ForeScout

Switch Commands in Use by the Switch Plugin

CounterACT® Technical Note

Updated for Switch Plugin 8.9.4

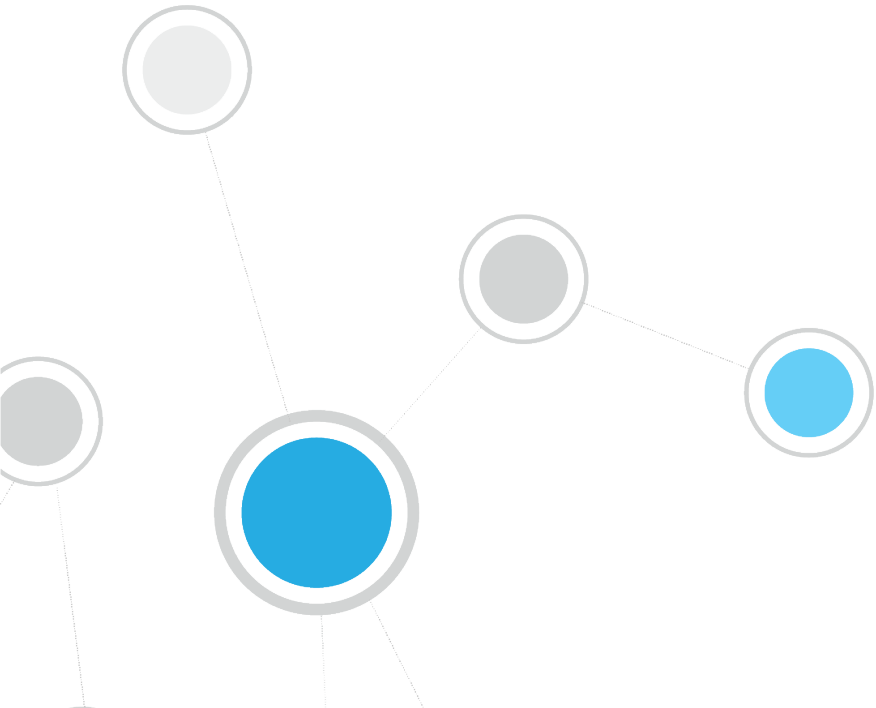


Table of Contents

About This Document

This document provides switch CLI commands and SNMP MIBs that are used by the Switch Plugin to manage Cisco switches. The plugin uses these commands to perform operations on switch devices that the plugin is configured to manage.

In each table, **CLI Commands and MIBs Used** are provided. The specific CLI command(s) or MIB(s) actually used by the Switch Plugin to perform an operation will vary based on switch device and plugin processing considerations.

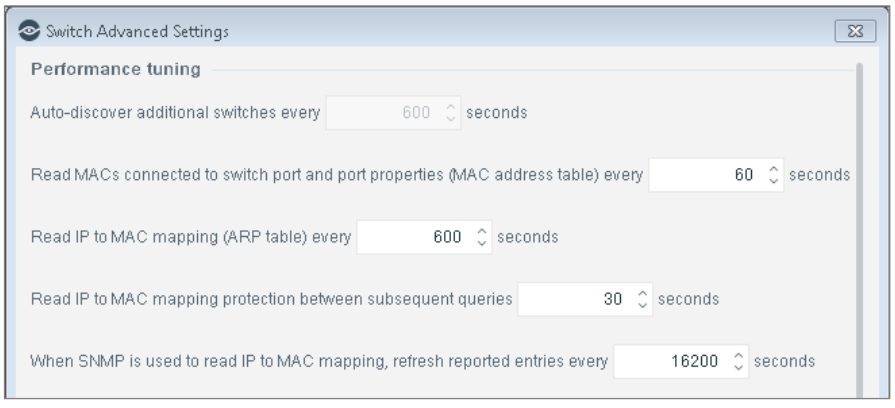
Switch Plugin Functionality

The switch commands in use by the Switch Plugin cover the following management functionality topics:

- Read/Write Permissions-Based Functionality
- Action Execution
- Port Configuration Querying
- Switch Device Querying
- SGT Mapping Querying
- SNMP Trap Processing

Performance tuning intervals mentioned in this document are defined per switch that the Switch Plugin is configured to manage. These performance tuning intervals control the frequency with which the Switch Plugin must periodically probe a managed switch device, when no other CounterACT processing events direct the Switch Plugin to do so. These time intervals settings are defined in the Console at:

Options > **Switch** pane > **Add** switch/**Edit** <*selected switch*> > **Permissions** > **Advanced** > **Switch Advanced Settings** window > **Performance tuning** section.



Read / Write Permissions-Based Functionality

Switch Plugin functionality based on the read/write permissions that are configured for the plugin to use when interoperating with a specific switch. This section presents the following topics:

Command Line Connection - Basic Command

Before each query via CLI, the following commands are executed:

Command	Purpose
`enable`	Used to enter the privileged mode
`terminal length 0`	Used to disable paging of the command output

ARP Table Operations

The Switch Plugin performs the following operations on a switch ARP table:

- Read ARP Table to obtain its IP to MAC mapping information
- Clear ARP Table to clear redundant ARP table entries

From the list of available commands, the Switch Plugin selects the best suited command for use on the managed switch. Plugin learning of the best suited command occurs the initial time that the plugin needs to perform the relevant operation (initial read, initial clear). The plugin sequentially issues commands in an effort to identify the first successful command, meaning that the command is responded to, without error, by the switch. Once identified, the plugin uses this command to perform all subsequent read/clear operations on the managed switch.

Read ARP Table

The following switch commands are used to read the ARP table:

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
CLI	Available Commands: **show ip arp** **show arp** **show ip arp client** Available Commands: **show ip arp vrf <vrf name>** **show arp vrf <vrf name>**	Every 600 seconds	▪ **Read - IP to MAC mapping (ARP table)** ▪ **Read –IP to MAC mapping (ARP table) for VRFs**	- Options' location in Console: ▪ **Permissions** tab > **ARP Permissions** section. ▪ **Permissions** tab > **Advanced** > **Switch Advanced Settings** window > **IP to MAC mapping** section - Performed during plugin test of switch configuration. - The Switch Plugin uses these commands to perform the Expedite IP Discovery action.
SNMP	**1.3.6.1.2.1.3.1.1.2 RFC1213-MIB::atPhysAddress** **1.3.6.1.2.1.4.22.1.2 RFC1213-MIB::ipNetToMediaPhysAddress**	Every 600 seconds	**Read - IP to MAC mapping (ARP table)**	- Option location in Console: **Permissions** tab > **ARP Permissions** section. - Performed during plugin test of switch configuration. - The Switch Plugin uses these commands to perform the Expedite IP Discovery action.

Clear ARP Table

The following switch commands are used to clear to the ARP table of redundant IP to MAC mapping entries:

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
CLI	Available Commands: **clear ip arp <ip of host to clear from arp table>** **clear arp <ip of host to clear from arp table>** **clear ip arp client <ip of host to clear from arp table>** **no arp <ip of host to clear from arp table>** **clear arp cache**		**Write – Clear redundant IP addresses associated with MAC (ARP table)**	- Option location in Console: **Permissions** tab > **ARP Permissions** section. - After performing a read ARP table operation, the plugin performs a clear ARP table operation. - Performed during plugin test of switch configuration. - After performing the *Assign to VLAN* action, the ***MAC ACL*** endpoint handling or the *Switch Block* action, the plugin performs a clear ARP table operation, see Action Execution. - Whenever a detected host is deleted from CounterACT, the plugin performs a clear ARP table operation.
SNMP	**1.3.6.1.2.1.4.22.1.4** **RFC1213-MIB::ipNetToMediaTable** **OBJECT-TYPE**		**Write – Clear redundant IP addresses associated with MAC (ARP table)**	- Option location in Console: **Permissions** tab > **ARP Permissions** section. - After performing a read ARP table operation, the plugin performs a clear ARP table operation. - Performed during plugin test of switch configuration. - After performing the *Assign to VLAN*

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
				action, the ***MAC ACL*** endpoint handling or the *Switch Block* action, the plugin performs a clear ARP table operation, see Action Execution. - Whenever a detected host is deleted from CounterACT, the plugin performs a clear ARP table operation.

Auto-Discovery

The Switch Plugin detects the neighboring switches of a switch configured to interoperate with the plugin. The auto-discovery feature supports the CDP, FDP and LLDP auto-discovery protocols.

The following switch commands are used to perform auto-discovery:

Connection Method	MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
SNMP	**1.3.6.1.4.1.9.9.23.1.2.1.1 .4 Cisco Discovery Protocol cache table** **1.3.6.1.4.1.9.9.23.1.2.1.1 Cisco Discovery Protocol capabilities table** **1.0.8802.1.1.2.1.4.2.1.3 Lldp general mib** **1.0.8802.1.1.2.1.4.1.1 lldpRemSysCapSupported** **1.3.6.1.4.1.45.1.6.13.2.1. 1.3 5EnMsTopNmmIpAddr**	Every 600 seconds (cdp query)	**Read - Auto-discover additional switches (CDP, FDP, LLDP)**	- Option location in Console: **Permissions** tab > **Discovery Permissions** section - Performed during plugin test of switch configuration.

MAC Address Table Operations

The Switch Plugin performs the following operation on a switch MAC Address table:

- Read MAC Address Table to obtain information about endpoint connections to switch port

From the list of available commands, the Switch Plugin selects the best suited command for use on the managed switch. Plugin learning of the best suited command occurs the initial time that the plugin needs to perform the relevant operation (initial read). The plugin sequentially issues commands in an effort to identify the first successful command, meaning that the command is responded to, without error, by the switch. Once identified, the plugin uses this command to perform all subsequent read operations on the managed switch.

Read MAC Address Table

The following switch commands are used to read the MAC Address table:

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
CLI	**show cdp entry *** Available Commands: **show mac address-table** **show mac-address-table**	Every 60 seconds	**Read - MACs connected to switch port and port properties (MAC address table)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed during plugin test of switch configuration. - The Switch Plugin uses these commands following receipt of an SNMP link status link up trap. See SNMP Trap Processing.
SNMP	**1.3.6.1.2.1.2.2.1.8 interfaces.ifTable.ifEntry.ifOperStatus** **1.3.6.1.2.1.17.7.1.2.2.1.2 dot1qTpFdbPort** **1.3.6.1.2.1.17.7.1.4.2.1.3 dot1qVlanFdbId** **1.3.6.1.2.1.17.1.4.1.2**	Every 60 seconds	**Read - MACs connected to switch port and port properties (MAC address table)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed during plugin test of switch configuration. - The Switch Plugin uses these commands

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
	dot1dBasePortIfIndex **1.3.6.1.2.1.17.4.3.1.2 dot1dTpFdbPort** **1.3.6.1.4.1.9.9.276.1.5.1.1.1 CISCO-IF-EXTENSION-MIB::cieIfDot1dBaseMappingPort** **1.3.6.1.2.1.1.7.0** **1.3.6.1.2.1.1.1.0** **1.3.6.1.4.1.9.6.1.101.48.22.1.1** **1.3.6.1.4.1.9.9.68.1.5.1.1.1** **1.3.6.1.4.1.9.9.68.1.2.1.1.3**			following receipt of an SNMP link status link up trap. See SNMP Trap Processing.

Action Execution

The Switch Plugin provides the following CounterACT actions:

- Access Port ACL (*restrict* action)
- Assign Security Group Tag (*restrict* action)
- Assign to VLAN (*restrict* action)
- Endpoint Address ACL (*restrict* action)
- Expedite IP Discovery (*remediate* action)
- Switch Block (*restrict* action)

The Switch Plugin executes a relevant action when any of the following events occurs:

- Endpoint connection to a switch device
- Endpoint disconnection from a switch device

The Switch Plugin is alerted about endpoint connections and disconnections, due to either receipt from a switch device of an SNMP trap or when reading the MAC Address table.

In the Console, work with actions in any of the following ways:

- Manually initiate on a selected endpoint from the **Detections** pane of the **NAC** tab.
- Add/edit a policy and incorporate use of the action from the **Policy Manager** pane of the **Policy** tab.

Modify Port Configuration

Accompanying any *restrict* action, the Switch Plugin also always writes to the switch device to perform a modify port configuration operation. The Switch Plugin carries out the modify port configuration as part of a restrict action being either performed on or canceled for a connected or disconnected endpoint.

The following switch commands are used by the Switch Plugin to perform a modify port configuration operation:

Connection Method	CLI Commands	Console Options	Notes
CLI	**`config t`** **`interface <interface name>`** **`description <new description>`** **`no description`** **`show running-config interface <interface name>|include description`**	**Set port alias on action**	- Option location in Console: **Permissions** tab > **Advanced** > **Switch Advanced Settings** window > **Settings** section - The plugin performs both the **`config t`** and the **`interface`** commands with all restrict actions. - Only when **Set port alias on action** is enabled, does the plugin also perform both the **`description`** and the **`show running-config interface`** commands with restrict actions.

Access Port ACL

Use Access Port ACL, a *restrict* action, to define an ACL that addresses one or more than one access control scenario, which is then applied to an endpoint's switch access port. Access control scenarios are typically role or classification driven, for example, registered guest or compliance, and not endpoint IP specific. For example, implement an ACL action that denies corporate network access to guests but permits Internet access, regardless of endpoint IP address (no IP address dependency). This

differs from *Endpoint Address ACL* blocking, where CounterACT limits the rules of the ACL – only allowing the adding/removing of endpoint addresses to the ACL's permit/deny rules.

The CounterACT user defines the ACL rules to be applied in the *Access Port ACL* action's **Parameters** tab. The Switch Plugin does not verify the provided rules rather, applies the rules as provided.

The following switch commands are used to perform the *Access Port ACL* action:

Connection Method	CLI Commands/ MIBs Used	Console Options	Notes
CLI	**Config t** **interface <interface_name>** **show running-config** **show access-lists** **show access-lists <acl name>** Available Commands: **ip access-list <name>** **ip access-list extend <name>** **no ip access-list <name>** **no ip access-list extend <name>** **access-group mode prefer port** **ip access-group <acl name> in** **no ip access-group <acl name> in**	▪ **Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)** ▪ **Enable ACL**	- Options' location in Console: ▪ **Permissions** tab > **MAC Permissions** section ▪ **ACL** tab - Performed during plugin test of switch configuration. - In addition to the listed CLI commands, the Access Port ACL action can include any command supported by the particular switch device that the CounterACT user wants to use; the commands included in the action are those that the Switch Plugin delivers to switch device. - Some Cisco switches do not require use of the word **extended** when creating an ACL. For Cisco switches that do require use of the word **extended**, the Switch Plugin uses the short form **extend**, instead of the longer form **extended** (Cisco accepts such shortening). - **Permit** rule examples: ▪ **permit ip any host <CounterACT ip>** ▪ **permit <protocol> any host <auth server ip> eq <port number>** where - **<protocol>** is the IP transport protocol to permit, for example,

Connection Method	CLI Commands/ MIBs Used	Console Options	Notes
			tcp or **udp** - **<port number>** is the port being permitted to receive sent data, for example, **22** (the SSH port) - **<auth server ip>** is taken from the CounterACT configuration
SNMP	**1.3.6.1.2.1.2.2.1.2** **1.3.6.1.2.1.31.1.1.1.1** **1.3.6.1.2.1.31.1.1.1.2**	▪ **Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)** ▪ **Enable ACL**	- Performed during plugin test of switch configuration

Assign Security Group Tag

Use the *Assign Security Group Tag* action to assign a Security Group Tag (SGT) to CounterACT-detected endpoints. Endpoints with an assigned SGT are connected to a managed Cisco switch in a Cisco TrustSec domain. An SGT is a number in the range of 1 - 65,535.

The following switch commands are used to perform the *Assign Security Group Tag* action:

Connection Method	CLI Commands	Console Options	Notes
CLI	**config t** **cts role-based sgt-map <ip> sgt <sgt_value>** **no cts role-based sgt-map <ip>** **show cts role-based sgt-map <ip>**	**Read / Write Switch SGT information**	- Option location in Console: **SGT** tab

Assign to VLAN

Use *Assign to VLAN*, a *restrict* action, to assign endpoints to a VLAN, rather than turning off their switch ports. The *Assign to VLAN* action prevents the propagation of unwanted traffic to other sections of the network.

The following switch commands are used to perform the *Assign to VLAN* action:

Connection Method	CLI Commands/ MIBs Used	Console Options	Notes
CLI	**show interface(s) <interface_name> status** **config t** **interface <interface_name>** **switchport access vlan <VLAN_ID> (used on access of non-VoIP ports)** **switchport trunk native vlan <VLAN ID> (used on access of VoIP ports)** **switchport trunk allowed vlan add <VLAN ID>** **switchport trunk allowed vlan remove <VLAN ID>** **shutdown, no shutdown (port bounce)**	**Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed during plugin test of switch configuration. - After performing this action, the plugin performs a clear the ARP table operation, see Clear ARP Table. - After performing this action, the plugin performs a port configuration query operation, see Port Configuration Querying.
SNMP	**1.3.6.1.4.1.9.5.1.9.3.1.3 CISCO-STACK-MIB :: vlanPortVlan** **1.3.6.1.4.1.9.9.68.1.2.2.1.1** **1.3.6.1.4.1.9.9.68.1.2.2.1.2** **1.3.6.1.2.1.2.2.1.7 interfaces.ifTable.ifEntry.ifAdminStatus (port bounce)** **1.3.6.1.2.1.17.7.1.4.3.1.4** (only used for ***Cisco Small Business 300 Series*** switch)	**Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed during plugin test of switch configuration. - After performing this action, the plugin performs a clear the ARP table operation, see Clear ARP Table. - After performing this action, the

Connection Method	CLI Commands/ MIBs Used	Console Options	Notes
			plugin performs a port configuration query operation, see Port Configuration Querying.

Endpoint Address ACL

Use Endpoint Address ACL, a *restrict* action, to define and apply any of the following, connected endpoint handling:

- ***IP ACL***: Instruct a switch to close (ACL rule) or to open (ACL exception) network zones, services or protocols to either traffic to or traffic from specific endpoint IP addresses connected to the switch.
- ***MAC ACL***: Instruct a switch to block all traffic sent from the affected, endpoint MAC address.

The following switch commands are used to perform the *Endpoint Address ACL* action:

Connection Method	CLI Commands	Console Options	Notes
CLI	**Config t** **interface <interface_name>** **show running-config** **show access-lists <acl name>** Available Commands: **no ip access-list** **ip access-list <name>**	▪ **Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)** ▪ **Enable ACL**	- Options' location in Console: - **Permissions** tab > **MAC Permissions** section - **ACL** tab - Performed during plugin test of switch configuration. - After performing the ***MAC ACL*** endpoint handling, the plugin performs a clear the ARP table operation, see Clear ARP Table. - Some Cisco switches do not require use of the word **extended** when creating an ACL. For Cisco switches that do require use of the word **extended**, the Switch Plugin uses the short form **extend**, instead of the longer form

Connection Method	CLI Commands	Console Options	Notes
	ip access-list extend <name> **mac access-list extend <acl name>** **no ip access-list <name>** **no ip access-list extend <name>** **no mac access-list extend <acl name>** **access-group mode prefer port** **ip access-group <acl name> in** **no ip access-group <acl name> in** **mac access-group <acl name> in** **no mac access-group <acl name> in**		**extended** (Cisco accepts such shortening). - **Permit** rule examples: ▪ **permit tcp any any** ▪ **permit udp any any** ▪ **permit icmp any any** ▪ **permit ip any host <CounterACT ip>** ▪ **permit <protocol> any host <auth server ip> eq <port number>** where - **<protocol>** is the IP transport protocol to permit, for example, **tcp** or **udp** - **<port number>** is the port being permitted to receive sent data, for example, **22** (the SSH port) - **<auth server ip>** is taken from the CounterACT configuration - **Deny** rule example: ▪ **deny host <mac address of host to restrict> any**

Expedite IP Discovery

Use *Expedite IP Discovery*, a *remediate* action, to address situations of delayed endpoint IP discovery. The action expedites the resolution of endpoint IP addresses by the Switch Plugin querying the ARP table of designated, adjacent, L3-enabled network devices.

To perform the *Expedite IP Discovery* action, the Switch Plugin uses the Read ARP Table switch commands.

Switch Block

Use *Switch Block*, a *restrict* action, to isolate endpoints from using the network by turning off the switch port and preventing endpoints, which are assigned to that port, from accessing the network.

The following switch commands are used to perform the *Switch Block* action:

Connection Method	CLI Commands/ MIBs Used	Console Options	Notes
CLI	**config t** **interface <interface_name>** Available Commands: **show interface <interface_name> status** or **show interfaces <interface_name> status** **shutdown** **show running-config interface <interface name>** **no shutdown**	**Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed as part of the test of plugin configuration for managing the switch. - After performing this action, the plugin performs a clear the ARP table operation, see Clear ARP Table.
SNMP	**1.3.6.1.2.1.2.2.1.7 interfaces.ifTable.ifEntry .ifAdminStatus**	**Write – Enable Actions (Switch block, Assign to VLAN, Port ACL)**	- Option location in Console: **Permissions** tab > **MAC Permissions** section. - Performed as part of the test of plugin configuration for managing the switch. - After performing this action, the plugin performs a clear the ARP table operation, see Clear ARP Table.

Port Configuration Querying

The Switch Plugin queries a switch device to obtain detailed information about switch ports; read port configurations to obtain port VLAN, description (alias), ACL and voice. The Switch Plugin performs these queries with the following frequency:

- Periodically, using the calculated value [10 * (**Read MACs connected to switch port and port properties (MAC address table)** timer]
- After performing an *Assign to VLAN* action

The following switch commands are used by the Switch Plugin to obtain port configuration information:

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
CLI	**show running-config** **show vlan brief** **show vlan-switch** **show access-lists** **show access-lists <acl name>** **show power inline** **show vlan-switch brief | include default** **show vlan brief | include default**	Every 600 seconds		- Performed as part of the test of plugin configuration for managing the switch.
SNMP	**1.3.6.1.2.1.2.2.1.8 interfaces.ifTable.ifEntry.ifOperStatus** **1.3.6.1.2.1.2.2.1.2 interfaces.ifTable.ifEntry.ifDescr** **1.3.6.1.2.1.31.1.1.1.1 ifXTable.ifXEntry.ifName**	Every 600 seconds		- Performed as part of the test of plugin configuration for managing the switch.

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
	1.3.6.1.2.1.2.2.1.7 interfaces.ifTable.ifEntry.ifAdminStatus 1.3.6.1.2.1.4.21.1 1.3.6.1.2.1.4.20.1.1 RFC1213-MIB :: ipAdEntAddr 1.3.6.1.4.1.9.9.68.1.2.2.1.2 1.3.6.1.4.1.9.9.68.1.2.2.1.1 1.3.6.1.4.1.9.9.68.1.2.1.1.2 vmMembershipSummaryMemberPorts 1.3.6.1.4.1.9.9.46.1.3.1.1.4 vtpVlanName 1.3.6.1.4.1.9.5.1.9.3.1.5 CISCO-STACK-MIB :: vlanPortIslVlansAllowed 1.3.6.1.2.1.2.2.1.6 1.3.6.1.4.1.9.9.46.1.6.1.1.13 vlanTrunkPortDynamicState 1.3.6.1.2.1.31.1.1.1.18 1.3.6.1.4.1.9.5.1.4.1.1.11 CISCO-STACK-MIB :: portIfIndex 1.3.6.1.4.1.9.5.1.9.3.1.3 CISCO-STACK-MIB			

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
	:: vlanPortVlan 1.3.6.1.4.1.9.5.1.9.3.1.7 CISCO-STACK-MIB::vlanPortIslAdminStatus 1.3.6.1.4.1.9.5.1.9.3.1.8 CISCO-STACK-MIB::vlanPortIslOperStatus 1.3.6.1.4.1.9.9.402.1.2.1.9 cpeExtPsePortPwrConsumption 1.3.6.1.2.1.105.1.1.1.9 pethPsePortType 1.3.6.1.4.1.9.6.1.101.48.54.8 1.3.6.1.2.1.17.1.4.1.2 1.3.6.1.4.1.9.9.276.1.5.1.1.1 cieIfDot1dBaseMappingPort 1.3.6.1.2.1.17.7.1.4.3.1.2 dot1qVlanStaticEgressPorts 1.3.6.1.2.1.17.7.1.4.2.1.5.0 dot1qVlanCurrentUntagPorts 1.3.6.1.4.1.9.6.1.101.48.22.1.1 vlanPortModeState 1.3.6.1.2.1.17.7.1.4.5.1.1 pvid of the			

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
	port 1.3.6.1.4.1.9.6.1.101.48.22.1.1 1.3.6.1.2.1.17.7.1.4.3.1.1 dot1qVlanStaticName 1.3.6.1.2.1.17.1.1.0 dot1dBaseBridgeAddress 1.3.6.1.2.1.17.2.15.1.3 dot1dStpPortState 1.3.6.1.2.1.17.2.15.1.8 dot1dStpPortDesignatedBridge 1.3.6.1.2.1.17.2.15.1.9 dot1dStpPortDesignatedPort 1.3.6.1.2.1.1.1.0 os			

Switch Device Querying

The Switch Plugin queries a switch device to obtain detailed, typically static, information about the managed device, including its location, operating system, uptime and model. In the Console, this information is displayed in any of the following locations:

- In the **Detections** pane of the **NAC** tab, view hosts that are managed devices
- In the **Detections** pane of the **NAC** tab, view endpoints that are connected to managed devices
- In the **Switch** pane, view managed switch properties

The following switch commands are used by the Switch Plugin to obtain information about a managed switch device:

Connection Method	CLI Commands / MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
CLI	Available Commands: **`show ip vrf brief`** or **`show vrf`**	Every hour	**Read – IP to MAC mapping (ARP table) for VRFs**	- Option location in Console: **Permissions** tab > **Advanced** > **Switch Advanced Settings** window > **IP to MAC mapping** section
	`show cts sxp connections` **`show crypto ikev2 sa detailed`**	Every hour	**Read / Write Switch SGT information**	- Option location in Console: **SGT** tab - Performed as part of the test of plugin configuration for managing the switch. - Performed, if needed, before applying the *Assign Security Group Tag* action.

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
SNMP	**1.3.6.1.2.1.1.6.0 system.sysLocation** **1.3.6.1.2.1.1.3.0 system.sysUpTime.0** **1.3.6.1.2.1.1.7.0** **1.3.6.1.2.1.1.1.0 OS** **1.3.6.1.2.1.1.2.0** **1.3.6.1.2.1.4.1.0 IP-MIB::ipForwarding** **1.3.6.1.2.1.47.1.1.1.1.13 entPhysicalModelName** **1.3.6.1.2.1.47.1.1.1.1.5 ENTITY-MIB :: entPhysicalClass** **1.3.6.1.2.1.47.1.3.2.1.2 ENTITY-MIB :: entAliasMappingIdentifier** **1.3.6.1.2.1.4.20.1.1 RFC1213-MIB :: ipAdEntAddr** **1.3.6.1.2.1.1.5.0system.sysName.0** **1.3.6.1.2.1.2.2.1.6** **1.3.6.1.2.1.31.1.1.1.1 ifXTable.ifXEntry.ifNamemy** **1.3.6.1.2.1.2.2.1.2 interfaces.ifTable.i**	Every hour		- When performed as part of the test of plugin configuration for managing the switch, only the following MIBs are used: ▪ **OS = '1.3.6.1.2.1.1.1.0';** ▪ **SYSTEM_LOCATION = '1.3.6.1.2.1.1.6.0'; # system.sysLocation** ▪ **SYSTEM_UPTIME = '.1.3.6.1.2.1.1.3.0'; # system.sysUpTime.0**

Connection Method	CLI Commands/ MIBs Used	Performance Tuning Interval (Default)	Console Options	Notes
	fEntry.ifDescr **1.3.6.1.4.1.9.9.402.1.2.1.9 cpeExtPsePortPwrConsumption**			

SGT Mapping Querying

The Switch Plugin queries a switch device to obtain detailed information about its SGT mapping. The Switch Plugin performs these queries with the following frequency:

- Periodically, using the calculated value [10 * (**Read MACs connected to switch port and port properties (MAC address table)** timer]

The following switch commands are used by the Switch Plugin to obtain detailed information about the SGT mapping of a managed switch device:

Connection Method	CLI Commands	Performance Tuning Interval (Default)	Console Options	Notes
CLI	**show cts role-based sgt-map all**	Every 600 seconds	**Read/Write Switch SGT information**	- Option location in Console: **SGT** tab

SNMP Trap Processing

The Switch Plugin handles the SNMP traps sent to it by managed switch devices. SNMP traps are sent to the plugin whenever a managed switch device detects an endpoint connecting to or disconnecting from the network. By default, the plugin is configured to **Handle SNMP Traps**.

The Switch Plugin handles the following types of SNMP traps:

- Link Status Traps: These traps report either that a MAC (not specified) connected to or that a MAC (not specified) disconnected from a specified switch interface. In the event of Switch Plugin receipt of a link status link-up trap, the plugin then queries the sending switch to determine the connecting endpoint (see commands in Read MAC Address Table).

- MAC Notification Traps: Only issued by Cisco switches. The *MAC Address Learned* trap is handled and informs the plugin that <**MAC address**> has connected to the specified switch interface.

The following SNMP trap-related MIBs are sent by managed switch devices to the Appliance that manages them:

Link Status Traps

Connection Method	MIBs Used	Console Option	Notes
SNMP	**1.3.6.1.6.3.1.1.5.3** **1.3.6.1.6.3.1.1.5.4** **1.3.6.1.6.3.1.1.4.1.0**	**Handle SNMP Traps**	- Option location in Console: **Switch** pane > **Options** > **Edit general parameters** window. - Plugin trap processing affects the **Read MACs connected to switch port and port properties (MAC address table)** timer.

MAC Notification Traps

Connection Method	CLI Commands/ MIBs Used	Console Option	Notes
CLI	**fstool sw traps**	**Console SNMP Traps**	
SNMP	**1.3.6.1.4.1.9.9.215.1.1.8.1.2**	**Handle SNMP Traps**	- Option location in Console: **Switch** pane > **Options** > **Edit general parameters** window.
	1.3.6.1.4.1.9.9.215.1.1.1.0 **1.3.6.1.4.1.9.9.215.1.1.5.0** **1.3.6.1.4.1.9.9.215.1.2.1.1.1** **1.3.6.1.4.1.9.9.215.1.2.1.1.2**	**Console SNMP Traps**	

Legal Notice

2018-04-10 09:21