Net-Net® 9000 MIB Reference Guide Release Version S-D7.1.0

Acme Packet, Inc.
100 Crosby Drive
Bedford, MA 01730
t 781-328-4400
f 781-275-8800
www.acmepacket.com

Last Updated: March 6, 2013
Document Number: 400-0077-71 Rev. 1.12

Notices

©2012 Acme Packet®, Inc., Bedford, Massachusetts. All rights reserved. Acme Packet®, Session Aware Networking, Net-Net®, and related marks are registered trademarks of Acme Packet, Inc. All other brand names are trademarks, registered trademarks, or service marks of their respective companies or organizations.

Patents Pending, Acme Packet, Inc.

The Acme Packet Documentation Set and the Net-Net systems described therein are the property of Acme Packet, Inc. This documentation is provided for informational use only, and the information contained within the documentation is subject to change without notice.

Acme Packet, Inc. shall not be liable for any loss of profits, loss of use, loss of data, interruption of business, nor for indirect, special, incidental, consequential, or exemplary damages of any kind, arising in any way in connection with the Acme Packet software or hardware, third party software or hardware, or the documentation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusions may not apply. These limitations are independent from all other provisions and shall apply notwithstanding the failure of any remedy provided herein.

Copying or reproducing the information contained within this documentation without the express written permission of Acme Packet, Inc., 100 Crosby Drive, Bedford MA 01730, USA is prohibited. No part may be reproduced or retransmitted.

Acme Packet Net-Net products are protected by one or more of the following patents: United States: 7072303, 7028092, 7002973, 7133923, 7031311, 7142532, 7151781. France: 1342348, 1289225, 1280297, 1341345, 1347621. Germany: 1342348, 1289225, 1280297, 1341345, 1347621. United Kingdom: 1342348, 1289225, 1280297, 1341345, 1347621. Other patents are pending.

Contents

About this Guide vii

Overview vii
About Net-Net Platforms vii
Acme Packet Platform sysObjectIDs vii
Documented Objects and Traps. viii
Who is Acme Packet? viii
Summary of Changes for Release S-D7.1.0 ix
Summary of Changes ix
Trap Event Monitoring ix
H.323 Stack Monitoring ix
Storage Space. ix
Network Management Control State ix
Policy Server Connection ix
Technical Assistance x
Customer Questions, Comments, or Suggestions x
Contact Us x
Revision History x

Acme Packet MIBs 11

Overview 11
About MIBs 11
Object Identifiers 11
Instance IDs 11
MIB Tree Structure 12
About Managed Objects 13
Scalar MIB Objects 13
Table MIB Objects 13
About SNMP Traps 13
MIBs Supported by Acme Packet 14
Standard MIBS. 14
Acme Packet Enterprise MIBs 14
Traps. 16
Standard Traps. 16
Enterprise Traps. 17
Alarms 21

Alarm Severity Levels 22
Alarm Descriptions 22
Hardware Alarms 22
I2C Hardware Alarms 23
Card Presence Alarms 23
I2C Alarm Types 23
I2C Link and Temperature Alarms 25
Voltage Alarms 25
Specific Card Alarms 26
System Alarms 27
NIU Link Alarms 27
MIU Link Alarms 27
NPU Link Alarms 28
TCU Link Alarms 29
Utilization Alarms 29
Health Score Alarms 30
Redundancy Alarms 30
System Task Alarms 31
System State Alarms 31
System Miscellaneous Alarms 32
Switch Alarms 32
NPU Switch 32
SPU Switch 33
Network Alarms 33
Media Alarms 33
Application Alarms 34
RADIUS Connection Down Alarm 34
Application Alarms 34
Configuration Alarms 35
Displaying and Clearing Alarms 35
Acme Packet Log Levels and syslog Level Severities 36
Acme Packet Log Levels 36
syslog Level Severities 37

Standard SNMP OIDs 39

Introduction 39
Platform Group 39
Interfaces Group 39
Interface Scalar Example 41
Interface Table Examples 41
ifXTable Support 42
Examples of ifIndex Values 43

IP Group 44
IP Scalar Example 46
IP Address Table Example 47
ICMP Group 48
ICMP Scalar Example 49
TCP Group 50
TCP Scalar Example 52
TCP Connection Table Example 52
UDP Group 53
UDP Scalar Example 53
UDP Table Example 54
System Group 54
System Scalar Example 55
Object Resource Information 56
SysORTableTable Examples 56
SNMP Group 57
SNMP Scalar Example 58
Physical Entity Table (rfc2737.mib) 59
entPhysicalTable Example 63
entity Physical Table Scalar Example 64

Enterprise SNMP OIDs 65

Introduction 65
Acme Packet System Management MIB (ap-smgmt.mib) 65
System Management Scalar Examples 73
Session Statistical Group Table Examples 74
SIP Session Agent Statistics Table Example 75
Signaling Realm Statistics Table Example 76
Acme Packet License MIB (ap-license.mib) 77
License Table Examples 78
Acme Packet Software Inventory MIB (ap-swinventory.mib) 79
Configuration Scalar Example 79
Software Image Table Examples 80
Backup Configuration Table Example 80
Acme Packet Environment Monitor MIB (ap-env-monitor.mib) 81
I2C State Scalar Examples 85
Voltage Status Table Examples 85
Temperature Status Table Examples 86
Fan Status Table Examples 86

Power Supply Status Table Examples 86
Physical Layer Card Status Table Examples 87
Acme Packet Syslog MIB (ap-slog.mib) 87
Acme Packet Codec and Transcoding MIB (ap-codec.mib) 89
Acme Packet H.323 MIB (ap-h323.mib) 90

About this Guide

Overview

The *Net-Net MIB Reference Guide* provides information about the following:

- 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 Net-Net® system alarms and the MIBs that support traps, and it provides reference information about Acme Packet log levels, and syslog level severities (the protocol used for the network logging of system and network events). Appendix A contains several trap examples.

About Net-Net Platforms

This guide supports the Net-Net 9000 series platforms. Acme Packet's Net-Net family of products also includes the Net-Net 4000 series, the Net-Net 3000 series and the Net-Net 2000 series. The 4000 series contains two systems: the Net-Net 4250 and the Net-Net 4500. The Net-Net 3000 series contains two systems: the Net-Net 3800 (Sku 3810) and the Net-Net 3820.

Acme Packet Platform sysObjectIDs

Each hardware platform in the Net-Net 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 Net-Net platforms and their corresponding sysDescr values. **X** stands for a string value of the software version, such as D7.0.0m3.

Platform	sysObjectID Object Identifier Name: Number	sysDescr
Net-Net 4250	`apNetNet4250:` `1.3.6.1.4.1.9148.1.1.1`	Acme Packet Net-Net 4000 Series SBC X
Net-Net 4500	`apNetNet4500:` `1.3.6.1.4.1.9148.1.1.2`	Acme Packet Net-Net 4500 X

Platform	sysObjectID Object Identifier Name: Number	sysDescr
Net-Net 3800 (Sku 3810)	`apNetNet3800:` `1.3.6.1.4.1.9148.1.3.1`	Acme Packet Net-Net 3800 X
Net-Net 3820	`apNetNet3820:` `1.3.6.1.4.1.9148.1.3.2`	Acme Packet Net-Net 3820 X
Net-Net 9200	`apNetNet9200:` `1.3.6.1.4.1.9148.1.2.1`	Acme Packet Net-Net 9200 X

Documented Objects and Traps

This *Net-Net MIB Reference Guide* only documents the traps and objects supported in the release version D7.1.0 for the 9000 platform. Acme Packet enterprise MIBs, however, can contain additional traps and objects not documented here.

Enterprise MIB files are global across all Net-Net session border controllers. Each MIB contains a superset of objects and traps for all Net-Net SBC:

- 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 version D7.2.0.

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 the 9000
- 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.

Who is Acme Packet?

Acme Packet enables service providers to deliver trusted, first class interactive communications—voice, video and multimedia sessions—across IP network borders. Our Net-Net family of session border controllers satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks. Our deployments support multiple applications—from VoIP trunking to hosted enterprise and residential services; multiple protocols—SIP, H.323, MGCP/NCS and H.248; and multiple border points—interconnect, access network and data center.

Established in August 2000 by networking industry veterans, Acme Packet is a public company trading on the NASDAQ and headquartered in Bedford, Massachusetts.

Summary of Changes for Release S-D7.1.0

Summary of Changes

This section provides a brief summary of changes to this document for release S-D7.1.0.

Trap Event Monitoring

New objects and traps added for recording trap information for any condition that triggers an alarm:

- `apTrapTableNumVariables`: The amount of details recorded for the trap.
- `apTrapTableSysUptime`: SNMP sysUpTime when the trap was generated.
- `apTrapInformationTableDataType`: SNMP type enumerated encoded in the trap.
- `apTrapInformationTableDataLength`: The octet length of the information encoded in the trap.
- `apTrapTableDataOctets`: The information represented in octets.

H.323 Stack Monitoring

New objects and traps added for monitoring for H.323 stacks:

- `apH323StackName`: Configured H.323 stack name
- `apH323StackCurrentCalls`: Number of current calls
- `apH323StackMaxCallThresholdTrap`: Generated when the number of H.323 calls increases percentage of the max-calls threshold
- `apH323StackMaxCallThresholdClearTrap`: Generated when the number of H.323 calls decreases to below the lowest max-calls theshold

Storage Space

New objects and traps added to monitor storage space.

- `apSysVolumeIndex`: Monotonically increasing integer for the purpose of indexing volumes
- `apSysVolumeName`: Name of the volume
- `apSysVolumeTotalSpace`: Total size of the volume in MB
- `apSysVolumeAvailableSpace`: Total space available on the volume in MB
- `apSysMgmtSpaceAvailThresholdTrap`: Generated when the space available on a partition crosses a configured space threshold
- `apSysMgmtSpaceAvailThresholdClearTrap`: Generated when the space available on a partition falls below the lowest configured threshold

Network Management Control State

New objects added to determine if a particular network management control is enabled or disabled.

- `apNetMgmtCtrlStatsState`: Collection of statistics reflecting the state of network management controls.

Policy Server Connection

New traps added for notification of policy server connection:

- `apSysMgmtExtPolicyServerConnDownTrap`: Generated when the SBC is unable to connect to an external policy server.

- `apSysMgmtExtPolicyServerConnEstTrap`: Generated when the SBC is able to re-establish a connection with an external policy server.

•Technical Assistance

If you need technical assistance with Acme Packet products, you can obtain it on-line by going to https://support.acmepacket.com. With your customer identification number and password, you can access Acme Packet's on-line resources 24 hours a day. If you do not have the information required to access the site, send an email to tac@acmepacket.com requesting a login.

In the event that you are experiencing a critical service outage and require live assistance, you can contact the Acme Packet Technical Assistance Center emergency hotline:

- From the United States, Canada, and Mexico call: 1 866 226 3758
- From all other locations, call: +1 781 756 6920

Please note that a valid support/service contract with Acme Packet is required to obtain technical assistance.

Customer Questions, Comments, or Suggestions

Acme Packet is committed to providing our customers with reliable documentation. If you have any questions, comments, or suggestions regarding our documentation, please contact your Acme Packet customer support representative directly or email support@acmepacket.com.

Contact Us

Acme Packet
100 Crosby Drive
Bedford, MA 01730 USA
t 781-328-4400
f 781-275-8800
www.acmepacket.com

Revision History

This section contains a revision history for this document.

Date	Revision Number	Description
December 1, 2010	Revision 1.01	• Removed unsupported trap-receiver filter functionality
April 30, 2012	Revision 1.10	• Corrected object name and OID number for apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1. • Added apEnvMonCpuCoreIndex to the apEnvMonCpuCoreEntry table. • Added note to the description for apSysMgmtSingleUnitRedundancyTrap • For apSigRealmStatsTotalSessionsOutbound and apSigRealmStatsTotalSessionsInbound, removed "during 100 second sliding window period" from the description.

Date	Revision Number	Description
January 24, 2013	Revision 1.11	• Removed appendix A
March 6, 2013	Revision 1.12	• Indicated that the apEnvMonPortChangeNotification trap is not supported on the 9000 platform.

1 Acme Packet MIBs

Overview

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

About MIBs

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

A 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, 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).38

Object Identifiers

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). 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 uniquely identifies the object. 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.

Instance IDs

An instance ID identifies specific instances of a given managed object 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
```

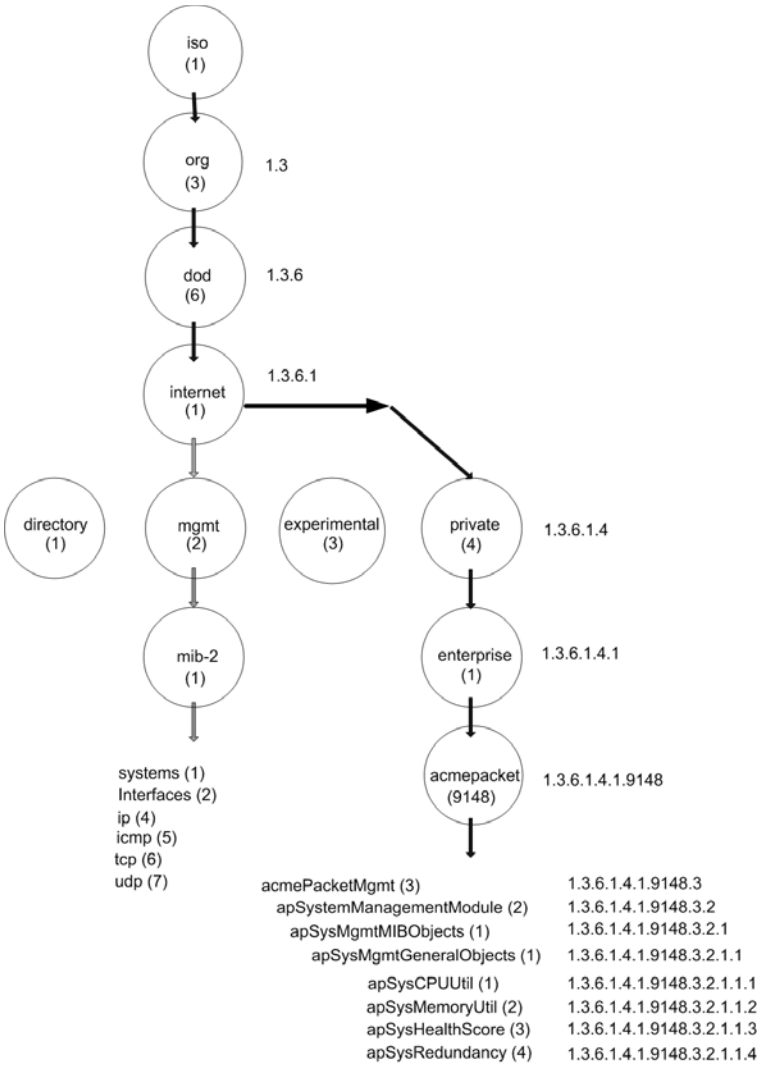
- `tcpConnState` is the OID
- `127.0.0.1` is an IPv4 address
- `1024` is the port number
- `127.0.0.1` is another IPv4 address
- `3000` is another port number

Together these make up the index for this table. The components that make-up the index are part of the definitions of any MIB table.

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 node has the value 9148. 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. The operator merely has to know the name of the object and no other information. Discrete objects often represent summary values for a device, good performance information is maintained in the tables too. 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 require a `.` (dot) extension to their names that uniquely distinguishes the particular value being referenced. The `.` (dot) extension is also referred to as the *instance* number of an SNMP object. For table objects, this instance number is the index into the SNMP table. (For scalar objects, this instance number is zero.)

SNMP tables allow parallel information to be supported. Unlike scalar objects, 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. Because 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.

MIBs Supported by Acme Packet

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

Standard MIBS

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 with 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:

- rfc1907-snmpv2.mib
- rfc2011-ip.mib
- rfc2737-entity.mib
- rfc2863-if.mib (Acme Packet supports the ifName and ifConnectorPresent entries of the ifXTable, which is an extension to the interface table and which replaces ifExtnsTable. See RFC 2863 for details.)
- rfc3411-framework.mib
- rfc4001-inetAddr.mib
- rfc4022-tcp.mib
- rfc4113-udp.mib
- ianaiftype.mib

Acme Packet Enterprise MIBs

Acme Packet provides the following enterprise MIBs:

MIB Name	Description
ap-agentcapability.mib	The Acme Packet Agent Capability MIB details the SNMP agent's capabilities that includes support for four 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. • **System management capabilities** include support for the contents of the Acme Packet System Management MIB (ap-smgmt.mib).
ap-ami.mib	Provides the means to gather information about the Acme Packet management interface on the Net-Net SBC.

MIB Name	Description
ap-codec.mib	Provides a means to gather codec and transcoding information generated by Acme Packet systems.
ap-ems.mib	Provides a means to gather information on the Net-Net EMS.
ap-entity-vendortype.mib	The Acme Packet Entity Vendor Type MIB provides Acme Packet OID assignments for Acme Packet hardware components.
ap-env-monitor.mib	The Acme Packet Environmental Monitor MIB gathers information about fan speed, voltage, temperature, and power supply for the Net-Net system. It also sends out traps when status changes occur.
ap-license.mib	The Acme Packet License MIB provides information about the status of your Net-Net licenses.
ap-products.mib	The Acme Packet Products MIB contains descriptions of the different Net-Net SD versions.
ap-security.mib	Provides a meansto gather security information on the Net-Net SBC.
ap-slog.mib	Provides the means to gather syslog messages generated by the Acme Packet session and media routers.
ap-smgmt.mib	The Acme Packet System Management MIB provides a means of gathering information about the status of the Net-Net system (for example, system memory or system health).
ap-smi.mib	Acme Packet Structured Management Information (SMI) MIB provides general information about the top level of Acme Packet enterprise MIBs.
ap-swinventory.mib	The Acme Packet Software Inventory MIB provides a means of gathering information about the status of the boot images, configuration information, and bootloader images for the Net-Net system.
ap-tc.mib	Provides textual conventions used in Acme Packet enterprise MIBs.

Traps

This section defines the standard and proprietary traps supported by the Net-Net system. A trap is initiated by tasks (such as the `sipd task`) to report that an event has happened on the Net-Net system. SNMP traps enable an SNMP agent to notify the NMS of significant events by way of an unsolicited SNMP message.

Acme Packet uses SNMPv2c. These notification definitions are used to send standard traps and Acme Packet'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 Net-Net system supports.

Trap Name	Description
linkUp	The SNMP agent detects that the ifOperStatus object for one of its communication links transitioned from the down state to another state (excluding the notPresent state). This other state is indicated by the included value of ifOperStatus. linkUp applies to PHY interfaces and control interfaces in MIU cards.
linkDown	The SNMP agent detects that the ifOperStatus object for one of its communication links is about to enter the down state from another state (excluding the notPresent state). This other state is indicated by the included value of ifOperStatus. Possible linkDown situations are: • ifAdminStatus is up and ifOperstatus goes from up to down. • ifOperStatus is up and ifAdminStatus goes from up to down. linkDown applies to PHY interfaces and control interfaces in MIU cards
coldStart	The SNMP agent is reinitializing itself and its configuration might have been altered. coldStart applies to SPU and Net-Net SD restarts. This trap is not associated with a Net-Net system alarm.

Trap Name	Description
authenticationFailure	The SNMP agent received a protocol message that was not properly authenticated. The snmpEnableAuthenTraps object indicates whether this trap will be generated. • ACLI: Set the system-config element's snmp-enabled and enable-snmp-auth-traps parameters to enabled. A snmpEnableAuthenTraps object is generated. • Net-Net EMS: Choose enabled from the State drop-down list and choose enabled from the Authentication traps drop-down list; both located on the General tab, accessed from the Management tab. This trap is not associated with a Net-Net system alarm.
entConfigChange	This trap is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls. An agent should not generate more than one entConfigChange 'notification-event' in a given time interval (five seconds is the suggested default). A 'notification-event' is the transmission of a single trap or inform PDU to a list of notification destinations. If additional configuration changes occur within the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away. An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events, e.g., due to throttling or transmission loss.

Enterprise Traps

The following table identifies the proprietary traps that Net-Net system supports.

Trap Name: OID Number	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	The 9000 platform does not support this trap.
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.
apEnvMonTempChangeNotification: 1.3.6.1.4.1.9148.3.3.4.0.3	Sent when a unit crosses a temperature threshold.
apEnvMonVoltageChangeNotification: 1.3.6.1.4.1.9148.3.3.4.0.4	Sent when a unit crosses a voltage threshold.

Trap Name: OID Number	Description
apH323StackMaxCallThresholdTrap 1.3.6.1.4.1.9148.3.10.3.0.1	Generated when the number of H.323 calls increases the percentage of the max calls threshold.
apH323StackMaxCallThresholdClearTrap 1.3.6.1.4.1.9148.3.10.3.0.2	Generated when the number of H.323 calls decreases to below the lowest max calls theshold.
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.
apSyslogMessageGenerated: 1.3.6.1.4.1.9148.3.1.2.0.1	Generated by a syslog/alarms event. Also if snmp-monotr and envmonitor are disabled, you received syslogMessage traps.
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 if the CPU utilization percentage of application tasks has fallen below the threshold algd-load-limit.
apSysMgmtAuthenticationFailedTrap: 1.3.6.1.4.1.9148.3.2.6.0.16	Generated when an attempt to login to the Net-Net SD through Telne, FTP, SFTP, SSH or by using the console fails for any reason. The trap sent to all configured trap FTP receivers includes the following information: • administration and access level (SSH, user, enable) • connection type (Telnet or console)
apSysMgmtCDRPushReceiverFailureTrap: 1.3.6.1.4.1.9148.3.2.6.0.53	Generated when an enabled CDR push receiver fails
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 occured on all 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 completes a push operation successfully. The trap contains the name of the node that generated the trap, the unique name for the file (fileID) that was transferred, and the IP address of the push receive to which the file was transferred.
apSysMgmtDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.1	Generated when the IP address and the realm ID is denied of service.
apSysMgmtExpDOSTrap: 1.3.6.1.4.1.9148.3.2.8.0.2	Gnerated when an IP address is placed on a deny list due to denial-of-service attempts. It provides: • IP address that has been demoted • realm of that IP address • URI portion of the SIP FROM header of the message that caused the demotion (if available).
apSysMgmtENUMStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.27	Generated if the reachability status of an ENUM server changes.
apSysMgmtFanTrap: 1.3.6.1.4.1.9148.3.2.6.0.3	Generated if a fan unit speed falls below the monitoring threshold.
apSysMgmtGatewayUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.10	Generated if the gateway specified becomes unreachable by the system.

Trap Name: OID Number	Description
apSysMgmtGatewayUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.21	Generated when the Net-Net 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 Net-Net 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 Net-Net peers only) falls below 60, the apSysMgmtGroupTrap is generated.
apSysMgmtGroupClearTrap: 1.3.6.1.4.1.9148.3.2.3.0.2	Generated when the Net-Net SBC's system resource use or its health score returns to levels that are within thresholds. For example, NAT table usage or memory usage could return to acceptable levels, and the systems health score could return to a level above 60.
apSysMgmntH248AssociationLostTrap: 1.3.6.1.4.1.9148.3.2.6.0.35	Generated when an H248 control association between a border gateway and session controller is lost. The included object is the border gateway identifier.
apSysMgmntH248AssociationLostClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.36	Generated when an H248 control association between a border gateway and session controller has been restoredt. The included object is the border gateway identifier.
apSysMgmtH323InitFailTrap: 1.3.6.1.4.1.9148.3.2.6.0.12	Generated if the H.323 stack has failed to initialize properly and has been terminated.
apSysMgmtHardwareErrorTrap: 1.3.6.1.4.1.9148.3.2.6.0.14	Provides a text string indicating the type of hardware error that has occurred. If the message text exceeds 255 bytes, the message is truncated to 255 bytes.
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.
apSysMgmtLDAPStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.42	Generated if the reachability status of an LDAP server 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. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
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.
apSysMgmtMediaOutOfMemoryClear: 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. Trap is generated when there are at least 5 failures within a 30 second window and a failure rate of 5% or more.
apSysMgmtMediaPortsClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.18	Generated when the rate of allocating media ports decreases to a level within thresholds.
apSysMgmtMediaSupervisionTimerExpTrap: 1.3.6.1.4.1.9148.3.2.6.0.34	Genrated when a media supervision timer has expired. This behavior is disabled by default but may be enabled by changing the media-supervision-traps parameter of the media-manager configuration element. The included object is the call identifier for the call which had the timer expire.
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 NTP has to adjust the clock by more than 1000 seconds.

Trap Name: OID Number	Description
apSysMgmtNTPServerUnreachableTrap: 1.3.6.1.4.1.9148.3.2.6.0.30	Generated if the server specified becomes unreachable by the NTP process.
apSysMgmtNTPServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.31	Generated if the server specified was unreachable by the NTP process and now is reachable.
apSysMgmtNTPServiceDownTrap: 1.3.6.1.4.1.9148.3.2.6.0.32	Generated if all servers specified are unreachable by the NTP process.
apSysMgmtNTPServiceDownClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.33	Generated if all servers specified are unreachable by the NTP process
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 server specified becomes unreachable by the system collector.
apSysMgmtPushServerUnreachableClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.29	Generated if the server specified becomes unreachable by the system collector.
apSysMgmtRFactorBelowThresholdTrap: 1.3.6.1.4.1.9148.3.2.6.0.37	Generated when a call using the vq-qos statistics has gone below a configured threshold. The included objects are the RFactor value and a call identifier.
apSysMgmtRFactorBelowThresholdClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.38	Generated when a call using the vq-qos statistics gathering function has recovered after going below a configured threshold. The included objects are the RFactor value and a call identifier.
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.
apSysMgmtRealmMinutesExceedTrap: 1.3.6.1.4.1.9148.3.2.6.0.40	Generated if monthly minutes exceed for a realm.
apSysMgmtRealmMinutesExceedClearTrap: 1.3.6.1.4.1.9148.3.2.6.0.41	Generated if monthly minutes reset.
apSysMgmtRealmStatusChangeTrap: 1.3.6.1.4.1.9148.3.2.6.0.45	Generated when there is a change in the status of 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.
apSysMgmtRegCacheThresholdTrap: 1.3.6.1.4.1.9148.3.2.6.0.46	Generated when the number of contracts 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 contracts stored in the registration cache falls below the configured threshold.
apSysMgmtRejectedMesagesThresholdExeededTrap: 1.3.6.1.4.1.9148.3.2.6.0.57	Generated when messages are rejected by the Net-Net SBC

Trap Name: OID Number	Description
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: • SIP signaling timeout • 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.
apSysMgmtShortSessionExceedTrap: 1.3.6.1.4.1.9148.3.2.6.0.48	Generated when the number of short sessions in a realm exceeds the short session threshold with the short session window.
apSysMgmtSingleUnitRedundancyTrap: 1.3.6.1.4.1.9148.3.2.3.0.3	Generated when the status of a slot changes. The varbinds contain the new informaton for the slot. Please see apHardwareModuleFamily in the ap-tc.mib for hardware module types. Note that as an example, SPU 1, 2 and 3 are not distinguished in the apHardwareModuleFamily table. All three share a value of 17.
apSysMgmtSipRejectionTrap: 1.3.6.1.4.1.9148.3.2.10.0.1	Generated when either a SIP INVITE or REGISTRATION request fails.
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.
apSysMgmtLPLookupExceededTrap 1.3.6.1.4.1.9148.3.2.6.0.65	Generated when the Additional Local Policy Lookups exceeds the configured threshold during the 100 second window period.
apSysMgmtSurrogateRegFailed: 1.3.6.1.4.1.9148.3.2.6.0.39	Generated if a surrogate registration failed after the maximum configured attempts.
apSysMgmtSystemStateTrap: 1.3.6.1.4.1.9148.3.2.6.0.17	Generated when the SBC is instructed to change system-stae or the transition from becoming_offline to offline occurs.
apSysMgmtTaskDeleteTrap: 1.3.6.1.4.1.9148.3.2.6.0.23	Generated if a task running on the system is deleted.
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 or stopped state.
apSysMgmtTempTrap: 1.3.6.1.4.1.9148.3.2.6.0.2	Generated if the temperature falls below the monitoring threshold.

Alarms

A Net-Net system alarm is triggered when a condition or event happens within either the Net-Net system hardware or software. Given a specific alarm, the Net-Net 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 Net-Net 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 Severity Levels

Five levels of alarm severity have been established for the Net-Net system. These levels have been designated so that the system can take action that is appropriate to the situation.

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 Net-Net system.
Critical	Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your Net-Net system.
Major	Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net 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. There will be no physical harm to your Net-Net system. However, you should attend to this type of alarm as soon as possible in order to keep your Net-Net 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 Net-Net system operating properly. For example, this type of alarm might indicate the Net-Net system is running low on bandwidth and you may need to contact your Acme Packet customer support representative to arrange for an upgrade.

Alarm Descriptions

Alarms are divided into seven categories: hardware, system, switch, network, media, application and configuration.

Hardware Alarms

Hardware alarms include information about fans, system power, system temperature, internal devices, MIU cards, and NIU cards on the Net-Net system.

> **Note:** If you suspect you have a hardware fault, contact Acme Packet Technical Support for assistance with running the diagnostics image loaded on the Net-Net 9200.

I2C Hardware Alarms

The following table lists the I2C hardware alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Example Log Message	Trap Generated
I2C Failure/ 11900200	MAJOR/ 50	The environmental sensor component detects a failure.	• MidPlane IDProm Write failure • PowerPlane IDProm Writer failure • I2C driver failure	apEnvMonI2CFailNotification OR apSyslogMessageGenerated (See Note 1)
I2C CARD FAILURE/ 118XX200	MAJOR/ 50	The environmental sensor component detects a card failure	• Unable to Read IDProm on <MODULE> x • Unable to Initialize I2C on <MODULE> x • Unable to Perform Health Scan on <MODULE> x • Unable to Switchover PHY PM 8380 Muxes to Active NPU • I2C Busy, where <MODULE> is one of the hardware modules	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Card Presence Alarms

The following table lists the card presence alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Trap Generated
CARD REMOVED/ 127XX100	NOTICE/ 0	A card has been removed.	Card in Slot XX has been Removed.	entConfigChange

I2C Alarm Types

The following table lists the I2C alarm types.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
I2C FAN FAULT/ 1186XX210	MAJOR/ 50	Fan fault detected.	Fan Fault on FAN Controller X - Affected fans are: Y.	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
	NORMAL/ 0	Fan fault cleared.	Clearing Fan Fault on FAN Controller X - Fan Mask Y.	
I2C COMM LOSS/ 1186XX211	MINOR/ 20	Communication error detected.	• Comm Error Detected on X in Slot N. • Comm Fault on FAN Controller X	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C POWER WARNING/ 118XX220	MAJOR/ 50 MINOR/ 20		Power Warning on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
I2C POWER FAULT/ 118XX221	MAJOR EMERGENCY/ 50	Power fault detected.	• Power Fault on X in slot N • Power not Present on Power Supply X • Voltage Input Fault detected on Power Supply X • Voltage Input Warning detected on Power Supply X • Temperature Fault detected on Power Supply X • Temperature Warning detected on Power Supply X • Fan Fault detected on Power Supply X • Voltage Output Fault detected on Power Supply X • Current Output Fault detected on Power Supply X	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TRACKING FAULT/ 118XX250	MAJOR/ 50	Tracking fault detected	Tracking Fault on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C CRC ERROR/ 118XX251	MAJOR/ 50	Power CRC error detected.	Power CRC Error on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TX FAULT/ 118XX252	MAJOR/ 50	Power transmission error detected.	Power Transmission Error in X on slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C SPEED FAULT/ 118XX212	MINOR/ 20	Fan speed fault detected.	Inconsistent Speed Setting on FAN Controller	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

I2C Link and Temperature Alarms

The following table lists the link and temperature alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
I2C LINK FAULT/ 118XX260 . . . . . 118XX26F	MINOR/ 20	Link fault has been detected.	• Tx Fault on Fiber PHY X::Port N • Bandwidth differs from value set on Fiber PHY X::Port N • Tx Disable differs from value set on Fiber PHY X::Port N • SFE has been removed on Fiber PHY X::Port N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)
	NORMAL/ 0	Clears the link fault alarms.	• Clearing Tx Fault on Fiber PHY X::Port N • Clearing Bandwidth Alarm on Fiber PHY X::Port N • Clearing Tx Disable Alarm on Fiber PHY X::PortN • SFE is present on Fiber PHY X::Port N	
I2C TEMP WARNING/ 128XX270 . . . . . 128XX27F	MINOR/ 20	• Temperature fault detected. • Minor temperature fault detected on fan controller.	• Temperature Warning on X in Slot N • Setting Minor Temperature Fault on FAN Controller X. Temp is XX.	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C TEMP HIGH/ 128XX280 . . . . . 128XX28F	MAJOR/ 50	• Temperature fault detected. • Major temperature fault detected on fan controller.	• Over Temperature Fault on X in slot N • Setting Major Temperature Fault on FAN Controller X. Temp is XX. • HIgh Temperature Alarm on X in Slot N	apEnvMonTempChangeNotification OR apSyslogMessageGenerated (See Note 1)

Voltage Alarms

The following table lists the voltage alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
I2C VOLTAGE FAULT/ 129XX230	MAJOR/ 50	Voltage fault detected.	Voltage Fault on X in slot N.	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C UNDER VOLTAGE/ 129XX231	MAJOR/ 50	Under voltage fault detected.	Under Voltage Fault on X in slot N	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C OVER VOLTAGE/ 129XX232	MAJOR/ 50	Over voltage fault detected.	Over Voltage Fault on something in slot N	apEnvMonVoltageChangeNotification OR apSyslogMessageGenerated (See Note 1)
I2C OVER CURRENT/ 118XX241	MAJOR/ 50	Over current fault detected.	Over Current Fault on X in slot N	apEnvMonStatusChangeNotification OR apSyslogMessageGenerated (See Note 1)

Specific Card Alarms The following table lists the card specific failure alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
PHY0 UNKNOWN TYPE/ 11450401	CRITICAL/ 100	Cannot identify PHY card type.	PHY 0 Unknown Type	apSysMgmtHardwareErrorTrap
PHY1 UNKNOWN TYPE/ 11451402	CRITICAL/ 100	Cannot identify PHY card type.	PHY 1 Unknown Type	apSysMgmtHardwareErrorTrap
PHY2 UNKNOWN TYPE/ 11452403	CRITICAL/ 100	Cannot identify PHY card type.	PHY 2 Unknown Type	apSysMgmtHardwareErrorTrap
PHY3 UNKNOWN TYPE/ 11453404	CRITICAL/ 100	Cannot identify PHY card type.	PHY 3 Unknown Type	apSysMgmtHardwareErrorTrap
PARITY ERROR/ 11420402	MAJOR/ 50	Parity error detected.	• Hardware Error in HSTRL: X, HINTR: Y • Hardware Error in HRSTR: X • Hardware Error in HPER: X • Hardware Error in CPER: X • Hardware Error in MPER: X • Hardware Error in XPER: X • Testing Alarm for PE/CAM exceptions	apSysMgmtHardwareErrorTrap
CAM EXCEPTION/ 11420403	• MAJOR-First time alarm is posted • CRITICAL-Second time alarm is posted without a clear • EMERGENCY-Third time alarm is posted without a clear/ • 50, 100	CAM exception detected.	• Cam Search Semaphore Error, Err Code X, Err: Y • Cam Operation Failure, Err Code X, Err: Y	apSysMgmtHardwareErrorTrap
QOS ERROR/ 11420404	MAJOR/ 50	QoS error detected.	• Hardware Error in QoS_FPGA_config ( ) • Error in QoS_daemon_init ( ) • Hardware Error: QoS FPGAs initialized in failed state • Gimp HW Error, Err: X, Gimp: Y ISR_Vector: Z	apSysMgmtHardwareErrorTrap
NPM FAILURE/ 11420405	MAJOR/ 100	NPM failure detected.	Media Startup failed	apSysMgmtHardwareErrorTrap
DSP FAILURE TCUX BASE/ 1003X5XX	MINOR CRITICAL/ 20, 100	DSP failed in TCU.	• DSP device N failed to boot • DSP device N failed to INITIALIZE • DSP DEVICE CRASHED • DSPComms Timeout • Rebooted DSP device • VAPI Request Timeout	None

System Alarms

System alarms include information about NIU and MIU port status, hardware threshold status, redundancy status and other system operating conditions on the Net-Net 9200.

NIU Link Alarms

The following table lists the NIU link alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
LINK DOWN ALARM GIGPORT/ 20250016-20250031	CRITICAL/ 75	Gigabit Ethernet interface goes down.	PHY X::Port N Link State is Inactive	linkDown

MIU Link Alarms

The following table lists the MIU link alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
LINK DOWN ALARM VXINTF 0/ 20240003	CRITICAL/ 75	MIU 0 goes down.	MIU X Link Is Down	linkDown
	CRITICAL/ 75	MIU 1 goes down.	MIU X Link Is Down	linkDown
	CRITICAL/ 75	MIU 2 goes down.	MIU X Link Is Down	linkDown

NPU Link Alarms The following table lists the NPU link alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SWING VIX ALARM/ 21420301	MINOR/ 20	Status check failed.	VIX Status Check Failed	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT A/ 21420302	WARNING/ 0	Inbound port A is down.	VIX In-Port-A Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT B/ 21420303	WARNING/ 0	Inbound port B is down	VIX In-Port-B Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT A/ 21420304	WARNING/ 0	Outbound port B is down.	VIX Out-Port-A Down	apSysMgmtHardwareErrorTrap
SWING VIX ALARM DOWN IN PORT B/ 21420305	WARNING/ 0	Outbound port B is down.	VIX Out-Port-B Down	apSysMgmtHardwareErrorTrap
SWING PLL ALARM/ 21420306	MINOR/ 20	Status check failed.	PLL Status Check Failed	apSysMgmtHardwareErrorTrap
SWING PLL ALARM DOWN PORT A/ 21420307	WARNING/ 0	Port A is down.	PLL Port A Down	apSysMgmtHardwareErrorTrap
SWING PLL ALARM DOWN PORT B/ 21420308	WARNING/ 0	Port B is down	PLL Port B Down	apSysMgmtHardwareErrorTrap
SWING QOS ALARM DOWN PORT A/ 21420309	WARNING/ 5	Port A is down.	QoS Port A Down	apSysMgmtHardwareErrorTrap
SWING QOS ALARM DOWN PORT B/ 2142030A	WARNING/ 5	Port B is down.	QoS Port B Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM/ 2142030B	MINOR/ 20	FPGA link check failed.	• Flair FPGA Link Check Failed • NPU X Failed to set Swingline FPGA port selector to N • NPU X Failed to set Swingline FPGA TCU Mask to N	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 0/ 2142030C	WARNING/ 0	Port 0 is down.	Flair FPGA Port 0 Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 1/ 2142030D	WARNING/ 0	Port 1 is down.	Flair FPGA Port 1 Down	apSysMgmtHardwareErrorTrap
SWING FLAIR ALARM DOWN PORT 2/ 2142030E	WARNING/ 0	Port 2 is down.	Flair FPGA Port 2 Down	apSysMgmtHardwareErrorTrap

TCU Link Alarms

The following table lists the TCU link alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
FLAIR SWING ALARM/ 21430301	MINOR/ 20	FLAIR driver was not set to the active NPU.	TCU *XX* Failed to Set FLAIR Driver to Active NPU *YY*.	apSysMgmtHardwareErrorTrap

Utilization Alarms

The following table lists the system utilization alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
MEM UTIL OVER THRESHOLD/ 21E00104	MINOR WARNING NOTICE/ 5	Memory usage has changed.	Memory usage was XX percent and now is YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
CPU UTIL OVER THRESHOLD/ 21E00103	WARNING NOTICE/ 5	CPU usage has changed.	CPU usage was XX percent and now is YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
NAT UTIL OVER THRESHOLD/ 21E20105	MINOR/ 20	NAT usage has changed.	NAT table capacity XX percentis over threshold YY percent (exclude deny list).	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
ARP UTIL OVER THRESHOLD/ 21E20106	MINOR/ 20	ARP table usage reached 90% or greater of its capacity.	ARP table capacity XX percent is over threshold YY percent	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)

Health Score Alarms

The following table lists the health score alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SYS HEALTH ALERT/ 200X0201	EMERGENCY CRITICAL MINOR/ 100, 75, 20	• Boot timeout occurs • Register timeout occurs • Manifest timeout occurs • Ready timeout occurs • Becoming Active timeout occurs • Becoming Standby timeout occurs • Becoming OOS timeout occurs	• Boot Timeout on slot XX • Register Timeout on slot XX • Manifest Timeout on slot XX • Ready Timeout on slot XX • Becoming Active Timeout on slot XX • Becoming Standby Timeout on slot XX • Becoming OOS Timeout on slot XX	apSyslogMessageGenerated
SYS HEALTH UNDER THRESHOLD/ 21EX0210	NOTICE/ 0	Net-Net system's health is under threshold 50.	Health Score Dropped to XX on Card YYY	apSysMgmtGroupTrap OR apSyslogMessageGenerated (See Note 2)
SYS HEALTH TIMEOUT/ 200X0202	MINOR/ 20	Health check timeout occurs	Health Check Timeout on Card XX	apSyslogMessageGenerated
SYS HEALTH RESET/ 200X0203	EMERGENCY/ 100	A card has failed to boot.	Card XX has failed to boot	apSyslogMessageGenerated

Redundancy Alarms

The following table lists the redundancy alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SYS SWITCH TO UNASSIGNED/ 226XX221	NOTICE/ 0	A state transition occurred to Unassigned.	<Name of HA peer> Switchover to Unassigned Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO ACTIVE/ 226XX222	NOTICE/ 0	A state transition occurred from Standby/BecomingStandby to BecomingActive.	<Name of HA peer> Switchover to Active Role	apSysMgmtSingleUnitRedundancyTrapOR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO STANDBY/ 226XX223	NOTICE/ 0	A state transition occurred from Active/BecomingActive to BecomingStandby/RelinquishingActive.	<Name of HA peer> Switchover to Standby Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SYS SWITCH TO RECOVERY/ 226XX224	NOTICE/ 0	A state transition occurred to Recovery.	<Name of HA peer> Switchover to Recovery Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)
SYS SWITCH TO OUTOFSERVICE/ 226XX225	NOTICE/ 0	Unable to synchronize with Active HA Net-Net system peer within BecomingStandby timeout.	<Name of HA peer> Switchover to Out-of-Service Role	apSysMgmtSingleUnitRedundancyTrap OR apSyslogMessageGenerated (See Note 2)

System Task Alarms The following table lists the system task alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SYS TASK SUSPENDED/ 20A00101	MAJOR/ 50	A Net-Net system task (process) suspends or fails.	Task XX Failed to Spawn	apSysMgmtTaskSuspendTrap
	EMERGENCY/ 100		Task XX with PID YY is Suspended	
	EMERGENCY/ 100		Task XX with PID YY is Stopped	
	EMERGENCY/ 100		Task XX no longer Running	
	WARNING/ 5		Task XX not ready	

System State Alarms The following table lists the system state alarm information.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
SYS SNMP AUTH FAILURE/ 20110233	MAJOR/ 50	SNMP authentication failure	• SNMP Agent got improper request from community XXX at address YYY • SNMP Agent received bad community string XXX from address YYY	authenticationFailure (See Note 3)
SYS PASSWORD RESET/ 20000236	NOTICE/ 0	Password reset to factory defaults	SA Status Change	None

System Miscellaneous Alarms

The following table lists miscellaneous system alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
NPU NONE ACTIVE/ 20020401	EMERGENCY/ 100	No NPUs are active or present.	• System Unable to Run - No NPUs Active • Systen Unable to Run - No NPUs present	apSyslogMessageGenerated
PHY NONE ACTIVE/ 20050402	EMERGENCY/ 100	No PHYs active or configured.	• No PHYs Active to Pass Media • No PHYs Configured to Pass Media	apSyslogMessageGenerated
RDP LINK DOWN ALARM/ 20XX0001	EMERGENCY NOTICE/ 0, 100	The core is non-responsive.	• Core X.X.X Link is Non-Responsive • Internal Communication Link Down (XX = => YY)	apSyslogMessageGenerated
IFSTRUCT CORRUPT ALARM/ 20000501	MAJOR/ 50	The interface structure is corrupt.	• <Interface Name/Unit>: ERROR Sysch_iflist: variable XX is 0 • ifVerify: NULL interface pointer • ifVerify: <Interface Name and Unit> XX is NULL • The driver does not support RFC2233	apSyslogMessageGenerated

Switch Alarms

NPU Switch

The following table lists the alarms for the NPU switch.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
DX240 ERROR/ 10020300	MINOR MAJOR/ 20	NPU failed to switch over.	• NPU nn Failed to Switchover to Active Status • NPU nn Failed to Switchover to Standby Status • NPU nn Failed to Switchover to OOS Status • NPU nn Switch Failed to Perform Health Check • NPU nn Failed to initialize PHY YY • NPU nn Failed to connect to Active PHY YY • DX240 Phy Reg Read Failed • DX240 Phy Reg Write Failed • DX240 Reg Write Failed • DX240 Reg Read Failed • Fatal Dx240 Interrupt • Minor DX240 Error	apSyslogMessageGenerated
DX240 DOWN ALARM GMAC 0/ 10020302-1002030A	MAJOR/ 50	GMAC port link state is inactive.	GMAC Port nn Link State is Inactive	apSyslogMessageGenerated

SPU Switch

The following table lists the alarms for the SPU switch.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
BCM56K PCI BUS ERR/ 10010300	MAJOR/ 50	PCI Error	BROADCOM 56304 sysconf_attach PCI error on soc_unit X	apSyslogMessageGenerated

Network Alarms

The following table lists the network alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
MEDIA GATEWAY ALARM/ 310X0XXX	MAJOR/ 25	Gateway is unreachable.	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 OR apSyslogMessageGenerated (See Note 2)

Media Alarms

Media alarms include events related to MBCD exception conditions. The following table lists the MBCD media alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
MBCD ALARM OUT OF MEMORY/ 40E00001	CRITICAL: for flow MAJOR: for media (if server cannot allocate a new context)/ 0	No further memory can be allocated for MBCD.	• Flow: Cannot create free port list for realm 'XXX'. • Failed to allocate new context • Media XX Timer Expired: camid=YY: unable to allocate request, context or command! dropping Flow.	apSysMgmtMediaOutOfMemory OR apSyslogMessageGenerated (See Note 2)
MBCD ALARM INTERNAL / 40000002	MAJOR MINOR/ 0	An internal software error.	Internal Error. No agent for socket <IPPort>.	apSyslogMessageGenerated
MBCD ALARM UNKNOWN REALM / 40F00003	MINOR/ 0	Media server is unable to find realm interface.	• ingress realm XXX not found • egress realm XXX not found	apSysMgmtMediaUnKnownRealm OR apSyslogMessageGenerated (See Note 2)

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
MBCD ALARM OUT OF BANDWIDTH / 40D00005	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50% / 0	The realm is out of bandwidth.	out of bandwidth	spSysMgmtMediaBandwidthTrap OR apSyslogMessageGenerated (See Note 2)
MBCD ALARM OUT OF PORTS / 40C00006	CRITICAL: failure rate = 100% MAJOR: failure rate > or = 50%/ 0	The realm is out of steering ports.	out of steering ports	apSysMgmtMediaPortsTrap OR apSyslogMessageGenerated (See Note 2)

Application Alarms

Application alarms include events related to application exceptions on the Net-Net system.

RADIUS Connection Down Alarm

The following table lists the RADIUS connection down alarm.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
APP ALARM LOST ACCT CONN/ 51100001	CRITICAL: if all enabled and configured 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./ 1	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.	apSysMgmtRadiusDownTrap OR apSyslogMessageGenerated (See Note 2)

Application Alarms

The following table lists the application alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Log Message	Traps Generated
APP ALARM APPROACH LIC SESS CAP/ 51B00004	MAJOR/ 1	Total number of active sessions on the system (across all protocols) is within 98 to 100% of the Net-Net system's licensed capacity.	Total number of sessions (<#>) is approaching licensed capacity (<#>)	XXapSyslogMessageGenerated (ap-slog.mib) apLicenseApproachingCapacityNotification (ap-smgmt.mib)

Configuration Alarms

The following table lists the configuration alarms.

Name/ID	Severity/ Health Degredation	Cause(s)	Example Log Message	SNMP Traps Sent
CFG ALARM SAVE FAILED/ 61300001	MAJOR/ 1	The save config command execution failed on a standby Net-Net SD peer operating as part of an HA pair.	Save Config Failed	apSysMgmtCfgSaveFailTrap

Note: 1. If the "enable-env-monitor-traps" parameter under the system-config configuration element is enabled, this trap is sent. If the parameter is disabled, the "asSyslogMessageGenerated" trap is sent instead.

Note: 2. If the "enable-snmp-monitor-traps" parameter under the system-config configuration element is enabled, this trap will be sent. If the parameter is disabled, the "apSyslogMessageGenerated" trap is sent instead.

Note: 3. If the "enable-snmp-auth-traps" option under system-config is disabled, this trap will not be sent.

Displaying and Clearing Alarms

See the *Net-Net 9200 Maintenance and Troubleshooting Guide* for complete details.

Acme Packet Log Levels and syslog Level Severities

There is a direct correlation between Acme Packet 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 Acme Packet 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 Net-Net system which requires immediate attention. If you do not attend to it immediately, there could be physical, irreparable damage to your Net-Net system.
2	CRITICAL	A serious condition within the Net-Net 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 Net-Net 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 Net-Net 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 Net-Net system. However, you should attend to it as soon as possible in order to keep your Net-Net system operating properly.
5	WARNING	The Net-Net 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 Net-Net system operating properly.
6	NOTICE	Used for Acme Packet customer support purposes.
7	INFO	
8	TRACE	
9	DEBUG	

syslog Level Severities

The following table defines the Acme Packet 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)

2 Standard SNMP OIDs

Introduction

This section explains the standard SNMP OIDs supported by the Net-Net system.

Platform Group

The following table describes the standard SNMP support for each Net-Net system platform.

Interfaces Group

The following table describes the standard SNMP support for the interfaces table, which contains information about the entity's media interfaces (PHY port) and management control interfaces in MIU cards.

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.
ifDescr	ifTable.ifEntry: 1.3.6.1.2.1.2.2.1.2	Textual string containing information about the interface. This string includes the configured interface name, sthe slot and port numbers, and the name of the manufacturer (can be truncated to 255 bytes).
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. When the system initializes, all interfaces start with ifAdminStatus in the down (2) state. As a result of either explicit action or per configuration information retained by the system, ifAdminStatus then changes to either the up (1) or testing (3) states (or remains in the down (2) state).
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. If ifAdminStatus is down (2), then ifOperStatus should be down (2). If ifAdminStatus changes to up (1), then ifOperStatus should change to up (1) if the interface is ready to transmit and receive network traffice. ifOperStatus should change to dormant (5) if the interfaces is waiting for external actions. It should remain in the down (2) state if and only if there is a fault that prevents it from going to the up (1) state. It should remain in the notPresent (6) state if the interface has missing components. **DOWN**: ifAdminstatus is down. The physical link is down. **UP**: ifAdminStatus is up, the DFU cared and PHY card are present, the link is good, and this interface is an active interface. **noPresent**: The PHY or DFU cards are not present.
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.

SNMP GET Query Name	Object Identifier Name: Number	Description
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.
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	spu0	spu1	phy0	phy1
ifType	ethernetCsmacd	ethernetCsmacd	ethernetCsmacd	ethernetCsmacd
ifMtu	1500	32768	1500	1500
ifSpeed	100000000	100000000	100000000	1000000000

OID	Table Index			
ifPhysAddress	0x00 0x08 0x25 0x01 0x48 0x40	0x00 0x08 0x25 0x01 0x48 0x41	0x00 0x08 0x25 0x01 0x48 0x42	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
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

ifXTable Support

Acme Packet supports the ifName and ifConnectorPresent entries 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.
- ifConnectorPresent has the value true (1) if the interface sublayer has a physical connector and the value false (2) if it does not.

Examples of ifIndex Values

The following table lists examples of ifIndex with four ports per PHY card.

ifIndex Value	Slot	Port
1	SPU0	Eth0
2	SPU1	Eth1
3	Phy0	0
4	Phy1	0
5	Phy2	0
6	Phy3	0
7	Phy0	1
8	Phy1	1
9	Phy2	1
10	Phy3	1
11	Phy0	2
12	Phy1	2
13	Phy2	2
14	Phy3	2
...	...	...

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 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP routers 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. Values are: forwarding(1) acting as a router notForwarding(2) not acting as a router
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.
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 routers 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 routers, 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.)

SNMP GET Query Name	Object Identifier Name: Number	Description
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.
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.

SNMP GET Query Name	Object Identifier Name: Number	Description
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
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 that 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					
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 end-points 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

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 (always Acme Packet) and version identification of the system's hardware type, operating system, and networking software.
sysObjectID	system: 1.3.6.1.2.1.1.2	The 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. This value is an Acme Packet SNMP agent number assigned by IANA (enterprises.9148.1.2).
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) Acme Packet supports Layers 1, 3, 4, and 7. The value is: 2^(1-1) + 2^(3-1) + 2^(4-1) +2^(7-1) Which equals: 1+4+8+64 Which in turn equals 79.
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 SD4
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.9148.1.1	enterprises.9148.2	enterprises.9148.3	enterprises.9148.4
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 IV 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 OIDs

Introduction

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

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 only populated for realms on which SIP is configured; this table does not support statistics for realms in which H.323 is running. 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	Not supported by Net-Net 9200.
apSysMemoryUtil	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.2	Not supported by Net-Net 9200.
apSysHealthScore	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.3	Not supported by Net-Net 9200.
apSysRedundancy	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.4	Not supported by Net-Net 9200.
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	Not supported by Net-Net 9200.
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.
apSysH323Registration	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.1.13	Number of H.323 registrations for the Net-Net SBC.
apSysRegCacheLimit	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.14	Maximum number of contacts allowed to be accepted into the registration cache. A value of 0 indicates no limit.
apSysShortSessionThreshold	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.15	Threshold for which a trap will be emitted when the amount of short sessions exceeds this value.
apSysRejectedMessages	apSysMgmtGeneralObjects: 1.3.6.1.4.1.9148.3.2.1.1.18	Number of messages rejected by the Net-Net SBC because of matching criteria.
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.
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 MB.
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.

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apH323SessionAgentStatsTable (1.3.6.1.4.1.9148.3.2.1.2.3)		
Object Identifier Name: apH323SessionAgentStatsEntry (1.3.6.1.4.1.9148.3.2.1.2.3.1)		
apH323SAStatsSessionAgentHostname	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.2	Host name of the session agent for which statistics are being calculated.
apH323SAStatsSessionAgentType	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.3	Type of session agent.
apH323SAStatsCurrentActiveSessionsInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.4	Number of current active inbound sessions.
apH323SAStatsCurrentSessionRateInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.5	Current inbound session rate in CPS.
apH323SAStatsCurrentActiveSessionsOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.6	Number of current active outbound sessions.
apH323SAStatsCurrentSessionRateOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.7	Current outbound session rate in CPS.
apH323SAStatsTotalSessionsInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.8	Total number of inbound sessions.
apH323SAStatsTotalSessionsNotAdmittedInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.9	Total number of inbound sessions rejected due to insufficient bandwidth.
apH323SAStatsPeriodHighInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.10	Highest number of concurrent inbound sessions during the period.
apH323SAStatsAverageRateInbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.11	Average rate of inbound sessions during the period in CPS.
apH323SAStatsTotalSessionsOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.12	Total number of outbound sessions.
apH323SAStatsTotalSessionsNotAdmittedOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.13	Total number of outbound sessions rejected due to insufficient bandwidth.
apH323SAStatsPeriodHighOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.14	Highest number of concurrent outbound sessions during the period.
apH323SAStatsAverageRateOutbound	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.15	Average rate of outbound sessions during the period in CPS.
apH323SAStatsMaxBurstRate	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.16	Maximum burst rate of traffice measured during the period (combined inbound and outbound).
apH323SAStatsPeriodSeizures	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.17	Total number of seizures during the period.
apH323SAStatsPeriodAnswers	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.18	Total number of answered questions during the period.
apH323SAStatsPeriodASR	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.19	The answer-toseizure ratio expressed as a percentage. For example, a value of 90 represents 90% or .90.

SNMP GET Query Name	Object Identifier Name: Number	Description
apH323SAStatsAverageLatency	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.20	Average observed one-way signaling latency during the period in milliseconds.
apH323SAStatsMaxLatency	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.21	Maximum observed one-way signaling latency during the period in milliseconds.
apH323SAStatsSessionAgentStatus	apH323SessionAgentStatsEntry: 1.3.6.1.4.1.9148.3.2.1.2.3.1.22	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)		
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 SIP is configured; the table does not support statistics for realms in which H.323 is running.		
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.
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.
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.

SNMP GET Query Name	Object Identifier Name: Number	Description
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.
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.
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 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.
Object Identifier Name: apSysMgmtMIBNetMgmtCtrlObjects (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)		
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 for which the statistics are being calculated.
apNetMgmtCtrlStatsType	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.2	Type of the specified network management control, which can be 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 that have matched a destination identifier of the specified network management control.
apNetMgmtCtrlStatsRejectedTotal	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.4	Total number of incoming calls that have been rejected by the specified network control.
apNetMgmtCtrlStatsDivertedTotal	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.5	Total number of incoming calls that have been diverted by the specified network management control.

SNMP GET Query Name	Object Identifier Name: Number	Description
apNetMgmtCtrlStatsIncomingCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.6	Number of incoming calls during the current period that have matched a destination identifier of the specified network management control.
apNetMgmtCtrlStatsRejectedCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.7	Number of incoming calls during the current period that have been rejected by the specified network management control.
apNetMgmtCtrlStatsDivertedCurrent	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.8	Number of incomimg calls during the current period that have been diverted by the specified network management control.
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 have matched a destination identifier of the specified network management control.
apNetMgmtCtrlStatsRejectedPeriodMax	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.10	Maximum number of incoming calls during a period that have been rejected by the specified network management control.
apNetMgmtCtrlStatsDivertedPeriodMax	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.11	Maximum number of incoming calls during a period that have been diverted by the specified network management control.
apNetMgmtCtrlStatsState	apNetMgmtCtrlStatsEntry: 1.3.6.1.4.1.9148.3.2.1.3.1.1.12	State of the specified network management control; either disabled or enabled.
Object Identifier Name: apENUIMServerStatusTable (1.3.6.1.4.1.9148.3.2.1.4.1)		
Object Identifier Name: apENUIMServerStatusEntry (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.
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	RPH value for which statistics are being calculated.
apNSEPStatsRPHCurrentActiveSessionsInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.1.2	Number of current active inbound NS/EP sessions.
apNSEPStatsRPHTotalSessionsInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.1.3	Total number of inbound NS/EP sessions during the period.

SNMP GET Query Name	Object Identifier Name: Number	Description
apNSEPStatsRPHPeriodHighInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.14.	Highest number of concurrent inbound NS/EP sessions during the period.
apNSEPStatsRPHTotalSessionsNotAdmittedInbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.15.	Total number of inbound NS/EP sessions rejected.
apNSEPStatsRPHCurrentActiveSessionsOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.1.6	Number of current active outbound NS/EP sessions.
apNSEPStatsRPHTotalSessionsOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.17.	Total number of outbound NS/EP sessions during the period.
apNSEPStatsRPHPeriodHighOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.1.8	Highest number of concurrent outbound NS/EP sessions during the period.
apNSEPStatsRPHTotalSessionsNotAdmittedOutbound	apNSEPStatsRPHEntry: 1.3.6.1.4.1.9148.3.2.1.5..5.1.9	Total number of outbound NS/EP sessions rejected.
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)		
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)		
apTrapTableNumVariables	apSysMgmtTrapTableEntry: 1.3.6.1.4.1.9148.3.2.1.7.1.1.3	Number of information 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.
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)		
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

SNMP GET Query Name	Object Identifier Name: Number	Description
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.

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
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
apCombinedStatsSessionAgentIndex	1
apCombinedStatsSessionAgentHostname	192.168.69.64
apCombinedStatsSessionAgentType	sip
apCombinedCurrentActiveSessionsInbound	0
apCombinedStatsSessionRateInbound	0
apCombinedStatsCurrentActiveSessionsOutbound	0
apCombinedStatsTotalSessionsInbound	0
apCombinedStatsTotalSessionsInbound	0
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
apSipSAStatsMaxBurstRate	1
apSipSAStatsPeriodSeizures	0
apSipSAStatsPeriodAnswers	0
apSipSAStatsPeriodASR	0
apSipSAStatsAverageLatency	0
apSipSAStatsMaxLatency	0
apSipSAStatsSessionAgentStatus	inService

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	0	0
apSigRealmStatsMaxLatency	0	0

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 Net-Net 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.
apLicenseACPFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.12	Value that indicates whether a Acme Control Protocol (ACP) license is present. A value of 1 indicates that ACP licensing is enabled. A value of 2 indicates that ACP licensing is not enabled.
apLicenseLPFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.13	Value that indicates whether a Local Policy (LP) license is present. A value of 1 indicates that LP licensing is enabled. A value of 2 indicates that LP licensing is not enabled.
apLicenseSAGFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.14	Value that indicates whether a Session Agent Group (SAG) license is present. A value of 1 indicates that SAG licensing is enabled. A value of 2 indicates that SAG licensing is not enabled. (load balancing feature)

SNMP GET Query Name	Object Identifier Name: Number	Description
apLicenseACCTFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.15	Value that indicates whether a ACCT license is present. An ACCT license allows the Net-Net system to create connections and send CDRs to one or more RADIUS servers. A value of 1 indicates that ACCT licensing is enabled. A value of 2 indicates that ACCT licensing is not enabled.
apLicenseHAFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.16	Value that indicates whether a High Availability (HA) license is present. A value of 1 indicates that HA licensing is enabled. A value of 2 indicates that HA licensing is not enabled.
apLicensePACFeature	apLicenseEntry: 1.3.6.1.4.1.9148.3.5.1.1.1.17	Value that indicates whether a PAC license is present. A value of 1 indicates that PAC licensing is enabled. A value of 2 indicates that PAC licensing is not enabled.

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	gjjt4vv602vhg387mrfuatjist093ggu42hbto3
apLicenseCapacity	32000	32000
apLicenseInstallDate	N/A	10:57:12 FEB 16 2006
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'.
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 montior located in the chassis.
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 for which the voltage value is monitored. Possible values are: v2p5(1) v3p3(2) v5(3) cpu(4) v1(5). v1p1(6) v1p15(7) v1p2(8) v1p212(9) v1p25(10) v1p3(11) v1p5(12) v1p8(13) v2p6(14) v2p5-2.5 v sensor: L3 cache core voltage, microprocessor and co-processor I/0 voltage, and FPGA memories I/O voltage v3p3-3.3V sensor: general TTL supply rail, control logic, micro-processor and co-processor, and SDRAM. V5-5V sensor: fans, micro-processor core voltage regulator CPU-CPU voltage micro-processcor core voltage.
apEnvMonVoltageStatusDescr	apEnvMonVoltageStatusEntry: 1.3.6.1.4.1.9148.3.3.1.2.1.1.3	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.

SNMP GET Query Name	Object Identifier Name: Number	Description
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 7450 and 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	The slot for which this voltage is found.
apEnvMonVoltageSlotType	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. The possible values are ds1624sMain(1) DS164sCPU(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: (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.
apEnvMonTemperatureSlotID	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.6	The slot for which this temperature is found.
apEnvMonTemperatureSlotType	apEnvMonTemperatureStatusEntry 1.3.6.1.4.1.9148.3.3.1.3.1.1.7	The type of module found in this slot.
Object Identifier Name: apEnvMonFanStatusEntry (1.3.6.1.4.1.9148.3.3.1.4.1.1)		
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: 0 which indicates the left fan. 1 which indicates the middle fan. 2 which indicates the right fan.
apEnvMonFanStatusDescr	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.3	Description of the fan, which can have one of the following values: 1 which indicates fan 1. 2 which indicates fan 2. 3 which indicates fan 3.
apEnvMonFanStatusValue	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.4	Current measurement of fan speed in percentage.

SNMP GET Query Name	Object Identifier Name: Number	Description
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.
apEnvMonFanSlotID	apEnvMonFanStatusEntry: 1.3.6.1.4.1.9148.3.3.1.4.1.1.6	The slot in which this fan is located.
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: indicates the left power supply A 1: indicates the right power supply B.
apEnvMonPowerSupplyStatusDescr	apEnvMonPowerSupplyStatusEntr: 1.3.6.1.4.1.9148.3.3.1.5.1.1.3	Description of the power supply, which can have one of the following values: 1: i power supply A 2: power supply B
apEnvMonPowerSupplyState	apEnvMonPowerSupplyStatusEntr: 1.3.6.1.4.1.9148.3.3.1.5.1.1.4	Current state of the which can have one of the following 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)		
These object identifiers are deprecated.		
Object Identifier Name: apEnvCardEntry (1.3.6.1.4.1.9148.3.3.1.7.1.1)		
apEnvMonCardSlot	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.1	Slot number of the card. The slot number is zero-based, 0 to n.
apEnvMonCardType	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.2	The type of card.
apEnvMonCardDescr	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.3	Textual description of the card.
apEnvMonCardHealthScore	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.4	Card health percentage, with a health percentage value of 100 (100%) being the healthiest.

SNMP GET Query Name	Object Identifier Name: Number	Description
apEnvMonCardState	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.5	Current state of the card.
apEnvMonCardRedundancy	apEnvCardEntry: 1.3.6.1.4.1.9148.3.3.1.7.1.1.6	Redundancy state of the card.
Object Identifier Name: apEnvMonCpuCoreEntry (1.3.6.1.4.1.9148.3.3.1.7.2.1)		
apEnvMonCpuCoreIndex	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.1	The core index of the CPU. For CoreID values, please see the Maintenance and Trouble Shooting Guide, System Management Chapter, CPU Core Index Mapping.
apEnvMonCpuCoreDescr	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.2	Description of the CPU core.
apEnvMonCpuCoreUsage	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.3	Current percentage of the CPU core being used.
apEnvMonCpuCoreState	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.4	State of the CPU core: unknown (0) present (1) booting (2) registered (3) readywait (4) ready (5) bootTimeout (7) registerTimeout (8) readyTimeout (9)
apEnvMonCpuCoreRamDescr	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.5	Description of the CPU core RAM.
apEnvMonCpuCoreRamUsage	apEnvMonCpuCoreEntry: 1.3.6.1.4.1.9148.3.3.1.7.2.1.6	Current percentage of CPU core RAM being used.

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

OID	Table Index			
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	left	middle	right
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

Physical Layer Card Status Table Examples

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

OID	Table Index	
	1	2
apEnvMonPhyCardStatusType	left	right
apEnvMonPhyCardStatusDesc	Phy 0	Phy 1
apEnvMonPhyCardState	normal	normal

Acme Packet Syslog MIB (ap-slog.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apSyslogMIBObjects (1.3.6.1.4.1.9148.3.1.1)		
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 that have been sent. This number might include notifications that were prevented from being transmitted due to reasons such as resource limitations and/or non-connectivity. If you are receiving notifications, you can periodically poll this object to determine if any notifications were missed.
apSyslogNotificationsEnabled	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.2	Indicates whether apSyslogMessageGenerated notifications will or will not be sent when a syslog message is generated by this device. Disabling notifications does not prevent syslog messages from being added to the apSyslogHistory table.
apSyslogMaxLevel	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.3	Indicates which syslog severity levels will be processed. Any syslog message with a log-level greater than this value will be ignored by the agent. Severity numeric values increase as their severity decreases. For example, major(3) is more severe than debug(8). Values include: emergency(1) critical(2) major(3) minor(4) warning(5) notice(6) info(7) trace(8) debug(9)

SNMP GET Query Name	Object Identifier Name: Number	Description
apSyslogMsgIgnores	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.4	Number of syslog messages that were ignored. There was no need to send apSyslog apSyslogMessageGenerated notification. A message is ignored if it has a log level greater than apSyslogMaxSeverity.
apSyslogMsgDrops	apSyslogBasic: 1.3.6.1.4.1.9148.3.1.1.1.5	Number of syslog messages that could no be processed because of a lack of system resources. Most likely this occurs at the same time that syslog messages are generated to indicate this lack of resources. Increases in the value might server as an indicaton that system resource levels should be examined using other MIB objects. A message that is dropped will not appear in the history table and no notificatioon 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 on the number of entries that the apSyslogHistoryTable might contain. A value of 0 will prevent any history from being retained. When this table 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. This object can be utilized to determine whether your polling frequency on the history table is fast enough and/or the size of your history table is large enough such that you are not missing messages.
Object Identifier Name: apSyslogHistoryTable (1.3.6.1.4.1.9148.3.1.1.2.3)		
Object Identifier Name: apSyslogHistory (1.3.6.1.4.1.9148.3.1.1.2.3.1)		
apSyslogHistFrom	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.3.1.2	Process name and host of the sending client. For example: anyclient@sr.acme.com
apSyslogHistLevel	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.3.1.3	The log level of the message.
apSyslogHistType	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.3.1.4	Textual identification for the log type, which categorizes the log message.
apSyslogHistContent	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.3.1.5	Text of the message. If the message text exceeds 255 bytes, it is truncated to 255 bytes.
apSyslogHistTimestamp	apSyslogHistory: 1.3.6.1.4.1.9148.3.1.1.2.3.1.6	Value of sysUpTime when this message was 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.
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.

SNMP GET Query Name	Object Identifier Name: Number	Description
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.
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.

Acme Packet H.323 MIB (ap-h323.mib)

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

SNMP GET Query Name	Object Identifier Name: Number	Description
Object Identifier Name: apH323MIBObjects (1.3.6.1.4.1.9148.3.10.1)		
Object Identifier Name: apH323StackTable (1.3.6.1.4.1.9148.3.10.1.1)		
Object Identifier Name: apH323StackEntry (1.3.6.1.4.1.9148.3.10.1.1,1)		
apH323StackName	apH323StackEntry: 1.3.6.1.4.1.9148.3.10.1.1.1.1	Configured H.323 stack name.
apH323StackCurrentCalls	apH323StackEntry: 1.3.6.1.4.1.9148.3.10.1.1.1.2	Number of current calls.
Object Identifier Name: apH323NotificationObjects (1.3.6.1.4.1.9148.3.10.2)		
apH323StackMaxCallThreshold	apH323StackNotificationObjects: 1.3.6.1.4.1.9148.3.10.2.1	Generated when the number of H.323 calls increases the percentage of the max calls threshold.
apH323StackMaxCallThresholdClear	apH323StackNotificationObjects: 1.3.6.1.4.1.9148.3.10.2.2	Generated when the number of H.323 calls decreases to below the lowest max calls theshold.