Oracle® Communications Session Border Controller

MIB Guide

Release S-Cz9.3.0
F92214-09
June 2026

Oracle Communications Session Border Controller MIB Guide, Release S-Cz9.3.0

F92214-09

Copyright © 2024, 2026, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

ADD THE FIRST PARAGRAPH HERE.

ADD THE NEXT PARAGRAPH HERE.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Contents

About this Guide

My Oracle Support i

Revision History

1 SNMP Configuration

Overview 1
- Basic SNMP Parameters 1
- SNMPv1v2 Community Configuration 2
- SNMPv1v2 Trap Receiver Configuration 2
- SNMP IPv6 Support 2

SNMP Configuration Overview 2
Configure SNMP System and Agent Parameters 2
SNMPv3 3
- SNMPv3 Users 4
  - Configure an SNMPv3 User Identity 4
- SNMPv3 User Groups 5
  - Configure SNMPv3 User Group 5
- SNMPv3 Manager Access 7
  - Configure SNMPv3 Manager Access 7
- SNMPv3 Views 8
  - Specify SNMPv3 View Access to a MIB 8

SNMPv1 and SNMPv2 9
- SNMPv1v2 Community Configuration 9
  - Configure the SNMP Community 9
- SNMPv1v2 Trap Receiver Configuration 10
  - Configure Trap Receivers 10

Specify an NMS for EMS Generated Traps 11
Enabling Administrative Trap Types 12
Enabling Media Supervision Traps 13
View SNMP Address, Statistics and User Information 13

Copyright © 2024, 2026, Oracle and/or its affiliates.

Consideration for HA Nodes 15

2 Introduction to MIBs and Traps

About MIBs 1
Object Identifiers and Instance IDs 1
MIB Tree Structure 2
Managed Objects 2
Scalar MIB Objects 2
Table MIB Objects 2
SNMP Traps 2
MIBs Supported 2
Standard MIBS 3
Enterprise MIBs 3
Traps 4
Standard Traps 4
Enterprise Traps 5
apSyslog Traps (ap-slog.mib) 5
apSysMgmt Traps (ap-smgmt.mib) 5
apSwinventory Traps (ap-swinventory.mib) 15
apEnvMon Traps (ap-env-monitor.mib) 15
apLicense Traps (ap-license.mib) 15
apSecurity Traps (ap-security.mib) 15
apSLB Traps (ap-slb.mib) 18
apH323 Traps (ap-h323.mib) 19
apDiameter Traps (ap-diameter.mib) 19
apDnsAlg Traps (ap-dnsalg.mib) 19
apSip Traps (ap-sip.mib) 20
apApps Traps (ap-apps.mib) 21
apAclDropOverThresholdTrap Objects 21
apUSBC Traps (ap-usbcsys.mib) 21
Specify an NMS for EMS Generated Traps 22
Persistent indexing of SNMP Tables 23
Log Levels and syslog Level Severities 24
Log Levels 24
syslog Level Severities 24
Mapping Trap Filter Levels to syslog and Alarm Severities 25
Platform sysObjectIDs 26

3 Standard SNMP GET Requests

Interfaces Object 1

Copyright © 2024, 2026, Oracle and/or its affiliates.

Interface Table 1
Interface Description in MIB 4
ifXTable Table 6
ip Object 10
ipAddrTable Table 13
icmp Object 14
TCP Object 15
tcpConnTable Table 17
UDP Object 17
System Object 18
Object Resource Information Object 20
SNMP Object 20
Physical Entity Table 21

4 Enterprise SNMP GET Requests

Applications MIB (ap-apps.mib) 1
apAppsENUMServerStatusTable Table 1
apAppsDnsServerStatusTable 1
apAppsStirMIBObjects Table 2
apAppsStirServerTable 3
apAppsStirServerTable 3
apAppsStirAgentStatsTable 5
apAppsStirSipInterfaceStatsTable 8
apAppsStirRealmStatsTable 10
apAppsStirSystemStatsTable 12
apAppsNSEPRealmTable 14
apAppsLatestPeakLicenseUsage 16
apDosThresholdCountersGroup 18
MSRP MIB Objects 19
Codec and Transcoding MIB (ap-codec.mib) 35
apCodecPairStatsTable 38
Transcoding Capacity in System Management MIB (ap-smgmt.mib) 39
Diameter MIB (ap-diameter.mib) 40
DNS ALG MIB (ap-dnsalg.mib) 41
apDNSALGServerStatusTable 41
apDNSALGStatsTable 42
Environment Monitor MIB (ap-env-monitor.mib) 43
H.323 MIB (ap-h323.mib) 47
License MIB (ap-license.mib) 47
Security MIB (ap-security.mib) 49
apSecurityCertificateTable 50

Copyright © 2024, 2026, Oracle and/or its affiliates.

SIP MIB (ap-sip.mib) 51
Realm Based SIP Method Statistics 58
syslog MIB (ap-slog.mib) 62
System Management MIB (ap-smgmt.mib) 64
Notes on ENUM Server Names 84
Software Inventory MIB (ap-swinventory.mib) 85
Multicore Monitoring MIB (ap-usbcsys.mib) 86
apUsbcSysDPDKObjects 89
apUsbcSysScalingObjects 89

5 SNMP-based Application Features

SNMP Reporting of Message Rate Statistics 1
apSIPRateIntfStatsTable 1
apSIPRateAgentStatsTable 1
apDnsAlgServerRateStatsTable 2
apEnumServerRateStatsTable 2
SNMP Reporting of Message Data Counters 2
Call Duration Counters for SNMP Retrieval 2
Local and Remote Call Termination (BYE) Counters for SNMP Retrieval 2
SIP Method Counters for SNMP Retrieval 3
SRVCC Objects for SNMP Retrieval 3
Rx Policy Server Objects for SNMP Retrieval 3
IKE Session Agent Objects for SNMP Retrieval 4
IMS-AKA Session Agent Objects for SNMP Retrieval 4
SRTP Session Agent Objects for SNMP Retrieval 4
Transcoding Load Objects for SNMP Retrieval 4
FQDN-resolved Session Agent Statistics SNMP Retrieval 5
CAC Utilization Statistics via SNMP 6
SNMP Get for CAC Utilization 6
CAC Utilization Traps 8
External Policy Server Connection Status Reporting 9

A Alarms Table

Alarm Severities A-20

Copyright © 2024, 2026, Oracle and/or its affiliates.

About this Guide

The Oracle Communications Session Border Controller MIB Reference Guide provides information about the following:

- Management Information Base (MIBs)
- Acme Packet'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
- 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. Appendix A contains several trap examples. Appendix B contains the location of documents where you can obtain more information.

Documentation Set

The following table describes the documentation set for this release.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Revision History

The following table provides the revision history for this document.

Date	Description
March 2024	• Initial release
October 2024	• Adds NTP SERVER alarm to Appendix A. • Fix apAppsStirMIBObjects tables. • Adds features for S-Cz9.3.0p3. • Adds OID numbers for CAC utilization traps. • Corrects three apSigRealmStats statistics descriptions. • Removes erroneous references to the deprecated TSCF feature.
December 2024	• Explains the use of the ConfigId and Index values in the apSecurityCertificateTable. • Updates Alarm Tables for accuracy.
February 2025	• Corrects trap description for apSipRecRecDlgFailNotify.
August 2025	• Adds feature for S-Cz9.3.0p8.
November 2025	• Updates description for apSysMgmtNTPServerUnreachableClearTrap.
January 2026	• Corrects the description for apCombinedStatsTotalSessionsOutbound in System Management MIB (ap-mgmt.mib). • Fixes various typographical errors.
June 2026	• Adds audit log alarms to Alarm Table.

Copyright © 2024, 2026, Oracle and/or its affiliates.

1

SNMP Configuration

The Simple Network Management Protocol (SNMP) allows you to monitor system and health conditions for an Oracle Communications Session Border Controller (SBC) through an external network management (northbound) system, such as the Oracle Communications Session Delivery Manager or an SNMP manager. The system supports SNMPv3, v2 or v1 to interface with a range of external NMS systems.

> **Note**
>
> SNMP configuration is not required for the service operation of the SBC, but is performed on the majority of systems. Most network administrators are familiar with, or become familiar with SNMP.

Overview

SNMP is comprised of three groups of settings on a Oracle Communications Session Border Controller (SBC). These settings includes:

- System-wide configuration
- Access Configuration, including:
  - SNMPv1v2 Community Settings
  - SNMP IPv3 Authentication, Encryption and Filter Settings
- Trap Receiver Configuration

You can configure an SNMP manager to query the SBC or be a trap receiver. You can configure an SNMP manager to perform both functions by configuring two **snmp-address-entry** elements that have the same IP address, but different names.

Basic SNMP Parameters

The Oracle Communications Session Border Controller (SBC) includes several parameters that control basic SNMP functionality and are common to both SNMPv1v2 and SNMPv3 deployments. The MIB-related elements are for informational purposes, and are helpful if set. The remainder of the parameters determine if certain SBC events are reported to the SNMP system.

System-wide configurations including:

- Enable SNMP operation (enabled by default)
- System-related contact information
- Enable the SBC to send information within traps, including:
  - syslog
  - authentication
  - environmental

Copyright © 2024, 2026, Oracle and/or its affiliates.

- system monitoring

SNMPv1v2 Community Configuration

SNMPv1v2 community configuration consists of setting a community name, an access mode and IP addresses of the servers. Configurations accept multiple addresses. You can provide both READ and WRITE mode to a single manager by creating two objects with different names and access modes, but the same IP address.

Determine your planned name, address type (IPv4 vs IPv6) and modes before starting.

SNMPv1v2 Trap Receiver Configuration

Determine the community, addressing (IPv4 or IPv6) and filter level for each trap receiver before configuration.

> **Note**
>
> Configure each Oracle Communications Session Delivery Manager that manages an SBC as trap receivers on the SBC.

SNMP IPv6 Support

The Oracle Communications Session Border Controller supports IPv6 addressing. This includes trap receiver configuration, statistics, and information within traps that use varbind data types (InetAddress and InetAddressType).

SNMP Configuration Overview

Use the to configure SNMP on the Oracle Communications Session Border Controller:

1. Configure SNMP System and Agent Parameters.
2. Configure SNMPv3 or SNMPv2.
3. Enable SNMP Traps.

Configure SNMP System and Agent Parameters

High level SNMP identification is configured by all SNMP users. This information includes system-level management Information, system contact information, system name and location information and is applicable to both SNMPv1v2 and SNMPv3 deployments. The *Oracle® Communications Session Border Controller MIB Reference Guide* includes detail on SNMP data.

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

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


Copyright © 2024, 2026, Oracle and/or its affiliates.

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

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

3. **mib-system-contact**—Specifies contact information that is used within SBC MIB transactions. This value is a textual identification and usually contains information about the company system contact person.

4. **mib-system-name**—Specifies the identity of this SBC that is presented within MIB transactions, which is the FQDN of the node.

5. **mib-system-location**—Specifies the physical location of the SBC that is reported within MIB transactions. This parameter is reported when an SNMP GET is issued by the NMS for the MIB-II sysLocation variable. This parameter has no direct relation to the location field in the system configuration element.

6. **snmp-agent-mode** —Select the operating mode of the SNMP agent.
   - **v1v2**—(Default) The SNMP agent supports SNMPv1 and SNMPv2. Configure the The **snmp-community** and **trap-receiver** elements only.
   - **v3**—The SNMP agent supports SNMPv3, but can also support SNMPv2 through **snmp-user-group** element configuration.

   > **Note**
   >
   > To create a v2 **snmp-user-group**, you configure the **mp-model** parameter to v1v2 and leave the **community-string** parameter blank. The system then matches hosts' SNMP version 2 community strings with the **user-list** parameter value. You also configure **snmp-user-entry** and **snmp-address-entry** elements to complete your v2 group configuration.

7. **snmp-engine-id-suffix**—Uniquely identifies the SNMP Engine by specifying a unique suffix for the SNMPEngineID. This attribute is optional.
8. **snmp-rate-limit**—Set the rate limit for SNMP traffic to prevent SNMP from interfering with service traffic. The range is from 0 to 9999 packets per second. The default is zero, which applies no limit.
9. **lower-snmp-priority**—This option allows you to lower the priority of the SNMP processing task to prevent SNMP from interfering with service processing.

```
ORACLE(system-config)options +lower-snmp-priority=enabled
```

   If you type the option without the plus sign, you overwrite any previously configured options. To append the new option to the options list, prepend the new option with a plus sign as shown in the previous example.

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

SNMPv3

The Oracle Communications Session Border Controller supports SNMPv3 by default. To secure your SNMPv3 system, you must configure SNMP users and groups, SNMP managers, and view access to MIB trees. SNMPv3 provides the SNMP agent and SNMP Network

Copyright © 2024, 2026, Oracle and/or its affiliates.

Management System (NMS) with protocol security enhancements used to protect your system against a variety of attacks, such as increased authentication, privacy, MIB object access control and trap filtering capabilities.

SNMPv3 Users

An identity must be created for an SNMPv3 user to specify their name, security protocol choices, passwords for secure authentication and privacy, and the ability to receive secured traps. You configure SNMPv3 users to protect your SNMPv3 system from any unauthorized SNMP agent that uses message capture and replay or a network traffic source that uses an incorrect password or security level.

Configure an SNMPv3 User Identity

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

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

2. Type **snmp-user-entry** and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters used to create an identity for an SNMPv3 user.

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

3. **user-name**—Enter the name of the user authorized for retrieving SNMPv3 traps.

   Values:

   - <user name string>—that is 1 to 24 characters.

4. **auth-protocol**—Specify the authentication protocol.
   - **sha256**—HMAC-SHA2-256 authentication protocol.
   - **sha512**—(Default) HMAC-SHA2-512 authentication protocol.
5. **priv-protocol**—Specify the privacy algorithm.
   - **aes128**—Authenticates using the AES128 algorithm.
6. **auth-password**—Enter the authorization password for this user.

   Value:

   - <password-string>— that is 6 to 64 characters.

7. **priv-password**—Enter the privilege password for this user.

   Value:

   - <password-string>— that is 6 to 64 characters.

8. **address-list**—Enter the host IP address(es) that are associated with this user.
   - <address-string>— that is 1 to 24 characters. You can specify multiple address list names by enclosing them within brackets "()".
9. Type **done** to save your configuration.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Repeat the previous steps if you need to add more SNMPv3 users.

SNMPv3 User Groups

A group of SNMPv3 users can be specified for easy management and access control.

Each SNMPv3 user can be configured to belong to a specific security model and security level. You can choose either the SNMPv1 and v2 model or the SNMPv3 model (which is selected for you by default). When you assign a security level to a group, this level is consistent for all users within this group and the security level can be used across multiple SBC devices. Also, these security levels determine how data is encrypted to prevent information leaks and stop an unauthorized user from scrambling the contents of an SNMP packet.

The following security levels can be assigned to an SNMPv3 group:

- The default authPriv security level specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols and the privacy password is encrypted using the AES128 authentication protocol. Using this security level provides user authentication and ensures message privacy so that the trap is not tampered with during transit.
- The noAuthNoPriv security level specifies that the user group is authenticated by a string match of the user name and requires no authorization and no privacy similar to SNMPv1 and SNMPv2.
- The authNoPriv security level specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols to produce a key used to authenticate the trap and ensure the identity of the user.

You can also configure an SNMPv3 user group to allow the co-existence of multiple SNMP message version types at the same time, specify a list of users belonging to the group, and assign the group privilege to read, write, and add SNMP objects and receive trap notifications.

Configure SNMPv3 User Group

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

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

2. Type **snmp-group-entry** and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters used to configure a group of users that belong to a particular security model who can read, write, and add SNMP objects and receive trap notifications.

   ```
   ORACLE(system)# snmp-group-entry
   ORACLE(snmp-group-entry)#
   ```

3. **name** <group-name-string>—Specify a group name that is 1 to 24 characters for the SNMPv3 group name.
4. **mp-model**—Specify the SNMP message processing model.

   Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- **v1v2**—The SNMPv1 and SNMPv2 model.
- **v3**—The SNMPv3 model (default).

> **Note**
>
> If the **mp-model** parameter is specified with the **v1v2** value, the **community-string** parameter (not configured) defines a coexistence configuration where SNMP version 2 messages with the community string from the hosts is indicated by the **user-list** parameter, and the corresponding **snmp-user-entry** and **snmp-address-entry** elements are accepted.

5. **security-level**—Specify the security level of the SNMP group, which are consistent for the user and can be used across multiple SBC devices.
   - **noAuthNoPriv**—This value specifies that the user group is authenticated by a string match of the user name and requires no authorization and no privacy similar to SNMPv1 and SNMPv2. This value is specified with the **mp-model** parameter and its **v1v2** value and can only be used with the **community-string** parameter not specified.
   - **authNoPriv**—This value specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols to produce a key used to authenticate the trap and ensure the identity of the user.
   - **authPriv**—This default value specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols and the privacy password is encrypted using the AES128 algorithm. Using this security level provides user authentication and ensures message privacy so that the trap is not tampered with during transit. This value is specified with the SNMP **mp-model** parameter and its **v3** value.

   > **Note**
   >
   > If there is a switchover on a high-availability SBC device, the SNMPEngineID varies and your network management system (NMS) should be updated with the SNMPEngineID of the standby SBC device.
6. **community-string** <community-string>—Specify the community name that is 1 to 24 characters to allow the co-existence of multiple SNMP message version types at the same time for this security group.
7. **user-list** <user-name string>—Specify a name for the user list that is 1 to 24 characters and must match the name of the **user-name** parameter of the **snmp-user-entry** element to configure user host names.
8. **read-view** <group-read-view-string>—Specify the name of the SNMP group's read view for a collection of MIB subtrees that can be 1 to 24 characters.
9. **write-view** <group-write-view-string>—Specify the name of the SNMP group's write view for a collection of MIB subtrees that can be 1 to 24 characters.
10. **notify-view** <group-notify-view-string>—Specify the name of the SNMP group's trap notification view for a collection of MIB subtrees that can be 1 to 24 characters.
11. Type **done** to save your configuration.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Repeat the previous steps if you need to add more groups.

SNMPv3 Manager Access

You identify an SNMPv3 manager by adding its name and IP address to authenticate and interpret traffic, such as secure traps that it receives from the SNMP agent device (SBC). This traffic is kept private during transit by using time stamps and boot counts to protect against delayed packets.

Configure SNMPv3 Manager Access

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

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

2. Type **snmp-address-entry** and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters used to identify the SNMP manager.

   ```
   ORACLE(system-config)# snmp-address-entry
   ORACLE(snmp-address-entry)#
   ```

3. **name**—Specify a name to be referenced when operating with this manager.

   Value:

   - <management-hostname-string>—that is 1 to 24 characters and is used to specify the name for the SNMPv3 target IP address.

4. **address**—Specify the IP address of the manager. The parameter requires an IP address followed by either the mask, in number of bits, or the port number.

   ```
   ORACLE(snmp-address-entry)# <ip-address> [/<num-bits>][:port]
   ```

   Values:

   - <ip-address>—IP address in IPv4 or IPv6 standard format.
   - /<num-bits>—specifies the mask, in number of bits, used to route to the address.
   - <:port>—this optional parameter to enter a subnetwork (subnet) mask. The default subnet mask is 255.255.255.255. Set this value if the manager is a trap-receiver. Do not set this value if the manager is performing queries.

5. **trap-filter-level**— Set this value if the manager is a trap-receiver. Select a priority level that is equal to or lower than the value of the filter-level. Do not set this value if the manager is performing queries.

   Values:

   - **"" (Default)**—The field's setting is blank. The user is not configured to receive any trap.
   - **ALL**—A user can view all trap conditions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- **Minor**—A user can view trap error conditions that exist on a device.
- **Major**—A user can view trap critical conditions that exist on a device.
- **Critical**—A user can view trap conditions that require an immediate action for a device.

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

> **Note**
>
> Repeat the previous steps if you need to add more SNMPv3 target IP addresses.

SNMPv3 Views

SNMPv3 utilizes a view-access-control model (VACM) for checking whether a specific type of access to a specific managed object is allowed through the SNMPv3. You can configure individual parameters used to include or exclude view access to single or multiple MIB OID nodes for an SNMPv3 view name.

Specify SNMPv3 View Access to a MIB

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

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

2. Type **snmp-view-entry** and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters used to include or exclude view access.

```
ORACLE(system)# snmp-view-entry
ORACLE(snmp-view-entry)#
```

3. **name** Specify the SNMPv3 view name.

   Valid value:

   - <SNMP-view-name-string>—that is 1 to 24 characters.

4. **included-list**— Use this parameter to include view access to a MIB OID subtree or multiple OID subtrees for this SNMPv3 view name.

   Valid value:

   - <OID(s)>—Object Identifier number separated by a dot (.), in which each subsequent number is a sub-identifier. Each subtree OID starts with the prefix 1.3.6.1.
     For example:
     - 1.3.6.1.6
     - (1.3.6.1.2 1.3.6.1.4.1.9148) - You can enter multiple values enclosed in parenthesis and separated by space or comma.

5. Repeat the previous step if you need to include or exclude additional views.

6. **excluded-list**—Use this parameter to exclude view access to a MIB OID node for this SNMPv3 view name.

   Valid value:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- <OID(s)>— Object Identifier number separated by a dot (.), in which each subsequent number is a sub-identifier. Each subtree OID starts with the prefix 1.3.6.1.
  For example:
  - 1.3.6.1.4.1.9148.3.3
  - (1.3.6.1.4.1.9148.3.3 1.3.6.1.4.1.9148.3.5) - You can enter multiple values enclosed in parenthesis and separated by space or comma.

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

> **Note**
>
> Repeat the previous steps if you need to add more SNMPv3 views.

SNMPv1 and SNMPv2

Use this task if you selected **v1v2** for the **snmp-agent-mode** parameter in the **system-config** element to configure SNMPv1 and SNMPv2, which includes the configuration of the SNMP community and the trap receiver.

SNMPv1v2 Community Configuration

SNMPv1v2 community configuration consists of setting a community name, an access mode and IP addresses of the servers. Configurations accept multiple addresses. You can provide both READ and WRITE mode to a single manager by creating two objects with different names and access modes, but the same IP address.

Determine your planned name, address type (IPv4 vs IPv6) and modes before starting.

Configure the SNMP Community

1. Access the **snmp-community** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# snmp-community
ORACLE(snmp-community)#
```

2. Type **community-name** to specify the SNMP community name of an active community where this Oracle Communications Session Border Controller can send or receive SNMP information.

3. **access-mode**—Set the access level for all network management servers (NMSs) defined within this SNMP community. The access level determines the permissions that other NMS hosts can wield over this Oracle Communications Session Border Controller. The default is **read-only**. The valid values are:
   - **read-only**—allows GET requests.
   - **read-write**—unsupported.

4. **ip-addresses**—Specify a valid IPv4 or IPv6 address within this SNMP community that corresponds to one or more NMS that monitors or configures this SBC. If you are

Copyright © 2024, 2026, Oracle and/or its affiliates.

specifying more than one IP address, separate each IP address with a space and enclose with parenthesis.

```
ORACLE#(snmp-community)ip-addresses (10.1.1.1 10.2.2.2)
```

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

SNMPv1v2 Trap Receiver Configuration

Determine the community, addressing (IPv4 or IPv6) and filter level for each trap receiver before configuration.

> **Note**
>
> Configure each Oracle Communications Session Delivery Manager that manages an SBC as trap receivers on the SBC.

Configure 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 specify a trap receiver.

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

ORACLE(trap-receiver)#
```

3. **ip-address** — Set the IPv4 or IPv6 address of an authorized network management system (NMS) where traps are sent. If you do not specify a port number, the default SNMP trap port of **162** is be used.
4. **filter-level** — Set the filter level threshold that indicates the severity level at which a trap is to be sent to this particular trap receiver. The default for this parameter is critical.

   Example: When a trap with a severity level of **critical** is generated, the SNMP agent sends this trap only to NMSs that are configured in a trap-receiver element and have a **filter-level** value of **critical**.

   The following table maps Syslog and SNMP alarms to trap receiver filter levels.

Filter Level	Syslog Severity Level	(SNMP) Alarm Severity Level
Critical	Emergency (1) Critical (2)	Emergency Critical
Major	Emergency (1) Critical (2) Major (3)	Emergency Critical Major

Copyright © 2024, 2026, Oracle and/or its affiliates.

Filter Level	Syslog Severity Level	(SNMP) Alarm Severity Level
Minor	Emergency (1) Critical (2)	Emergency Critical
	Major (3)	Major
	Minor (4)	Minor
All	Emergency (1) Critical (2)	Emergency Critical
	Major (3)	Major
	Minor (4)	Minor
	Warning (5)	Warning
	Notice (6)	
	Info (7)	
	Trace (8)	
	Debug (9)	

When configuring the trap-receiver element for use with Oracle Communications Session Element Manager systems, Oracle recommends that the value of **filter-level** be set to **All** for that configuration element that includes those servers.

5. **community-name** — Set the community name to which this trap receiver belongs. This community must be defined in the SNMP community element.
6. Type **done** to save your configuration.

Specify an NMS for EMS Generated Traps

You must configure a northbound network management server (NMS) such as an SNMP management system as the receiver of element manager system (EMS) traps. An EMS, such as the Session Element Manager, generates the (EMS MIB) traps shown in the table below when it detects the following conditions:

- There is a failure to discover or rediscover a SBC configuration.
- There is a failure to save a SBC configuration.
- There is a failure to activate a SBC configuration.
- There are missing components when validating a SBC configuration.
- The node status changes from reachable to unreachable.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap Name	Description
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.
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.

Enabling Administrative Trap Types

Use this task to enable traps for certain Oracle Communications Session Border Controller (SBC) events that are reported to a network management system. These settings are applicable to both SNMPv1v2 and SNMPv3 deployments. The SBC does not require you to enable traps other than those in the following steps.

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
   ORACLE(system-config)#
   ```

3. **enable-snmp-monitor-traps**—When this parameter is enabled, the Oracle Communications Session Border Controller generates traps with unique trap-IDs for each syslog event. If this parameter is disabled , a single trap-ID is used for all events, with different values in the description string. The default is **disabled**. The valid values are:
   - enabled | disabled
4. **enable-snmp-auth-traps**—Set whether the SNMP authentication traps are enabled. If an SNMP request fails authentication because of SNMP community mismatch, the SNMP request will be rejected. This field determines if an SNMP trap will be sent in response to the authentication failure. The default is **disabled**. Valid values for this parameter are:
   - **enabled** | **disabled**
5. **enable-env-monitor-traps**—Set whether or not the SNMP environment monitor traps are enabled. Environment traps include main board PROM temperature, power supplies, fan speeds, etc. The default is **disabled**. Valid values for this parameter are:
   - enabled | disabled
6. **enable-snmp-syslog-notify**—Set whether SNMP traps are sent when the system generates an alarm message. The SNMP agent sends a trap when an alarm is generated if the following conditions are met:
   - SNMP is enabled.
   - This field is enabled.
   - The syslog severity level is equal to or greater than the severity level configured in the SNMP Syslog Level field.

Copyright © 2024, 2026, Oracle and/or its affiliates.

The default is **disabled**. Valid values are:

- **enabled** | **disabled**

7. **snmp-syslog-his-table-length**—Set the length of the syslog trap history table. When a syslog message that meets the SNMP syslog level field criteria is generated and SNMP is enabled, the SNMP agent adds that message to a history table. This parameter indicates the number of entries the table can contain. The default is **1**. The valid range is:
   - Minimum—1
   - Maximum—500

     Once the last table entry is filled, the oldest entry will be overwritten with a new entry.
8. **snmp-syslog-level**—Set the log severity level threshold that will cause the syslog trap to be sent to an NMS. When this criteria is met and the appropriate SNMP trap is sent, an entry is written to the SNMP Syslog History Table. The default is **warning**. The following are valid values:
   - emergency | critical | major | minor | warning | notice | info | trace | debug | detail

Enabling Media Supervision Traps

The Oracle Communications Session Border Controller (SBC) sends the following media supervision trap when functioning as a border gateway and the media supervision timer expires:

```
apSysMgmtMediaSupervisionTimerExpTrap    NOTIFICATION-TYPE
      OBJECTS          { apSysMgmtCallId }
      STATUS            current
      DESCRIPTION
            " The trap will be generated when a media supervision timer
            has expired.  This behavior is disabled by default but may
            be enabled by changing the 'media-supervision-traps'
            parameter of the 'media-manager' configuration element.  The
            included object is the call identifer for the call which had
            the timer expire."
      ::= { apSystemManagementMonitors 34 }
```

> **Note**
>
> The system does not send this trap when functioning as an integrated SBC.

The media supervision trap is disabled by default. You can enable the trap by changing the **media-supervision-traps** parameter to **enabled** in the media-manager configuration element.

View SNMP Address, Statistics and User Information

The user can view real-time information on agent traffic using the **show snmp-info** command.

show snmp-info address—View the traffic to and from the SNMPv3 addresses that you configured in Superuser mode. For example:

```
<device># show snmp-info address
snmp-address-entry
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
        name              : acme82
        address           : 172.30.0.82:161
        mask              : 255.255.255.255
        total requests in : 3
        total replies out : 3
        total traps out   : 1
snmp-address-entry
        name              : acmepc58
        address           : 10.1.20.58:161
        mask              : 255.255.255.255
        total requests in : 0
        total replies out : 0
        total traps out   : 1
```

show snmp-info statistics—View the SNMP agent mode and statistics for the SNMP engine in Superuser mode. For example:

```
<device># show snmp-info statistics
SNMP Agent Mode           : V3
SNMP Engine ID Base          : 0x800023bc05ac1e50e8
SNMP Engine ID Suffix     :
SNMP Engine ID            : 0x800023bc05ac1e50e8
SNMP Engine Boots         : 622
Total packets in          : 17
Total packets out         : 10
Total traps out           : 2
Unknown security models   : 0
Invalid Messsages         : 0
Unsupported SecLevels     : 0
Not In Time Windows       : 0
Unknown User Names        : 1
Unknown EngineIDs         : 3
Stats Wrong Digests       : 0
Decryption Errors         : 0
```

show snmp-info snmp-user—View information and traffic associated with SNMP users in Superuser mode. For example:

```
<device># show snmp-info snmp-user
snmp-user-entry
        name              : snmpuser1
        auth-protocol     :
        auth-password     :
        priv-protocol     :
        priv-password     :
        address-list      : address1 address2
        total requests in : 0
        total get reqs in : 0
        total next reqs in: 0
        total replies out : 0
        total traps out   : 0
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

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 Communications Session Border Controller.

Copyright © 2024, 2026, Oracle and/or its affiliates.

2

Introduction to MIBs and Traps

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Tree Structure

MIBs are arranged in a tree-structured fashion, similar in many ways to a operating system directory structure of files.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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
- rfc4113-udp.mib

Enterprise MIBs

Oracle provides the following enterprise MIBs:

MIB Name	Description
ap-agentcapability.mib	Details the SNMP agent's capabilities that includes support for different modules: • 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, 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Name	Description
ap-slog.mib	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. If the following conditions are present, the SNMP agent sends an SNMP trap when a message is sent to the syslog system: • 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. No trap is sent under the following conditions: • 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap Name	Description
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.

Enterprise Traps

The following sections list traps available on the Oracle Communications Session Border Controller. Traps are divided by the mib file they are contained within.

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 `ap-smgmt.mib` includes the following traps, which are generally used for system management.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
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.
apSysMgmtFanTrap 1.3.6.1.4.1.9148.3.2.6.0.3	Generated if a fan unit speed falls below the monitoring level.
apSysMgmtGatewayUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.10	Generated if the gateway specified becomes unreachable by the system.
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.
apSysMgmtAuthenticationFailedTrap: 1.3.6.1.4.1.9148.3.2.6.0.16	Generated upon an unsuccessful login attempt. The trap includes the following information: • level (login, user, priv, shell, li-admin, provisioners) • protocol (console, telnet, ftp, ssh, sftp, http, https) • origin (<IP address>:<port>)
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.
apSysMgmtENUMStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.27	Generated if the reachability status of an ENUM server changes; contains: • apENUMConfigName • apENUMServerIpAddress • apENUMServerStatus
apSysMgmtCollectorPushSuccessTrap: 1.3.6.1.4.1.9148.3.2.6.0.44	Generated when the collector successfully completes a push operation.
apSysMgmtGatewaySynchronizedTrap: 1.3.6.1.4.1.9148.3.2.6.0.49	Generated when the default gateway is synchronized in the ARP table.
apSysMgmtCallRecordingStateChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.50	Generated when a call recording server changes state.
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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSysMgmtAdminAuditLogFullTrap: 1.3.6.1.4.1.9148.3.2.6.0.58	Generated when one of the audit logs full threshold is met: • 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.
apSysMgmtCdrFileDeleteTrap 1.3.6.1.4.1.9148.3.2.6.0.70	Generated when a CDR file is deleted because of lack of space on the partition or the drive exceeds the number of files specified.
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.
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.
apSysMgmtH323InitFailTrap 1.3.6.1.4.1.9148.3.2.6.0.12	Generated if an H.323 stack has failed to initialize properly and has been terminated.
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. • 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 constraintExceeded (4) (OID 1.3.6.1.4.1.9148.3.2.5.27)

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
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. • apSysMgmtNTPServer—Server that is or was formerly unreachable (OID 1.3.6.1.4.1.9148.3.2.5.31)
apSysMgmtNTPServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.31	Generated when an NTP server deemed unreachable subsequently becomes reachable or the NTP server has been removed or unconfigured.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
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.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSysMgmtTacacsDownTrap 1.3.6.1.4.1.9148.3.2.6.0.78	Generated when a TACACS+ server becomes unreachable.
apSysMgmtTacacsDownClearTrap 1.3.6.1.4.1.9148.3.2.6.0.79	Generated when a TACACS+ server that was unreachable becomes reachable.
apSysMgmtRealmIcmpFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.51	Generated when ICMP heartbeat failure occurs.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSysMgmtRealmIcmpFailureClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.52	Generated when ICMP heartbeat failure clears.
apSysMgmtRegCacheThresholdTrap: 1.3.6.1.4.1.9148.3.2.6.0.46	Generated when the number of contacts stored in the registration cache exceeds the configured threshold.
apSysMgmtRegCacheThresholdClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.47	Generated when the number of contacts stored in the registration cache falls below the configured threshold.
apSysMgmtRealmMinutesExceedTrap: 1.3.6.1.4.1.9148.3.2.6.0.40	Generated if the monthly minutes for a realm are exceeded.
apSysMgmtRealmMinutesExceedClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.41	Generated if monthly minutes for a realm are reset.
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: • 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. • 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: • 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSysMgmtTaskDeleteTrap: 1.3.6.1.4.1.9148.3.2.6.0.23	[Reserved for future use.] 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 the admin audit or a history file fails.
apSysMgmtAdminWriteFailClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.63	Generated when a write to the admin audit or a history file succeeds after a write to either had previously failed.
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
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.
apSysMgmntH248AssociationLostClearTrap 1.3.6.1.4.1.9148.3.2.6.0.36	This trap will be generated when an H248 control association between a border gateway and session controller has been restored. The included object is the border gateway identifier.
apSysMgmntH248AssociationLostTrap 1.3.6.1.4.1.9148.3.2.6.0.35	This trap will be generated when an H248 control association between a border gateway and session controller is lost. The included object is the border gateway identifier.
apSysMgmtDatabaseRegCacheCapClearTrap 1.3.6.1.4.1.9148.3.2.6.0.77	The trap will be generated when the number of database-type contacts stored in the registration cache falls below the licensed threshold.
apSysMgmtDatabaseRegCacheCapTrap 1.3.6.1.4.1.9148.3.2.6.0.76	The trap will be generated when the number of database-type contacts stored in the registration cache exceeds the licensed threshold.
apSysMgmtH248PortMapUsageClearTrap 1.3.6.1.4.1.9148.3.2.6.0.85	The trap will be generated when the port map usage on H.248 core side Goes down below 90%.
apSysMgmtH248PortMapUsageTrap 1.3.6.1.4.1.9148.3.2.6.0.84	The trap will be geenerated when the port map usage on H.248 core side Exceeds 90%.
apSysMgmtLPLookupExceededTrap 1.3.6.1.4.1.9148.3.2.6.0.65	The trap will be generated the first time the Additional Local Policy Lookups limit is reached in the recent window period. This trap will only occur once during a window period.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSysMgmtMediaSupervisionTimerExpTrap 1.3.6.1.4.1.9148.3.2.6.0.34	The trap will be generated when a media supervision timer has expired. This behavior is disabled by default but may be enabled by changing the 'media-supervision-traps' parameter of the 'media-manager' configuration element. The included object is the call identifier for the call which had the timer expire.
apSysMgmtSataAccessErrorTrap 1.3.6.1.4.1.9148.3.2.6.0.71	The trap will be generated when there is fatal access error on the SATA hard drive.
apSysMgmtShortSessionExceedTrap 1.3.6.1.4.1.9148.3.2.6.0.48	The trap will be generated when the amount of short sessions in a realm exceeds the short session threshold within the short session window.
apSysMgmtSingleUnitRedundancyTrap 1.3.6.1.4.1.9148.3.2.3.0.3	The trap will generated a slot's status changes. The varbinds contain the new information for the generating slot.
apSysMgmtSipInterfaceRegCacheThresholdClearTrap 1.3.6.1.4.1.9148.3.2.6.0.83	The trap will be generated when the number of contacts stored in the registration cache falls below the configured threshold for the sip interface.
apSysMgmtSipInterfaceRegCacheThresholdTrap 1.3.6.1.4.1.9148.3.2.6.0.82	The trap will be generated when the number of contacts stored in the registration cache exceeds the configured threshold for the sip interface.
apSysMgmtTcaClearTrap 1.3.6.1.4.1.9148.3.2.6.0.73	The trap will be generated when a Threshold Crossing Alert counter has fallen below the lowest configured TCA reset-threshold value
apSysMgmtTcaTrap 1.3.6.1.4.1.9148.3.2.6.0.72	The trap will be generated when a Threshold Crossing Alert counter crosses a configured TCA threshold

apSysMgmtGroupTrap Traps

The apSysMgmtGroupTrap (1.3.6.1.4.1.9148.3.2.3.0.1) can convey multiple traps by identifying a system event and corresponding value. The apSysMgmtGroupClearTrap (1.3.6.1.4.1.9148.3.2.3.0.2) is sent when this condition is cleared, according to the application.

apSysMgmtTrapType	Description
apSysXCodeOpusCapacity 1.3.6.1.4.1.9148.3.2.1.1.46	When Opus session utilization exceeds 90%, this object is sent in the apSysMgmtGroupTrap. When utilization falls below 85%, the apSysMgmtGroupClearTrap is sent.
apSysXCodeSILKCapacity 1.3.6.1.4.1.9148.3.2.1.1.47	When SILK session utilization exceeds 90%, this object is sent in the apSysMgmtGroupTrap. When utilization falls below 85%, the apSysMgmtGroupClearTrap is sent.
apSysResrvdNsepSessionCapacity 1.3.6.1.4.1.9148.3.2.1.1.50	When enabled, the system detects when it has exceeded either the minor, major or critical number of reserved NSEP sessions, it sends this object in the apSysMgmtGroupTrap. These thresholds are, by default, 70%, 80% and 90% of your reserved NSEP session pool, respectively. When NSEP session utilization falls below the triggered threshold, the system sends the apSysMgmtGroupClearTrap.

Copyright © 2024, 2026, Oracle and/or its affiliates.

apSwinventory Traps (ap-swinventory.mib)

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

Trap	Description
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. This trap includes the next two objects in this table.
apSwCfgTrapPreviousVersion 1.3.6.1.4.1.9148.3.4.2.1.1	The previous version before this trap happened
apSwCfgTrapCurrentVersion 1.3.6.1.4.1.9148.3.4.2.1.2	The current version after this trap happened

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`.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
apSecurityRadiusFailureNotification 1.3.6.1.4.1.9148.3.9.3.1.0.2	The notification will be generated whenever RADIUS authentication request fails.
apSecurityAuthFailureThresholdNotification 1.3.6.1.4.1.9148.3.9.3.1.0.3	Generated when IKE DDos auth-failure-threshold is reached and report mode includes SNMP trap.
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: • a TACACS+ daemon becomes unreachable • an unreachable TACACS+ daemon becomes reachable • an authentication error occurs • an authorization error occurs
apSecurityTunnelFailureInetNotification 1.3.6.1.4.1.9148.3.9.3.1.0.5	The notification will be generated whenever IPSEC IKEV2 tunnel fails to establish.
apSecurityAuthFailureThresholdInetNotification 1.3.6.1.4.1.9148.3.9.3.1.0.6	Generated when IKE DDos auth-failure-threshold is reached and report mode includes SNMP trap.
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).
apSecurityIPsecTunCapNotification 1.3.6.1.4.1.9148.3.9.3.2.0.2	This notification is sent when the percentage of licensed IPsec tunnels exceeds an IPsec tunnel alarm threshold. The apSecurityIPsecTunCapPct object indicates the current percentage.
apSecurityIPsecTunCapClearNotification 1.3.6.1.4.1.9148.3.9.3.2.0.3	This trap is sent when the percentage of licensed IPsec tunnels no longer exceeds an IPsec tunnel alarm threshold. The apSecurityIPsecTunCapPct object indicates the current percentage.
apSecurityTunnelDPDInetNotification 1.3.6.1.4.1.9148.3.9.3.2.0.4	The notification will be generated whenever IPSEC IKEV2 tunnel fails due to 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.
apSecurityCRLRetrievalFailNotification 1.3.6.1.4.1.9148.3.9.3.5.0.1	This notification is sent when there is a failure in CRL retrieval.
apSecurityCRLRetrievalClearNotification 1.3.6.1.4.1.9148.3.9.3.5.0.2	This notification is sent when there is a success in CRL retrieval.
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.
apSecurityGTPLinkFailureNotification 1.3.6.1.4.1.9148.3.9.3.7.0.1	This notification is sent when there is a link failure with GGSN/PGW on GTP Profile.
apSecurityGTPLinkClearNotification 1.3.6.1.4.1.9148.3.9.3.7.0.2	This notification is sent when the link is restored with GGSN/PGW on GTP Profile.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSecurityTacacsDownLocalAuthUsedTrap 1.3.6.1.4.1.9148.3.9.3.9.0.1	The trap will be generated when a user remotely logs into a system configured for TACACS+ authentication and is authenticated locally by the system because all of the configured and enabled TACACS+ servers have become unreachable or unresponsive.
apSecurityTacacsDownLocalAuthUsedClearTrap 1.3.6.1.4.1.9148.3.9.3.9.0.2	The trap will be generated when a user remotely logs into a system configured for TACACS+ authentication and is successfully authenticated (i.e., access accepted or denied) remotely by a configured and enabled TACACS+ server.
apSecurityTlsEncryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.10.0.1	These notifications are sent when there is a failure during TLS packet encryption. The MIB objects involved are: • apSecuritySrcAddressFamily (1.3.6.1.4.1.9148.3.9.2.23) • apSecuritySrcAddress (1.3.6.1.4.1.9148.3.9.2.24) • apSecuritySrcPort • apSecurityDstAddressFamily (1.3.6.1.4.1.9148.3.9.2.25) • apSecurityDstAddress (1.3.6.1.4.1.9148.3.9.2.26) • apSecurityDstPort • apSecurityTlsEncryptionFailureCause (1.3.6.1.4.1.9148.3.9.2.38) • apSecurityTlsCipherSuite (1.3.6.1.4.1.9148.3.9.2.36) • apSecurityTlsSessionId (1.3.6.1.4.1.9148.3.9.2.34) • apSecurityTlsPacketFailureCount (1.3.6.1.4.1.9148.3.9.2.35)
apSecurityTlsDecryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.10.0.2	These notifications are sent when there is a failure during TLS packet decryption. The MIB objects involved are: • apSecuritySrcAddressFamily (1.3.6.1.4.1.9148.3.9.2.23) • apSecuritySrcAddress (1.3.6.1.4.1.9148.3.9.2.24) • apSecuritySrcPort • apSecurityDstAddressFamily (1.3.6.1.4.1.9148.3.9.2.25) • apSecurityDstAddress (1.3.6.1.4.1.9148.3.9.2.26) • apSecurityDstPort • apSecurityTlsDecryptionFailureCause (1.3.6.1.4.1.9148.3.9.2.37) • apSecurityTlsCipherSuite (1.3.6.1.4.1.9148.3.9.2.36) • apSecurityTlsSessionId (1.3.6.1.4.1.9148.3.9.2.34) • apSecurityTlsPacketFailureCount (1.3.6.1.4.1.9148.3.9.2.35)

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSecuritySrtpEncryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.11.0.1	These notifications are sent when there is a failure during SRTP packet encryption. The MIB objects involved are: • apSecuritySrcAddressFamily (1.3.6.1.4.1.9148.3.9.2.23) • apSecuritySrcAddress (1.3.6.1.4.1.9148.3.9.2.24) • apSecuritySrcPort • apSecurityDstAddressFamily (1.3.6.1.4.1.9148.3.9.2.25) • apSecurityDstAddress (1.3.6.1.4.1.9148.3.9.2.26) • apSecurityDstPort • apSecuritySrtpEncryptionFailureCause (1.3.6.1.4.1.9148.3.9.2.39) • apSecuritySrtpEncrAlgorithm (1.3.6.1.4.1.9148.3.9.2.41) • apSecuritySrtpAuthAlgorithm (1.3.6.1.4.1.9148.3.9.2.42)
apSecuritySrtpDecryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.11.0.2	These notifications are sent when there is a failure during SRTP packet decryption. The MIB objects involved are: • apSecuritySrcAddressFamily (1.3.6.1.4.1.9148.3.9.2.23) • apSecuritySrcAddress (1.3.6.1.4.1.9148.3.9.2.24) • apSecuritySrcPort • apSecurityDstAddressFamily (1.3.6.1.4.1.9148.3.9.2.25) • apSecurityDstAddress (1.3.6.1.4.1.9148.3.9.2.26) • apSecurityDstPort • apSecuritySrtpDecryptionFailureCause (1.3.6.1.4.1.9148.3.9.2.40) • apSecuritySrtpEncrAlgorithm (1.3.6.1.4.1.9148.3.9.2.41) • apSecuritySrtpAuthAlgorithm (1.3.6.1.4.1.9148.3.9.2.42)
apSecurityAuthFailureThresholdInetNotification	

apSLB Traps (ap-slb.mib)

The following traps are found in `ap-slb.mib`. They are used generally for reporting on the Session Load Balancer.

Trap	Description
apSLBEndpointCapacityThresholdTrap 1.3.6.1.4.1.9148.3.11.3.0.1	The trap will be generated when the number of endpoints on the SLB exceeds the configured threshold.
apSLBEndpointCapacityThresholdClearTrap 1.3.6.1.4.1.9148.3.11.3.0.2	The trap will be generated when the number of endpoints on the SLB falls below the configured threshold.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apSLBUntrustedEndpointCapacityThresholdTrap 1.3.6.1.4.1.9148.3.11.3.0.3	The trap will be generated when the number of untrusted endpoints on the SLB exceeds the configured threshold.
apSLBUntrustedEndpointCapacityThresholdClearTrap 1.3.6.1.4.1.9148.3.11.3.0.4	The trap will be generated when the number of untrusted endpoints on the SLB falls below the configured threshold.

apH323 Traps (ap-h323.mib)

The following traps are found in `ap-env-h323.mib`. They are used generally for reporting on environmental changes.

Trap	Description
apH323StackMaxCallThresholdTrap: 1.3.6.1.4.1.9148.3.10.3.0.1	Generated when the number of H.323 calls increases the percentage of the max calls threshold.
apH323StackMaxCallThresholdClearTrap: 1.3.6.1.4.1.9148.3.10.3.0.2	Generated when the number of H.323 calls decreases to below the lowest max calls threshold.

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).
1.3.6.1.4.1.9148.3.13.1.2.2.0.7 apAcctMsgQueueUpperThresholdTrap	Generated when ACRq usage reaches the Upper Threshold value.
1.3.6.1.4.1.9148.3.13.1.2.2.0.8 apAcctMsgQueueUpperThresholdClearTrap	Generated when ACRq usage reaches the Lower Threshold value.

apDnsAlg Traps (ap-dnsalg.mib)

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap	Description
apDnsAlgStatusChangeTrap 1.3.6.1.4.1.9148.3.14.2.2.0.1	Generated if the reachability status of an 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 an 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.
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.

apSip Traps (ap-sip.mib)

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

Trap Name	Description
apSipSecInterfaceRegThresholdExcededTrap: 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.
apSipSurvivabilityModeEnter 1.3.6.1.4.1.9148.3.15.2.2.2.0.1	The trap will be generated when SIP interface enters Survivability Mode.
apSipSurvivabilityModeExit 1.3.6.1.4.1.9148.3.15.2.2.2.0.2	The trap will be generated when SIP interface exits Survivability Mode and resumes normal operation.
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.
apSipRecRecDlgFailNotify, 1.3.6.1.4.1.9148.3.15.4.1.0.1	This trap will be generated when either: • The session recording server responds with a call failure response, including 4xx, 5xx and 6xx responses. • A Recording Dialog fails to send a timely response to a requests, typically an in-dialog OPTIONS request.
apSipRecCommSessionNotify 1.3.6.1.4.1.9148.3.15.4.1.0.2	This trap will be generated when a Communications Session is terminated because a recording dialog could not be established or prematurely terminated.
apSip503RespThresholdCrossedNotify 1.3.6.1.4.1.9148.3.15.5.1.0.1	Generated if the percentage of local 503 errors sent by the system exceeds the monitoring threshold set in the **internal-503-threshold**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap Name	Description
apSipSteeringPoolThresholdCrossedNotify 1.3.6.1.4.1.9148.3.15.6.1.0.1	Generated if the percentage of steering pool ports exceeds the monitoring threshold set in the **steering-pool-threshold** configured in a realm.
apConfigPushReceiverFailureTrap 1.3.6.1.4.1.9148.3.15.7.1.0.1	Generated if the system fails to upload the backup configuration file within the context of configuration backup push receiver failures only.

apApps Traps (ap-apps.mib)

The `ap-apps.mib` includes the following traps.

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.
apAclDropOverThresholdTrap 1.3.6.1.4.1.9148.3.16.2.2.4.0.1	Generated when the acl drop ratio exceeds the configured threshold.
apAclDropOverThresholdClearTrap 1.3.6.1.4.1.9148.3.16.2.2.4.0.2	Generated when the acl drop ratio goes below the configured threshold.
apMonitorCollectorDownTrap 1.3.6.1.4.1.9148.3.16.2.2.3.0.1	Generated when there is a disconnect between a Session Border Controller and a CommMonitor.
apMonitorCollectorClearTrap 1.3.6.1.4.1.9148.3.16.2.2.3.0.2	Generated when a Session Border Controller reconnects with the CommMonitor and normal operation resumes.
apStirServerUnreachableTrap 1.3.6.1.4.1.9148.3.16.2.2.5.0.1	Generated when experiencing repeated sequential REST STI server response timeouts the SBC.
apStirServerUnreachableClearTrap 1.3.6.1.4.1.9148.3.16.2.2.5.0.2	Generated when experiencing repeated sequential REST STI server response timeouts the SBC stop occurring.

apAclDropOverThresholdTrap Objects

The following objects, which are part of the apAclDropOverThresholdTrap, are not available with an SNMP GET.

MIB Object	Description
apAclDropType 1.3.6.1.4.1.9148.3.16.4.1.1	ACL drop type.
apAclDropCount 1.3.6.1.4.1.9148.3.16.4.1.2	ACL drop count within monitor time window.
apAclDropRatio 1.3.6.1.4.1.9148.3.16.4.1.3	ACL drop ratio as permillage of current time window.

apUSBC Traps (ap-usbcsys.mib)

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 de-activated.
apUsbcSysThreadNotRespondingTrap 1.3.6.1.4.1.9148.3.17.2.2.1.0.7	The trap is generated when a thread is not responding.
apMutexDeadLockDetectedTrap 1.3.6.1.4.1.9148.3.17.2.2.1.0.5	The trap is generated when the system detects a deadlock.
apMutexDeadLockClearTrap 1.3.6.1.4.1.9148.3.17.2.2.1.0.6	The trap is generated when the system detects that a deadlock us clear.
apUsbcSysFdCountClearTrap 1.3.6.1.4.1.9148.3.17.2.2.2.0.2	The trap will be generated when the FD count drops below the pre-defined threshold.
apUsbcSysFdCountExceedingTrap 1.3.6.1.4.1.9148.3.17.2.2.2.0.1	The trap will be generated when the FD count is over a threshold.

Specify an NMS for EMS Generated Traps

You must configure a northbound network management server (NMS) such as an SNMP management system as the receiver of element manager system (EMS) traps. An EMS, such as the Session Element Manager, generates the (EMS MIB) traps shown in the table below when it detects the following conditions:

- There is a failure to discover or rediscover a SBC configuration.
- There is a failure to save a SBC configuration.
- There is a failure to activate a SBC configuration.
- There are missing components when validating a SBC configuration.
- The node status changes from reachable to unreachable.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Trap Name	Description
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.
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.

Persistent indexing of SNMP Tables

Certain Oracle Communications Session Border Controller 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.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 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)

Copyright © 2024, 2026, Oracle and/or its affiliates.

syslog Level (Numerical Code)	BSD syslog Severity Level (Number)
WARNING (5)	Warning - warning conditions (4)
NOTICE (6)	Notice - normal, but significant condition (5)
INFO (7)	Informational - informational messages (6)
TRACE (8) DEBUG (9)	Debug - debug level messages (7)

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).

Copyright © 2024, 2026, Oracle and/or its affiliates.

Event Category	Description
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.

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.

Platform	sysObjectID
Acme Packet 3900	apNetNet3900: 1.3.6.1.4.1.9148.1.3.3
Acme Packet 3950	apNetNet3950: 1.3.6.1.4.1.9148.1.3.4
Acme Packet 4900	apNetNet4900: 1.3.6.1.4.1.9148.1.1.4
Acme Packet 4600	apNetNet4600: 1.3.6.1.4.1.9148.1.1.3
Acme Packet 6100	apNetNet6100: 1.3.6.1.4.1.9148.1.5.2
Acme Packet 6300	apNetNet6300: 1.3.6.1.4.1.9148.1.5.1

Copyright © 2024, 2026, Oracle and/or its affiliates.

3

Standard SNMP GET Requests

This section explains the standard SNMP GET requests supported by the Oracle Communications Session Border Controller. 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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. The ifIndex values for the mgmt and media interfaces can be mapped as follows: Media Port • Slot 0/Port 0: 1.3.6.1.2.1.2.2.1.1.5 (ifIndex value is 5) • Slot 0/Port 1: 1.3.6.1.2.1.2.2.1.1.7 (ifIndex value is 7) • Slot 0/Port 2 (or Slot 1/port 0): 1.3.6.1.2.1.2.2.1.1.9 (ifIndex value is 9) • Slot 0/Port 3 (or Slot 1/port 1): 1.3.6.1.2.1.2.2.1.1.11 (ifIndex value is 11) HA Ports • wancom1 (Management HA Port slot 0/port 1): 1.3.6.1.2.1.2.2.1.1.2 (ifIndex value is 2) • wancom2 (Management HA Port slot 0/port 2): 1.3.6.1.2.1.2.2.1.1.3 (ifIndex value is 3)
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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.2.2.1 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.2.2.1 +	Description
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 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,

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 Communications Session Border Controllers 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)

Copyright © 2024, 2026, Oracle and/or its affiliates.

ifXTable Table

The ifXTable is available to support 64-bit counters for interface statistics. Only Gets are supported for this MIB Table, and are supported on all interfaces.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
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. 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
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.
ifHCOutOctets	.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
ifHCOutUcastPkts	.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 management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.2.1.31.1.1 +	Description
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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.4 +	Description
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 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.4 +	Description
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 inipForwDatagrams 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.4 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.5 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.6 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.6 +	Description
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.7 +	Description
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.
updLocalPort	.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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.1 +	Description
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 raised to (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.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 Communications Session Border Controller 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1.1 +	Description
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 a 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, 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1.1 +	Description
entPhysicalParentRelPos	.6	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). 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. 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. If the agent cannot determine the parent-relative position for some reason, or if the associated value 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. This ordering might be sparse or dense, depending on agent

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
		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
entPhysicalName	.7	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.
entPhysicalHardwareRev	.8	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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
entPhysicalFirmwareRev	.9	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 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
entPhysicalSerialNum	.11	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. 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. 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. 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1.1 +	Description
entPhysicalMfgName	.12	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.
entPhysicalModeName	.13	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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1.1 +	Description
entPhysicalAlias	.14	Alias name for the physical entity as specified by a network manager, it provides a non-volatile handle for the physical entity. 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. 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.2.1.47.1.1.1.1 +	Description
entPhysicalAssetID	.15	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. Not every physical component will have a asset tracking identifier, or even need one. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to false(2), do not need their own unique asset tracking identifier. 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
entPhysicalIsFRU	.16	Whether this physical entity is considered a field replaceable unit by the vendor. • true(1) means this is a field replaceable unit. • false(2) means this is not a replaceable unit

Copyright © 2024, 2026, Oracle and/or its affiliates.

4

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, DNS, DoS threshold and STIR statistics and states.

apAppsENUMServerStatusTable Table

The following table all configured ENUM servers' status.

MIB Object	Description
apAppsENUMServerStatusEntry 1.3.6.1.4.1.9148.3.16.1.2.1.1.1	Numbered table entry.
apAppsENUMConfigName 1.3.6.1.4.1.9148.3.16.1.2.1.1.1.1	The name of the **enum-config** element that contains this ENUM server.
apAppsENUMServerInetAddressType 1.3.6.1.4.1.9148.3.16.1.2.1.1.1.2	The internet address type of this ENUM server.
apAppsENUMServerInetAddress 1.3.6.1.4.1.9148.3.16.1.2.1.1.1.3	The IP address of this ENUM server.
apAppsENUMServerStatus 1.3.6.1.4.1.9148.3.16.1.2.1.1.1.4	The status of this ENUM server.

apAppsDnsServerStatusTable

The following table all configured ENUM servers' status.

MIB Object	Description
apAppsDnsServerStatusEntry 1.3.6.1.4.1.9148.3.16.1.2.2.1.1	An entry designed to hold the status of a single DNS server
apAppsDnsInterfaceName 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.1	The name of the dns interface that contains this dns server.
apAppsDnsServerInetAddressType 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.2	The internet address type of this DNS server.
apAppsDnsServerInetAddress 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.3	The IP address of this DNS server.
apAppsDnsServerStatus 1.3.6.1.4.1.9148.3.16.1.2.2.1.1.4	The status of this DNS server.

Copyright © 2024, 2026, Oracle and/or its affiliates.

apAppsStirMIBObjects Table

The apAppsStirMIBObjects is an object that consists of all the STIR-related tables. This table collects and assembles all STIR/SHAKEN MIB data for presentation using SNMP.

Tables within the apAppsStirMIBObjects (1.3.6.1.4.1.9148.3.16.1.2.4) table include:

- apAppsStirServerTable (1.3.6.1.4.1.9148.3.16.1.2.4.1), which references:
  - apAppsStirServerEntry
  - apStirServerIndex
  - apStirServerName
- apAppsStirStatsTable (1.3.6.1.4.1.9148.3.16.1.2.4.2), which references:
  - apAppsStirStatsEntry
  - apStirStatsServerIndex
  - apCounterStatsType
  - apStirServerStats
  - apStirStatsType
- apAppsStirAgentTable (1.3.6.1.4.1.9148.3.16.1.2.4.3), which references:
  - apAppsStirAgentEntry
  - apStirAgentIndex
  - apStirAgentName
- apAppsStirAgentStatsTable (1.3.6.1.4.1.9148.3.16.1.2.4.4), which references:
  - apAppsStirAgentStatsEntry
  - apStirStatsAgentIndex
  - apCounterStatsAgentType
  - apStirAgentStatsType
  - apStirAgentStats
- apAppsStirSipInterfaceTable (1.3.6.1.4.1.9148.3.16.1.2.4.5), which references:
  - apAppsStirSipInterfaceEntry
  - apStirSipInterfaceIndex
  - apStirSipInterfaceName
- apAppsStirSipInterfaceStatsTable (1.3.6.1.4.1.9148.3.16.1.2.4.6), which references:
  - apAppsStirSipInterfaceStatsEntry
  - apStirStatsSipInterfaceIndex
  - apCounterStatsSipInterfaceType
  - apStirSipInterfaceStatsType
  - apStirSipInterfaceStats
- apAppsStirRealmTable (1.3.6.1.4.1.9148.3.16.1.2.4.7), which references:
  - apAppsStirRealmEntry

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - apStirRealmIndex
  - apStirRealmName
- apAppsStirRealmStatsTable (1.3.6.1.4.1.9148.3.16.1.2.4.8), which references:
  - apAppsStirRealmStatsEntry
  - apStirStatsRealmIndex
  - apCounterStatsRealmType
  - apStirRealmStatsType
  - apStirRealmStats
- apAppsStirSystemStatsTable (1.3.6.1.4.1.9148.3.16.1.2.4.9) , which references:
  - apAppsStirSystemStatsEntry
  - apCounterStatsSystemType
  - apStirSystemStatsType
  - apStirSystemStats

apAppsStirServerTable

The table lists STIR server names with object apStirServerName indexed by a persistent index apStirServerIndex.

apAppsStirServerTable

The following table collects information on all configured STIR servers' status.

The apStirServerName OID is 1.3.6.1.4.1.9148.3.16.1.2.4.1.1.2.

The apAppsStirServerStatsTable uses three variables to specify each object, as follows:

1. The first index is the server index.
   This component of the SNMP table uses the config-object ID the system creates when you create the object. The STI server labels are contained in OID APAPPS-MIB::apStirServerName.
2. The second index is an enumeration of the counter types:
   - recent = 1
   - total = 2
   - permax = 3
3. The third index is the data category.

For example, the apStirServerStats instances have an OID of the form apStirServerStats.x.y.z, where:

- apStirServerStats is 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4;
- x is the stir server's index;
- y is the ApCounterStatsType (recent = 1, total = 2, or permax = 3)
- z is the data category

Each data category is found within each ApCounterStatsType. The "asQueries" category, for example, is found within the recent, total, and permax counter types.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.x
apStirServerStats.<index>.recent.asQueries	1.1
apStirServerStats.<index>.total.asQueries	2.1
apStirServerStats.<index>.permax.asQueries	3.1

To find the complete OID for a data category:

1. Start with the OID of apStirServerStats (1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4)
2. Append your server index (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.10).
3. Append your ApCounterStatsType (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.10.2)
4. Append your data category (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.10.2.1)

OID 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.10.2.1 gets the total number (ApCounterStatsType = 2) of queries made to the AS server (data category = 1) for STIR server 10.

Table 4-1 Data Categories

Data Category Name	Data Category Number	Description
asQueries	.1	Queries made to the named AS server
asSuccessResponses	.2	Successful responses received from the named AS server
asFailResponses	.3	Failed responses received from the named AS server
asFailServiceException	.4	Failed responses received from the named AS server caused by a service exception
asFailPolicyException	.5	Failed responses received from the named AS server caused by a policy exception
vsQueries	.6	Queries made to the named VS server
vsSuccessResponses	.7	Successful responses received from the named VS server
vsFailResponses	.8	Successful responses received from the named VS server
vsSuccessVerification	.9	Successful verifications received from the named VS server
vsFailVerification	.10	Failed responses received from the named VS server indicating verification failure
vsFailServiceException	.11	Failed responses received from the named VS server caused by a service exception
vsFailPolicyException	.12	Failed responses received from the named VS server caused by a policy exception
serverUnreachable	.13	Number of unsuccessful attempts to reach a server
asSentInviteswithShakenPASSportA	.14	Sent INVITES that included a SHAKEN passport with attestation level A

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 4-1 (Cont.) Data Categories

Data Category Name	Data Category Number	Description
asSentInviteswithShakenPASSportB	.15	Sent INVITES that included a SHAKEN passport with attestation level B
asSentInviteswithShakenPASSportC	.16	Sent INVITES that included a SHAKEN passport with attestation level C
asSentInviteswithdivPASSport	.17	Sent INVITES that included a DIV passport
vsReceivedInviteswithNoPASSport	.18	Recevied INVITEs that had no passport
vsReceivedInviteswithShakenPASSport	.19	Received INVITEs that had at least one SHAKEN passport
vsReceivedInviteswithDivPASSport	.20	Received INVITEs that had at least one DIV passport
vsSentInviteswithTNValidationPassed	.21	Sent INVITES that included a TN validation that passed
vsSentInviteswithTNValidationFailed	.22	Sent INVITES that included a TN validation that failed
vsSentInviteswithNoTNValidation	.23	Sent INVITES that included a no TN validation parameter
asServiceUnreachable	.24	Number of unreachable Service to AS
vsServiceUnreachable	.25	Number of unreachable Service to VS Server
vsInviteRejected	.26	Number of calls rejected based on verstat and reason code from sti-vs server
asBypass	.27	Number of calls that bypassed the STI-AS server signature request based on message contents
vsBypass	.28	Number of calls that bypassed the STI-VS server verification request based on message contents
apStirStatsTypeMax	.29	Marker indicating the end of the stats types

The apStirStatsTypeMax marks the end of the defined types. No object should have the index with its value. If an object has this value, the number of the apStirServerStatsType values has been expanded and either this MIB Guide or the MIB Package should be updated.

apAppsStirAgentStatsTable

The following table collects information on all configured STIR session agents status. The apAppsStirAgentStats reference is the name for all apAppsStirAgentStatsTable stats elements.

The apStirAgentName OID is 1.3.6.1.4.1.9148.3.16.1.2.4.3.1.2.

The apAppsStirAgentStatsTable uses three variables to specify each object, as follows:

1. The first index is the STIR session agent index.

Copyright © 2024, 2026, Oracle and/or its affiliates.

This component of the SNMP table uses the config-object ID the system creates when you create the object. The STI agent labels are contained in OID APAPPS-MIB::apStirAgentName.

2. The second index is an enumeration of the counter types:
   - recent = 1
   - total = 2
   - permax = 3
3. The third index is the data category.

For example, the apAppsStirAgentStats instances have an OID of the form apAppsStirAgentStats.x.y.z, where:

- apStirAgentStats is 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4
- x is the STIR sesion agent's index
- y is the ApCounterStatsType (recent = 1, total = 2, or permax = 3)
- z is the data category

Each data category is found within each ApCounterStatsType. The "asQueries" category, for example, is found within the recent, total, and permax counter types.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.x
apStirAgentStats.<index>.recent.asQueries	1.1
apStirAgentStats.<index>.total.asQueries	2.1
apStirAgentStats.<index>.permax.asQueries	3.1

To find the complete OID for a data category:

1. Start with the OID of apStirAgentStats (1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4)
2. Append your STIR session agent index (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.10).
3. Append your ApCounterStatsType (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.10.2)
4. Append your data category (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.10.2.1)

OID 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.10.2.1 gets the total number (ApCounterStatsType = 2) of queries made to the AS server (data category = 1) for STIR session agent 10.

Table 4-2 Data Categories

Data Category Name	Data Category Number	Description
asQueries	.1	Queries made to the named AS server
asSuccessResponses	.2	Successful responses received from the named AS server
asFailResponses	.3	Failed responses received from the named AS server
asFailServiceException	.4	Failed responses received from the named AS server caused by a service exception
asFailPolicyException	.5	Failed responses received from the named AS server caused by a policy exception

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 4-2 (Cont.) Data Categories

Data Category Name	Data Category Number	Description
vsQueries	.6	Queries made to the named VS server
vsSuccessResponses	.7	Successful responses received from the named VS server
vsFailResponses	.8	Successful responses received from the named VS server
vsSuccessVerification	.9	Successful verifications received from the named VS server
vsFailVerification	.10	Failed responses received from the named VS server indicating verification failure
vsFailServiceException	.11	Failed responses received from the named VS server caused by a service exception
vsFailPolicyException	.12	Failed responses received from the named VS server caused by a policy exception
asSentInviteswithShakenPASSportA	.14	Sent INVITES that included a SHAKEN passport with attestation level A
asSentInviteswithShakenPASSportB	.15	Sent INVITES that included a SHAKEN passport with attestation level B
asSentInviteswithShakenPASSportC	.16	Sent INVITES that included a SHAKEN passport with attestation level C
asSentInviteswithdivPASSport	.17	Sent INVITES that included a DIV passport
vsReceivedInviteswithNoPASSport	.18	Recevied INVITEs that had no passport
vsReceivedInviteswithShakenPASSport	.19	Received INVITEs that had at least one SHAKEN passport
vsReceivedInviteswithDivPASSport	.20	Received INVITEs that had at least one DIV passport
vsSentInviteswithTNValidationPassed	.21	Sent INVITES that included a TN validation that passed
vsSentInviteswithTNValidationFailed	.22	Sent INVITES that included a TN validation that failed
vsSentInviteswithNoTNValidation	.23	Sent INVITES that included a no TN validation parameter
vsInviteRejected	.26	Number of calls rejected based on verstat and reason code from sti-vs server
asBypass	.27	Number of calls that bypassed the STI-AS server signature request based on message contents
vsBypass	.28	Number of calls that bypassed the STI-VS server verification request based on message contents

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 4-2 (Cont.) Data Categories

Data Category Name	Data Category Number	Description
apStirStatsTypeMax	.29	Marker indicating the end of the stats types

The apStirStatsTypeMax marks the end of the defined types. No object should have the index with its value. If an object has this value, the number of the apStirServerStatsType values has been expanded and either this MIB Guide or the MIB Package should be updated.

apAppsStirSipInterfaceStatsTable

The following table collects information on all configured sip-interface status. The apStirSipInterfaceStats reference is the name for all apAppsStirSipInterfaceStatsTable stats elements. The following topics address SNMP changes with new OIDs labeled within the tables below.

The apStirSipInterfaceName OID is 1.3.6.1.4.1.9148.3.16.1.2.4.5.1.2.

The apAppsStirSipInterfaceStatsTable uses three variables to specify each object, as follows:

1. The first index is the sip-interface index.
   This component of the SNMP table uses the config-object ID the system creates when you create the object. The STI labels are contained in OID APAPPS-MIB::apStirSipInterfaceName.
2. The second index is an enumeration of the counter types:
   - recent = 1
   - total = 2
   - permax = 3
3. The third index is the data category.

For example, the apStirSipInterfaceStats instances have an OID of the form apAppsStirSipInterfaceStats.x.y.z, where:

- apAppsStirSipInterfaceStats is 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4
- x is the sip-interface index
- y is the ApCounterStatsType (recent = 1, total = 2, or permax = 3)
- z is the data category

Each data category is found within each ApCounterStatsType. The "asQueries" category, for example, is found within the recent, total, and permax counter types.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.x
apAppsStirSipInterfaceStats.<index>.recent.asQueries	1.1
apAppsStirSipInterfaceStats.<index>.total.asQueries	2.1
apAppsStirSipInterfaceStats.<index>.permax.asQueries	3.1

To find the complete OID for a data category:

Copyright © 2024, 2026, Oracle and/or its affiliates.

1. Start with the OID of apStirSipInterfaceStats (1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4)
2. Append your sip-interface index (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.3).
3. Append your ApCounterStatsType (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.3.2)
4. Append your data category (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.3.2.1)

OID 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.3.2.1 gets the total number (ApCounterStatsType = 2) of queries made to the AS server (data category = 1) for sip-interface 3.

Data Categories

Data Category Name	Data Category Number	Description
asQueries	.1	Queries made to the named AS server
asSuccessResponses	.2	Successful responses received from the named AS server
asFailResponses	.3	Failed responses received from the named AS server
asFailServiceException	.4	Failed responses received from the named AS server caused by a service exception
asFailPolicyException	.5	Failed responses received from the named AS server caused by a policy exception
vsQueries	.6	Queries made to the named VS server
vsSuccessResponses	.7	Successful responses received from the named VS server
vsFailResponses	.8	Successful responses received from the named VS server
vsSuccessVerification	.9	Successful verifications received from the named VS server
vsFailVerification	.10	Failed responses received from the named VS server indicating verification failure
vsFailServiceException	.11	Failed responses received from the named VS server caused by a service exception
vsFailPolicyException	.12	Failed responses received from the named VS server caused by a policy exception
asSentInviteswithShakenPASSportA	.14	Sent INVITES that included a SHAKEN passport with attestation level A
asSentInviteswithShakenPASSportB	.15	Sent INVITES that included a SHAKEN passport with attestation level B
asSentInviteswithShakenPASSportC	.16	Sent INVITES that included a SHAKEN passport with attestation level C
asSentInviteswithdivPASSport	.17	Sent INVITES that included a DIV passport
vsReceivedInviteswithNoPASSport	.18	Recevied INVITEs that had no passport

Copyright © 2024, 2026, Oracle and/or its affiliates.

Data Category Name	Data Category Number	Description
vsReceivedInviteswithShakenPASSport	.19	Received INVITEs that had at least one SHAKEN passport
vsReceivedInviteswithDivPASSport	.20	Received INVITEs that had at least one DIV passport
vsSentInviteswithTNValidationPassed	.21	Sent INVITES that included a TN validation that passed
vsSentInviteswithTNValidationFailed	.22	Sent INVITES that included a TN validation that failed
vsSentInviteswithNoTNValidation	.23	Sent INVITES that included a no TN validation parameter
vsInviteRejected	.26	Number of calls rejected based on verstat and reason code from sti-vs server
asBypass	.27	Number of calls that bypassed the STI-AS server signature request based on message contents
vsBypass	.28	Number of calls that bypassed the STI-VS server verification request based on message contents
apStirStatsTypeMax	.29	Marker indicating the end of the stats types

The apStirStatsTypeMax marks the end of the defined types. No object should have the index with its value. If an object has this value, the number of the apStirServerStatsType values has been expanded and either this MIB Guide or the MIB Package should be updated.

apAppsStirRealmStatsTable

The following table collects information on all configured STIR realm' status. The apRealmServerStats reference is the name for all apAppsStirRealmStatsTable stats elements.

The apStirRealmName OID is 1.3.6.1.4.1.9148.3.16.1.2.4.7.1.2.

The apAppsStirRealmStatsTable uses three variables to specify each object, as follows:

1. The first index is the realm index.
   This component of the SNMP table uses the config-object ID the system creates when you create the object. The STI labels are contained in OID APAPPS-MIB::apStirRealmName.
2. The second index is an enumeration of the counter types:
   - recent = 1
   - total = 2
   - permax = 3
3. The third index is the data category.

For example, the apAppsStirRealmStats instances have an OID of the form apAppsRealmServerStats.x.y.z, where:

- apStirRealmStats is 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4
- x is the realm index
- y is the ApCounterStatsType (recent = 1, total = 2, or permax = 3)

Copyright © 2024, 2026, Oracle and/or its affiliates.

- z is the data category

Each data category is found within each ApCounterStatsType. The "asQueries" category, for example, is found within the recent, total, and permax counter types.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.x
apStirRealmStats.<index>.recent.asQueries	1.1
apStirRealmStats.<index>.total.asQueries	2.1
apStirRealmStats.<index>.permax.asQueries	3.1

To find the complete OID for a data category:

1. Start with the OID of apStirRealmStats (1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4)
2. Append your realm index (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.3).
3. Append your ApCounterStatsType (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.3.2)
4. Append your data category (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.3.2.1)

OID 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.3.2.1 gets the total number (ApCounterStatsType = 2) of queries made to the AS server (data category = 1) for realm 3.

Data Categories

Data Category Name	Data Category Number	Description
asQueries	.1	Queries made to the named AS server
asSuccessResponses	.2	Successful responses received from the named AS server
asFailResponses	.3	Failed responses received from the named AS server
asFailServiceException	.4	Failed responses received from the named AS server caused by a service exception
asFailPolicyException	.5	Failed responses received from the named AS server caused by a policy exception
vsQueries	.6	Queries made to the named VS server
vsSuccessResponses	.7	Successful responses received from the named VS server
vsFailResponses	.8	Successful responses received from the named VS server
vsSuccessVerification	.9	Successful verifications received from the named VS server
vsFailVerification	.10	Failed responses received from the named VS server indicating verification failure
vsFailServiceException	.11	Failed responses received from the named VS server caused by a service exception
vsFailPolicyException	.12	Failed responses received from the named VS server caused by a policy exception

Copyright © 2024, 2026, Oracle and/or its affiliates.

Data Category Name	Data Category Number	Description
asSentInviteswithShakenPASSportA	.14	Sent INVITES that included a SHAKEN passport with attestation level A
asSentInviteswithShakenPASSportB	.15	Sent INVITES that included a SHAKEN passport with attestation level B
asSentInviteswithShakenPASSportC	.16	Sent INVITES that included a SHAKEN passport with attestation level C
asSentInviteswithdivPASSport	.17	Sent INVITES that included a DIV passport
vsReceivedInviteswithNoPASSport	.18	Recevied INVITEs that had no passport
vsReceivedInviteswithShakenPASSport	.19	Received INVITEs that had at least one SHAKEN passport
vsReceivedInviteswithDivPASSport	.20	Received INVITEs that had at least one DIV passport
vsSentInviteswithTNValidationPassed	.21	Sent INVITES that included a TN validation that passed
vsSentInviteswithTNValidationFailed	.22	Sent INVITES that included a TN validation that failed
vsSentInviteswithNoTNValidation	.23	Sent INVITES that included a no TN validation parameter
vsInviteRejected	.26	Number of calls rejected based on verstat and reason code from sti-vs server
asBypass	.27	Number of calls that bypassed the STI-AS server signature request based on message contents
vsBypass	.28	Number of calls that bypassed the STI-VS server verification request based on message contents
apStirStatsTypeMax	.29	Marker indicating the end of the stats types

The apStirStatsTypeMax marks the end of the defined types. No object should have the index with its value. If an object has this value, the number of the apStirServerStatsType values has been expanded and either this MIB Guide or the MIB Package should be updated.

apAppsStirSystemStatsTable

The following table collects information on the system's status. The apStirSystemStats reference is the name for all apAppsStirSystemStatsTable stats elements.

The apAppsStirSystemStatsTable uses two variables to specify its data, as follows:

1. The first is an enumeration of the counter types:
   - recent = 1
   - total = 2
   - permax = 3

Copyright © 2024, 2026, Oracle and/or its affiliates.

2. The second is the data category.

For example, the apStirSystemStats instances have an OID of the form apStirSystemStats.y.z, where:

- y is the ApCounterStatsType (recent = 1, total = 2, or permax = 3)
- z is the data category

Each data category is found within each ApCounterStatsType. The "asQueries" category, for example, is found within the recent, total, and permax counter types.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3
apStirSystemStats.recent.asQueries	1.1
apStirSystemStats.total.asQueries	2.1
apStirSystemStats.permax.asQueries	3.1

To find the complete OID for a data category:

1. Start with the OID of apStirSystemStats (1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3)
2. Append your ApCounterStatsType (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3.2)
3. Append your data category (for example, 1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3.2.1)

OID1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3.2.1 gets the total number (ApCounterStatsType = 2) of queries made to the AS server (data category = 1) for the system.

Data Categories

Data Category Name	Data Category Number	Description
asQueries	.1	Queries made to the named AS server
asSuccessResponses	.2	Successful responses received from the named AS server
asFailResponses	.3	Failed responses received from the named AS server
asFailServiceException	.4	Failed responses received from the named AS server caused by a service exception
asFailPolicyException	.5	Failed responses received from the named AS server caused by a policy exception
vsQueries	.6	Queries made to the named VS server
vsSuccessResponses	.7	Successful responses received from the named VS server
vsFailResponses	.8	Successful responses received from the named VS server
vsSuccessVerification	.9	Successful verifications received from the named VS server
vsFailVerification	.10	Failed responses received from the named VS server indicating verification failure
vsFailServiceException	.11	Failed responses received from the named VS server caused by a service exception

Copyright © 2024, 2026, Oracle and/or its affiliates.

Data Category Name	Data Category Number	Description
vsFailPolicyException	.12	Failed responses received from the named VS server caused by a policy exception
asSentInviteswithShakenPASSportA	.14	Sent INVITES that included a SHAKEN passport with attestation level A
asSentInviteswithShakenPASSportB	.15	Sent INVITES that included a SHAKEN passport with attestation level B
asSentInviteswithShakenPASSportC	.16	Sent INVITES that included a SHAKEN passport with attestation level C
asSentInviteswithdivPASSport	.17	Sent INVITES that included a DIV passport
vsReceivedInviteswithNoPASSport	.18	Recevied INVITEs that had no passport
vsReceivedInviteswithShakenPASSport	.19	Received INVITEs that had at least one SHAKEN passport
vsReceivedInviteswithDivPASSport	.20	Received INVITEs that had at least one DIV passport
vsSentInviteswithTNValidationPassed	.21	Sent INVITES that included a TN validation that passed
vsSentInviteswithTNValidationFailed	.22	Sent INVITES that included a TN validation that failed
vsSentInviteswithNoTNValidation	.23	Sent INVITES that included a no TN validation parameter
vsInviteRejected	.26	Number of calls rejected based on verstat and reason code from sti-vs server
asBypass	.27	Number of calls that bypassed the STI-AS server signature request based on message contents
vsBypass	.28	Number of calls that bypassed the STI-VS server verification request based on message contents
apStirStatsTypeMax	.29	Marker indicating the end of the stats types

The apStirStatsTypeMax marks the end of the defined types. No object should have the index with its value. If an object has this value, the number of the apStirServerStatsType values has been expanded and either this MIB Guide or the MIB Package should be updated.

apAppsNSEPRealmTable

To produce realm-based SNMP statistics for NSEP traffic, the SBC establishes 3 tables populated within the apAppNSEPRealmMIBObjects group, which is the parent object from which the system organizes this SNMP output:

- apAppsNSEPRealmTable
- apAppsNSEPRealmRvalueTable

Copyright © 2024, 2026, Oracle and/or its affiliates.

- apNSEPRealmRvalueStatsTable

These tables include key value objects that use variables to segregate specific value objects. The system assembles name objects, which specify realm and value names concatenated with the statistic value.

The variables used in building the output include:

- X—represents realm-index
- Y—represents rvalue or dialed-number index
- Z—represents the corresponding counter, per realm and per value

The actual data, realm name, value name and statistic, are present within the MIB as follows:

- apNSEPRealmName (1.3.6.1.4.1.9148.3.16.1.2.6.1.1.2.X)—X ranges from 1 to n, where n is the number of configured realms, and is pulled from all realms for which you have enabled **nsep-stats**.
- apNSEPRvalueName (1.3.6.1.4.1.9148.3.16.1.2.6.2.1.2.Y)—Y ranges from 1 to n, where n is a fixed number and includes all possible r-values, which is statically assigned and the value 100, which is assigned for dialed numbers. The values correspond to the rvalues you have configured in the **nsep-stats-profile**. The system chooses the respective number for each rvalue statically assigned in the ApNSEPRealmRvalueDNIndex OID.
- apNSEPRealmStats (1.3.6.1.4.1.9148.3.16.1.2.6.3.1.4.X.Y.Z)—Z ranges from 1 to 8 and is pulled from the apNSEPRealmStatsType OID.

The apNSEPRealmName object has the OID 1.3.6.1.4.1.9148.3.16.1.2.6.1.1.2.X. The apNSEPRvalueName object has the OID 1.3.6.1.4.1.9148.3.16.1.2.6.2.1.2.Y. The apNSEPRealmStats object has the OID 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.4. and produces the statistic value when assembled with the X, Y, and Z variables.

This table lists and describes the apNSEPRealmName MIB objects.

Sequence Number	Object ID apNSEPRealmName 1.3.6.1.4.1.9148.3.16.1.2.6.1.1.2.X	Description
1	.1	Gives the starting realm-name
2	.2	Gives the consecutive realm-name
n	n	Gives the next consecutive rvalue

This table lists and describes the apNSEPRvalueName MIB objects.

Sequence Number	Object ID apNSEPRvalueName 1.3.6.1.4.1.9148.3.16.1.2.6.2.1.2.Y	Description
1	.1	Gives the starting rvalue
2	.2	Gives the consecutive rvalue
3	n	Gives the next consecutive realm-name
4	100	Gives the index of dialed-numbers

This table lists and describes the apNSEPRealmStats MIB objects.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Sequence Number	Object ID apNSEPRealmStats 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.4 +	Description
1	.X.Y.1	Current Active Sessions Inbound
2	.X.Y.2	Total Sessions Inbound
3	.X.Y.3	Max of current window Session Inbound
4	.X.Y.4	Total session rejected Inbound
5	.X.Y.5	Current Active Sessions Outbound
6	.X.Y.6	Total Sessions Outbound
7	.X.Y.7	Max of current window Session Outbound
8	.X.Y.8	Total session rejected Outbound

To maintain index values for different rValues, the SBC uses a static mapping between all possible rValues and their corresponding indexes. This mapping resides in a table that assigns an idex to every possible r-value and maps all dialed numbers to the index number 100. This maintains a fixed, non-configurable assignment of a particular index number for each rValues and dialed-numbers.

apAppsLatestPeakLicenseUsage

The latest-peak-license-usage MIBOIDs provide you with data collected by the Latest Peak License Usage feature on the SBC. This data includes total, SRTP, and transcoding peak session utilization. The system collects this data every 15 minutes, and updates each session type's peak usage KPI for that window.

You can access the data captured by this feature using SNMP. The data returned by SNMP includes a response with the timestamp on which the most recent 15-minute window collection event occurred, and the data captured within that window.

> **Note**
>
> You cannot retrieve the output of the **show peak-concurrent-license-usage** command via SNMP.

The SBC uses a set of tables and indexes to create usable output for this peak license usage feature. The applicable SNMP objects are contained within apapps.mib. The root label for this SNMP table is APAPPS-MIB:: ApAppsLatestPeakLicenseUsageEntry.

The applicable SNMP walk produces the apAppsLatestPeakLicenseUsageTable. This table lists the ApAppsLatestPeakLicenseUsageEntry entries, which consist of one index and two groups.

- Index—ApLatestPeakLicenseUsageSessionsType, which uses the following enumerated values:
  - totalSessions(1)
  - srtpSessions(2)
  - amrTranscodingSessions(3)

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - amrwbTranscodingSessions(4)
  - evsTranscodingSessions(5)
  - opusTranscodingSessions(6)
  - silkTranscodingSessions(7)
  - evrcTranscodingSessions(8)
  - evrcbTranscodingSessions(9)
  - sessionsTypeMax(10)
- Group—apLatestPeakLicenseUsageHighCount
- Group—apLatestPeakLicenseUsageTimeStamp

Assuming you have all 9 Session License Usages configured, the SBC would fetch 18 OIDs, two each generated by the 9 Session Types. Each session type would have one highcount OID and one timestamp OID (when highcount is reached).

These system generates all OIDs by appending the digits 1 through 9 to their prefix OID. This table uses the root prefix, apLatestPeakLicenseUsageHighCount (1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*), with the high count value available via the last digit.

SessionType	Prefix OID (apLatestPeakLicenseUsageHighCount)	highcount
totalSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.1
srtpSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.2
amrTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.3
amrwbTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.4
evsTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.5
opusTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.6
silkTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.7
evrcTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.8
evrcbTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2.*	.9

This table uses the root prefix, apLatestPeakLicenseUsageTimeStamp (1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*), with the timestamp value available via the last digit.

SessionType	Prefix OID (apLatestPeakLicenseUsageTimeStamp)	timestamp
totalSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.1
srtpSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.2

Copyright © 2024, 2026, Oracle and/or its affiliates.

SessionType	Prefix OID (apLatestPeakLicenseUsageTimeStamp)	timestamp
amrTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.3
amrwbTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.4
evsTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.5
opusTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.6
silkTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.7
evrcTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.8
evrcbTranscodingSessions	1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3.*	.9

apDosThresholdCountersGroup

The following describes the dos-threshold-counters SNMP MIB.

- ap-apps.mib
- apDosThresholdCountersGroup
- 1.3.6.1.4.1.9148.3.16.5

The following table lists and describes the apDosThresholdCountersGroup MIB objects. To form the OID, add 1.3.6.1.4.1.9148.3.16.5 to the value in the OID # column. The OID for Trusted Minor Counter, for example, is 1.3.6.1.4.1.9148.3.16.5.2.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.5 +	Description
apDosTrustedMinorCounter	.1	Counter incremented, when trusted bandwidth crossed the minor threshold percentage
apDosTrustedMajorCounter	.2	Counter incremented, when trusted bandwidth crossed the major threshold percentage
apDosTrustedCriticalCounter	.3	Counter incremented, when trusted bandwidth crossed the critical threshold percentage
apDosUntrustedMinorCounter	.4	Counter incremented, when untrusted bandwidth crossed the minor threshold percentage
apDosUntrustedMajorCounter	.5	Counter incremented, when untrusted bandwidth crossed the major threshold percentage
apDosUntrustedCriticalCounter	.6	Counter incremented, when untrusted bandwidth crossed the critical threshold percentage
apDosArpMinorCounter	.7	Counter incremented, when ARP bandwidth crossed the minor threshold percentage

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.5 +	Description
apDosArpMajorCounter	.8	Counter incremented, when ARP bandwidth crossed the major threshold percentage
apDosArpCriticalCounter	.9	Counter incremented, when ARP bandwidth crossed the critical threshold percentage

MSRP MIB Objects

The following tables describe the SNMP MSRP Get query objects for the SIP MIB (ap-app.mib). There are two categories, including system-wide statistics and realm specific statistics:

- MSRP System Objects—These OIDs append to apMSRPKPISystemStats (1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.*). These OIDs are within ap-apps.mib under the package apAppsMSRPKPISystemStatsTable.
- MSRP Realm Objects—These OIDs append to apMSRPKPIRealmStats (1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.*). These OIDs are within ap-apps.mib under the package apAppsMSRPKPIRealmTable.

System Level Objects

The table below lists and describes the GET query names for MSRP Extended system KPI Objects when reporting on the system.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3. (counter type).+	Description
msrp-AvgSENDTransTx	1	The average number of MSRP SEND transactions transmitted by the SBC per session
msrp-AvgChatSENDTransTx	2	The average number of CHAT message SEND transactions transmitted by the SBC per session
msrp-AvgIsTypingSENDTransTx	3	The average number of IsTyping message SEND transactions transmitted by the SBC per session
msrp-AvgReceiptSENDTransTx	4	The average number of Receipt message SEND transactions transmitted by the SBC per session
msrp-AvgSENDMsgBytesTx	5	The average number of bytes in SEND transactions transmitted by the SBC per session
msrp-AvgChatSENDMsgBytesTx	6	The average number of bytes in CHAT message SEND transactions transmitted by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.(counter type).+	Description
msrp-AvgIsTypingSENDMsgBytesTx	7	The average number of bytes in IsTyping message SEND transactions transmitted by the SBC per session
msrp-AvgReceiptSENDMsgBytesTx	8	The average number of bytes in Receipt message SEND transactions transmitted by the SBC per session
msrp-SENDMsgBytesTx	9	The number of bytes in MSRP SEND transactions transmitted by the SBC
msrp-ChatSENDMsgBytesTx	10	The number of bytes in Chat message SEND transactions transmitted by the SBC
msrp-IsTypingMsgBytesTx	11	The number of bytes in IsTyping message SEND transactions transmitted by the SBC
msrp-ReceiptMsgBytesTx	12	The number of bytes in Receipt message SEND transactions transmitted by the SBC
msrp-SuccessREPORTTransTx	13	The number of Success Reports transmitted by the SBC
msrp-FailureREPORTTransTx	14	The number of Failure Reports transmitted by the SBC
msrp-AvgSuccessREPORTMsgBytesTx	15	The average number of bytes in Success Reports transmitted by the SBC per session
msrp-AvgREPORTFailureBytesTx	16	The average number of bytes in Failure Reports transmitted by the SBC per session
msrp-AvgREPORTFailureRateTx	17	The average number of Success and Failure Reports that were Failure Reports transmitted by the SBC
msrp-AvgREPORTSuccessRateTx	18	The average number of Success and Failure Reports that were Success Reports transmitted by the SBC
msrp-REPORTResp400Tx	19	The total number of Report responses that were 400 messages transmitted by the SBC
msrp-REPORTResp401Tx	20	The total number of Report responses that were 401 messages transmitted by the SBC
msrp-REPORTResp403Tx	21	The total number of Report responses that were 403 messages transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3. (counter type).+	Description
msrp-REPORTResp404Tx	22	The total number of Report responses that were 404 messages transmitted by the SBC
msrp-REPORTResp408Tx	23	The total number of Report responses that were 408 messages transmitted by the SBC
msrp-REPORTResp413Tx	24	The total number of Report responses that were 413 messages transmitted by the SBC
msrp-REPORTResp415Tx	25	The total number of Report responses that were 415 messages transmitted by the SBC
msrp-REPORTResp423Tx	26	The total number of Report responses that were 423 messages transmitted by the SBC
msrp-REPORTResp424Tx	27	The total number of Report responses that were 424 messages transmitted by the SBC
msrp-REPORTResp425Tx	28	The total number of Report responses that were 425 messages transmitted by the SBC
msrp-REPORTResp428Tx	29	The total number of Report responses that were 428 messages transmitted by the SBC
msrp-REPORTResp481Tx	30	The total number of Report responses that were 481 messages transmitted by the SBC
msrp-REPORTResp501Tx	31	The total number of Report responses that were 501 messages transmitted by the SBC
msrp-REPORTResp506Tx	32	The total number of Report responses that were 506 messages transmitted by the SBC
msrp-AvgREPORTFailureBytes400Tx	33	The average number of bytes in 400 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes401Tx	34	The average number of bytes in 401 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes403Tx	35	The average number of bytes in 403 Report Failure messages transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.(counter type).+	Description
msrp-AvgREPORTFailureBytes404Tx	36	The average number of bytes in 404 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes408Tx	37	The average number of bytes in 408 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes413Tx	38	The average number of bytes in 413 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes415Tx	39	The average number of bytes in 415 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes423Tx	40	The average number of bytes in 423 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes424Tx	41	The average number of bytes in 424 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes425Tx	42	The average number of bytes in 425 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes428Tx	43	The average number of bytes in 428 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes481Tx	44	The average number of bytes in 481 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes501Tx	45	The average number of bytes in 501 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes506Tx	46	The average number of bytes in 506 Report Failure messages transmitted by the SBC
msrp-TransResponsesTx	47	The total number of Responses transmitted by the SBC
msrp-SuccessTransResponsesTx	48	The total number of Success Responses transmitted by the SBC
msrp-TransResp400Tx	49	The total number of 400 Responses transmitted by the SBC
msrp-TransResp401Tx	50	The total number of 401 Responses transmitted by the SBC
msrp-TransResp403Tx	51	The total number of 403 Responses transmitted by the SBC
msrp-TransResp404Tx	52	The total number of 404 Responses transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3. (counter type).+	Description
msrp-TransResp408Tx	53	The total number of 408 Responses transmitted by the SBC
msrp-TransResp413Tx	54	The total number of 413 Responses transmitted by the SBC
msrp-TransResp415Tx	55	The total number of 415 Responses transmitted by the SBC
msrp-TransResp423Tx	56	The total number of 423 Responses transmitted by the SBC
msrp-TransResp424Tx	57	The total number of 424 Responses transmitted by the SBC
msrp-TransResp425Tx	58	The total number of 425 Responses transmitted by the SBC
msrp-TransResp428Tx	59	The total number of 428 Responses transmitted by the SBC
msrp-TransResp481Tx	60	The total number of 481 Responses transmitted by the SBC
msrp-TransResp501Tx	61	The total number of 501 Responses transmitted by the SBC
msrp-TransResp506Tx	62	The total number of 506 Responses transmitted by the SBC
msrp-AvgSENDTransRx	63	The average number of MSRP SEND transactions received by the SBC per session
msrp-AvgChatSENDTransRx	64	The average number of CHAT message SEND transactions received by the SBC per session
msrp-AvgIsTypingSENDTransRx	65	The average number of IsTyping message SEND transactions received by the SBC per session
msrp-AvgReceiptSENDTransRx	66	The average number of Receipt message SEND transactions received by the SBC per session
msrp-AvgSENDMsgBytesRx	67	The average number of bytes in SEND transactions received by the SBC per session
msrp-AvgChatSENDMsgBytesRx	68	The average number of bytes in Chat message SEND transactions received by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.(counter type).+	Description
msrp-AvgIsTypingSENDMsgBytesRx	69	The average number of bytes in IsTyping message SEND transactions received by the SBC per session
msrp-AvgReceiptSENDMsgBytesRx	70	The average number of bytes in Receipt message SEND transactions received by the SBC per session
msrp-SENDMsgBytesRx	71	The number of bytes in MSRP SEND transactions received by the SBC
msrp-ChatSENDMsgBytesRx	72	The number of bytes in Chat message SEND transactions received by the SBC
msrp-IsTypingMsgBytesRx	73	The number of bytes in IsTyping message SEND transactions received by the SBC
msrp-ReceiptMsgBytesRx	74	The number of bytes in Receipt message SEND transactions received by the SBC
msrp-SuccessREPORTTransRx	75	The number of Success Reports received by the SBC
msrp-FailureREPORTTransRx	76	The number of Failure Reports received by the SBC
msrp-AvgSuccessREPORTMsgBytesRx	77	The average number of bytes in Success Reports received by the SBC per session
msrp-AvgREPORTFailureBytesRx	78	The average number of bytes in Success Reports received by the SBC per session
msrp-AvgREPORTFailureRateRx	79	The average number of Reports received by the SBC that were Failure Reports
msrp-AvgREPORTSuccessRateRx	80	The average number of Reports received by the SBC that were Success Reports
msrp-REPORTResp400Rx	81	The total number of Report responses conveying 400 messages received by the SBC
msrp-REPORTResp401Rx	82	The total number of Report responses conveying 401 messages received by the SBC
msrp-REPORTResp403Rx	83	The total number of Report responses conveying 403 messages received by the SBC
msrp-REPORTResp404Rx	84	The total number of Report responses conveying 404 messages received by the SBC
msrp-REPORTResp408Rx	85	The total number of Report responses conveying 408 messages received by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3. (counter type).+	Description
msrp-REPORTResp413Rx	86	The total number of Report responses conveying 413 messages received by the SBC
msrp-REPORTResp415Rx	87	The total number of Report responses conveying 415 messages received by the SBC
msrp-REPORTResp423Rx	88	The total number of Report responses conveying 423 messages received by the SBC
msrp-REPORTResp424Rx	89	The total number of Report responses conveying 424 messages received by the SBC
msrp-REPORTResp425Rx	90	The total number of Report responses conveying 425 messages received by the SBC
msrp-REPORTResp428Rx	91	The total number of Report responses conveying 428 messages received by the SBC
msrp-REPORTResp481Rx	92	The total number of Report responses conveying 481 messages received by the SBC
msrp-REPORTResp501Rx	93	The total number of Report responses conveying 501 messages received by the SBC
msrp-REPORTResp506Rx	94	The total number of Report responses conveying 506 messages received by the SBC
msrp-AvgREPORTFailureBytes400Rx	95	The average number of Failure Report bytes conveying 400 messages received by the SBC per session
msrp-AvgREPORTFailureBytes401Rx	96	The average number of Failure Report bytes conveying 401 messages received by the SBC per session
msrp-AvgREPORTFailureBytes403Rx	97	The average number of Failure Report bytes conveying 403 messages received by the SBC per session
msrp-AvgREPORTFailureBytes404Rx	98	The average number of Failure Report bytes conveying 404 messages received by the SBC per session
msrp-AvgREPORTFailureBytes408Rx	99	The average number of Failure Report bytes conveying 408 messages received by the SBC per session
msrp-AvgREPORTFailureBytes413Rx	100	The average number of Failure Report bytes conveying 413 messages received by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.(counter type).+	Description
msrp-AvgREPORTFailureBytes415Rx	101	The average number of Failure Report bytes conveying 415 messages received by the SBC per session
msrp-AvgREPORTFailureBytes423Rx	102	The average number of Failure Report bytes conveying 423 messages received by the SBC per session
msrp-AvgREPORTFailureBytes424Rx	103	The average number of Failure Report bytes conveying 424 messages received by the SBC per session
msrp-AvgREPORTFailureBytes425Rx	104	The average number of Failure Report bytes conveying 425 messages received by the SBC per session
msrp-AvgREPORTFailureBytes428Rx	105	The average number of Failure Report bytes conveying 428 messages received by the SBC per session
msrp-AvgREPORTFailureBytes481Rx	106	The average number of Failure Report bytes conveying 481 messages received by the SBC per session
msrp-AvgREPORTFailureBytes501Rx	107	The average number of Failure Report bytes conveying 501 messages received by the SBC per session
msrp-AvgREPORTFailureBytes506Rx	108	The average number of Failure Report bytes conveying 506 messages received by the SBC per session
msrp-TransResponsesRx	109	The total number of Response transactions received by the SBC
msrp-SuccessTransResponsesRx	110	The total number of Success Response transactions received by the SBC
msrp-TransResp400Rx	111	The total number of Response transactions conveying 400 messages received by the SBC
msrp-TransResp401Rx	112	The total number of Response transactions conveying 401 messages received by the SBC
msrp-TransResp403Rx	113	The total number of Response transactions conveying 403 messages received by the SBC
msrp-TransResp404Rx	114	The total number of Response transactions conveying 404 messages received by the SBC
msrp-TransResp408Rx	115	The total number of Response transactions conveying 408 messages received by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3.(counter type).+	Description
msrp-TransResp413Rx	116	The total number of Response transactions conveying 413 messages received by the SBC
msrp-TransResp415Rx	117	The total number of Response transactions conveying 415 messages received by the SBC
msrp-TransResp423Rx	118	The total number of Response transactions conveying 423 messages received by the SBC
msrp-TransResp424Rx	119	The total number of Response transactions conveying 424 messages received by the SBC
msrp-TransResp425Rx	120	The total number of Response transactions conveying 425 messages received by the SBC
msrp-TransResp428Rx	121	The total number of Response transactions conveying 428 messages received by the SBC
msrp-TransResp481Rx	122	The total number of Response transactions conveying 481 messages received by the SBC
msrp-TransResp501Rx	123	The total number of Response transactions conveying 501 messages received by the SBC
msrp-TransResp506Rx	124	The total number of Response transactions conveying 506 messages received by the SBC

Realm Level Objects

The table below lists and describes the GET query names for MSRP Extended system KPI Objects when reporting on realms.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-AvgSENDTransTx	1	The average number of MSRP SEND transactions transmitted by the SBC per session
msrp-AvgChatSENDTransTx	2	The average number of CHAT message SEND transactions transmitted by the SBC per session
msrp-AvgIsTypingSENDTransTx	3	The average number of IsTyping message SEND transactions transmitted by the SBC per session
msrp-AvgReceiptSENDTransTx	4	The average number of Receipt message SEND transactions transmitted by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-AvgSENDMsgBytesTx	5	The average number of bytes in SEND transactions transmitted by the SBC per session
msrp-AvgChatSENDMsgBytesTx	6	The average number of bytes in CHAT message SEND transactions transmitted by the SBC per session
msrp-AvgIsTypingSENDMsgBytesTx	7	The average number of bytes in IsTyping message SEND transactions transmitted by the SBC per session
msrp-AvgReceiptSENDMsgBytesTx	8	The average number of bytes in Receipt message SEND transactions transmitted by the SBC per session
msrp-SENDMsgBytesTx	9	The number of bytes in MSRP SEND transactions transmitted by the SBC
msrp-ChatSENDMsgBytesTx	10	The number of bytes in Chat message SEND transactions transmitted by the SBC
msrp-IsTypingMsgBytesTx	11	The number of bytes in IsTyping message SEND transactions transmitted by the SBC
msrp-ReceiptMsgBytesTx	12	The number of bytes in Receipt message SEND transactions transmitted by the SBC
msrp-SuccessREPORTTransTx	13	The number of Success Reports transmitted by the SBC
msrp-FailureREPORTTransTx	14	The number of Failure Reports transmitted by the SBC
msrp-AvgSuccessREPORTMsgBytesTx	15	The average number of bytes in Success Reports transmitted by the SBC per session
msrp-AvgREPORTFailureBytesTx	16	The average number of bytes in Failure Reports transmitted by the SBC per session
msrp-AvgREPORTFailureRateTx	17	The average number of Success and Failure Reports that were Failure Reports transmitted by the SBC
msrp-AvgREPORTSuccessRateTx	18	The average number of Success and Failure Reports that were Success Reports transmitted by the SBC
msrp-REPORTResp400Tx	19	The total number of Report responses that were 400 messages transmitted by the SBC
msrp-REPORTResp401Tx	20	The total number of Report responses that were 401 messages transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-REPORTResp403Tx	21	The total number of Report responses that were 403 messages transmitted by the SBC
msrp-REPORTResp404Tx	22	The total number of Report responses that were 404 messages transmitted by the SBC
msrp-REPORTResp408Tx	23	The total number of Report responses that were 408 messages transmitted by the SBC
msrp-REPORTResp413Tx	24	The total number of Report responses that were 413 messages transmitted by the SBC
msrp-REPORTResp415Tx	25	The total number of Report responses that were 415 messages transmitted by the SBC
msrp-REPORTResp423Tx	26	The total number of Report responses that were 423 messages transmitted by the SBC
msrp-REPORTResp424Tx	27	The total number of Report responses that were 424 messages transmitted by the SBC
msrp-REPORTResp425Tx	28	The total number of Report responses that were 425 messages transmitted by the SBC
msrp-REPORTResp428Tx	29	The total number of Report responses that were 428 messages transmitted by the SBC
msrp-REPORTResp481Tx	30	The total number of Report responses that were 481 messages transmitted by the SBC
msrp-REPORTResp501Tx	31	The total number of Report responses that were 501 messages transmitted by the SBC
msrp-REPORTResp506Tx	32	The total number of Report responses that were 506 messages transmitted by the SBC
msrp-AvgREPORTFailureBytes400Tx	33	The average number of bytes in 400 Report Failure messages transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-AvgREPORTFailureBytes401Tx	34	The average number of bytes in 401 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes403Tx	35	The average number of bytes in 403 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes404Tx	36	The average number of bytes in 404 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes408Tx	37	The average number of bytes in 408 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes413Tx	38	The average number of bytes in 413 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes415Tx	39	The average number of bytes in 415 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes423Tx	40	The average number of bytes in 423 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes424Tx	41	The average number of bytes in 424 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes425Tx	42	The average number of bytes in 425 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes428Tx	43	The average number of bytes in 428 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes481Tx	44	The average number of bytes in 481 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes501Tx	45	The average number of bytes in 501 Report Failure messages transmitted by the SBC
msrp-AvgREPORTFailureBytes506Tx	46	The average number of bytes in 506 Report Failure messages transmitted by the SBC
msrp-TransResponsesTx	47	The total number of Responses transmitted by the SBC
msrp-SuccessTransResponsesTx	48	The total number of Success Responses transmitted by the SBC
msrp-TransResp400Tx	49	The total number of 400 Responses transmitted by the SBC
msrp-TransResp401Tx	50	The total number of 401 Responses transmitted by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-TransResp403Tx	51	The total number of 403 Responses transmitted by the SBC
msrp-TransResp404Tx	52	The total number of 404 Responses transmitted by the SBC
msrp-TransResp408Tx	53	The total number of 408 Responses transmitted by the SBC
msrp-TransResp413Tx	54	The total number of 413 Responses transmitted by the SBC
msrp-TransResp415Tx	55	The total number of 415 Responses transmitted by the SBC
msrp-TransResp423Tx	56	The total number of 423 Responses transmitted by the SBC
msrp-TransResp424Tx	57	The total number of 424 Responses transmitted by the SBC
msrp-TransResp425Tx	58	The total number of 425 Responses transmitted by the SBC
msrp-TransResp428Tx	59	The total number of 428 Responses transmitted by the SBC
msrp-TransResp481Tx	60	The total number of 481 Responses transmitted by the SBC
msrp-TransResp501Tx	61	The total number of 501 Responses transmitted by the SBC
msrp-TransResp506Tx	62	The total number of 506 Responses transmitted by the SBC
msrp-AvgSENDTransRx	63	The average number of MSRP SEND transactions received by the SBC per session
msrp-AvgChatSENDTransRx	64	The average number of CHAT message SEND transactions received by the SBC per session
msrp-AvgIsTypingSENDTransRx	65	The average number of IsTyping message SEND transactions received by the SBC per session
msrp-AvgReceiptSENDTransRx	66	The average number of Receipt message SEND transactions received by the SBC per session
msrp-AvgSENDMsgBytesRx	67	The average number of bytes in SEND transactions received by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-AvgChatSENDMsgBytesRx	68	The average number of bytes in Chat message SEND transactions received by the SBC per session
msrp-AvgIsTypingSENDMsgBytesRx	69	The average number of bytes in IsTyping message SEND transactions received by the SBC per session
msrp-AvgReceiptSENDMsgBytesRx	70	The average number of bytes in Receipt message SEND transactions received by the SBC per session
msrp-SENDMsgBytesRx	71	The number of bytes in MSRP SEND transactions received by the SBC
msrp-ChatSENDMsgBytesRx	72	The number of bytes in Chat message SEND transactions received by the SBC
msrp-IsTypingMsgBytesRx	73	The number of bytes in IsTyping message SEND transactions received by the SBC
msrp-ReceiptMsgBytesRx	74	The number of bytes in Receipt message SEND transactions received by the SBC
msrp-SuccessREPORTTransRx	75	The number of Success Reports received by the SBC
msrp-FailureREPORTTransRx	76	The number of Failure Reports received by the SBC
msrp-AvgSuccessREPORTMsgBytesRx	77	The average number of bytes in Success Reports received by the SBC per session
msrp-AvgREPORTFailureBytesRx	78	The average number of bytes in Success Reports received by the SBC per session
msrp-AvgREPORTFailureRateRx	79	The average number of Reports received by the SBC that were Failure Reports
msrp-AvgREPORTSuccessRateRx	80	The average number of Reports received by the SBC that were Success Reports
msrp-REPORTResp400Rx	81	The total number of Report responses conveying 400 messages received by the SBC
msrp-REPORTResp401Rx	82	The total number of Report responses conveying 401 messages received by the SBC
msrp-REPORTResp403Rx	83	The total number of Report responses conveying 403 messages received by the SBC
msrp-REPORTResp404Rx	84	The total number of Report responses conveying 404 messages received by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-REPORTResp408Rx	85	The total number of Report responses conveying 408 messages received by the SBC
msrp-REPORTResp413Rx	86	The total number of Report responses conveying 413 messages received by the SBC
msrp-REPORTResp415Rx	87	The total number of Report responses conveying 415 messages received by the SBC
msrp-REPORTResp423Rx	88	The total number of Report responses conveying 423 messages received by the SBC
msrp-REPORTResp424Rx	89	The total number of Report responses conveying 424 messages received by the SBC
msrp-REPORTResp425Rx	90	The total number of Report responses conveying 425 messages received by the SBC
msrp-REPORTResp428Rx	91	The total number of Report responses conveying 428 messages received by the SBC
msrp-REPORTResp481Rx	92	The total number of Report responses conveying 481 messages received by the SBC
msrp-REPORTResp501Rx	93	The total number of Report responses conveying 501 messages received by the SBC
msrp-REPORTResp506Rx	94	The total number of Report responses conveying 506 messages received by the SBC
msrp-AvgREPORTFailureBytes400Rx	95	The average number of Failure Report bytes conveying 400 messages received by the SBC per session
msrp-AvgREPORTFailureBytes401Rx	96	The average number of Failure Report bytes conveying 401 messages received by the SBC per session
msrp-AvgREPORTFailureBytes403Rx	97	The average number of Failure Report bytes conveying 403 messages received by the SBC per session
msrp-AvgREPORTFailureBytes404Rx	98	The average number of Failure Report bytes conveying 404 messages received by the SBC per session
msrp-AvgREPORTFailureBytes408Rx	99	The average number of Failure Report bytes conveying 408 messages received by the SBC per session

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-AvgREPORTFailureBytes413Rx	100	The average number of Failure Report bytes conveying 413 messages received by the SBC per session
msrp-AvgREPORTFailureBytes415Rx	101	The average number of Failure Report bytes conveying 415 messages received by the SBC per session
msrp-AvgREPORTFailureBytes423Rx	102	The average number of Failure Report bytes conveying 423 messages received by the SBC per session
msrp-AvgREPORTFailureBytes424Rx	103	The average number of Failure Report bytes conveying 424 messages received by the SBC per session
msrp-AvgREPORTFailureBytes425Rx	104	The average number of Failure Report bytes conveying 425 messages received by the SBC per session
msrp-AvgREPORTFailureBytes428Rx	105	The average number of Failure Report bytes conveying 428 messages received by the SBC per session
msrp-AvgREPORTFailureBytes481Rx	106	The average number of Failure Report bytes conveying 481 messages received by the SBC per session
msrp-AvgREPORTFailureBytes501Rx	107	The average number of Failure Report bytes conveying 501 messages received by the SBC per session
msrp-AvgREPORTFailureBytes506Rx	108	The average number of Failure Report bytes conveying 506 messages received by the SBC per session
msrp-TransResponsesRx	109	The total number of Response transactions received by the SBC
msrp-SuccessTransResponsesRx	110	The total number of Success Response transactions received by the SBC
msrp-TransResp400Rx	111	The total number of Response transactions conveying 400 messages received by the SBC
msrp-TransResp401Rx	112	The total number of Response transactions conveying 401 messages received by the SBC
msrp-TransResp403Rx	113	The total number of Response transactions conveying 403 messages received by the SBC
msrp-TransResp404Rx	114	The total number of Response transactions conveying 404 messages received by the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object IDs: 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4.(realm ID).(counter type).+	Description
msrp-TransResp408Rx	115	The total number of Response transactions conveying 408 messages received by the SBC
msrp-TransResp413Rx	116	The total number of Response transactions conveying 413 messages received by the SBC
msrp-TransResp415Rx	117	The total number of Response transactions conveying 415 messages received by the SBC
msrp-TransResp423Rx	118	The total number of Response transactions conveying 423 messages received by the SBC
msrp-TransResp424Rx	119	The total number of Response transactions conveying 424 messages received by the SBC
msrp-TransResp425Rx	120	The total number of Response transactions conveying 425 messages received by the SBC
msrp-TransResp428Rx	121	The total number of Response transactions conveying 428 messages received by the SBC
msrp-TransResp481Rx	122	The total number of Response transactions conveying 481 messages received by the SBC
msrp-TransResp501Rx	123	The total number of Response transactions conveying 501 messages received by the SBC
msrp-TransResp506Rx	124	The total number of Response transactions conveying 506 messages received by the SBC

Note

The system establishes realm level stats OIDs for the first (or single) realm by adding the system-assigned realm identifier and the type and category as the suffix (.first realm identifier.*.*) to the base OID. Should there be multiple realms, the OID is similarly numbered using the suffix (.second realm identifier.*.*) for the second realm, and (.third realm identifier.*.*) for the third realm and so forth.

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). 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

apCodecMIBObjects

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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.7.1.1.1 +	Description
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.
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.
apCodecRealmCountEVRCNW	.30	The count of SDP media streams received in the realm which negotiated to the EVRCNW codec.
apCodecRealmCountEVRCNW0	.31	The count of SDP media streams received in the realm which negotiated to the EVRCNW0 codec.
apCodecRealmCountEVRCNW1	.32	The count of SDP media streams received in the realm which negotiated to the EVRCNW1 codec
apCodecRealmCountEVS	.33	The count of SDP media streams received in the realm which negotiated to the EVS codec.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
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.
apCodecTranscodingInUsePercentCurrent	.4	Transcoding sessions currently in-use as a percentage of total available sessions.
apCodecTranscodingInUsePercentHigh	.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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
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.
apSysXCodeEVRCBCapacity	.40	Percentage of licensed EVRCB transcoding sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP Object Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
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.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.13.1.1.2.1 +	Description
apDiamClfErrorStatsEntry	.1	N/A
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: 1.3.6.1.4.1.9148.3.13.1.2.1 +	Description
apDiamAcctSrvrHostName	.1	The Diameter Accounting Server host name.
apDiamAcctSrvrIPPort	.2	The Diameter Accounting Server IP address and port number: XX.XX.XX.XX:P
apDiamAcctSrvrOriginRealm	.3	The Diameter Accounting Server Origin Realm.
apDiamAcctSrvrOriginHost	.4	The Diameter Accounting Server Origin Host.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.13.1.2.1 +	Description
apDiamAcctSrvrTransportType	.5	The Diameter Accounting Server Transport Type.
apAcctMsgQueueAvailCurrent	.6	The current measured percentage value of space available
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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. • 0 - in service • 1 - lover 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.
apDnsAlgCurrentSucess	.1.5	Number of success responses in a recent period received on the DNS-ALG server in the given realm.
apDnsAlgTotalSucess	.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 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.14.1.2.2 +	Description
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).

To form the OID for an object, append the value in the OID column to 1.3.6.1.4.1.9148.3.3.1. For example, the OID for apEnvMonI2CState is 1.3.6.1.4.1.9148.3.3.1.1.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

The apEnvMonVoltageStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.2.1.1. This object is deprecated.

The apEnvMonTemperatureStatusEntry object has the OID 1.3.6.1.4.1.9148.3.3.1.3.1.1.

To form the OID for an object, append the value in the OID column to 1.3.6.1.4.1.9148.3.3.1.3.1.1. For example, the OID for apEnvMonTemperatureStatusType is 1.3.6.1.4.1.9148.3.3.1.3.1.1.2.

SNMP GET Query Name	OID	Description
apEnvMonTemperatureStatusType	2	Indicates the entity being monitored for temperature. Values are: • ds1624sMain (1) • ds1624sCPU (2) • lm84 (3) • lm75 (4) • lm75Main (5) • lm75Cpu (6) • lm75Phy (7)
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	OID	Description
apEnvMonTemperatureState	5	Current state of the temperature which can have one of the following values: • 1: initial: Temperature is at its initial state. • 2: normal: The temperature is normal. • 6: shutdown: The system should be shutdown immediately • 7: not present: The temperature sensor does not exist • 8: not functioning: The temperature sensor is not functioning properly. • 9: unknown. Cannot obtain information due to an internal error. Values specific to 3900/3950/4900: • 3: minor alarm - the temperature is greater than or equal to 69.7 degrees Celsius and less than 73.8 degrees Celsius. • 4: major alarm. The temperature is greater than or equal to 73.8 degrees Celsius and less than 77.9 degrees Celsius. • 5: critical alarm. The temperature is greater than or equal to 77.9 degrees Celsius. In general, the critical alarm is sent at 95% of the maximum allowed temperature, the major alarm at 90%, and the minor alarm at 85%.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.4.1.1 +	Description
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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.3.1.6.1.1 +	Description
apEnvMonPhyCardState	.4	The current state of the phy card. Values: 1: initial. 2: normal. 3: minor. 4: major. 5: critical. 6: shutdown. The system should be shutdown immediately 7: not present. The sensor does not exist. 8: not functioning. The sensor is not functioning properly. 9: unknown. Cannot obtain information due to an internal error. 10: undetectable. The component is not detectable.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.5.1.1.1 +	Description
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.
apLicenseACPFeature	.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.
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.
apLicenseIKEFeature	.18	
apLicenseIPsecTunCap	.19	IPsec Tunnel Capacity

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.5.1.1.1 +	Description
apLicenseAuthFeature	.20	
apLicenseDatabaseRegFeature	.21	
apLicenseDatabaseRegCap	.22	Database registration contact capacity
apLicenseSLBEndpointCap	.23	SLB endpoint capacity
apLicenseAMRLicensedCap	.24	AMR codec licensed capacity
apLicenseAMRWBLicensedCap	.25	AMR-WB codec licensed capacity
apLicenseEVRCLicensedCap	.26	EVRC codec licensed capacity
apLicenseEVRCBLicensedCap	.27	EVRCB codec licensed capacity
apLicenseOPUSLicensedCap	.28	OPUS codec licensed capacity
apLicenseSILKLicensedCap	.29	SILK codec licensed capacity
apLicenseEVSLicensedCap	.30	EVS codec licensed capacity

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.9.1.4.1 +	Description
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.

To fully identify an object you may need to access, you may need to consider two additional values that extend after the OIDs listed in the table above. To fully understand this detail, consider that the apSecurityCertificateTable has two indices:

- apSecurityCertificateConfigId (1.3.6.1.4.1.9148.3.9.1.10.1.1)
- apSecurityCertificateIndex (1.3.6.1.4.1.9148.3.9.1.10.1.2)

The combination of these two uniquely identify a certificate. Any instance of the tabular objects of this table, however, would have two additional numbers included the end of its OID.

Take the example of apSecurityCertificateCertSubject (1.3.6.1.4.1.9148.3.9.1.10.1.4). A possible OID of an instance could be 1.3.6.1.4.1.9148.3.9.1.10.1.4.18.3. In this example:

- 1.3.6.1.4.1.9148.3.9.1.10.1.4 is apSecurityCertificateCertSubject
- 18 would be the apSecurityCertificateConfigId value
- 3 would be the apSecurityCertificateIndex value

Copyright © 2024, 2026, Oracle and/or its affiliates.

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. +	Description
apSipSecInterfaceTotalRegistrations	.1.1	Total number of registrations on all secondary SIP interfaces.
apSipSecInterfaceRegThreshold	.1.2	The maximum threshold for registrations on all secondary SIP interfaces. If this threshold is exceeded, an alarm is raised.
apSipSecInterfaceClearThreshold	.1.3	The threshold for registrations on all secondary SIP interfaces to clear an alarm.
apSipVideoCallsActive	.2.1	Total number of Active Video Calls
apSipAudioCallsActive	.2.2	Total number of Active Audio Calls
apSipSRVCCStatsTotalSuccess	.3.1	Total successful SRVCC HO
apSipSRVCCStatsTotalFailed	.3.2	Total failed SRVCC HO
apSipSRVCCStatsTotalCallsAfterAnswer	.3.3	Total calls subjected to SRVCC after answer
apSipSRVCCStatsAfterAnswerSuccess	.3.4	Total successful SRVCC HO after answer
apSipSRVCCStatsAfterAnswerFailed	.3.5	Total failed SRVCC HO after answer
apSipSRVCCStatsTotalCallsDuringAlerting	.3.6	Total calls subjected to SRVCC during alerting.
apSipSRVCCStatsDuringAlertingSuccess	.3.7	Total successful SRVCC HO during alerting.
apSipSRVCCStatsDuringAlertingFailed	.3.8	Total failed SRVCC HO during alerting.
apSipSRVCCStatsAtcfCancel	.3.9	Total ATCF cancellations
apSipSRVCCStatsEmergencySuccess	.3.10	Total successful SRVCC HO for Emergency calls
apSipSRVCCStatsEmergencyFailed	.3.11	Total failed SRVCC HO for Emergency calls
apSipSRVCCStatsEatfCancel	.3.12	Total EATF Cancellations
apSipSRVCCStatsTotalCallsDuringPreAlerting	.3.13	Total calls subjected to SRVCC during pre-alerting
apSipSRVCCStatsDuringPreAlertingSuccess	.3.14	Total successful SRVCC HO during pre-alerting
apSipSRVCCStatsDuringPreAlertingFailed	.3.15	Total failed SRVCC HO during pre-alerting
apSipStatsActiveSubscriptionsRegEvt	4.1	Number of Active Reg Event Subscriptions in the SBC.
apSipStatsPerMaxSubscriptionsRegEvt	4.2	Lifetime PerMax Reg Event Subscriptions count in the SBC.
apSipStatsMaximumActiveSubscriptionsRegEvt	4.3	Count of Lifetime Maximum Active Reg Event Subscriptions in the SBC

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1. +	Description
apSipStatsTotalSubscriptionsRegEvt	4.4	Count of Lifetime Total Reg Event Subscriptions in the SBC.

Object Group	Object Name	Description
Object group in ap-sip.mib	apSipSecInterfaceRegObjectsGroup Includes: apSipSecInterfaceTotalRegistrations apSipSecInterfaceRegThreshold apSipSecInterfaceClearThreshold (apSipObjectGroups 1)	Object group to monitor registrations for secondary SIP interfaces.
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.
Object group in ap-sip.mib	apSipRegEvtSubStatsObjects (apSipMIBGeneralObjects 4)	Object group to monitor registration event subscriptions in the SBC.

MSRP Objects for SNMP

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPFdTableSize	1	The number of entries in the MSRP File Descriptor Table. The actual object counter on physical platforms is 32-bit long while on virtual platforms it is 64-bit.
apSipMSRPSessionIdTableSize	2	The number of entries in the MSRP Session-Id table.
apSipMSRPActiveSessions	3	The number of total Active MSRP Sessions.
apSipMSRPMaxActiveSessions	4	The number of max active MSRP sessions.
apSipMSRPEstablishedSessions	5	Total number of MSRP Established Sessions.
apSipMSRPProvisionedSessions	6	Total number of MSRP Provisioned Sessions.
apSipMSRPFinishedSessions	7	Total number of MSRP Finished Sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPAcceptedConnections	8	Total number of Accepted Connections in MSRP sessions.
apSipMSRPConnectedConnections	9	Total number of Connected Connections in MSRP sessions.
apSipMSRPReleasedConnections	10	Total number of Released Connections in MSRP sessions.
apSipMSRPStreamRequestReceived	11	Total number of Stream Requests Received in MSRP sessions.
apSipMSRPStreamRequestSent	12	Total number of stream Requests Sent in MSRP sessions.
apSipMSRPStreamResponseReceived	13	Total number of Stream Responses Received in MSRP sessions.
apSipMSRPStreamResponseSent	14	Total number of Stream Responses Sent in MSRP sessions.
apSipMSRPGlobalBufferedData	15	Current Global Buffer Data size for MSRP sessions.
apSipMSRPFlowAdd	16	Total number of MSRP Nat Flows Added.
apSipMSRPFlowDelete	17	Total number of MSRP Nat Flows Deleted.
apSipMSRPFailedSessionsCannotRoute	18	Total number of Failed MSRP Sessions due to No Session Route Failure.
apSipMSRPFailedSessionsCannotConnect	19	Total number of Failed MSRP Sessions that can not connect.
apSipMSRPFailedSessionsFingerprintMismatch	20	Total number of Falied MSRP Sessions due to Fingerprint Mismatches.
apSipMSRPFailedMessagesCannotBeSent	21	Total number of Message Send Failures in MSRP sessions.
apSipMSRPFailedMessagesMalformed	22	Total number of Malformed Messages Received in MSRP sessions.
apSipMSRPSendQFullEvents	23	Total number of TCP Send-Q Full Events in MSRP sessions.
apSipMSRPSendQCongestedEvents	24	Total number of TCP Send-Q Congested Events in MSRP sessions.
apSipMSRPSendQCongestionRelievedEvents	25	Total number of TCP Send-Q Relieved Events in MSRP sessions.
apSipMSRPStreamErrorNoTransId	26	Total number of No Trans-Id Stream Errors in MSRP sessions.
apSipMSRPStreamErrorNoMsgType	27	Total number of No Message Type Stream Errors in MSRP Sessions.
apSipMSRPStreamErrorNoByteLength	28	Total number of No Byte Length stream Errors in MSRP Sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPBufferLimitExceeded	29	Total number of Buffer Limit Exceeded Errors in MSRP Sessions.
apSipMSRPFailedConnectionInit	30	Total number of Connection Attempts Failed in MSRP Sessions.
apSipMSRPSessReprovMismatch	31	Total number of Session Reprovision Mismatches.
apSipMSRPTcpListenErrors	32	Total number of TCP Listen Errors in MSRP Sessions.
apSipMSRPTcpConnectError	33	Total number of TCP Connect Errors in MSRP Sessions.
apSipMSRPTcpError	34	Total number of TCP Errors in MSRP Sessions.
apSipMSRPNoFromHeaderSessionID	35	Total number of FROM Header without a session-id in MSRP Sessions.
apSipMSRPNoFromHeader	36	Total number of Messages without FROM Header in MSRP Sessions.
apSipMSRPFromHdrAddrParseError	37	Total number of FROM Header Parse errors in MSRP Sessions.
apSipMSRPNoFromHdrAddr	38	Total number of FROM Header with no Address in MSRP Sessions.
apSipMSRPNoFromHdrPort	39	Total number of FROM Header with no port in MSRP Sessions.
apSipMSRPNoFromHdrAuthority	40	Total number of From Header with no Authority in MSRP Sessions.
apSipMSRPFromHdrSrvMismatch	41	Total number of FROM Header service type mismatches in MSRP Sessions.
apSipMSRPSendFailNoDestFd	42	Total number of send failures due to No Destination File Descriptor found in MSRP Sessions.
apSipMSRPSendFailedNoDstSession	43	Total number of send failures due to No Destination Session found in MSRP Sessions.
apSipMSRPNoToHeaderSessionID	44	Total number of TO Headers without a session-id in MSRP Sessions.
apSipMSRPNoToHeader	45	Total number of Messages without TO Header in MSRP Sessions.
apSipMSRPToHdrAddrParseError	46	Total number of TO Headers Parse errors in MSRP Sessions.
apSipMSRPNoToHdrAddr	47	Total number of TO Headers with no Address in MSRP Sessions.
apSipMSRPNoToHdrPort	48	Total number of TO Headers with no port in MSRP Sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPNoToHdrAuthority	49	Total number of TO Headers with no Authority in MSRP Sessions.
apSipMSRPToHdrSrvMismatch	50	Total number of TO Header service type mismatches in MSRP Sessions.
apSipMSRPNoDestFdEntry	51	Total number of No Destination File Descriptor Entry Errors in MSRP Sessions.
apSipMSRPTcpSendFailure	52	Total number of TCP Send Failures in MSRP Sessions.
apSipMSRPFdTableInsertErrorCollision	53	Total number of Insert Collisions errors in File Descriptor Table.
apSipMSRPFdTableInsertErrorNoData	54	Total number of No Data Insert Errors in File Descriptor Table.
apSipMSRPFdTableInsertErrorMemory	55	Total number of Memory Insert Errors in File Descriptor Table.
apSipMSRPFdTableInsertErrorMaxHops	56	Total number of Max Hops Insert Errors in File Descriptor Table.
apSipMSRPFdTableInsertErrorBad	57	Total number of Bad Insert Errors in File Descriptor Table.
apSipMSRPSessionTableInsertErrorCollision	58	Total number of Insert Collisions Errors in Session Table.
apSipMSRPSessionTableInsertErrorNoData	59	Total number of No Data Insert Errors in Session Table.
apSipMSRPSessionTableInsertErrorMemory	60	Total number of Memory Insert Errors in Session Table.
apSipMSRPSessionTableInsertErrorMaxHops	61	Total number of Max Hops Insert Errors in Session Table.
apSipMSRPSessionTableInsertErrorBad	62	Total number of Bad Insert Errors in Session Table.
apSipMSRPFlowToSessionTableInsertError	63	Total number of Insert Errors in Flow-To-Session Table.
apSipMSRPNumPreProvSessions	64	Total number of PreProvisioned Sessions in MSRP Sessions.
apSipMSRPNumPreProvMessages	65	Total number of PreProvision RX Messages in MSRP Sessions.
apSipMSRPConnectionStateNoSession	66	Total number of Sockets in Initial State in MSRP Sessions.
apSipMSRPConnectionStateListening	67	Total number of Sockets in Listening State in MSRP Sessions.
apSipMSRPConnectionStatePending	68	Total number of Sockets in Pending State in MSRP Sessions.
apSipMSRPConnectionStateConnecting	69	Total number of Sockets in Connecting State in MSRP Sessions.
apSipMSRPConnectionStateConnected	70	Total number of Sockets in Connected State in MSRP Sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPConnectionStateEstablished	71	Total number of Sockets in Established State in MSRP Sessions.
apSipMSRPConnectionStateFinished	72	Total number of Sockets in Finished State in MSRP Sessions.
apSipMSRPConnectionStateReleased	73	Total number of Sockets in Released State in MSRP Sessions.
apSipMSRPUnqualifiedConnections	74	Total number of Sockets in Unqualified Status in MSRP Sessions.
apSipMSRPSessionStateNone	75	Total number of Sessions in Initial State.
apSipMSRPSessionStateListening	76	Total number of Sessions in Listening State.
apSipMSRPSessionStatePreProvisioned	77	Total number of Sessions in Pre-Provisioned State.
apSipMSRPSessionStateProvisioned	78	Total number of Sessions in Provisioned State.
apSipMSRPSessionStateEstablished	79	Total number of Sessions in Established State.
apSipMSRPSessionStateFinished	80	Total number of Sessions in Finished State.
apSipMSRPClosedFdTableSize	81	Closed FD Table Size.
apSipMSRPClosedFdTableInsertErrors	82	Total number of Insert Errors in Closed File Descriptor Table.
apSipMSRPNumFdForcedReleases	83	Total number of Forced Release File Descriptor in MSRP Sessions.
apSipMSRPNumForcedReleasedListenFdNotFound	84	Total number of Forced Release Listen File Descriptor Not Found in MSRP Sessions.
apSipMSRPNumForcedReleasedForkedFdNotFound	85	Total number of Forced Release Forked File Descriptor Not Found in MSRP Sessions.
apSipMSRPNumListenFdForcedReleased	86	Total number of Forced Release Listen File Descriptor in MSRP Sessions.
apSipMSRPRequestBytesReceived	87	Total number of Request Bytes Received in MSRP Sessions.
apSipMSRPRequestBytesSent	88	Total number of Request Bytes Sent in MSRP Sessions.
apSipMSRPResponseBytesReceived	89	Total number of Response Bytes Received in MSRP Sessions.
apSipMSRPResponseBytesSent	90	Total number of Response Bytes Sent in MSRP Sessions.
apSipMSRPUnqualifiedClose	91	Total number of Unqualified Closes in MSRP Sessions.
apSipMSRPUnconnectedClose	92	Total number of File Descriptor did not get any connection in MSRP Sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.1.5. +	Description
apSipMSRPAcceptErrorClose	93	Total number of Accept Error Closes in MSRP Sessions.
apSipMSRPPreProvisionClose	94	Total number of Pre-provision Closes in MSRP Sessions.
apSipMSRPReadErrorClose	95	Total number of Read Error Closes in MSRP Sessions.
apSipMSRPStreamErrorClose	96	Total number of Stream Error Closes in MSRP Sessions.
apSipMSRPBufferClose	97	Total number of Buffer Error Closes in MSRP Sessions.
apSipMSRPReleaseNotificationFailures	98	Total number of Release Notification send failures.
apSipMSRPReleaseNotificationUnsentNoId	99	Total number of Unsent Release Notifications due to No session ID.
apSipMSRPReleaseNotificationUnsentNoFd	100	Total number of Unsent Release Notifications due to invalid File Descriptor.
apSipMSRPReleaseNotificationUnsentNoListenFd	101	Total number of Unsent Release Notifications due to No Listen File Descriptor.
apSipMSRPAcceptedConnectionsCema	102	Total number of CEMA Accepted Connections.
apSipMSRPConnectedConnectionsCema	103	Total number of CEMA Connected Connections.
apSipMSRPActiveCemaSessions	104	Total number of Active CEMA Sessions.
apSipMSRPEstablishedSessionsSessmatch	105	Total number of Established Sessmatch Sessions.
apSipMSRPProvisionedSessionsSessmatch	106	Total number of Provisioned Sessmatch Sessions.
apSipMSRPActiveSessmatchSessions	107	Total number of Active Sessmatch Sessions.
apSipMSRPMessageFromHost	108	Total number of Messages Received from Host in MSRP Sessions.
apSipMSRPMessageToHost	109	Total number of Messages Sent to Host in MSRP Sessions.
apSipMSRPMessageToHostFail	110	Total number of Messages Sent to Host Failed in MSRP sessions.

Rate Statistics for Method Events

When configured, the SBC calculates SUCCESS, TIMEOUT and FAILURE percentages of client and server transactions for the SUBSCRIBE, NOTIFY and MESSAGE methods and makes them available via SNMP OIDs. The SBC contains these OIDs within apSipMethodStatsEventCount (1.3.6.1.4.1.9148.3.15.1.2.10.1.4.*). These OIDs are established in ap-sip.mib under the apSipMethodStatsTable package.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.2.10.1.4.*	Description
eventSuccessRate	9.1.55	Success Rate of SUBSCRIBE request on server transaction
eventTimeoutRate	9.1.56	Timeout Rate of SUBSCRIBE request on server transaction
eventFailureRate	9.1.57	Failure Rate of SUBSCRIBE request on server transaction
eventSuccessRate	9.2.55	Success Rate of SUBSCRIBE request on client transaction
eventTimeoutRate	9.2.56	Timeout Rate of SUBSCRIBE request on client transaction
eventFailureRate	9.2.57	Failure Rate of SUBSCRIBE request on client transaction
eventSuccessRate	10.1.55	Success Rate of NOTIFY request on server transaction
eventTimeoutRate	10.1.56	Timeout Rate of NOTIFY request on server transaction
eventFailureRate	10.1.57	Failure Rate of NOTIFY request on server transaction
eventSuccessRate	10.2.55	Success Rate of NOTIFY request on client transaction
eventTimeoutRate	10.2.56	Timeout Rate of NOTIFY request on client transaction
eventFailureRate	10.2.57	Failure Rate of NOTIFY request on client transaction
eventSuccessRate	13.1.55	Success Rate of MESSAGE request on server transaction
eventTimeoutRate	13.1.56	Timeout Rate of MESSAGE request on server transaction
eventFailureRate	13.1.57	Failure Rate of MESSAGE request on server transaction
eventSuccessRate	13.2.55	Success Rate of MESSAGE request on client transaction
eventTimeoutRate	13.2.56	Timeout Rate of MESSAGE request on client transaction
eventFailureRate	13.2.57	Failure Rate of MESSAGE request on client transaction

Realm Based SIP Method Statistics

You can configure the SBC to generate the same SIP method statistics that are provided on a system-wide basis on a realm basis by enabling the **snmp-sipmethod-stats** parameter in the applicable **realm-config**. These statistics are only available when you perform an SNMP WALK, GET or SNMPGETNEXT from you SNMP manager.

When deployed in high availability mode, statistics generated by this function are not replicated on a standby node, similar to system-wide SIP method statistics.

```
ORACLE(realm-config)#snmp-sipmethod-stats enabled
```

With respect to SNMP gets, this data is available within the same context as system-wide SIP method statistics, from the applicable table objects in ap-sip.mib. The applicable OID uses the

Copyright © 2024, 2026, Oracle and/or its affiliates.

same prefix as the system-wide statistics, 1.3.6.1.4.1.9148.3.15.1.2 under the package apSipRealmTable. The system nests the realm-based statistics under the package apSipRealmMethodStatsTable, completing each individual OID using the identifier and variables 11.2.1.5.X1.X2.X3.X4, with the variables enumerating specific statistics:

- X1 ranges from 1 to n, where n is the number of configured realms, enumerated within apSIPRealmIndex.
  The system generates the realm-index dynamically for all realms on which you have enabled **snmp-sipmethod-stats**. Perform an snmpwalk on the OID 1.3.6.1.4.1.9148.3.15.1.2.11.1.1.2 to retrieve this realm-index. This walk lists each applicable **real-config**, enumerating the value you use for X1.
- X2 values are 9,10 and 13, which enumerate the SIP Method types SUBSCRIBE (9), NOTIFY (10) and MESSAGE (13). This is the applicable subset of the 15 method types enumerated within ApSipMethodType.
- X3 ranges from 1 to 2, which enumerate the transaction types, including Server Transaction (1) and Client Transaction (2), which are the contents of ApSipMethodEventCode.
- X4 ranges from 1 to 57, which enumerates the event code types within ApSipMethodEventCode.

To collect this data,open your MIB browser, browse to the apSipRealmMIBTabularObjects package and perform GETNEXT. To interpret this data, identify your realm index and decode the output using apSIPRealmName, ApSipMethodType, ApSipMethodTransType, and ApSipMethodEventCode.

Rate Statistics for Method Events

When Configured, SBC keeps track of all requests and responses codes and success-rate, timeout-rate, and failure-rate for SUBSCRIBE, NOTIFY and MESSAGE SIP methods.

When configured, the SBC keeps track of all requests and responses codes and success-rate, timeout-rate, and failure-rate for SUBSCRIBE, NOTIFY and MESSAGE SIP methods. and makes them available via SNMP OIDs. The SBC contains these OIDs within apSipMethodStatsEventCount, which you retrieve using the walk (1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5.X1.X2.X3.X4), where:

- X1—Realm-index
- X2—SIP Method types SUBSCRIBE (9), NOTIFY (10) and MESSAGE (13)
- X3—transaction types (Server Transaction (1) and Client Transaction (2)
- X4—Eventcodes (1-57)

These OIDs are established in ap-sip.mib under the apSipMethodStatsTable package.

There are over 50 method statistics in the apSipMethodStatsEventCode table. The table below presents the method rates only, a table of SUBSCRIBE, NOTIFY and MESSAGE methods rates presented as client and server rate statistics. This table presents an example of how to access specific statistics, and can be understood to be expanded to include all of the methods within the apSipMethodStatsEventCode table.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5.X1.*	Description
eventSuccessRate	9.1.55	Success Rate of SUBSCRIBE request on server transaction

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5.X1.*	Description
eventTimeoutRate	9.1.56	Timeout Rate of SUBSCRIBE request on server transaction
eventFailureRate	9.1.57	Failure Rate of SUBSCRIBE request on server transaction
eventSuccessRate	9.2.55	Success Rate of SUBSCRIBE request on client transaction
eventTimeoutRate	9.2.56	Timeout Rate of SUBSCRIBE request on client transaction
eventFailureRate	9.2.57	Failure Rate of SUBSCRIBE request on client transaction
eventSuccessRate	10.1.55	Success Rate of NOTIFY request on server transaction
eventTimeoutRate	10.1.56	Timeout Rate of NOTIFY request on server transaction
eventFailureRate	10.1.57	Failure Rate of NOTIFY request on server transaction
eventSuccessRate	10.2.55	Success Rate of NOTIFY request on client transaction
eventTimeoutRate	10.2.56	Timeout Rate of NOTIFY request on client transaction
eventFailureRate	10.2.57	Failure Rate of NOTIFY request on client transaction
eventSuccessRate	13.1.55	Success Rate of MESSAGE request on server transaction
eventTimeoutRate	13.1.56	Timeout Rate of MESSAGE request on server transaction
eventFailureRate	13.1.57	Failure Rate of MESSAGE request on server transaction
eventSuccessRate	13.2.55	Success Rate of MESSAGE request on client transaction
eventTimeoutRate	13.2.56	Timeout Rate of MESSAGE request on client transaction
eventFailureRate	13.2.57	Failure Rate of MESSAGE request on client transaction

The following table contains all of the method events tracked for SUBSCRIBE, NOTIFY and MESSAGE methods as client and server transaction statistics. By extrapolating from the table above, you can identify the applicable OIDs by using the assembly sequence presented above and substituting the last digit in the OID with the applicable method event.

For example:

- 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5.10.9.1.55 displays the Success Rate of SUBSCRIBE requests on server transactions (realm index #10).
- 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5.10.9.1.1 displays the number of detected server transaction 100 trying events (realm index #10).

SNMP GET Query Name	apSipMethodStatsEventCode 1.3.6.1.4.1.9148.3.15.1.2.10.1.3	Description
event100Trying	.1	Detected 100 trying event

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	apSipMethodStatsEventCode 1.3.6.1.4.1.9148.3.15.1.2.10.1.3	Description
event180Ringing	.2	Detected 180 ringing event
event181Forwarded	.3	Detected 181 forwarding event
event182Queued	.4	Detected 182 queued event
event183Progress	.5	Detected 183 progress event
event1xxProvisional	.6	Detected 1xx provisional event
event200OK	.7	Detected 200 OK event
event202Accepted	.8	Detected 202 accepted event
event2xxSuccess	.9	Detected 2xx success event
event30xMoved	.10	Detected 30x moved event
event305UseProxy	.11	Detected 305 use proxy event
event380Alternative	.12	Detected 380 alternative event
event3xxRedirect	.13	Detected 3xx redirect event
event400BadRequest	.14	Detected 400 bad request event
event401Unauthorized	.15	Detected 401 unauthorized event
event403Forbidden	.16	Detected 403 forbidden event
event404NotFound	.17	Detected 404 not found event
event405NotAllowed	.18	Detected 405 not allowed event
event406NotAcceptable	.19	Detected 406 not acceptable event
event407ProxyAuthReq	.20	Detected 407 proxy authorize request event
event408RequestTimeout	.21	Detected 308 timeout request event
event415BadMediaType	.22	Detected 415 bad media type event
event420BadExtension	.23	Detected 420 bad extension event
event421ExtensionReqd	.24	Detected 421 extension requested event
event422TooShort	.25	Detected 422 too short event
event423TooBrief	.26	Detected 423 too brief event
event480Unavailable	.27	Detected 480 unavailable event
event481DoesNotExist	.28	Detected 481 does not exist event
event482LoopDetected	.29	Detected 482 loop detected event
event483TooManyHops	.30	Detected 483 too many hops event
event484AddressIncompl	.31	Detected 484 address incomplete event
event485Ambiguous	.32	Detected 485 ambiguous event
event486BusyHere	.33	486 busy here event
event487Terminated	.34	Detected 487 terminated event
event488NotAcceptable	.35	Detected 488 not acceptable event
event489BadEvent	.36	Detected 489 bad event event
event491ReqPending	.37	Detected 491 request pending event
event4xxClientError	.38	Detected 4xx client error event

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	apSipMethodStatsEventCode 1.3.6.1.4.1.9148.3.15.1.2.10.1.3	Description
event500InternalError	.39	Detected 500 internal error event
event501NotImplemented	.40	Detected 501 not implemented event
event502BadGateway	.41	Detected 502 bad gateway event
event503ServiceUnavail	.42	Detected 503 service unavailble event
event504GatewayTimeout	.43	Detected 504 gateway timeout event
event513MsgTooLarge	.44	Detected 513 message too large event
event580PreconFailure	.45	Detected 580 preconditions failure event
event5xxServerError	.46	Detected 5xx server error event
event600BusyEverywhere	.47	Detected 600 busy everywhere event
event603Decline	.48	Detected 603 decline event
event606NotAcceptable	.49	Detected 606 not acceptable event
event6xxGlobalError	.50	Detected 6xx global error event
eventRequests	.51	Detected request event
eventRetransmissions	.52	Detected retransmission event
eventResponseRetrans	.53	Detected response retransmission event
eventTransactionTimeouts	.54	Detected transaction timeout event
eventSuccessRate	.55	Detected success rate
eventTimeoutRate	.56	Detected timeout rate
eventFailureRate	.57	Detected failure rate

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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).
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.example.com)
apSyslogHistLevel	.3	Log level of the message.
apSyslogHistType	.4	Textual identification for the log type, which categorizes the log message.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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	System-wide global calls per second. This counter is calculated based on a sliding window of 100 seconds.
apSysNATCapacity	.7	Percentage of NAT table in Content Addressable Memory (CAM) utilization.
apSysARPCapacity	.8	Percentage of ARP table (in CAM) utilization.
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 (CPUa + CPUb)/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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.1 +	Description
apSysMgcpEndptDemTrustToUntrust	.21	Not Supported.
apSysMgcpEndptDemUntrustToDeny	.22	Not Supported.
apSysSipTotalCallsRejected	.25	Global counter for SIP calls that are rejected by the SBC
apSysCurrentEndptsDenied	.26	Global counter for current endpoints denied 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.
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.
apSysCPULoadAvgFiftnMinute	.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** ACLI command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
apCombinedStatsTotalSessionsNotAdmittedInbound	.9	Total number of non-bandwidth constraints that exceeded rejections on inbound sessions (for example, max-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 since the last time the system was rebooted or the statistics were manually cleared.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.1.1 +	Description
apCombinedStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.2.1 +	Description
apSipSAStatsSessionAgentIndex	.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.
apSipSAStatsSessionAgentHostname	.2	The hostname of the session agent for which the following statistics are being calculated.
apSipSAStatsSessionAgentType	.3	The type of the specified session agent, either SIP or H323.
apSipSAStatsCurrentActiveSessionsInbound	.4	Number of current active inbound sessions.
apSipSAStatsCurrentSessionRateInbound	.5	Current Inbound Session rate in CPS.
apSipSAStatsCurrentActiveSessionsOutbound	.6	Number of current active outbound sessions.
apSipSAStatsCurrentSessionRateOutbound	.7	Current outbound session rate in CPS.
apSipSAStatsTotalSessionsInbound	.8	Total number of inbound sessions during the 100 second sliding window period.
apSipSAStatsTotalSessionsNotAdmittedInbound	.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apSipSAStatsPeriodHighInbound	.10	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apSipSAStatsAverageRateInbound	.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apSipSAStatsTotalSessionsOutbound	.12	Total number of outbound sessions during the 100 second sliding window period.
apSipSAStatsTotalSessionsNotAdmittedOutbound	.13	Total number of outbound sessions rejected because of insufficient bandwidth.
apSipSAStatsPeriodHighOutbound	.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.2.1 +	Description
apSipSAStatsAverageRateOutbound	.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apSipSAStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apSipSAStatsPeriodSeizures	.17	Total number of seizures during the 100 second sliding window period.
apSipSAStatsPeriodAnswers	.18	Total number of answered sessions during the 100 second sliding window period.
apSipSAStatsPeriodASR	.19	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
apSipSAStatsAverageLatency	.20	Average observed one-way signaling latency during the 100 second sliding window period.
apSipSAStatsMaxLatency	.21	Maximum observed one-way signaling latency during the 100 second sliding window period.
apSipSAStatsSessionAgentStatus	.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
apH323SAStatsSessionAgentIndex	.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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.3.1 +	Description
apH323SAStatsSessionAgentHostname	.2	The hostname of the session agent for which the following statistics are being calculated.
apH323SAStatsSessionAgentType	.3	The type of the specified session agent, H323.
apH323SAStatsCurrentActiveSessionsInbound	.4	Number of current active inbound sessions.
apH323SAStatsCurrentSessionRateInbound	.5	Current Inbound Session rate in CPS.
apH323SAStatsCurrentActiveSessionsOutbound	.6	Number of current active outbound sessions
apH323SAStatsCurrentSessionRateOutbound	.7	Current outbound session rate in CPS
apH323SAStatsTotalSessionsInbound	.8	Total Number of inbound sessions during the 100 second sliding window period.
apH323SAStatsTotalSessionsNotAdmittedInbound	.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apH323SAStatsPeriodHighInbound	.10	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apH323SAStatsAverageRateInbound	.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apH323SAStatsTotalSessionsOutbound	.12	Total number of outbound sessions during the 100 second sliding window period.
apH323SAStatsTotalSessionsNotAdmittedOutbound	.13	Total number of outbound sessions rejected because of insufficient bandwidth.
apH323SAStatsPeriodHighOutbound	.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apH323SAStatsAverageRateOutbound	.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.3.1 +	Description
apH323SAStatsMaxBurstRate	.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apH323SAStatsPeriodSeizures	.17	Total number of seizures during the 100 second sliding window period.
apH323SAStatsPeriodAnswers	.18	Total number of answered sessions during the 100 second sliding window period.
apH323SAStatsPeriodASR	.19	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apH323SAStatsAverageLatency	.20	Average observed one-way signalling latency during the 100 second sliding window period.
apH323SAStatsMaxLatency	.21	Maximum observed one-way signalling latency during the 100 second sliding window period
apH323SAStatsSessionAgentStatus	.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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 calls per second (CPS) during the sliding window period. For example, if the query is made at 65th second after SBC application restart, CPS from 36th to 65th second is considered for this statistics calculation (sliding window period = 30 sec).
apSigRealmStatsCurrentActiveSessionsOutbound	.5	Number of current active outbound sessions.
apSigRealmStatsCurrentSessionRateOutbound	.6	Current outbound session rate in calls per second (CPS) during the sliding window period. For example, if the query is made at 65th second after SBC application restart, CPS from 36th to 65th second is considered for this statistics calculation (sliding window period = 30 sec).
apSigRealmStatsTotalSessionsInbound	.7	Total number of inbound sessions during the 100 second sliding window period.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
apSigRealmStatsMaxBurstRate	.15	Burst rate of traffic (both inbound and outbound) measured during the current window period. The time period is equal to the value of the configuration parameter burst-rate-window in the session constraint. It is equal to 1 if not configured. Its value is the number of active calls plus 1 divided by the time period.

Note

This is different from the MaxBurstRa

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1.1 +	Description
		tevalueinthe ACLIcommand "showsipdrealm". In the ACLI, it ist

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
		the high-water mark during the window period.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.2.4.1 +	Description
apSigRealmStatsAverageLatency (not supported)	.19	Average observed one-way signaling latency in milliseconds during the period.
apSigRealmStatsMaxLatency (not supported)	.20	Maximum observed one-way signaling 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.
apSigRealmStatsAverageQoSRFactor	.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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
apNetMgmtCtrlStatsStatsIncomingCurrent	.6	Number of incoming calls during the current period that match a destination identifier
apNetMgmtCtrlStatsStatsRejectedCurrent	.7	Number of apNetMgmtCtrlStatsIncomingCurrent that are rejected.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.3.1.1 +	Description
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
apNSEPStatsCurentActiveSessionsInbound	.1	Number of currently active inbound NSEP sessions.
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.)

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5 +	Description
apNSEPStatsReserveCurrentSessions	.6	Number of incoming NSEP calls from reserved NSEP session pool that occurred during current time period
apNSEPStatsReservePeriodHigh	.7	Maximum number of incoming NSEP calls from reserved NSEP session pool that occurred during a single time period.
apNSEPStatsReserveTotal	.8	Total number of incoming NSEP calls from reserved NSEP session pool that occurred during lifetime period.
apNSEPStatsCurrentActiveSessionsOutbound	.9	Active outbound sessions for current window
apNSEPStatsTotalSessionsOutbound	.10	Total outbound sessions in lifetime window
	.11	Highest outbound session in particular window

The apNSEPStatsRPHTable object has the OID 1.3.6.1.4.1.9148.3.2.1.5.5, and the apNSEPStatsRPHEntry 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

SNMP GET Query Name	Object ID: 1.3.6.1.4.1.9148.3.2.1.5.5.1 +	Description
apNSEPStatsRPHCurrentActiveSessionsOutbound	.6	Number of current active outbound NSEP sessions for this specific RPH value.
apNSEPStatsRPHTotalSessionsOutbound	.7	Total number of outbound NSEP sessions for this 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.
apLDAPServerIPAddress	.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 informarion encoded in the trap.
apTrapTableSysUptime	.4	SNMP sysUpTime when the trap was generated.
apTrapTableTrapID	.5	Trap ID assoicated 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 and … .3.66.66.66.3.3.3.3
3. aaa entries would appear last, represented by the instance IDs: ... .3.97.97.97.1.1.1.1 and 3.97.97.97.1.1.1.2

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: 1.3.6.1.4.1.9148.3.4.1.1.1.1 +	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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Multicore Monitoring MIB (ap-usbcsys.mib)

A variety of statistics that report information on the CPUs/Cores within the Oracle Communications Session Border Controller 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.
apUsbcSysSmMsgRate	.1.1.14.1	Session Manager SIP Messages, Enum Messages, and Cx Diameter messages per second
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.
apUsbcThreadUsageTable	.1.2.1.1	A table to hold the thread usage information, on a Session Border Controller.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Object Name	Object ID: 1.3.6.1.4.1.9148.3.17 +	Description
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.
apThreadEventPendingCurhigh	.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.
apThreadEventDroppedCurhigh	.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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Object Name	Object ID: 1.3.6.1.4.1.9148.3.17 +	Description
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.
apUsbcMbcdObjects	.1.2.5	An object grouping MBCD-related per-thread CPU utilization information.
apMbcdNumberOfThreads	.1.2.5.1	Number of MBCD threads.
apMbcdAverageCpuUtil	.1.2.5.2	Average CPU utilization.
apUsbcEbmdObjects	.1.2.6	
apEbmdNumberOfThreads	.1.2.6.1	Number of EBMD threads.
apEbmdAverageCpuUtil	.1.2.6.2	Average CPU utilization.
apUsbcDnsObjects	.1.2.7	
apDnsNumberOfThreads	.1.2.7.1	Number of DNS threads.
apDnsAverageCpuUtil	.1.2.7.2	Average CPU utilization.
apUsbcSysThreadNotRespondingTrap		System Thread is not responding

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
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

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

apUsbcSysDPDKObjects

This group of objects, found in the `ap-usbcsys.mib`, provide a listing of DPDK statistics.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.17.1.1.13 +	Description
apUsbcSysDPDKFwdPurpose	.1	A bitset representing Forwarding cores. 1s represent forwarding cores, while 0s represent non-forwarding cores.
apUsbcSysDPDKDOSPurpose	.2	A bitset representing DoS cores. Bits set to 1 represent DoS cores, while 0s represent non-DoS cores.
apUsbcSysDPDKSigPurpose	.3	A bitset representing signaling cores. Bits set to 1 represent signaling cores, while 0s represent non-signaling cores.
apUsbcSysDPDKTransPurpose	.4	A bitset representing transcoding Cores. Bits set to 1 represent transcoding cores, while 0s represent non-transcoding cores.
apUsbcSysDPDKCmdLine	.5	System CmdLine string - as defined in /proc/cmdline. (including relevant bootparams.)
apUsbcSysDPDKFileMem	.6	Total DPDK File Memory.
apUsbcSysDPDKSysMem	.7	Total DPDK System Memory
apUsbcSysDPDKNum1G	.8	Number of 1GB Hugepages allocated.
apUsbcSysDPDKNum2MB	.9	Number of 2MB hugepages allocated.
apUsbcSysDPDKHypervisorType	.10	The description regarding the system type and what hypervisor the system is running on (OVM, KVM, VMWare,...).
apUsbcSysDPDKAddFwdCores	.11	Number of additional cores that may be used for forwarding.
apUsbcSysDPDKAddSigCores	.12	Number of additional cores that may be used for signaling.
apUsbcSysDPDKAddTransCores	.13	Number of additional cores that may be used for transcoding.

apUsbcSysScalingObjects

This group of objects, found in the `ap-usbcsys.mib`, provide a listing of objects relating to scaling VMs.

Copyright © 2024, 2026, Oracle and/or its affiliates.

MIB Object	Object ID: 1.3.6.1.4.1.9148.3.17.1.1.12+	Description
apUsbcSysEstSessions	.1	Estimated number of unecrypted media sessions.
apUsbcSysEstG711G729Trans	.2	Estimated number of G711<->G729 transcoded media sessions.
apUsbcSysEstSigTPS	.3	Estimated number of signaling TPS.
apUsbcSysEstACLs	.4	Estimated number of ACLs.
apUsbcSysEstTCP	.5	Estimated number of TCP connections.
apUsbcSysEstTLS	.6	Estimated number of TLS connections.
apUsbcSysEstVLANs	.7	Estimated number of VLANs.

Copyright © 2024, 2026, Oracle and/or its affiliates.

5

SNMP-based Application Features

This chapter contains Oracle Communications Session Border Controller 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**

> **Note**
>
> Enabling **extra-method-stats** performs additional functions. Refer to this parameter's description in the *ACLI Reference Guide* to see what other functionality you are enabling.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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).

SNMP Reporting of Message Data Counters

The message data counter statistics feature enables the system to provide message rate statistics for Call Duration, Call Termination and SIP Methods output. These statistics can be retrieved via SNMP.

Call Duration Counters for SNMP Retrieval

Call duration counters are available by way of SNMP retrieval. These counters are the same as that reported by the **show sipd agents** and **show sipd realms** commands. The pertinent MIB objects are found in the ap-sip.mib file.

The applicable Call Duration counters and tables include:

- apSipSACallInfoStatusTable, which contains:
  - apSipSAStatsTotalCallDurationInbound
  - apSipSAStatsTotalCallDurationOutbound
- apSigRealmCallInfoStatusTable, which contains:
  - apSigRealmStatsTotalCallDurationInbound
  - apSigRealmStatsTotalCallDurationOutbound

Local and Remote Call Termination (BYE) Counters for SNMP Retrieval

Local and Remote Call Termination (BYE) counters are available by way of SNMP retrieval. These counters are the same as that reported by the **show sipd agents** and **show sipd realms** commands. The pertinent MIB objects are found in the ap-sip.mib file.

- apSipSaCallInfoStatusTable, including the Call Termination (BYE) counters:
  - apSipSAStatsTotalCallDropsNormal
  - apSipSAStatsTotalCallDropsLocal

Copyright © 2024, 2026, Oracle and/or its affiliates.

- apSigRealmCallInfoStatusTable, including the Call Duration counters:
  - apSigRealmStatsTotalCallDropsNormal
  - apSigRealmStatsTotalCallLocal

SIP Method Counters for SNMP Retrieval

Global SIP method counters are available by way of SNMP retrieval. These SIP Method counters are the same as that reported by the show sipd <method> command. The pertinent MIB objects are found in the ap-sip.mib file.

The apSipMethodStatsTable holds counters:

- apSipMethodStatsEventCount for each SIP method.
- apSipMethodStatsIndex, whether that SIP method is from server- or client- transaction perspective.
- apSipMethodStatsTransType, and the returned SIP response code.
- apSipMethodStatsEventCode associated with that method transaction and perspective.

The SBC supports an extension to its SIP methods counters for the INVITE method. The SBC uses the apSipInviteDetailStatsEventCodeTable and apSipInviteDetailStatsEventCodeTable tables to implement the list of configured responseCodeAndPhrase element details in SNMP. This follows a similar sequence to that of the apSipMethodStatsEntry table. The pertinent MIB objects are also found in the ap-sip.mib file.

The apSipInviteDetailStatsEventCodeEntry holds:

- apSipInviteDetailStatsEventCode, which is the code + phrase configured in ACLI.
- apSipInviteDetailStatsEventCodeIndex, which is the index of the configured response code + response phrase.

The apSipInviteDetailStatsEventCodeTable table is indexed by apSipInviteDetailStatsEventCodeIndex.

The apSipInviteDetailStatsEntry holds:

- apSipInviteDetailStatsTransType, which has the values of the server and client transaction set.
- apSipInviteDetailStatsEventCodeIndex, which is the index of the ACLI configuration element from the apSipInviteDetailStatsEventCodeTable.
- apSipInviteDetailStatsEventCount, which is the counter value of type Counter32

SRVCC Objects for SNMP Retrieval

SRVCC counters are available from the apSipSRVCCStatsobjects. The OID prefix is `1.3.6.1.4.1.9148.3.15.1.1.3` which is found in the `ap-sip.mib` file. The These counters are the same as that reported by the **show sipd srvcc** command.

The apSipSRVCCStatsobjects contains numerous SRVCC statistics and corresponds to the **show sipd srvcc** command and the **sip-srvcc** HDR group.

Rx Policy Server Objects for SNMP Retrieval

Rx policy server counters are available from the apDiamRxPolicyServerStatsTable. The OID prefix is `1.3.6.1.4.1.9148.3.13.1.1.2.3` which is found in the `ap-diameter.mib` file.

Copyright © 2024, 2026, Oracle and/or its affiliates.

The apDiamRxPolicyServerStatsTable contains numerous policy server statistics and corresponds to the **show policy-server stats** command and the **ext-Rx-policy-server** HDR group.

When system boots, every policy server object is assigned id which persists across subsequent reboots. If policy server objects are deleted, the id does not change. This is similar to how session agent objects have persistent indexing.

IKE Session Agent Objects for SNMP Retrieval

IKE Session Agent counters are available from apSecuritySAIKEStats. The OID prefix is `1.3.6.1.4.1.9148.3.9.5.1`which is found in the `ap-security.mib` file.

The apSecuritySAIKEStats contains numerous session agent statistics concerning IKE traffic and corresponds to the **show sa stats ike** command and **sa-ike** HDR group.

IMS-AKA Session Agent Objects for SNMP Retrieval

IMS-AKA session agent counters are available from apSecuritySAIMSAKAStats. The OID prefix is 1.3.6.1.4.1.9148.3.9.5.2 which is found in the ap-security.mib file.

The apSecuritySAIMSAKAStats contains numerous IMS-AKA session agent statistics and corresponds to the **show sa stats ims-aka all** command and **sa-imsaka** HDR group.

SRTP Session Agent Objects for SNMP Retrieval

SRTP Session Agent counters are available from apSecuritySASRTPStats. The OID prefix is `1.3.6.1.4.1.9148.3.9.5.3` which is found in the `ap-security.mib` file.

The apSecuritySASRTPStats contains numerous session agent statistics concerning SRTP traffic and corresponds to the **show sa stats srtp** command and **sa-srtp** HDR group.

Transcoding Load Objects for SNMP Retrieval

Transcoding load and resource utilization counters are available in the ap-codec.mib file. There are three groups which are presented, currently active transcoded session per licensed codec, maximum licensed capacity per licensed codec, load per DSP.

Active Transcoded Sessions

The apCodecTranscodingResourceUtilMIBObjects, OID: 1.3.6.1.4.1.9148.3.7.2.5 presents the current number of active sessions of licensed codecs. This is found in `ap-codec.mib`.

This object corresponds to **show xcode load** ACLI Command and **xcode-codec-util** HDR group.

DSP Load of Transcoding Module

The apCodecTranscodingTCULoadStatsTable, OID: 1.3.6.1.4.1.9148.3.7.2.6.1 presents a table of the following information in `ap-codec.mib`:

- TCU identifier
- TCM Identifier
- DSP Identifier
- Session Count for that DSP

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Current load for that DSP
- Peak load for that DSP
- DSP Overload state

> **Note**
>
> If the DSP is neither Active nor Overloaded then that DSP will not appear as an instance of the table.

This object corresponds to show xcode load -detail ACLI Command and xcode-tcm-util HDR group.

Licensed Codec Capacity

MIB Objects that present maximum capacity of licensed codecs are found in `ap-license.mib`, as part of the apLicenseEntry, OID:1.3.6.1.4.1.9148.3.5.1.1.1

This object corresponds to **show xcode load** ACLI Command and **xcode-codec-util** HDR group.

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: "sa1.dg.com"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000000 = STRING:
"sa1.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.15.1.2.3.1.210000001 = STRING:
"sa1.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: 1000000
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: "sa1.dg.com"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000000 = STRING:
"sa1.dg.com#192.168.26.2"
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.2.10000001 = STRING:
"sa1.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.9148.3.2.1.2.2.1.3.1000001 = INTEGER: 1
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
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. The values populated in each of these trap's fields/varbinds include:

- 1.3.6.1.2.1.1.3.0—System uptime
- 1.3.6.1.6.3.1.1.4.1.0—OID of the trap
- 1.3.6.1.4.1.9148.3.2.5.16.0—hostname/FQDN of the SA
- 1.3.6.1.4.1.9148.3.2.5.17.0—IP address of the SA
- 1.3.6.1.4.1.9148.3.2.5.18.0—state (Inservice/Out of Service)
- 1.3.6.1.4.1.9148.3.2.5.19.0—status (Inservice/standby/Out of Service)

This feature requires that you enable the **sa-routes-stats** and **sa-routes-traps** parameters in the **sip-config**. This feature also requires that the session agent's **ping-all-addresses** function be active.

CAC Utilization Statistics via SNMP

TheOracle Communications Session Border Controller 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 Communications Session Border Controller 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "Realm Connection Admission Control Stats Table."
        ::= { apSipMIBTabularObjects 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

TheOracle Communications Session Border Controller 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 Communications Session Border Controller 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Trap OIDs include:

- apSipCACUtilAlertTrap—1.3.6.1.4.1.9148.3.15.2.3.2.0.1
- apSipCACUtilClearTrap—1.3.6.1.4.1.9148.3.15.2.3.2.0.2

External Policy Server Connection Status Reporting

When the Oracle Communications Session Border Controller (SBC) loses connection to the external policy server or an attempt is unsuccessful, the SBC generates an SNMP trap. In addition to this trap, the SBC generates major or minor, non-health effecting alarms. When a connection is restored, the SBC sends a clear trap and clears the associated alarm.

> **Note**
>
> The SBC does not raise SNMP traps or connection down alarms when you cause the event with a configuration change, such as disabling a server element.

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 SBC
- 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

- 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 to establish a connection, the SBC makes another attempt without an additional trap.

During a switchover, the newly activated SBC 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. After the switchover, and upon every subsequent failed attempt to establish a connection, the SBC makes another attempt without an additional trap.

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

Alarms

Alarms that correspond with the traps above notify the user, as follows:

- When the SBC sends a connection down trap for a connection configured within a policy server cluster, it generates a minor alarm.
- When the SBC sends a connection down trap for a connection configured with an IP address and port, it generates a minor alarm.
- When the diameter connection is re-established, the SBC clears the alarm.
- When all connections associated with a single ext-policy-server are down, the SBC generates a major alarm.

The table below shows alarm information associated with a failed connection to an **ext-policy-server**.

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

You see this alarm using the **display-alarms** command.

```
ORACLE# display-alarms
1 alarms to show
ID      Task    Severity        First Occurred          Last Occurred
327689  97      4       2018-03-20 01:29:46     2018-03-20 01:29:46
Count   Description
1       External Policy Server (RACF) connection lost!!!
```

When multiple server connections are lost, the alarm appears as follows:

```
ORACLE# display-alarms
1 alarms to show
ID      Task    Severity        First Occurred          Last Occurred
327689  97      4       2018-03-20 01:30:56     2018-03-20 01:30:56
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
Count   Description
1       2 External Policy Server (RACF) connections lost!!!
```

The alarm definition is as follows:

- Definition: APP_ALARM_LOST_RACF_CONN - ID: 327689
- Text: External Policy Server (RACF) connection lost!!!
- Definition: APP_ALARM_LOST_CLF_CONN - ID: 327690
- Text: External Policy Server (CLF) connection lost!!!

These alarms remain cleared as long as all diameter connections are established. The alarm text provides counts of the number of connections that are down, which the system updates as connections go down or are re-established.

The alarm text differs, based on the number of servers down, as follows:

- External Policy Server (RACF) connection lost!!!" (one connection down)
- 2 External Policy Servers (RACF) connection lost!!!" (more than one connection down)

Copyright © 2024, 2026, Oracle and/or its affiliates.

A

Alarms Table

This topic lists alarms available on the SBC, their details, and when available, the corresponding SNMP traps enabled.

Table A-1 Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
CFG ALARM SAVE FAILED	393217	MAJOR	The save-config command execution failed on a standby Oracle Communications Session Border Controller 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)	1. Execute the command after 5 minutes or so. 2. Reboot the standby server if problem persists.	apSysMgmtCfgSaveFailTrap
MBCD ALARM INTERNAL	262146	MINOR	An internal software error.	Internal Error. No agent for socket <IPPort>.	Perform switchover & restart the systemIn case the problem still exists, the software may have encountered an error. Please contact Oracle Support.	No trap associated with this alarm.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
SD5_TEMPERATURE_HIGH_PHY0	NONE	CRITICAL:>100 °C MAJOR:>95°C MINOR:>90°C	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XXC (where XX.XX is the temperature in degrees)	Temperature X is at Y degrees C over minor/ major/critical threshold of Z (Where X is sensor name, Y is temperature and Z is threshold) 1. Check if fans or air vents that are obstructed 2. Check dust accumulation on vents or fans 3. Check Heating, Ventillation and Air Conditioning (HVAC) of the room. 4. Clean the filter	ap-env-monitor
No DSPs Present with Transcoding Feature Card (DSP_NONE_PRESENT)	NONE	Minor/0	A transcoding feature card is installed but no DSP modules are discovered.	NONE	Check transcoding modules are plugged in properly. Check for loose connection and reseat the TCU card. Run HW Diagnostics if this was not performed by administrator.	apSysMgmtHardwareErrorTrap
DSP Boot Failure (DSP_BOOT_FAILURE)	NONE	Critical/0	A DSP device fails to boot properly at system initialization. This alarm is not health affecting for a single DSP boot failure. DSPs that fail to boot will remain uninitialized and will be avoided for transcoding.	NONE	Run HW Diagnostics and contact Oracle Support.	apSysMgmtHardwareErrorTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
DSP Communications Timeout (DSP_COMMS_TIMEOUT)	NONE	Critical/100	A DSP fails to respond after 2 seconds with 3 retry messages. This alarm is critical and is health affecting.	NONE	Run HW Diagnostics and contact Oracle Support.	apSysMgmtHardwareErrorTrap
DSP Alerts (DSP_CORE_HALT)	NONE	Critical/100	A problem with the health of the DSP such as a halted DSP core. The software will attempt to reset the DSP and gather diagnostic information about the crash. This information will be saved in the /code directory to be retrieved by the user.	NONE	Run HW Diagnostics and contact Oracle Support.	apSysMgmtHardwareErrorTrap
DSP Temperature(DSP_TEMPERATURE_HIGH)	NONE	Clear 85°C Warning 86°C / 5 Minor 90°C / 25 Major 95°C/ 50 Critical 100°C/ 100	A DSP device exceeds the temperature threshold. If the temperature exceeds 90°C, a minor alarm will be set. If it exceeds 95°C, a major alarm will be set. If it exceeds 100°C, a critical alarm will be set. The alarm is cleared if the temperature falls below 85°C. The alarm is health affecting.	NONE	Check for Defective DSP, HVAC & environmental condition	apSysMgmtHardwareErrorTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
Transcoding Capacity Threshold Alarm (XCODE_UTIL_OVER_THRESHOLD) / 131329	NONE	Clear 80% Warning 95%	A warning alarm will be raised when the transcoding capacity exceeds a high threshold of 95%. The alarm will be cleared after the capacity falls below a low threshold of 80%. This alarm warns the user that transcoding resources are nearly depleted. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap
Licensed AMR Transcoding Capacity Threshold Alarm/131330	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the AMR transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
Licensed AMR-WB Transcoding Capacity Threshold Alarm/131331	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the AMR-WB transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap
Licensed EVRC Transcoding Capacity Threshold Alarm/131332	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the EVRC transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap
Licensed EVRCB Transcoding Capacity Threshold Alarm/131333	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the EVRCB transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
Licensed Opus Transcoding Capacity Threshold Alarm/131159	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the Opus transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap
Licensed SILK Transcoding Capacity Threshold Alarm/131159	NONE	Clear 80% Warning 95%	A warning alarm is triggered if the SILK transcoding capacity exceeds a high threshold of 95% of licensed session in use. The alarm clears after the capacity falls below a low threshold of 80%. This alarm is not health affecting.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apSysMgmtGroupTrap
LICENSE ALARM APPROACHING SESSION CAPACITY	327684	MAJOR	Total number of active sessions on the system (across all protocols) is within 98 to 100% of the system's licensed capacity.	total number of sessions (<#>) is approaching licensed capacity (<#>)	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apLicenseApproachingCapacityNotification
PLD POWER A UP	65541	MINOR	Power supply A is now present and functioning.	Back Power Supply A is present!	Run Hardware Diagnostics to rule out any issues, if there was no power fluctuation at datacentre.	apEnvMonPowerSupplyStatusEntr

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
PLD POWER B UP	65543	MINOR	Power supply B is now present and functioning.	Back Power Supply B is present!	Run Hardware Diagnostics to rule out any issues, if there was no power fluctuation at datacentre.	apEnvMonVoltageStatusEntry
PHY0 Removed	65550	MAJOR	Physical interface card 0 was removed.	PHY card 0 has been removed.	Check for loose connection and reseat the card. Run HW Diagnostics if this was not performed by administrator.	apEnvPhyCardStatusEntry
PHY0 Inserted	65552	MAJOR	Physical interface card 0 was inserted.	None	N/A	apEnvPhyCardStatusEntry
PHY1 Removed	65553	MAJOR	Physical interface card 1 was removed.	PHY card 1 has been removed.	Check for loose connection and reseat the card. Run HW Diagnostics if this was not performed by administrator.	apEnvPhyCardStatusEntry
PHY1 Inserted	65554	MAJOR	Physical interface card 1 was inserted.	None	N/A	apEnvPhyCardStatusEntry
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	Contact Oracle Support	apSysMgmtGroupTrap
ARP TABLE UTILIZATION	131103	MINOR	ARP table usage reached 90% or greater of its capacity.	ARP table X% over threshold X%	Contact Oracle Support	apSysMgmtGroupTrap
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	You may have reached configured bandwidth limit. Check the bandwidth configured	apSysMgmtMediaBandwidthTrap
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	You may have reached configured steering ports. Check the steering ports configured	apSysMgmtMediaPortsTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
H.323 ALARM STACK INITIALIZATION FAILURE	327682	CRITICAL	The H.323 stack has failed to initialize properly and is terminated.	[H.323 | IWF] stack <stack-name> has failed to initialize and is terminated	The software may have encountered an error. Please contact Oracle Support.	apSysMgmtH323InitFail
LINK DOWN ALARM FEPORT	131091	MAJOR	Fast Ethernet slot 1, port 0 goes down.	Slot 1 port 0 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
LINK DOWN ALARM FEPORT	131093	MAJOR	Fast Ethernet slot 1, port 1 goes down.	Slot 1 port 1 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
LINK DOWN ALARM FEPORT	131094	MAJOR	Fast Ethernet slot 2, port 1 goes down.	Slot 2 port 1 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
LINK DOWN ALARM FEPORT	131095	MAJOR	Fast Ethernet slot 1, port 2 goes down.	Slot 1 port 2 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
LINK DOWN ALARM FEPORT	131096	MAJOR	Fast Ethernet slot 2, port 2 goes down.	Slot 2 port 2 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
LINK DOWN ALARM FEPORT	131097	MAJOR	Fast Ethernet slot 1, port 3 goes down.	Slot 1 port 3 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
LINK DOWN ALARM FEPORT	131098	MAJOR	Fast Ethernet slot 2, port 3 goes down.	Slot 2 port 3 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
TEMPERATURE HIGH	65538	CRITICAL: -100 MAJOR: -50 MINOR: -25	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XXC (where XX.XX is the temperature in degrees)	1. Check if fans or air vents that are obstructed 2. Check dust accumulation on vents or fans 3. Check Heating, Ventillation and Air Conditioning (HVAC) of the room. 4. Clean the filter	apSysMgmtTempTrap
FAN STOPPED	65537	CRITICAL (-100): any fan speed is <50%. Or speed of two or more fans is >50% and <75%. MAJOR (-50): speed of two or more fans is > 75% and < 90%. Or speed of one fan is >50% and <75% and the other two fans are at normal speed. MINOR (-25): speed of one fan> 75% and <90%, the other two fans are at normal speed	Fan speed failure.	Fan speed: XXXX XXXX XXXX where xxxx xxxx xxxx is the Revolutions per Minute (RPM) of each fan on the fan module	1. Check if fans or air vents that are obstructed 2. Check dust accumulation on vents or fans. 3. Clean the filter	apSysMgmtFanTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
ENVIRONMENTAL SENSOR FAILURE	65539	CRITICAL (-10)	The environmental sensor component cannot detect fan speed and temperature.	Hardware monitor failure! Unable to monitor fan speed and temperature!	Power cycle the standby Oracle Communications Session Border Controller peer using the power supply on/off switches located on the rear panel of the chassis Force a manual switchover by executing the ACLI notify berpd force command Power cycle the active Oracle Communications Session Border Controller peer	apEnvMonI2CFailNotification
PLD POWER A FAILURE	65540	MINOR (-10)	Power supply A has failed.	Back Power Supply A has failed!	1. Check if the power supply is powered down. 2. Check whether the physical layer is functioning properly. This includes the server hardware, any attached peripherals, and the cabling.	apSysMgmtPowerTrap
PLD POWER B FAILURE	65542	MINOR (-10)	Power supply B has failed.	Back Power Supply B has failed!	1. Check if the power supply is powered down. 2. Check whether the physical layer is functioning properly. This includes the server hardware, any attached peripherals, and the cabling.	apSysMgmtPowerTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
CPU UTILIZATION	131099	MINOR	CPU usage reached 90% or greater of its capacity.	CPU usage X% over threshold X%	show processes top/show platform cpu-load. Contact Oracle Support	apSysMgmtGroupTrap
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)	Reboot (if the system is configured to do so)	apSysMgmtTaskSuspendTrap
MEMORY UTILIZATION	131100	MAJOR	Memory usage reached 90% or greater of its capacity.	Memory usage X% over threshold X%	Review the capacity on the sbc: show memory usage and contact Oracle Support.	apSysMgmtGroupTrap
HEALTH SCORE	131101	MAJOR	System's health score fell below 60.	Health score X is under threshold (where X is the health score)	Review the health on the device: show health to see the reason for the decrease in health.	apSysMgmtGroupTrap
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	Check if switchover was forced by command or due to unacceptable health	apSysMgmtRedundancyTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
REDUNDANT SWITCH-TO-STANDBY	131105	CRITICAL	A state transition occurred from Active/ BecomingActive to BecomingStandby/ RelinquishingActive.	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	Check for poor health score or a forced switchover	apSysRedundancy
REDUNDANT TIMEOUT	131106	MAJOR	A HA system peer was not heard from within a time period.	Peer <name of HA peer> timed out in state x, my state is x (where x is the state (for example, BecomingStandby))	Check for poor health score or a forced switchover	apSysRedundancy
REDUNDANT OUT OF SERVICE	131107	CRITICAL	Unable to synchronize with Active HA system peer within BecomingStandby timeout.	Unable to synchronize with Active redundant peer within BecomingStandby timeout, going OutOfService	Check network connection	apSysRedundancy
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.	1. Look for processes consuming excessive memory and consider restarting those processes 2. Perform SBC health check and verify any possible packet overload	apSysMgmtMediaOutofMemory
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	View Media Statistics to determine port utilization show mbcd realms show mbcd realms <realm name> show flows	apSysMgmtMediaUnknownRealm

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
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.	Verify the accounting status by running show radius command, ORACLE# show radius accounting.	apSysMgmtRadiusDownTrap
GATEWAY UNREACHABLE	dynamicID	MAJOR	The Oracle Communications Session Border Controller lost ARP connectivity to the 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 number, Z is the front interface port number, and ZZ is the subport ID)	Check to see if Gateway IP has changed or is down, show arp and ping test to down gateway	apSysMgmtGatewayUnreachableTrap
LINK UP ALARM GIGPORT	131073	MINOR	Gigabit Ethernet interface 1 goes up.	Slot 1 port 0 UP	N/A	linkUp
LINK UP ALARM GIGPORT	131074	MINOR	Gigabit Ethernet interface 2 goes up.	Slot 2 port 0 UP	N/A	linkUp

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
LINK DOWN ALARM GIGPORT	131075	MAJOR	Gigabit Ethernet interface 1 goes down.	Slot 1 port 0 DOWN	show interface ethernet - to check status of the link.	linkDown
LINK DOWN ALARM GIGPORT	131076	MAJOR	Gigabit Ethernet interface 2 goes down.	Slot 2 port 0 DOWN	show interface ethernet - to check status of the link.	linkDown
LINK UP ALARM VXINTF	131077	MINOR	Control interface 0 goes up.	Port 0 UP	N/A	linkUp
LINK UP ALARM VXINTF	131078	MINOR	Control interface 1 goes up.	Port 1 UP	N/A	linkUp
LINK UP ALARM VXINTF	131079	MINOR	Control interface 2 goes up.	Port 2 UP	N/A	linkUp
LINK DOWN ALARM VXINTF	131080	MAJOR	Control interface 0 goes down.	Port 0 DOWN	Gigabit Ethernet Interface :s1p0 XE goes down. The show arp command is one of the many show commands available to you on the Oracle Communications Session Border Controller. It displays the Link Level ARP table, ARP entries, and ARP table statistics.	linkDown

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
LINK DOWN ALARM VXINTF	131081	MAJOR	Control interface 1 goes down.	Port 1 DOWN	Gigabit Ethernet Interface:s1p1 XE goes down. The show arp command is one of the many show commands available to you on the Oracle Communications Session Border Controller. It displays the Link Level ARP table, ARP entries, and ARP table statistics.	linkDown
LINK DOWN ALARM VXINTF	131082	MAJOR	Control interface 2 goes down.	Port 2 DOWN	Gigabit Ethernet Interface: s0p3 XE goes down. The show arp command is one of the many show commands available to you on the Oracle Communications Session Border Controller. It displays the Link Level ARP table, ARP entries, and ARP table statistics.	linkDown
LINK UP ALARM FEPORT	131083	MAJOR	Fast Ethernet slot 1, port 0 goes up.	Slot 1 port 0 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131084	MAJOR	Fast Ethernet slot 2, port 0 goes up.	Slot 2 port 0 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131085	MINOR	Fast Ethernet slot 1, port 1 goes up.	Slot 1 port 1 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131086	MINOR	Fast Ethernet slot 2, port 1 goes up.	Slot 2 port 1 UP	linkUp trap generated syslog N/A	linkUp

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
LINK UP ALARM FEPORT	131087	MINOR	Fast Ethernet slot 1, port 2 goes up.	Slot 1 port 2 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131088	MINOR	Fast Ethernet slot 2, port 2 goes up.	Slot 2 port 2 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131089	MINOR	Fast Ethernet slot 1, port 3 goes up.	Slot 1 port 3 UP	linkUp trap generated syslog N/A	linkUp
LINK UP ALARM FEPORT	131090	MINOR	Fast Ethernet slot 2, port 3 goes up.	Slot 2 port 3 UP	linkUp trap generated syslog N/A	linkUp
LINK DOWN ALARM FEPORT	131092	MAJOR	Fast Ethernet slot 2, port 0 goes down.	Slot 2 port 0 DOWN	Indicates that the physical cable is disconnected. Verify that the cables are inserted correctly on both ends of the cable. Verify cable integrity. Replace cable.	linkDown
COMM MONITOR CONNECTION DOWN	327716 (Hex 50024)	Major	CommMonitor disconnected	One or more CommMonitors are disconnected	Check OCOM servers for connectivity and liveliness.	apMonitorCollectorDow nTrap
SRTP DECRYPTION ERROR	NONE	MAJOR	Decryption for SRTP packets fails	SRTP Decryption Failed	Check log.npsoft for the errors	apSecuritySrtpDecryptio nFailureNotification
SRTP ENCRYPTION ERROR	327744	MAJOR	Encryption integrity check for SRTP packets fails.	SRTP Encryption Failed	Check log.npsoft for the errors	apSecuritySrtpEncryption FailureNotification
TLS DECRYPTION ERROR	NONE	MAJOR	Decryption for TLS packets fails.	TLS Decryption Failed	Check log.atcpd for the errors	apSecurityTlsDecryption FailureNotification
TLS ENCRYPTION ERROR	NONE	MAJOR	Encryption integrity check for TLS packets fails.	TLS Encryption Failed	Check log.atcpd for the errors	apSecurityTlsEncryption FailureNotification

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
ENUM SERVER STATUS	327686	CRITICAL: All ENUM servers are unreachable MAJOR: Some ENUM servers are unreachable	The enabled connections to ENUM servers have been lost.	CRITICAL: All ENUM Servers are currently unreachable! MAJOR: One or more ENUM Servers are currently unreachable!	Check Enum Servers for connectivity and liveness.	apSysMgmtENUMStatusChangeTrap
DIAM ACCT BUFFER THRESHOLD EXCEED	327738	MINOR by default. The severity is configurable.	A Diameter Accounting Server has lost connectivity with the system	Diameter Accounting Server lost connection!!! Diameter Accounting Server Returned Error Result Code	1. Confirm the network latency with configured CCF servers and adjust queue size (account-config->msg-queue-size) 2. Suggestion would be to ajust below thresholds accordingly based on latency account-config->acr-buffer-upper-threshold account-config->acr-buffer-lower-threshold 3. Monitor show queues radd	apAcctMsgQueueUpperThresholdTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
STIR SERVER UNREACHABLE	327936	MAJOR or MINOR	A STIR SERVER or set of STIR SERVERS has lost connectivity with the system.	STIR Server 'stirDemo' connection timeout	1. Check for host resolution issues if FQDN was configured for STIR Server 2. Check for STIR Server reachability issue If IP Address was configured 3. check for network latency and verify associated config (stl-server->timeout) timeout value. 4. Check and verify tls profile attributes for STI-AS or STI-VS (http-client->tls-profile)	apStirServerUnreachable Trap
APP_ALARM_SC HBKP_PUSH_FAI L	327751	WARNING	The SBC has failed to upload the current configuration of the one (or more) configured push receivers.	Config backup failed to upload to remote server Hostname: <hostname>, IP: <ipaddress>, Path: <Path>	1. Check log file (log.schbkpd) for the failure reason 2. Some of the failure reasons could be a. remote server is not reachable b. remote path to where config file is to be copied does not exist or has permissions issue etc. NOTE: This alarm is to be cleared manually once the issue is cleared.	apConfigPushReceiverFailureTrap

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table A-1 (Cont.) Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
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% of license capacity.	NONE	Evaluate capacity planning & check your consumption to see if more capacity is needed. If that's the case, reach out to Oracle Sales	apLicenseApproachingCapacityNotification
ALARM_AUDIT_LOG_FULL	327694	MAJOR	Audit log full threshold met: time interval, file size, percentage full, or max storage handling.	File rotation time interval has elapsed, rotating file / code/audit/...	Check audit log rotation/full thresholds, audit file location, storage availability, and whether old audit files are being deleted/ rotated as expected.	apSysMgmtAdminAuditLogFullTrap (1.3.6.1.4.1.9148.3.2.6.0.58)
ALARM_AUDIT_WRITE_FAILED	327695	MAJOR	Audit write failed: audit file not open, I/O error, syslog send failure, or syslog logger unavailable.	Write to Audit file Failed to send audit logs to syslog server, error 0	Check audit output mode, audit file path, file permissions/ storage, syslog server reachability/ config, and auditd logs around AuditAgent::outputAsText.	apSysMgmtAdminWriteFailTrap (1.3.6.1.4.1.9148.3.2.6.0.62)
ALARM_ADMIN_AUDIT_PUSH_FAIL	327696	MAJOR	SFTP audit file transfer failed to configured push receiver. Common causes: bad receiver/port, SSH key/known-host issue, auth failure, remote path/server problem.	SFTP of /code/ audit/... to <server> failed	Check audit push receiver config, SFTP server/port, username/auth type, SSH keys/ known-host setup, remote path, network reachability, and audit pusher logs.	apSysMgmtAdminAuditPushFailTrap (1.3.6.1.4.1.9148.3.2.6.0.60)

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.