Extreme OS ONE Switching and Routing v22.2.2.0 SNMP MIB Reference Guide

MIB Structure, Supported Objects, and Network Management

9039558-00 Rev AA
April 2026

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

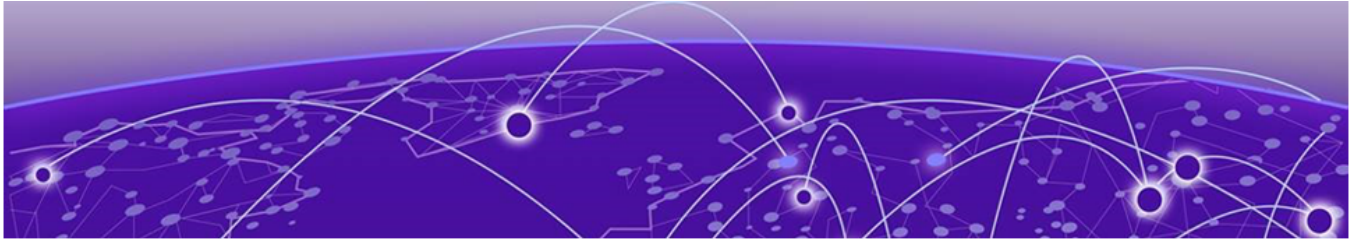
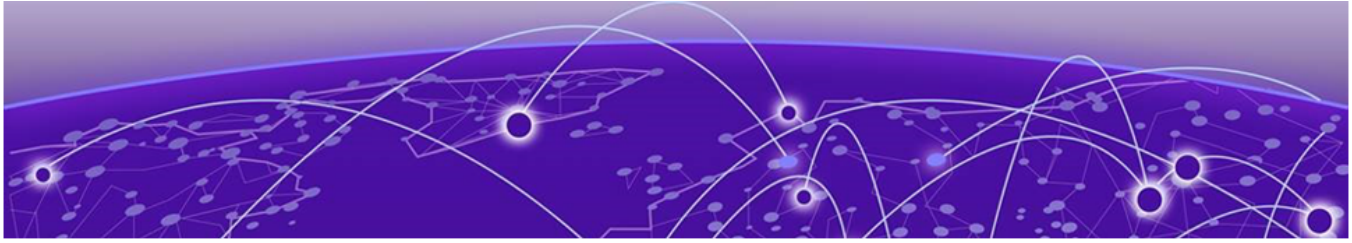


Table of Contents



Abstract

The Extreme OS ONE Switching SNMP MIB Reference Guide version 22.2.2.0 describes the MIB architecture, OIDs, access models, and trap mechanisms. The supported platforms include Extreme 8520/8720/8730/8820, enabling advanced, standards-aligned network management for intermediate to advanced IT professionals.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

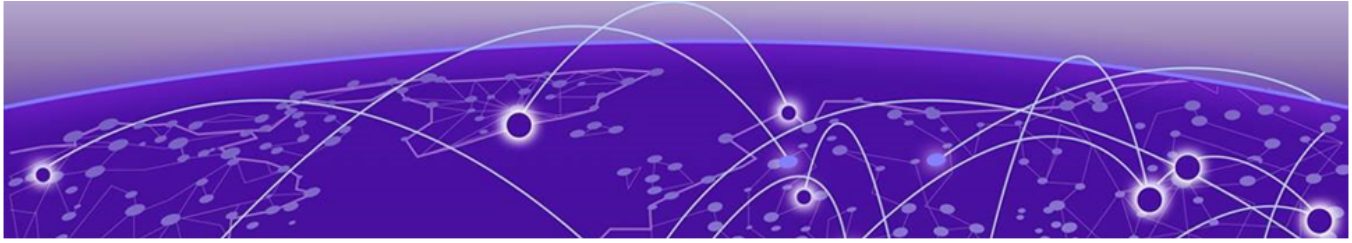
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



What's New in this Document

There are no changes to the Extreme OS ONE SR SNMP MIB Reference Guide, release 22.2.2.0.

For more information about this release, see the *Extreme OS ONE SR Release Notes*.

Supported Platforms

Extreme OS ONE Switching and Routing 22.2.1.0 and later releases support Extreme 8520, Extreme 8720, Extreme 8730, and Extreme 8820 hardware platforms.

Note

Although many software and hardware configurations are tested and supported for this release, all possible configurations and scenarios are beyond this document's scope.

For information about other releases, see the documentation for those releases.

MIB Overview

This document provides conceptual information about MIBs operation and structure on Extreme OS ONE Switching and Routing.

Understanding MIBs

The management information base (MIB) is a database of monitored and managed information on an Extreme device.

The MIB structure can be represented by a tree hierarchy. The root splits into three main branches:

- International Organization for Standardization (ISO)
- Consultative Committee for International Telegraph and Telephone (CCITT)
- Joint ISO and CCITT

These branches have short text strings and integers (object identifiers) to identify them. Text strings describe object names. Integers allow software to create compact, encoded representations of the names.

MIB Structure

Each MIB variable is assigned an object identifier (OID). The OID is the sequence of numeric labels on the nodes along a path from the root to the object. For example, as shown in the following figure, the `sysDescr` is:

```
1.3.6.1.2.1.1.1
```

The corresponding name is:

```
iso.org.dod.internet.mgmt.mib-2.system.sysDescr
```

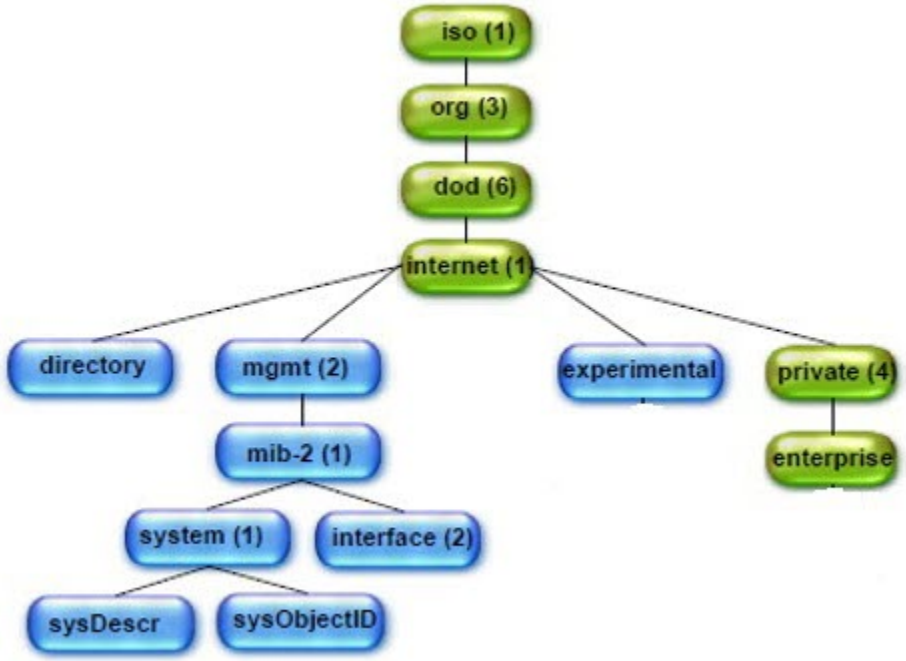
```
1.3.6.1.2.1.47
```

The corresponding name is:

```
iso.org.dod.internet.mgmt.mib-2.entityMIB
```

The other branches are part of the standard MIBs.

Figure 1: MIB tree



Access to MIB Variables

You can use a MIB browser to access the MIB variables. All MIB browsers load MIBs and perform queries.

Once the MIBs are loaded, read-only access provides access levels between the agent and management station. The access levels are described in the following table.

Table 4: MIB access levels

Access level	Description
Not accessible/None	You cannot read or write to this variable.
Read-create	Specifies a tabular object that can be read, modified, or created as a new row in a table.
Read-only	You can only monitor information.
Read-write	You can read or modify this variable.
Accessible-to-notify	You can read this information only through traps.

Supported MIBs - Extreme OS ONE Switching and Routing

The following topics list the standard MIB objects supported by Extreme OS ONE Switching and Routing.

Standard MIB Objects

Interface Group MIB

The Interface Group MIB defines the managed objects for an interface.

The Interfaces Group MIB (ifMIB) is specified in RFC 2863. Extreme OS ONE Switching and Routing supports ifTable and ifNumber. The following table describes the supported MIB objects:

Table 5: Supported MIB objects

Name	OID	Syntax	Description
ifNumber	.1.3.6.1.2.1.2.1	Integer32	Number of network interfaces on the system
ifIndex	.1.3.6.1.2.1.2.2.1.1	InterfaceIndex	Value between 1 and the value of the ifNumber
ifDescr	.1.3.6.1.2.1.2.2.1.2	DisplayString (Octet string)	Description of the interface
ifType	.1.3.6.1.2.1.2.2.1.3	IANAifType	
ifMtu	.1.3.6.1.2.1.2.2.1.4	Integer32	Size of the largest packet that can be sent or received on the interface
ifSpeed	.1.3.6.1.2.1.2.2.1.5	Gauge32	Estimation of the interface bandwidth in bits per second
ifPhysAddress	.1.3.6.1.2.1.2.2.1.6	PhysAddress(Octet string)	Interface address at the protocol sub-layer

Table 5: Supported MIB objects (continued)

Name	OID	Syntax	Description
ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	Integer	Administrative state of the interface: up (1), down (2), testing (3)
ifOperStatus	.1.3.6.1.2.1.2.2.1.8	Integer	Operational state of the interface: up (1), down (2), testing (3), unknown (4), dormant (5), not present (6) lower layer down (7)
ifLastChange	.1.3.6.1.2.1.2.2.1.9	TimeTicks	Value of sysUpTime when the interface entered the current operational state
ifInOctets	.1.3.6.1.2.1.2.2.1.10	Counter32	Number of octets received on the interface
ifInUcastPkts	.1.3.6.1.2.1.2.2.1.11	Counter32	Number of unicast packets delivered by the sublayer to a higher sublayer
ifInNUcastPkts	.1.3.6.1.2.1.2.2.1.12	Counter32	Number of multicast or broadcast packets delivered by the sublayer to a higher sublayer
ifInDiscards	.1.3.6.1.2.1.2.2.1.13	Counter32	Number of discarded inbound packets
ifInErrors	.1.3.6.1.2.1.2.2.1.14	Counter32	Number of inbound packets containing errors that prevented delivery to a higher-layer protocol
ifInUnknownProtos	.1.3.6.1.2.1.2.2.1.15	Counter32	Number of packets received from the interface that were discarded for an unknown or unsupported protocol
ifOutOctets	.1.3.6.1.2.1.2.2.1.16	Counter32	Number of octets sent from the interface
ifOutUcastPkts	.1.3.6.1.2.1.2.2.1.17	Counter32	Number of packets requested by a higher-level protocol that were addressed to a unicast address
ifOutNUcastPkts	.1.3.6.1.2.1.2.2.1.18	Counter32	Number of packets requested by a higher-level protocol that were addressed to a multicast or broadcast address
ifOutDiscards	.1.3.6.1.2.1.2.2.1.19	Counter32	Number of discarded outbound packets

Table 5: Supported MIB objects (continued)

Name	OID	Syntax	Description
ifOutErrors	.1.3.6.1.2.1.2.2.1.20	Counter32	Number of outbound packets containing errors that prevented transmission
ifOutQLen	.1.3.6.1.2.1.2.2.1.21	Gauge32	Length of the outbound packet queue
ifSpecific	.1.3.6.1.2.1.2.2.1.22	Object Identifier	OID of the MIB

System Group MIB

The System Group MIB defines the essential managed objects, or entities, for a system.

The System Group MIB is specified in RFC 1213. Extreme OS ONE Switching and Routing supports the following.

Table 6: Supported MIB objects

Name	OID	Syntax	Description
sysDescr	.1.3.6.1.2.1.1.1	DisplayString (Octet string)	Description of the entity
sysObjectID	.1.3.6.1.2.1.1.2	Object Identifier	OID of the device model
sysUpTime	.1.3.6.1.2.1.1.3	TimeTicks	Amount of time since the network management subsystem was last initialized
sysContact	.1.3.6.1.2.1.1.4	DisplayString (octet string)	Description of the contact person for the entity
sysName	.1.3.6.1.2.1.1.5	DisplayString (octet string)	Name of the entity. Usually the FQDN.
sysLocation	.1.3.6.1.2.1.1.6	DisplayString (octet string)	Physical location of the entity
sysServices	.1.3.6.1.2.1.1.7	Integer	Description of the services that the entity offers

Entity MIB

The Entity MIB identifies the physical entities that are supported by an SNMP agent.

The Entity MIB is specified in RFC 4133. Extreme OS ONE Switching and Routing supports entPhysicalTable. The following table describes the supported MIB objects:

Table 7: Supported MIB objects

Name	OID	Syntax	Description
entPhysicalIndex	.1.3.6.1.2.1.47.1.1.1.1.1	PhysicalIndex	Value that uniquely identifies the physical entity
entPhysicalDescr	.1.3.6.1.2.1.47.1.1.1.1.2	SnmpAdminString	Description of the physical entity
entPhysicalVendorType	.1.3.6.1.2.1.47.1.1.1.1.3	AutonomousType	Vendor-specific indicator of the hardware type for the physical entity
entPhysicalContainedIn	.1.3.6.1.2.1.47.1.1.1.1.4	PhysicalIndexOrZero	Value of entPhysicalIndex of the physical entity that contains this physical entity
entPhysicalClass	.1.3.6.1.2.1.47.1.1.1.1.5	PhysicalClass	Indicator of the hardware type of the physical entity
entPhysicalParentRelPos	.1.3.6.1.2.1.47.1.1.1.1.6	Integer32	Indicator of this child component relative to its sibling components
entPhysicalName	.1.3.6.1.2.1.47.1.1.1.1.7	SnmpAdminString	Name of the physical entity
entPhysicalHardwareRev	.1.3.6.1.2.1.47.1.1.1.1.8	SnmpAdminString	Vendor-specific identifier of the hardware revision for the physical entity
entPhysicalFirmwareRev	.1.3.6.1.2.1.47.1.1.1.1.9	SnmpAdminString	Vendor-specific identifier of the firmware revision for the physical entity
entPhysicalSoftwareRev	.1.3.6.1.2.1.47.1.1.1.1.10	SnmpAdminString	Vendor-specific identifier of the software revision for the physical entity

Table 7: Supported MIB objects (continued)

entPhysicalSerialNum	.1.3.6.1.2.1.47.1.1.1.1.11	SnmpAdminString	Vendor-specific serial number for the physical entity
entPhysicalMfgName	.1.3.6.1.2.1.47.1.1.1.1.12	SnmpAdminString	Name of the manufacturer of the physical entity
entPhysicalModelName	.1.3.6.1.2.1.47.1.1.1.1.13	SnmpAdminString	Vendor-specific model name for the physical entity
entPhysicalAlias	.1.3.6.1.2.1.47.1.1.1.1.14	SnmpAdminString	Alias for the physical entity, as specified by the network manager
entPhysicalAssetID	.1.3.6.1.2.1.47.1.1.1.1.15	SnmpAdminString	Tracking identifier for the physical entity, as specified by the network manager
entPhysicalIsFRU	.1.3.6.1.2.1.47.1.1.1.1.16	TruthValue	Indicates whether the vendor considers this physical entity to be a field replaceable unit
entPhysicalMfgDate	.1.3.6.1.2.1.47.1.1.1.1.17	DateAndTime	Date that the physical entity was manufactured
entPhysicalUris	.1.3.6.1.2.1.47.1.1.1.1.18	Octet String	Extra information about the physical entity

ifXTable Extended MIB

The ifXTable is a list of interface entries, the number of which is determined by the value of ifNumber.

The ifXTable Extended MIB is specified in RFC 2863, which also specifies the Interface Group MIB. Extreme OS ONE Switching and Routing supports the following.

Table 8: Supported MIB objects

Name	OID	Syntax	Comments
ifName	.1.3.6.1.2.1.31.1.1.1.1	DisplayString (Octet string)	Name of the interface
ifInMulticastPkts	.1.3.6.1.2.1.31.1.1.1.2	Counter32	Number of packets addressed to a multicast address at this sublayer
ifInBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.3	Counter32	Number of packets addressed to a broadcast address at this sublayer
ifOutMulticastPkts	.1.3.6.1.2.1.31.1.1.1.4	Counter32	Number of packets requested by a higher-level protocol that were addressed to a multicast address at this sublayer
ifOutBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.5	Counter32	Number of packets requested by a higher-level protocol that were addressed to a broadcast address at this sublayer
ifHCInOctets	.1.3.6.1.2.1.31.1.1.1.6	Counter64	Number of octets received on the interface
ifHCInUcastPktss	.1.3.6.1.2.1.31.1.1.1.7	Counter64	Number of unicast packets delivered by the sublayer to a higher sublayer
ifHCInMulticastPkts	.1.3.6.1.2.1.31.1.1.1.8	Counter64	Number of multicast packets delivered by the sublayer to a higher sublayer
ifHCInBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.9	Counter64	Number of broadcast packets delivered by the sublayer to a higher sublayer
ifHCOutOctets	.1.3.6.1.2.1.31.1.1.1.10	Counter64	Number of octets sent from the interface

Table 8: Supported MIB objects (continued)

ifHCOutUcastPkts	.1.3.6.1.2.1.31.1.1.1.11	Counter64	Number of packets requested by a higher-level protocol that were addressed to a unicast address at this sublayer
ifHCOutMulticastPkts	.1.3.6.1.2.1.31.1.1.1.12	Counter64	Number of packets requested by a higher-level protocol that were addressed to a multicast address at this sublayer
ifHCOutBroadcastPkts	.1.3.6.1.2.1.31.1.1.1.13	Counter64	Number of packets requested by a higher-level protocol that were addressed to a broadcast address at this sublayer
ifLinkUpDownTrapEnable	.1.3.6.1.2.1.31.1.1.1.14	Integer	Indicates whether linkUp and linkDown traps are generated for the interface
ifHighSpeed	.1.3.6.1.2.1.31.1.1.1.15	Gauge32	Estimation of the interface's current bandwidth
ifPromiscuousMode	.1.3.6.1.2.1.31.1.1.1.16	TruthValue	Value of false (2) if the interface accepts only those packets or frames that are addressed to the interface. Value of true (1) if the interface accepts all packets and frames.
ifConnectorPresent	.1.3.6.1.2.1.31.1.1.1.17	TruthValue	Value of true (1) if the sublayer has a physical connector. Value of false (2) if the sublayer does not have a physical connector.
ifAlias	.1.3.6.1.2.1.31.1.1.1.18	DisplayString	Alias for the interface, as specified by the network manager
ifCounterDiscontinuityTime	.1.3.6.1.2.1.31.1.1.1.19	TimeStamp	Value of sysUpTime at the most recent occurrence of discontinuity for any of the interface's counters

Enterprise MIB Objects

Hardware Resource Threshold Monitoring MIB

The following table shows the hardware resources threshold monitoring MIB objects supported for SNMPwalk:

Trap Name and OID	Access	Description
extremeHWResourceUsage Table 1.3.6.1.4.1.1916.1.58.4.2	not-accessible	Table of L2/L3 hardware resources monitored for utilization.
extremeHWResourceUsage TableEntry 1.3.6.1.4.1.1916.1.58.4.2.1	not-accessible	Conceptual row within the extremeHWResourceUsage Table.
extremeHWResourceID 1.3.6.1.4.1.1916.1.58.4.2.1.1	not-accessible (INDEX)	Identifier for the hardware resource. Possible values include macAddressTable(0), vxlanTunnelTable(1), lifTable(2), bfdSession(3), bfdIPv4Session(4), bfdIPv6Session(5), ipv4Route(6), ipv6Route(7), routeTable(8), ipv4Host(9), ipv6Host(10), hostTable(11), nextHop(12), nextHopTable(13), ecmp(14), ecmpTable(15), routeHostTable(16), encapTable(17), resilientHashing(18), tcamMacIngress(19), tcamMacEgress(20), tcamIPv4Ingress(21), tcamIPv4Egress(22), tcamIPv6Ingress(23), and tcamIPv6Egress(24).
extremeHWResourceUsage HighLimit 1.3.6.1.4.1.1916.1.58.4.2.1.2	read-write	High threshold value for hardware resource usage.
extremeHWResourceUsage LowLimit 1.3.6.1.4.1.1916.1.58.4.2.1.3	read-write	Low threshold value for hardware resource usage.
extremeHWResourceUsage 1.3.6.1.4.1.1916.1.58.4.2.1.4	read-only	Current hardware resource utilization status: normal (0), high (1).

CPU and Memory Threshold Monitoring MIB

The following table shows the CPU and memory threshold monitoring MIB objects supported for SNMPwalk:

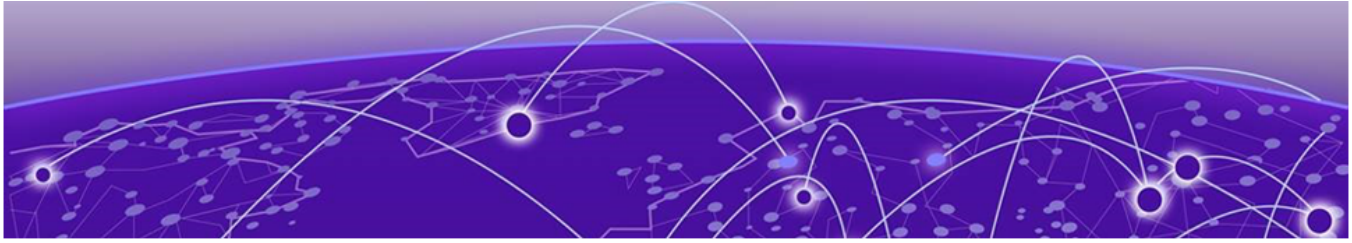
Trap Name and OID	Access	Description
swCpuUsage 1.3.6.1.4.1.1916.1.64.2.1.1	read-only	Current CPU usage of the system.
swCpuNoOfRetries 1.3.6.1.4.1.1916.1.64.2.1.2	read-only	Number of CPU usage samples taken before sending an SNMP trap.
swCpuUsageLimit 1.3.6.1.4.1.1916.1.64.2.1.3	read-only	CPU usage threshold limit.
swCpuPollingInterval 1.3.6.1.4.1.1916.1.64.2.1.4	read-only	Time interval between consecutive CPU usage samples.
swCpuAction 1.3.6.1.4.1.1916.1.64.2.1.5	read-only	Actions triggered when CPU usage exceeds the threshold: 0 - None, 1 - RAS Log, 2 - SNMP Trap, 3 - Both.
swMemUsage 1.3.6.1.4.1.1916.1.64.2.1.6	read-only	Current memory usage of the system.
swMemNoOfRetries 1.3.6.1.4.1.1916.1.64.2.1.7	read-only	Number of memory usage samples taken before sending an SNMP trap.

Extreme Temperature Sensor Table MIB

The following table shows the Extreme temperature sensor MIB objects:

Trap Name and OID	Access	Description
extremeTempSensorTable 1.3.6.1.4.1.1916.1.60.1.2	Not Accessible	This OID subtree defines the structure for temperature sensor data.
extremeTempSensorEntry 1.3.6.1.4.1.1916.1.60.1.2.1	Not Accessible	Each entry in the table represents a specific temperature sensor and its corresponding OID subtree.
extremeTempSensorDesc 1.3.6.1.4.1.1916.1.60.1.2.1.1	Read Only	Sensor Description: A brief description of the temperature sensor.

Trap Name and OID	Access	Description
extremeTempSensorGrid 1.3.6.1.4.1.1916.1.60.1.2.1.2	Read Only	Sensor Location: The physical location of the sensor on the grid. **Note:** Not applicable in Extreme OS ONE (always set to 0).
extremeTempSensorStatus 1.3.6.1.4.1.1916.1.60.1.2.1.3	Read Only	Sensor State: The current state of the sensor, which can be: • 0 (Normal) • 1 (Alarm) • 2 (Critical)
extremeTempSensorALThreshold 1.3.6.1.4.1.1916.1.60.1.2.1.4	Read Only	Alarm Threshold: The configured threshold for alarm triggers (returns -1 if not set).
extremeTempSensorCRThreshold 1.3.6.1.4.1.1916.1.60.1.2.1.5	Read Only	Critical Threshold: The configured threshold for critical triggers (returns -1 if not set).



Supported Traps - Extreme OS ONE Switching and Routing

Standard MIB Traps

The following generic traps are supported:

Use this topic to learn about the following standard MIB traps:

Traps	Description
coldstart (.1.3.6.1.6.3.1.1.5.1)	The coldStart trap is generated when the sending protocol entity undergoes reinitialization, potentially modifying the agent's configuration or the implementation of the protocol entity.
linkDown (.1.3.6.1.6.3.1.1.5.3)	The linkDown trap is triggered by the sending protocol entity upon detecting a failure in one of the communication links represented within the agent's configuration, indicating a loss of connectivity.
linkUp (.1.3.6.1.6.3.1.1.5.4)	A linkUp trap is generated when the sending protocol entity identifies that a communication link represented in the agent's configuration has become available.

LLDP MIB Traps

Trap Name and OID	Description
lldpRemTablesChange 1.0.8802.1.1.2.0.0.1	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be used by an NMS to trigger LLDP remote systems table maintenance polls. Note that transmission of lldpRemTablesChange notifications are throttled by the agent, as specified by the 'lldpNotificationInterval' object.

varbind	Description
lldpStatsRemTablesInserts 1.0.8802.1.1.2.1.2.2	Indicates the number of new neighbors.
lldpStatsRemTablesDeletes 1.0.8802.1.1.2.1.2.3	Indicates the number of neighbors that are deleted.
lldpStatsRemTablesDrops 1.0.8802.1.1.2.1.2.4	Indicates the number of neighbors that are discarded.
lldpStatsRemTablesAgeouts 1.0.8802.1.1.2.1.2.5	Indicates the number of neighbors that are aged.

BGP MIB Traps

BGP Standard-MIB notifications are sent for IPv4-type peers. The BGP Standard MIB specifies the following trap OID and associated Varbind list:

Trap Name and OID	Varbinds	Description
bgpEstablishedNotification 1.3.6.1.2.1.15.0.1	bgpPeerRemoteAddr bgpPeerLastError bgpPeerState	The bgpEstablishedNotification event is triggered when the BGP FSM transitions into the established state.
bgpBackwardTransNotification 1.3.6.1.2.1.15.0.2	bgpPeerRemoteAddr bgpPeerLastError bgpPeerState	The bgpBackwardTransNotification event is triggered when the BGP FSM transitions from a higher-numbered state to a lower-numbered state.

Enterprise MIB Traps

Use this topic to learn about the following MIB traps:

- Extreme Certificate MIB Traps on page 27
- Extreme User MIB Traps on page 27
- NTPv4-MIB Traps on page 29

Extreme Certificate MIB Traps

The Extreme Certificate MIB traps enable the configuration of traps for impending app certificate and CA certificate expirations. The feature supports four severity levels of traps. Traps are triggered when any server certificate stored on the device, linked to an application, is nearing expiration within a user-defined timeframe (specified in days).

For information on CLI command for the alert levels, see *Extreme OS ONE Switching Command Reference Guide*.

Only trap notifications are supported, Get or GetNext operations for MIB objects are not supported.

Trap Names and OIDs	Varbinds	Description
extremeCertExpiryWarning .1.3.6.1.4.1.1916.1.59.0.1	extremeCertSubject, extremeCertIssuerName, extremeCertSerialNumber, extremeCertValidNotAfterTime, extremeCertExpiryPendingDays, extremeCertExpiryAlertLevel	This notification is sent before a certificate expires, based on the configured certification expiry alert settings. The specific certificate (extremeCertName) can be identified by referencing the INDEX part of the notification's varbinds in the extremeCertTable.
extremeCertExpired .1.3.6.1.4.1.1916.1.59.0.2	extremeCertSubject, extremeCertIssuerName, extremeCertSerialNumber, extremeCertValidNotAfterTime, extremeCertExpiryExpiredDays	This notification is sent when a certificate has expired. The expired certificate (extremeCertName) can be identified by referencing the INDEX part of the notification's varbinds in the extremeCertTable.

Extreme User MIB Traps

Extreme User MIB traps enable you to configure traps for password expiry notifications. Four severity levels of traps are supported. For information on CLI command for the alert levels, see *Extreme OS ONE Switching Command Reference Guide*.

Only trap notifications are supported, Get or GetNext operations for MIB objects are not supported.

Trap Names and OID	Varbinds	Description
extremePaswdExpiryWarning 1.3.6.1.4.1.1916.1.61.0.1	extremeUserName extremePasswdExpiryDate extremePasswdExpiryPendingDays extremePasswdExpiryAlertLevel	This notification is sent before a user account's password expires, based on the global password expiry alert configuration.
extremePasswdExpiringToday 1.3.6.1.4.1.1916.1.61.0.2	extremeUserName extremePasswdExpiryDate	This notification is sent when a user account's password is set to expire today. It includes the following details: • **extremeUserName**: The name of the user account whose password is expiring. • **extremePasswdExpiryDate**: The exact date on which the password will expire.
extremePasswdExpired 1.3.6.1.4.1.1916.1.61.0.3	extremeUserName extremePasswdExpiryDate extremePasswdExpiryExpiredDays	This notification is sent when a user account's password has already expired. It includes the following information: • **extremeUserName**: The name of the user account with the expired password. • **extremePasswdExpiryDate**: The date on which the password expired. • **extremePasswdExpiryExpiredDays**: The number of days that have passed since the password expired.

Note

The following points describe the daily expiry checks and alerts:

- Daily Checks: User and certificate expiry checks run daily at 00:00 UTC, triggering alerts at this time.
- Startup Check : Expiry checks also occur when the security management system starts up.
- Alert Frequency:
  1. Warning alerts are sent only once on the configured alert day.
  2. Critical alerts (extremeCertExpired and extremePasswdExpired) are sent daily until the certificate is replaced or password is reset.
- Expiry Time Display:
  1. Certificate Expiry: extremeCertValidNotAfterTime:shows the exact date and time of certificate expiry.
  2. Password Expiry: extremePasswdExpiryDate displays expiry date with a time stamp of 00:00, as password expiry time granularity is not tracked.

NTPv4-MIB Traps

The following table describes the supported NTPv4-MIB traps. Get or GetNext for the MIB objects are not supported.

Trap Names and OIDs	Varbinds	Description
ntpEntNotifModeChange 1.3.6.1.2.1.197.0.1	ntpEntStatusCurrentMode	This notification is generated when the NTP entity changes mode such as not running, not synchronised.
ntpEntStatusCurrentMode 1.3.6.1.2.1.197.1.2.1	NA	The current mode of NTP, and is indicated by the following values: • notRunning(1) - NTP is inactive. • notSynchronized(2) - NTP is not synchronized with any time source. • noneConfigured(3) - NTP is unsynchronized and lacks a reference configured. • syncToLocal(4) - NTP is distributing time based on its local clock compromising accuracy and reliability. • syncToRefclock(5) - NTP is synchronized with a local hardware reference clock (for example, GPS). • syncToRemoteServer(6) - NTP is synchronized with a remote upstream NTP server. • unknown(99) - The NTP state is unknown.

Extreme System Sensor MIB

The Extreme System Sensor Notification MIB Objects are supported.

The following table describes Extreme System Sensor Notification MIB Objects:

Trap name and OID	Varbinds	Description
extremeTempSensorStatusChange 1.3.6.1.4.1.1916.1.60.0.1	extremeTempSensorTransitionEvent extremeTempSensorAggrStatus	A notification is triggered whenever a temperature sensor's status changes to normal, alarm, or critical.

The following table describes Extreme Temperature Sensor Objects:

Varbinds	Access	Description
extremeTempSensorAggrStatus 1.3.6.1.4.1.1916.1.60.1.1	Accessible for Notify	**Aggregate Temperature Sensor Status** This value encodes the state of multiple temperature sensors, with each sensor occupying 4 bits. **Encoding Scheme** Byte 1: Sensor 1 (most significant nibble), Sensor 2 (least significant nibble) Byte 2: Sensor 3 (most significant nibble), Sensor 4 (least significant nibble) **Handling Odd Number of Sensors** If there's an odd number of sensors, the last nibble is padded with zeros (0x0000). The nibbles are set as follows: • 0x0000 - for normal state • 0x0001 - for alarm state • 0x0010 - for critical state
extremeTempSensorTransitionEvent 1.3.6.1.4.1.1916.1.60.1.3	Accessible for Notify	This MIB specifies the temperature sensor state transition that triggers the extremeTempSensorStatusChange notification. The values for each state change are: • 1 - Normal to Alarm • 2 - Alarm to Critical • 3 - Normal to Critical • 4 - Critical to Alarm • 5 - Alarm to Normal • 6 - Critical to Norma

CPU and Memory Utilization - MIB Traps

Object Name and OID	Varbind	Description
swCpuRisingThresholdNotification 1.3.6.1.4.1.1916.1.64.1.1.0.16	swCpuUsage swCpuUsageLimit swCpuNoOfRetries swCpuPollingInterval	Trigger a notification when CPU usage surpasses the set threshold.
swCpuFallingThresholdNotification 1.3.6.1.4.1.1916.1.64.1.1.0.17	swCpuUsage swCpuUsageLimit swCpuNoOfRetries swCpuPollingInterval	Trigger a notification when CPU usage falls to or below the specified threshold.
swMemRisingThresholdNotification 1.3.6.1.4.1.1916.1.64.1.1.0.18	swMemUsage swMemUsageLimit swMemNoOfRetries swMemPollingInterval	Trigger a notification when memory usage surpasses the set threshold.
swMemFallingThresholdNotification 1.3.6.1.4.1.1916.1.64.1.1.0.19	swMemUsage swMemUsageLimit swMemNoOfRetries swMemPollingInterval	Trigger a notification when memory usage falls to or below the specified limit.

Extreme Threshold Monitoring MIB Traps

The following table shows the SNMP threshold monitoring MIB notifications:

Trap Name and OID	Varbinds	Description
ExtremeHWResourceUsageAlert 1.3.6.1.4.1.1916.1.58.0.2	extremeHWResourceOverallUsage	This notification is generated when the monitored resource usages exceeds the configured high threshold level or falls below the low threshold level. The number of notifications that are generated for a particular time period is configured globally. The total number of generated notifications cannot exceed this configuration.

Extreme ONE MLAG MIB

The following traps are generated when peer is Up or Down:

Trap Names and OIDs	Varbinds
extremeMlagPeerDownTrap 1.3.6.1.4.1.1916.1.63.0.1	• extremeMlagPeerAddr: Peer address • extremeMlagPeerAddrType: Peer address type • sysName: The local host name assigned for this switch
extremeMlagPeerUpTrap 1.3.6.1.4.1.1916.1.63.0.2	• extremeMlagPeerAddr: Peer address • extremeMlagPeerAddrType: Peer address type • sysName: The local host name assigned for this switch

BFD Enterprise MIB

The following trap notifications are supported. Get/GetNext are not supported for this MIB.

Trap Name and OID	Varbind	Description
`extremeBfdSessUp` 1.3.6.1.4.1.1916.1.55.0.1	bfdSessDiag bfdSessInterface bfdSessSrcAddrType bfdSessSrcAddr bfdSessDstAddrType bfdSessDstAddr ifName extremeBfdVrfName	A notification is generated when the `bfdSessState` object for one of the entries in `bfdSessTable` is about to enter the up (4) state from some other state. The value of `bfdSessDiag` is set equal to `noDiagnostic` (0).
`extremeBfdSessDown` 1.3.6.1.4.1.1916.1.55.0.2	bfdSessDiag bfdSessInterface bfdSessSrcAddrType bfdSessSrcAddr bfdSessDstAddrType bfdSessDstAddr ifName extremeBfdVrfName	A notification is generated when the `bfdSessState` object for one of the entries in `bfdSessTable` is about to enter the down (2) or adminDown (1) state from some other state. The values of `bfdSessDiag` returns the Diagnostic code providing the reason for the new state (for example, pathDown (5)).

BGP Enterprise MIB

The BGP Enterprise MIB notifications are sent for the **peers of IPv6 types**. The BGP Enterprise MIB defines the following trap OIDs and Varbind:

extremeBGP4V2EstablishedNotification: An extremeBGP4V2EstablishedNotification event is generated when the BGP FSM enters the established state.

extremeBGP4V2BackwardTransitionNotification: An extremeBGP4V2BackwardTransitionNotification event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

Trap Name and OID	Varbinds	Description
extremeBGP4V2EstablishedNotification 1.3.6.1.4.1.1916.1.51.0.1	extremeBgp4V2PeerState extremeBgp4V2PeerLocalPort extremeBgp4V2PeerRemotePort extremeBgp4V2PeerRemoteAddr	The event is triggered when the BGP FSM reaches the established state.
extremeBGP4V2BackwardTransitionNotification 1.3.6.1.4.1.1916.1.51.0.2	extremeBgp4V2PeerState extremeBgp4V2PeerLocalPort extremeBgp4V2PeerRemotePort extremeBgp4V2PeerLastErrorCodeReceived extremeBgp4V2PeerLastErrorSubCodeReceived extremeBgp4V2PeerLastErrorReceivedText extremeBgp4V2PeerRemoteAddr	The event is triggered when the BGP FSM transitions from a higher-numbered state to a lower-numbered state.

Maintenance Mode MIB

Trap Name and OID	Varbind	Description
extremeMaintenanceModeEntryTrap 1.3.6.1.4.1.1916.1.57.0.1	extremeMaintenanceModeConvergenceStatus extremeMaintModeReasonCode sysName	A trap is generated when the switch enters the maintenance mode
extremeMaintenanceModeExitTrap 1.3.6.1.4.1.1916.1.57.0.2	extremeMaintenanceModeConvergenceStatus extremeMaintModeReasonCode sysName	A trap is generated when the switch exits from the maintenance mode.

Varbinds	Access	Description
extremeMaintenanceModeConvergenceStatus 1.3.6.1.4.1.1916.1.57.1	Accessible-for-notify	This object indicates the convergence status at the time of trap generation, with the following states: 1. **Completed (1):** Convergence finished within the expected time. Default is 90 secs, which is configurable. 2. **Timed Out (2):** Convergence took longer than the expected convergence time.
extremeMaintModeReasonCode 1.3.6.1.4.1.1916.1.57.2	Accessible-for-notify	This object indicates the reason for entering or exiting maintenance mode, with the following states: 1. **User Action (1):** Maintenance mode is triggered immediately by a user. 2. **On Switch Reboot (2):** The switch enters maintenance mode during reboot, as specified in the startup configuration (enable-on-reboot).

Traps after Device Reload

When a device reloads, interfaces (management or inband) take time to become operational.

To ensure SNMP traps are delivered successfully once interfaces are up, a retry mechanism is implemented for the following traps:

1. Coldstart traps
2. Device boot-up traps

The retry mechanism may cause a delay (approximately 60 seconds) between the trap event occurrence and delivery to recipient hosts.