStatsAverageRateOutbound	.15	Average rate of outbound sessions during the 100 second sliding window period in CPS. This value is found on the ACLI at show sipd agents , "Outbound Rate" column.
apCombinedStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
		sliding window period (combined inbound and outbound). This value is found on the ACLI at show sipd agents , "Max Burst" counter.
apCombinedStatsPeriodSeizures	.17	Total number of seizures during the 100 second sliding window period.
apCombinedStatsPeriodAnswers	.18	Total number of answered sessions during the 100 second sliding window period.
apCombinedStatsPeriodASR	.19	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apCombinedStatsAverageLatency	.20	Average observed one-way signalling latency during the period.
apCombinedStatsMaxLatency	.21	Maximum observed one-way signalling latency during the 100 second sliding window period.
apCombinedStatsSessionAgentStatus	.22	The current status of the specified session agent, which is expressed as INS, OOSnonresp, OOSconstraintsviolation, BecomingOOS, or ForcedOOS.

The apSipSessionAgentStatsEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.2.2.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.2.1 +	Description
apSipSASStatsSessionAgentIndex	.1	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
apSipSASStatsSessionAgentHostname	.2	The hostname of the session agent for which the following statistics are being calculated.
apSipSASStatsSessionAgentType	.3	The type of the specified session agent, either SIP or H323.
apSipSASStatsCurrentActiveSessionsInbound	.4	Number of current active inbound sessions.
apSipSASStatsCurrentSessionRateInbound	.5	Current Inbound Session rate in CPS.
apSipSASStatsCurrentActiveSessionsOutbound	.6	Number of current active outbound sessions.
apSipSASStatsCurrentSessionRateOutbound	.7	Current outbound session rate in CPS.
apSipSASStatsTotalSessionsInbound	.8	Total number of inbound sessions during the 100 second sliding window period.
apSipSASStatsTotalSessionsNotAdmittedInbound	.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apSipSASStatsPeriodHighInbound	.10	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apSipSASStatsAverageRateInbound	.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apSipSASStatsTotalSessionsOutbound	.12	Total number of outbound sessions during the 100 second sliding window period.
apSipSASStatsTotalSessionsNotAdmittedOutbound	.13	Total number of outbound sessions rejected because of insufficient bandwidth.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.2.1 +	Description
apSipSASStatsPeriodHighOutbound	.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apSipSASStatsAverageRateOutbound	.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apSipSASStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apSipSASStatsPeriodSeizures	.17	Total number of seizures during the 100 second sliding window period.
apSipSASStatsPeriodAnswers	.18	Total number of answered sessions during the 100 second sliding window period.
apSipSASStatsPeriodASR	.19	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apSipSASStatsAverageLatency	.20	Average observed one-way signaling latency during the 100 second sliding window period.
apSipSASStatsMaxLatency	.21	Maximum observed one-way signaling latency during the 100 second sliding window period.
apSipSASStatsSessionAgentStatus	.22	The current status of the specified session agent, which is expressed as INS, OOSnonresp, OOSconstraintsviolation, BecomingOOS, or ForcedOOS.


The apH323SessionAgentStatsTable object has the OID 1.3.6.1.4.1.9148.3.2.1.2.3, and the apH323SessionAgentStatsEntry has the OID 1.3.6.1.4.1.9148.3.2.1.2.3.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.3.1 +	Description
apH323SASStatsSessionAgentIndex	.1	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1.
apH323SASStatsSessionAgentHostname	.2	The hostname of the session agent for which the following statistics are being calculated.
apH323SASStatsSessionAgentType	.3	The type of the specified session agent, H323.
apH323SASStatsCurrentActiveSessionsInbound	.4	Number of current active inbound sessions.
apH323SASStatsCurrentSessionRateInbound	.5	Current Inbound Session rate in CPS.
apH323SASStatsCurrentActiveSessionsOutbound	.6	Number of current active outbound sessions
apH323SASStatsCurrentSessionRateOutbound	.7	Current outbound session rate in CPS
apH323SASStatsTotalSessionsInbound	.8	Total Number of inbound sessions during the 100 second sliding window period.
apH323SASStatsTotalSessionsNotAdmittedInbound	.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apH323SASStatsPeriodHighInbound	.10	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apH323SASStatsAverageRateInbound	.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apH323SASStatsTotalSessionsOutbound	.12	Total number of outbound sessions during the 100 second sliding window period.
apH323SASStatsTotalSessionsNotAdmittedOutbound	.13	Total number of outbound sessions

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.3.1 +	Description
		rejected because of insufficient bandwidth.
apH323SASStatsPeriodHighOutbound	.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apH323SASStatsAverageRateOutbound	.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apH323SASStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apH323SASStatsPeriodSeizures	.17	Total number of seizures during the 100 second sliding window period.
apH323SASStatsPeriodAnswers	.18	Total number of answered sessions during the 100 second sliding window period.
apH323SASStatsPeriodASR	.19	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apH323SASStatsAverageLatency	.20	Average observed one-way signalling latency during the 100 second sliding window period.
apH323SASStatsMaxLatency	.21	Maximum observed one-way signalling latency during the 100 second sliding window period
apH323SASStatsSessionAgentStatus	.22	The current status of the specified session agent, which is expressed as INS, OOSnonresp, OOSconstraintsviolation, BecomingOOS, or ForcedOOS

The apSigRealmStatsTable object has the OID 1.3.6.1.4.1.9148.3.2.1.2.4 and the apSigRealmStatsEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.2.4.1.

 **Note:** This table is populated for realms on which H.323 and SIP are configured; this supports aggregate statistics for H.323 and SIP.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
apSigRealmStatsRealmIndex	.1	A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
apSigRealmStatsRealmName	.2	The name of the realm for which the following statistics are being calculated.
apSigRealmStatsCurrentActiveSessionsInbound	.3	Number of current active inbound sessions.
apSigRealmStatsCurrentSessionRateInbound	.4	Current inbound session rate in CPS.
apSigRealmStatsCurrentActiveSessionsOutbound	.5	Number of current active outbound sessions.
apSigRealmStatsCurrentSessionRateOutbound	.6	Current outbound session rate in CPS.
apSigRealmStatsTotalSessionsInbound	.7	Total number of inbound sessions during the 100 second sliding window period.
apSigRealmStatsTotalSessionsNotAdmittedInbound	.8	Total number of inbound sessions rejected because of insufficient bandwidth.
apSigRealmStatsPeriodHighInbound	.9	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apSigRealmStatsAverageRateInbound	.10	Average rate of inbound sessions during the 100 second sliding window period in CPS.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
apSigRealmStatsTotalSessionsOutbound	.11	Total number of outbound sessions during the 100 second sliding window period.
apSigRealmStatsTotalSessionsNotAdmittedOutbound	.12	Total number of outbound sessions rejected because of insufficient bandwidth.
apSigRealmStatsPeriodHighOutbound	.13	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apSigRealmStatsAverageRateOutbound	.14	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apSigRealmStatsMaxBurstRate	.15	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apSigRealmStatsPeriodSeizures	.16	Total number of seizures during the 100 second sliding window period.
apSigRealmStatsPeriodAnswers	.17	Total number of answered sessions during the 100 second sliding window period.
apSigRealmStatsPeriodASR	.18	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apSigRealmStatsAverageLatency (not supported)	.19	Average observed one-way signaling latency in milliseconds during the period.
apSigRealmStatsMaxLatency	.20	Maximum observed one-way signaling

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
(not supported)		latency in milliseconds during the period.
apSigRealmStatsMinutesLeft	.21	Number of monthly-minutes left in the pool per calendar year for a given realm.
apSigRealmStatsMinutesReject	.22	Peg counts of the number of calls rejected because the monthly-minutes constraints are exceeded.
apSigRealmStatsShortSessions	.23	Lifetime number of sessions whose duration was less than the configured short session durations.
apSigRealmStatsAverageQoSFactor	.24	Average QoS factor observed during the period.
apSigRealmStatsMaximumQoSFactor	.25	Maximum QoS factor observed during the period.
apSigRealmStatsCurrentMajorRFactorExceeded	.26	Peg counts of the number of times the major Rfactor threshold was exceeded during the period.
apSigRealmStatsTotalMajorRFactorExceeded	.27	Peg counts of the number of times the major Rfactor threshold was exceeded during the lifetime.
apSigRealmStatsCurrentCriticalRFactorExceeded	.28	Peg counts of the number of times the critical Rfactor threshold was exceeded during the period.
apSigRealmStatsTotalCriticalRfactorExceeded	.29	Peg counts of the number of times the critical Rfactor threshold was exceeded during the lifetime.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
apSigRealmStatsRealmStatus	.30	Current status of the specified realm, which is expressed as INS, constraintviolation, or callLoadReduction.
apSigRealmStatsActiveLocalContacts	.31	An unsigned 32-bit integer that specifies the current domain count of active SIP registrations.
apSigRealmStatsActiveSubscriptions	.32	Number of active subscriptions for the given realm.
apSigRealmStatsPerMaxSubscriptions	.33	Lifetime PerMax subscriptions count for the given realm.
apSigRealmStatsMaximumActiveSubscriptions	.34	Count of lifetime maximum active subscriptions for the given realm.
apSigRealmStatsTotalSubscriptions	.35	Count of lifetime total subscriptions for the system.

The apSysMgmtNetMgmtCtrlObjects object has the OID 1.3.6.1.4.1.9148.3.2.1.3, the apNetMgmtCtrlStatsTable object has the OID 1.3.6.1.4.1.9148.3.2.1.3.1, and the apNetMgmtCtrlStatsEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.3.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.3.1.1 +	Description
apNetMgmtCtrlStatsName	.1	Name of the network management control (NMC) the for which statistics are being calculated.
apNetMgmtCtrlStatsType	.2	Type of specified NMC: gap-rate, gap-percent, or priority.
apNetMgmtCtrlStatsIncomingTotal	.3	Total number of incoming calls matching a destination identifier of the NMC.
apNetMgmtCtrlStatsRejectedTotal	.4	Number of apNetMgmtCtrlStatsIncomingTotal that are rejected.
apNetMgmtCtrlStatsStatsDivertedTotal	.5	Number of apNetMgmtCtrlStatsIncomingTotal that are diverted.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.3.1.1 +	Description
apNetMgmtCtrlStatsStatsIncomingCurrent	.6	Number of incoming calls during the current period that match a destination identifier
apNetMgmtCtrlStatsStatsRejectedCurrent	.7	Number of apNetMgmtCtrlStatsIncomingCurrent that are rejected.
apNetMgmtCtrlStatsStatsDivertedCurrent	.8	Number of apNetMgmtCtrlStatsIncomingCurrent that are diverted.
apNetMgmtCtrlStatsIncomingPeriodMax	.9	Maximum number of incoming calls during a period that match a destination identifier of the NMC.
apNetMgmtCtrlStatsStatsRejectedPeriodMax	.10	Number of apNetMgmtCtrlStatsIncomingPeriodMax that are rejected.
apNetMgmtCtrlStatsStatsDivertedPeriodMax	.11	Number of apNetMgmtCtrlStatsIncomingPeriodMax that are diverted.
apNetMgmtCtrlStatsState	.12	The state of the specified network management control, which can be disabled or enabled

The apSysMgmtMIBENUMServerStatusObjects object has the OID 1.3.6.1.4.1.9148.3.2.1.4, the apENUMServerStatusTable object has the OID 1.3.6.1.4.1.9148.3.2.1.4.1, and the apENUMServerStatusEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.4.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.4.1.1 +	Description
apENUMConfigname	.1	Name of the ENUM configuration element that contains this ENUM server.
apENUMServerIpAddress	.2	IP address of this ENUM server.
apENUMServerStatus	.3	Status of this ENUM server.

The apSysMgmtMIBNSEPStatsObjects object has the OID 1.3.6.1.4.1.9148.3.2.1.5.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5 +	Description
apNSEPStatsCurrentActiveSessionsInbound	.1	Number of currently active inbound NSEP sessions.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5 +	Description
apNSEPStatsTotalSessionsInbound	.2	Total number of inbound NSEP sessions during lifetime.
apNSEPStatsPeriodHighInbound	.3	Highest number of concurrent inbound NSEP sessions during the period.
apNSEPStatsPeriod	.4	The period for which all statistics are collected (in seconds). (Currently a non-configurable value of 30 minutes.)

The apNSEPStatsRPHTable object has the OID 1.3.6.1.4.1.9148.3.2.1.5.5, and the apNSEPStatsRPHEntire object has the OID 1.3.6.1.4.1.9148.3.2.1.5.5.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5.5.1 +	Description
apNSEPStatsRPHValue	.1	The specific RPH value used for indexing (namespace.rpriority).
apNSEPStatsRPHCurrentActiveSessionsInbound	.2	Number of current active inbound NSEP sessions for this specific RPH value.
apNSEPStatsRPHTotalSessionsInbound	.3	Total number of inbound NSEP sessions for this specific RPH value during lifetime.
apNSEPStatsRPHPeriodHighInbound	.4	Highest number of concurrent inbound NSEP sessions during the period for this specific RPH value.
apNSEPStatsRPHTotalSessionsNotAdmittedInbound	.5	Total number of inbound NSEP sessions rejected for this specific RPH value during lifetime.
apNSEPStatsRPHCurrentActiveSessionsOutbound	.6	Number of current active outbound NSEP sessions for this specific RPH value.
apNSEPStatsRPHTotalSessionsOutbound	.7	Total number of outbound NSEP sessions for this

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5.5.1 +	Description
		specific RPH value during lifetime.
apNSEPStatsRPHPeriodHighOutbound	.8	Highest number of concurrent outbound NSEP sessions during the period for this specific RPH value.
apNSEPStatsRPHTotalSessionsNotAdmittedOutbound	.9	Total number of outbound NSEP sessions rejected for this specific RPH value during lifetime

The apLDAPServerStatusTable object has the OID 1.3.6.1.4.1.9148.3.2.1.6.1, and the apLDAPServerStatusEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.6.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.6.1.1 +	Description
apLDAPConfigName	.1	Name of the LDAP configuration element that contains this LDAP server.
apLDAPServerIPAddresses	.2	IP address of this LDAP server.
apLDAPServerStatus	.3	Status of this LDAP server.

The apSysMgmtTrapTable object has the OID 1.3.6.1.4.1.9148.3.2.1.7.1, and the apSysMgmtTrapTableEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.7.1.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.7.1.1 +	Description
apTrapTableSystemTime	.1	System time of the session border controller.
apTrapTableInstanceIndex	.2	Instance index of the trap ID incremented with a resolution of a second.
apTrapTableNumVariables	.3	Number of information encoded in the trap.
apTrapTableSysUptime	.4	SNMP sysUpTime when the trap was generated.
apTrapTableTrapID	.5	Trap ID associated with the fault condition.

The apSysMgmtTrapInformationTable object has the OID 1.3.6.1.4.1.9148.3.2.1.7.2, and the apSysMgmtTrapInformationTableEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.7.2.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.7.2.1 +	Description
apTrapInformationTableDataIndex	.1	Index of the information encoded in the trap.

Enterprise SNMP GET Requests

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.7.2.1 +	Description
apTrapInformationTableDataType	.2	SNMP type enumerated encoded in the trap. snmpTypeInteger is the size of integer snmpTypeObjectIpAddress is an octet string of length 4
apTrapInformationTableDataLength	.3	Octet length of the information encoded in the trap.
apTrapInformationTableDataOctets	.4	Information represented in octets: snmpTypeInteger, snmpTypeObjectCounter32, snmpTypeObjectGauge, snmpTypeObjectOpaque, and snmpUnsignedInteger32 are 4 octets long snmpType counter is 8 octets long snmpTypeObjectIpAddress, snmpTypeObjectNSAPAddress are 4 octets long Data is aligned in network order.

The apSysMgmtInterfaceObjects object has the OID 1.3.6.1.4.1.9148.3.2.1.8, the apSysMgmtPhyUtilTable object has the OID 1.3.6.1.4.1.9148.3.2.1.8.1, and the apSysMgmtPhyUtilTableEntry object has the OID 1.3.6.1.4.1.9148.3.2.1.8.1.1

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.8.1.1 +	Description
apPhyUtilTableRxUtil	.1	RX network utilization of the physical port measured over a one second period.
apPhyUtilTableTxUtil	.2	TX network utilization of the physical port measured over a one second period

Notes on ENUM Server Names

Note that the characters of the name are given in the ASCII values because of SNMP's restrictions. This representation affects the order in which entries in the table appear. Entries are listed:

- By the length of their names
- Then by a comparison of the characters they contain; this comparison is not limited to alphabetical order in that uppercase letter precede lowercase characters
- Last, by the IP address of the server for that entry

Take, for example, the case where there are three ENUM configurations:

- aaa, with servers 1.1.1.1 and 1.1.1.2
- BBB, with servers 3.3.3.3 and 3.3.3.2
- cc, with server 2.2.2.2

The entries would appear in the following order, with the following instance IDs:

1. cc 2.2.2.2 would appear first because cc is the shortest name), and would be represented by the instance ID:2.99.99.2.2.2.2
2. BBB entries would be next, sorted by IP address, because "BBB" is considered less than aaa, and would be represented by the instance IDs:3.66.66.66.3.3.3.2 and3.66.66.66.3.3.3.3
3. aaa entries would appear last, represented by the instance IDs:3.97.97.97.1.1.1.1 and3.97.97.97.1.1.1.2

Software Inventory MIB (ap-swinventory.mib)

The following table describes the SNMP GET query names for the Software Inventory MIB (ap-swinventory.mib).

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.4.1.1.1 +	Description
apSwBootDescr	.2	Description of the software image which may consist of a filename, data and time this image was built or the unique identifier of the software. For example: boot image: 10.0.1.12/sd201p3.gz for host address is 10.0.1.12, and image name is sd201p3.gz boot image: /tffs0/sd201p3.gz for boot from flash 0 and image name is sd201p3.gz boot loader: bank0:03/18/2005 10:58:25 for boot from bank 0, and version is March 18 2005, 10:58:25'.
apSwBootType	.3	Type of software image. A value of 1 indicates a boot Image. A value of 2 indicates a bootloader image.
apSwBootStatus	.4	Status of the software image. A value of 1 indicates an image that is currently being used. A value of 2 indicates a previously used image.

The object apSwInventoryCfgObjects has the OID 1.3.6.1.4.1.9148.3.4.1.2.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.4.1.2 +	Description
apSwCfgCurrentVersion	.1	Current version of the saved configuration.
apSwCfgRunningVersion	.2	Current version of the running configuration.

The object apSwCfgBackupEntry has the OID 1.3.6.1.4.1.9148.3.4.1.2.3.1.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.4.1.2.3.1 +	Description
apSwCfgBackupName	.2	Description of the configuration filename, for example: p1604, 063004-cfg.

Multicore Monitoring MIB (ap-usbcsys.mib)

A variety of statistics that report information on the CPUs/Cores within the Oracle USM are available via the `ap-usbcsys.mib` MIB. These statistics are:

Object Name	Object ID: 1.3.6.1.4.1.9148.3.17 +	Description
apUsbcSysModule		
apUsbcSysMIBObjects	.1	
apUsbcSysObjects	.1.1	
apUsbcSysCpuUtilAll	.1.1.1	The percentage of total Cpu utilization.
apUsbcSysCpuCount	.1.1.2	The number of cpus for this system.
apUsbcSysCpuSpeedMHz	.1.1.3	The speed in MHz of the cpus for this system.
apUsbcSysMemSzMB	.1.1.4	The number of megabytes of all cpus for this system.
apUsbcSysMemSzGB	.1.1.5	The number of gigabytes of all cpus for this system. This value is derived from the apUsbcSysMemSzMB object.
apUsbcSysAppMemUtil	.1.1.6	The number of megabytes of memory used by the applications.
apUsbcSysKernelMemUtil	.1.1.7	The number of megabytes of memory used by the kernel.
apUsbcSysMyBogoMips	.1.1.8	The processor speed measured in millions of instructions per second per processor, calculated by the kernel at boot time.
apUsbcSysAllBogoMips	.1.1.9	The sum of all bogo mips(millions of instructions per second) of all cpus for this system.
apUsbcSysCpuTblObjects	.1.1.10	
apUsbcSysCpuTable	.1.1.10.1	A read-only table to hold information for a cpu indexed by the cpu number i + 1.
apUsbcSysCpuEntry	.1.1.10.1.1	A entry designed to hold the status of a single Cpu.
apUsbcSysCpuNum	.1.1.10.1.1.1	The cpu number + 1 of this entry.
apUsbcSysCpuUtil	.1.1.10.1.1.2	The percent of cpu utilization of this cpu.
apUsbcSysThreadObjects	.1.2	A collection of objects providing the USBC thread level statistics.
apUsbcThreadUsageTableObject	.1.2.1	An identifier provided for each object in the thread usage table.

Object Name	Object ID: 1.3.6.1.4.1.9148.3.17 +	Description
apUsbcThreadUsageTable	.1.2.1.1	A table to hold the thread usage information, on a Session Border Controller.
apThreadUsageEntry	.1.2.1.1.1	A table entry designed to hold the thread usage information, on a Session Border Controller.
apThreadId	.1.2.1.1.1.1	The instance index of the thread.
apThreadName	.1.2.1.1.1.2	The name of the thread.
apThreadCurrentUsage	.1.2.1.1.1.3	The current cpu usage of the thread. Multiply by 100 from % value.
apThreadOverloaded	.1.2.1.1.1.4	Indicator if thread is in overload control.
apUsbcThreadEventTableObject	.1.2.2	An object within the table holding thread event information.
apUsbcThreadEventTable	.1.2.2.1	A table to hold the thread event information, on a Session Border Controller. These are all read only.
apThreadEventEntry	.1.2.2.1.1	A table entry designed to hold the thread event information, on a Session Border Controller.
apThreadEventPendingCurrent	.1.2.2.1.1.1	The event pending Active counter.
apThreadEventPendingCurrentHigh	.1.2.2.1.1.2	The event pending High counter.
apThreadEventPendingWindow	.1.2.2.1.1.3	The event pending window.
apThreadEventPendingTotal	.1.2.2.1.1.4	The event pending Total counter.
apThreadEventPendingMaximum	.1.2.2.1.1.5	The event pending PerMax counter.
apThreadEventPendingHigh	.1.2.2.1.1.6	The event pending High counter.
apThreadEventDroppedCurrent	.1.2.2.1.1.7	The event dropped Active counter.
apThreadEventDroppedCurrentHigh	.1.2.2.1.1.8	The event dropped High counter.
apThreadEventDroppedWindow	.1.2.2.1.1.9	The event dropped window.
apThreadEventDroppedTotal	.1.2.2.1.1.10	The event dropped Total counter.
apThreadEventDroppedMaximum	.1.2.2.1.1.11	The event dropped PerMax counter.

Enterprise SNMP GET Requests

Object Name	Object ID: 1.3.6.1.4.1.9148.3.17 +	Description
apThreadEventDroppedHigh	.1.2.2.1.1.12	The event dropped High counter.
apThreadLatencyPendingAverage	.1.2.2.1.1.13	The thread average latency.
apThreadLatencyPendingMax	.1.2.2.1.1.14	The thread max latency.
apThreadLatencyProcessingAverage	.1.2.2.1.1.15	The thread average latency.
apThreadLatencyProcessingMax	.1.2.2.1.1.16	The thread max latency.
apUsbcSipObjects	.1.2.3	An object grouping SIPD-related per-thread CPU utilization information.
apSipNumberOfThreads	.1.2.3.1	Number of SIP threads.
apSipAverageCpuUtil	.1.2.3.2	Average CPU utilization.
apSipPendingAverageLatency	.1.2.3.3	The average latency of SIP Pending events.
apSipPendingMaxLatency	.1.2.3.4	The max latency of SIP Pending events.
apSipProcessingAverageLatency	.1.2.3.5	The average latency of SIP Processing events.
apSipProcessingMaxLatency	.1.2.3.6	The max latency of SIP Processing events.
apUsbcAtcpObjects	.1.2.4	An object grouping ATCP-related per-thread CPU utilization information.
apAtcpNumberOfThreads	.1.2.4.1	Number of ATCP threads.
apAtcpAverageCpuUtil	.1.2.4.2	Average CPU utilization.
apAtcpPendingAverageLatency	.1.2.4.3	The average latency of ATCP Pending events.
apAtcpPendingMaxLatency	.1.2.4.4	The max latency of ATCP Pending events.
apAtcpProcessingAverageLatency	.1.2.4.5	The average latency of ATCP Processing events.
apAtcpProcessingMaxLatency	.1.2.4.6	The max latency of ATCP Processing events.

This MIB reflects statistics displayed by the **show platform cpu**, **show platform cpu-load**, and **show platform memory** commands. The following screen capture is annotated with the correspondence.

```
ORACLE#show platform cpu
CPU count : 8 //apUsbcSysCpuCount
CPU speed : 2301 MHz //apUsbcSysCpuSpeedMHz
CPU model : Intel(R) Core(TM) i7-3615QE CPU @ 2.30GHz
CPU flags : [...]
```

```
CPU workload: Capacity : 80000 bogoMIPS //apUsbcSysAllBogoMips
App load : 4599 bogoMIPS //apUsbcSysMyBogoMips

ORACLE> show platform cpu-load
Total load: 9% //apUsbcSysCpuUtilAll
CPU#00 4% //apUsbcSysCpuNum + apUsbcSysCpuUtil
CPU#01 13% //apUsbcSysCpuNum + apUsbcSysCpuUtil

ORACLE> show platform memory Mem
Total : 1892 MB //apUsbcSysMemSzMB Mem App : 213 MB //apUsbcSysAppMemUtil Mem
OS : 849 MB //apUsbcSysKernelMemUtil
```

SNMP-based Application Features

This chapter contains Oracle USM features that involve SNMP reporting on application activity.

SNMP Reporting of Message Rate Statistics

The message rate statistics feature enables the system to provide message rate statistics for SIP, DNS, and ENUM traffic via ACLI and HDR output. These statistics can be retrieved via SNMP.

Message rate statistics are available through four tables. These tables correspond to SIP Method message rate per SIP Interface, SIP Method message rate per SIP Agent, DNS ALG message rate, and ENUM server message rate. Ensure that the following parameters are **enabled** for the type of statistics you wish to collect:

Statistic Type	configuration element	parameter
SIP Message Rate	sip-config	extra-method-stats
DNS Message Rate	media-manager > dns-config	extra-dnsalg-stats
ENUM Message Rate	sip-config	extra-enum-stats

apSIPRateIntfStatsTable

This table, found in the `Ap-sip.mib`, provides a listing of SIP message rate statistics per SIP interface. It conveys the same information displayed in the **show sipd rate interface** command. The table is indexed by the SIP Interface index and SIP method. The SIP Interface to index number mapping is found in the `apSipInterfaceTable` in `Ap-sip.mib`. The SIP method to index mapping is found in the `ApSipMethod` object in `Ap-tc.mib`.

apSIPRateAgentStatsTable

This table, found in the `Ap-sip.mib`, provides a listing of SIP message rate statistics per SIP agent (SIP session agent). It conveys the same information displayed in the **show sipd rate agent** command. The table is indexed by the SIP agent index and SIP method. The SIP Agent to index number mapping is found in the `apSipAgentTable` in `Ap-sip.mib`. The SIP method to index mapping is found in the `ApSipMethod` object in `Ap-tc.mib`.

apDnsAlgServerRateStatsTable

This table, found in the `Ap-dnsalg.mib`, provides a listing of message rate statistics for a specific DNS Alg Server. It conveys the same information displayed in the `show dnsalg rate realm-id` and `show dnsalg rate server-ip-addr` commands. The table is indexed by the DNS ALG realm index and DNS ALG server index. The table of rate statistics also includes the DNS ALG server IP address and IP address type (IPv4 or IPv6). If a DNS ALG client realm, DNS ALG server, and IP address are not configured, then the combination of those indices will return no data. The DNS ALG Server to index mapping is found in the `apDnsAlgServerTable` in the `Ap-dnsalg.mib`. The DNS ALG realm to index mapping is found in the `apDnsAlgConfigTable` in the `Ap-dnsalg.mib`.

apEnumServerRateStatsTable

This table, found in the `Ap-apps.mib`, provides a listing of ENUM message rate statistics for a specific ENUM server. It conveys the same information displayed in the `show enum rate` command. This table is indexed by the ENUM configuration name, ENUM Server IP address and IP address type (IPv4 or IPv6).

FQDN-resolved Session Agent Statistics SNMP Retrieval

When FQDN-resolved Session Agent Statistics are enabled, you can retrieve each IP target's session agent statistics via SNMP.

The `apSipAgentTable` returns a list of configured sessions agent with an index corresponding and configuration name. The mapping of index to configuration name is persistent across system reboot.

The index of the additional entries that correspond to the individual IP targets are identified by starting at 10000000. Because the IP targets that are retrieved from the DNS server may change on any DNS query, they are not persistent across a reboot. An `snmpwalk` query on `asSIPAgentTable` appears as:

```
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.2.36 = STRING: "sal.dg.com"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000000 = STRING:
"sal.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000001 = STRING:
"sal.dg.com#192.168.26.3"
```

The following `snmpwalk` query on `asSipSessionAgentStatsTable` appears as:

```
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.36 = INTEGER: 36
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.10000000 = INTEGER: 10000000
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.1.10000001 = INTEGER: 1000001
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.36 = STRING: "sal.dg.com"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000000 = STRING:
"sal.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000001 = STRING:
"sal.dg.com#192.168.26.3"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.36 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.10000000 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.3.10000001 = INTEGER: 1
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.36 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000000 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000001 = Gauge32: 0
FQDN-resolved Session Agent Statistics SNMP Traps
```

The `apSysMgmtSAStatusChangeTrap` trap is generated when a session agent's individual IP target changes state.

CAC Utilization Statistics via SNMP

The Oracle USM allows you to retrieve information on current session utilization and burst rate as a percentage of their configured maximums on per session-agent and/or realm basis. The Oracle USM uses

the configured **max-session** and **max-burst-rate** settings in conjunction with a percentage formula to calculate this value. The system also uses an ACLI configuration setting to establish the threshold at which trap and trap clear messages are sent from the SNMP agent to the configured manager(s).

The user must load the MIB version associated with this software version on all pertinent SNMP managers to query these CAC utilization (occupancy) values and interpret the traps. In addition, the user must configure the threshold at which the system generates the CAC utilization trap. Note that the corresponding clear trap uses the same threshold setting, sending the clear trap when utilization falls below 90% of the threshold.

SNMP Get for CAC Utilization

Using a MIB browser, the user can query the current percentage utilization values for both **max-session** and **max-burst-rate** for any session-agent or realm. The calculations for these utilization levels are:

- Session utilization level = (current session count * 100) / max-sessions
- Burst rate utilization level = (current burst rate * 100) / max-burst-rate

The MIB objects associated with these statistics are parallel for session agent and realm and include a table to contain the objects, an object associating the objects containing the values with the applicable table, and objects containing the values themselves. These objects are listed below.

The MIB objects containing CAC utilization data for Session Agents are listed below.

The object establishing the statistics table for session agent CAC utilization follows:

```
--apSip Session Agent Connection Admission Control Stats Table
apSipSaCacStatsTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF ApSipSaCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "SIP Session Agent Connection Admission Control Stats Table."
    ::= { apSipMIBTabularObjects 5 }
```

The object establishing the session agent CAC utilization statistics objects follows:

```
apSipSaCacStatsEntry OBJECT-TYPE
    SYNTAX          ApSipSaCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Connection Admission Control Statistics."
    AUGMENTS { apSipSessionAgentStatsEntry }
    ::= { apSipSaCacStatsTable 1 }
The session agent CAC utilization statistics values include:
ApSipSaCacStatsEntry ::= SEQUENCE {
    apSipSaCacSessionUtilLevel      Gauge32,
    apSipSaCacBurstRateUtilLevel    Gauge32
}
```

The above objects, specifying the CAC utilization value for sessions and burst rate utilization for session agents include:

```
apSipSaCacSessionUtilLevel      OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current session utilization level."
    ::= { apSipSaCacStatsEntry 1 }
apSipSaCacBurstRateUtilLevel     OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
```

SNMP-based Application Features

```
MAX-ACCESS      read-only
STATUS          current
DESCRIPTION
    "Current burst rate utilization level."
 ::= { apSigSaCacStatsEntry 2 }
```

The MIB objects containing CAC utilization data for Realms are listed below.

The object establishing the statistics table for realm CAC utilization follows:

```
--apSig Realm Connection Admission Control Stats Table
apSigRealmCacStatsTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF ApSigRealmCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Realm Connection Admission Control Stats Table."
    ::= { apSigMIBTabularObjects 6 }
```

The object establishing the realm CAC utilization statistics objects follows:

```
apSigRealmCacStatsEntry OBJECT-TYPE
    SYNTAX          ApSigRealmCacStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "Connection Admission Control Statistics."
    AUGMENTS { apSigRealmStatsEntry }
    ::= { apSigRealmCacStatsTable 1 }
```

The session agent CAC utilization statistics values include:

```
ApSigRealmCacStatsEntry ::= SEQUENCE {
    apSigRealmCacSessionUtilLevel      Gauge32,
    apSigRealmCacBurstRateUtilLevel    Gauge32
}
```

The above objects, specifying the CAC utilization value for sessions and burst rate utilization for realms include:

```
apSigRealmCacSessionUtilLevel      OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current session utilization level."
    ::= { apSigRealmCacStatsEntry 1 }
apSigRealmCacBurstRateUtilLevel    OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "percentage"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Current burst rate utilization level."
    ::= { apSigRealmCacStatsEntry 2 }
```

CAC Utilization Traps

The Oracle USM can issue a trap when either the value of max-session or CAC burst rate exceeds a configured value. The system only sends one trap when the threshold is exceeded. When the value falls back under 90% of this threshold, the Oracle USM sends a clear trap.

You configure the value that triggers these traps as a percentage of the max-session and max-burst-rate settings configured for the applicable session agent and/or realm. The system uses the same setting to

specify when to send both the sessions and burst rate traps. The name of this parameter is the cac-trap-threshold.

For realms, you configure a session-constraint element with the **cac-trap-threshold** setting and apply that session constraint to the realm. For a session agent however, you configure the **cac-trap-threshold** directly within the session agent's configuration. You must express the value as a number less than 100. There is no default setting; the system does not generate a trap if you have not configured this setting.

The apSipCACUtilAlertTrap identifies the threshold exceeded on a per-element and per-value (session count or burst rate) for each trap, including:

- apSipSaCacSessionUtilLevel
- apSipSaCacBurstRateUtilLevel
- apSipRealmCacSessionUtilLevel
- apSipRealmCacBurstRateUtilLevel

External Policy Server Connection Status Reporting

When the Oracle USM is deployed to act as a P-CSCF between the core IMS network and UEs, and the P-CSCF loses connection to the external policy server or an attempt is unsuccessful, the Oracle USM generates an SNMP trap. In addition to this trap, a minor, non-health effecting alarm is generated. Once connection has been restored, a trap is sent to clear the event. In the case of an HA policy server cluster, the alarm is generated only when all of the policy servers in the top-level cluster are down.

Enterprise Traps

The following table identifies the proprietary traps that the ap-diameter supports.

Trap Name	Description
apSysMgmtExtPolicyServerConnDownTrap 1.3.6.1.4.1.9148.3.2.6.0.74	Generated when the SBC is unable to connect to an external policy server
apSysMgmtExtPolicyServerConnEstTrap 1.3.6.1.4.1.9148.3.2.6.0.75	Generated when the SBC is able to re-establish a connection with an external policy server

These traps contain the following information:

- Name of the policy server as it is configured on the Oracle USM
- FQDN of the policy server cluster (This is left empty if the policy server is entered as an IP address)
- IP Address and port of the active policy server in the form <IP-Address>:<Port>
- Realm to which the policy server belongs
- Operation type (RACF/CLF) of the policy server

A connection is deemed successful when the Diameter CER/CEA transaction completes. In the case of FQDN, a connection-established trap is sent when each policy server in the top-level cluster completes its CER/CEA action.

During a reboot, a connection-down trap is sent initially. An attempt is made to connect; if the attempt is successful, a connection-established trap is sent. Upon every subsequent failed attempt by the Oracle USM to establish connection with the policy server, additional connection-down traps are sent.

During a switchover, the newly activated Oracle USM behaves in the same way as a reboot process. Initially, a connection down trap is sent. An attempt is made to connect; if the attempt is successful, a connection-established trap is sent. Upon every subsequent failed attempt by the Oracle USM to establish connection with the policy server after a switchover, additional connection-down traps are sent.

SNMP-based Application Features

In the event that a TCP connection is established but a Diameter connection is unsuccessful, the existing TCP connection is closed and a connection down trap is sent.

Alarms

When a connection down trap is sent, a minor alarm is generated. In the case of a policy server cluster, the alarm is generated when all the external policy servers in the top-level are down.

Once the TCP connection is re-established, the alarm is cleared. In a policy server cluster, only one policy server must be re-established to clear the alarm.

The following table lists an alarm associated with a failed connection to an external policy server.

Name/ID	Severity/Health Degradation	Cause(s)	Log Message	Traps Generated
APP_ALARM_EPS_RACF_CONN_FAILURE	MINOR/0	Connection to External Policy Server has been lost.	Connection to External Policy Server (RACF) has been lost!!!	apSysMgmtExtPolicyServerConnDownTrap

System Alarms

A system alarm is triggered when a condition or event happens within either the system hardware or software. Given a specific alarm, the system generates the appropriate SNMP trap. These traps include a description of the event or condition that caused the trap to be generated; or provides information associated with the alarm, such as the interface ID (ifIndex)/status or object identifier/object type integer values.

The following table maps system alarms to SNMP traps. This table includes the following information:

- alarm names
- alarm IDs
- alarm severities (including threshold values)
- alarm causes
- example log messages




In addition, this table specifies the type of traps that are generated for SNMP and the trap reference locations (the supported MIB or RFC).

Table 3: Hardware Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
FAN STOPPED	65537	<p>CRITICAL: any fan speed is <50%. Or speed of two or more fans is >50% and <75%.</p> <p>MAJOR: speed of two or more fans is > 75% and < 90%. Or speed of one fan is >50%</p>	<p>Fan speed failure.</p> <p>NOTE: If this alarm occurs, the system turns up the fan speed to the fastest possible speed.</p>	<p>fan speed: XXXX, XXXX, XXXX</p> <p>(where xxxx xxxx xxxx is the revolutions per minute (RPM) of each fan on the fan module)</p>	<p>apSyslogMessageGenerated (ap-slog.mib)</p> <p>apEnvMonStatusChange Notification (ap-env- monitor.mib)</p> <p>apSysMgmtFanTrap (ap- smgmt.mib)</p>

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
		and <75% and the other two fans are at normal speed. MINOR: speed of one fan > 75% and <90%, the other two fans are at normal speed.			
TEMPERATURE HIGH	65538	SD1: CRITICAL: >70°C MAJOR: >60°C MINOR: >50°C SD2: CRITICAL: >75°C MAJOR: >65°C MINOR: >55°C SD3: CRITICAL: >105°C MAJOR: >95°C MINOR: >85°C	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XX C (where XX.XX is the temperature in degrees)	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtTempTrap (ap-smgmt.mib)
ENVIRONMENTAL SENSOR FAILURE	65539	CRITICAL	The environmental sensor component cannot detect fan speed and temperature.	Hardware monitor failure! Unable to monitor fan speed and temperature!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonI2CFailNotification (ap-env-monitor.mib)
PLD POWER A FAILURE	65540	MINOR	Power supply A has failed.	Back Power Supply A has failed!	apSyslogMessageGenerated

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
					(ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
 Note: PLD stands for Programmable Logical Device.					
PLD POWER A UP	65541	MINOR	Power supply A is now present and functioning.	Back Power Supply A is present!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
 Note: If the system boots up with one power supply, the health score is 100, and an alarm is not generated. If another power supply is then added to that same system, this alarm is generated, but the health score is not decremented.					
PLD POWER B FAILURE	65542	MINOR	Power supply B has failed.	Back Power Supply B has failed!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
PLD POWER B UP	65543	MINOR	Power supply B is now present and functioning.	Back Power Supply B is present!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
 Note: If the system boots up with one power supply, the health score is 100, and an alarm is not generated. If another power supply is then added to that same system, this alarm is generated, but the health score is not decremented.					

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
PLD VOLTAGE ALARM 2P5V	65544	Host Processor 7455 CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v Host Processor 7457 Version 1.0 CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.35v or 1.45v to 1.6v Version 1.1 and later CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PLD VOLTAGE ALARM 3P3V	65545	Host Processor 7455 CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v Host Processor 7457 Version 1.0 CRITICAL: <1.0v or >1.6v			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
		MINOR: 1.00v to 1.35v or 1.45v to 1.6v Version 1.1 and later CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			
PLD VOLTAGE ALARM 5V	65546	Host Processor 7455 CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v Host Processor 7457 Version 1.0 CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.35v or 1.45v to 1.6v Version 1.1 and later CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			apSyslogMessageGenerat ed (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PLD VOLTAGE ALARM CPU	65547	Host Processor 7455			apSyslogMessageGenerat ed

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
		Host Processor 7457			(ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PHY0 Removed	65550	MAJOR	Physical interface card 0 was removed.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PHY0 Inserted	65552	MAJOR	Physical interface card 0 was inserted.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PHY1 Removed	65553	MAJOR	Physical interface card 1 was removed.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)
PHY1 Inserted	65554	MAJOR	Physical interface card 1 was inserted.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChange Notification (ap-env-monitor.mib)

Table 4: System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
LINK UP ALARM GIGPORT	131073	MINOR	Gigabit Ethernet interface 1 goes up.	Slot 0 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM GIGPORT	131074	MINOR	Gigabit Ethernet interface 2 goes up.	Slot 1 port 0 UP	linkUp(IETF RFC 2233)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
LINK DOWN ALARM GIGPORT	131075	MAJOR	Gigabit Ethernet interface 1 goes down.	Slot 0 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM GIGPORT	131076	MAJOR	Gigabit Ethernet interface 2 goes down.	Slot 1 port 0 DOWN	linkDown (IETF RFC 2233)
LINK UP ALARM VXINTF	131077	MINOR	Control interface 0 goes up.	wancom0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM VXINTF	131078	MINOR	Control interface 1 goes up.	wancom1 UP	linkUp (IETF RFC 2233)
LINK UP ALARM VXINTF	131079	MINOR	Control interface 2 goes up.	wancom2 UP	linkUp (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131080	MAJOR	Control interface 0 goes down.	wancom0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131081	MAJOR	Control interface 1 goes down.	wancom1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131082	MAJOR	Control interface 2 goes down.	wancom2 DOWN	linkDown (IETF RFC 2233)
LINK UP ALARM FEPORT	131083	MAJOR	Fast Ethernet slot 0, port 0 goes up.	Slot 0 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131084	MAJOR	Fast Ethernet slot 1, port 0 goes up.	Slot 1 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131085	MINOR	Fast Ethernet slot 0, port 1 goes up.	Slot 0 port 1 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131086	MINOR	Fast Ethernet slot 1, port 1 up.	Slot 1 port 1 DOWN	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131087	MINOR	Fast Ethernet slot 0, port 2 goes up.	Slot 0 port 2 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131088	MINOR	Fast Ethernet slot 1, port 2 goes up.	Slot 1 port 2 UP	linkUp (IETF RFC 2233)

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
LINK UP ALARM FEPORT	131089	MINOR	Fast Ethernet slot 0, port 3 goes up.	Slot 0 port 3 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131090	MINOR	Fast Ethernet slot 1, port 3 goes up.	Slot 1 port 3 UP	linkUp (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131091	MAJOR	Fast Ethernet slot 0, port 0 goes down.	Slot 0 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131092	MAJOR	Fast Ethernet slot 1, port 0 goes down.	Slot 1 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131093	MAJOR	Fast Ethernet slot 0, port 1 goes down.	Slot 0 port 1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131094	MAJOR	Fast Ethernet slot 1, port 1 goes down.	Slot 1 port 1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131095	MAJOR	Fast Ethernet slot 0, port 2 goes down.	Slot 0 port 2 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131096	MAJOR	Fast Ethernet slot 1, port 2 goes down.	Slot 1 port 2 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131097	MAJOR	Fast Ethernet slot 0, port 3 goes down.	Slot 0 port 3 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131098	MAJOR	Fast Ethernet slot 1, port 3 goes down.	Slot 1 port 3 DOWN	linkDown (IETF RFC 2233)
CPU UTILIZATION	131099	MINOR	CPU usage reached 90% or greater of its capacity.	CPU usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
MEMORY UTILIZATION	131100	CRITICAL	Memory usage reached 90% or greater of its capacity.	Memory usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
HEALTH SCORE	131101	MAJOR	system's health score fell below 60.	Health score X is under threshold (where X is the health score)	apSysMgmtGroupTrap (ap-smgmt.mib)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
REDUNDANT SWITCH-TO-ACTIVE	131104	CRITICAL	A state transition occurred from Standby/ BecomingStandby to BecomingActive.	Switchover, <state to state>, active peer <name of HA peer> has timed out or Switchover, <state to state>, active peer <name of HA peer> has unacceptable health (x) (where x is the health score) or Switchover, <state to state>, forced by command	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRedundancyTrap (ap-smgmt.mib)
REDUNDANT SWITCH-TO-STANDBY	131105	CRITICAL	A state transition occurred from Active/ BecomingActive to BecomingStandby/ Relinquishing Active.	Switchover, <state to state>, peer <name of HA peer> is healthier (x) than us (x) (where x is the health score) or Switchover, <state to state>, forced by command	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRedundancyTrap (ap-smgmt.mib)
REDUNDANT TIMEOUT	131106	MAJOR	An HA system peer was not heard from within the configured silence window.	Peer <name of HA peer> timed out in state x, my state is x (where x is the state (e.g., BecomingStandby))	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRedundancyTrap (ap-smgmt.mib)
REDUNDANT OUT OF SERVICE	131107	CRITICAL	Unable to synchronize	Unable to synchronize	apSyslogMessageGenerated

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
			with Active HA system peer within BecomingStandby timeout.	with Active redundant peer within BecomingStandby timeout, going OutOfService or activate-config failed, process busy or activate-config failed, must do save-config before activating. or activate-config failed, could not get current config version from file or activate-config failed, could not set running config version to file.	(ap-slog.mib) apSysMgmtRedundancyTrap (ap-smgmt.mib)
 Note: The activate-config failed log message appears for those cases in which the execution of the activate config command failed on the standby SBC.					
SYSTEM TASK SUSPENDED	131108	CRITICAL	A system task (process) suspends or fails.	Task X suspended, which decremented health by 75! (where X is the task/process name)	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtTaskSuspendTrap (ap-smgmt.mib)

Table 5: Media Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaOutOfMemory (ap-smgmt.mib)
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtUnknownRealm (ap-smgmt.mib)
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaBandwidthTrap (ap-smgmt.mib)
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaPortsTrap (ap-smgmt.mib)

Table 6: Network Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
GATEWAY UNREACHABLE	dynamicID	MAJOR	The SBC lost ARP connectivity to a front interface gateway.	gateway X.X.X.X unreachable on slot Y port Z subport ZZ (where X.X.X.X is the IPv4 address of the front interface gateway, Y is the front interface slot	apSysMgmtGatewayUnreachableTrap (ap-smgmt.mib)

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
				number, Z is the front interface port number, and ZZ is the subport ID)	


 **Note:** The value of this alarm ID is dynamic. That is, it changes based on a numbers of factors, but the total alarm ID range falls between 196608 and 262143. The alarm ID is calculated based on the compilation of the following information: a hexadecimal number that represents the VLAN ID and the front interface port/slot numbers.

Table 7: Application Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
RADIUS ACCOUNTING CONNECTION DOWN	327681	CRITICAL: if all enabled and configured Remote Authentication Dial-in User Service (RADIUS) accounting server connections have timed-out without response from the RADIUS server MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server.	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost! Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost! Check accounting status for more details.	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRadiusDown Trap (ap-smgmt.mib)
ENUM SERVER STATUS	XX	CRITICAL: All ENUM	The enabled connections to	CRITICAL: All ENUM Servers	apSysMgmtENUMStatusChangeTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
New to Release C5.0		servers are unreachable MAJOR: Some ENUM servers are unreachable	ENUM servers have been lost.	are currently unreachable! MAJOR: One or more ENUM Servers are currently unreachable!	(ap-smgmt.mib)

Table 8: Configuration Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby SBC peer operating as part of an HA pair.	save-config failed on targetName!/ code full, config sync stopped! or save-config failed on targetName!/ code full, config sync stopped! (where the targetName is the target name (tn) configured in the boot parameters)	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtCfgSaveFailTrap (ap-smgmt.mib)

Table 9: License Alarm

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
LICENSE APPROACH CAPACITY	50004	MAJOR	Total session count is approaching the license capacity allowed (98% or higher) This alarm is cleared when total sessions is less than 90%		apSyslogMessageGenerated (ap-slog.mib) apLicenseApproachingCapacityNotification (ap-smgmt.mib)

System Alarms

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
			of license capacity.		

For additional information about system alarms for the components of the system, refer to the Alarms section of the Monitoring via the ACLI chapter of the Administration and Configuration Guide for the ACLI.

Alarm Severities

The system architecture includes five levels of alarm severity. These levels have been designated so that the system can take action that is appropriate to the situation triggering the alarm.

Alarm Severity	Description
Emergency	Requires immediate attention. If you do not attend to this condition immediately, there will be physical, permanent, and irreparable damage to your system.
Critical	System is inoperable, causing a complete loss of service in a production environment. Requires attention as soon as it is noted.
Major	Functionality has been seriously compromised. This situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your system will suffer no physical harm, but it will cease to function.
Minor	Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. You should attend to this type of alarm as soon as possible in order to keep your system operating properly.
Warning	Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your system operating properly. For example, this type of alarm might indicate the system is running low on bandwidth and you may need to contact your Oracle customer support representative to arrange for an upgrade.

Glossary

