AOS-CX 10.09 SNMP/MIB Guide

All AOS-CX Series Switches

a Hewlett Packard Enterprise company

Published: April 2022
Edition: 4

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Chapter 1
About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products

This document applies to the following products:

- Aruba 4100i Switch Series (JL817A, JL818A)
- Aruba 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A)
- Aruba 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)
- Aruba 6200 Switch Series (JL724A, JL725A, JL726A, JL727A, JL728A)
- Aruba 6300 Switch Series (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A, JL665A, JL666A, JL667A, JL668A, JL762A)
- Aruba 6400 Switch Series (JL741A, R0X26A, R0X27A, R0X29A, R0X30A)
- Aruba 8320 Switch Series (JL479A, JL579A, JL581A)
- Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- Aruba 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL704C, JL705C, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL717C, JL718C)
- Aruba 8400 Switch Series (JL375A, JL376A)
- Aruba 10000 Switch Series (R8P13A, R8P14A)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in Support and Other Resources.

Command syntax notation conventions

Convention	Usage
`example-text`	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (`[ ]`).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *example-text*	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are

Convention	Usage
▪ *example-text*	enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value. ▪ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
|	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[ ]	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ▪ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ▪ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term `switch`, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

```
switch(CONTEXT-NAME)#
```

Indicates the configuration context for a feature. For example:

```
switch(config-if)#
```

Identifies the `interface` context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100)#
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>)#
```

Where *<VLAN-ID>* is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:
member/slot/port

On the 4100i Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on the switch.

On the 6000 and 6100 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on the switch.

On the 6200 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 8. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 in slot 1 on member 1.

On the 6300 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on member 1.

On the 6400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- *port*: Physical number of a port on a line module.

For example, the logical interface `1/3/4` in software is associated with physical port 4 in slot 3 on member 1.

On the 83xx and 10000 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on the switch.

If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split to 4 x 10G or 4 x 25G. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

On the 8400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/5 and 1/6.
  - Line modules are on the front of the switch in slots 1/1 through 1/4, and 1/7 through 1/10.
- *port*: Physical number of a port on a line module

For example, the logical interface `1/1/4` in software is associated with physical port 4 in slot 1 on member 1.

Identifying modular switch components

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: *member/power supply*:
  - *member*: 1.
  - *power supply*: 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: *member/tray/fan*:
  - *member*: 1.
  - *tray*: 1 to 4.
  - *fan*: 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: *member/module*:
  - *member*: 1.
  - *member*: 1 or 2.
- The display module on the rear of the switch is not labeled with a member or slot number.

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and monitoring the devices connected to a network by collecting, organizing and modifying information about managed devices on IP networks.

SNMP write: PoE write capabilities

PoE enable

The PoE enable is requested through SNMP to enable the PoE interface. The `admin_disable` SNMP value is updated to enable the PoE interface.

PoE disable

The PoE disable is requested through SNMP to disable the PoE interface. The `admin_disable` SNMP value is updated to disable the PoE interface.

PoE cycle

The PoE cycle is a feature where you can request a PoE port reset with a timeout ranging from 1 to 60 seconds. The PoE cycle is requested through the SNMP server to disable and enable a PoE interface with an input timeout of 1 to 60 seconds. The PoE handles the PoE disable and enable events when the SNMP value is updated for `admin_disable` correspondingly. The value of timeout ranges from 1-60 seconds. It is a one-time operation.

SNMP traps

Event log traps

When SNMP is configured, interface daemons event log messages for link-up and link-down events will be sent as traps.

Event log trap OID: 1.3.6.1.4.1.47196.4.1.1.3.4.1.1

Parameter	OID	Description
`sysUpTimeInstance`	1.3.6.1.2.1.1.3.0	Contains the uptime for the system in centiseconds
`snmpTrapOID`	1.3.6.1.6.3.1.1.4.1	Contains the OID for the event log trap
`eventIndex`	1.3.6.1.2.1.16.9.1.1.1	Contains an index that uniquely identifies an event
`eventDescription`	1.3.6.1.2.1.16.9.1.1.2	Contains the event log message

Link-up and link-down traps

Standard IF-MIB link-up and link-down traps will be sent on link-state change when an interface is configured using `trap link-status` or when `user_config:link_state_snmp_trap` is set to true. The trap sends the current information for ifindex, admin status, operational status, and interface name.

Link up trap OID: 1.3.6.1.6.3.1.1.5.4

Link down trap OID: 1.3.6.1.6.3.1.1.5.3

Parameter	OID	Description
`sysUpTimeInstance`	1.3.6.1.2.1.1.3.0	Contains the uptime for the system in centiseconds
`snmpTrapOID`	1.3.6.1.6.3.1.1.4.1	Contains the OID for the link up or linkdown trap
`ifIndex`	1.3.6.1.2.1.2.2.1.1.X	Contains the ifindex for the interface
`ifAdminStatus`	1.3.6.1.2.1.2.2.1.7.X	Contains the admin status for the interface
`ifOperStatus`	1.3.6.1.2.1.2.2.1.8.X	Contains the operational status for the interface
`ifDescr`	1.3.6.1.2.1.2.2.1.2.X	Contains the name for the interface

Configuring SNMP

SNMP agent provides read-write access for specific OIDs. Refer OIDs that supports SNMP write for the list of OIDs that supports write operations.

Procedure

1. SNMP is not enabled on the switch by default, unless the user enables it over any available VRF or with the `default`/`mgmt` VRF using the command `snmp-server vrf <NAME>`. For example, use the command `snmp-server vrf mgmt` to enable SNMP on the management interface. Use the command `snmp-server vrf default` to enable SNMP on the default VRF. Use the command `snmp-server vrf <USERDEFINED_VRF_NAME>` to enable SNMP on the user created VRF.
2. Set the system contact, location, and description for the switch with the following commands:
   - `snmp-server system-contact`
   - `snmp-server system-location`
   - `snmp-server system-description`

You can also set the system location and system contact values using SNMP.

3. If required, change the default SNMP port on which the agent listens for requests with the command `snmp-server agent-port`.
4. By default, the agent uses the community string **public** to protect access through SNMPv1/v2c. Set a new community string with the command `snmp-server community`.
5. Configure the trap receivers to which the SNMP agent will send trap notifications with the command `snmp-server host`.
6. Create an SNMPv3 context and associate it with any available SNMPv3 user to perform context specific v3 MIB polling using the command `snmpv3 user <V3_USERNAME> context <CONTEXT_NAME>`.

7. Create an SNMPv3 context and associate it with an available SNMPv1/v2c community string to perform context specific v1/v2c MIB polling using the command `snmpv3 context <CONTEXT_NAME> vrf <VRF_NAME> community <COMMUNITY_NAME>`.
8. Review your SNMP configuration settings with the following commands:
   - `show snmp agent-port`
   - `show snmp community`
   - `show snmp system`
   - `show snmpv3 context`
   - `show snmp trap`
   - `show snmp vrf`
   - `show snmpv3 users`
   - `show tech snmp`

Example 1

This example creates the following configuration:

- Enables SNMP on the out-of-band management interface (VRF **mgmt**).
- Sets the contact, location, and description for the switch to: **JaniceM**, **Building2**, **LabSwitch**.
- Sets the community string to **Lab8899X**.

```
switch(config)# snmp-server vrf mgmt
switch(config)# snmp-server system-contact JaniceM
switch(config)# snmp-server system-location Building2
switch(config)# snmp-server system-description LabSwitch
switch(config)# snmp-server community Lab8899X
```

Example 2

This example creates the following configuration:

- Creates an SNMPv3 user named **Admin** using **sha** authentication with the plaintext password **mypassword** and using **des** security with the plaintext password **myprivpass**.
- Associates the SNMPv3 user `Admin` with a context named `newContext`.

```
switch(config)# snmpv3 user Admin auth sha auth-pass plaintext mypassword priv des
     priv-pass plaintext myprivpass
switch(config)# snmpv3 user Admin context newContext
```

SNMP commands

event-trap-enable

```
event-trap-enable
no event-trap-enable
```

Description

Enables the notification of events to be sent as traps to the SNMP management stations. It is enabled by default.

The `no` form of this command disables the event traps.

Examples

Enabling the event traps:

```
switch(config)# event-trap-enable
```

Disabling the event traps:

```
switch(config)# no event-trap-enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

lldp trap enable

```
lldp trap enable
no lldp trap enable
```

Description

Enables sending SNMP traps for LLDP related events from a particular interface. LLDP trap generation is enabled by default on all the interfaces and has to be disabled for interfaces on which traps are not required to be generated.

The `no` form of this command disables the LLDP trap generation.

LLDP trap generation is disabled by default at the global level and must be enabled before any LLDP traps are sent.

Examples

Enabling LLDP trap generation on global level:

```
switch(config)# lldp trap enable
```

Enabling LLDP trap generation on interface level:

```
switch(config-if)# lldp trap enable
```

Disabling LLDP trap generation on global level:

```
switch(config)# no lldp trap enable
```

Disabling LLDP trap generation on interface level:

```
switch(config-if)# no lldp trap enable
```

Displaying LLDP global configuration:

```
switch# show lldp configuration


LLDP Global Configuration
=========================
LLDP Enabled                 : No
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : No


TLVs Advertised
===============
Management Address
Port Description
Port VLAN-ID
System Description
System Name

LLDP Port Configuration
=======================
PORT           TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-------------------------------------------------------------------------
1/1/1          Yes                 Yes                 Yes
1/1/2          Yes                 Yes                 Yes
1/1/3          Yes                 Yes                 Yes
1/1/4          Yes                 Yes                 Yes
1/1/5          Yes                 Yes                 Yes
1/1/6          Yes                 Yes                 Yes
...........
...........
mgmt           Yes                 Yes                 Yes
```

Displaying LLDP Configuration for the interface:

```
switch# show lldp configuration 1/1/1

LLDP Global Configuration
=========================
LLDP Enabled                 : Yes
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : No
```

```
LLDP Port Configuration
=======================
PORT           TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-------------------------------------------------------------------------------
1/1/1          Yes                 Yes                 Yes
```

Displaying LLDP Configuration for the management interface:

```
switch# show lldp configuration mgmt

LLDP Global Configuration
=========================
LLDP Enabled                 : Yes
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : Yes


LLDP Port Configuration
=======================
PORT           TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-------------------------------------------------------------------------------
mgmt           Yes                 Yes                 Yes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` and `config-if`	Administrators or local user group members with execution rights for this command.

mac-notify traps

```
mac-notify traps {aged | learned | moved | removed}
no mac-notify traps {aged | learned | moved | removed}
```

Description

Configures a Layer 2 interface to generate SNMP trap notifications for up to four different types of dynamic MAC address related events on the trunk or access in physical or lag interfaces.

The `no` form of this command removes the traps from the interface.

Parameter	Description
`aged`	Notifies when a MAC address aged out on the interface.
`learned`	Notifies when a MAC address is learned on the interface.
`moved`	Notifies when a MAC address moved from the interface.
`removed`	Notifies when a MAC address is removed from the interface.

MAC notification trap addition to or removal from an interface can be in any combination, quantity, or order. The addition of existing configured traps or removal of non-configured traps will be accepted and ignored.

The mac-notify feature must be enabled globally for any interface configurations to generate SNMP traps.

MAC notification cannot be configured on a Layer 3 (routing) interface. A Layer 2 interface that is changed to a Layer 3 interface through the `routing` command will discard any existing MAC notification configurations.

Usage

The following are the limitation for SNMP MAC notify traps:

- SNMP MAC change notification trap is not supported for VxLAN – Overlay hosts.
- Mac notify trap will not generate for Static MACs.
- `vsx-sync` is not supported for this feature. Hence, you must enable the MAC notify traps explicitly on secondary to ensure the traps are generated.
- MAC notification trap events are not generated for the Port-Access-Security MACs.

Examples

MAC notification types and the associated events only apply to Layer 2 interfaces, hence routing might need to be disabled on the relevant interfaces.

Enabling the traps on an L2 interface:

```
switch(config)# interface 1/1/1
switch(config-if)# mac-notify traps learned
1/1/1 is not an L2 port
switch(config-if)# no routing
switch(config-if)# mac-notify traps learned removed
switch(config-if)# mac-notify traps aged
```

```
switch(config)# interface lag101
switch(config-if)# mac-notify traps removed
```

Disabling the `learned` and `removed` traps from the interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no mac-notify traps learned removed
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command. Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

rmon alarm

```
rmon alarm index <INDEX> snmp-oid <SNMP-OID> rising-threshold <RISING-THRESHOLD>
     falling-threshold <FALLING-THRESHOLD> [sample-interval <SAMPLE-INTERVAL>] [sample-type
<ABSOLUTE|DELTA>]
no rmon alarm [index <INDEX>]
```

Description

Stores configuration entries in an alarm table that defines the sample interval, sample-type, and threshold parameters for an SNMP MIB object. Only the SNMP MIB objects that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge32, or TimeTicks) will be monitored.

The `no` form of this command removes all RMON alarms and allows you to specify an index to remove a particular RMON alarm.

Parameter	Description
`index <INDEX>`	Specifies the RMON alarm index. Range: 1 to 20.
`snmp-oid <SNMP-OID>`	Specifies the SNMP MIB object to be monitored by RMON.
`rising-threshold <RISING-THRESHOLD>`	Specifies the upper threshold value for the RMON alarm.
`falling-threshold <FALLING-THRESHOLD>`	Specifies the falling threshold value for the RMON alarm. The falling threshold must be less than the rising threshold.
`sample-interval <SAMPLE-INTERVAL>`	Sample interval in seconds. Default: 30.
`sample-type <ABSOLUTE|DELTA>`	Specifies the method of sampling of the SNMP MIB object. Default: Absolute.

Examples

Configuring RMON for the MIB object **ifOutErrors.15** with an index **1**, rising threshold of **2147483647** and falling threshold of **-2134** using **absolute** sampling for a sample interval of **100** seconds:

```
switch(config)# rmon alarm index 1 snmp-oid ifOutErrors.15 rising-threshold
2147483647
     falling-threshold -2134 sample-type absolute sample-interval 100
```

Removing RMON alarm with the index 5:

```
switch(config)# no rmon alarm index 5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

rmon alarm {enable | disable} {index | all}

```
rmon alarm {enable | disable} {index <INDEX> | all}
no rmon alarm [enable | disable] [index <INDEX> | all]
```

Description

Enables and disables the RMON alarm and its index. RMON alarm is enabled by default.

Parameter	Description
`enable`	Enables the RMON alarm index
`disable`	Disables the RMON alarm index.
`index <INDEX>`	Specifies the RMON alarm index. Range: 1 to 20.
`all`	Specifies all the RMON alarms.

Examples

Enabling or disabling all the RMON alarm:

```
switch(config)# rmon alarm enable all
switch(config)# rmon alarm disable all
```

Enabling or disabling RMON alarm by index:

```
switch(config)# rmon alarm enable index 1
switch(config)# rmon alarm disable index 1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

show mac-notify

`show mac-notify`

Description

Displays whether the MAC notification feature in the SNMP module is enabled or not. It also displays the trap notification types configured on the Layer 2 ports in the system.

Examples

Showing the MAC notification configuration on all configured ports in the system:

```
switch# show mac-notify

MAC notification global setting : Enabled

Port         Enabled Traps
---------------------------------------
1/1/1        aged learned moved
1/1/5        moved
lag101       removed
lag104       aged learned moved removed
...
...
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-notify port

```
show mac-notify [port <PORTS>]
```

Description

Displays the MAC notification configuration on a range of ports.

Parameter	Description
`[port <PORTS>]`	Specifies a port, range of ports, or list of ports.

Examples

Showing the MAC notification configuration on a range of ports:

```
switch(config)# show mac-notify port 1/1/1,1/1/3,1/1/5,lag101-lag104

MAC notification global Setting: Enabled

Port         Enabled Traps
-------------------------------------
1/1/1        aged learned moved
1/1/3        --
1/1/5        moved
lag101       removed
lag102       --
lag103       --
lag104       aged learned moved removed
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show rmon alarm

```
show rmon alarm [index <INDEX>]
```

Description

Displays the RMON alarm configurations.

Parameter	Description
`index <INDEX>`	Specifies the RMON alarm index. Range: 1 to 20.

Examples

Showing all RMON alarm configurations:

```
switch# show rmon alarm
Index               : 1
Enabled             : true
Status              : valid
MIB object          : ifOutErrors.15
Sample type         : delta
Sampling interval   : 6535 seconds
Rising threshold    : 100
Falling threshold   : 10
Last sampled value  : 0
Last sample time    : 2020-09-21 05:58:11

Index               : 3
Enabled             : true
Status              : invalid
MIB object          : IF-MIB::ifDescr.19
Sample type         : absolute
Sampling interval   : 10000 seconds
Rising threshold    : 4000
Falling threshold   : 10
Last sampled value  : 0
```

Showing RMON alarm with alarm index 1:

```
switch# show rmon alarm index 1
Index               : 1
Enabled             : true
Status              : valid
MIB object          : ifOutErrors.15
Sample type         : delta
Sampling interval   : 6535 seconds
Rising threshold    : 100
Falling threshold   : 10
Last sampled value  : 0
Last sample time    : 2020-06-21 05:58:11
```

Showing disabled RMON alarm information:

```
switch# show  rmon   alarm
Index               : 1
Enabled             : false
Status              : valid
MIB object          : ifOutErrors.15
Sample type         : delta
Sampling interval   : 6535 seconds
Rising threshold    : 100
Falling threshold   : 10
Last sampled value  : 0
Last sample time    : 2020-09-21 05:58:11

Index               : 3
Enabled             : false
Status              : invalid
MIB object          : IF-MIB::ifDescr.19
Sample type         : absolute
Sampling interval   : 10000 seconds
Rising threshold    : 4000
```

```
Falling threshold  : 10
Last sampled value : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

show snmp agent-port

```
show snmp agent-port
```

Description

Displays SNMP agent UDP port number.

Example

Displaying SNMP agent UDP port number:

```
switch# show snmp agent-port
SNMP agent port : 161
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp community

```
show snmp community
```

Description

Displays a list of all configured SNMPv1/v2c communities.

Usage

When a user creates a custom community before enabling an SNMP agent, AOS-CX automatically removes the default `public` community from the system.

Example

Displaying a list of all configured SNMPv1/v2c communities:

```
switch#show snmp community

SNMP-COMMUNITIES

------------------------------------------------------------------------------
Community                          Access-level  ACL Name    ACL Type
------------------------------------------------------------------------------
private                              ro          my_acl      ipv4
private                              ro          my_acl      ipv6
private2                             rw          new_Acl     ipv6
private3                             rw          none        none
```

Release	Modification
10.08	Added *ACL Type* column to the command output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show snmp system

`show snmp system`

Description

Displays SNMP description, location, and contact information.

Example

Displaying SNMP description, location, and contact information:

```
switch# show snmp system
SNMP system information
---------------------------
System description : Aggregation router
System location : Main lab
System contact : John Smith, Lab Admin
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp trap

```
show snmp trap
```

Description

Displays all configured SNMP traps/informs receivers.

Example

Displaying all configured SNMP trap and informs receivers:

```
switch# show snmp trap
HOST                                    PORT   TYPE    VER COMMUNITY/USER NAME VRF
--------------------------------------------------------------------------------
10.10.10.10                             162    trap    v1  public              default
10.10.10.10                             162    inform  v2c public              default
10.10.10.10                             162    inform  v3  name                default
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp vrf

```
show snmp vrf
```

Description

Displays the VRF on which the SNMP agent service is running.

Example

Displaying SNMP services enabled on VRF:

```
switch#show snmp vrf
SNMP enabled VRF
----------------------------
mgmt
default
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 context

```
show snmpv3 context
```

Description

Displays all configured SNMP contexts.

Examples

Displaying all configured SNMP contexts:

```
switch# show snmpv3 context
------------------------------------------------------------------------------
name                            vrf                              community
------------------------------------------------------------------------------
contextA                        default                          private
contextB                        vrf_A                            public
```

```
switch# show snmpv3 context
------------------------------------------------------------------------------
Name           vrf             Community          ype[Instance_id]
-----------------------------------------------------------------
A              default         public             vrf
switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 engine-id

```
show snmpv3 engine-id
```

Description

Displays the configured SNMPv3 snmp engine-id.

If the SNMPv3 engine-id is not configured, by default a unique engine-id is created by the switch using a combination of the enterprise OID value and the switch's mac address.

Example

Displaying the configured SNMPv3 engine-id:

```
switch# show snmpv3 engine-id
SNMP engine-id : 80:00:B8:5C:08:00:09:1d:de:a5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 security-level

```
show snmpv3 security-level
```

Description

Displays the configured SNMPv3 security level.

Examples

Displaying the configured SNMPv3 security level:

```
switch# show snmpv3 security-level
SNMPv3 security-level : auth
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 users

```
show snmpv3 users
```

Description

Displays all configured SNMPv3 users.

For more details on the user enabled status, see snmpv3 security-level.

Example

Displaying all configured SNMPv3 users:

```
switch# show snmpv3 users
------------------------------------------------------------------------
User                            AuthMode  PrivMode  Context  Enabled
------------------------------------------------------------------------
name                            md5       none      none     False
name2                           sha       aes       none     True
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

snmp-server agent-port

```
snmp-server agent-port <PORT>
no snmp-server agent-port [<PORT>]
```

Description

Sets the UDP port number that the SNMP master agent uses to communicate. UDP port 161 is the default port.

The `no` form of this command sets the SNMP master agent port to the default value.

Parameter	Description
<PORT>	Specifies the UDP port number that the SNMP master agent will use. Range: 1 to 65535. Default: 161.

Examples

Setting the SNMP master agent port to **2000**:

```
switch(config)# snmp-server agent-port 2000
```

Resetting the SNMP master agent port to the default value:

```
switch(config-schedule)# no snmp-server agent-port 2000
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server community

```
snmp-server community <STRING>
no snmp-server community <STRING>
```

Description

Adds an SNMPv1/SNMPv2c community string. A community string is like a password that controls read/write access to the SNMP agent. A network management program must supply this name when attempting to get SNMP information from the switch. A maximum of 10 community strings are supported. Once you create your own community string, the default community string (`public`) is deleted.

The `no` form of this command removes the specified SNMPv1/SNMPv2c community string. When no community string exists, a default community string with the value `public` is automatically defined.

Parameter	Description
<STRING>	Specifies the SNMPv1/SNMPv2c community string. Range: 1 to 32 printable ASCII characters, excluding space and question mark.

Subcommands

```
access-level {ro | rw}
no access-level {ro | rw}
```

This subcommand changes the access level of the SNMP community. The default access level is read-only (`ro`).

The `no` form of this subcommand changes the access level of the community to default.

Parameter	Description
`ro`	Specifies Read-Only access with the SNMP community.
`rw`	Specifies Read-Write access with the SNMP community.

```
access-list {ipv4 | ipv6} <ACL-NAME>
no access-list {ipv4 | ipv6} <ACL-NAME>
```

This subcommand associates an ACL with the SNMP community. If an ACL is not associated with the SNMP community, the default access is allowed for all the hosts.

The `no` form of this subcommand removes association of the ACL with the SNMP community.

Parameter	Description
`ipv4`	Specifies the IPv4 ACL type.
`ipv6`	Specifies the IPv6 ACL type.
<ACL-NAME>	Specifies the ACL name. It supports a maximum of 64 characters.

Examples

Setting the SNMPv1/SNMPv2c community string to **private**:

```
switch(config)# snmp-server community private
```

Removing SNMPv1/SNMPv2c community string **private**:

```
switch(config)# no snmp-server community private
```

Configuring the access level for the SMNP community to read-only:

```
switch(config-community)# access-level ro
```

Changing the access level of the SNMP community to default:

```
switch(config-community)# no access-level rw
```

Associating an IPv4 ACL named **my_acl** with the SMNP community:

```
switch(config-community)# access-list ipv4 my_acl
```

Removing the associated IPv4 ACL named **my_acl** from the SNMP community:

```
switch(config-community)# no access-list ipv4 my_acl
```

The `deny` rule is not supported for SNMP ACL.

Configuration supported for SNMP ACL:

```
access-list ip ipv4_acl
    10 permit any 4.4.4.4 4.4.4.1
    20 permit any 3.3.3.3 3.3.3.1
access-list ipv6 ipv6_acl
    10 permit any 2001::2 2001::1
    20 permit any 3001::2 3001::1
snmp-server vrf default
snmp-server community my_comm_1
    access-list ipv4 ipv4_acl
    access-list ipv6 ipv6_acl
```

Configuration not supported for SNMP ACL:

```
access-list ip ipv4_acl
    10 deny any 6.6.6.6 6.6.6.1
access-list ipv6 ipv6_acl
    10 deny any 6001::6 6000::1
snmp-server vrf default
snmp-server community my_comm_1
    access-list ipv4 ipv4_acl
    access-list ipv6 ipv6_acl
```

`hitcounts` for SNMP ACL will not be incremented.
Example:`show access-list hitcounts ip all` will not show the hit count of SNMP ACL.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` `config-community`	Administrators or local user group members with execution rights for this command.

snmp-server historical-counters-monitor

```
snmp-server historical-counters-monitor
no snmp-server historical-counters-monitor
```

Description

Enables the Remote Network Monitoring agent (rmond) to start collecting historical interface statistics. The no form of this command stops the historical interface statistics collection.

Example

Enabling the rmond agent to start historical interface statistics collection:

```
switch(config)# snmp-server historical-counters-monitor
```

Disabling the rmond agent to stop historical interface statistics collection:

```
switch(config)# no snmp-server historical-counters-monitor
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

snmp-server host

```
snmp-server host <IPv4-ADDR | IPv6-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>]

snmp-server host <IPv4-ADDR | IPv6-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>]

snmp-server host <IPv4-ADDR | IPv6-ADDR> [trap version v3 | inform version v3] user <NAME>
[port <UDP-PORT>] [<VRF-NAME>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> [trap version v3 | inform version v3] user
<NAME>
[port <UDP-PORT>] [<VRF-NAME>]
Description
```

Configures a trap/informs receiver to which the SNMP agent can send SNMP v1/v2c/v3 traps or v2c informs. A maximum of 30 SNMP traps/informs receivers can be configured.

The no form of this command removes the specified trap/inform receiver.

Parameter	Description
<IPv4-ADDR>	Specifies the IP address of a trap receiver in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can

Parameter	Description
	remove leading zeros. For example, the address `192.169.005.100` becomes `192.168.5.100`.
<IPv6-ADDR>	Specifies the IP address of a trap receiver in IPv6 format (`x:x::x:x`).
`trap version` *<VERSION>*	Specifies the trap notification type for SNMPv1, v2c or v3. Available options are: `v1`, `v2c` or `v3`.
`inform version v2c`	Specifies the inform notification type for SNMPv2c.
`trap version v3`	Specifies the trap notification type for SNMPv3.
`user` *<NAME>*	Specifies the SNMPv3 user name to be used in the SNMP trap notifications.
`community` *<STRING>*	Specifies the name of the community string to use when sending trap notifications. Range: 1 - 32 printable ASCII characters, excluding space and question mark. Default: `public`.
<UDP-PORT>	Specifies the UDP port on which notifications are sent. Range: 1 - 65535. Default: 162.
<VRF-NAME>	Specifies the VRF on which the SNMP agent listens for incoming requests.

Examples

```
switch(config)# snmp-server host 10.10.10.10 trap version v1
switch(config)# no snmp-server host 10.10.10.10 trap version v1
switch(config)# snmp-server host a:b::c:d trap version v1
switch(config)# no snmp-server host a:b::c:d trap version v1
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
switch(config)# snmp-server host a:b::c:d trap version v2c community public
switch(config)# no snmp-server host a:b::c:d trap version v2c community public
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public port
5000
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public port
5000 vrf default
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
port 5000 vrf default
switch(config)# snmp-server host a:b::c:d trap version v2c community public port
5000
switch(config)# no snmp-server host a:b::c:d trap version v2c community public port
5000
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public
switch(config)# snmp-server host a:b::c:d inform version v2c community public
switch(config)# no snmp-server host a:b::c:d inform version v2c community public
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
port 5000
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
port 5000 vrf default
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community public
```

```
port 5000 vrf default
switch(config)# snmp-server host a:b::c:d inform version v2c community public port
5000
switch(config)# no snmp-server host a:b::c:d inform version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin
switch(config)# snmp-server host a:b::c:d trap version v3 user Admin
switch(config)# no snmp-server host a:b::c:d trap version v3 user Admin
switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin port 2000
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin port 2000
switch(config)# snmp-server host a:b::c:d trap version v3 user Admin port 2000
switch(config)# no snmp-server host a:b::c:d trap version v3 user Admin port 2000
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server system-contact

```
snmp-server system-contact <INFO>
no snmp-server system-contact [<INFO>]
```

Description

Sets SNMP contact information.

The no form of this command removes the SNMP contact information.

Parameter	Description
<INFO>	Specifies SNMP contact information. Range: 1 to 128 printable ASCII characters, except for question mark (?).

Examples

Defines SNMP contact information to be **John Smith, Lab Admin**:

```
switch(config)# snmp-server system-contact John Smith, Lab Admin
```

Removes SNMP contact information:

```
switch(config)# no snmp-server system-contact
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server system-description

```
snmp-server system-description <DESCRIPTION>
no snmp-server system-description
```

Description

Sets the SNMP system description.

The `no` form of this command removes the SNMP system description.

Parameter	Description
<DESCRIPTION>	Specifies the SNMP system description. Typical content to include would be the full name and version of the following: ▪ Hardware type of the system ▪ Software operating system ▪ Networking software Range: 1 to 64 printable ASCII characters, except for the question mark (?).

Examples

Defines the SNMP system description to be **mainSwitch**:

```
switch(config)# snmp-server system-description mainSwitch
```

Removes the SNMP system description:

```
switch(config)# no snmp-server system-description mainSwitch
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server system-location

```
snmp-server system-location <INFO>
no snmp-server system-location
```

Description

Sets the SNMP location information.

The `no` form of this command removes the SNMP location information.

Parameter	Description
<INFO>	Specifies the SNMP location information. Range: 1 to 128 printable ASCII characters, except for the question mark (?).

Examples

Defines the SNMP location information to be **Main Lab**:

```
switch(config)# snmp-server system-location Main Lab
```

Removes the SNMP location information:

```
switch(config)# no snmp-server system-location
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server vrf

```
snmp-server vrf <VRF-NAME>
no snmp-server vrf <VRF-NAME>
```

Description

Configures a VRF on which the SNMP agent listens for incoming requests. By default, the SNMP agent does not listen on any VRF. 4100i, 6000, and 6100 only support default VRF. The SNMP agent can listen on multiple VRFs.

The `no` form of this command stops the SNMP agent from listening for incoming requests on the specified VRF.

Parameter	Description
<VRF-NAME>	Specifies the name of a VRF.

Examples

Configuring the SNMP agent to listen on VRF `default`.

```
switch(config)# snmp-server vrf default
```

Configuring the SNMP agent to listen on VRF `mgmt`.

```
switch(config)# snmp-server vrf mgmt
```

Configuring the SNMP agent to listen on used-defined VRF `myvrf`.

```
switch(config)# snmp-server vrf myvrf
```

Stopping the SNMP agent from listening on VRF `default`.

```
switch(config)# no snmp-server vrf default
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server trap aaa-server-reachability-status

```
snmp-server trap aaa-server-reachability-status
no snmp-server trap aaa-server-reachability-status
```

Description

Enables the SNMP trap for AAA server status. When enabled, traps are sent whenever AAA server (RADIUS, TACACS) status changes from reachable to unreachable and vice versa.

The `no` form of this command disables sending SNMP trap for AAA server status.

Examples

Enabling the SNMP trap for AAA server status:

```
switch(config)# snmp-server trap aaa-server-reachability-status
```

Disabling the SNMP trap for AAA server status:

```
switch(config)# no snmp-server trap aaa-server-reachability-status
```

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
6200 6300 6400	`config`	Administrators or local user group members with execution rights for this command.

snmp-server trap mac-notify

```
snmp-server trap mac-notify
no snmp-server trap mac-notify
```

Description

Enables the MAC notification traps within the SNMP module at a global level. When enabled, traps are sent for interfaces that are configured for MAC notification events.

The `no` form of this command disables sending MAC notification traps at a global level. When disabled, existing `mac-notify` interface configuration is preserved but MAC notification events on configured interfaces will not cause SNMP traps to be transmitted.

Examples

Enabling the SNMP MAC notification feature in the system globally:

```
switch(config)# snmp-server trap mac-notify
```

Disabling the SNMP MAC notification feature in the system globally:

```
switch(config)# no snmp-server trap mac-notify
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server trap-source interface vrf

```
snmp-server trap-source {interface <IF-NAME> | <IPv4-Address> | <IPv6-Address>} [vrf <VRF-NAME>]
no snmp-server trap-source {interface <IF-NAME> | <IPv4-Address> | <IPv6-Address>} [vrf <VRF-NAME>]
```

Description

Configures SNMP trap source interface or IP address for a VRF.

The `no` form of this command removes the SNMP `trap-source` configuration for a VRF.

Parameter	Description
<IF-NAME>	Specifies the source interface name. Interface name can be physical interface, loopback interface, LAG interface, or VLAN interface.
<IPv4-Address>	Specifies the IPv4 address of source interface for the SNMP trap.
<IPv6-Address>	Specifies the IPv6 address of source interface for the SNMP trap.
<VRF-NAME>	Specifies the name of a VRF associated to the source interface for the SNMP trap.

Examples

Configuring SNMP trap source interface for a VRF.

```
switch(config)# snmp-server trap-source interface 1/1/12 vrf sample
switch(config)# snmp-server trap-source interface loopback10 vrf sample
switch(config)# snmp-server trap-source interface vlan23 vrf sample
```

Configuring SNMP trap source IP address for a VRF.

```
switch(config)# snmp-server trap-source 10.0.0.1 vrf red
switch(config)# snmp-server trap-source 1001::1 vrf red
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap

```
snmp-server trap {cpu-utilization | memory-utilization | rmon-events}
no snmp-server trap {cpu-utilization | memory-utilization | rmon-events}
```

Description

Enables the SNMP traps. The SNMP traps are enabled by default.

The `no` form of this command disables the SNMP traps.

Parameter	Description
cpu-utilization	Enables the CPU utilization traps.
memory-utilization	Enables the memory utilization traps.
rmon-events	Enables the RMON event traps.

Examples

Enabling the SNMP traps:

```
switch(config)# snmp-server trap cpu-utilization
switch(config)# snmp-server trap memory-utilization
switch(config)# snmp-server trap rmon-events
```

Disabling the SNMP traps:

```
switch(config)# no snmp-server trap cpu-utilization
switch(config)# no snmp-server trap memory-utilization
switch(config)# no snmp-server trap rmon-events
```

Displaying the SNMP trap configuration:

```
switch(config)# show running-config all | inc snmp
snmp-server trap rmon-events
snmp-server trap cpu-utilization
snmp-server trap memory-utilization
```

Displaying CPU and Memory usage:

```
switch(config)# show system
Hostname           : XXXX
System Description : XX.10.07.0001CI
System Contact     :
System Location    :
Vendor             : Aruba
Product Name       : JLXXXX XXXX Base Chassis/3xFT/18xFans/Cbl Mgr/X462 Bundle
```

```
Chassis Serial Nbr : SG6ZOO9068
Base MAC Address   : f40343-806400
AOS-CX Version : XX.10.07.0001CI
Time Zone          : UTC
Up Time            : 8 minutes
CPU Util (%)       : 1
Memory Usage (%)   : 10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmp-server trap vsx

```
snmp-server trap vsx
no snmp-server trap vsx
```

Description

Enables sending the SNMP traps for VSX related events. VSX trap generation is disabled by default.

The `no` form of this command disables sending the SNMP traps for VSX related events.

The trap support is available for the following VSX events:

- ISL up and down
- KA up and down
- MCLAG up and down

Parameter	Description
`vsx`	Specifies SNMP traps for VSX events.

Examples

Enabling the VSX traps:

```
switch(config)# snmp-server trap vsx
```

```
switch(config)# show vsx configuration trap
SNMP traps : Enabled
```

Disabling the VSX traps:

```
switch(config)# no snmp-server trap vsx
```

```
switch(config)# show vsx configuration trap
SNMP traps : Disabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmpv3 context

```
snmpv3 context <NAME> vrf <VRF-NAME> [community <STRING>]
no snmpv3 context <NAME> [vrf <VRF-NAME>] [community <STRING>]
```

Description

Creates an SNMPv3 context on the specified VRF.

The no form of this command removes the specified SNMP context.

Parameter	Description
<NAME>	Specifies the name of the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark (?).
vrf *<VRF-NAME>*	Specifies the VRF associated with the context. Default: default.
community *<STRING>*	Specifies the SNMP community string associated with the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark. Default: public.

Examples

Creating an SNMPv3 context named **newContext**:

```
switch(config)# snmpv3 context newContext
```

Creating an SNMPv3 context named **newContext** on VRF **myVrf** and with community string **private**.

```
switch(config)# snmpv3 context newContext vrf myVrf community private
```

Removing the SNMPv3 context named **newContext** on VRF **myVrf**:

```
switch(config)# no snmpv3 context newContext vrf myVrf
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmpv3 engine-id

Syntax

`snmpv3 engine-id <ENGINE-ID>`

`no snmpv3 engine-id <ENGINE-ID>`

Description

Configures the SNMPv3 SNMP engine-id allowing an administrator to configure a unique SNMP engine-id for the switch. This engine-id is used by the NMS management tool to identify and distinguish multiple switches on the same network.

The `no` form of this command restores the default engine-id, created by the switch using a combination of the enterprise OID value and the switch's mac address.

Command context

`config`

Parameters

<ENGINE-ID>

SNMPv3 SNMP engine-id in colon separated hexadecimal notation.

Authority

Administrators or local user group members with execution rights for this command.

Examples

Configuring the SNMPv3 engine-id:

```
switch(config)#
switch(config)# snmpv3 engine-id
  WORD  SNMPv3 snmp engine-id in colon seperated hexadecimal notation
switch(config)# snmpv3 engine-id 01:23:45:67:89:ab:cd:ef:01:23:45:67
```

Restoring the default SNMPv3 engine-id:

```
switch(config)# no snmpv3 engine-id
```

snmpv3 security-level

```
snmpv3 security-level {auth | auth-privacy}
no snmpv3 security-level {auth | auth-privacy}
```

Description

Configures the SNMPv3 security level. The security level determines which SMNPv3 users defined by the command `snmpv3 user` are able to connect.

The `no` form of this command changes the security level as follows:

- `no snmpv3 security-level auth`: Sets the security level to `auth-privacy`.
- `no snmpv3 security-level auth-privacy`: Sets the security level to no authentication or privacy, allowing any SNMP user to connect.

Parameter	Description
`auth`	SNMPv3 users that support authentication, or authentication and privacy are allowed.
`auth-privacy`	Only SNMPv3 users with both authentication and privacy are allowed. This is the highest level of SNMPv3 security. Default.

Examples

Setting the SNMPv3 security level to authentication and privacy:

```
switch(config)# snmpv3 security-level auth-privacy
```

Setting the SNMPv3 security level to authentication only:

```
switch(config)# snmpv3 security-level auth
```

Setting the SNMPv3 security level to no authentication and no privacy:

```
switch(config)# no snmpv3 security-level auth-privacy
```

Restoring the default SNMPv3 security level to authentication and privacy:

```
switch(config)# no snmpv3 security-level auth
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

snmpv3 user

```
snmpv3 user <NAME>
      [auth <AUTH-PROTO> auth-pass [{plaintext | ciphertext} <AUTH-PASS>]]
      [priv <PRIV-PROTO> priv-pass [{plaintext | ciphertext} <PRIV-PASS>]]
no snmpv3 user <NAME>
         [auth <AUTH-PROTO> auth-pass [{plaintext | ciphertext} <AUTH-PASS>]]
         [priv <PRIV-PROTO> priv-pass [{plaintext | ciphertext} <PRIV-PASS>]]
```

Description

Creates an SNMPv3 user and adds it to an SNMPv3 context. The SNMPv3 security level (set with command `snmpv3 security-level`) determines which users are allowed to authenticate.

The `no` form of this command removes the specified SNMPv3 user.

Parameter	Description
<NAME>	Specifies the SNMPv3 username. Range 1 to 32 printable ASCII characters, excluding space and question mark (?).
`auth` *<AUTH-PROTO>*	Selects the authentication protocol used to validate user logins: `md5` or `sha1`.
`auth-pass [{plaintext | ciphertext} <AUTH-PASS>]`	Specifies the SNMPv3 user authentication password. Range for `plaintext` is 8 to 32 printable ASCII characters, excluding space and question mark (?). Range for `ciphertext` is 1 to 256 printable ASCII characters. Ciphertext is used when copying user configuration settings between switches.
`priv` *<PRIV-PROTO>*	Selects the SNMPv3 privacy protocol (encryption method): `aes` or `des`.
`priv-pass [{plaintext | ciphertext} <PRIV-PASS>]`	Specifies the SNMPv3 user privacy encryption password. Range for `plaintext` is 8 to 32 printable ASCII characters, excluding space and question mark (?). Range for `ciphertext` is 1 to 256 printable ASCII characters. Ciphertext is used when copying user configuration settings between switches.

When the authentication password is not provided on the command line, plaintext authentication password prompting occurs upon pressing Enter, followed by privacy encryption protocol prompting, and finally plaintext encryption password prompting. The entered password characters are masked with asterisks.

When the authentication type and password plus the privacy protocol (encryption method) are provided on the command line but the encryption password is not provided, plaintext encryption password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Defining SNMPv3 user **Admin1** using **sha** authentication and **des** privacy encryption with provided plaintext passwords:

```
switch(config)# snmpv3 user Admin1 auth sha auth-pass plaintext F82#450h
                priv des priv-pass plaintext F82#4eva
```

Defining SNMPv3 user **Admin2** using **MD5** authentication and **AES** privacy encryption with provided authentication password and privacy encryption type but prompted encryption password:

```
switch(config)# snmpv3 user Admin2 auth md5 auth-pass plaintext F82#450h
                priv aes priv-pass
Enter the privacy encryption key: ********
Re-Enter the privacy encryption key: ********
```

Defining SNMPv3 user **Admin2** using **MD5** authentication and **AES** privacy encryption with plaintext password prompting and privacy encryption selection:

```
switch(config)# snmpv3 user Admin2 auth md5 auth-pass
Enter the authentication password: ********
Re-Enter the authentication password: ********

Configure the privacy protocol (y/n)? y
Enter the privacy protocol (aes/des)? aes

Enter the privacy encryption key: ********
Re-Enter the privacy encryption key: ********
```

Removing SNMPv3 user **Admin1**:

```
switch(config)# no snmpv3 user Admin1
```

Creating an SNMP user on switch 1 and then creating the same user on switch 2 by copying from the switch 1 configuration:

On switch 1, configure a user named **Admin3**, and then use the `show running-config` command to display switch configuration. Save a copy of the full `snmpv3 user` command (shown by `show running-config`). This saved command is used on switch 2.

```
switch1(config)# snmpv3 user Admin3 auth sha auth-pass plaintext F82#450h
                 priv des priv-pass plaintext F82#4eva
switch1(config)# exit
switch1# show running-config
Current configuration:
!
!Version AOS-CX xx.xx.xx.xxxxxx
!
snmpv3 user Admin3 auth sha auth-pass ciphertext AQBaf2d...FJVcZ3o=
priv des priv-pass ciphertext AQBaH2p...2jfTFwQ=
ssh server vrf mgmt
!
interface mgmt
    no shutdown
    ip dhcp
```

```
vlan 1
```

On switch 2, execute the `snmpv3 user` command that you saved from switch 1 (as shown by `show running-config`). This creates the user on switch 2 with the same configuration.

```
switch2(config)# snmpv3 user Admin3 auth sha auth-pass ciphertext AQBaf2d...FJVcZ3o=
                 priv des priv-pass ciphertext AQBaH2p...2jfTFwQ=
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

Entity MIB support

The Entity MIB, rfc 6933, allows network managers to retrieve physical containment and logical relationships for devices in the network. The entconfigChange trap is sent to configured SNMP-server hosts when a change occurs. The trap is configured to send notifications no more than once every 5 seconds. We will be supporting the Entity MIB for read-only.

Physical components that are supported include:

- Stack
- Chassis
- Fabric cards
- Fan trays
- Fans
- Line cards and their interfaces
- Management modules and the intake temperature sensor
- Power supplies

The slots for any removable component are also represented.

The logical table of the Entity MIB represents configured VLANs and the associated ports.

entConfigChange trap/notification is sent to configured snmp-server hosts.

Location of the MIB files on the web

The MIB files for Aruba switches can be found on the Aruba Service Portal. You can apply the various filters to filter by product series, software versions, and software release types.

Newly introduced MIBs and Traps for 10.09

The following list contains the newly introduced MIBs and Traps for each software feature. Software is provided along with the MIB and Traps supported name.

AAA

MIB file

ARUBAWIRED-AAA-MIB

Implemented MIB objects:

- arubaWiredRadiusServerTable
  - arubaWiredRadiusServerVrfName
  - arubaWiredRadiusServerAddress
  - arubaWiredRadiusServerPort
  - arubaWiredRadiusServerPortType
  - arubaWiredRadiusServerReachabilityStatus
- arubaWiredTacacsServerTable
  - arubaWiredTacacsServerVrfName
  - arubaWiredTacacsServerAddress
  - arubaWiredTacacsServerPort
  - arubaWiredTacacsServerReachabilityStatus

Traps supported

- arubaWiredRadiusServerStatusChange
- arubaWiredTacacsServerStatusChange

MODULE

MIB file

ARUBAWIRED-MODULE-MIB

Implemented MIB objects

- arubaWiredModuleTable
  - arubaWiredModuleGroupIndex
  - arubaWiredModuleTypeIndex
  - arubaWiredModuleSlotIndex
  - arubaWiredModuleName
  - arubaWiredModuleType
  - arubaWiredModuleProductDescription
  - arubaWiredModuleSerialNumber
  - arubaWiredModuleProductNumber
  - arubaWiredModuleAdminState
  - arubaWiredModulePowerPriority

Traps supported

- arubaWiredModuleStateNotification

NETWORKING

MIB file

ARUBAWIRED-NETWORKING-OID

Implemented MIB objects

- arubaWiredSwitchJL717C
- arubaWiredSwitchJL718C
- arubaWiredSwitchJL719C
- arubaWiredSwitchJL720C
- arubaWiredSwitchJL721C
- arubaWiredSwitchJL722C
- arubaWiredSwitchModuleJL717C
- arubaWiredSwitchModuleJL718C
- arubaWiredSwitchModuleJL719C
- arubaWiredSwitchModuleJL720C
- arubaWiredSwitchModuleJL721C
- arubaWiredSwitchModuleJL722C
- arubaWiredSwitchR8S96A
- arubaWiredSwitchModuleR8S96A
- arubaWiredSwitch10000PowerSupplySlot
- arubaWiredSwitch10000FanTraySlot
- arubaWiredSwitchPowerSupplyUnitR8R51A
- arubaWiredSwitchPowerSupplyUnitR8R52A
- arubaWiredSwitchFanTrayR8R53A
- arubaWiredSwitchFanTrayR8R54A

OIDs that supports SNMP write

The following table contains the OIDs that supports SNMP write:

Software Feature	MIB File	OID
SNMPv2 System	SNMPv2-MIB.mib	▪ sysContact ▪ sysName ▪ sysLocation
PoE	▪ ARUBAWIRED-POE.mib ▪ POWER-ETHERNET-MIB	▪ arubaWiredPoePethPsePortPoECycle ▪ pethPsePortAdminEnable
Interface	IF-MIB	▪ ifAdminStatus ▪ ifAlias

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Hardware Documentation and Translations	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

Portal	
Aruba software	https://asp.arubanetworks.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP account.

Warranty Information

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Aruba is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

Documentation Feedback

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.