Oracle® Communications Unified Session Manager (USM)

MIB Reference Guide

Release S-CZ7.2.5

November 2014

About this Guide

Introduction

The *Oracle Communications Unified Session Manager 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
- Example of scalar and table objects
- 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.

Supported Platforms

Release Version S-CZ7.2.5 includes both the Oracle Core Session Manager (CSM) and Unified Session Manager (USM) products. The Oracle USM is supported on the Acme Packet 4500, 6100, and 6300 series platforms. The Oracle CSM is supplied as virtual machine software or as a software-only delivery suitable for operation on server hardware. Refer to sales documentation updates for information further specifying hardware support.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4500 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 6100 System Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100 system.

Document Name	Document Description
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the USM.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle USM logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the USM's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the USM's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the USM's support for its Administrative Security license.

Hardware documentation is relevant only to the Oracle USM. Refer to your hardware vendor's documentation for information required for Oracle CSM operation.

Version SCZ725 software relies on version SCZ720 documentation for some documentation. This documentation includes:

- The ACLI Reference Guide
- The Troubleshooting and Maintenance Guide
- The Administrative Security Essentials Guide

About this MIB Reference Guide

Documented Objects and Traps

This *MIB Reference Guide* only documents the traps and objects supported in the release version S-CZ7.2.5 for virtual machine, COTS, Acme Packet 6100, and Acme

Packet 6300 platforms. Enterprise MIBs, however, can contain additional traps and objects not documented here.

Enterprise MIB files are global across Oracle CSM and USM products. Each MIB contains a superset of objects and traps for all device:

- platforms
- current releases
- prior releases

In addition, a MIB might contain objects and traps intended for future releases. For example, the ap-smgmt.mib might contain traps intended for support in release Release S-CZ7.2.5.

Objects and traps are not supported in this release version and not documented in this guide if they are intended for a:

- platform other than an Acme Packet platform
- future release

You can verify what is supported in this release version by:

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

Platform sysObjectIDs

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

The table below provides sysObjectID values for all Oracle platforms and their corresponding sysDescr values. X stands for a string value of the software version, such as SCX6.1.0.

Platform	sysObjectID Object Identifier Name: Number	sysDescr
Acme Packet 4500	apNetNet4500: 1.3.6.1.4.1.9148.1.1.2	Acme Packet 4500 X
Acme Packet 3800 (Sku 3810)	apNetNet3800: 1.3.6.1.4.1.9148.1.3.1	Acme Packet 3800 X
Acme Packet 3820	apNetNet3820: 1.3.6.1.4.1.9148.1.3.2	Acme Packet 3820 X
Acme Packet 6000 series	apNetNet6000Series: 1.3.6.1.4.1.9148.1.5	Acme Packet 6000 Series
Acme Packet 6300:	apNetNet6300 1.3.6.1.4.1.9148.1.5.1	Acme Packet 6300 product

Revision History

This section contains a revision history for this document.

Date	Description
November 2014	• Initial Release

Contents

1 Acme Packet (Oracle) MIBs

Overview

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 system log levels, syslog level severities (the protocol used for the network logging of system and network events), and trap receiver filter levels.

MIBs for the Oracle USM retain legacy naming, which often includes “Acme Packet” or “ap” based on their origin.

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
```

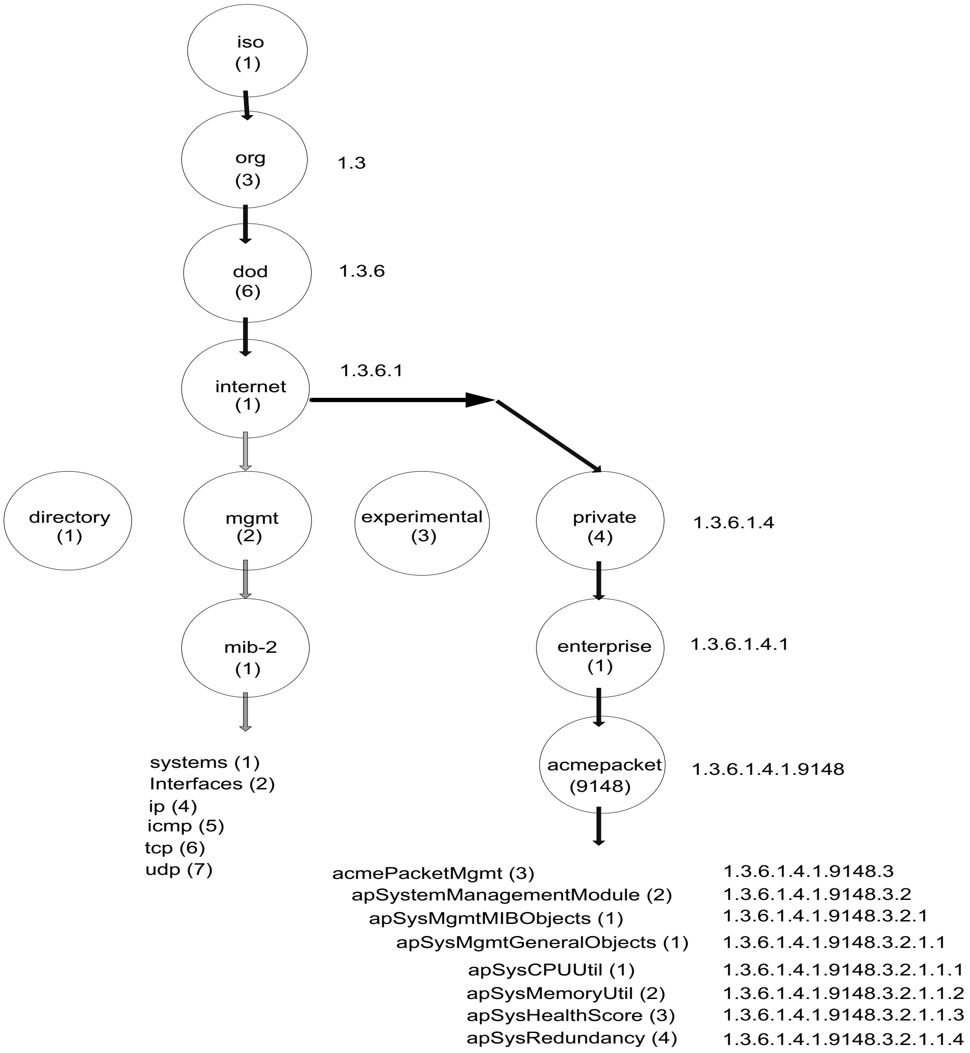
- `tcpConnState` is the OID
- `127.0.0.1` is an IPv4 address
- `1024` is the port number
- `127.0.0.1` is another IPv4 address

- `3000` is another port number

MIB Tree Structure

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

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



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

About 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.

About 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.

SNMPv3 Secure Traps

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

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

Authentication and Privacy

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

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

Four parameters generate keys under the designated algorithm:

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

Password-to-Key Conversion

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

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

Enabling SNMPv3

The table below gives a brief overview of the SNMPv3 configuration on your Oracle USM. The Caveats column describes the SNMPv1V2 configuration attributes that are ignored if **SECURE-TRAP** mode is enabled.

Configuration	Description	Caveat
snmp-agent-mode	Set this attribute to **SECURE-TRAP** to enable SNMPv3.	Once SNMPv3 is enabled, the **snmp-community** and **community-name** attributes are ignored.
snmp-engine-id-suffix	Set this attribute as a string to customize and uniquely identify the SNMP Engine.	The **show snmp-info** command has been expanded to include the SNMP Engine Base, the SNMP Engine Suffix, and the SNMP Engine ID.
snmp-user-entry	Enter the user name, authorization password and privacy password.	The user, as defined in this object, must be added to the attribute **user-list** under **trap-receiver** in order to receive secured traps.

Configuration	Description	Caveat
trap-receiver	Configure a **trap-receiver** with the IP address of the NMS that receives secured traps.	
user-list	Add users who are authorized to receive secured traps.	If instances of **snmp-user-entry** are configured, but no users are listed under **user-list**, a warning message is sent during a **verify-config** execution.

Retaining Existing SNMPv1v2 Behavior

If you are upgrading to software version S-CX6.3.0 or above and want to retain your existing SNMP configurations, you do not need to take any action. The Oracle USM sets **snmp-agent-mode** to **V1V2** by default, disabling all SNMPv3 configurations.

Downgrading Software After Enabling SNMPv3

If you enable SNMPv3 on an Oracle USM running S-CX6.3.0 or above, and you downgrade to a previous software version, the software does not recognize the SNMPv3 configuration objects or attributes.

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 USM.

ACLI Instructions and Examples

This section shows you how to enable SNMPv3 on your system, how to add users, and how to add users to authorized trap receivers.

Enabling SNMPv3

To enable SNMPv3 on the Oracle USM for sending secured traps:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter>.

```
ACMEPACKET(configure)# system
```

3. Type **system-config** and press <Enter>.

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

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

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

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

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

Users and Password Configuration

To configure users for SNMPv3:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter>.

```
ACMEPACKET(configure)# system
```

3. Type **snmp-user-entry** and press <Enter>.

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

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

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

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

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

The system will prompt you to enter the password again.

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

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

The system will prompt you to enter the password again.

Adding Authorized Trap Receivers

To add users as authorized trap-receivers:

1. In Superuser mode, type **configure terminal** and press <Enter>.

```
ACMEPACKET# configure terminal
```

2. Type **system** and press <Enter>.

```
ACMEPACKET(configure)# system
```

3. Type **trap-receiver** and press <Enter>.

```
ACMEPACKET(system)# trap-receiver
ACMEPACKET(trap-receiver)#
```

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

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

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

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

MIBs Supported by Oracle

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

Standard MIBS

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

Acme Packet 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

Acme Packet (Oracle) 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 Acme Packet MIBs listed in this table. Refer to the individual MIBs for details.
ap-ami.mib	Acme Packet management interface on the system.
ap-codec.mib	Codec and transcoding information generated by the system.

MIB Name	Description
ap-ems.mib	EMS traps.
ap-entity-vendortype.mib	Acme Packet (Oracle) OID assignments for Acme Packet hardware components.
ap-env-monitor.mib	Fan speed, voltage, temperature, and power supply for the system. It also sends out traps when status changes occur.
ap-license.mib	Status of your icenses.
ap-products.mib	Descriptions of the different Oracle USM versions.
ap-security.mib	Information about the Management Interface running on the Oracle USM.
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 ystem.
ap-tc.mib	Textual conventions used in Acme Packet enterprise MIBs.

About Traps

This section defines the standard and proprietary traps supported by the Oracle USM. A trap is initiated by tasks to report that an event has happened on the Oracle USM 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 traps and Oracle's own 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 T*he Interfaces Group MIB using SMIv2*
- Appropriate enterprise MIB (for example the Acme Packet syslog MIB or the Acme Packet System Management MIB).

Standard Traps

The following table identifies the standard traps that the Oracle USM supports.

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

Enterprise Traps

The following table identifies the proprietary traps that Oracle USM supports.

Trap Name	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 Acme Packet 4500 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.
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).
apSecurityTunnelFailureNotification: 1.3.6.1.4.1.9148.3.9.3.1.0.1	Generated when an IPSec IKEV2 tunnel cannot be established.
apSecurityTunnelDPDNotification: 1.3.6.1.4.1.9148.3.9.3.2.0.1	Generated when an IPSec IKEV2 tunnel fails because of Dead Peer Detection (DPD).
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.
apSysMgmtAlgdCPULoadTrap: 1.3.6.1.4.1.9148.3.2.6.0.24	Generated if the CPU utilization percentage of application tasks has exceeded the threshold algd-load-limit.
apSysMgmtAlgdCPULoadClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.25	Generated when the CPU utilization percentage of application tasks has fallen below the threshold algd-load-limit.
apSysMgmtRejectedMesagesThresholdExeededTrap 1.3.6.1.4.1.9148.3.2.6.0.57	Generates when the number of rejected messages exceeds the configured threshold within the configured window. This trap is used for both whitelists and HMR rejected messages. The trap does not indicate which feature enabled this trap. To indicate which messages and rules generated the trap, you can consult the matched.log file.
apSysMgmtAdminAuditLogFullTrap: 1.3.6.1.4.1.9148.3.2.6.0.58	Generated when one of the audit logs full threshold is met: • 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.

Trap Name	Description
apSysMgmtAuthenticationFailedTrap: 1.3.6.1.4.1.9148.3.2.6.0.16	Generated when an attempt to login to the Oracle USM through Telnet, SSH, or by using the console fails for any reason; also sent when if a user fails authentication on the console or over FTP, SSH, or SFTP. The trap sent to all configured trap receivers includes the following information: • administration and access level (SSH, user, enable) • connection type (Telnet or console) FTP support is new to Release C5.0.
apSysMgmtCallRecordingStateChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.50	Generated when a call recording server changes state.
apSysMgmtCdrFileDeleteTrap	Generated when a CDR file is deleted because of lack of space on the partition or the drive exceeds the number of files specified.
apSysMgmtCDRPushReceiverFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.53	Generated when an enabled CDR push receiver fails. Returns the address, the address type, and the failure reason code.
apSysMgmtCDRPushReceiverFailureClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.54	Generated when an enabled CDR push receiver resumes normal operation after a failure.
apSysMgmtCDRPushAllReceiversFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.55	Generated when all enabled CDR push receivers fail.
apSysMgmtCDRPushAllReceiversFailureClearTrap 1.3.6.1.4.1.9148.3.2.6.0.56	Generated when one or more enabled CDR push receivers return to normal operation after failures were encountered on all push receivers.
apSysMgmtCfgSaveFailTrap: 1.3.6.1.4.1.9148.3.2.6.0.13	Generated if an error occurs while the system is trying to save the configuration to memory.
apSysMgmtCollectorPushSuccessTrap: 1.3.6.1.4.1.9148.3.2.6.0.44	Generated when the collector successfully completes a push operation.
apSysMgmtENUMStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.27	Generated if the reachability status of an ENUM server changes; contains: • apENUMConfigName • apENUMServerIpAddress • apENUMServerStatus
apSysMgmtExpDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.2	Generated when a device exceeds configured thresholds and is denied access by the Oracle USM.
apSysMgmtFanTrap: 1.3.6.1.4.1.9148.3.2.6.0.3	Generated if a fan unit speed falls below the monitoring level.
apSysMgmtGatewaySynchronizedTrap: 1.3.6.1.4.1.9148.3.2.6.0.49	Generated when the default gateway is synchronized in the ARP table.
apSysMgmtGatewayUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.10	Generated if the gateway specified becomes unreachable by the system.
apSysMgmtGatewayUnreachableClear: 1.3.6.1.4.1.9148.3.2.6.0.21	Generated when the system determines that the gateway in question is once again reachable.
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.

Trap Name	Description
apSysMgmtGroupClearTrap: 1.3.6.1.4.1.9148.3.2.3.0.2	Generated when the Oracle USM's system resource use or its health score returns to levels that are within thresholds. For example, NAT table usage or memory usage could return to acceptable levels, and the systems health score could return to a level above 60.
apSysMgmtHardwareErrorTrap: 1.3.6.1.4.1.9148.3.2.6.0.14	Provides a text string indicating the type of hardware error that has occurred. If the message text exceeds 255 bytes, the message is truncated to 255 bytes.
apSysMgmtInetAddrWithReasonDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.4	Generated when an IP address is placed on a deny list because of denial-of-service attempts. It provides the IP address that has been demoted, the realm ID of that IP address (if available), the URI portion of the SIP From header for the message that caused the demotion, and the reason for the demotion.
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)
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)

Trap Name	Description
apSysMgmtNTPServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.31	Generated when an NTP server deemed unreachable subsequently becomes reachable.
apSysMgmtNTPServiceDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.32	Generated if all configured NTP servers are unreachable.
apSysMgmtNTPServiceDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.33	Generated if NTP service again becomes available.
apSysMgmtPhyUtilThresholdTrap	Generated when the media port's utilization crosses a configured threshold. Indicates whether the OverloadProtection feature is active.
apSysMgmtPhyUtilThresholdClearTrap	Generated when a media port's utilization falls below the lowest configured threshold.
apSysMgmtPowerTrap: 1.3.6.1.4.1.9148.3.2.6.0.1	Generated if a power supply is powered down, powered up, inserted/present or removed/not present.
apSysMgmtPushServerUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.28	Generated if the system collector cannot reach a specified server; used with the historical data recording (HDR) feature.
apSysMgmtPushServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.29	Generated if the system collector can again reach a specified server that was unreachable; used with the historical data recording (HDR) feature.
apSysMgmtRadiusDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.11	Generated if all or some configured RADIUS accounting servers have timed out from a RADIUS server.
apSysMgmtRadiusDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.22	Generated when some or all of the previously unreachable RADIUS servers can be again be reached.
apSysMgmtRealmIcmpFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.51	Generated when ICMP heartbeat failure occurs.
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.

Trap Name	Description
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 Oracle USM 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.
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 file fails.
apSysMgmtAdminWriteFailClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.63	Generated when a write to file succeeds.
apSwCfgActivateNotification: 1.3.6.1.4.1.9148.3.4.3.0.1	Generated when an activate-config command is issued and the configuration has been changed at running time.
apSecurityOCSRDownNotification: 1.3.6.1.4.1.9148.3.9.3.3.0.1	Generated when an OSCR server becomes unreachable.
apSecurityOCSRUpNotification: 1.3.6.1.4.1.9148.3.9.3.3.0.2	Generated when an OSCR server becomes available.
apSysMgmtOCSRDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.80	Generated if all or some of the configured OSCR accounting servers are down.
apSysMgmtOCSRDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.81	Generated if all OSCR accounting servers have resumed communications.
apSecurityCRLInvalidNotification: 1.3.6.1.4.1.9148.3.9.3.4.0.1	Generated when an invalid CRL is detected.
apDiameterAcctSrvrUpTrap: .1.3.6.1.4.1.9148.3.13.1.2.2.0.1	Generated when a Diameter Accounting Server goes up.

Trap Name	Description
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).
apSipSecInterfaceRegThresholdExceededTrap: 1.3.6.1.4.1.9148.3.15.2.1.2.0.1	Generated if the total number of registrations on all secondary SIP interfaces exceeds the configured threshold.
apSipSecInterfaceRegThresholdClearTrap: 1.3.6.1.4.1.9148.3.15.2.1.2.0.2	Generated if the total number of registrations on all secondary SIP interfaces falls below the configured threshold.

Refer to Appendix A for examples of enterprise traps.

EMS Traps

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

- failure to discover or rediscover an Oracle USM configuration
- failure to save an Oracle USM configuration
- failure to activate an Oracle USM configuration
- missing components when validating an Oracle USM configuration
- node status change from reachable to unreachable

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

EMS generates the following traps:

Trap Name	Description
apEMSDiscoveryFailure	Generated when the EMS fails to discover or rediscover a Oracle USM 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 Oracle USM's node ID, the start and end time of the discovery or rediscovery operation, and the user who initiated the operation.
apEMSSaveFailure	Generated when the 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 Oracle USM node ID, the start and stop time of the save configuration attempt, and the user initiating the save operation.

Trap Name	Description
apEMSActivateFailure	Generated when the EMS fails to activate a configuration, whether initiated from the SOAP XML API or EMS GUI for the save/activate or activate operations.
apEMSInvalidConfigDiscoveredNotification	Generated when the EMS validates a discovered Oracle USMs configuration (for example confirms each referenced realm is configured) and detects missing components. The trap contains the time and the Oracle USM node ID.
apEMSNodeUnreachableNotification	Generated when a node’s status changes from reachable to unreachable. The trap contains the Oracle USM’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 Oracle USM’s node ID and the time of the event.

System Alarms

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

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

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

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

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
Hardware Alarms					
FAN STOPPED	65537	CRITICAL: any fan speed is <50%. Or speed of two or more fans is >50% and ≤75%. MAJOR: 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: speed of one fan> 75% and ≤90%, the other two fans are at normal speed.	Fan speed failure. NOTE: If this alarm occurs, the system turns up the fan speed to the fastest possible speed.	fan speed: XXXX, XXXX, XXXX (where xxxx xxxx xxxx is the revolutions per minute (RPM) of each fan on the fan module)	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtFanTrap (ap-smgmt.mib)
TEMPERATURE HIGH	65538	SD1: CRITICAL: ≥70°C MAJOR: ≥60°C MINOR: ≥50°C SD2: CRITICAL: ≥75°C MAJOR: ≥65°C MINOR: ≥55°C SD3: CRITICAL: ≥105°C MAJOR: ≥95°C MINOR: ≥85°C	Fans are obstructed or stopped. The room is abnormally hot.	Temperature: XX.XX C (where XX.XX is the temperature in degrees)	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtTempTrap (ap-smgmt.mib)
ENVIRONMENTAL SENSOR FAILURE	65539	CRITICAL	The environmental sensor component cannot detect fan speed and temperature.	Hardware monitor failure! Unable to monitor fan speed and temperature!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonI2CFailNotification (ap-env-monitor.mib)
PLD POWER A FAILURE	65540	MINOR	Power supply A has failed.	Back Power Supply A has failed!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
PLD stands for Programmable Logical Device					

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
PLD POWER A UP	65541	MINOR	Power supply A is now present and functioning.	Back Power Supply A is present!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
NOTE: If the system boots up with one power supply, the health score is 100, and an alarm is not generated. If another power supply is then added to that same system, this alarm is generated, but the health score is not decremented.					
PLD POWER B FAILURE	65542	MINOR	Power supply B has failed.	Back Power Supply B has failed!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
PLD POWER B UP	65543	MINOR	Power supply B is now present and functioning.	Back Power Supply B is present!	apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib) apSysMgmtPowerTrap (ap-smgmt.mib)
NOTE: If the system boots up with one power supply, the health score is 100, and an alarm is not generated. If another power supply is then added to that same system, this alarm is generated, but the health score is not decremented.					
PLD VOLTAGE ALARM 2P5V	65544	**Host Processor 7455** CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v **Host Processor 7457** *Version 1.0* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.35v or 1.45v to 1.6v *Version 1.1 and later* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
PLD VOLTAGE ALARM 3P3V	65545	**Host Processor 7455** CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v **Host Processor 7457** *Version 1.0* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.35v or 1.45v to 1.6v *Version 1.1 and later* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
PLD VOLTAGE ALARM 5V	65546	**Host Processor 7455** CRITICAL: <1.4v or >1.8v MINOR: 1.4v to 1.55v or 1.65v to 1.8v **Host Processor 7457** *Version 1.0* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.35v or 1.45v to 1.6v *Version 1.1 and later* CRITICAL: <1.0v or >1.6v MINOR: 1.00v to 1.25v or 1.35v to 1.6v			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
PLD VOLTAGE ALARM CPU	65547	**Host Processor 7455** **Host Processor 7457**			apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
PHY0 Removed	65550	MAJOR	Physical interface card 0 was removed.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
PHY0 Inserted	65552	MAJOR	Physical interface card 0 was inserted.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
PHY1 Removed	65553	MAJOR	Physical interface card 1 was removed.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
PHY1 Inserted	65554	MAJOR	Physical interface card 1 was inserted.		apSyslogMessageGenerated (ap-slog.mib) apEnvMonStatusChangeNotification (ap-env-monitor.mib)
System Alarms					
LINK UP ALARM GIGPORT	131073	MINOR	Gigabit Ethernet interface 1 goes up.	Slot 0 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM GIGPORT	131074	MINOR	Gigabit Ethernet interface 2 goes up.	Slot 1 port 0 UP	linkUp(IETF RFC 2233)
LINK DOWN ALARM GIGPORT	131075	MAJOR	Gigabit Ethernet interface 1 goes down.	Slot 0 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM GIGPORT	131076	MAJOR	Gigabit Ethernet interface 2 goes down.	Slot 1 port 0 DOWN	linkDown (IETF RFC 2233)
LINK UP ALARM VXINTF	131077	MINOR	Control interface 0 goes up.	wancom0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM VXINTF	131078	MINOR	Control interface 1 goes up.	wancom1 UP	linkUp (IETF RFC 2233)
LINK UP ALARM VXINTF	131079	MINOR	Control interface 2 goes up.	wancom2 UP	linkUp (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131080	MAJOR	Control interface 0 goes down.	wancom0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131081	MAJOR	Control interface 1 goes down.	wancom1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM VXINTF	131082	MAJOR	Control interface 2 goes down.	wancom2 DOWN	linkDown (IETF RFC 2233)
LINK UP ALARM FEPORT	131083	MAJOR	Fast Ethernet slot 0, port 0 goes up.	Slot 0 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131084	MAJOR	Fast Ethernet slot 1, port 0 goes up.	Slot 1 port 0 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131085	MINOR	Fast Ethernet slot 0, port 1 goes up.	Slot 0 port 1 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131086	MINOR	Fast Ethernet slot 1, port 1 up.	Slot 1 port 1 DOWN	linkUp (IETF RFC 2233)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
LINK UP ALARM FEPORT	131087	MINOR	Fast Ethernet slot 0, port 2 goes up.	Slot 0 port 2 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131088	MINOR	Fast Ethernet slot 1, port 2 goes up.	Slot 1 port 2 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131089	MINOR	Fast Ethernet slot 0, port 3 goes up.	Slot 0 port 3 UP	linkUp (IETF RFC 2233)
LINK UP ALARM FEPORT	131090	MINOR	Fast Ethernet slot 1, port 3 goes up.	Slot 1 port 3 UP	linkUp (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131091	MAJOR	Fast Ethernet slot 0, port 0 goes down.	Slot 0 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131092	MAJOR	Fast Ethernet slot 1, port 0 goes down.	Slot 1 port 0 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131093	MAJOR	Fast Ethernet slot 0, port 1 goes down.	Slot 0 port 1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131094	MAJOR	Fast Ethernet slot 1, port 1 goes down.	Slot 1 port 1 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131095	MAJOR	Fast Ethernet slot 0, port 2 goes down.	Slot 0 port 2 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131096	MAJOR	Fast Ethernet slot 1, port 2 goes down.	Slot 1 port 2 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131097	MAJOR	Fast Ethernet slot 0, port 3 goes down.	Slot 0 port 3 DOWN	linkDown (IETF RFC 2233)
LINK DOWN ALARM FEPORT	131098	MAJOR	Fast Ethernet slot 1, port 3 goes down.	Slot 1 port 3 DOWN	linkDown (IETF RFC 2233)
CPU UTILIZATION	131099	MINOR	CPU usage reached 90% or greater of its capacity.	CPU usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
MEMORY UTILIZATION	131100	CRITICAL	Memory usage reached 90% or greater of its capacity.	Memory usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)
HEALTH SCORE	131101	MAJOR	The system's health score fell below 60.	Health score X is under threshold (where X is the health score)	apSysMgmtGroupTrap (ap-smgmt.mib)
NAT TABLE UTILIZATION	131102	MINOR	NAT table usage reached 90% or greater of its capacity.	NAT table usage X% over threshold X%	apSysMgmtGroupTrap (ap-smgmt.mib)

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

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
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 or activate-config failed, process busy or activate-config failed, must do save-config before activating. or activate-config failed, could not get current config version from file or activate-config failed, could not set running config version to file.	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRedundancyTrap (ap-smgmt.mib)
The activate-config failed log message appears for those cases in which the execution of the activate config command failed on the standby Oracle USM.					
SYSTEM TASK SUSPENDED	131108	CRITICAL	A system task (process) suspends or fails.	Task X suspended, which decremented health by 75! (where X is the task/process name)	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtTaskSuspendTrap (ap-smgmt.mib)
Media Alarms					
MBCD ALARM OUT OF MEMORY	262145	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)	No further memory can be allocated for MBCD.	Flow: Cannot create free port list for realm. Media Server: Failed to allocate new context.	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaOutofMemory (ap-smgmt.mib)
MBCD ALARM UNKNOWN REALM	262147	MAJOR: if media server is adding a new flow	Media server is unable to find realm interface.	Realm type (ingress, egress, hairpin) X, not found	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtUnknownRealm (ap-smgmt.mib)
MBCD ALARM OUT OF BANDWIDTH	262149	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of bandwidth.	Out of bandwidth	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaBandwidthTrap (ap-smgmt.mib)
MBCD ALARM OUT OF PORTS	262150	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%	The realm is out of steering ports.	Out of steering ports	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtMediaPortsTrap (ap-smgmt.mib)
Network Alarms					

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
GATEWAY UNREACHABLE	dynamic ID	MAJOR	The device lost ARP connectivity to a front interface gateway.	gateway X.X.X.X unreachable on slot Y port Z subport ZZ (where X.X.X.X is the IPv4 address of the front interface gateway, Y is the front interface slot number, Z is the front interface port number, and ZZ is the subport ID)	apSysMgmtGatewayUnreachableTrap (ap_smgmt.mib)
NOTE: The value of this alarm ID is dynamic. That is, it changes based on a numbers of factors, but the total alarm ID range falls between 196608 and 262143. The alarm ID is calculated based on the compilation of the following information: a hexidecimal number that represents the VLAN ID and the front interface port/slot numbers.					

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Trap Generated (Trap Reference)
Application Alarms					
RADIUS ACCOUNTING CONNECTION DOWN	327681	CRITICAL: if all enabled and configured Remote Authentication Dial-in User Service (RADIUS) accounting server connections have timed-out without response from the RADIUS server MAJOR: if some, but not all configured RADIUS accounting server connections have timed-out without response from the RADIUS server.	The enabled connections to RADIUS servers have timed-out without a response from the RADIUS server.	CRITICAL: All enabled accounting connections have been lost! Check accounting status for more details. MAJOR: One or more enabled accounting connections have been lost! Check accounting status for more details.	apSyslogMessageGenerated (ap-slog.mib) apSysMgmtRadiusDownTrap (ap-smgmt.mib)
ENUM SERVER STATUS New to Release C5.0	XX	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!	apSysMgmtENUMStatusChangeTrap (ap-smgmt.mib)

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

For additional information about system alarms for the components of the system, refer to *Oracle CSM Configuration Guide.*

Alarm Severities

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

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

Alarm Clearing

When alarms conditions occur on the Oracle USM, corresponding SNMP traps are sent to alert SNMP monitoring utilities. Traps are sent to the SNMP monitoring device when the conditions causing the alarms have been cleared or have subsided. You can now use a monitoring tool to track the current alarm state on the Oracle USM using SNMP traps sent when conditions change.

The following traps are triggered when alarms conditions on the Oracle USM are cleared:

- apSysMgmtGroupClearTrap—Generated when the Oracle USM'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.
- apSysMgmtPortsClearTrap—Generated when the rate of allocating media ports decreases to a level within thresholds.
- apSysMgmtMediaBandwidthClearTrap—Generated when the percentage rate of failure for media bandwidth allocation decreases to the default allowable threshold.
- apSysMgmtMediaOutOfMemoryClear—Generated when the alarm for insufficient memory for media processes is cleared manually.
- apSysMgmtGatewayUnreachableClear—Generated when the system determines that the gateway in question is once again reachable.
- apSysMgmtRadiusDownClearTrap—Generated when some or all of the previously unreachable RADIUS servers can be again be reached.

Acme Packet Log Levels and syslog Level Severities

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

Acme Packet Log Levels

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

Numerical Code	Acme Packet 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 7 8 9	NOTICE INFO TRACE DEBUG	All used for customer support purposes.

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.

Acme Packet syslog Level (Numerical Code)	BSD syslog Severity Level (Number)
EMERGENCY (1)	Emergency - system is unusable (0)
CRITICAL (2)	Alert - action must be taken immediately (1)
MAJOR (3)	Critical - critical conditions (2)
MINOR (4)	Error - error conditions (3)
WARNING (5)	Warning - warning conditions (4)
NOTICE (6)	Notice - normal, but significant condition (5)
INFO (7)	Informational - informational messages (6)
TRACE (8) DEBUG (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	Acme Packet syslog Level (Numerical Code)	Alarm Severity Levels
CRITICAL	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to CRITICAL (with a lesser log level numerical code). The corresponding NMS receives only error events.	• EMERGENCY (1) • CRITICAL (2)	• EMERGENCY • CRITICAL
MAJOR	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to MAJOR (with a lesser log level numerical code). The corresponding NMS receives warning and error events.	• EMERGENCY (1) • CRITICAL (2) • MAJOR (3)	• EMERGENCY • CRITICAL • MAJOR
MINOR	The SNMP agent sends a trap for all alarms and syslogs with a severity level that is greater than or equal to MINOR (i.e., with a lesser log level numerical code) a generate a trap. The corresponding NMS receives informational, warning, and error events.	• EMERGENCY (1) • CRITICAL (2) • MAJOR (3) • MINOR (4)	• EMERGENCY • CRITICAL • MAJOR • MINOR
ALL	The SNMP agent sends a trap for all alarms, syslogs, and other traps. The corresponding NMS receives informational, warning, and error events.	• EMERGENCY (1) • CRITICAL (2) • MAJOR (3) • MINOR (4) • WARNING (5) • NOTICE (6) • INFO (7) • TRACE (8) • DEBUG (9)	• EMERGENCY • CRITICAL • MAJOR • MINOR • WARNING

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

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

For more information about the `filter-level` field specifically or the `trap-receiver` element in general, refer to the *Oracle CSM Configuration Guide*.

2 Standard SNMP GET Requests

Introduction

This section explains the standard SNMP GET requests supported by the system. 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 Group

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

SNMP GET Query Name	Object Identifier Name: Number	Description
interfaces (1.3.6.1.2.1.2)		
ifNumber	interfaces: 1.3.6.1.2.1.2.1	Number of network interfaces (regardless of their current state) present on this system.
The Interfaces Table		
ifTable.ifEntry (1.3.6.1.2.1.2.2.1)		
ifIndex	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.1	Unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization. See for examples of ifIndex values.
ifDescr	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.2	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.3	Information about the type of interface, distinguished according to the physical/link protocol(s) immediately *below* the network layer in the protocol stack.
ifMtu	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.4	Size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface.
ifSpeed	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.5	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
ifPhysAddress	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.6	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.7	Current administrative state of the interface. The testing(3) state indicates that operational packets cannot be passed.
ifOperStatus	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.8	Current operational state of the interface. The testing(3) state indicates that operational packets cannot be passed.
ifLastChange	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.9	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.10	Total number of octets received on the interface, including framing characters.
ifInUcastPkts	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.11	Number of subnetwork-unicast packets delivered to a higher-layer protocol.
ifInNUcastPkts	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.12	Number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
ifInDiscards	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.13	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.14	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.15	Number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
ifOutOctets	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.16	Total number of octets transmitted out of the interface, including framing characters.
ifOutUcastPkts	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.17	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
ifOutNUcastPkts	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.18	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.19	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	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.20	Number of outbound packets that could not be transmitted because of errors.

SNMP GET Query Name	Object Identifier Name: Number	Description
ifOutQLen	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.21	Length of the output packet queue (in packets).
ifSpecific	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.22	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 Scalar Example

The following example shows the scalar variable associated with the interface MIB. The value given in the example will differ from your value.

Instance ID	Value
IfNumber.0	4

Interface Table Examples

The following table contains examples of Interface table values. The values are for the purpose of the example and differ from yours.

OID	Table Index			
	1	2	3	4
ifIndex	1	2	3	4
ifDescr	wancom0	lo0	wancom1	F00
ifType	ethernet-csmacd	sortwareLoopback	ethernet-csmacd	gigabitEthernet
ifMtu	1500	32768	1500	1500
ifSpeed	100000000	100000000	100000000	1000000000
ifPhysAddress	0x00 0x08 0x25 0x01 0x48 0x40		0x00 0x08 0x25 0x01 0x48 0x41	0x00 0x08 0x25 0x01 0x48 0x44
ifAdminStatus	up	up	down	up
ifOperStatus	up	up	down	up
ifLastChange	4318	4318	4318	4099
ifInOctets	0	0	0	0
ifInUcastPkts	461	431	0	0
ifInNUcastPkts	37975	0	0	43
ifInDiscards	0	0	0	0
ifInErrors	0	0	0	0

OID	Table Index			
ifOutOctets	0	0	0	2752
ifOutUcastPkts	810	431	0	0
ifOutNUcastPkts	0	0	0	43
ifOutDiscards	0	0	0	0
ifOutErrors	0	0	0	0
ifSpecific	.0.0	.0.0	.0.0	.0.0

ifName Support (RFC 2863)

Acme Packet supports the ifName entry of the ifXTable, which is an extension to the interface table and which replaces ifExtnsTable. See RFC 2863 for details.

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.

Examples of ifIndex Values

The following table lists examples of ifIndex values.

ifIndex Value	Interface	Slot and Port
Rear interfaces		
1	VXINTF 0	wancom 0
2	loopback interface (lo0)	
3	VXINTF 1	wancom 1
4	VXINTF 2	wancom 2
Single-port GigE physical layer cards		
5	GIGPORT 0	slot 1, port 0
6	GIGPORT 1	slot 1, port 1
Dual-port GigE physical layer cards		
5	GIGPORT 0	slot 1, port 0
6	GIGPORT 1	slot 2, port 0
7	GIGPORT 2	slot 1, port 1
8	GIGPORT 3	slot 2, port 1
Fast Ethernet 10/100 physical layer cards		
5	FEPORT 0	slot 1, port 0

ifIndex Value	Interface	Slot and Port
6	FEPORT 1	slot 2, port 0
7	FEPORT 2	slot 1, port 1
8	FEPORT 3	slot 2, port 1
9	FEPORT 4	slot 1, port 2
10	FEPORT 5	slot 2, port 2
11	FEPORT 6	slot 1, port 3
12	FEPORT 7	slot 2, port 3
Virtual Interfaces		
13 (and continuing)	sp0 (and continuing)	slow path Values will increment starting at ifIndex 13 for each virtual interface that you have configured on your Oracle USM.

High Capacity MIB Counters (ifXtable Support)

New to Release C5.0.

To support 64-bit counters for interface statistics, the Oracle USM now supports the ifXTable MIB (OID 1.3.6.1.2.1.31.1.1) from the IFMIB (1.2.3.1.2.1.31). Only Gets are supported for this MIB object, and only media interfaces will be returned in an SNMP query. All other interfaces do not support 64-bit counters.

SNMP GET Query Name	Object Identifier Name: Number	Description
interfaces (1.3.6.1.2.1.2)		
ifNumber	interfaces: 1.3.6.1.2.1.2.1	Number of network interfaces (regardless of their current state) present on this system.
ifMIB (1.3.6.1.2.1.31)		
ifXTable.ifXEntry (1.3.6.1.2.1.31.1.1.1)		
ifName	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.1	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. Note that for an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface 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.

SNMP GET Query Name	Object Identifier Name: Number	Description
ifInMulticastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.2	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.3	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifOutMulticastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.4	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.5	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 ifCounterDiscontinuityTime.
ifHCInOctets	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.6	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.7	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.
ifHCMulticastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.8	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
ifHCInBroadcastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.9	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.10	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 ifCounterDiscontinuityTime.
ifHCOutUcastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.11	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.
ifHCOutMulticastPkts	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.12	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.13	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.14	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.15	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
ifPromiscuousMode	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.16	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	ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1.17	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise.

IP Group

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.

SNMP GET Query Name	Object Identifier Name: Number	Description
	The IP Group	
	ip (1.3.6.1.2.1.4)	
ipForwarding	ip: 1.3.6.1.2.1.4.1	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	ip: 1.3.6.1.2.1.4.2	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	ip: 1.3.6.1.2.1.4.3	Total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors	ip: 1.3.6.1.2.1.4.4	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
ipInAddrErrors	ip: 1.3.6.1.2.1.4.5	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, 0.0.0.0) 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	ip: 1.3.6.1.2.1.4.6	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	ip: 1.3.6.1.2.1.4.7	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards	ip: 1.3.6.1.2.1.4.8	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	ip: 1.3.6.1.2.1.4.9	Total number of input datagrams successfully delivered to IP user-protocols including ICMP.
ipOutRequests	ip: 1.3.6.1.2.1.4.10	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	ip: 1.3.6.1.2.1.4.11	Number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). (Note that this counter would include datagrams counted in`ipForwDatagrams` if any such packets met this (discretionary) discard criterion.)
ipOutNoRoutes	ip: 1.3.6.1.2.1.4.12	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	ip: 1.3.6.1.2.1.4.13	Maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
ipReasmReqds	ip: 1.3.6.1.2.1.4.14	Number of IP fragments received which needed to be reassembled at this entity.
ipReasmOKs	ip: 1.3.6.1.2.1.4.15	Number of IP datagrams successfully re-assembled.

SNMP GET Query Name	Object Identifier Name: Number	Description
ipReasmFails	ip: 1.3.6.1.2.1.4.16	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	ip: 1.3.6.1.2.1.4.17	Number of IP datagrams that have been successfully fragmented at this entity.
ipFragFails	ip: 1.3.6.1.2.1.4.18	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	ip: 1.3.6.1.2.1.4.19	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
The IP Address Table		
ipAddrTable.ipAddrEntry (1.3.6.1.2.1.4.20.1)		
ipAdEntAddr	ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1.1	IP address to which this entry's addressing information pertains.
ipAdEntIfIndex	ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1.2	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	ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1.3	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 0.
ipAdEntBcastAddr	ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1.4	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	ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1.5	Size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

IP Scalar Example

The following example shows the scalar variables associated with the IP MIB. The values given in the example will differ from your values.

Instance ID	Value
IpForwarding.0	Forwarding
IpDefaultTTL.0	64
IpInReceives.0	15716
IpInHdrErrors.0	0
IpInAddrErrors.0	1024

Instance ID	Value
IpForwDatagrams.0	0
IPInUnknownProtos.0	177
IpInDiscards.0	0
IpInDelivers.0	14521
IpOutRequests.0	30319
IpOutDiscards.0	0
IpOutNoRoutes.0	0
IpReasmTimeout.0	60
IpReasmReqds.0	0
IpReasmOKs.0	0
IpReasmFails.0	0
IpFragOKs.0	0
IpFragFails.0	0
IpFragCreates.0	0

IP Address Table Example

The following table contains examples of IP address table values. The values are for the purpose of the example and differ from yours.

OID	Table Index			
	11.0.0.1	127.0.0.1	172.30.29.31	192.168.0.71
ipAdEntAddr	11.0.0.1	127.0.0.1	172.30.29.31	192.168.0.71
ipAdEntIfIndex	3	2	1	5
ipAdEntNetMask	255.0.0.0	255.0.0.0	255.255.0.0	255.255.255.0
ipAdEntBcastAddr	1	1	1	1
ipAdEntReasmMaxSize	65535	65535	65535	65535

ICMP Group

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.

SNMP GET Query Name	Object Identifier Name: Number	Description
The ICMP Group		
icmp (1.3.6.1.2.1.5)		
icmpInMsgs	icmp: 1.3.6.1.2.1.5.1	Total number of ICMP messages which the entity received. (Note that this counter includes all those counted by `icmpInErrors`.)
icmpInErrors	icmp: 1.3.6.1.2.1.5.2	Number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
icmpInDestUnreachs	icmp: 1.3.6.1.2.1.5.3	Number of ICMP Destination Unreachable messages received.
icmpInTimeExcds	icmp: 1.3.6.1.2.1.5.4	Number of ICMP Time Exceeded messages received.
icmpInParmProbs	icmp: 1.3.6.1.2.1.5.5	Number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs	icmp: 1.3.6.1.2.1.5.6	Number of ICMP Source Quench messages received.
icmpInRedirects	icmp: 1.3.6.1.2.1.5.7	Number of ICMP Redirect messages received.
icmpInEchos	icmp: 1.3.6.1.2.1.5.8	Number of ICMP Echo (request) messages received.
icmpInEchoReps	icmp: 1.3.6.1.2.1.5.9	Number of ICMP Echo Reply messages received.
icmpInTimestamps	icmp: 1.3.6.1.2.1.5.10	Number of ICMP Timestamp (request) messages received.
icmpInTimestampReps	icmp: 1.3.6.1.2.1.5.11	Number of ICMP Timestamp Reply messages received.
icmpInAddrMasks	icmp: 1.3.6.1.2.1.5.12	Number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps	icmp: 1.3.6.1.2.1.5.13	Number of ICMP Address Mask Reply messages received.
icmpOutMsgs	icmp: 1.3.6.1.2.1.5.14	Total number of ICMP messages which this entity attempted to send. (This counter includes all those counted by `icmpOutErrors`.)
icmpOutErrors	icmp: 1.3.6.1.2.1.5.15	Number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
icmpOutDestUnreachs	icmp: 1.3.6.1.2.1.5.16	Number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	icmp: 1.3.6.1.2.1.5.17	Number of ICMP Time Exceeded messages sent.
icmpOutParmProbs	icmp: 1.3.6.1.2.1.5.18	Number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs	icmp: 1.3.6.1.2.1.5.19	Number of ICMP Source Quench messages sent.
icmpOutRedirects	icmp: 1.3.6.1.2.1.5.20	Number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

SNMP GET Query Name	Object Identifier Name: Number	Description
icmpOutEchos	icmp: 1.3.6.1.2.1.5.21	Number of ICMP Echo (request) messages sent.
icmpOutEchoReps	icmp: 1.3.6.1.2.1.5.22	Number of ICMP Echo Reply messages sent.
icmpOutTimestamps	icmp: 1.3.6.1.2.1.5.23	Number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps	icmp: 1.3.6.1.2.1.5.24	Number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks	icmp: 1.3.6.1.2.1.5.25	Number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps	icmp: 1.3.6.1.2.1.5.26	Number of ICMP Address Mask Reply messages sent.

ICMP Scalar Example

The following example shows the scalar variables associated with the ICMP MIB. The values given in the example will differ from your values.

Instance ID	Value
IcmpInMsgs.0	246
IcmpInErrors.0	0
IcmpInDestUnreachs.0	246
IcmpInTimeExcds.0	0
IcmpInParmProbs.0	0
IcmpInSrcQuenchs.0	0
IcmpInRedirects.0	0
IcmpInEchos.0	0
IcmpInEchoReps.0	0
IcmpInTimestamps.0	0
IcmpInTimestampReps.0	0
IcmpInAddrMasks.0	60
IcmpInAddrMaskReps.0	0
IcmpOutMsgs.0	132
IcmpOutErrors.0	132
IcmpOutDestUnreachs.0	132
IcmpOutTimeExcds.0	0
IcmpOutParmProbs.0	0
IcmpOutSrcQuenchs.0	0
IcmpOutRedirects.0	0
IcmpOutEchos.0	0
IcmpOutEchoReps.0	0
IcmpOutTimestamps.0	0

Instance ID	Value
IcmpOutTimestampReps.0	0
IcmpOutAddrMasks.0	0
IcmpOutAddrMaskReps.0	0

TCP Group

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

SNMP GET Query Name	Object Identifier Name: Number	Description
The TCP Group		
tcp (1.3.6.1.2.1.6)		
tcpRtoAlgorithm	tcp: 1.3.6.1.2.1.6.1	Algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin	tcp: 1.3.6.1.2.1.6.2	Minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is `rsre(3)`, an object of this type has the semantics of the LBOUND quantity described in RFC 793.
tcpRtoMax	tcp: 1.3.6.1.2.1.6.3	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	tcp: 1.3.6.1.2.1.6.4	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	tcp: 1.3.6.1.2.1.6.5	Number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens	tcp: 1.3.6.1.2.1.6.6	Number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpAttemptFails	tcp: 1.3.6.1.2.1.6.7	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	tcp: 1.3.6.1.2.1.6.8	Number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

SNMP GET Query Name	Object Identifier Name: Number	Description
tcpCurrEstab	tcp: 1.3.6.1.2.1.6.9	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
tcpInSegs	tcp: 1.3.6.1.2.1.6.10	Total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs	tcp: 1.3.6.1.2.1.6.11	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs	tcp: 1.3.6.1.2.1.6.12	Total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpInErrs	tcp: 1.3.6.1.2.1.6.14	Total number of segments received in error (for example, bad TCP checksums).
tcpOutRsts	tcp: 1.3.6.1.2.1.6.15	Number of TCP segments sent containing the RST flag.
The TCP Connection Table		
tcpConnTable.tcpConnEntry (1.3.6.1.2.1.6.13.1)		
tcpConnState	tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.1	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	tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.2	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	tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.3	Local port number for this TCP connection.
tcpConnRemAddress	tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.4	Remote IP address for this TCP connection.
tcpConnRemPort	tcpConnTable.tcpConnEntry: 1.3.6.1.2.1.6.13.1.5	Remote port number for this TCP connection.

TCP Scalar Example

The following example shows the scalar variables associated with the TCP MIB. The values given in the example will differ from your values.

Instance ID	Value
TcpRtoAlgorithm.0	vanj
TcpRtoMin.0	1000
TcpRtoMax.0	64000
TcpMaxConn.0	-1
TcpActiveOpens.0	9
TcpPassiveOpens.0	9
TcpAttemptFails.0	0
TcpEstabResets.0	0
TcpCurrEstab.0	18
TcpInSegs.0	70
TcpOutSegs.0	70
TcpRetranSegs.0	0
TcpInErrs.0	0
TcpOutRsts.0	0

TCP Connection Table Example

The following table contains examples of the TCP connection table indexed by tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, and tcpConnRemPort. The values used in the example will differ from what you see.

OID	Table Index Values	Table Index					
	tcpConnLocalAddress	0.0.0.0	0.0.0.0	127.0.0.1	127.0.0.1	172.30.29.31	172.30.29.31
	tcpConnLocalPort	0	21	1024	3000	3000	3001
	tcpConnRemAddress	0.0.0.0	0.0.0.0	127.0.0.1	127.0.0.1	0.0.0.0	0.0.0.0
	tcpConnRemPort	0	0	3000	1040	0	0
tcpConnState		closed	listen	established	established	listen	listen
tcpConnLocal Address		0.0.0.0	0.0.0.0	127.0.0.1	127.0.0.1	172.30.29.31	172.30.29.31
tcpConnLocal Port		0	21	1024	3000	3000	3001
tcpConnRem Address		0.0.0.0	0.0.0.0	127.0.0.1	127.0.0.1	0.0.0.0	0.0.0.0
tcpConnRem Port		0	0	3000	1040	0	0

UDP Group

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 endpoints on which a local application is currently accepting datagrams.

SNMP GET Query Name	Object Identifier Name: Number	Description
The UDP Group		
udp (1.3.6.1.2.1.7)		
udpInDatagrams	udp: 1.3.6.1.2.1.7.1	Total number of UDP datagrams delivered to UDP users.
udpNoPorts	udp: 1.3.6.1.2.1.7.2	Total number of received UDP datagrams for which there was no application at the destination port.
udpInErrors	udp: 1.3.6.1.2.1.7.3	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpOutDatagrams	udp: 1.3.6.1.2.1.7.4	Total number of UDP datagrams sent from this entity.
The UDP Listener Table		
udpTable.udpEntry (1.3.6.1.2.1.7.5.1)		
udpLocalAddress	udpTable.udpEntry: 1.3.6.1.2.1.7.5.1.1	Local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.
udpLocalPort	udpTable.udpEntry: 1.3.6.1.2.1.7.5.1.2	Local port number for this UDP listener.

UDP Scalar Example

The following example shows the scalar variables associated with the UDP MIB. The values given in the example will differ from your values.

Instance ID	Value
UdpInDatagrams.0	5007
UdpNoPorts.0	21434
UdpInErrors.0	0
UdpOutDatagrams.0	51525

UDP Table Example

The following table contains examples of the UDP table values. The values used in the example will differ from what you see.

OID	Table Index Values	Table Index					
	UdpLocalAddress	0.0.0.0	11.0.0.1	127.0.0.1	127.0.0.1	172.30.29.31	172.30.29.31
	UdpLocalPort	0	1985	123	5060	123	1030
UdpLocalAddress		0.0.0.0	11.0.0.1	127.0.0.1	127.0.0.1	172.30.29.31	172.30.29.31
UdpLocalPort		0	1985	123	5060	123	1030

System Group

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

SNMP GET Query Name	Object Identifier Name: Number	Description
The System Group		
system (1.3.6.1.2.1.1)		
sysDescr	system: 1.3.6.1.2.1.1.1	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	system: 1.3.6.1.2.1.1.2	Vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed. For example, if vendor Flintstones, Inc. was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its Fred Router.
sysUpTime	system: 1.3.6.1.2.1.1.3	Time (in hundredths of a second) since the network management portion of the system was last re-initialized.
sysContact	system: 1.3.6.1.2.1.1.4	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	system: 1.3.6.1.2.1.1.5	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	system: 1.3.6.1.2.1.1.6	Physical location of this node (for example, telephone closet, 3rd floor). If the location is unknown, the value is the zero-length string.

SNMP GET Query Name	Object Identifier Name: Number	Description
sysServices	system: 1.3.6.1.2.1.1.7	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)). In the context of the Internet suite of protocols, values should be calculated accordingly: **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.
sysORLastChange	system: 1.3.6.1.2.1.1.8	Value of `sysUpTime` at the time of the most recent change in state or value of any instance of `sysORID`.

System Scalar Example

The following example shows the scalar variables associated with the system MIB. The values given in the example will differ from your values.

Instance ID	Value
SysDescr.0	Acme Packet Agent
SysObjectID.0	enterprises.9148
SysUpTime.0	(1518227) 4:13:02.27
SysContact.0	Xyz (configurable)
SysName.0	performance1 (configurable)
SysLocation.0	Burlington, MA (configurable)
SysServices.0	79
SysORLastChange.o	(1518227) 4:13:02.27

Object Resource Information

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.

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Resource Information		
sysORTable.sysOREntry (1.3.6.1.2.1.1.9.1)		
sysORID	sysORTable.sysOREntry: 1.3.6.1.2.1.1.9.1.2	Authoritative identification of a capabilities statement with respect to various MIB modules supported by the local SNMPv2 entity acting in an agent role.
sysORDescr	sysORTable.sysOREntry: 1.3.6.1.2.1.1.9.1.3	Textual description of the capabilities identified by the corresponding instance of `sysORID`.
sysORUpTime	sysORTable.sysOREntry: 1.3.6.1.2.1.1.9.1.4	Value of `sysUpTime` at the time this conceptual row was last instantiated.

SysORTableTable Examples

The following table contains examples of the SysORTable values. Using this table, you can see that the instance index sysORID.1 corresponds to enterprises.0148.2.1.1.

OID	Table Index			
	1	2	3	4
sysORID	enterprises.9148. 2.1.1	enterprises.9148. 2.1.2	enterprises.9148. 2.1.3	enterprises.9148. 2.1.4
sysORDescr	Acme Packet Inc. Agent supports SNMPv2.	Acme Packet Inc. Agent supports MIB-II. No set requests for ifAdminStatus and tcpConnStat.	Acme Packet Inc. Agent supports Acme Syslog MIBs.	Acme Packet Inc. Agent supports Acme system management MIBs.
sysORUpTime	(1518227) 4:13:02.27	(1518227) 4:13:02.27	(1518228) 4:13:02.28	(1518228) 4:13:02.28

SNMP Group

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.

SNMP GET Query Name	Object Identifier Name: Number	Description
The SNMP Group		
snmp (1.3.6.1.2.1.11)		
snmpInPkts	snmp: 1.3.6.1.2.1.11.1	Total number of messages delivered to the SNMP entity from the transport service.
snmpInBadVersions	snmp: 1.3.6.1.2.1.11.3	Total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	snmp: 1.3.6.1.2.1.11.4	Total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
snmpInBadCommunityUses	snmp: 1.3.6.1.2.1.11.5	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	snmp: 1.3.6.1.2.1.11.6	Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
snmpEnableAuthenTraps	snmp: 1.3.6.1.2.1.11.30	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	snmp: 1.3.6.1.2.1.11.31	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	snmp: 1.3.6.1.2.1.11.32	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.

SNMP Scalar Example

The following example shows the scalar variables associated with the SNMP MIB. The values given in the example will differ from the values you will see.

Instance ID	Value
SnmpOutPkts.0	5134
SnmpInBadVersions.0	3
SnmpInBadCommunityNames.0	0
SnmpInBadCommunityUses.0	0
SnmpInASNParseErrs.0	0
SnmpInTooBigs.0	0
SnmpInNoSuchNames.0	0
SnmpInBadValues.0	0
SnmpInReadOnlys.0	0
SnmpInGenErrs.0	0
SnmpInTotalReqVars.0	4853
SnmpInTotalSetVars.0	0
SnmpInGetRequests.0	1
SnmpInGetNexts.0	4860
SnmpInSetRequests.0	0
SnmpInGetResponses.0	0
SnmpInTraps.0	0
SnmpOutTooBigs.0	0
SnmpOutNoSuchNames.0	0
SnmpOutBadValues.0	0
SnmpOutGenErrs.0	0
SnmpOutGetRequests.0	0
SnmpOutGetNexts.0	0
SnmpOutSetRequests.0	0
SnmpOutGetResponses.0	4871
SnmpOutTraps.0	287
SnmpEnableAuthenTraps.0	disabled
SnmpSilentDrops.0	0
SnmpProxyDrops.0	0

Physical Entity Table (rfc2737.mib)

Acme Packet 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.

SNMP GET Query Name	Object Identifier Name: Number	Description
Physical Entity Table		
entityMIB (1.3.6.1.2.1.47)		
entityMIBObjects (1.3.6.1.2.1.47.1)		
entityPhysical (1.3.6.1.2.1.47.1.1)		
entityPhysicalTable (1.3.6.1.2.1.47.1.1.1)		
entityPhysicalEntry (1.3.6.1.2.1.47.1.1.1.1)		
entPhysicalIndex	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.1	The index for this entry.
entPhysicalDescr	entityPhysicalEntry1.3.6.1.2.1.47.1.1.1.1.2	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	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.3	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	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.4	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	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.5	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

SNMP GET Query Name	Object Identifier Name: Number	Description
entPhysicalParentRelPos	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.6	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 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	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.7	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
entPhysicalHardwareRev	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.8	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.
entPhysicalFirmwareRev	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.9	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	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.10	Vendor-specific software revision string for the physical entity. If revision information is stored internally in a non-printable (for example, binary) format, the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software programs are associated with the physical component, or this information is unknown to the agent, this object contains a zero-length string.
entPhysicalSerialNum	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.11	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
entPhysicalMfgName	entityPhysicalEntry:1.3.6.1.2.1.47. 1.1.1.1.12	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	entityPhysicalEntry:1.3.6.1.2.1.47. 1.1.1.1.13	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.
entPhysicalAlias	entityPhysicalEntry:1.3.6.1.2.1.47. 1.1.1.1.14	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.
entPhysicalAssetID	entityPhysicalEntry:1.3.6.1.2.1.47. 1.1.1.1.15	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

SNMP GET Query Name	Object Identifier Name: Number	Description
entPhysicalIsFRU	entityPhysicalEntry:1.3.6.1.2.1.47.1.1.1.1.16	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
entityGeneral (1.3.6.1.2.1.47.1.4)		
entLastChangeTime	entityPhysicalEntry:1.3.6.1.2.1.47.1.4.1	Currently the only object in the entGeneral group, this scalar object represents the value of sysUptime when any part of the Entity MIB configuration last changed.

entPhysicalTable Example

The following table contains examples of the entityPhysicalTable values. The values are for the purpose of the example and are not intended to be a complete list. The table skips from column 3 in the table to column 30.

OID	Table Index				
	1	2	3	......	30
entPhysicalDescr	Assy, Session Director II with QOS	Power Supply tray A	Assy, 150 Watt 110V Power Supply	......	Single voltage sensor with multiple inputs
entPhysicalVendorType	.9148.6.1.1.3.2.4	.9148.6.1.1.4.4	.9148.6.1.1.5.2	......	.9148.6.1.1.7.3
entPhysicalContainedIn	0	1	2	......	1
entPhysicalClass	chassis	container	powerSupply	......	Sensor
entPhysicalParentRelPos	0	1	1	......	12
entPhysicalName	Session Director	Power Tray A		......	Voltage Sensor
entPhysicalHardwareRev	5			......	
entPhysicalFirmwareRev	1.35			......	
entPhysicalSoftwareRev	050448002513			......	
entPhysicalSerialNum	Unknown manufacturer			......	
entPhysicalMfgName	102-1002-00			......	
entPhysicalModelName				......	
entPhysicalAlias				......	
entPhysicalAssetID				......	
entPhysicalIsFRU	2	2	1	......	2

entity Physical Table Scalar Example

The following example shows the scalar variable associated with the entityPhysicalTable. The value given in the example will differ from your value.

Instance ID	Value
EntLastChangeTime.0	0

3 Enterprise SNMP GET Requests

Introduction

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

Acme Packet syslog MIB (ap-slog.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSyslogBasic (1.3.6.1.4.1.9148.3.1.1.1)		
apSyslogNotificationsSent	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.1	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	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.2	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	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.3	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	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.4	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSyslogMsgDrops	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.5	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.
Object identifier Name: apSyslogHistory (1.3.6.1.4.1.9148.3.1.1.2)		
apSyslogHistTableMaxLength	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.1	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	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.2	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.
Object Identifier Name: apSyslogHistoryEntry (1.3.6.1.4.1.9148.3.1.1.2.3)		
apSyslogHistIndex	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.1	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	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.2	Process name and host of the sending client (for example, anyclient@sr.acme.com)
apSyslogHistLevel	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.3	Log level of the message.
apSyslogHistType	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.4	Textual identification for the log type, which categorizes the log message.
apSyslogHistContent	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.5	Text of the syslog message. If the text of the message exceeds 255 bytes, it is truncated to 255 bytes.
apSyslogHistTimestamp	apSyslogHistoryEntry: 1.3.6.1.4.1.9148.3.1.1.2.3.6	Value of sysUpTime when this message was generated.

Syslog Scalar Example

The following example shows the scalar variables associated with the syslog MIB. The values given in the example are samples that will differ from your values.

Instance ID	Value
ApSyslogNotificationsSent.0	955
ApSyslogNotificationsEnabled.0	TRUE
ApSyslogMaxLevel.0	warning
ApSyslogMsgIgnores.0	0
ApSyslogMsgDrops.0	0
ApSyslogHistTableMaxLength.0	1
ApSyslogHistMsgsFlushed.0	954

Syslog History Table Examples

The following example shows the scalar variables associated with the syslog MIB. The values given in the example are samples that will differ from your values.

OID	Table Index
ApSyslogHistIndex	955
ApSyslogHistFrom	performance1
ApSyslogHistLevel	critical
ApSyslogHistType	application
ApSyslogHistContent	All enabled accounting connections have been lost! Check accounting status for more details.
ApSyslogHistTimestamp	1132330978

Acme Packet System Management MIB (ap-smgmt.mib)

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

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSysMgmtMIBObjects (1.3.6.1.4.1.9148.3.2.1)		
Object Identifier Name: apSysMgmtGeneralObjects (1.3.6.1.4.1.9148.3.2.1.1)		
apSysCPUUtil	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.1	Percentage of CPU utilization.
apSysMemoryUtil	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.2	Percentage of memory utilization.
apSysHealthScore	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.3	System health percentage, with a system health percentage value of 100 (100%) being the healthiest.
apSysRedundancy	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.4	For HA pairs, information about whether this Oracle USMis 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	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.5	Total instant number of global concurrent sessions at the moment.
apSysGlobalCPS	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.6	Number of global calls per second. This is an instant value, which is the sum of SIP, H.323, and MGCP calls.
apSysNATCapacity	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.7	Percentage of NAT table in Content Addressable Memory (CAM) utilization.
apSysARPCapacity	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.8	Percentage of ARP table (in CAM) utilization.
apSysState	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.9	Current system state. Online denotes regular call processing and offline implies no call processing occurring but other administrative functions are available.
apSysLicenseCapacity	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.10	Percentage of licensed sessions currently in progress.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSysSipStatsActiveLocalContacts	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.11	Number of currently cached registered contacts in the Oracle USM.
apSysRegCacheLimit	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.14	Maximum number of contacts to be accepted into the registration cache. A value of 0 indicates no limit.
apSysApplicationCPULoadRate	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.16	Average load rate of the service applications taken over a period up to 10 seconds.
apSysRejectedMessages	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.18	Number of messages rejected by the Oracle USM due to matching criteria.
apSysSipEndptDemTrustToUntrust	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.19	Global counter for SIP endpoint demotion from trusted to untrusted.
apSysSipEndptDemUntrustToDeny	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.20	Global counter for SIP endpoint demotion from untrusted to deny.
apSysMgcpEndptDemTrustToUntrust	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.21	Global counter for MGCP endpoint demotion from trusted to untrusted.
apSysMgcpEndptDemUntrustToDeny	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.22	Global counter for MGCP endpoint demotion from untrusted to deny.
apSysSipTotalCallsRejected	1.3.6.1.4.1.9148.3.2.1.1.25	Global counter for SIP calls that are rejected by the USM
apSysSipStatsActiveSubscriptions	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.27	An unsigned 32-bit integer that specifies the current global count of active SIP subscriptions.
apSysSipStatsPerMaxSubscriptions	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.28	An unsigned 32-bit integer that specifies the maximum global count of SIP subscriptions initiated during any 100 second period since the last USM re-boot.
apSysSipStatsPerMaximumActiveSubscriptions	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.29	An unsigned 32-bit integer that specifies the maximum global count of active SIP subscriptions since the last USM re-boot.
apSysSipStatsTotalSubscriptions	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.30	An unsigned 32-bit integer that specifies the global count of active SIP subscriptions since the last USM r e-boot.
Object Identifier Name: apSysStorageSpaceTable (1.3.6.1.4.1.9148.3.2.1.1.23)		
Object Identifier Name: apSysStorageSpaceEntry (1.3.6.1.4.1.9148.3.2.1.1.23.1)		
apSysVolumeIndex	apSysStorageSpaceEntry: 1.3.6.1.4.1.9148.3.2.1.1.23.1.1	Monotonically increasing integer for the purpose of indexing volumes.
apSysVolumeName	apSysStorageSpaceEntry: 1.3.6.1.4.1.9148.3.2.1.1.23.1.2	Name of the volume.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSysVolumeTotalSpace	apSysStorageSpaceEntry: 1.3.6.1.4.1.9148.3.2.1.1.23.1.3	Total size of the volume in MB.
apSysVolumeAvailSpace	apSysStorageSpaceEntry: 1.3.6.1.4.1.9148.3.2.1.1.23.1.4	Total space available on the volume in KB.
Object Identifier Name: apCombinedSessionAgentStatsEntry (1.3.6.1.4.1.9148.3.2.1.2.1,1)		
apCombinedStatsSessionAgentIndex	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.1	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	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.2	The hostname of the session agent for which the following statistics are being calculated.
apCombinedStatsSessionAgentType	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.3	The type of the specified session agent, either SIP or H323.
apCombinedStatsCurrentActiveSessionsInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.4	Number of current active inbound sessions.
apCombinedStatsCurrentSessionRateInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.5	Current inbound session rate in CPS.
apCombinedStatsCurrentActiveSessionsOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.6	Number of current active outbound sessions.
apCombinedStatsCurrentSessionRateOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.7	Current outbound session rate in CPS.
apCombinedStatsTotalSessionsInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.8	Total number of inbound sessions during the 100 second sliding window period.
apCombinedStatsTotalSessionsNotAdmittedInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.9	Total number of non-bandwidth constraints that exceeded rejections on inbound sessions (for example, max-sessions, burst rate, etc.).
apCombinedStatsPeriodHighInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.10	Highest number of concurrent inbound sessions during the period.
apCombinedStatsAverageRateInbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apCombinedStatsTotalSessionsOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.12	Total number of outbound sessions during the 100 second sliding window period.
apCombinedStatsTotalSessionsNotAdmittedOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.13	Total number of non-bandwidth constraints that exceeded rejections on outbound sessions (for example, max-sessions, burst rate, etc.).
apCombinedStatsPeriodHighOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.

SNMP GET Query Name	Object Identifier Name: Number	Description
apCombinedStatsAverageRateOutbound	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apCombinedStatsMaxBurstRate	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apCombinedStatsPeriodSeizures	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.17	Total number of seizures during the 100 second sliding window period.
apCombinedStatsPeriodAnswers	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.18	Total number of answered sessions during the 100 second sliding window period.
apCombinedStatsPeriodASR	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.19	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apCombinedStatsAverageLatency	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.20	Average observed one-way signalling latency during the period.
apCombinedStatsMaxLatency	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.21	Maximum observed one-way signalling latency during the 100 second sliding window period.
apCombinedStatsSessionAgentStatus	apCombinedSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.1.1.22	The current status of the specified session agent, which is expressed as INS, OOSnonresp, OOSconstraintsviolation, BecomingOOS, or ForcedOOS.
Object Identifier Name: apSipSessionAgentStatsEntry (1.3.6.1.4.1.9148.3.2.1.2.2.1)		
apSipSAStatsSessionAgentIndex	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.1	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	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.2	The hostname of the session agent for which the following statistics are being calculated.
apSipSAStatsSessionAgentType	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.3	The type of the specified session agent, either SIP or H323.
apSipSAStatsCurrentActiveSessionsInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.4	Number of current active inbound sessions.
apSipSAStatsCurrentSessionRateInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.15	Current Inbound Session rate in CPS.
apSipSAStatsCurrentActiveSessionsOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.6	Number of current active outbound sessions.
apSipSAStatsCurrentSessionRateOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.7	Current outbound session rate in CPS.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSipSAStatsTotalSessionsInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.8	Total number of inbound sessions during the 100 second sliding window period.
apSipSAStatsTotalSessionsNotAdmittedInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apSipSAStatsPeriodHighInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.10	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apSipSAStatsAverageRateInbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.11	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apSipSAStatsTotalSessionsOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.12	Total number of outbound sessions during the 100 second sliding window period.
apSipSAStatsTotalSessionsNotAdmittedOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.13	Total number of outbound sessions rejected because of insufficient bandwidth.
apSipSAStatsPeriodHighOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.14	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apSipSAStatsAverageRateOutbound	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.15	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apSipSAStatsMaxBurstRate	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.16	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apSipSAStatsPeriodSeizures	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.17	Total number of seizures during the 100 second sliding window period.
apSipSAStatsPeriodAnswers	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.18	Total number of answered sessions during the 100 second sliding window period.
apSipSAStatsPeriodASR	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.19	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
apSipSAStatsAverageLatency	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.20	Average observed one-way signaling latency during the 100 second sliding window period.
apSipSAStatsMaxLatency	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.21	Maximum observed one-way signaling latency during the 100 second sliding window period.
apSipSAStatsSessionAgentStatus	apSIPSessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.2.1.22	The current status of the specified session agent, which is expressed as INS, OOSnonresp, OOSconstraintsviolation, BecomingOOS, or ForcedOOS.

Object Identifier Name: apSigRealmStatsTable (1.3.6.1.4.1.9148.3.2.1.2.4)

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSigRealmStatsEntry (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.		
apSigRealmStatsRealmIndex	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.1	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	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.2	The name of the realm for which the following statistics are being calculated.
apSigRealmStatsCurrentActiveSessionsInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.3	Number of current active inbound sessions.
apSigRealmStatsCurrentSessionRateInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.4	Current inbound session rate in CPS.
apSigRealmStatsCurrentActiveSessionsOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.5	Number of current active outbound sessions.
apSigRealmStatsCurrentSessionRateOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.6	Current outbound session rate in CPS.
apSigRealmStatsTotalSessionsInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.7	Total number of inbound sessions during the 100 second sliding window period.
apSigRealmStatsTotalSessionsNotAdmittedInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.8	Total number of inbound sessions rejected because of insufficient bandwidth.
apSigRealmStatsPeriodHighInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.9	Highest number of concurrent inbound sessions during the 100 second sliding window period.
apSigRealmStatsAverageRateInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.10	Average rate of inbound sessions during the 100 second sliding window period in CPS.
apSigRealmStatsTotalSessionsOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.11	Total number of outbound sessions during the 100 second sliding window period.
apSigRealmStatsTotalSessionsNotAdmittedOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.12	Total number of outbound sessions rejected because of insufficient bandwidth.
apSigRealmStatsPeriodHighOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.13	Highest number of concurrent outbound sessions during the 100 second sliding window period.
apSigRealmStatsAverageRateOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.14	Average rate of outbound sessions during the 100 second sliding window period in CPS.
apSigRealmStatsMaxBurstRate	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.15	Maximum burst rate of traffic measured during the 100 second sliding window period (combined inbound and outbound).
apSigRealmStatsPeriodSeizures	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.16	Total number of seizures during the 100 second sliding window period.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSigRealmStatsPeriodAnswers	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.17	Total number of answered sessions during the 100 second sliding window period.
apSigRealmStatsPeriodASR	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.18	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
apSigRealmStatsAverageLatency (not supported)	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.19	Average observed one-way signaling latency in milliseconds during the period.
apSigRealmStatsMaxLatency (not supported)	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.20	Maximum observed one-way signaling latency in milliseconds during the period.
apSigRealmStatsMinutesLeft	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.21	Number of monthly-minutes left in the pool per calendar year for a given realm.
apSigRealmStatsMinutesReject	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.22	Peg counts of the number of calls rejected because the monthly-minutes constraints are exceeded.
apSigRealmStatsShortSessions	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.23	Lifetime number of sessions whose duration was less than the configured short session durations.
apSigRealmStatsAverageQoSRFactor	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.24	Average QoS factor observed during the period.
apSigRealmStatsMaximumQoSFactor	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.25	Maximum QoS factor observed during the period.
apSigRealmStatsCurrentMajorRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.26	Peg counts of the number of times the major Rfactor threshold was exceeded during the period.
apSigRealmStatsTotalMajorRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.27	Peg counts of the number of times the major Rfactor threshold was exceeded during the lifetime.
apSigRealmStatsCurrentCriticalRFactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.28	Peg counts of the number of times the critical Rfactor threshold was exceeded during the period.
apSigRealmStatsTotalCriticalRfactorExceeded	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.29	Peg counts of the number of times the critical Rfactor threshold was exceeded during the lifetime.
apSigRealmStatsRealmStatus	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.30	Current status of the specified realm, which is expressed as INS, constraintviolation, or callLoadReduction.
apSigRealmStatsActiveLocalContacts	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.31	An unsigned 32-bit integer that specifies the current domain count of active SIP registrations.

Object Identifier Name: apSysMgmtNetMgmtCtrlObjects (1.3.6.1.4.1.9148.3.2.1.3)

Object Identifier Name: apNetMgmtCtrlStatsTable (1.3.6.1.4.1.9148.3.2.1.3.1)

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apNetMgmtCtrlStatsEntry (1.3.6.1.4.1.9148.3.2.1.3.1.1)		
apNetMgmtCtrlStatsName	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.1	Name of the network management control (NMC) the for which statistics are being calculated.
apNetMgmtCtrlStatsType	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.2	Type of specified NMC: gap-rate, gap-percent, or priority.
apNetMgmtCtrlStatsIncomingTotal	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.3	Total number of incoming calls matching a destination identifier of the NMC.
apNetMgmtCtrlStatsRejectedTotal	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.4	Number of apNetMgmtCtrlStatsIncomingTotal that are rejected.
apNetMgmtCtrlStatsStatsDivertedTotal	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.5	Number of apNetMgmtCtrlStatsIncomingTotal that are diverted.
apNetMgmtCtrlStatsStatsIncomingCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.6	Number of incoming calls during the current period that match a destination identifier
apNetMgmtCtrlStatsStatsRejectedCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.7	Number of apNetMgmtCtrlStatsIncomingCurrent that are rejected.
apNetMgmtCtrlStatsStatsDivertedCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.8	Number of apNetMgmtCtrlStatsIncomingCurrent that are diverted.
apNetMgmtCtrlStatsIncomingPeriodMax	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.9	Maximum number of incoming calls during a period that match a destination identifier of the NMC.
apNetMgmtCtrlStatsStatsRejectedPeriodMax	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.10	Number of apNetMgmtCtrlStatsIncomingPeriodMax that are rejected.
apNetMgmtCtrlStatsStatsDivertedPeriodMax	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.11	Number of apNetMgmtCtrlStatsIncomingPeriodMax that are diverted.
apNetMgmtCtrlStatsState	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.12	The state of the specified network management control, which can be disabled or enabled
Object Identifier Name: apSysMgmtMIBENUMServerStatusObjects (1.3.6.1.4.1.9148.3.2.1.4)		
Object Identifier Name: apENUMServerStatusTable (1.3.6.1.4.1.9148.3.2.1.4.1)		
Object Identifier Name: apENUMServerStatusEntry (1.3.6.1.4.1.9148.3.2.1.4.1.1)		
apENUMConfigname	apENUMServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.4.1.1.1	Name of the ENUM configuration element that contains this ENUM server.
apENUMServerIpAddress	apENUMServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.4.1.1.2	IP address of this ENUM server.
apENUMServerStatus	apENUMServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.4.1.1.3	Status of this ENUM server.

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSysMgmtMIBNSEPStatsObjects (1.3.6.1.4.1.9148.3.2.1.5)		
apNSEPStatsCurentActiveSessionsInbound	apSysMgmtMIBNSEPStatsObjects: 1.3.6.1.4.1.9148.3.2.1.5.1	Number of currently active inbound NSEP sessions.
apNSEPStatsTotalSessionsInbound	apSysMgmtMIBNSEPStatsObjects: 1.3.6.1.4.1.9148.3.2.1.5.2	Total number of inbound NSEP sessions during lifetime.
apNSEPStatsPeriodHighInbound	apSysMgmtMIBNSEPStatsObjects: 1.3.6.1.4.1.9148.3.2.1.5.3	Highest number of concurrent inbound NSEP sessions during the period.
apNSEPStatsPeriod	apSysMgmtMIBNSEPStatsObjects: 1.3.6.1.4.1.9148.3.2.1.5.4	The period for which all statistics are collected (in seconds). (Currently a non-configurable value of 30 minutes.)
Object Identifier Name: apSysMgmtMIBNSEPStatsObjects (1.3.6.1.4.1.9148.3.2.1.5)		
Object Identifier Name: apNSEPStatsRPHTable (1.3.6.1.4.1.9148.3.2.1..5.5)		
Object Identifier Name: apNSEPStatsRPHEntry (1.3.6.1.4.1.9148.3.2.1..5.5.1)		
apNSEPStatsRPHValue	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.1	The specific RPH value used for indexing (namespace.rpriority).
apNSEPStatsRPHCurrentActiveSessionsInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.2	Number of current active inbound NSEP sessions for this specific RPH value.
apNSEPStatsRPHTotalSessionsInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.3	Total number of inbound NSEP sessions for this specific RPH value during lifetime.
apNSEPStatsRPHPeriodHighInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.4	Highest number of concurrent inbound NSEP sessions during the period for this specific RPH value.
apNSEPStatsRPHTotalSessionsNotAdmittedInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.5	Total number of inbound NSEP sessions rejected for this specific RPH value during lifetime.
apNSEPStatsRPHCurrentActiveSessionsOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.6	Number of current active outbound NSEP sessions for this specific RPH value.
apNSEPStatsRPHTotalSessionsOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.7	Total number of outbound NSEP sessions for this specific RPH value during lifetime.
apNSEPStatsRPHPeriodHighOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.8	Highest number of concurrent outbound NSEP sessions during the period for this specific RPH value.
apNSEPStatsRPHTotalSessionsNotAdmittedOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5.5.1.9	Total number of outbound NSEP sessions rejected for this specific RPH value during lifetime
Object Identifier Name: apLDAPServerStatusTable (1.3.6.1.4.1.9148.3.2.1.6.1)		
Object Identifier Name: apLDAPServerStatusEntry (1.3.6.1.4.1.9148.3.2.1.6.1.1)		

SNMP GET Query Name	Object Identifier Name: Number	Description
apLDAPConfigName	apLDAPServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.6.1.1.1	Name of the LDAP configuration element that contains this LDAP server.
apLDAPServerIPAddress	apLDAPServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.6.1.1.2	IP address of this LDAP server.
apLDAPServerStatus	apLDAPServerStatusEntry: 1.3.6.1.4.1.9148.3.2.1.6.1.1.3	Status of this LDAP server.
Object Identifier Name: apSysMgmtTrapTable (1.3.6.1.4.1.9148.3.2.1.7.1)		
Object Identifier Name: apSysMgmtTrapTableEntry (1.3.6.1.4.1.9148.3.2.1.7.1.1)		
apTrapTableSystemTime	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.1	System time of the session border controller.
apTrapTableInstanceIndex	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.2	Instance index of the trap ID incremented with a resolution of a second.
apTrapTableNumVariables	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.3	Number of informarion encoded in the trap.
apTrapTableSysUptime	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.4	SNMP sysUpTime when the trap was generated.
apTrapTableTrapID	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.5	Trap ID assoicated with the fault condition.
Object Identifier Name: apSysMgmtTrapInformationTable (1.3.6.1.4.1.9148.3.2.1.7.2)		
Object Identifier Name: apSysMgmtTrapInformationTableEntry (1.3.6.1.4.1.9148.3.2.1.7.2.1)		
apTrapInformationTableDataIndex	apSysMgmtTrapInformationTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.2.1.1	Index of the information encoded in the trap.
apTrapInformationTableDataType	apSysMgmtTrapInformationTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.2.1.2	SNMP type enumerated encoded in the trap. • snmpTypeInteger is the size of integer • snmpTypeObjectIpAddress is an octet string of length 4
apTrapInformationTableDataLength	apSysMgmtTrapInformationTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.2.1.3	Octet length of the information encoded in the trap.
apTrapInformationTableDataOctets	apSysMgmtTrapInformationTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.2.1.4	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.
Object Identifier Name: apSysMgmtInterfaceObjects (1.3.6.1.4.1.9148.3.2.1.8)		

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSysMgmtPhyUtilTable (1.3.6.1.4.1.9148.3.2.1.8.1)		
Object Identifier Name: apSysMgmtPhyUtilTableEntry (1.3.6.1.4.1.9148.3.2.1.8.1.1)		
apPhyUtilTableRxUtil	apSysMgmtPhyUtilTableEntry: 1.3.6.1.4.1.9148.3.2.1.8.1.1.1	RX network utilization of the physical port measured over a one second period.
apPhyUtilTableTxUtil	apSysMgmtPhyUtilTableEntry: 1.3.6.1.4.1.9148.3.2.1.8.1.1.2	TX network utilization of the physical port measured over a one second period

System Management Scalar Examples

The following example shows the scalar variables associated with the system management MIB. The values given in the example are samples that will differ from your values.

Instance ID	Value
ApSysCPUUtil.0	0
ApSysMemoryUtil.0	32
ApSysHealthScore.0	0
ApSysRedundancy.0	active
ApSysGlobalConSess.0	0
ApSysGlobalCPS.0	0
ApSysNATCapacity.0	0
ApSysARPCapacity.0	1
ApSysState.0	online

Session Statistical Group Table Examples

The following example system management MIB session statistical values. The values given in the example are samples that will differ from your values.

OID	Table Index
	1
apCombinedStatsSessionAgentIndex	1
apCombinedStatsSessionAgentHostname	192.168.69.64
apCombinedStatsSessionAgentType	sip
apCombinedCurrentActiveSessionsInbound	0
apCombinedStatsSessionRateInbound	0
apCombinedStatsCurrentActiveSessionsOutbound	0
apCombinedStatsTotalSessionsInbound	0
apCombinedStatsTotalSessionsInbound	0

OID	Table Index
apCombinedStatsTotalSessionsNotAdmittedInbound	0
apCombinedStatsPeriodHighInbound	0
apCombinedStatsAverageRateInbound	0
apCombinedStatsTotalSessionsOutbound	0
apCombinedStatsTotalSessionsNotAdmittedOutbound	0
apCombinedStatsPeriodHighOutbound	0
apCombinedStatsAverageRateOutbound	0
apCombinedStatsMaxBurstRate	1
apCombinedStatsPeriodSeizures	0
apCombinedStatsPeriodAnswers	0
apCombinedStatsPeriodASR	0
apCombinedStatsAverageLatency	0
apCombinedStatsMaxLatency	0
apCombinedStatsSessionAgent	inService

SIP Session Agent Statistics Table Example

The following example shows system management SIP session agent statistical values. The values given in the example are samples that will differ from your values.

OID	Table Index
	1
apSipSAStatsSessionAgentIndex	1
apSipSAStatsSessionAgentHostname	192.168.69.64
apSipSAStatsSessionAgentType	sip
apSipSAStatsCurrentActiveSessionsInbound	0
apSipSAStatsCurrentSessionRateInbound	0
apSipSAStatsCurrentActiveSessionsOutbound	0
apSipSAStatsCurrentSessionRateOutbound	0
apSipSAStatsTotalSessionsInbound	0
apSipSAStatsTotalSessionsNotAdmittedInbound	0
apSipSAStatsPeriodHighInbound	0
apSipSAStatsAverageRateInbound	0
apSipSAStatsTotalSessionsOutbound	0
apSipSAStatsTotalSessionsNotAdmittedOutbound	0
apSipSAStatsPeriodHighOutbound	0
apSipSAStatsAverageRateOutbound	0

OID	Table Index
apSipSAStatsMaxBurstRate	1
apSipSAStatsPeriodSeizures	0
apSipSAStatsPeriodAnswers	0
apSipSAStatsPeriodASR	0
apSipSAStatsAverageLatency	0
apSipSAStatsMaxLatency	0
apSipSAStatsSessionAgentStatus	inService

H.323 Session Agent Statistics Table Example

The following example shows system management H.323 session agent statistical values. The values given in the example are samples that will differ from your values.

OID	Table Index
	1
apH323SAStatsSessionAgentIndex	1
apH323SAStatsSessionAgentHostname	There are no session agents of this type defined.
apH323SAStatsSessionAgentType	sip
apH323SAStatsCurrentActiveSessionsInbound	0
apH323SAStatsCurrentSessionRateInbound	0
apH323SAStatsCurrentActiveSessionsOutbound	0
apH323SAStatsCurrentSessionRateOutbound	0
apH323SAStatsTotalSessionsInbound	0
apH323SAStatsTotalSessionsNotAdmittedInbound	0
apH323SAStatsPeriodHighInbound	0
apH323SAStatsAverageRateInbound	0
apH323SAStatsTotalSessionsOutbound	0
apH323SAStatsTotalSessionsNotAdmittedOutbound	0
apH323SAStatsPeriodHighOutbound	0
apH323SAStatsAverageRateOutbound	0
apH323SAStatsMaxBurstRate	1
apH323SAStatsPeriodSeizures	0
apH323SAStatsPeriodAnswers	0
apH323SAStatsPeriodASR	0
apH323SAStatsAverageLatency	0
apH323SAStatsMaxLatency	0
apH323SAStatsSessionAgentStatus	outOfService

Signaling Realm Statistics Table Example

The following example shows system management signaling realm statistical values. The values given in the example are samples that will differ from your values.

OID	Table Index	
	1	2
apSigRealmStatsRealmIndex	1	2
apSigRealmStatsRealmName	sip192	sip192a
apSigRealmStatsCurrentActiveSessionsInbound	0	0
apSigRealmStatsCurrentSessionRateInbound	0	0
apSigRealmStatsCurrentActiveSessionsOutbound	0	0
apSigRealmStatsCurrentSessionRateOutbound	0	0
apSigRealmStatsTotalSessionsInbound	0	0
apSigRealmStatsTotalSessionsNotAdmittedInbound	0	0
apSigRealmStatsPeriodHighInbound	0	0
apSigRealmStatsAverageRateInbound	0	0
apSigRealmStatsTotalSessionsOutbound	0	0
apSigRealmStatsTotalSessionsNotAdmittedOutbound	0	0
apSigRealmStatsPeriodHighOutbound	0	0
apSigRealmStatsAverageRateOutbound	0	0
apSigRealmStatsMaxBurstRate	0	0
apSigRealmStatsPeriodSeizures	1	0
apSigRealmStatsPeriodAnswers	0	0
apSigRealmStatsPeriodASR	0	0
apSigRealmStatsAverageLatency (not supported)	0	0
apSigRealmStatsMaxLatency (not supported)	0	0

Notes on ENUM Server Names

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

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

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

- aaa, with servers 1.1.1.1 and 1.1.1.2
- BBB, with servers 3.3.3.3 and 3.3.3.2

- cc, with server 2.2.2.2

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

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

Acme Packet License MIB (ap-license.mib)

The following table describes the SNMP GET query names for the Acme Packet License MIB (ap-license.mib).

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apLicenseEntry (1.3.6.1.4.1.9148.3.5.1.1.1)		
apLicenseKey	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.2	Key, not applicable to the first index, which represents the consolidated license. Displays N/A.
apLicenseCapacity	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.3	Maximum number of simultaneous sessions allowed by a system for all combined protocols.
apInstallDate	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.4	Installation time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
apLicenseBeginDate	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.5	Installation time and date in the following format: hh:mm:ss month day year. Displays N/A if a license is not enabled.
apLicenseExpireDate	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.6	Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
apLicenseSIPFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.7	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.8	Value that indicates whether a Media Gateway Control Protocol (MGCP) license is present. A value of 1 indicates that MGCP licensing is enabled. A value of 2 indicates that MGCP licensing is not enabled.
apLicenseH323Feature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.9	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.10	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.11	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.

apLicenseExpireDate	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.6	Expiration time and date in the following format: hh:mm:ss Month Day Year. Displays N/A if a license is not enabled.
apLicenseSIPFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.7	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.8	Value that indicates whether a Media Gateway Control Protocol (MGCP) license is present. A value of 1 indicates that MGCP licensing is enabled. A value of 2 indicates that MGCP licensing is not enabled.
apLicenseH323Feature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.9	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.10	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	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.11	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.

License Table Examples

The following example shows license table values. The values given in the example are samples that will differ from your values.

OID	Table Index	
	1	2
apLicenseKey	N/A	gjjt4vv602vhg387mrfuatjist093gg u42hbto3
apLicenseCapacity	32000	32000
apLicenseInstallDate	N/A	10:57:12 FEB 16 2005
apLicenseBeginDate	N/A	N/A
apLicenseExpireDate	N/A	N/A
apLicenseSIPFeature	TRUE	TRUE
apLicenseMGCPFeature	TRUE	TRUE
apLicenseH323Feature	TRUE	TRUE
apLicenseIWFFeature	TRUE	TRUE
apLicenseQOSFeature	TRUE	TRUE
apLicenseACPFeature	TRUE	TRUE
apLicenseLPFeature	TRUE	TRUE
apLicenseSAGFeature	TRUE	TRUE
apLicenseACCTFeature	TRUE	TRUE
apLicenseHAFeature	TRUE	TRUE
apLicensePACFeature	TRUE	TRUE

Acme Packet Software Inventory MIB (ap-swinventory.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSwBootEntry (1.3.6.1.4.1.9148.3.4.1.1.1.1)		
apSwBootDescr	apSwBootEntry: 1.3.6.1.4.1.9148.3.4.1.1.1.1.2	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'.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSwBootType	apSwBootEntry: 1.3.6.1.4.1.918.3.4.1.1.1.1.3	Type of software image. A value of 1 indicates a boot Image. A value of 2 indicates a bootloader image.
apSwBootStatus	apSwBootEntry: 1.3.6.1.4.1.918.3.4.1.1.1.1.4	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.
Object Identifier Name: apSwInventoryCfgObjects (1.3.6.1.4.1.9148.3.4.1.2)		
apSwCfgCurrentVersion	apSwInventoryCfgObjects: 1.3.6.1.4.1.9148.3.4.1.2.1	Current version of the saved configuration.
apSwCfgRunningVersion	apSwInventoryCfgObjects: 1.3.6.1.4.1.9148.3.4.1.2.2	Current version of the running configuration.
Object Identifier Name: apSwCfgBackupEntry (1.3.6.1.4.1.9148.3.4.1.2.3.1)		
apSwCfgBackupName	apSwCfgbackupEntry: 1.3.6.1.4.1.9148.3.4.1.2.3.1.2	Description of the configuration filename, for example: p1604, 063004-cfg.

Configuration Scalar Example

The following example shows the configuration scalar variables associated with the software inventory MIB. The values given in the table are samples that will differ from your values.

Instance ID	Value
ApSwCfgCurrentVersion.0	80
ApSwCfgRunningVersion.0	80

Software Image Table Examples

The following example shows software image table values. The values given in the table are samples that will differ from your values.

OID	Table Index		
	1	2	3
apSwBootDescr	111.22.3.44/prod1.gz	111.22.3.44/distrib2.gz	bank0:01/21/2005 08:17:26
apSwBootType	bootImage	bootImage	bootLoader
apSwBootStatus	previousUsed	currentUsing	currentUsing

Backup Configuration Table Example

The following example shows backup configuration table values. The values given in the table are samples that will differ from your values.

OID	Table Index		
	1	2	3
apSwCfgBackupName	Perf1-SingleSipNat.tar.gz	perf1_200.tar.gz	my3-single-sip-nat.tar.gz

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

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apEnvMonObjects(1.3.6.1.4.1.9148.3.3.1)		
apEnvMonI2CState	apEnvMonObjects: 1.3.6.1.4.1.9148.3.3.1.1	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
Object Identifier Name: apEnvMonVoltageStatusEntry (1.3.6.1.4.1.9148.3.3.1.2.1.1)		
apEnvMonVoltageStatusType	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.2	Entity part type from which the voltage value is from: • v2p5- 2.5v sensor: L3 cache core voltage; micro-processor and co-processor I/O voltage; Field-Programmable Gate Array (FPGA) memories I/O voltage. • v3p3 - 3.3V sensor: general TTL supply rail; control logic; micro-processor; micro-processor and co-processor; SDRAM • v5 - 5V sensor: fans; micro-processor core voltage regulator • CPU sensor: CPU voltage; micro-processor core voltage

SNMP GET Query Name	Object Identifier Name: Number	Description
apEnvMonVoltageStatusDescr	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.3	Textual description of the entity being monitored for voltage.
apEnvMonVoltageStatusValue	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.4	Current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value.
apEnvMonVoltageState	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.5	Current state of the voltage for the device being monitored. Possible values are: **Host Processor 7455** • normal range: 1.55v to 1.65v • minor range: 1.4v to 1.55v or 1.65v to 1.8v • shutdown range: <1.4v or >1.8v **Host Processor 7457** Version 1.0 • normal range: 1.35v to 1.45v • minor range: 1.00v to 1.35v or 1.45v to 1.6v • shutdown range: <1.0v or >1.6v Version 1.1 and later • normal range: 1.25v to 1.35v • minor range: 1.00v to 1.25v or 1.35v to 1.6v • shutdown range: <1.0v or >1.6v
apEnvMonVoltageSlotID	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.6	Slot for this voltage.
apEnvMonSlotType	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.7	Type of module found in this slot.
Object Identifier Name: apEnvMonTemperatureStatusEntry (1.3.6.1.4.1.9148.3.3.1.3.1.1)		
apEnvMonTemperatureStatusType	apEnvMonTemperatureObjects: 1.3.6.1.4.1.9148.3.3.1.3.1.1.2	Indicates the entity being monitored for temperature. Values are: • ds1624sMain (1) • ds1624sCPU (2) • lm84 (3) • lm75 (4) • lm75Main (5) • lm75Cpu (6) • lm75Phy (7)
apEnvMonTemperatureStatusDescr	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.3	Description of the temperature being monitored. It has the value of the Main Board PROM Temperature (in Celsius).
apEnvMonTemperatureStatusValue	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.4	The current temperature of the main board PROM in Celsius.

SNMP GET Query Name	Object Identifier Name: Number	Description
apEnvMonTemperatureState	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.5	Current state of the temperature which can have one of the following values: Net-Net 3800: 1: initial. Temperature is at its initial state. 2: normal. The temperature is normal. 3: minor alarm - the temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius. 4: major alarm. The temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius. 5: critical alarm. The temperature is greater than 73 degrees Celsius. 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. Net-Net 4500: 1: initial. Temperature is at its initial state. 2: normal. The temperature is normal. 3: minor alarm - the temperature is greater than or equal to 95 degrees Celsius and less than 100 degrees Celsius. 4: major alarm. The temperature is greater than or equal to 100 degrees Celsius and less than 105 degrees Celsius. 5: critical alarm. The temperature is greater than or equal to 105 degrees Celsius. 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.
apEnvMonTemperatureSlotID	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.6	Slot for which this temperature is found.
apEnvMonTemperatureSlotType	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.7	Type of module found in this slot.

```
Object Identifier Name: apEnvMonFanStatusEntry (1.3.6.1.4.1.9148.3.3.1.4.1.1)
```

SNMP GET Query Name	Object Identifier Name: Number	Description
apEnvMonFanStatusType	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.2	Location of the fan, which can have one of the following values: 11: fan1 12: fan2 13: fan3 14: fan4
apEnvMonFanStatusDescr	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.3	Textual description of the fan.
apEnvMonFanStatusValue	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.4	Current measurement of fan speed in percentage.
apEnvMonFanState	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.5	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	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.6	Current state of the fan being monitored.
apEnvMonFanSlotID	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.7	Slot where this fan is found. A zero is returned if this fan is not the type slot.
Object Identifier Name: apEnvMonPowerSupplyStatusEntry (1.3.6.1.4.1.9148.3.3.1.5.1.1)		
apEnvMonPowerSupplyStatusType	apEnvMonPowerSupplyStatusEntr: 1.3.6.1.4.1.9148.3.3.1.5.1.1.2	Location of the power supply, which can have one of the following values: 0: left power supply A 1: right power supply B 3: slot
apEnvMonPowerSupplyStatusDescr	apEnvMonPowerSupplyStatusEntr: 1.3.6.1.4.1.9148.3.3.1.5.1.1.3	Textual description of the power supply.
apEnvMonPowerSupplyState	apEnvMonPowerSupplyStatusEntr: 1.3.6.1.4.1.9148.3.3.1.5.1.1.4	Current state of the power supply. Values: 2: normal. The power supply is normal. 7: not present: The power supply sensor does not exist.
Object Identifier Name: apEnvPhyCardStatusEntry (1.3.6.1.4.1.9148.3.3.1.6.1.1)		

SNMP GET Query Name	Object Identifier Name: Number	Description
apEnvMonPhyCardStatusDescr	apEnvPhyCardStatusEntry: 1.3.6.1.4.1.9148.3.3.1.6.1.1.3	Textual description of the phy card.
apEnvMonPhyCardState	apEnvPhyCardStatusEntry: 1.3.6.1.4.1.9148.3.3.1.6.1.1.4	The current state of the phy card. Values: 2: normal 7: not present

I2C State Scalar Examples

The following example shows the I2C scalar variables associated with the environment monitoring MIB. The values given in the example are samples that will differ from your values.

Instance ID	Value
ApEnvMonI2Cstate.0	normal
ApEnvMonEnableStatChangeNotif.0	32

Voltage Status Table Examples

The following example shows voltage status table values. The values given in the example are samples that will differ from your values.

OID	Table Index			
	1	2	3	4
apEnvMonVoltageStatusType	v2p5	v3p3	v5	cpu
apEnvMonVoltageStatusDesc	2.5V voltage (millivolts)	3.3V voltage (millivolts)	5V voltage (millivolts)	CPU voltage (millivolts)
apEnvMonVoltageStatusValue	2526	3265	5052	1253
apEnvMonVoltageState	normal	normal	normal	normal

Temperature Status Table Examples

The following example shows temperature status values. The values given in the example are samples that will differ from your values.

OID	Table Index
	1
apEnvMonTemperatureStatusType	ds1624sCPU
apEnvMonTemperatureStatusDescr	Host processor PROM Temperature (degrees Celsius)
apEnvMonTemperatureStatusValue	38
apEnvMonTemperatureState	Normal

Fan Status Table Examples

The following table shows fan status values. The values given in the example are samples that will differ from your values.

OID	Table Index			
	1	2	3	
apEnvMonFanStatusType	Fan1	Fan2	Fan3	Fan4
apEnvMonFanStatusDesc	Fan 1 speed	Fan 2 speed	Fan 3 speed	
apEnvMonFanStatusValue	99	100	98	
apEnvMonFanState	normal	normal	normal	

Power Supply Status Table Examples

The following table shows power supply status values. The values given in the example are samples that will differ from your values.

OID	Table Index	
	1	2
apEnvMonPowerSupplyStatusType	left	right
apEnvMonPowerSupplyStatusDesc	Power supply A	Power supply B
apEnvMonPowerSupplyState	normal	notPresent

Acme Packet Security MIB (ap-security.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSecurityMIBObjects (1.3.6.1.4.1.9148.3.9.1)		
apSecurityOCSRIpAddress	1.3.6.1.4.1.9148.3.9.1.5	OCSR server IP Address
apSecurityOCSRHostname	1.3.6.1.4.1.9148.3.9.1.6	OCSR server hostname
Object Identifier Name: apSecurityTacacsTable (1.3.6.1.4.1.9148.3.9.1.4)		
Object Identifier Name: apSecurityTacacsEntry (1.3.6.1.4.1.9148.3.9.1.4.1)		
apSecurityTacacsCliCommands	apSecurityTacacsEntry: 1.3.6.1.4.1.9148.3.9.1.4.1.3	Number of CLI commands sent for TACACS+ accounting
apSecurityTacacsSuccessAuthentication	apSecurityTacacsEntry: 1.3.6.1.4.1.9148.3.9.1.4.1.4	Number of successful TACACS+ authentication requests
apSecurityTacacsFailureAuthentication	apSecurityTacacsEntry: 1.3.6.1.4.1.9148.3.9.1.4.1.5	Number of failed TACACS+ authentication requests
apSecurityTacacsSuccessAuthorization	apSecurityTacacsEntry: 1.3.6.1.4.1.9148.3.9.1.4.1.6	Number of successful TACACS+ authorization requests
apSecurityTacacsFailureAuthorization	apSecurityTacacsEntry: 1.3.6.1.4.1.9148.3.9.1.4.1.7	Number of failed TACACS+ authorization requests

Acme Packet Diameter MIB (ap-diameter.mib)

The following table describes the SNMP Get query names for the Acme Packet Diameter MIB (ap-diameter.mib).

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apDiamMIBObjects (.1.3.6.1.4.1.9148.3.13.1.1)		
Object Identifier Name: apDiamMIBTabularObjects (.1.3.6.1.4.1.9148.3.13.1.1.2)		
Object Identifier Name: apDiamClfErrorStatsTable (.1.3.6.1.4.1.9148.3.13.1.1.2.1)		
Object Identifier Name: apDiamClfErrorStatsEntry (.1.3.6.1.4.1.9148.3.13.1.1.2.1.1)		
apDiamClfExtPolSvrName	1.3.6.1.4.1.9148.3.13.1.1.2.1.1.2	External policy server name
apDiamClfErrorsRecent	1.3.6.1.4.1.9148.3.13.1.1.2.1.1.3	Number of diameter errors in recent period received on e2 interface with the CLF.
apDiamClfErrorsTotal	1.3.6.1.4.1.9148.3.13.1.1.2.1.1.4	Total number of diameter errors in life time received on e2 interface with the CLF.
apDiamClfErrorsPerMax	1.3.6.1.4.1.9148.3.13.1.1.2.1.1.5	PerMax count of diameter errors in life time received on e2 interface with the CLF.

Object group in ap-diameter.mib	apDiamACCTObjectsGroup Objects: • apDiamAcctSrvrHostName • apDiamAcctSrvrIPPort • apDiamAcctSrvrOriginRealm • apDiamAcctSrvrOriginHost • apDiamAcctSrvrOriginTransportType (apDiamNotificationGroups 1)	Object group accessible only to traps for Diameter Server information.
Object group in ap-diameter.mib	apDiamACCTNotificationsGroup Objects: • apDiameterAcctSrvrUpTrap • apDiamAcctSrvrDownTrap • apAcctMsgQueueFullTrap • apAcctMsgQueueFullClearTrap (apDiamNotificationGroups 2)	Notification group for Diameter server events.

Object group in ap-diameter.mib	apDiamClfErrorStatsGroup Includes: • apDiamClfExtPolSvrName • apDiamClfErrorsRecent • apDiamClfErrorsTotal • apDiamClfErrorsPerMax (apDiamObjectGroups 1)	Object group for CLF statistics of external policy server errors.
Object group in ap-diameter.mib	apDiamACCTResultObjectsGroup Includes: • apDiameterResultCode (apDiamNotificationGroups 3)	Object group accessible only to traps for Result-Code (268) AVP value.

Acme Packet SIP MIB (ap-sip.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSipMIBGeneralObjects (		
apSipSecInterfaceTotalRegistrations	1.3.6.1.4.1.9148.3.15.1.1.1.1.0	Total number of registrations on all secondary SIP interfaces.
apSipSecInterfaceRegThreshold	1.3.6.1.4.1.9148.3.15.1.1.1.2.0	The maximum threshold for registrations on all secondary SIP interfaces. If this threshold is exceeded, an alarm is raised.
apSipSecInterfaceClearThreshold	1.3.6.1.4.1.9148.3.15.1.1.1.3.0	The threshold for registrations on all secondary SIP interfaces to clear an alarm.

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.

Acme Packet Codec and Transcoding MIB (ap-codec.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apCodecMIBObjects (1.3.6.1.4.1.9148.3.7.1)		
Object Identifier Name: apCodecRealmStatsTable (1.3.6.1.4.1.9148.3.7.1.1)		
Object Identifier Name: apCodecRealmStatsEntry (1.3.6.1.4.1.9148.3.7.1.1.1)		
apCodecRealmCountOther	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.1	Count of the SDP media streams received in the realm which negotiated to a codec not defined in this table.

SNMP GET Query Name	Object Identifier Name: Number	Description
apCodecRealmCountPCMU	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.2	Count of SDP media streams received in the realm which negotiated to the PCMU codec.
apCodecRealmCountPCMA	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.3	Count of SDP media streams reveived in the realm which negotiated to the PCMA codec.
apCodecRealmCountG722	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.4	Count of SDP media streams reveived in the realm which negotiated to the G722 codec.
apCodecRealmCountG723	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.5	Count of SDP media streams reveived in the realm which negotiated to the G723 codec.
apCodecRealmCountG726-16	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.6	Count of SDP media streams reveived in the realm which negotiated to the G726-16 codec.
apCodecRealmCountG726-24	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.7	Count of SDP media streams reveived in the realm which negotiated to the G726-24 codec.
apCodecRealmCountG726-32	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.8	Count of SDP media streams reveived in the realm which negotiated to the G726-32 codec.
apCodecRealmCountG726-40	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.9	Count of SDP media streams reveived in the realm which negotiated to the G726-40 codec.
apCodecRealmCountG728	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.10	Count of SDP media streams reveived in the realm which negotiated to the G728 codec.
apCodecRealmCountG729	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.11	Count of SDP media streams reveived in the realm which negotiated to the G729 codec.
apCodecRealmCountGSM	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.12	Count of SDP media streams reveived in the realm which negotiated to the GSM codec.
apCodecRealmCountILBC	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.13	Count of SDP media streams reveived in the realm which negotiated to the iLBC codec.
apCodecRealmCountAMR	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.14	Count of SDP media streams reveived in the realm which negotiated to the AMR codec.
apCodecRealmCountEVRC	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.15	Count of SDP media streams reveived in the realm which negotiated to the EVRC codec.
apCodecRealmCountH261	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.16	Count of SDP media streams reveived in the realm which negotiated to the H261 codec.
apCodecRealmCountH263	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.17	Count of SDP media streams reveived in the realm which negotiated to the H.263 codec.
apCodecRealmCountT38	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.18	Count of SDP media streams reveived in the realm which negotiated to the T.38 codec.
apCodecRealmCountAMRWB	apCopdecRealmStatsEntry 1.3.6.1.4.1.9148.3.7.1.1.1.19	Count of SDP media streams reveived in the realm which negotiated to the AMR-WB codec.
Object Identifier Name: apTranscodingMIBObjects (1.3.6.1.4.1.9148.3.7.2)		
Object Identifier Name: apCodecTranscodingRealmStatsTable (1.3.6.1.4.1.9148.3.7.2.1)		
Object Identifier Name: apTranscodingRealmStatsEntry (1.3.6.1.4.1.9148.3.7.2.1.1)		
apCodecRealmSessionsTransparent	apCodecTranscodingRealmStatsEntry: 1.3.6.1.4.1.9148.3.7.2.1.1.1	Number of sessions in the realm that did not use any DSP resources for transcoding or transrating.

SNMP GET Query Name	Object Identifier Name: Number	Description
apCodecRealmSessionsTransrated	apCodecTranscodingRealmStatsEntry: 1.3.6.1.4.1.9148.3.7.2.1.1.2	Number of sessions in the realm that had a common codec but used DSP resources to modify packetization rate.
apCodecRealmSessionsTranscoded	apCodecTranscodingRealmStatsEntry: 1.3.6.1.4.1.9148.3.7.2.1.1.3	Number of sessions in the realm that had used DSP resources to transcode between codecs.
Object Identifier Name: apSysMgmtMIBSessionObjects (1.3.6.1.4.1.9148.3.2.1.2)		
Object Identifier Name: apSigRealmStatsTable (1.3.6.1.4.1.9148.3.2.1.2.4)		
Object Identifier Name: apSigRealmStatsEntry (1.3.6.1.4.1.9148.3.2.1.2.4.1)		
apSigRealmStatsRealmName	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.2	Nmae of the realm the following for which the following statistics are being calculated.
apSigRealmStatsCurrentActiveSessionsInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.3	Number of current active inbouind sessions.
apSigRealmStatsCurrentSessionRateInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.4	Current inbound session rate in CPS.
apSigRealmStatsCurrentActiveSessionsOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.5	Number of current active outbound sessions.
apSigRealmStatsCurrentSessionRateOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.6	Current outbound session rate in CPS.
apSigRealmStatsTotalSessionsInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.7	Total number of inbound sessions.
apSigRealmStatsTotalSessionsNotAdmittedInbouind	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.8	Total number of inbound sessions rejected due to insufficient bandwidth.
apSigRealmStatsPeriodHighInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.9	Highest number of concurrent inbound sessions during the period.
apSigRealmStatsAverageRateInbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.10	Average rate of inbound sessions during the period in CPS.
apSigRealmStatsTotalSessionsOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.11	Total number of outbound sessions.
apSigRealmStatsTotalSessionsNotAdmittedOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.12	Total number of outbound sessions rejected due to insufficient bandwidth.
apSigRealmStatsPeriodHighOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.13	Highest number of concurrent outbound sessions during the period.
apSigRealmStatsAverageRateOutbound	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.14	Average rate of outbound sessions during the period in CPS.
apSigRealmStatsMaxBurstRate	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.15	Maximum burst rate of traffic measured during the period (combined inbound and outbound).
apSigRealmStatsPeriodSeizures	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.16	Total number of seizures during the period.
apSigRealmStatsPeriodAnswers	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.17	Total number of answered sessions during the period.

SNMP GET Query Name	Object Identifier Name: Number	Description
apSigRealmStatsPeriodASR	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.18	Answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 represents 90% or .90.
apSigRealmStatsAverageLatency (not supported)	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.19	Average observed one-way signaling latency during the period in milliseconds.
apSigRealmStatsMaxLatency (not supported)	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.20	Maximum observed one-way signaling latency during the period in milliseconds.
apSigRealmStatsMinutesLeft	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.21	Number of montly-minutes left in the pool per calendar month for a given realm.
apSigRealmStatsMinutesReject	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.22	Peg counts of number of rejected calls due to monthly-minutes constraints exceeded.
apSigRealmStatsShortSessions	apSigRealmStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.4.1.23	Lifetime number of sessions whose duration was less than the configured short session duration.

Transcoding Capacity in Acme Packet 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.

SNMP Object Name	Object Identifier Name: Number	Description
Object Identifier Name: apSysMgmtMIBObjects (1.3.6.1.4.1.9148.3.2.1)		
Object Identifier Name: apSysMgmtGeneralObjects (1.3.6.1.4.1.9148.3.2.1.1)		
apSysXCodeCapacity	apSysMgmtGeneralObjects 1.3.6.1.4.1.9148.3.2.1.1.34	Percentage of transcoding utilization.
apSysXCodeAMRCapacity	apSysMgmtGeneralObjects 1.3.6.1.4.1.9148.3.2.1.1.35	Percentage of licensed AMR transcoding sessions.
apSysXCodeAMRWBCapacity	apSysMgmtGeneralObjects 1.3.6.1.4.1.9148.3.2.1.1.36	Percentage of licensed AMR-WB transcoding sessions.
apSysXCodeEVRCCapacity	apSysMgmtGeneralObjects 1.3.6.1.4.1.9148.3.2.1.1.39	Percentage of licensedEVRC transcoding sessions.
apSysXCodeEVRCBCapacity	apSysMgmtGeneralObjects 1.3.6.1.4.1.9148.3.2.1.1.39	Percentage of licensedEVRCB transcoding sessions.

Acme Packet (ap-usbcsys.mib) Multicore Monitoring MIB

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

OID	Object Name	Description
1.3.6.1.4.1.9148.3.17	apUsbcSysModule	
1.3.6.1.4.1.9148.3.17.1	apUsbcSysMIBObjects	
1.3.6.1.4.1.9148.3.17.1.1	apUsbcSysObjects	

OID	Object Name	Description
1.3.6.1.4.1.9148.3.17.1.1.1	apUsbcSysCpuUtilAll	The percentage of total Cpu utilization.
1.3.6.1.4.1.9148.3.17.1.1.2	apUsbcSysCpuCount	The number of cpus for this system.
1.3.6.1.4.1.9148.3.17.1.1.3	apUsbcSysCpuSpeedMHz	The speed in MHz of the cpus for this system.
1.3.6.1.4.1.9148.3.17.1.1.4	apUsbcSysMemSzMB	The number of megabytes of all cpus for this system.
1.3.6.1.4.1.9148.3.17.1.1.5	apUsbcSysMemSzGB	The number of gigabytes of all cpus for this system. This value is derived from the apUsbcSysMemSzMB object.
1.3.6.1.4.1.9148.3.17.1.1.6	apUsbcSysAppMemUtil	The number of megabytes of memory used by the applications.
1.3.6.1.4.1.9148.3.17.1.1.7	apUsbcSysKernelMemUtil	The number of megabytes of memory used by the kernel.
1.3.6.1.4.1.9148.3.17.1.1.8	apUsbcSysMyBogoMips	The processor speed measured in millions of instructions per second per processor, calculated by the kernel at boot time.
1.3.6.1.4.1.9148.3.17.1.1.9	apUsbcSysAllBogoMips	The sum of all bogo mips(millions of instructions per second) of all cpus for this system.
1.3.6.1.4.1.9148.3.17.1.1.10	apUsbcSysCpuTblObjects	
1.3.6.1.4.1.9148.3.17.1.1.10.1	apUsbcSysCpuTable	A read-only table to hold information for a cpu indexed by the cpu number i + 1.
1.3.6.1.4.1.9148.3.17.1.1.10.1.1	apUsbcSysCpuEntry	A entry designed to hold the status of a single Cpu.
1.3.6.1.4.1.9148.3.17.1.1.10.1.1.1	apUsbcSysCpuNum	The cpu number + 1 of this entry.
1.3.6.1.4.1.9148.3.17.1.1.10.1.1.2	apUsbcSysCpuUtil	The percent of cpu utilization of this cpu.

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.

```
ACMEPACKET# 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

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

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

SNMP Reporting of Message Rate Statistics

The message rate statistics feature was introduced in S-CX6.4.0. It enables the system to provide message rate statistics for SIP, DNS, and ENUM traffic via ACLI and HDR output. This feature has been enhanced to offer the same statistics 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 extra-method-stats parameter in the sip-config is enabled for the system to collect these statistics.

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 apSipInterface table in Ap-sip.mib. The SIP method to index mapping is found in the ApSipMethod object in Ap-tc.mib.

```
&lt;127:%&gt;- snmpwalk -v 2c -c public 172.30.68.100
apSipRateIntfStatsTable
APSIP-MIB::apSipRateIntfMsgRcvd.21.other = Gauge32: 0 messages per 10
seconds
APSIP-MIB::apSipRateIntfMsgRcvd.21.invite = Gauge32: 0 messages per 10
seconds
```

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 agentcommand. The table is indexed by the SIP agent index and SIP method. The SIP Agent to index number mapping is found in the apSipAgent table in Ap-sip.mib. The SIP method to index mapping is found in the ApSipMethod object in Ap-tc.mib.

apDnsAlgServerRateStatsTable

This table, found in the Ap-dnsalg.mib, provides a listing of message rate statistics for a specific DNS Alg Server. It conveys the same information displayed in the show dnsalg rate realm-id and show dnsalg rate server-ip-addr commands. The table is indexed by the DNS ALG realm index, 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 realm, DNS ALG server, lf 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.

```
-<%>- snmpwalk -v 2c -c public 172.30.68.100
apDnsAlgServerRateStatsTable
MIB::apDnsAlgServerInetAddressType.37.1.ipv4."2.2.2.2" = INTEGER:
ipv4(1)
APDNSALG-MIB::apDnsAlgServerInetAddressType.38.1.ipv4."4.4.4.4" =
INTEGER: ipv4(1)
APDNSALG-MIB::apDnsAlgServerInetAddress.37.1.ipv4."2.2.2.2" = Hex-
STRING: 02 02 02 02
APDNSALG-MIB::apDnsAlgServerInetAddress.38.1.ipv4."4.4.4.4" = Hex-
STRING: 04 04 04 04
```

```
APDNSALG-MIB::apDnsAlgServerRateMsgRcvd.37.1.ipv4."2.2.2.2" =
Gauge32: 0 messages per 10 seconds
```

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).

```
-<%>- snmpwalk -v 2c -c public 172.30.68.100 apEnumServerRateStatsTable
APAPPS-MIB::apEnumServerRateMsgRcvd."enumTest".ipv4."172.30.68.85" =
Gauge32: 0 messages per 10 seconds
```

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
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.36 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000000 = Gauge32: 0
SNMPv2-SMI::enterprises.9148.3.2.1.2.2.1.4.10000001 = Gauge32: 0
FQDN-resolved Session Agent Statistics SNMP Traps
```

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

CAC Utilization Statistics via SNMP

The Oracle USM allows you to retrieve information on current session utilization and burst rate as a percentage of their configured maximums on per session-agent and/or realm basis. The Oracle USM uses the configured max-session and max-burst-rate settings in conjunction with a percentage formula to calculate this value. The system also uses an ACLI configuration setting to establish the threshold at which trap and trap clear messages are sent from the SNMP agent to the configured manager(s).

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

SNMP Get for CAC Utilization

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

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

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

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

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

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

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

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

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

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

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

You configure the value that triggers these traps as a percentage of the max-session and max-burst-rate settings configured for the applicable session agent and/or realm. The system uses the same setting to specify when to send both the sessions and burst rate traps. The name of this parameter is the cac-trap-threshold.

For realms, you configure a session-constraint element with the cac-trap-threshold setting and apply that session constraint to the realm. For a session agent however, you configure the cac-trap-threshold directly within the session agent's configuration.

The syntax for the command is the same within session constraint and session agent configurations.

cac-trap-threshold [0-99]

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

A Enterprise Trap Examples

Overview

This appendix provides examples of traps sent according to the criteria established in the Acme Packet syslog MIB (`ap-slog.mib`) and an example of a trap sent according to the criteria established in the Acme Packet System Management MIB (ap-smgmt.mib).

Enterprise Trap Examples

Two Oracle USMs, both capable of sending out traps, generated these examples. One Oracle USM's IP address is 10.0.1.144 and the other Oracle USM's IP address is 10.0.2.233.

> **Note:** The display format of SNMP traps depends on the type of packet capture or SNMP test tools that you use.

snmp-community and trap-receiver Elements

The following ACLI examples show the Oracle USM's configured `snmp-community` and `trap-receiver` configuration elements used in the syslog MIB and System management MIB trap examples. Although two different Oracle USM's were used to generate these examples, the configured `snmp-community` and `trap-receiver` elements and field values are the same.

> **Note:** To access the `snmp-community and` `trap-receiver` configuration elements, you must first access the ACLI in Superuser mode. From the system prompt, enter configure terminal and follow the system ACLI path to access these configuration elements.

The trap receiver (configured in the `trap-receiver` element) corresponds to an SNMP test tool with an IP address of 10.0.1.27. Acme Packet's enterprise MIBs have been compiled in this tool.

> **Note:** The **`bold`** text indicates what you should enter at the prompt to display the configured `snmp-community` and `trap-receiver` elements.

The following example shows the configured snmp-community configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# snmp-community
ACMEPACKET(snmp-community)# select
<community-name>:
1: public
selection:1
```

```
ACMEPACKET(snmp-community)# show
snmp-community
   community-name                 public
   access-mode                    READ-WRITE
   ip-addresses
                                 10.0.1.27
                                 10.0.0.43
                                 10.0.1.13
   last-modified-date            2003-11-01 00:04:50
```

The following example shows the `trap-receiver` element:

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# trap-receiver
ACMEPACKET(trap-receiver)# select
<ip-address>:
1: 10.0.1.27
selection:1
ACMEPACKET(trap-receiver)# show
trap-receiver
   ip-address                    10.0.1.27
   filter-level                  All
   community-name                public
   last-modified-date            2003-11-01 00:05:12
```

For more information about the `snmp-community` or `trap-receiver` elements, refer to the *ACLI Reference Guide*.

syslog MIB Trap Examples

The Acme Packet System Management MIB trap (`apSysMgmtGroupTrap`) displays syslog severity information in the trap itself. The following section shows Acme Packet syslog MIB trap examples.

You can display the severity of the system alarm(s) that maps to Acme Packet syslog traps by executing the `display-alarms` command in the Superuser Mode of the ACLI.

> **Note:** Only system Superusers (Level 1) have access to all system commands and information pertaining to the configuration and management of the device. This mode can be password-protected in order to allow only system administrators to utilize the entire range of ACLI system commands.

Hardware Monitor Failure Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by the failure of the system's environmental sensor. This generated a Critical-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=307 bytes
IP:  D=[10.0.1.27] S=[10.0.2.233] LEN=273 ID=317
UDP: D=162 S=161  LEN=273
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 1
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 5145 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = Hardware monitor failure! Unable to monitor fan speed and
temperature!
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 50 (time ticks)
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .Ð.n ...%..p..E.
0010: 01 25 01 3d 00 00 40 11 60 88 0a 00 02 e9 0a 00 | .%.=..@.`ˆ...é..
0020: 01 1b 00 a1 00 a2 01 11 fd 08 30 82 01 05 02 01 | ...¡.¢..ý.0,....
0030: 01 04 06 70 75 62 6c 69 63 a7 81 f7 02 01 01 02 | ...public§_÷....
0040: 01 00 02 01 00 30 81 eb 30 0e 06 08 2b 06 01 02 | .....0_ë0...+...
0050: 01 01 03 00 43 02 14 19 30 1a 06 0a 2b 06 01 06 | ....C...0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 02 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 59 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0Y..+....Ç<...
00d0: 02 03 01 05 01 04 46 48 61 72 64 77 61 72 65 20 | ......FHardware
00e0: 6d 6f 6e 69 74 6f 72 20 66 61 69 6c 75 72 65 21 | monitor failure!
```

```
00f0: 20 55 6e 61 62 6c 65 20 74 6f 20 6d 6f 6e 69 74 |  Unable to monit
0100: 6f 72 20 66 61 6e 20 73 70 65 65 64 20 61 6e 64 | or fan speed and
0110: 20 74 65 6d 70 65 72 61 74 75 72 65 21 30 14 06 |  temperature!0..
0120: 0f 2b 06 01 04 01 c7 3c 03 01 01 02 03 01 06 01 | .+....Ç<........
0130: 43 01 32                                        | C.2
============SAME PACKET RECEIVED BY SNMP TEST TOOL================
Tue Nov 11 17:09:50 2003  SNMPv2c trap from [10.0.2.233]
   sysUpTime.0 :  (5145) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (2) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (Hardware monitor failure! Unable to monitor
fan speed and temperature!) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (50) type TimeStamp, indexed by
apSyslogHistIndex
```

Minor Over-Temperature Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by the Acme Packet 4250's temperature rising to between 53 °C - 63 °C. This trap generated a Minor-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=258 bytes
IP:  D=[10.0.1.27] S=[10.0.2.233] LEN=224 ID=322
UDP: D=162 S=161  LEN=224
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 1
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 5794313 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.1}
(enterprise.9148.3.1.1.2.3.1.2.1)
   SNMP: Value  = ACMEPACKET
   SNMP:
SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.1}
(enterprise.9148.3.1.1.2.3.1.3.1)
```

```
   SNMP: Value  = 4
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.1}
(enterprise.9148.3.1.1.2.3.1.4.1)
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = Temperature: 60.32 C
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 1102 (time ticks)
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .Ð.n ...%..p..E.
0010: 00 f4 01 42 00 00 40 11 60 b4 0a 00 02 e9 0a 00 | .ô.B..@.`´...é..
0020: 01 1b 00 a1 00 a2 00 e0 d0 81 30 81 d5 02 01 01 | ...¡.¢.àÐ_0_Õ...
0030: 04 06 70 75 62 6c 69 63 a7 81 c7 02 01 01 02 01 | ..public§_Ç.....
0040: 00 02 01 00 30 81 bb 30 0f 06 08 2b 06 01 02 01 | ....0_»0...+....
0050: 01 03 00 43 03 58 6a 09 30 1a 06 0a 2b 06 01 06 | ...C.Xj.0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 04 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 27 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0'..+....Ç<...
00d0: 02 03 01 05 01 04 14 54 65 6d 70 65 72 61 74 75 | .......Temperatu
00e0: 72 65 3a 20 36 30 2e 33 32 20 43 30 15 06 0f 2b | re: 60.32 C0...+
00f0: 06 01 04 01 c7 3c 03 01 01 02 03 01 06 01 43 02 | ....Ç<........C.
0100: 04 4e                                           | .N
============SAME PACKET RECEIVED BY SNMP TEST TOOL================
Wed Nov 12 10:01:40 2003  SNMPv2c trap from [10.0.2.233]
   sysUpTime.0 :  (5794313) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (4) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (Temperature: 60.32 C) type DisplayString,
indexed by apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (1102) type TimeStamp, indexed by
apSyslogHistIndex
```

Major Over-Temperature Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by the Acme Packet 4250's temperature rising to between 63 ºC - 73 ºC. This trap generated a Major-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=258 bytes
IP:  D=[10.0.1.27] S=[10.0.2.233] LEN=224 ID=323
UDP: D=162 S=161  LEN=224
SNMP: ----- Simple Network Management Protocol (Version 2) -----
      SNMP:
      SNMP: SNMP Version = 2
      SNMP: Community    = public
      SNMP: Command      = SNMPv2-trap
      SNMP: Request ID   = 2
      SNMP: Error status = 0 (No error)
      SNMP: Error index  = 0
      SNMP:
      SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
      SNMP: Value  = 5868423 hundredths of a second
      SNMP:
      SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
      SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
      SNMP:
      SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.2}
(enterprise.9148.3.1.1.2.3.1.2.2)
      SNMP: Value  = ACMEPACKET
      SNMP:
      SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.2}
(enterprise.9148.3.1.1.2.3.1.3.2)
      SNMP: Value  = 3
      SNMP:
      SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.2}
(enterprise.9148.3.1.1.2.3.1.4.2)
      SNMP: Value  = type
      SNMP:
      SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.2}
(enterprise.9148.3.1.1.2.3.1.5.2)
      SNMP: Value  = Temperature: 71.12 C
      SNMP:
      SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.2}
(enterprise.9148.3.1.1.2.3.1.6.2)
      SNMP: Value  = 1232 (time ticks)
      SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .Đ.n ...%..p..E.
0010: 00 f4 01 43 00 00 40 11 60 b3 0a 00 02 e9 0a 00 | .ô.C..@.`³...é..
0020: 01 1b 00 a1 00 a2 00 e0 ac 7d 30 81 d5 02 01 01 | ...¡.¢.à¬}0_Õ...
0030: 04 06 70 75 62 6c 69 63 a7 81 c7 02 01 02 02 01 | ..public§_Ç.....
0040: 00 02 01 00 30 81 bb 30 0f 06 08 2b 06 01 02 01 | ....0_»0...+....
```

```
0050: 01 03 00 43 03 59 8b 87 30 1a 06 0a 2b 06 01 06 | ...C.Y‹‡0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 02 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 02 02 01 03 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 02 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 27 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0'..+....Ç<...
00d0: 02 03 01 05 02 04 14 54 65 6d 70 65 72 61 74 75 | .......Temperatu
00e0: 72 65 3a 20 37 31 2e 31 32 20 43 30 15 06 0f 2b | re: 71.12 C0...+
00f0: 06 01 04 01 c7 3c 03 01 01 02 03 01 06 02 43 02 | ....Ç<........C.
0100: 04 d0                                           | .Ð
==============SAME PACKET RECEIVED SNMP TEST TOOL=================
Wed Nov 12 10:14:01 2003  SNMPv2c trap from [10.0.2.233]
   sysUpTime.0 :  (5868423) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.2 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.2 :  (3) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.2 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.2 :  (Temperature: 71.12 C) type DisplayString,
indexed by apSyslogHistIndex
   apSyslogHistTimestamp.2 :  (1232) type TimeStamp, indexed by
apSyslogHistIndex
```

Critical Over-Temperature Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by the Acme Packet 4250's temperature rising to be greater (i.e., higher) than or equal to 73 °C. This trap generated a Critical-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=258 bytes
IP:  D=[10.0.1.27] S=[10.0.2.233] LEN=224 ID=324
UDP: D=162 S=161  LEN=224
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 3
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 5872242 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.3}
(enterprise.9148.3.1.1.2.3.1.2.3)
   SNMP: Value  = ACMEPACKET
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.3}
(enterprise.9148.3.1.1.2.3.1.3.3)
   SNMP: Value  = 2
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.3}
(enterprise.9148.3.1.1.2.3.1.4.3)
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.3}
(enterprise.9148.3.1.1.2.3.1.5.3)
   SNMP: Value  = Temperature: 80.01 C
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.3}
(enterprise.9148.3.1.1.2.3.1.6.3)
   SNMP: Value  = 1325 (time ticks)
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 00 70 08 00 45 00 | .Đ.n ...%..p..E.
0010: 00 f4 01 44 00 00 40 11 60 b2 0a 00 02 e9 0a 00 | .ô.D..@.`²...é..
0020: 01 1b 00 a1 00 a2 00 e0 9c 33 30 81 d5 02 01 01 | ...¡.¢.àœ30_Õ...
0030: 04 06 70 75 62 6c 69 63 a7 81 c7 02 01 03 02 01 | ..public§_Ç.....
0040: 00 02 01 00 30 81 bb 30 0f 06 08 2b 06 01 02 01 | ....0_»0...+....
0050: 01 03 00 43 03 59 9a 72 30 1a 06 0a 2b 06 01 06 | ...C.Yšr0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 03 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 03 02 01 02 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 03 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 27 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0'..+....Ç<...
00d0: 02 03 01 05 03 04 14 54 65 6d 70 65 72 61 74 75 | .......Temperatu
00e0: 72 65 3a 20 38 30 2e 30 31 20 43 30 15 06 0f 2b | re: 80.01 C0...+
00f0: 06 01 04 01 c7 3c 03 01 01 02 03 01 06 03 43 02 | ....Ç<........C.
0100: 05 2d                                           | .-
===========SAME PACKET RECEIVED BY SNMP TEST TOOL================
Wed Nov 12 10:14:39 2003  SNMPv2c trap from [10.0.2.233]
   sysUpTime.0 :  (5872242) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.3 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.3 :  (2) type SyslogLevel, indexed by
apSyslogHistIndex
```

```
   apSyslogHistType.3 :  (type) type DisplayString, indexed by
apSyslogHistIndex

   apSyslogHistContent.3 :  (Temperature: 80.01 C) type DisplayString,
indexed by apSyslogHistIndex

   apSyslogHistTimestamp.3 :  (1325) type TimeStamp, indexed by
apSyslogHistIndex
```

Minor Fan Speed Failure Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by one fan’s speed being less than (i.e., slower than) 90%, but faster than 75% of the full fan speed. This trap generated a Minor-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=265 bytes
IP:  D=[10.0.1.27] S=[10.0.1.144] LEN=231 ID=844
UDP: D=162 S=161  LEN=231
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 86
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 355710 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.1}
(enterprise.9148.3.1.1.2.3.1.2.1)
   SNMP: Value  = ACMEPACKET
   SNMP:
SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.1}
(enterprise.9148.3.1.1.2.3.1.3.1)
   SNMP: Value  = 4
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.1}
(enterprise.9148.3.1.1.2.3.1.4.1)
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = fan speed: 8820, 8820, 7300
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 154 (time ticks)
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 07 a0 08 00 45 00 | .Ð.n ...%.. ..E.
0010: 00 fb 03 4c 00 00 40 11 5f fc 0a 00 01 90 0a 00 | .û.L..@._ü..._..
0020: 01 1b 00 a1 00 a2 00 e7 d7 5e 30 81 dc 02 01 01 | ...¡.¢.ç×^0_Ü...
0030: 04 06 70 75 62 6c 69 63 a7 81 ce 02 01 56 02 01 | ..public§_Î..V..
0040: 00 02 01 00 30 81 c2 30 0f 06 08 2b 06 01 02 01 | ....0_Â0...+....
0050: 01 03 00 43 03 05 6d 7e 30 1a 06 0a 2b 06 01 06 | ...C..m~0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 04 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 2e 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0...+....Ç<...
00d0: 02 03 01 05 01 04 1b 66 61 6e 20 73 70 65 65 64 | .......fan speed
00e0: 3a 20 38 38 32 30 2c 20 38 38 32 30 2c 20 37 33 | : 8820, 8820, 73
00f0: 30 30 30 15 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | 000...+....Ç<...
0100: 02 03 01 06 01 43 02 00 9a                      | .....C..š
===========SAME PACKET RECEIVED BY SNMP TEST TOOL=================
Tue Nov 04 10:44:49 2003  SNMPv2c trap from [10.0.1.144]
   sysUpTime.0 :  (355710) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (4) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (fan speed: 8820, 8820, 7300) type
DisplayString, indexed by apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (154) type TimeStamp, indexed by
apSyslogHistIndex
```

Major Fan Speed Failure Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by one fan's speed being slower than (less than) 75%, but faster than 50% of the full fan speed. This trap generated a Major-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=264 bytes
IP:  D=[10.0.1.27] S=[10.0.1.144] LEN=230 ID=714
UDP: D=162 S=161  LEN=230
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 78
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 245635 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.1}
(enterprise.9148.3.1.1.2.3.1.2.1)
   SNMP: Value  = ACMEPACKET
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.1}
(enterprise.9148.3.1.1.2.3.1.3.1)
   SNMP: Value  = 3
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.1}
(enterprise.9148.3.1.1.2.3.1.4.1)
   SNMP: Value  = type
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = fan speed: 8820, 8820, 5600
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 121 (time ticks)
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 07 a0 08 00 45 00 | .Đ.n ...%.. ..E.
0010: 00 fa 02 ca 00 00 40 11 60 7f 0a 00 01 90 0a 00 | .ú.Ê..@.`-..._..
0020: 01 1b 00 a1 00 a2 00 e6 25 eb 30 81 db 02 01 01 | ...¡.¢.æ%ë0_Û...
0030: 04 06 70 75 62 6c 69 63 a7 81 cd 02 01 4e 02 01 | ..public§_Í..N..
0040: 00 02 01 00 30 81 c1 30 0f 06 08 2b 06 01 02 01 | ....0_Á0...+....
0050: 01 03 00 43 03 03 bf 83 30 1a 06 0a 2b 06 01 06 | ...C..¿ƒ0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 03 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 2e 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0...+....Ç<...
00d0: 02 03 01 05 01 04 1b 66 61 6e 20 73 70 65 65 64 | .......fan speed
00e0: 3a 20 38 38 32 30 2c 20 38 38 32 30 2c 20 35 36 | : 8820, 8820, 56
00f0: 30 30 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | 000...+....Ç<...
0100: 02 03 01 06 01 43 01 79                         | .....C.y
============SAME PACKET RECEIVED BY SNMP TEST TOOL================
Tue Nov 04 10:26:29 2003  SNMPv2c trap from [10.0.1.144]
   sysUpTime.0 :  (245635) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (3) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (fan speed: 8820, 8820, 5600) type
DisplayString, indexed by apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (121) type TimeStamp, indexed by
apSyslogHistIndex
```

Critical Fan Speed Failure Trap Example

The following is an example of an `apSyslogMessageGenerated` trap caused by one fan's speed being less than (i.e., slower than) 50% of the full fan speed. This trap generated a Critical-level alarm.

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=262 bytes
IP:  D=[10.0.1.27] S=[10.0.1.144] LEN=228 ID=703
UDP: D=162 S=161  LEN=228
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 70
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 241607 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.1.2.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.2.1}
(enterprise.9148.3.1.1.2.3.1.2.1)
   SNMP: Value  = ACMEPACKET
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.3.1}
(enterprise.9148.3.1.1.2.3.1.3.1)
   SNMP: Value  = 2
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.4.1}
(enterprise.9148.3.1.1.2.3.1.4.1)
   SNMP: Value  = type
   SNMP:
```

```
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.5.1}
(enterprise.9148.3.1.1.2.3.1.5.1)
   SNMP: Value  = fan speed: 8820, 8820, 60
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.1.1.2.3.1.6.1}
(enterprise.9148.3.1.1.2.3.1.6.1)
   SNMP: Value  = 101 (time ticks)
   SNMP:
ADDR  HEX                                                ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 07 a0 08 00 45 00 | .Đ.n ...%.. ..E.
0010: 00 f8 02 bf 00 00 40 11 60 8c 0a 00 01 90 0a 00 | .ø.¿..@.`Œ..._..
0020: 01 1b 00 a1 00 a2 00 e4 6d ff 30 81 d9 02 01 01 | ...¡.¢.ämÿ0_Ù...
0030: 04 06 70 75 62 6c 69 63 a7 81 cb 02 01 46 02 01 | ..public§_Ë..F..
0040: 00 02 01 00 30 81 bf 30 0f 06 08 2b 06 01 02 01 | ....0_¿0...+....
0050: 01 03 00 43 03 03 af c7 30 1a 06 0a 2b 06 01 06 | ...C..¯Ç0...+...
0060: 03 01 01 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 | ........+....Ç<.
0070: 01 02 00 01 30 1d 06 0f 2b 06 01 04 01 c7 3c 03 | ....0...+....Ç<.
0080: 01 01 02 03 01 02 01 04 0a 61 63 6d 65 73 79 73 | .........acmesys
0090: 74 65 6d 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 | tem0...+....Ç<..
00a0: 01 02 03 01 03 01 02 01 02 30 17 06 0f 2b 06 01 | .........0...+..
00b0: 04 01 c7 3c 03 01 01 02 03 01 04 01 04 04 74 79 | ..Ç<..........ty
00c0: 70 65 30 2c 06 0f 2b 06 01 04 01 c7 3c 03 01 01 | pe0,..+....Ç<...
00d0: 02 03 01 05 01 04 19 66 61 6e 20 73 70 65 65 64 | .......fan speed
00e0: 3a 20 38 38 32 30 2c 20 38 38 32 30 2c 20 36 30 | : 8820, 8820, 60
00f0: 30 14 06 0f 2b 06 01 04 01 c7 3c 03 01 01 02 03 | 0...+....Ç<.....
0100: 01 06 01 43 01 65                               | ...C.e
============SAME PACKET RECEIVED BY SNMP TEST TOOL================
Tue Nov 04 10:25:48 2003  SNMPv2c trap from [10.0.1.144]
   sysUpTime.0 :  (241607) type TimeTicks
   snmpTrapOID.0 : apSyslogMessageGenerated (1.3.6.1.4.1.9148.3.1.2.0.1)
type ObjectID
   apSyslogHistFrom.1 :  (ACMEPACKET) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistLevel.1 :  (2) type SyslogLevel, indexed by
apSyslogHistIndex
   apSyslogHistType.1 :  (type) type DisplayString, indexed by
apSyslogHistIndex
   apSyslogHistContent.1 :  (fan speed: 8820, 8820, 60) type DisplayString,
indexed by apSyslogHistIndex
   apSyslogHistTimestamp.1 :  (101) type TimeStamp, indexed by
apSyslogHistIndex
```

System Management MIB Trap Example

Execute the `display-alarms` command in the Superuser Mode of the ACLI to display the severity of the system alarm(s) that maps to Acme Packet System Management traps. The following section shows Acme Packet System Management MIB trap example.

CPU Usage Over-Threshold Trap Example

The following is an example of an `apSysMgmtGroupTrap` trap caused by CPU usage exceeding the threshold value (i.e., the system's CPU usage reached 90% or greater of its capacity). This trap output is similar to that of other System Management MIB traps (e.g., memory utilization, health score, NAT table utilization, and ARP table utilization).

```
==============PACKET CAPTURED================
DLC: Ethertype=0800, size=161 bytes
IP:  D=[10.0.1.27] S=[10.0.1.144] LEN=127 ID=686
UDP: D=162 S=161  LEN=127
SNMP: ----- Simple Network Management Protocol (Version 2) -----
   SNMP:
   SNMP: SNMP Version = 2
   SNMP: Community    = public
   SNMP: Command      = SNMPv2-trap
   SNMP: Request ID   = 62
   SNMP: Error status = 0 (No error)
   SNMP: Error index  = 0
   SNMP:
   SNMP: Object = {1.3.6.1.2.1.1.3.0} (sysUpTime.0)
   SNMP: Value  = 236161 hundredths of a second
   SNMP:
   SNMP: Object = {1.3.6.1.6.3.1.1.4.1.0} (internet.6.3.1.1.4.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.2.3.0.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.2.2.1.0} (enterprise.9148.3.2.2.1.0)
   SNMP: Value  = {1.3.6.1.4.1.9148.3.2.1.1.1}
   SNMP:
   SNMP: Object = {1.3.6.1.4.1.9148.3.2.2.2.0} (enterprise.9148.3.2.2.2.0)
   SNMP: Value  = 96
   SNMP:
ADDR  HEX                                               ASCII
0000: 00 d0 09 6e a0 0c 00 08 25 01 07 a0 08 00 45 00 | .Đ.n ...%.. ..E.
0010: 00 93 02 ae 00 00 40 11 61 02 0a 00 01 90 0a 00 | .“.®..@.a...._..
0020: 01 1b 00 a1 00 a2 00 7f 9f 62 30 75 02 01 01 04 | ...¡.¢.-Ÿb0u....
0030: 06 70 75 62 6c 69 63 a7 68 02 01 3e 02 01 00 02 | .public§h..>....
0040: 01 00 30 5d 30 0f 06 08 2b 06 01 02 01 01 03 00 | ..0]0...+.......
0050: 43 03 03 9a 81 30 1a 06 0a 2b 06 01 06 03 01 01 | C..š_0...+......
0060: 04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 02 03 00 | .....+....Ç<....
0070: 01 30 1b 06 0c 2b 06 01 04 01 c7 3c 03 02 02 01 | .0...+....Ç<....
0080: 00 06 0b 2b 06 01 04 01 c7 3c 03 02 01 01 30 11 | ...+....Ç<....0.
0090: 06 0c 2b 06 01 04 01 c7 3c 03 02 02 02 00 02 01 | ..+....Ç<.......
00a0: 60                                              | `
```

```
===========SAME PACKET RECEIVED BY SNMP TEST TOOL================
Tue Nov 04 10:24:54 2003  SNMPv2c trap from [10.0.1.144]
   sysUpTime.0 :  (236161) type TimeTicks
   snmpTrapOID.0 : apSysMgmtGroupTrap (1.3.6.1.4.1.9148.3.2.3.0.1) type
ObjectID
   apSysMgmtTrapType.0 : apSysCPUUtil (1.3.6.1.4.1.9148.3.2.1.1.1) type
ObjectID
   apSysMgmtTrapValue.0 :  (96) type Integer32
```

Environmental Monitor MIB Trap Example

Execute the `display-alarms` command in the Superuser Mode of the ACLI to display the severity of the system alarm(s) that maps to Acme Packet Environmental Monitor traps. The following section shows an Acme Packet Environmental Monitor MIB trap example.

Voltage Trap Example

The following example shows the apEnvMonStatusChangeNotification trap for voltage state change from init to unknown.

```
No.    Time        Source              Destination          Protocol Info
    47 4.963457    172.30.55.127       10.0.200.61          SNMP     TRAP-V2
iso.3.6.1.2.1.1.3.0 iso.3.6.1.6.3.1.1.4.1.0 iso.3.6.1.4.1.9148.3.3.3.1.0
iso.3.6.1.4.1.9148.3.3.3.2.0 iso.3.6.1.4.1.9148.3.3.3.3.0


Frame 47 (184 bytes on wire, 184 bytes captured)
   Arrival Time: Jan 18, 2006 14:27:46.746685000
   Time delta from previous packet: 0.000118000 seconds
   Time since reference or first frame: 4.963457000 seconds
   Frame Number: 47
   Packet Length: 184 bytes
   Capture Length: 184 bytes
Ethernet II, Src: 00:0f:23:4a:d8:80, Dst: 00:a0:cc:e1:1e:ec
   Destination: 00:a0:cc:e1:1e:ec (10.0.200.61)
   Source: 00:0f:23:4a:d8:80 (10.0.0.1)
   Type: IP (0x0800)
Internet Protocol, Src Addr: 172.30.55.127 (172.30.55.127), Dst Addr: 10.0.200.61
(10.0.200.61)
   Version: 4
   Header length: 20 bytes
   Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
   Total Length: 170
   Identification: 0x02b7 (695)
   Flags: 0x00
   Fragment offset: 0
   Time to live: 63
   Protocol: UDP (0x11)
   Header checksum: 0xc2b1 (correct)
   Source: 172.30.55.127 (172.30.55.127)
   Destination: 10.0.200.61 (10.0.200.61)
User Datagram Protocol, Src Port: snmp (161), Dst Port: snmptrap (162)
```

```
    Source port: snmp (161)
    Destination port: snmptrap (162)
    Length: 150
    Checksum: 0x10cc (correct)
Simple Network Management Protocol
    Version: 2C (1)
    Community: public
    PDU type: TRAP-V2 (7)
    Request Id: 0x0000000b
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.3.0 (iso.3.6.1.2.1.1.3.0)(sysUpTime)
    Value: Timeticks: (3915) 0:00:39.15
    Object identifier 2: 1.3.6.1.6.3.1.1.4.1.0 (iso.3.6.1.6.3.1.1.4.1.0) (snmpTrapOID)
    Value: OID: iso.3.6.1.4.1.9148.3.3.4.0.2 (apEnvMonStatusChangeNotification)
    Object identifier 3: 1.3.6.1.4.1.9148.3.3.3.1.0
(iso.3.6.1.4.1.9148.3.3.3.1.0)(apEnvMonTrapInstance)
   Value: OID: iso.3.6.1.4.1.9148.3.3.1.2.1.1.1.2 (apEnvMonVoltageStatusIndex.2, which
is v3p3 (3.3v voltage) )
    Object identifier 4: 1.3.6.1.4.1.9148.3.3.3.2.0 (iso.3.6.1.4.1.9148.3.3.3.2.0)
(apEnvMonTrapPreviousState)
    Value: INTEGER: 1 (initial, detail in TEXTUAL-CONVENTION of ApEnvMonState)
    Object identifier 5: 1.3.6.1.4.1.9148.3.3.3.3.0 (iso.3.6.1.4.1.9148.3.3.3.3.0)
(apEnvMonTrapCurrentState)
    Value: INTEGER: 9 (unknown, detail in TEXTUAL-CONVENTION of ApEnvMonState)
```

Raw packet:

```
0000  00 a0 cc e1 1e ec 00 0f 23 4a d8 80 08 00 45 00   ........#J....E.
0010  00 aa 02 b7 00 00 3f 11 c2 b1 ac 1e 37 7f 0a 00   ......?.....7...
0020  c8 3d 00 a1 00 a2 00 96 10 cc 30 81 8b 02 01 01   .=........0.....
0030  04 06 70 75 62 6c 69 63 a7 7e 02 01 0b 02 01 00   ..public.~......
0040  02 01 00 30 73 30 0e 06 08 2b 06 01 02 01 01 03   ...0s0...+......
0050  00 43 02 0f 4b 30 1a 06 0a 2b 06 01 06 03 01 01   .C..K0...+......
0060  04 01 00 06 0c 2b 06 01 04 01 c7 3c 03 03 04 00   .....+.....<....
0070  02 30 1f 06 0c 2b 06 01 04 01 c7 3c 03 03 03 01   .0...+.....<....
0080  00 06 0f 2b 06 01 04 01 c7 3c 03 03 01 02 01 01   ...+.....<......
0090  01 02 30 11 06 0c 2b 06 01 04 01 c7 3c 03 03 03   ..0...+.....<...
00a0  02 00 02 01 01 30 11 06 0c 2b 06 01 04 01 c7 3c   .....0...+.....<
00b0  03 03 03 03 00 02 01 09                           ........
```

B References

Overview

This following table lists the topic and the Internet Engineering Task Force Request for Comments (IETF RFC) document where you can obtain more information.

Topic	More Information
SNMPv2c **Trap criteria** coldStart Trap authenticationFailure Trap	IETF RFC 1907, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)." (http://www.ietf.org/rfc/rfc1907.txt)
MIBs	IETF RFC 1213, "Management Information Base for Network Management of TCP/IP-based Internets: MIB-II." (http://www.ietf.org/rfc/rfc1213.txt)
MIB-II **Trap criteria** linkUp Trap linkDown Trap	IETF RFC 2233, "Interfaces Group MIB using SMIv2." http://www.ietf.org/rfc/rfc2233.txt
University of California Berkeley Software Distribution (BSD) syslog severities	IETF RFC 3164 "The BSD syslog Protocol." (http://www.ietf.org/rfc/rfc3164.txt),
IP datagram reassembly algorithms	RFC 815 "IP Datagram Reassembly Algorithms" (http://www.ietf.org/rfc/rfc0815.txt),
LBOUND quantity UBOUND quantity Deleting the TCB	IETF RFC 793 "TRANSMISSION CONTROL PROTOCOL, DARPA INTERNET PROGRAM, PROTOCOL SPECIFICATION" (http://www.ietf.org/rfc/rfc0793.txt.)