AOS-CX 10.09 Fundamentals Guide
4100i, 6000, 6100 Switch Series

Aruba
a Hewlett Packard Enterprise company

Published: December 2021
Edition: 1
**Copyright Information**

© Copyright 2021 Hewlett Packard Enterprise Development LP.

**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.


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.

**Acknowledgments**

Bluetooth is a trademark owned by its proprietor and used by Hewlett Packard Enterprise under license.
<table>
<thead>
<tr>
<th>Contents</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About this document</strong></td>
<td>9</td>
</tr>
<tr>
<td>3.1 Applicable products</td>
<td>9</td>
</tr>
<tr>
<td>3.2 Latest version available online</td>
<td>9</td>
</tr>
<tr>
<td>3.3 Command syntax notation conventions</td>
<td>9</td>
</tr>
<tr>
<td>3.4 About the examples</td>
<td>10</td>
</tr>
<tr>
<td>3.5 Identifying switch ports and interfaces</td>
<td>10</td>
</tr>
<tr>
<td><strong>About AOS-CX</strong></td>
<td>12</td>
</tr>
<tr>
<td>3.6 AOS-CX system databases</td>
<td>12</td>
</tr>
<tr>
<td>3.7 Aruba Network Analytics Engine introduction</td>
<td>12</td>
</tr>
<tr>
<td>3.8 AOS-CX CLI</td>
<td>13</td>
</tr>
<tr>
<td>3.9 Aruba NetEdit</td>
<td>13</td>
</tr>
<tr>
<td>3.10 Ansible modules</td>
<td>13</td>
</tr>
<tr>
<td>3.11 AOS-CX Web UI</td>
<td>13</td>
</tr>
<tr>
<td>3.12 AOS-CX REST API</td>
<td>14</td>
</tr>
<tr>
<td>3.13 In-band management</td>
<td>14</td>
</tr>
<tr>
<td>3.14 SNMP-based management support</td>
<td>14</td>
</tr>
<tr>
<td>3.15 User accounts</td>
<td>14</td>
</tr>
<tr>
<td><strong>Initial Configuration</strong></td>
<td>16</td>
</tr>
<tr>
<td>3.16 Initial configuration using ZTP</td>
<td>16</td>
</tr>
<tr>
<td>3.17 Initial configuration using the CLI</td>
<td>16</td>
</tr>
<tr>
<td>3.18 Connecting to the console port</td>
<td>17</td>
</tr>
<tr>
<td>3.19 Connecting to the in-band management port</td>
<td>17</td>
</tr>
<tr>
<td>3.20 Configure using DHCP or static IP</td>
<td>18</td>
</tr>
<tr>
<td>3.21 Logging into the switch for the first time</td>
<td>19</td>
</tr>
<tr>
<td>3.22 Setting switch time using the NTP client</td>
<td>19</td>
</tr>
<tr>
<td>3.23 Configuring banners</td>
<td>20</td>
</tr>
<tr>
<td>3.24 Using the Web UI</td>
<td>20</td>
</tr>
<tr>
<td>3.25 Configuring the in-band management interface</td>
<td>21</td>
</tr>
<tr>
<td>3.26 Restoring the switch to factory default settings</td>
<td>21</td>
</tr>
<tr>
<td>3.27 NTP commands</td>
<td>23</td>
</tr>
<tr>
<td>3.28 show ntp associations</td>
<td>30</td>
</tr>
<tr>
<td>3.29 show ntp authentication-keys</td>
<td>31</td>
</tr>
<tr>
<td>3.30 show ntp servers</td>
<td>32</td>
</tr>
<tr>
<td>3.31 show ntp statistics</td>
<td>33</td>
</tr>
<tr>
<td>3.32 show ntp status</td>
<td>33</td>
</tr>
<tr>
<td><strong>Interface configuration</strong></td>
<td>35</td>
</tr>
<tr>
<td>3.33 Configuring a layer 2 interface</td>
<td>35</td>
</tr>
</tbody>
</table>
checkpoint post-configuration ...................................... 79
checkpoint post-configuration timeout .............................. 80
checkpoint rename ..................................................... 81
checkpoint rollback ................................................... 82
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL> .......... 82
copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config} ........ 83
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL> .......... 84
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> .......... 85
copy <REMOTE-URL> {running-config | startup-config} .......... 86
copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>} .......... 87
copy {running-config | startup-config} <REMOTE-URL> .......... 88
copy {running-config | startup-config} <STORAGE-URL> .......... 89
copy startup-config running-config ............................. 90
copy <STORAGE-URL> running-config ............................. 91
erase {checkpoint <CHECKPOINT-NAME> | startup-config | all} .......... 92
show checkpoint <CHECKPOINT-NAME> ........................... 93
show checkpoint <CHECKPOINT-NAME> hash ....................... 95
show checkpoint post-configuration ............................. 96
show checkpoint ..................................................... 97
show checkpoint date .............................................. 98
show running-config hash ....................................... 98
show startup-config hash ....................................... 99
write memory ......................................................... 100

Boot commands ................................................................ 101
  boot set-default ..................................................... 101
  boot system .......................................................... 101
  show boot-history .................................................. 103

Firmware management commands .................................... 104
  copy {primary | secondary} <REMOTE-URL> ..................... 104
  copy {primary | secondary} <FIRMWARE-FILENAME> .......... 105
  copy primary secondary .......................................... 106
  copy <REMOTE-URL> .................................................. 107
  copy secondary primary .......................................... 108
  copy <STORAGE-URL> .............................................. 109

Dynamic Segmentation ...................................................... 111
User-based tunneling ..................................................... 111
User-based tunneling commands ...................................... 115
  backup-controller ip .............................................. 115
  enable ............................................................... 116
  ip source-interface (ubt) ........................................... 116
  papi-security-key .................................................. 117
  primary-controller ip ............................................. 119
  sac-heartbeat-interval ............................................. 119
  show ip source-interface ubt ..................................... 120
  show capacities ubt .............................................. 121
  show ubt ........................................................... 122
  show ubt information ............................................. 124
  show ubt state ..................................................... 126
  show ubt statistics ................................................. 129
  show ubt users ..................................................... 133
  uac-keepalive-interval ........................................... 133
  ubt ................................................................. 135
  ubt-client-vlan .................................................... 136
  ubt mode vlan-extend ............................................. 138
<table>
<thead>
<tr>
<th>Contents</th>
<th>6</th>
</tr>
</thead>
</table>

### SNMP
- Configuring SNMP .................................................. 139

### Aruba Central integration
- Connecting to Aruba Central ...................................... 141
- Custom CA certificate ............................................. 141
- Support mode in Aruba Central .................................. 142
- Aruba Central commands .......................................... 142
  - `aruba-central` .................................................. 142
  - `aruba-central support-mode` ............................. 143
  - `configuration-lockout` central managed .................. 144
  - `disable` ...................................................... 145
  - `enable (aruba central)` .................................... 145
  - `location-override` .......................................... 146
  - `show aruba-central` ....................................... 147
  - `show running-config current-context` .................. 148

### Port filtering
- Port filtering commands ......................................... 150
  - `portfilter` .................................................. 150
  - `show portfilter` .......................................... 151

### DNS
- DNS client ................................................................ 153
- Configuring the DNS client ...................................... 153
- DNS client commands .............................................. 154
  - `ip dns domain-list` ....................................... 154
  - `ip dns domain-name` ...................................... 155
  - `ip dns host` .................................................. 155
  - `ip dns server address` .................................... 156
  - `show ip dns` .................................................. 157

### Device discovery and configuration
- Device profiles ....................................................... 159
- Configuring a device profile for LLDP .......................... 160
- Configuring a device profile for CDP ........................... 160
- Configuring a device profile for local MAC match .......... 160
- Device profile commands ......................................... 161
  - `aaa authentication port-access allow-cdp-bpdu` .... 161
  - `aaa authentication port-access allow-lldp-bpdu` ... 162
  - `associate cdp-group` ........................................ 164
  - `associate lldp-group` ...................................... 164
  - `associate mac-group` ...................................... 165
  - `associate role` .............................................. 166
  - `disable (port-access device-profile)` .................... 167
  - `enable` ....................................................... 167
  - `ignore (for CDP groups)` .................................. 168
  - `ignore (for LLDP groups)` ................................ 169
  - `ignore (for MAC groups)` .................................. 170
  - `mac-group` .................................................. 176
  - `match (for CDP groups)` .................................. 176
  - `match (for LLDP groups)` ................................ 178
  - `match (for MAC groups)` .................................. 179
  - `port-access cdp-group` .................................... 183
  - `port-access device-profile` ................................ 184
  - `port-access device-profile mode block-until-profile-applied` 185
port-access lldp-group .................................................. 186
show port-access device-profile ........................................ 187

LLDP .............................................................................. 188
   LLDP agent .................................................................... 189
   LLDP MED support ..................................................... 191
   Configuring the LLDP agent ......................................... 191
   LLDP commands ........................................................... 192
      clear lldp neighbors .................................................. 192
      clear lldp statistics .................................................... 192
      lldp ........................................................................ 193
      lldp dot3 .................................................................. 194
      lldp holdtime ............................................................ 194
      lldp management-ipv4-address .................................. 195
      lldp management-ipv6-address .................................. 196
      lldp med .................................................................... 197
      lldp med-location ....................................................... 198
      lldp receive ............................................................... 199
      lldp reinit .................................................................. 200
      lldp select-tlv ............................................................ 200
      lldp timer .................................................................. 201
      lldp transmit .............................................................. 203
      lldp txdelay ............................................................... 203
      lldp trap enable .......................................................... 204
      show lldp configuration ............................................. 206
      show lldp local-device ............................................... 207
      show lldp neighbor-info .............................................. 209
      show lldp neighbor-info detail ..................................... 211
      show lldp statistics ..................................................... 213
      show lldp tlv ................................................................ 215

Cisco Discovery Protocol (CDP) ............................................. 216
   CDP support .................................................................. 216
   CDP commands ............................................................ 216
      cdp ........................................................................ 216
      clear cdp counters .................................................... 217
      clear cdp neighbor-info ............................................. 218
      show cdp .................................................................. 218
      show cdp neighbor-info .............................................. 219
      show cdp traffic ........................................................ 220

Zero Touch Provisioning ....................................................... 222
   ZTP support .................................................................. 222
   Setting up ZTP on a trusted network ............................... 223
   ZTP process during switch boot ...................................... 224
   ZTP commands ............................................................. 225
      show ztp information .................................................. 225
      ztp force provision ..................................................... 228

Switch system and hardware commands ................................ 230
   clear events .................................................................. 230
   console baud-rate ........................................................ 230
   domain-name ............................................................... 231
   hostname .................................................................... 232
   show capacities ............................................................ 233
   show capacities-status .................................................. 236
   show console ............................................................... 237
   show core-dump ........................................................... 238
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)

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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                                                                 |
  ■ example-text                                                                 |
| 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. |
### Convention Usage

<table>
<thead>
<tr>
<th></th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Brackets. Indicates that the enclosed item or items are optional.</td>
</tr>
<tr>
<td>... or</td>
<td>Ellipsis:</td>
</tr>
<tr>
<td>...</td>
<td>- In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

### 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.
AOS-CX is a new, modern, fully programmable operating system built using a database-centric design that ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including:

- Automated visibility to help IT organizations scale: The Aruba Network Analytics Engine allows IT to monitor and troubleshoot network, system, application, and security-related issues easily through simple scripts. This engine comes with a built-in time series database that enables customers and developers to create software modules that allow historical troubleshooting, as well as analysis of historical trends to predict and avoid future problems due to scale, security, and performance bottlenecks.

- Programmability simplified: A switch that is running the AOS-CX operating system is fully programmable with a built-in Python interpreter as well as REST-based APIs, allowing easy integration with other devices both on premise and in the cloud. This programmability accelerates IT organization understanding of and response to network issues. The database holds all aspects of the configuration, statistics, and status information in a highly structured and fully defined form.

- Faster resolution with network insights: With legacy switches, IT organizations must troubleshoot problems after the fact, using traditional tools like CLI and SNMP, augmented by separate, expensive monitoring, analytics, and troubleshooting solutions. These capabilities are built in to the AOS-CX operating system and are extensible.

- High availability: For switches that support active and standby management modules, the AOS-CX database can synchronize data between active and standby modules and maintain current configuration and state information during a failover to the standby management module.

- Ease of roll-back to previous configurations: The built-in database acts as a network record, enabling support for multiple configuration checkpoints and the ability to roll back to a previous configuration checkpoint.

### AOS-CX system databases

The AOS-CX operating system is a modular, database-centric operating system. Every aspect of the switch configuration and state information is modeled in the AOS-CX switch configuration and state database, including the following:

- Configuration information
- Status of all features
- Statistics

The AOS-CX operating system also includes a time series database, which acts as a built-in network record. The time series database makes the data seamlessly available to Aruba Network Analytics Engine agents that use rules that evaluate network conditions over time. Time-series data about the resources monitored by agents are automatically collected and presented in graphs in the switch Web UI.

### Aruba Network Analytics Engine introduction
The Aruba Network Analytics Engine is a first-of-its-kind built-in framework for network assurance and remediation. Combining the full automation and deep visibility capabilities of the AOS-CX operating system, this unique framework enables monitoring, collecting network data, evaluating conditions, and taking corrective actions through simple scripting agents.

This engine is integrated with the AOS-CX system configuration and time series databases, enabling you to examine historical trends and predict future problems due to scale, security, and performance bottlenecks. With that information, you can create software modules that automatically detect such issues and take appropriate actions.

With the faster network insights and automation provided by the Aruba Network Analytics Engine, you can reduce the time spent on manual tasks and address current and future demands driven by Mobility and IoT.

**AOS-CX CLI**

The AOS-CX CLI is an industry standard text-based command-line interface with hierarchical structure designed to reduce training time and increase productivity in multivendor installations.

The CLI gives you access to the full set of commands for the switch while providing the same password protection that is used in the Web UI. You can use the CLI to configure, manage, and monitor devices running the AOS-CX operating system.

**Aruba NetEdit**

Aruba NetEdit enables the automation of multidevice configuration change workflows without the overhead of programming.

The key capabilities of NetEdit include the following:

- Intelligent configuration with validation for consistency and compliance
- Time savings by simultaneously viewing and editing multiple configurations
- Customized validation tests for corporate compliance and network design
- Automated large-scale configuration deployment without programming
- Ability to track changes to hardware, software, and configurations (whether made through NetEdit or directly on the switch) with automated versioning

For more information about Aruba NetEdit, search for NetEdit at the following website:

www.hpe.com/support/hpesc

**Ansible modules**

Ansible is an open-source IT automation platform.

Aruba publishes a set of Ansible configuration management modules designed for switches running AOS-CX software. The modules are available from the following places:

- The `arubanetworks.aoscx_role` role in the Ansible Galaxy at: [https://galaxy.ansible.com/arubanetworks/aoscx_role](https://galaxy.ansible.com/arubanetworks/aoscx_role)
- The `aoscx-ansible-role` at the following GitHub repository: [https://github.com/aruba/aoscx-ansible-role](https://github.com/aruba/aoscx-ansible-role)

**AOS-CX Web UI**
The Web UI gives you quick and easy visibility into what is happening on your switch, providing faster problem detection, diagnosis, and resolution. The Web UI provides dashboards and views to monitor the status of the switch, including easy to read indicators for: power supply, temperature, fans, CPU use, memory use, log entries, system information, firmware, interfaces, VLANs, and LAGs. In addition, you use the Web UI to access the Network Analytics Engine, run certain diagnostics, and modify some aspects of the switch configuration.

**AOS-CX REST API**

Switches running the AOS-CX software are fully programmable with a REST (REpresentational State Transfer) API, allowing easy integration with other devices both on premises and in the cloud. This programmability—combined with the Aruba Network Analytics Engine—accelerates network administrator understanding of and response to network issues.

The AOS-CX REST API enables programmatic access to the AOS-CX configuration and state database at the heart of the switch. By using a structured model, changes to the content and formatting of the CLI output do not affect the programs you write. And because the configuration is stored in a structured database instead of a text file, rolling back changes is easier than ever, thus dramatically reducing a risk of downtime and performance issues.

The AOS-CX REST API is a web service that performs operations on switch resources using HTTPS POST, GET, PUT, and DELETE methods.

A switch resource is indicated by its Uniform Resource Identifier (URI). A URI can be made up of several components, including the host name or IP address, port number, the path, and an optional query string.

The AOS-CX operating system includes the AOS-CX REST API Reference, which is a web interface based on the Swagger UI. The AOS-CX REST API Reference provides the reference documentation for the REST API, including resources URIs, models, methods, and errors. The AOS-CX REST API Reference shows most of the supported read and write methods for all switch resources.

**In-band management**

Management communications with a managed switch can be:

**In band**

In-band management communications occur through ports on the line modules of the switch, using common communications protocols such as SSH and SNMP.

When you use an in-band management connection, management traffic from that connection uses the same network infrastructure as user data. User data uses the data plane, which is responsible for moving data from source to destination. Management traffic that uses the data plane is more likely to be affected by traffic congestion and other issues affecting the user network.

**SNMP-based management support**

The AOS-CX operating system provides SNMP read access to the switch. SNMP support includes support of industry-standard MIB (Management Information Base) plus private extensions, including SNMP events, alarms, history, statistics groups, and a private alarm extension group. SNMP access is disabled by default.

**User accounts**

To view or change configuration settings on the switch, users must log in with a valid account. Authentication of user accounts can be performed locally on the switch, or by using the services of an external TACACS+ or RADIUS server.
Two types of user accounts are supported:

- **Operators:** Operators can view configuration settings, but cannot change them. No operator accounts are created by default.
- **Administrators:** Administrators can view and change configuration settings. A default locally stored administrator account is created with username set to `admin` and no password. You set the administrator account password as part of the initial configuration procedure for the switch.
Perform the initial configuration of a factory default switch using one of the following methods:

- Load a switch configuration using zero-touch provisioning (ZTP). When ZTP is used, the configuration is loaded from a server automatically when the switch booted from the factory default configuration.
- Connect the management port on the switch to your network, and then use SSH client software to reach the switch from a computer connected to the same network. This requires that a DHCP server is installed on the network. Configure switch settings and features by executing CLI commands.
- Connect a computer running terminal emulation software to the console port on the switch. Configure switch settings and features by executing CLI commands.

**Initial configuration using ZTP**

Zero Touch Provisioning (ZTP) configures a switch automatically from a remote server.

**Prerequisites**

- The switch must be in the factory default configuration.
- Do not change the configuration of the switch from its factory default configuration in any way, including by setting the administrator password.
- Your network administrator or installation site coordinator must provide a Category 6 (Cat6) cable connected to the network that provides access to the servers used for Zero Touch Provisioning (ZTP) operations.

**Procedure**

1. Connect the network to a data port.
   
   See the *Installation Guide* for switch to determine the location of the switch ports.
2. If the switch is powered on, power off the switch.
3. Power on the switch. During the ZTP operation, the switch might reboot if a new firmware image is being installed. ZTP goes to "Failed" state if the switch receives DHCP IP for vlan1 and does not receive any ZTP options within 60 seconds.

**Initial configuration using the CLI**

This procedure describes how to connect to the switch for the first time and configure basic operational settings using the CLI. In this procedure, you use a computer to connect to the switch using the either the console port or management port.

**Procedure**
1. Connect to the console port or the management port.
2. Log into the switch for the first time.
3. Configure switch time using the NTP client.

Connecting to the console port

Prerequisites

- A switch installed as described in its hardware installation guide.
- A computer with terminal emulation software.

Procedure

1. Start the terminal emulation software on the computer and configure a new serial session with the following settings:
   - Speed: 115200 bps
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow control: None
2. Start the terminal emulation session.
3. Press Enter once. If the connection is successful, you are prompted to login.

Optional console port speed setting

If desired, the console port speed can be set with the console baud-rate command. For example, setting the console port speed to 9600 bps:

```
switch(config)# console baud-rate 9600
```

This command will configure the baud rate immediately for the active serial console session. After the command is executed the user will be prompted to re-login. The serial console will be inaccessible until the terminal client settings are updated to match the baud rate of the switch.

```
Continue (y/n)? y
```

Showing the console port current speed:

```
switch# show console
Baud Rate: 9600
```

For details on the console baud-rate and show console commands, see Switch system and hardware commands.

Connecting to the in-band management port

Prerequisites

- Two Ethernet cables
- SSH client software

Procedure
1. By default, the in-band management interface is set to automatically obtain an IP address from a DHCP server, and SSH support is enabled. If there is no DHCP server on your network, you must configure a static address on the in-band management interface:
   a. Connect to the console port
   b. Configure using DHCP or static IP.
   c. Configure the in-band management interface and interface VLAN1.

2. Use an Ethernet cable to connect the management port to your network.
3. Use an Ethernet cable to connect your computer to the same network.
4. Start your SSH client software and configure a new session using the address assigned to the in-band management interface. (If the in-band management interface is set to operate as a DHCP client, retrieve the IP address assigned to the in-band management interface from your DHCP server.)
5. Start the session. If the connection is successful, you are prompted to log in.

**Configure using DHCP or static IP**

Users can use any data ports for in-band management purposes. IP DHCP is supported on interface VLAN 1 only. All switch ports are part of access VLAN 1 by default. Static IP address and IP DHCP configuration can co-exist on VLAN 1, however static addresses take precedence whenever configured.

**DHCP Configuration**

```plaintext
switch#: config
switch(config)#: vlan 1
Switch(config-vlan-1)#: description Management VLAN
Switch(config-vlan-1)#: end
Switch#

! Switch(config)#: interface 1/1/1
Switch(config-if)#: description IN-BAND Management Port
Switch(config-if)#: vlan access 1
Switch(config-if)#: no shutdown
Switch(config-if)#: end
Switch#

! Switch(config)#: interface vlan 1
Switch(config-if-vlan)#: description IN-BAND Management Interface
Switch(config-if-vlan)#: ip dhcp
Switch(config-if-vlan)#: no shutdown
Switch(config-if-vlan)#: end
Switch#
```

**Without DHCP Configuration**

```plaintext
switch#: config
switch(config)#: vlan 1
Switch(config-vlan-1)#: description Management VLAN
Switch(config-vlan-1)#: end
Switch#

! Switch(config)#: interface 1/1/1
Switch(config-if)#: description IN-BAND Management Port
Switch(config-if)#: vlan access 1
Switch(config-if)#: no shutdown
```
Switch(config-if)#: end
Switch#
!
Switch(config)#: interface vlan 1
Switch(config-if-vlan)#: description IN-BAND Management Interface
Switch(config-if-vlan)#: no ip dhcp
Switch(config-if-vlan)#: ip address 192.168.10.1/24
Switch(config-if-vlan)#: no shutdown
Switch(config-if-vlan)#: end
Switch#

Logging into the switch for the first time

The first time you log in to the switch you must use the default administrator account. This account has no password, so you will be prompted on login to define one to safeguard the switch.

Procedure

1. When prompted to log in, specify admin. When prompted for the password, press ENTER. (By default, no password is defined.)
   For example:
   
   switch login: admin
   password:

2. Define a password for the admin account. The password can contain up to 32 alphanumeric characters in the range ASCII 32 to 127, which includes special characters such as asterisk (*), ampersand (&), exclamation point (!), dash (-), underscore (_), and question mark (?).
   For example:
   
   Please configure the 'admin' user account password.
   Enter new password: ********
   Confirm new password: ********
   switch#

3. You are placed into the manager command context, which is identified by the prompt: switch#, where switch is the model number of the switch. Enter the command config to change to the global configuration context config.
   For example:
   
   switch# config
   switch(config)#

Setting switch time using the NTP client

Prerequisites

- The IP address or domain name of an NTP server.
- If the NTP server uses authentication, obtain the password required to communicate with the NTP server.
Procedure

1. If the NTP server requires authentication, define the authentication key for the NTP client with the command `ntp authentication`.
2. Configure an NTP server with the command `ntp server`.
3. By default, NTP traffic is sent on the default VRF.
4. Review your NTP configuration settings with the commands `show ntp servers` and `show ntp status`.
5. See the current switch time, date, and time zone with the command `show clock`.

Example

This example creates the following configuration:

- Defines the authentication key 1 with the password `myPassword`.
- Defines the NTP server `my-ntp.mydomain.com` and makes it the preferred server.

```
switch(config)# ntp authentication-key 1 md5 myPassword
switch(config)# ntp server my-ntp.mydomain.com key 10 prefer
switch(config)# ntp vrf default
```

Configuring banners

1. Configure the banner that is displayed when a user connects to a device using a console port or in-band management interface. Use the command `banner motd`. For example:

```
switch(config)# banner motd ^
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> This is an example of a banner text which a connecting user
>> will see before they are prompted for their password.
>>
>> As you can see it may span multiple lines and the input
>> will be terminated when the delimiter character is
>> encountered. ^
Banner updated successfully!
```

2. Configure the banner that is displayed after a user is authenticated. Use the command `banner exec`. For example:

```
switch(config)# banner exec &
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> This is an example of a different banner text. This time
>> the banner entered will be displayed after a user has
>> authenticated.
>>
>> & This text will not be included because it comes after the ' &' 
Banner updated successfully!
```

Using the Web UI

Prerequisites
A connection to the switch CLI.

On the 6000 and 6100, the HTTPS server can only be enabled by the default VRF.

On the 4100i, the HTTPS server can only be enabled by the default VRF.

**Procedure**

1. Log in to the CLI.
2. Switch to config context.
   
   For example:

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

3. The Web UI starts and you are prompted to log in.

**Configuring the in-band management interface**

**Prerequisites**
A connection to the console port.

**Procedure**

1. Switch to the in-band management interface context with the command `interface vlan 1`.
2. By default, the in-band management interface is enabled. If it was disabled, re-enable it with the command `no shutdown`.
3. Use the command `ip dhcp` to configure the in-band management interface to automatically obtain an address from a DHCP server on the network (factory default setting). Or, assign a static IPv4 or IPv6 address with the commands `ip address` or `ipv6 address`.
4. SSH is enabled by default on the default VRF. If disabled, enable SSH with the command `ssh server vrf default`.

**Examples**
This example enables the in-band management interface with static addressing:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip dhcp
switch(config-if-vlan)# ip address 192.168.100.200/24
switch(config-if-vlan)# no shutdown
```

**Restoring the switch to factory default settings**

**Prerequisites**
You are connected to the switch through its Console port.
This procedure erases all user information and configuration settings. Consider backing up your running configuration first.

1. Optionally, back up the running configuration with either `copy running-config <REMOTE-URL>` or `copy running-config <STORAGE-URL>`. The JSON storage format is required for later configuration restoration.

2. Switch to the configuration context with the command `config`.

3. Erase all user information and configuration, restoring the switch to its factory default state with the command `erase all zeroize`. Enter `y` when prompted to continue. The switch automatically restarts.

4. Optionally restore your saved configuration (it must be in JSON format) with either `copy <REMOTE-URL> running-config` or `copy <STORAGE-URL> running-config` followed by `copy running-config startup-config`.

**Example**

Backing up the running configuration to a file on a remote server (using TFTP), resetting the switch to its factory default state, and then restoring the saved configuration.

```
switch# copy running-config tftp://10.100.1.12/backup_cfg json vrf default

% Total  % Received % Xferd     Average Speed Time  Time  Time     Current
     100   10340   0       0  100 10340      0  1329k --:--:-- --:--:-- --:--:-- 1329k
     100   10340   0       0  100 10340      0  1313k --:--:-- --:--:-- --:--:-- 1313k

switch#
switch# erase all zeroize

This will securely erase all customer data and reset the switch to factory defaults. This will initiate a reboot and render the switch unavailable until the zeroization is complete. This should take several minutes to one hour to complete.

Continue (y/n)? y

The system is going down for zeroization.

[ OK ] Stopped PSPO Module Daemon.
[ OK ] Stopped AOS-CX Switch Daemon for BCM.
...
[ OK ] Reached target Shutdown.

reboot: Restarting system
Press Esc for boot options

ServiceOS Information:

Version: GT.01.03.0006
Build Date: 2018-10-30 14:20:44 PDT
Build ID: ServiceOS:GT.01.03.0006:8ee0faaa52da:201810301420
SHA: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
...

Preparing for zeroization

Storage zeroization

WARNING: DO NOT POWER OFF UNTIL

ZEROIZATION IS COMPLETE

This should take several minutes to one hour to complete

Restoring files
```
Boot Profiles:
0. Service OS Console
1. Primary Software Image [XL.10.02.0010]

Select profile (primary):

Booting primary software image...
Verifying Image...

Image Info:
    Name: AOS-CX
    Version: XL.10.02.0010
    Build Id: AOS-CX:XL.10.02.0010:feaf5b9b7f09:201901292014
    Build Date: 2019-01-29 12:43:50 PST

Extracting Image...
Loading Image...
Done.

kexec_core: Starting new kernel
System is initializing
fips_post_check[5473]: FIPS_POST: Cryptographic selftest started...SUCCESS
[ OK ] Started Login banner readiness check.
...
8400X login: admin
Password:

switch#
switch#
switch# **copy tftp://192.168.1.10/backup_cfg running-config** json vrf default

Large configuration changes will take time to process, please be patient.

switch#

NTP commands

ntp authentication

ntp authentication
no ntp authentication

Description

Enables support for authentication when communicating with an NTP server.
The no form of this command disables authentication support.

Examples

Enabling authentication support:
switch(config)# ntp authentication

Disabling authentication support:

switch(config)# no ntp authentication

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp authentication-key**

ntp authentication-key <KEY-ID> {md5 | sha1}

[[ <PLAINTXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> ]]

no ntp authentication-key <KEY-ID> {md5 | sha1}

[[ <PLAINTXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> ]]

**Description**

Defines an authentication key that is used to secure the exchange with an NTP time server. This command provides protection against accidentally synchronizing to a time source that is not trusted.

The no form of this command removes the authentication key.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;KEY-ID&gt;</td>
<td>Specifies the authentication key ID. Range: 1 to 65534.</td>
</tr>
<tr>
<td>md5</td>
<td>Selects MD5 key encryption.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specifies SHA1 key encryption.</td>
</tr>
<tr>
<td>&lt;PLAINTXT-KEY&gt;</td>
<td>Specifies the plaintext authentication key. Range: 8 to 40 characters. The key may contain printable ASCII characters excluding &quot;#&quot; or be entered in hex. Keys longer than 20 characters are assumed to be hex. To use an ASCII key longer than 20 characters, convert it to hex.</td>
</tr>
<tr>
<td>trusted</td>
<td>Specifies that this is a trusted key. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.</td>
</tr>
<tr>
<td>Parameter</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>ciphertext &lt;ENCRYPTED-KEY&gt;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the ciphertext authentication key in Base64 format. This is used to restore the NTP authentication key when copying configuration files between switches or when uploading a previously saved configuration.</td>
</tr>
</tbody>
</table>

**NOTE:**
When the key is not provided on the command line, plaintext key prompting occurs upon pressing Enter, followed by prompting as to whether the key is to be trusted. The entered key characters are masked with asterisks.

**Examples**

Defining key 10 with MD5 encryption and a provided plaintext trusted key:

```
switch(config)# ntp authentication-key 10 md5 F82#450b trusted
```

Defining key 5 with SHA1 encryption and a prompted plaintext trusted key:

```
switch(config)# ntp authentication-key 5 sha1
Enter the NTP authentication key: *********
Re-Enter the NTP authentication key: *********
Configure the key as trusted (y/n)? y
```

Removing key 10:

```
switch(config)# no ntp authentication-key 10
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp disable**

**Description**

Disables the NTP client on the switch. The NTP client is disabled by default.
Examples
Disabling the NTP client.

```
switch(config)# ntp disable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp enable**

```
ntp enable
no ntp enable
```

**Description**

Enables the NTP client on the switch to automatically adjust the local time and date on the switch. The NTP client is disabled by default.

The no form of this command disables the NTP client.

**Examples**

Enabling the NTP client.

```
switch(config)# ntp enable
```

Disabling the NTP client.

```
switch(config)# no ntp enable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp server**

ntp server `<IP-ADDR>` [key `<KEY-NUM>`] [minpoll `<MIN-NUM>`] [maxpoll `<MAX-NUM>`][burst | iburst] [prefer] [version `<VER-NUM>`]

no ntp server `<IP-ADDR>` `<IP-ADDR>` [key `<KEY-NUM>`] [minpoll `<MIN-NUM>`] [maxpoll `<MAX-NUM>`] [burst | iburst] [prefer] [version `<VER-NUM>`]

**Description**

Defines an NTP server to use for time synchronization, or updates the settings of an existing server with new values. Up to eight servers can be defined.

The no form of this command removes a configured NTP server.

---

The default NTP version is 4; it is backwards compatible with version 3.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server <code>&lt;IP-ADDR&gt;</code></td>
<td>Specifies the address of an NTP server as a DNS name, an IPv4 address (x.x.x.x), where x is a decimal number from 0 to 255, or an IPv6 address (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. When specifying an IPv4 address, you can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100. When specifying an IPv6 address, you can use two colons (:) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222::3333::4444:55.</td>
</tr>
<tr>
<td>key <code>&lt;KEY-NUM&gt;</code></td>
<td>Specifies the key to use when communicating with the server. A trusted key must be defined with the command ntp authentication-key and authentication must be enabled with the command ntp authentication. Range: 1 to 65534.</td>
</tr>
<tr>
<td>minpoll <code>&lt;MIN-NUM&gt;</code></td>
<td>Specifies the minimum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 6 (64 seconds).</td>
</tr>
<tr>
<td>maxpoll <code>&lt;MAX-NUM&gt;</code></td>
<td>Specifies the maximum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 10 (1024 seconds).</td>
</tr>
<tr>
<td>burst</td>
<td>Send a burst of packets instead of just one when connected to the server. Useful for reducing phase noise when the polling interval is long.</td>
</tr>
<tr>
<td>iburst</td>
<td>Send a burst of six packets when not connected to the server. Useful for reducing synchronization time at startup.</td>
</tr>
<tr>
<td>prefer</td>
<td>Make this the preferred server.</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version &lt;VER-NUM&gt;</td>
<td>Specifies the version number to use for all outgoing NTP packets. Range: 3 or 4. Default: 4. NOTE: NTP is backwards compatible.</td>
</tr>
</tbody>
</table>

#### Usage

For features such as Activate and ZTP, a switch that has a factory default configuration will automatically be configured with pool.ntp.org. NTP server configurations via DHCP options are supported. The DHCP server can be configured with maximum of two NTP server addresses which will be supported on the switch. Only IPV4 addresses are supported.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 time server.

When using multiple servers with same stratum setting, the best practice to configure a preferred server, so NTP will attempt to use the preferred server as the primary NTP connection. If a preferred server is not manually set when NTP is enabled, the configured server with the lowest stratum will automatically be set as the preferred server. If there are servers with the same stratum, this auto prefer status will prevent AOS-CX from toggling between different servers as the primary server. Auto prefer selection of servers with same stratum (if not manually selected) may change after reconfiguring the switch, or after executing the `reboot` command.

#### Examples

Defining the ntp server pool.ntp.org, using iburst, and NTP version 4.

```
switch(config)# ntp server pool.ntp.org iburst version 4
```

Removing the ntp server pool.ntp.org.

```
switch(config)# no ntp server pool.ntp.org
```

Defining the ntp server my-ntp.mydomain.com and makes it the preferred server.

```
switch(config)# ntp server my-ntp.mydomain.com prefer
```

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

#### Command Information
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp trusted-key**

`ntp trusted-key <KEY-ID>`
`no ntp trusted-key <KEY-ID>`

**Description**

Sets a key as trusted. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.

The `no` form of this command removes the trusted designation from a key.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;KEY-ID&gt;</td>
<td>Specifies the identification number of the key to set as trusted. Range: 1 to 65534.</td>
</tr>
</tbody>
</table>

**Examples**

Defining key 10 as a trusted key.

```
switch(config)# ntp trusted-key 10
```

Removing trusted designation from key 10:

```
switch(config)# no ntp trusted-key 10
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ntp vrf**

`ntp vrf <VRF-NAME>`
`no ntp vrf <VRF-NAME>`

**Description**
6000 and 6100 only support default VRF.

4100i only supports default VRF.

Specifies the VRF on which the NTP client communicates with an NTP server.
The no form of the command returns to default VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF.</td>
</tr>
</tbody>
</table>

**Example**

Setting the switch to use the default VRF for NTP client traffic.

```
switch(config)# ntp vrf default
```

Returning the switch to use the default VRF for NTP client traffic.

```
switch(config)# no ntp vrf
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ntp associations**

**Description**

Shows the status of the connection to each NTP server. The following information is displayed for each server:

- **Tally code**: The first character is the Tally code:
  - (blank): No state information available (e.g. non-responding server)
  - x: Out of tolerance (discarded by intersection algorithm)
  - .: Discarded by table overflow (not used)
  - -: Out of tolerance (discarded by the cluster algorithm)
+ : Good and a preferred remote peer or server (included by the combine algorithm)
# : Good remote peer or server, but not utilized (ready as a backup source)
*: Remote peer or server presently used as a primary reference
o : PPS peer (when the prefer peer is valid)

ID: Server number.
NAME: NTP server FQDN/IP address (Only the first 24 characters of the name are displayed).
REMOTE: Remote server IP address.
REF_ID: Reference ID for the remote server (Can be an IP address).
ST: (Stratum) Number of hops between the NTP client and the reference clock.
LAST: Time since the last packet was received in seconds unless another unit is indicated.
POLL: Interval (in seconds) between NTP poll packets. Maximum (1024) reached as server and client sync.
REACH: 8-bit octal number that displays status of the last eight NTP messages (377 = all messages received).

Example

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>REMOTE</th>
<th>REF- ID</th>
<th>ST</th>
<th>LAST</th>
<th>POLL</th>
<th>REACH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.0.1.1</td>
<td>192.0.1.1</td>
<td>.INIT.</td>
<td>16</td>
<td>-</td>
<td>64</td>
<td>0</td>
</tr>
<tr>
<td>*</td>
<td>time.apple.com</td>
<td>17.253.2.253</td>
<td>.GPSs.</td>
<td>2</td>
<td>70</td>
<td>128</td>
<td>377</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show ntp authentication-keys

Description
Shows the currently defined authentication keys.

Examples
switch# show ntp authentication-keys
----------------------------------------
Auth key  Trusted  MD5 password
----------------------------------------
  10      No **********
  20     Yes **********

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show ntp servers

show ntp servers

Description

Shows all configured NTP servers, including any DHCP servers, default pool servers or any server with the status auto prefer.

Example

switch# show ntp servers
----------------------------------------
                                      NTP SERVER  KEYID MINPOLL MAXPOLL OPTION VER
----------------------------------------
  192.0.1.18 -    5   10  iburst   3
  192.0.1.19 -    6   10   none   4
  192.0.1.20 -    6    8  burst   3  prefer
----------------------------------------

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
**show ntp statistics**

```
switch(config)# show ntp statistics
Rx-pkts 100
Current Version Rx-pkts 80
  Old Version Rx-pkts 20
    Err-pkts 2
    Auth-failed-pkts 1
    Declined-pkts 0
    Restricted-pkts 0
    Rate-limited-pkts 0
    KoD-pkts 0
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ntp status**

```
switch(config)# show ntp status
```

**Description**

Shows the status of NTP on the switch.

**Examples**
Displaying the status information when the switch is not synced to an NTP server:

```plaintext
switch# show ntp status
NTP is enabled.
NTP authentication is enabled.
NTP is using the default VRF for NTP server connections.

NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds

Not synchronized with an NTP server.
```

Displaying the status information when the switch is synced to an NTP server:

```plaintext
switch# show ntp status
NTP is enabled.
NTP authentication is enabled.
NTP is using the default VRF for NTP server connections.

NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds

Synchronized to NTP Server 17.253.2.253 at stratum 2.
Poll interval = 1024 seconds.
Time accuracy is within 0.994 seconds
Reference time: Thu Jan 28 2016 0:57:06.647 (UTC)
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
Configuring a layer 2 interface

Procedure

1. Change to the interface configuration context for the interface with the command `interface`.
2. Set the interface MTU (maximum transmission unit) with the command `mtu`.
3. Review interface configuration settings with the command `show interface`.

Single source IP address

Certain IP-based protocols used by the switch (such as RADIUS, sFlow, TACACS, and TFTP), use a client-server model in which the client's source IP address uniquely identifies the client in packets sent to the server. By default, the source IP address is defined as the IP address of the outgoing switch interface on which the client is communicating with the server. Since the switch can have multiple routing interfaces, outgoing packets can potentially be sent on different paths at different times. This can result in different source IP addresses being used for a client, which can create a client identification problem on the server. For example, it can be difficult to interpret system logs and accounting data on the server when the same client is associated with multiple IP addresses.

To resolve this issue, you can use the commands `ip source-interface` and `ipv6 source-interface` to define a single source IP address that applies to all supported protocols (RADIUS, sFlow, TACACS, and TFTP), or an individual address for each protocol. This ensures that all traffic sent by a client to a server uses the same IP address.

Priority-based flow control

Priority-based flow control (PFC) is defined in the IEEE 802.1Qbb standard. It is a link-level flow control mechanism intended to eliminate packet loss due to congestion on a network link.

For interfaces that auto-negotiate, link-level flow control is subject to negotiation, along with speed and other parameters. Both ends of the link must negotiate the same flow control mode for it to be applied.

For interfaces that do not auto-negotiate, the configured link-level flow control mode is always applied and the user is responsible for ensuring that both ends of the link are configured for the same mode.

Unsupported transceiver support

Transceiver products (optical, DAC, AOCs) that are listed as supported by a switch model are detailed in the Transceiver Guide. Transceiver products that are not listed, are considered unsupported; this would include transceivers that are:

- Non-Aruba branded products
- HPE branded products that were designed for non-AOS-CX switch models (e.g. Comware)
- HPE branded products designated for use in HPE Compute Servers or Storage
- Transceivers originally designated for use in Aruba WLAN controllers or former Mobility Access Switch (MAS) products
- End-of-life Aruba Transceivers

The unsupported transceiver mode (UT-mode) is designed to allow the possible use of these unsupported products. Not all unsupported products can be recognized and enabled; they may be unable to be identified (do not follow the proper MSA standards for identification). These unsupported transceiver products are enabled only on a best-effort basis and there are no guarantees implied for their continued operation.

This feature is enabled by default. A periodic system log will be generated by default at an interval of 24 hours listing the ports on which unsupported transceivers are present. The log interval is configurable and can be disabled by setting the log-interval to none.

### Interface commands

**allow-unsupported-transceiver**

allow-unsupported-transceiver [confirm | log-interval {none | <INTERVAL>}]  
no allow-unsupported-transceiver

**Description**

Allows unsupported transceivers to be enabled or establish connections. Only 1G and 10G transceivers are enabled by this command, unsupported transceivers of other speeds will remain disabled.

As of AOS-CX 10.06.0100, this command is enabled by default, allowing the use of third party transceiver products without adding the command in the config. Disabling this command with the no form will now display the command in the running and stored configurations.

The no form of this command disallows using unsupported transceivers.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>confirm</td>
<td>Specifies that unsupported transceiver warnings are to be automatically confirmed.</td>
</tr>
<tr>
<td>log-interval none</td>
<td>Disables unsupported transceiver logging.</td>
</tr>
<tr>
<td>log-interval &lt;INTERVAL&gt;</td>
<td>Sets the unsupported transceiver logging interval in minutes. Default: 1440 minutes. Range: 1440 to 10080 minutes.</td>
</tr>
</tbody>
</table>

**Usage**

When none of the parameters are specified it will display a warning message to accept the warranty terms. With confirm option the warning message is displayed but the user is not prompted to (y/n) answering. Warranty terms must be agreed to as part of enablement and the support is on best effort basis.

**Examples**

Allowing unsupported transceivers with follow-up confirmation:
switch(config)# **allow-unsupported-transceiver**
Warning: The use of unsupported transceivers, DACs, and AOCs is at your own risk and may void support and warranty. Please see HPE Warranty terms and conditions.

Do you agree and do you want to continue (y/n)? y

Allowing unsupported transceivers with confirmation in command syntax:

```
switch(config)# **allow-unsupported-transceiver confirm**
Warning: The use of unsupported transceivers, DACs, and AOCs is at your own risk and may void support and warranty. Please see HPE Warranty terms and conditions.
```

Configuring unsupported transceiver logging with an interval of every 48 hours:

```
switch(config)# **allow-unsupported-transceiver log-interval 2880**
```

Disabling unsupported transceiver logging:

```
switch(config)# **allow-unsupported-transceiver log-interval none**
```

Disallowing unsupported transceivers with follow-up confirmation:

```
switch(config)# **no allow-unsupported-transceiver**
Warning: Unsupported transceivers, DACs, and AOCs will be disabled, which could impact network connectivity. Use 'show allow-unsupported-transceiver' to identify unsupported transceivers, DACs, and AOCs.
Continue (y/n)? y
```

Disallowing unsupported transceivers with confirmation in command syntax:

```
switch(config)# **no allow-unsupported-transceiver confirm**
Warning: Unsupported transceivers, DACs, and AOCs will be disabled, which could impact network connectivity. Use 'show allow unsupported-transceiver' to identify unsupported transceivers, DACs, and AOCs.
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
**default interface**

default interface <INTERFACE-ID>

**Description**
Sets an interface (or a range of interfaces) to factory default values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;INTERFACE-ID&gt;</td>
<td>Specifies the ID of a single interface or range of interfaces. Format: member/slot/port or member/slot/port-member/slot/port to specify a range.</td>
</tr>
</tbody>
</table>

**Examples**

Resetting an interface:

```
switch(config)# default default interface 1/1/1
```

Resetting a range of interfaces:

```
switch(config)# default default interface 1/1/1-1/1/10
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
<DESCRIPTION> | Specify a description for the interface. Range: 1 to 64 ASCII characters (including space, excluding question mark).

**Examples**

Setting the description for an interface to **DataLink 01**:

```
switch(config-if)# description DataLink 01
```

Removing the description for an interface:

```
switch(config-if)# no description
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**energy-efficient-ethernet**

**energy-efficient-ethernet**

**Description**

Enables auto-negotiation of Energy-Efficient Ethernet (EEE) on an interface. EEE Negotiation is established only on auto-link negotiation with supported link partners.

**Examples**

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# energy-efficient-ethernet
```

Disabling Energy Efficient Ethernet on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no energy-efficient-ethernet
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### flow-control

**Syntax**

- `flow-control rxtx`
- `no flow-control rxtx`

**Description**

Enables negotiation of IEEE 802.3x link-level flow control on the current interface. The switch advertises link-level flow-control support to the link partner. The final configuration is determined based on the capabilities of both partners.

The `no` form disables flow control support on the current interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rxtx</td>
<td>Enables the ability to respect and generate IEEE 802.3x link-level pause frames on the current interface.</td>
</tr>
</tbody>
</table>

**Usage**

Care must be taken to ensure proper lossless flow control operation:

- Lossless flow control will only operate correctly when both the ingress and egress interfaces have flow control enabled.
- All members of a LAG must have the same flow control configuration.
- Lossless flow control is only supported for single destination unicast traffic. Replicated traffic (e.g., broadcast, multicast, mirroring) cannot be guaranteed to be lossless.
- Lossless behavior is not supported when operating in a VSF stack configuration.
- Any queue used by protocol or control traffic must not be configured for lossless behavior. Routing protocols and VSX-synchronization messages use local-priority 7, therefore the CoS priority mapped to local-priority 7 should not be used in any lossless configuration.

For example, in a default configuration, the CoS map assigns local-priority 7 to packets arriving with VLAN priority 7. This means that lossless pools should not be configured to use priority 7, and that interfaces should not be configured with 'flow-control priority 7', since that VLAN priority maps to local-priority 7.

**Examples**
Enable support for RX and TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control rxtx
```

Disable support for RX and TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control rxtx
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### interface (port)

**interface <PORT-NUM>**

**Description**

Switches to the config-if context for a physical port. This is where you define the configuration settings for the logical interface associated with the physical port.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PORT-NUM&gt;</td>
<td>Specifies a physical port number. Format: member/slot/port.</td>
</tr>
</tbody>
</table>

### Examples

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)#
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information
interface vlan

interface vlan <VLAN-ID>
no interface vlan <VLAN-ID>

Description
Creates an interface VLAN also know as an SVI (switched virtual interface) and changes to the `config-if-vlan` context. The specified VLAN must already be defined on the switch. The `no` form of this command deletes an interface VLAN.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>Specifies the interface ID. Range: 2 to 4094</td>
</tr>
</tbody>
</table>

Examples

```
switch# config
switch(config)# vlan 10
switch(config-vlan-10)# exit
switch(config)# interface vlan 10
switch(config-if-vlan)#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ip address

ip address <IPV4-ADDR>/<MASK> [secondary]
no ip address <IPV4-ADDR>/<MASK> [secondary]

Description
Sets an IP/IPv6 address on the interface VLAN.
The `no` form of this command removes the IP/IPv6 address from the interface.
Parameter | Description
---|---
<IPV4-ADDR> | Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.
<MASK> | Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
secondary | Specifies a secondary IP address.

Examples
Assigning the IP address **192.168.199.1** with a mask of **24** bits to interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 192.168.199.1/24
```

Removing the IP address **192.168.199.1** with a mask of **24** bits from interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no ip address 192.168.199.1/24
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip mtu**

```
ip mtu <VALUE>
no ip mtu
```

Description

Sets the IP MTU (maximum transmission unit) for an interface. This defines the largest IP packet that can be sent or received by the interface.

The **no** form of this command sets the IP MTU to the default value 1500.

Parameter | Description
---|---
Examples
Setting the IP MTU to 576 bytes:

```
switch(config-if-vlan)# ip mtu 576
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Subinterface support added.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip source-interface**

```
ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | simplivity | dns | all} [interface <IFNAME> | <IPV4-ADDR>] [vrf <VRF-NAME>]
no ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | simplivity | dns | all} [interface <IFNAME> | <IPV4-ADDR>] [vrf <VRF-NAME>]
```

Description
Sets a single source IP address for a feature on the switch. This ensures that all traffic sent the feature has the same source IP address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The no form of this command deletes the single source IP address for all supported services, or a specific service.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>tftp</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the name of the interface from which the specified service obtains its source IP address. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.</td>
</tr>
</tbody>
</table>
Parameter | Description
--- | ---
<IPV4-ADDR> | Specifies the source IP address to use for the specified service. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the default VRF, if the vrf option is not used). Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Setting the IPv4 address 10.10.10.5 as the global single source address:

```
switch# config
switch(config)# ip source-interface all 10.10.10.5
```

Clearing the global single source IP address 10.10.10.5:

```
switch(config)# no ip source-interface all 10.10.10.5
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 address**

```
ipv6 address <IPV6-ADDR>/<MASK>{eui64 | [tag <ID>])
nipv6 address <IPV6-ADDR>/<MASK>
```

Description

Sets an IPv6 address on the interface.
The no form of this command removes the IPv6 address on the interface.

This command automatically creates an IPv6 link-local address on the interface. However, it does not add the ipv6 address link-local command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the ipv6 address link-local command.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the IP address in IPv6 format (xxxx::xxxx::xxxx::xxxx::xxxx::xxxx), where x is a hexadecimal number from 0 to F. You can use two colons (:) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:4444:0055 becomes 2222:0:3333::4444:55.</td>
</tr>
<tr>
<td>&lt;MASK&gt;</td>
<td>Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.</td>
</tr>
<tr>
<td>eui64</td>
<td>Configure the IPv6 address in the EUI-64 bit format.</td>
</tr>
<tr>
<td>tag &lt;ID&gt;</td>
<td>Configure route tag for connected routes. Range: 0 to 4294967295. Default: 0.</td>
</tr>
</tbody>
</table>

**Examples**

Setting the IPv6 address 2001:0db8:85a3::8a2e:0370:7334 with a mask of 24 bits:

```
switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```

Removing the IP address 2001:0db8:85a3::8a2e:0370:7334 with mask of 24 bits:

```
switch(config-if)# no ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 source-interface**

```
ipv6 source-interface {sflow | tftp | radius | tacacs | ntp | syslog | simplivity | dns | all} [interface <IFNAME> | <IPV6-ADDR>]
no ipv6 source-interface {sflow | tftp | radius | tacacs | ntp | syslog | simplivity | dns | all} [interface <IFNAME> | <IPV6-ADDR>]
```

**Description**

Sets a single source IP address for a feature on the switch. This ensures that all traffic sent the feature has the same source IP address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.
This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The no form of this command deletes the single source IP address for all supported protocols, or a specific protocol.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>tftp</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the name of the interface from which the specified protocol obtains its source IP address.</td>
</tr>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the source IP address to use for the specified protocol. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the default VRF). Specify the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring the IPv6 address 2001:DB8::1 as the global single source address:

```
switch# config
switch(config)# ip source-interface all 2001:DB8::1/32
```

Stop the source IP address from using the IP address on interface 1/1/1 on VRF default.

```
switch(config)# no ip source-interface all interface 1/1/1 vrf default
```

Clear the source IP address 2001:DB8::1.

```
switch(config)# no ip source-interface all 2001:DB8::1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**mtu**
mtu <VALUE>
no mtu

**Description**
Sets the MTU (maximum transmission unit) for an interface. This defines the maximum size of a layer 2 (Ethernet) frame. Frames larger than the MTU (1500 bytes by default) are dropped.
To support jumbo frames (frames larger than 1522 bytes), increase the MTU as required by your network. A frame size of up to 9198 bytes is supported.
The largest possible layer 1 frame will be 18 bytes larger than the MTU value to allow for link layer headers and trailers.
The no form of this command sets the MTU to the default value 1500.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VALUE&gt;</td>
<td>Specifies the MTU in bytes. Range: 46 to 9198. Default: 1500.</td>
</tr>
</tbody>
</table>

**Examples**
Setting the MTU on interface **1/1/1** to 1000 bytes:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# mtu 1000
```

Setting the MTU on interface **1/1/1** to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# no mtu
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**persona**

`persona {access | uplink | custom <PERSONA>}
no persona`

**Description**
Associates one of three persona types with an interface to classify the purpose or role of an interface. On the 10000 Switch Series, “access” persona ports are typically connected to workloads / VMs, and the “uplink” (fabric) persona ports are connected to the core / spine.

Although this command is available on every platform, as of AOS-CX 10.09, the persona setting is only used by the 10000 Switch Series.

The no form of this command removes the interface persona.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Selects the access persona type.</td>
</tr>
<tr>
<td>uplink</td>
<td>Selects the uplink persona type.</td>
</tr>
<tr>
<td>custom &lt;PERSONA&gt;</td>
<td>Selects the custom persona type with a user-provided name. Range: 1 to 64 printable ASCII characters including space.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring an access persona:

```text
switch(config-if)# persona access
```

Configuring an uplink persona:

```text
switch(config-if)# persona uplink
```

Configuring a custom persona:

```text
switch(config-if)# persona custom special
```

Removing the persona setting:

```text
switch(config-if)# no persona
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.09</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
show allow-unsupported-transceiver

Description
Displays configuration and status of unsupported transceivers.

Examples
Showing unallowed unsupported transceivers:

```
switch(config)# show allow-unsupported-transceiver
Allow unsupported transceivers : no
Logging interval : 1440 minutes

-----------------------------
Port | Type     | Status
-----------------------------
1/1/31 | SFP-SX   | unsupported
1/1/32 | SFP-1G-BXD | unsupported
1/1/2  | SFP28DAC3 | unsupported
```

Showing allowed unsupported transceivers:

```
switch# show allow-unsupported-transceiver
Allow unsupported transceivers : yes
Logging interval : 1440 minutes

-----------------------------
Port | Type     | Status
-----------------------------
1/1/31 | SFP-SX   | unsupported-allowed
1/1/32 | SFP-1G-BXD | unsupported-allowed
1/1/2  | SFP28DAC3 | unsupported
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show interface

```
show interface [<IFNAME>|<IFRANGE>] [brief | physical | extended [non-zero]]
show interface [lag | vlan ] [<ID>] [brief | physical]
show interface [lag | vlan ] [<ID>] [extended [non-zero]]
```

Description
Shows active configurations and operational status information for interfaces.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IFNAME&gt;</code></td>
<td>Specifies a interface name.</td>
</tr>
<tr>
<td><code>&lt;IFRANGE&gt;</code></td>
<td>Specifies the port identifier range.</td>
</tr>
<tr>
<td>brief</td>
<td>Shows brief info in tabular format.</td>
</tr>
<tr>
<td>physical</td>
<td>Shows the physical connection info in tabular format.</td>
</tr>
<tr>
<td>extended</td>
<td>Shows additional statistics.</td>
</tr>
<tr>
<td>non-zero</td>
<td>Shows only non zero statistics.</td>
</tr>
<tr>
<td>LAG</td>
<td>Shows LAG interface information.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Shows VLAN interface information.</td>
</tr>
<tr>
<td><code>&lt;LAG-ID&gt;</code></td>
<td>Specifies the LAG number. Range: 1-256</td>
</tr>
<tr>
<td><code>&lt;VLAN-ID&gt;</code></td>
<td>Specifies the VLAN ID. Range: 1-4094</td>
</tr>
</tbody>
</table>

Examples

The following example shows when interface 1/1/1 is configured:

```
switch# show interface 1/1/1
Interface 1/1/1 is up
  Admin state is up
  Link state: up for 1 minute (since Thu Nov 26 10:26:34 UTC 2020)
  Link transitions: 3
  Description:
    Hardware: Ethernet, MAC Address: 88:3a:30:47:d1:df
    MTU 1500
    Type 1GbT
    Full-duplex
    qos trust cos
    Speed 1000 Mb/s
    Auto-negotiation is on
    Energy-Efficient Ethernet is disabled
    Flow-control: off
    Error-control: off
    MDI mode: MDIX
    VLAN Mode: native-untagged
    Native VLAN: 1
    Allowed VLAN List: all
  Rate collection interval: 300 seconds

Rates RX TX Total (RX+TX)
----------------- -------- -------- ------------
Mbits / sec      0.00      0.00      0.00
KPkts / sec      0.00      0.00      0.00
Unicast          0.00      0.00      0.00
Multicast        0.00      0.00      0.00
Broadcast        0.00      0.00      0.00
Utilization %    0.00      0.00      0.00

Statistics RX TX Total
------------------------
```
When the interface is currently linked at a downshifted speed:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...  
Auto-negotiation is on with downshift active
```

When the interface is currently linked with energy-efficient-ethernet negotiated:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...  
Energy-Efficient Ethernet is enabled and active
```

When the interface is configured with EEE and the EEE has auto-negotiated:

```
switch(config-if)# show interface 1/1/1 physical
```

```
---
<table>
<thead>
<tr>
<th>EEE Port Status</th>
<th>Power Type</th>
<th>PoE Power Status</th>
<th>Link Admin Status</th>
<th>Flow-Control Port Status</th>
<th>Config Status</th>
<th>Config State Information</th>
<th>Config Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1, 1G</td>
<td>--</td>
<td>1G</td>
<td>up</td>
<td>off</td>
<td>on</td>
<td>10M/100M/1G</td>
<td>--</td>
</tr>
</tbody>
</table>
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show interface dom

`show interface [<INTERFACE-ID>] dom [detail]`

Description

Shows diagnostics information and alarm/warning flags for the optical transceivers (SFP, SFP+). This information is known as DOM (Digital Optical Monitoring). DOM information also consists of vendor determined thresholds which trigger high/low alarms and warning flags.

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>Show detailed information.</td>
</tr>
</tbody>
</table>

Example

```
switch# show interface dom
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Channel</th>
<th>Temperature (Celsius)</th>
<th>Voltage (Volts)</th>
<th>Tx Bias (mA)</th>
<th>Rx Power (mW/dBm)</th>
<th>Tx Power (mW/dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>SFP+SR</td>
<td></td>
<td>47.65</td>
<td>3.31</td>
<td>8.40</td>
<td>0.08, -10.96</td>
<td>0.63, -2.49</td>
</tr>
<tr>
<td>1/1/2</td>
<td>SFP+SR</td>
<td></td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1/1/3</td>
<td>SFP+DA3</td>
<td></td>
<td>42.10</td>
<td>3.24</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1/1/4</td>
<td>QSFP+SR4</td>
<td>1</td>
<td>44.46</td>
<td>3.30</td>
<td>6.12</td>
<td>0.08, -10.96</td>
<td>0.63, -1.95</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>44.46</td>
<td>3.30</td>
<td>6.04</td>
<td>0.08, -10.96</td>
<td>0.63, -2.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>44.46</td>
<td>3.30</td>
<td>6.51</td>
<td>0.08, -10.96</td>
<td>0.60, -2.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>44.46</td>
<td>3.30</td>
<td>6.19</td>
<td>0.08, -10.96</td>
<td>0.63, -1.94</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
show interface energy-efficient ethernet

show interface [<IFNAME>|<IFRANGE>] energy-efficient-ethernet

Description
Displays Energy-Efficient Ethernet information for the interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IFNAME&gt;</td>
<td>Specifies the name of an interface on the switch. Use the format member/slot/port (for example, 1/1/1).</td>
</tr>
<tr>
<td>&lt;IFRANGE&gt;</td>
<td>Specifies the port identifier range of an interface on the switch. Use the format member/slot/port (for example, 1/1/1).</td>
</tr>
</tbody>
</table>

Example
The following example shows when the interfaces are Energy-Efficient Ethernet capable

switch# show interface energy-efficient-ethernet
-----------------------------------------
<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Negotiated</th>
<th>Speed (Mb/s)</th>
<th>TX Wake Time (us)</th>
<th>RX Wake Time (us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>no</td>
<td>no</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/1/2</td>
<td>yes</td>
<td>yes</td>
<td>100</td>
<td>36</td>
<td>36</td>
</tr>
<tr>
<td>1/1/3</td>
<td>yes</td>
<td>yes</td>
<td>1000</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>1/1/4</td>
<td>no</td>
<td>no</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>1/1/5</td>
<td>yes</td>
<td>no</td>
<td>1000</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

switch# show interface 1/1/1 energy-efficient-ethernet
-----------------------------------------
<table>
<thead>
<tr>
<th>Port</th>
<th>Enabled</th>
<th>Negotiated</th>
<th>Speed (Mb/s)</th>
<th>TX Wake Time (us)</th>
<th>RX Wake Time (us)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>no</td>
<td>no</td>
<td>1000</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

switch#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i 6000 6100</td>
<td>config</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show interface flow-control

show interface [<IFNAME>|<IFRANGE>] flow-control [detail]
Description
Displays the flow control configuration, status, and statistics of the specified interface.

If `detail` is not specified, the command displays a summary of all flow controlled interfaces with one interface per line. If `detail` is specified, the command displays details and statistics about flow control in a long form on the specified interfaces.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IFNAME&gt;</code></td>
<td>Specifies an interface name.</td>
</tr>
<tr>
<td><code>&lt;IFRANGE&gt;</code></td>
<td>Specifies the port identifier range.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>Show details and statistics of flow control.</td>
</tr>
</tbody>
</table>

Examples
Showing interfaces with flow control enabled in config or status:

```
switch# show interface flow-control
---------------------------
Port Flow Control Flow Control
     Config     Status
---------------------------
1/1/1  rxtx      rxtx
1/1/2  rxtx      off
```

Showing all interfaces in detail form:

```
switch# show interface flow-control detail
Interface 1/1/1 is up
 Admin state is up
 Flow-control: off

Interface 1/1/2 is up
 Admin state is up
 Flow-control: off

...```

Showing RXTX enabled flow control:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
 Admin state is up
 Flow-control: rxtx

Statistics
 Unconfigured Pause Frames
 Dot3 Pause Frames 0 0
```

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**show interface transceiver**

`show interface [<INTERFACE-ID>] transceiver [detail | threshold-violations]`

**Description**

Displays information about transceivers present in the switch. The information shown varies for different transceiver types and manufacturers. Only basic information is shown for unsupported HPE and third-party transceivers installed in the switch and they are also identified with an asterisk in the output.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INTERFACE-ID&gt;</code></td>
<td>Specifies the name or range of an interface on the switch. Use the format <code>member/slot/port</code> (for example, 1/3/1).</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed information for the interfaces.</td>
</tr>
<tr>
<td>threshold-violations</td>
<td>Show threshold violations for transceivers.</td>
</tr>
</tbody>
</table>

**Example**

Showing summary transceiver information with identification of unsupported transceivers:

```
switch(config)# show interface transceiver
```

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Product Number</th>
<th>Serial Number</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/15</td>
<td>SFP+SR</td>
<td>J9150D</td>
<td>xxxxxxxxxxxx</td>
<td>1990-4634</td>
</tr>
<tr>
<td>1/1/16</td>
<td>SFP+SR</td>
<td>J9150D</td>
<td>xxxxxxxxxxxx</td>
<td>1990-4634</td>
</tr>
</tbody>
</table>
```

Showing detailed transceiver information:

```
switch(config)# show interface transceiver detail
Transceiver in 1/1/15
   Interface Name : 1/1/15
   Type : SFP+SR
   Connector Type : LC
   Wavelength : 850nm
   Transfer Distance : 0.00km (SMF), 20m (OM1), 80m (OM2), 300m (OM3)
   Diagnostic Support : DOM
   Product Number : J9150D
   Serial Number : xxxxxxxxxxx
```
Part Number : 1990-4634

Status
Temperature : 30.38C
Voltage : 3.26V
Tx Bias : 5.54mA
Rx Power : 0.56mW, -2.52dBm
Tx Power : 0.62mW, -2.08dBm

Recent Alarms:
Recent Errors:

Transceiver in 1/1/16
Interface Name : 1/1/16
Type : SFP+SR
Connector Type : LC
Wavelength : 850nm
Transfer Distance : 0.00km (SMF), 20m (OM1), 80m (OM2), 300m (OM3)
Diagnostic Support : DOM
Product Number : J9150D
Serial Number : xxxxxxxxxxx
Part Number : 1990-4634

Status
Temperature : 30.62C
Voltage : 3.28V
Tx Bias : 5.64mA
Rx Power : 0.61mW, -2.15dBm
Tx Power : 0.59mW, -2.29dBm

Recent Alarms:
Recent Errors:

Showing detailed transceiver information with identification of unsupported transceivers:

```
switch# show interface transceiver detail
Transceiver in 1/1/2
Interface Name : 1/1/2
Type : SFP+ER (unsupported)
Connector Type : LC
Wavelength : 3590nm
Transfer Distance : 80m (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
Diagnostic Support : DOM
Vendor Name : INNOLIGHT
Vendor Part Number : TR-PX15Z-NHP
Vendor Part Revision : 1A
Vendor Serial number : MYxxxxxxxx

Status
Temperature : 28.88C
Voltage : 3.30V
Tx Bias : 65.53mA
Rx Power : 0.00mW, -inf
Tx Power : 1.47mW, 1.67dBm

Recent Alarms:
Rx Power low alarm
Rx Power low warning
```
Recent Errors:
Rx loss of signal

Showing transceiver threshold-violations:

```
switch(config)# show interface transceiver threshold-violations
```  

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Channel#</th>
<th>Recent Threshold Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/15</td>
<td>SFP+SR</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>1/1/16</td>
<td>SFP+SR</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ip interface**

```
show ip interface <INTERFACE-ID>
```

Description

Shows status and configuration information for an IPv4 interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INTERFACE-ID&gt;</code></td>
<td>Specifies the name of an interface. Format: member/slot/port.</td>
</tr>
</tbody>
</table>

Example

```
switch# show ip interface vlan1
```

Interface vlan1 is up
Admin state is up
Hardware: Ethernet, MAC Address: f8:60:f0:c9:11:60
IP MTU 1500
IPv4 address 10.120.3.8/26

Command History
## Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

### show ip source-interface

```
show ip source-interface {sflow | tftp | radius | tacacs | all} [vrf <VRF-NAME>]
```

### Description

Shows single source IP address configuration settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>tftp</td>
</tr>
</tbody>
</table>

### Examples

Showing single source IP address configuration settings for sFlow:

```
switch# show ip source-interface sflow
Source-interface Configuration Information
-------------------------------
Protocol     Source Interface
-------------- ----------
sflow         10.10.10.1
```

Showing single source IP address configuration settings for all protocols:

```
switch# show ip source-interface all
Source-interface Configuration Information
------------------------------------------
Protocol     Src-Interface     Src-IP     VRF
------------------ ------------- ----------
all             vlan2          2.2.2.2    default
```

### Command History
### Command Information

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

### show ipv6 interface

**show ipv6 interface <INTERFACE-ID>**

**Description**

Shows status and configuration information for an IPv6 interface.

**Parameter** | **Description**
--- | ---
<INTERFACE-ID> | Specifies an interface ID. Format: member/slot/port.

**Examples**

```
switch# show ipv6 interface vlan2

Interface vlan2 is up
 Admin state is up
 IPv6 address: 2001::1/64 [VALID]
 IPv6 link-local address: fe80::883a:3080:247:c1c0/64 [VALID]
 IPv6 Forwarding feature: enabled
 IPv6 multicast groups locally joined:
   ff02::1  ff02::1:ff00:1  ff02::1:ff47:c1c0  ff02::1:ff00:0
   ff02::2
 IPv6 MTU 1500
 IPv6 unicast reverse path forwarding: none
 IPv6 load sharing: none
switch#
```

### Command History

**Release** | **Modification**
--- | ---
10.07 or earlier | --

**Command Information**

**Platforms** | **Command context** | **Authority**
--- | --- | ---
All platforms | 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 ipv6 source-interface
show ipv6 source-interface {sflow | tftp | radius | tacacs | all} [vrf <VRF-NAME>]

Description
Shows single source IP address configuration settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>tftp</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF.</td>
</tr>
</tbody>
</table>

Examples
Showing single source IP address configuration settings for sFlow:

```
switch# show ipv6 source-interface sflow
Source-interface Configuration Information
-----------------------------
Protocol Source Interface
-------- -----------
sflow 2001:DB8::1
```

Showing single source IP address configuration settings for all protocols:

```
switch# show ipv6 source-interface all
Source-interface Configuration Information
----------------------------------------------
Protocol Src-Interface Src-IP VRF
----------------------------- --------------
all vlan2 2001::1 default
switch#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

shutdown
shutdown
no shutdown

Description
Disables an interface. Interfaces are disabled by default when created. The no form of this command enables an interface.

Examples
Disabling an interface:

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

Enabling an interface:

```
switch(config-if)# no shutdown
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Source interface selection commands

**ip source-interface (protocol <ip-addr>)**

```
ip source-interface <PROTOCOL> <IP-ADDR> [vrf <VRF-NAME>]
no ip source-interface <PROTOCOL> <IP-ADDR> [vrf <VRF-NAME>]
```

**Description**

Configures the source-interface IPv4 address to use for the specified protocol. If a VRF is not given, the default VRF applies. If no interface option is given, the device floods through interfaces and VRFs to reach Aruba Central. Whichever reaches Aruba Central will be picked automatically. The no form of this command removes all configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;PROTOCOL&gt;</code></td>
<td>Specifies the protocol to configure.</td>
</tr>
<tr>
<td>all</td>
<td>Selects all protocols that can be configured by this command.</td>
</tr>
<tr>
<td>central</td>
<td>Selects Aruba Central.</td>
</tr>
<tr>
<td>dns</td>
<td>Selects DNS.</td>
</tr>
<tr>
<td>ntp</td>
<td>Selects NTP.</td>
</tr>
<tr>
<td>radius</td>
<td>Selects radius.</td>
</tr>
<tr>
<td>sflow</td>
<td>Selects sFlow.</td>
</tr>
<tr>
<td>simplivity</td>
<td>Selects simplivity.</td>
</tr>
</tbody>
</table>

If the source interface and source IP are configured, Source IP will have priority.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>Selects syslog.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Selects TACACS.</td>
</tr>
<tr>
<td>tftp</td>
<td>Selects TFTP.</td>
</tr>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies the IPv4 address.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring source-interface IPv4 10.1.1.1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the TFTP protocol on VRF green:

```
switch(config)# ip source-interface tftp 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for TFTP protocol on VRF green:

```
switch(config)# no ip source-interface tftp 10.1.1.2 vrf green
```

Configuring source-interface IPv4 10.1.1.1 to use for the DNS protocol:

```
switch(config)# ip source-interface dns 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the DNS protocol on VRF green:

```
switch(config)# ip source-interface dns 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the DNS protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for the DNS protocol on VRF green:

```
switch(config)# no ip source-interface dns 10.1.1.2 vrf green
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip source-interface (<protocol> interface)**

`ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]`

`no ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]`

**Description**

Configures the IPv4 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The `no` form of this command removes the specified configuration.

**Parameter | Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;PROTOCOL&gt;</code></td>
<td>Specifies the protocol to configure.</td>
</tr>
<tr>
<td>all</td>
<td>Selects all protocols that can be configured by this command.</td>
</tr>
<tr>
<td>central</td>
<td>Selects Aruba Central.</td>
</tr>
<tr>
<td>dns</td>
<td>Selects DNS.</td>
</tr>
<tr>
<td>ntp</td>
<td>Selects NTP.</td>
</tr>
<tr>
<td>radius</td>
<td>Selects radius.</td>
</tr>
<tr>
<td>sflow</td>
<td>Selects sFlow.</td>
</tr>
<tr>
<td>syslog</td>
<td>Selects syslog.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Selects TACACS.</td>
</tr>
<tr>
<td>tftp</td>
<td>Selects TFTP.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td><code>&lt;IFNAME&gt;</code></td>
<td>Specifies the interface name.</td>
</tr>
</tbody>
</table>

**Examples**
Configuring IPv4 source-interface interface 1/1/1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp interface 1/1/1
```

Configuring IPv4 source-interface interface 1/1/2 to use for the TFTP protocol on VRF green:

```
switch(config)# ip source-interface tftp interface 1/1/2 vrf green
```

Removing IPv4 source-interface 1/1/1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp interface 1/1/1
```

Removing source-interface interface 1/1/2 configuration for TFTP protocol on VRF green:

```
switch(config)# no ip source-interface tftp interface 1/1/2 vrf green
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 source-interface (<protocol> <ip-addr>)**

```
ipv6 source-interface <PROTOCOL> <IPV6-ADDR> [vrf <VRF-NAME>]
no source-interface <PROTOCOL> <IPV6-ADDR> [vrf <VRF-NAME>]
```

**Description**

Configures the source-interface IPv6 address to use for the specified protocol. If a VRF is not given, the default VRF applies.

The no form of this command removes the specified protocol configuration.

**Parameter** | **Description**
---|---
<PROTOCOL> | Specifies the protocol to configure.
  - all: Selects all protocols supported by this command.
  - central: Selects Aruba Central.
  - ntp: Selects NTP.
  - radius: Selects radius.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sflow</td>
<td>Selects sFlow.</td>
</tr>
<tr>
<td>syslog</td>
<td>Selects syslog.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Selects TACACS.</td>
</tr>
<tr>
<td>tftp</td>
<td>Selects TFTP.</td>
</tr>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the IPv6 address.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring source-interface IPv6 1111:2222 to use for the TFTP protocol:

```
switch(config)# ipv6 source-interface tftp 1111:2222
```

Configuring source-interface IPv6 1111:3333 to use for TFTP protocol on VRF green:

```
switch(config)# ipv6 source-interface tftp 1111:3333 vrf green
```

Removing source-interface IPv6 1111:2222 configuration for TFTP protocol:

```
switch(config)# no ipv6 source-interface tftp 1111:2222
```

Removing source-interface IPv6 1111:3333 configuration for TFTP protocol on VRF green:

```
switch(config)# no ipv6 source-interface tftp 1111:3333 vrf green
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 source-interface (<protocol> interface)**

ipv6 source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]

no ipv6 source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]

**Description**
Configures the IPv6 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The no form of this command removes all configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <PROTOCOL> | Specifies the protocol to configure.  
  all  
  ntp  
  radio  
  sflow  
  syslog  
  tacacs  
  tftp  
  Selects all protocols supported by this command.  
  Selects NTP.  
  Selects radius.  
  Selects sFlow.  
  Selects syslog.  
  Selects TACACS.  
  SelectsTFTP.  |
| <IFNAME>  | Specifies the interface name.  |
| vrf <VRF-NAME> | Specifies the VRF name.  |

<IFNAME>  
Specifies the interface name.  

vrf <VRF-NAME>  
Specifies the VRF name.

**Examples**

**Configuring IPv6 source-interface interface 1/1/1 to use for the TFTP protocol:**

```
switch(config)# ipv6 source-interface tftp interface 1/1/1
```

**Configuring IPv6 source-interface interface 1/1/2 to use for the TFTP protocol on VRF green:**

```
switch(config)# ipv6 source-interface tftp interface 1/1/2 vrf green
```

**Removing IPv6 source-interface interface 1/1/1 configuration for the TFTP protocol:**

```
switch(config)# no ipv6 source-interface tftp interface 1/1/1
```

**Removing IPv6 source-interface interface 1/1/2 configuration for the TFTP protocol on VRF green:**

```
switch(config)# no ipv6 source-interface tftp interface 1/1/2 vrf green
```

**Command History**
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ip source-interface**

*show ip source-interface  <PROTOCOL>  [vrf  <VRF-NAME>  |  all-vrfs]*

**Description**

Displays the source interface information for all VRFs or a specific VRF. If a VRF is not specified, the default is displayed.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PROTOCOL&gt;</td>
<td>Specifies the protocol to show.</td>
</tr>
<tr>
<td>all</td>
<td>Shows the source interface configuration for all other protocols.</td>
</tr>
<tr>
<td>central</td>
<td>Shows the source interface configuration for Aruba Central.</td>
</tr>
<tr>
<td>dns</td>
<td>Shows the source interface configuration for DNS.</td>
</tr>
<tr>
<td>ntp</td>
<td>Shows the source interface configuration for NTP.</td>
</tr>
<tr>
<td>radius</td>
<td>Shows the source interface configuration for radius.</td>
</tr>
<tr>
<td>sflow</td>
<td>Shows the source interface configuration for sFlow.</td>
</tr>
<tr>
<td>syslog</td>
<td>Shows the source interface configuration for syslog.</td>
</tr>
<tr>
<td>tacacs</td>
<td>Shows the source interface configuration for TACACS.</td>
</tr>
<tr>
<td>tftp</td>
<td>Shows the source interface configuration for TFTP.</td>
</tr>
<tr>
<td>vrf  &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>all-vrfs</td>
<td>Shows the source interface configuration for all VRFs.</td>
</tr>
</tbody>
</table>

**Examples**

Displaying all source-interface protocol configurations for VRF red:
switch# show ip source-interface all vrf red
Source-interface Configuration Information
-----------------------------------------
Protocol  Src-Interface  Src-IP  VRF
-----------------------------------------
all       1/1/1          red
switch#

Displaying all source-interface protocol configurations for default VRF:

switch# show ip source-interface all
Source-interface Configuration Information
-----------------------------------------
Protocol  Src-Interface  Src-IP  VRF
-----------------------------------------
all       1.1.1.1         default
switch#

Displaying all source-interface protocol configurations for all VRFs:

switch# show ip source-interface all all-vrfs
Source-interface Configuration Information
-----------------------------------------
Protocol  Src-Interface  Src-IP  VRF
-----------------------------------------
all       2.2.2.2         all-vrfs
all       1.1.1.1         default
all       1/1/1/1         red
switch#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ipv6 source-interface**

*show ipv6 source-interface <PROTOCOL> [detail] [vrf <VRF-NAME> | all-vrfs]*

**Description**

Displays the IPV6 source interface information configured in the router for all VRFs or a specific VRF. If a VRF is not specified, the default is displayed.
<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;PROTOCOL&gt;</code></td>
<td>Specifies the protocol to show.</td>
</tr>
<tr>
<td></td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for all other protocols.</td>
</tr>
<tr>
<td></td>
<td>central</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for Aruba Central.</td>
</tr>
<tr>
<td></td>
<td>ntp</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for NTP.</td>
</tr>
<tr>
<td></td>
<td>radius</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for radius.</td>
</tr>
<tr>
<td></td>
<td>sflow</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for sFlow.</td>
</tr>
<tr>
<td></td>
<td>syslog</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for syslog.</td>
</tr>
<tr>
<td></td>
<td>tacacs</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for TACACS.</td>
</tr>
<tr>
<td></td>
<td>tftp</td>
</tr>
<tr>
<td></td>
<td>Shows the source interface configuration for TFTP.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies the VRF name.</td>
</tr>
<tr>
<td>all-vrfs</td>
<td>Shows the source interface configuration for all VRF.</td>
</tr>
</tbody>
</table>

**Examples**

Displaying all IPv6 source-interface protocol configurations for default VRF:

```
switch# show ipv6 source-interface all
Source-interface Configuration Information
----------------------------------------------
Protocol          Src-Interface      Src-IP     VRF  
----------------------------------------------
all                1111:2222          default
switch#
```

Displaying all IPv6 source-interface protocol configuration for VRF red:

```
switch# show ipv6 source-interface all vrf red
Source-interface Configuration Information
----------------------------------------------
Protocol          Src-Interface      Src-IP     VRF  
----------------------------------------------
all                1/1/1                 red
switch#
```

Displaying all IPv6 source-interface protocol configurations for all VRFs:

```
switch# show ipv6 source-interface all all-vrfs
Source-interface Configuration Information
----------------------------------------------
```
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Src-Interface</th>
<th>Src-IP</th>
<th>VRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td></td>
<td>2.2.2.3:3.3.3.3</td>
<td>all-vrf</td>
</tr>
<tr>
<td>all</td>
<td></td>
<td>1.1.1.2:2.2.2.2</td>
<td>default</td>
</tr>
<tr>
<td>all</td>
<td>1/1/1</td>
<td>2::2</td>
<td>red</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show running-config**

**Description**

Displays the current running configuration.

**Examples**

Displaying the running configuration (only items of interest to source interface selection are shown in this example output command):

```
switch# show running-config
vrf green
  ip source-interface tftp interface 1/1/2 vrf green
  ip source-interface radius interface 1/1/2 vrf green
  ip source-interface ntp interface 1/1/2 vrf green
  ip source-interface tacacs interface 1/1/2 vrf green
  ip source-interface dns interface 1/1/2 vrf green
  ip source-interface central interface 1/1/2 vrf green
  ipv6 source-interface tftp 2222::3333 vrf green
  ipv6 source-interface radius 2222::3333 vrf green
  ipv6 source-interface ntp 2222::3333 vrf green
  ipv6 source-interface tacacs 2222::3333 vrf green
  ipv6 source-interface central 2222::3333 vrf green
  ipv6 source-interface all 2222::3333 vrf green
  ip source-interface tftp 10.20.3.1
  ip source-interface radius 10.20.3.1
  ip source-interface ntp 10.20.3.1
  ip source-interface tacacs 10.20.3.1
```

Aruba Central is the priority agent. If no command is specified for ip source-interface, Central will choose the command automatically if it is reachable on any of the known ports.
ip source-interface dns 10.20.3.1
ip source-interface central 10.20.3.1
ip source-interface all 10.20.3.1
interface 1/1/1
  no shutdown
  ip address 10.20.3.1/24
interface 1/1/2
  vrf attach green
  ip address 20.1.1.1/24
  ipv6 address 2222::3333/64
interface 1/1/45
  no shutdown
  ip address 100.1.0.1/24
  ipv6 address 1111::2222/64
ip route 100.2.0.0/24 10.20.3.2
switch#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; ) only.</td>
</tr>
</tbody>
</table>
VLANs are primarily used to provide network segmentation at layer 2. VLANs enable the grouping of users by logical function instead of physical location. They make managing bandwidth usage within networks possible by:

- Allowing grouping of high-bandwidth users on low-traffic segments
- Organizing users from different LAN segments according to their need for common resources and individual protocols
- Improving traffic control at the edge of networks by separating traffic of different protocol types.
- Enhancing network security by creating subnets to control in-band access to specific network resources.

VLANs are generally assigned on an organizational basis rather than on a physical basis. For example, a network administrator could assign all workstations and servers used by a particular workgroup to the same VLAN, regardless of their physical locations.

Hosts in the same VLAN can directly communicate with one another. A router or a Layer 3 switch is required for hosts in different VLANs to communicate with one another.

VLANs help reduce bandwidth waste, improve LAN security, and enable network administrators to address issues such as scalability and network management.

Refer to the Layer 2 Bridging Guide for VLAN configuration and commands.
Chapter 7
Configuration and firmware management

Checkpoints

A checkpoint is a snapshot of the running configuration of a switch and its relevant metadata during the time of creation. Checkpoints can be used to apply the switch configuration stored within a checkpoint whenever needed, such as to revert to a previous, clean configuration. Checkpoints can be applied to other switches of the same platform. A switch is able to store multiple checkpoints.

Checkpoint types

The switch supports two types of checkpoints:

- **System generated checkpoints**: The switch automatically generates a system checkpoint whenever a configuration change occurs.
- **User generated checkpoints**: The administrator can manually generate a checkpoint whenever required.

Maximum number of checkpoints

- Maximum checkpoints: 64 (including the startup configuration)
- Maximum user checkpoints: 32
- Maximum system checkpoints: 32

User generated checkpoints

User checkpoints can be created at any time, as long as one configuration difference exists since the last checkpoint was created. Checkpoints can be applied to either the running or startup configurations on the switch.

All user generated checkpoints include a time stamp to identify when a checkpoint was created.

A maximum of 32 user generated checkpoints can be created.

System generated checkpoints

System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.

System generated checkpoints are named with the prefix CPC followed by a time stamp in the format <YYYYMMDHHMMSS>. For example: CPC20170630073127.

System checkpoints can be applied using the checkpoint rollback feature or copy command.

A maximum of 32 system checkpoints can be created. Beyond this limit, the newest system checkpoint replaces the oldest system checkpoint.

Supported remote file formats
You can restore a switch configuration by copying a switch configuration stored on a USB drive or a remote network device through SFTP/TFTP. The remote file formats that the switch supports depends on where you plan to restore the checkpoint.

<table>
<thead>
<tr>
<th>Restoring a checkpoint to a...</th>
<th>File type supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running configuration</td>
<td>▪ CLI</td>
</tr>
<tr>
<td></td>
<td>▪ JSON</td>
</tr>
<tr>
<td></td>
<td>▪ Checkpoint</td>
</tr>
<tr>
<td>Startup configuration</td>
<td>▪ JSON</td>
</tr>
<tr>
<td></td>
<td>▪ Checkpoint</td>
</tr>
<tr>
<td>Specified checkpoint</td>
<td>Specified checkpoint</td>
</tr>
</tbody>
</table>

**Rollback**

The term rollback is used to refer to when a switch configuration is reverted to a pre-existing checkpoint.

For example, the following command applies the configuration from checkpoint `ckpt1`. All previous configurations are lost after the execution of this command: `checkpoint rollback ckpt1`  
You can also specify the rollback of the running configuration or of the startup configuration with a specified checkpoint, as shown with the following command: `copy checkpoint <checkpoint-name> {running-config | startup-config}`

**Checkpoint auto mode**

Checkpoint auto mode configures the switch with failover support, causing it to automatically revert to a previous configuration if it becomes inoperable or inaccessible due to configuration changes that are being made.

After entering checkpoint auto mode, you have a set amount of time to add, remove, or modify the existing switch configuration. To save your changes, you must execute the `checkpoint auto confirm` command before the auto mode timer expires. If you do not execute the `checkpoint auto confirm` command within the specified time, all configuration changes you made are discarded and the running configuration reverts to the state it was before entering checkpoint auto mode.

**Testing a switch configuration in checkpoint auto mode**

Process overview:

1. Enable the checkpoint auto mode.
2. To save the configuration, enter the `checkpoint auto confirm` command before the specified time set in step 1.

**Checkpoint commands**

**checkpoint auto**

checkpoint auto <TIME-LAPSE-INTERVAL>

**Description**

Starts auto checkpoint mode. In auto checkpoint mode, the switch temporarily saves the runtime configuration as a checkpoint only for the specified time lapse interval. Configuration changes must be
saved before the interval expires, otherwise the runtime configuration is restored from the temporary checkpoint.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME-LAPSE-INTERVAL&gt;</td>
<td>Specifies the time lapse interval in minutes. Range: 1 to 60.</td>
</tr>
</tbody>
</table>

**Usage**

To save the runtime checkpoint permanently, run the `checkpoint auto confirm` command during the time lapse interval. The filename for the saved checkpoint is named `AUTO<YYYYMMDDHHMMSS>`. If the `checkpoint auto confirm` command is not entered during the specified time lapse interval, the previous runtime configuration is restored.

**Examples**

Confirming the auto checkpoint:

```
switch# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
switch# WARNING Please "checkpoint auto confirm" within 2 minutes
switch# checkpoint auto confirm
checkpoint AUTO20170801011154 created
```

In this example, the runtime checkpoint was saved because the `checkpoint auto confirm` command was entered within the value set by the `time-lapse-interval` parameter, which was 20 minutes.

Not confirming the auto checkpoint:

```
switch# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
switch# WARNING Please "checkpoint auto confirm" within 2 minutes
WARNING: Restoring configuration. Do NOT add any new configuration.
Restoration successful
```

In this example, the runtime checkpoint was reverted because the `checkpoint auto confirm` command was not entered within the value set by the `time-lapse-interval` parameter, which was 20 minutes.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`checkpoint auto confirm`

`checkpoint auto confirm`
**Description**
Signals to the switch to save the running configuration used during the auto checkpoint mode. This command also ends the auto checkpoint mode.

**Usage**
To save the runtime checkpoint permanently, run the `checkpoint auto confirm` command during the time lapse value set by the `checkpoint auto <TIME-LAPSE-INTERVAL>` command. The generated checkpoint name will be in the format `AUTO<YYYYMMDDHHMMSS>`. If the `checkpoint auto confirm` command is not entered during the specified time lapse interval, the previous runtime configuration is restored.

**Examples**
Confirming the auto checkpoint:

```bash
switch# checkpoint auto confirm
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**checkpoint diff**

`checkpoint diff {<CHECKPOINT-NAME1> | running-config | startup-config} {<CHECKPOINT-NAME2> | running-config | startup-config}

**Description**
Shows the difference in configuration between two configurations. Compare checkpoints, the running configuration, or the startup configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{&lt;CHECKPOINT-NAME1&gt;</td>
<td>running-config</td>
</tr>
<tr>
<td>`{&lt;CHECKPOINT-NAME2&gt;</td>
<td>running-config</td>
</tr>
</tbody>
</table>

**Usability**
The output of the `checkpoint diff` command has several symbols:
The plus sign (+) at the beginning of a line indicates that the line exists in the comparison but not in the baseline.

The minus sign (-) at the beginning of a line indicates that the line exists in the baseline but not in the comparison.

Examples

In the following example, the configurations of checkpoints cp1 and cp2 are displayed before the checkpoint diff command, so that you can see the context of the checkpoint diff command.

```
switch# checkpoint diff chkpt01 chkpt02
--- /tmp/chkpt011607564301327
+++ /tmp/chkpt021607564301353
@@ -1,7 +1,7 @@
!Version AOS-CX PL.10.06.0100V
!export-password: default
-hostname Switch
+hostname Switch1
 user admin group administrators password ciphertext
AQBapTyg9tpaiAaTfSVV5eNdFz0ORRv26CMpq1h1P+LQUHQLYgAAAGAhmRqFbkNvrgy2SBVkJH8CShvg/I1b
 8rWYFZL2EA5crobNP9EwM+u+hLMN0xmsh45yG8dncP7WkxjwrW4p4Qra6dYF0r0E88xh/lpQf8F/2Wk12OLc9JL
  X1Yge7ti0H6cVn+G
 radius-server tracking interval 60
 no usb
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**checkpoint post-configuration**

callpoint post-configuration

no checkpoint post-configuration

**Description**

Enables creation of system generated checkpoints when configuration changes occur. This feature is enabled by default.

The **no** form of this command disables system generated checkpoints.

**Usage**

System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration
change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.

System generated checkpoints are named with the prefix **CPC** followed by a time stamp in the format `<YYYYMMDDHHMMSS>`. **For example:** CPC20170630073127.

System checkpoints can be applied using the checkpoint rollback feature or copy command.

A maximum of 32 system checkpoints can be created. Beyond this limit, the newest system checkpoint replaces the oldest system checkpoint.

**Examples**

Enabling system checkpoints:

```
switch(config)# checkpoint post-configuration
```

Disabling system checkpoints:

```
switch(config)# no checkpoint post-configuration
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`checkpoint post-configuration timeout`

`checkpoint post-configuration timeout <TIMEOUT>`

`no checkpoint post-configuration timeout <TIMEOUT>`

**Description**

Sets the timeout for the creation of system checkpoints. The timeout specifies the amount of time since the latest configuration for the switch to create a system checkpoint.

The `no` form of this command resets the timeout to 300 seconds, regardless of the value of the `<TIMEOUT>` parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Specifies the timeout in seconds. Range: 5 to 600. Default: 300.</td>
</tr>
</tbody>
</table>

**Examples**

Setting the timeout for system checkpoints to 60 seconds:
switch(config)# checkpoint post-configuration timeout 60

Resetting the timeout for system checkpoints to 300 seconds:

switch(config)# no checkpoint post-configuration timeout 1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

checkpoint rename

checkpoint rename <OLD-CHECKPOINT-NAME> <NEW-CHECKPOINT-NAME>

Description

Renames an existing checkpoint.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;OLD-CHECKPOINT-NAME&gt;</td>
<td>Specifies the name of an existing checkpoint to be renamed.</td>
</tr>
<tr>
<td>&lt;NEW-CHECKPOINT-NAME&gt;</td>
<td>Specifies the new name for the checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Do not start the checkpoint name with CPC because it is used for system-generated checkpoints.</td>
</tr>
</tbody>
</table>

Examples

Renaming checkpoint ckpt1 to cfg001:

switch# checkpoint rename ckpt1 cfg001

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**checkpoint rollback**

cHECKPOINT-NAME> | startup-config

**Description**

Applies the configuration from a pre-existing checkpoint or the startup configuration to the running configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CHECKPOINT-NAME&gt;</td>
<td>Specifies a checkpoint name.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Specifies the startup configuration.</td>
</tr>
</tbody>
</table>

**Examples**

Applying a checkpoint named ckpt1 to the running configuration:

```
switch# checkpoint rollback ckpt1
Success
```

Applying a startup checkpoint to the running configuration:

```
switch# checkpoint rollback startup-config
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Copies a checkpoint configuration to a remote location as a file. The configuration is exported in checkpoint format, which includes switch configuration and relevant metadata.

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CHECKPOINT-NAME&gt;</code></td>
<td>Specifies the name of a checkpoint.</td>
</tr>
<tr>
<td><code>&lt;REMOTE-URL&gt;</code></td>
<td>Specifies the remote destination and filename using the syntax: [tftp</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies a VRF name.</td>
</tr>
</tbody>
</table>

### Examples

**Copying checkpoint configuration to remote file through TFTP:**

```bash
switch# copy checkpoint ckpt1 tftp://192.168.1.10/ckptmeta vrf default
#########################################################################
100.0% Success
```

**Copying checkpoint configuration to remote file through SFTP:**

```bash
switch# copy checkpoint ckpt1 sftp://root@192.168.1.10/ckptmeta vrf default
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is SHA256:FtOm6Uxuxumil7VCwLnhz92H9LkjY+eURbddOEy50.
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.1.10's password:
sftp> put /tmp/ckptmeta ckptmeta
Warning: Permanently added '192.168.1.10' (ECDSA) to the list of known hosts.
Connected to 192.168.1.10.
Success
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy checkpoint `<CHECKPOINT-NAME>` {running-config | startup-config}**

**Description**

Copies an existing checkpoint configuration to the running configuration or to the startup configuration.
Parameter | Description
---|---
<CHECKPOINT-NAME> | Specifies the name of an existing checkpoint.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| {running-config | startup-config} | Selects whether the running configuration or the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.

**Examples**

Copying ckpt1 checkpoint to the running configuration:

```
switch# copy checkpoint ckpt1 running-config
Success
```

Copying ckpt1 checkpoint to the startup configuration:

```
switch# copy checkpoint ckpt1 startup-config
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

```
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>
```

**Description**

Copies an existing checkpoint configuration to a USB drive. The file format is defined when the checkpoint was created.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CHECKPOINT-NAME&gt;</td>
<td>Specifies the name of the checkpoint to copy. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).</td>
</tr>
<tr>
<td>&lt;STORAGE-URL&gt;</td>
<td>Specifies the name of the target file on the USB drive using the following syntax: <code>usb:/&lt;FILE&gt;</code> The USB drive must be formatted with the FAT file system.</td>
</tr>
</tbody>
</table>

**Examples**
Copying the test checkpoint to the testCheck file on the USB drive:

```
switch# copy checkpoint test usb:/testCheck
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

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

**copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME>**

copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> [vrf <VRF-NAME>]

**Description**

Copies a remote configuration file to a checkpoint. The remote configuration file must be in checkpoint format.

**Parameter** | **Description**
---|---
<REMOTE-URL> | Specifies a remote file using the following syntax: {tftp | sftp}://<IP-ADDRESS>[:<PORT-NUMBER>] [:blocksize=<BLOCKSIZE-VALUE>]/<FILE-NAME>

<CHECKPOINT-NAME> | Specifies the name of the target checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). Required.

**NOTE:**
Do not start the checkpoint name with CPC because it is used for system-generated checkpoints.

vrf <VRF-NAME> | Specifies a VRF name. Default: default.

**Examples**

Copying a checkpoint format file to checkpoint ckpt5 on the default VRF:

```
switch# copy tftp://192.168.1.10/ckptmeta checkpoint ckpt5
#----------------------------------------# 100.0%
100.0%
Success
```

**Command History**
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy <REMOTE-URL> {running-config | startup-config}**

*copy <REMOTE-URL> {running-config | startup-config} [vrf <VRF-NAME>]*

**Description**

Copies a remote file containing a switch configuration to the running configuration or to the startup configuration.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;REMOTE-URL&gt;</td>
<td>Specifies a remote file with the following syntax: {tftp</td>
</tr>
<tr>
<td>{running-config</td>
<td>startup-config}</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Default: default.</td>
</tr>
</tbody>
</table>

**Usage**

The switch copies only certain file types. The format of the file is automatically detected from contents of the file. The `startup-config` option only supports the JSON file format and checkpoints, but the `running-config` option supports the JSON and CLI file formats and checkpoints.

When a file of the CLI format is copied, it overwrites the running configuration. The CLI command does not clear the running configuration before applying the CLI commands. All of the CLI commands in the file are applied line-by-line. If a particular CLI command fails, the switch logs the failure and it continues to the next line in the CLI configuration. The event log (`show events -d hpe-config`) provides information as to which command failed.

**Examples**

Copying a JSON format file to the running configuration:

```
switch# copy tftp://192.168.1.10/runjson running-config
#------------------------------------------------------------------------------------- 100.0%
Configuration may take several minutes to complete according to configuration file size
--0%---10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Success
```
Copying a CLI format file to the running configuration with an error in the file:

```
switch# copy tftp://192.168.1.10/runcli running-config
#########################################################################
Configuration may take several minutes to complete according to configuration file size
--0%----10%-----20%----30%----40%-----50%-----60%----70%----80%----90%----100%--
Some of the configuration lines from the file were NOT applied. Use 'show events -d hpe-config' for more info.
```

Copying a CLI format file to the startup configuration:

```
switch# copy tftp://192.168.1.10/startjson startup-config
#########################################################################
100.0%
Success
```

Copying an unsupported file format to the startup configuration:

```
switch# copy tftp://192.168.1.10/startfile startup-config
#########################################################################
100.0%
unsupported file format
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>}

**Description**

Copies the running configuration to the startup configuration or to a new checkpoint. If the startup configuration is already present, the command overwrites the existing startup configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup-config</td>
<td>Specifies that the startup configuration receives a copy of the running configuration.</td>
</tr>
</tbody>
</table>
### Parameter: `checkpoint <CHECKPOINT-NAME>`

Specifies the name of a new checkpoint to receive a copy of the running configuration. The checkpoint name can be alphanumeric. It can also contain underscores `_` and dashes `-`.

**NOTE:**
Do not start the checkpoint name with `CPC` because it is used for system-generated checkpoints.

### Examples

**Copying the running configuration to the startup configuration:**

```
switch# copy running-config startup-config
Success
```

**Copying the running configuration to a new checkpoint named `ckpt1`:**

```
switch# copy running-config checkpoint ckpt1
Success
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy {running-config | startup-config} <REMOTE-URL>**

**copy {running-config | startup-config} <REMOTE-URL> {cli | json} [vrf <VRF-NAME>]**

### Description

Copies the running configuration or the startup configuration to a remote file in either CLI or JSON format.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{running-config</td>
<td>startup-config}</td>
</tr>
<tr>
<td>&lt;REMOTE-URL&gt;</td>
<td>Specifies the remote file using the syntax: `{tftp</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>{cli</td>
<td>json}</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Default: default.</td>
</tr>
</tbody>
</table>

**Examples**

Copying a running configuration to a remote file in CLI format:

```
switch# copy running-config tftp://192.168.1.10/runcli cli
#########################################################################
100.0% Success
```

Copying a running configuration to a remote file in JSON format:

```
switch# copy running-config tftp://192.168.1.10/runjson json
#########################################################################
100.0% Success
```

Copying a startup configuration to a remote file in CLI format:

```
switch# copy startup-config sftp://root@192.168.1.10/startcli cli
root@192.168.1.10's password:
sftp> put /tmp/startcli startcli
Uploading /tmp/startcli to /root/startcli
Connected to 192.168.1.10.
Success
```

Copying a startup configuration to a remote file in JSON format:

```
switch# copy startup-config sftp://root@192.168.1.10/startjson json
root@192.168.1.10's password:
sftp> put /tmp/startjson startjson
Uploading /tmp/startjson to /root/startjson
Connected to 192.168.1.10.
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`copy {running-config | startup-config} <STORAGE-URL>`
copy {running-config | startup-config} <STORAGE-URL> {cli | json}

**Description**
Copies the running configuration or a startup configuration to a USB drive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{running-config</td>
<td>startup-config}</td>
</tr>
<tr>
<td>&lt;STORAGE-URL&gt;</td>
<td>Specifies a remote file with the following syntax: usb:/&lt;file&gt;</td>
</tr>
<tr>
<td>{cli</td>
<td>json}</td>
</tr>
</tbody>
</table>

**Usage**
The switch supports JSON and CLI file formats when copying the running or starting configuration to the USB drive. The USB drive must be formatted with the FAT file system.
The USB drive must be enabled and mounted with the following commands:

```bash
switch(config)# usb
switch(config)# end
switch# usb mount
```

**Examples**
Copying a running configuration to a file named runCLI on the USB drive:

```bash
switch# copy running-config usb:/runCLI cli
Success
```

Copying a startup configuration to a file named startCLI on the USB drive:

```bash
switch# copy startup-config usb:/startCLI cli
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
<td></td>
</tr>
</tbody>
</table>
Description
Copies the startup configuration to the running configuration.

Examples

```markdown
switch# copy startup-config running-config
Success
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`copy <STORAGE-URL> running-config`

`copy <STORAGE-URL> {running-config | startup-config | checkpoint <CHECKPOINT-NAME>}`

Description
This command copies a specified configuration from the USB drive to the running configuration, to a startup configuration, or to a checkpoint.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;STORAGE-URL&gt;</code></td>
<td>Specifies the name of a configuration file on the USB drive with the syntax: <code>usb:&lt;FILE&gt;</code></td>
</tr>
<tr>
<td>running-config</td>
<td>Specifies that the configuration file is copied to the running configuration. The file must be in CLI, JSON, or checkpoint format or the copy will fail. The copy will not work.</td>
</tr>
<tr>
<td>startup-config</td>
<td>Specifies that the configuration file is copied to the startup configuration. The switch stores this configuration between reboots. The startup configuration is used as the operating configuration following a reboot of the switch. The file must be in JSON or checkpoint format or the copy will fail.</td>
</tr>
</tbody>
</table>
| checkpoint `<CHECKPOINT-NAME>` | Specifies the name of a new checkpoint file to receive a copy of the configuration. The configuration file on the USB drive must be in checkpoint format.  
**NOTE:**  
Do not start the checkpoint name with CPC because it is used for system-generated checkpoints. |

Usage
This command requires that the USB drive is formatted with the FAT file system and that the file be in the appropriate format as follows:

- **running-config**: This option requires the file on the USB drive be in CLI, JSON, or checkpoint format.
- **startup-config**: This option requires the file on the USB drive be in JSON or checkpoint format.
- **checkpoint <checkpoint-name>**: This option requires the file on the USB drive be in checkpoint format.

**Examples**

Copying the file runCli from the USB drive to the running configuration:

```
switch# copy usb:/runCli running-config
Configuration may take several minutes to complete according to configuration file size
--0%--10%--20%--30%--40%--50%--60%--70%--80%--90%--100%--
Success
```

Copying the file startUp from the USB drive to the startup configuration:

```
switch# copy usb:/startUp startup-config
Success
```

Copying the file testCheck from the USB drive to the abc checkpoint:

```
switch# copy usb:/testCheck checkpoint abc
Success
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**erase {checkpoint <CHECKPOINT-NAME> | startup-config | all}**

erase {checkpoint <CHECKPOINT-NAME> | startup-config | all}

**Description**

Deletes an existing checkpoint, startup configuration, or all checkpoints.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkpoint &lt;CHECKPOINT-NAME&gt;</td>
<td>Specifies the name of a checkpoint.</td>
</tr>
</tbody>
</table>
### show checkpoint <CHECKPOINT-NAME>

**Description**

Shows the configuration of a checkpoint.

**Examples**

Showing the configuration of the `ckpt1` checkpoint in CLI format:

```
show checkpoint ckpt1
```

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CHECKPOINT-NAME&gt;</td>
<td>Specifies the name of a checkpoint.</td>
</tr>
<tr>
<td>[json]</td>
<td>Specifies that the output is displayed in JSON format.</td>
</tr>
</tbody>
</table>
switch# show checkpoint ckpt1
Checkpoint configuration:
! Version AOS-CX PL.10.07.0000K-75-g55e5193
! export-password: default
lacp system-priority 65535
user admin group administrators password ciphertext
AQBapOjiwpeh36io0jFfdm72ZrrHcknca11D+3n8XFTZKQdmYgAADEtYOeHMe93xzdD0uz6Vr9Kl+XBzB+
2GB0U8xSF7rvgN2x8KSgkqv71qXVQ0Tey6LkSMH4BdNaT3Bf25qyvoQgmr4YakO1V3rg8zAOADkJfktQD8j0TH
Xf1zwomoIzcmv/uX
cli-session
  timeout 0
  !
  !
  ! ssh server vrf default
vlan 1
spanning-tree
interface lag 1
  no shutdown
  vlan access 1
interface lag 128
  no shutdown
  vlan access 1
interface lag 129
  shutdown
  vlan access 1
lacp mode active
interface 1/1/1
  no shutdown
  lag 128
  lacp port-id 65535
interface 1/1/2
  no shutdown
  vlan access 1
interface 1/1/3
  no shutdown
  vlan access 1
interface 1/1/4
  no shutdown
  vlan access 1
interface 1/1/5
  no shutdown
  vlan access 1
interface 1/1/6
  no shutdown
  vlan access 1
interface 1/1/7
  no shutdown
  vlan access 1
interface 1/1/8
  no shutdown
  vlan access 1
interface 1/1/9
  no shutdown
  vlan access 1
interface 1/1/10
  no shutdown
  vlan access 1
interface 1/1/11
  no shutdown
vlan access 1
interface 1/1/12
  no shutdown
  vlan access 1
interface 1/1/13
  no shutdown
  vlan access 1
interface 1/1/14
  no shutdown
  vlan access 1
interface 1/1/15
  no shutdown
  vlan access 1
interface 1/1/16
  no shutdown
  vlan access 1
interface vlan 1
  ip dhcp
  snmp-server vrf default
!
!
!
!
!
https-server vrf default

Showing the configuration of the ckpt1 checkpoint in JSON format:

```
switch# show checkpoint ckpt1 json
Checkpoint configuration:
{
  "AAA_Server_Group": {
    "local": {
      "group_name": "local"
    },
    "none": {
      "group_name": "none"
    }
  }
}
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager ($)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show checkpoint <CHECKPOINT-NAME> hash
show checkpoint <CHECKPOINT-NAME> hash [cli | json]

**Description**

Shows a configuration checkpoint hash calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;CHECKPOINT-NAME&gt;</td>
<td>Specifies an existing checkpoint name.</td>
</tr>
<tr>
<td>[cli</td>
<td>json]</td>
</tr>
</tbody>
</table>

**Examples**

Showing a checkpoint SHA-256 hash in JSON format:

```
switch# show checkpoint ckpt1 hash json
Calculating the hash: [Success]

The SHA-256 hash of the checkpoint in JSON format, created in image XX.10.08.xxxx:
cc7a57a9bbb4e6600d3b4180296a35f6af9e797ce9c439955dfe5de58b06da9e

This hash is only valid for comparison to a baseline hash if the configuration has not been explicitly changed (such as with a CLI command, REST operation, etc.) or implicitly changed (such as by changing a hardware module, upgrading the SW version, etc.).
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show checkpoint post-configuration**

**Description**

Shows the configuration settings for creating system checkpoints.

**Examples**

```
switch# show checkpoint post-configuration
```
Checkpoint Post-Configuration feature
------------------------------------
Status : enabled
Timeout (sec) : 300

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show checkpoint
desc show checkpoint

Description
Shows a detailed list of all saved checkpoints.

Examples
Showing a detailed list of all saved checkpoints:

```
switch# show checkpoint
NAME     TYPE     WRITER DATE (YYYY/MM/DD) IMAGE VERSION
ckpt1    checkpoint User  2017-02-23T00:10:02Z XX.01.01.000X
ckpt2    checkpoint User  2017-03-08T18:10:01Z XX.01.01.000X
ckpt3    checkpoint User  2017-03-09T23:11:02Z XX.01.01.000X
ckpt4    checkpoint User  2017-03-11T00:00:03Z XX.01.01.000X
ckpt5    latest     User  2017-03-14T01:12:27Z XX.01.01.000X
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command syntax show checkpoint list all is replaced with show checkpoint.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
show checkpoint date

show checkpoint date <START-DATE> <END-DATE>

**Description**

Shows detailed list of all saved checkpoints created within the specified date range.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;START-DATE&gt;</td>
<td>Specifies the starting date for the range of saved checkpoints to show. Format: YYYY-MM-DD.</td>
</tr>
<tr>
<td>&lt;END-DATE&gt;</td>
<td>Specifies the ending date for the range of saved checkpoints to show. Format: YYYY-MM-DD.</td>
</tr>
</tbody>
</table>

**Examples**

Showing a detailed list of saved checkpoints for a specific date range:

```
switch# show checkpoint date 2017-03-08 2017-03-12
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>WRITER</th>
<th>DATE (YYYY/MM/DD)</th>
<th>IMAGE VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ckpt2</td>
<td>checkpoint</td>
<td>User</td>
<td>2017-03-08T18:10:01Z</td>
<td>XX.01.01.000X</td>
</tr>
<tr>
<td>ckpt3</td>
<td>checkpoint</td>
<td>User</td>
<td>2017-03-09T23:11:02Z</td>
<td>XX.01.01.000X</td>
</tr>
<tr>
<td>ckpt4</td>
<td>checkpoint</td>
<td>User</td>
<td>2017-03-11T00:00:03Z</td>
<td>XX.01.01.000X</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td><strong>Command syntax</strong> show checkpoint list date &lt;START-DATE&gt; &lt;END-DATE&gt; is replaced with show checkpoint date &lt;START-DATE&gt; &lt;END-DATE&gt;</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Shows the running-config checkpoint hash, calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[cli</td>
<td>json]</td>
</tr>
</tbody>
</table>

**Examples**

Showing the running-config checkpoint SHA-256 hash in CLI format:

```
switch# show running-config hash cli
Calculating the hash: [Success]
SHA-256 hash of the config in CLI format:
8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62a1d715075b89e
```

This hash is only valid for comparison to a baseline hash if the configuration has not been explicitly changed (such as with a CLI command, REST operation, etc.) or implicitly changed (such as by changing a hardware module, upgrading the SW version, etc.).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show startup-config hash**

```
show startup-config hash [cli | json]
```

**Description**

Shows the startup-config checkpoint hash, calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[cli</td>
<td>json]</td>
</tr>
</tbody>
</table>

**Examples**

Showing the startup-config checkpoint SHA-256 hash in CLI format:
switch# show startup-config hash cli
Calculating the hash: [Success]

SHA-256 hash of the config in CLI format:
8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62a1d715075b89e

This hash is only valid for comparison to a baseline hash if the configuration has not been explicitly changed (such as with a CLI command, REST operation, etc.) or implicitly changed (such as by changing a hardware module, upgrading the SW version, etc.).

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

write memory
write memory

Description

Saves the running configuration to the startup configuration. It is an alias of the command `copy running-config startup-config`. If the startup configuration is already present, this command overwrites the startup configuration.

Examples

switch# write memory
Success

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
**Boot commands**

**boot set-default**

`boot set-default {primary | secondary}`

**Description**
Sets the default operating system image to use when the system is booted.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Selects the primary network operating system image.</td>
</tr>
<tr>
<td>secondary</td>
<td>Selects the secondary network operating system image.</td>
</tr>
</tbody>
</table>

**Example**
Selecting the primary image as the default boot image:

```
switch# boot set-default primary
Default boot image set to primary.
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**boot system**

`boot system [primary | secondary | serviceos]`

**Description**
Reboots all modules on the switch. By default, the configured default operating system image is used. Optional parameters enable you to specify which system image to use for the reboot operation and for future reboot operations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Selects the primary operating system image for this reboot and sets the configured default operating system image to primary for future reboots.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>secondary</td>
<td>Selects the secondary operating system image for this reboot and sets the configured default operating system image to secondary for future reboots.</td>
</tr>
<tr>
<td>serviceos</td>
<td>Selects the service operating system for this reboot. Does not change the configured default operating system image. The service operating system acts as a standalone bootloader and recovery OS for switches running the AOS-CX operating system and is used in rare cases when troubleshooting a switch.</td>
</tr>
</tbody>
</table>

**Usage**

This command reboots the entire system. If you do not select one of the optional parameters, the system reboots from the configured default boot image.

You can use the `show images` command to show information about the primary and secondary system images.

Choosing one of the optional parameters affects the setting for the default boot image:

- If you select the `primary` or `secondary` optional parameter, that image becomes the configured default boot image for future system reboots. The command fails if the switch is not able to set the operating system image to the image you selected.
  
  You can use the `boot set-default` command to change the configured default operating system image.

- If you select `serviceos` as the optional parameter, the configured default boot image remains the same, and the system reboots all management modules with the service operating system.

If the configuration of the switch has changed since the last reboot, when you execute the `boot system` command you are prompted to save the configuration and you are prompted to confirm the reboot operation.

Saving the configuration is not required. However, if you attempt to save the configuration and there is an error during the save operation, the `boot system` command is aborted.

**Examples**

Rebooting the system from the configured default operating system image:

```
switch# boot system
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This will reboot the entire switch and render it unavailable until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
```

Rebooting the system from the secondary operating system image, setting the secondary operating system image as the configured default boot image:

```
switch# boot system secondary
Default boot image set to secondary.

Do you want to save the current configuration (y/n)? n
```
This will reboot the entire switch and render it unavailable until the process is complete.
Continue (y/n)? y
The system is going down for reboot.

Canceling a system reboot:

switch# boot system
Do you want to save the current configuration (y/n)? n
This will reboot the entire switch and render it unavailable until the process is complete.
Continue (y/n)? n
Reboot aborted.
switch#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show boot-history

show boot-history [all]

Description

Shows boot information. When no parameters are specified, shows the most recent information about the boot operation, and the three previous boot operations for the active management module. When the all parameter is specified, shows the boot information for the active management module.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows boot information for the active management module and all available line modules.</td>
</tr>
</tbody>
</table>

Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

Index
The position of the boot in the history file. Range: 0 to 3.
Boot ID
A unique ID for the boot. A system-generated 128-bit string.
Current Boot, up for <SECONDS> seconds
For the current boot, the show boot-history command shows the number of seconds the module has been running on the current software.

Timestamp boot reason
For previous boot operations, the show boot-history command shows the time at which the operation occurred and the reason for the boot. The reason for the boot is one of the following values:
<DAEMON-NAME> crash
The daemon identified by <DAEMON-NAME> caused the module to boot.
Kernel crash
The operating system software associated with the module caused the module to boot.
Reboot requested through database
The reboot occurred because of a request made through the CLI or other API.
Uncontrolled reboot
The reason for the reboot is not known.

Examples
Showing the boot history of the active management module:

```
switch# show boot-history
Management module
====================
Index : 3
Boot ID : f1bf071bdd04492bbf8439c6e479d612
Current Boot, up for 22 hrs 12 mins 22 secs

Index : 2
Boot ID : edfa2d6598d24e989668306c4a56a06d
07 Aug 18 16:28:01 : Reboot requested through database

Index : 1
Boot ID : 0bda8d0361df4a7e8e3acdc1dba5caad
07 Aug 18 14:08:46 : Reboot requested through database

Index : 0
Boot ID : 23da2b0e26d048d7b3f4b6721b69c110
07 Aug 18 13:00:46 : Reboot requested through database
switch#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

Firmware management commands

copy {primary | secondary} <REMOTE-URL>
copy {primary | secondary} <REMOTE-URL> [vrf <VRF-NAME>]

**Description**

Uploads a firmware image to a TFTP or SFTP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{primary</td>
<td>secondary}</td>
</tr>
<tr>
<td>&lt;REMOTE-URL&gt;</td>
<td>Specifies the URL to receive the uploaded firmware using SFTP or TFTP. For information on how to format the remote URL, see URL formatting for copy commands.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>

**Examples**

TFTP upload:

```bash
switch# copy primary tftp://192.0.2.0/00_10_00_0002.swi
####################################################
100.0%
Verifying and writing system firmware...
```

SFTP upload:

```bash
switch# copy primary sftp://swuser@192.0.2.0/00_10_00_0002.swi
swuser@192.0.2.0's password: Connected to 192.0.2.0.
sftp> put primary.swi XL_10_00_0002.swi
Uploading primary.swi to /users/swuser/00_10_00_0002.swi
primary.swi 100% 179MB 35.8MB/s 00:05
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy {primary | secondary} <FIRMWARE-FIILENAME>**

Copies a firmware image to USB storage.
### Configuration and firmware management

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{primary</td>
<td>secondary}</td>
</tr>
<tr>
<td>&lt;FIRMWARE-Filename&gt;</td>
<td>Specifies the name of the firmware file to create on the USB storage device. Prefix the filename with usb:/. For example:</td>
</tr>
<tr>
<td></td>
<td>usb:/firmware_v1.2.3.swi For information on how to format the path to a firmware file on a USB drive, see USB URL.</td>
</tr>
</tbody>
</table>

#### Examples

```bash
switch# copy primary usb:/11.10.00.002.swi
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### copy primary secondary

**copy primary secondary**

**Description**

Copies the firmware image from the primary to the secondary location.

**Examples**

```bash
switch# copy primary secondary
The secondary image will be deleted.

Continue (y/n)? y
Verifying and writing system firmware...
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy <REMOTE-URL>**

**copy <REMOTE-URL> {primary | secondary} [vrf <VRF-NAME>]**

**Description**

Downloads and installs a firmware image from a TFTP or SFTP server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;REMOTE-URL&gt;</td>
<td>Specifies the URL from which to download the firmware using SFTP or TFTP.</td>
</tr>
<tr>
<td>TFTP format:</td>
<td>tftp://&lt;IP-ADDR&gt;[:&lt;PORT-NUM&gt;] [;blocksize=&lt;Value&gt;]/&lt;FILENAME&gt;</td>
</tr>
<tr>
<td>SFTP format:</td>
<td>sftp://&lt;USERNAME&gt;@&lt;IP-ADDR&gt;[:&lt;PORT-NUM&gt;]/&lt;FILENAME&gt;</td>
</tr>
<tr>
<td>{primary</td>
<td>secondary}</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Default: default.</td>
</tr>
</tbody>
</table>

**TFTP usage**

To specify a URL with:

- an IPv4 address: tftp://1.1.1.1/a.txt
- an IPv6 address: tftp://[2000::2]/a.txt
- a hostname: tftp://hpe.com/a.txt

To specify TFTP with:

- the port number of the server in the URL: tftp://1.1.1.1:12/a.txt
- the blocksize in the URL: tftp://1.1.1.1:blocksize=1462/a.txt
  The valid blocksize range is 8 to 65464.
- the port number of the server and blocksize in the URL: tftp://1.1.1.1:12:blocksize=1462/a.txt

To specify a file in a directory of URL: tftp://1.1.1.1/dir/a.txt

**SFTP usage**

To specify:

- A URL with an IPv4 address: sftp://user@1.1.1.1/a.txt
- A URL with an IPv6 address: sftp://user@[2000::2]/a.txt
- A URL with a hostname: sftp://user@hpe.com/a.txt
- SFTP port number of a server in the URL: sftp://user@1.1.1.1:12/a.txt
- A file in a directory of URL: `sftp://user@1.1.1.1/dir/a.txt`
- To specify a file with absolute path in the URL: `sftp://user@1.1.1.1/home/user/a.txt`

**Examples**

**TFTP download:**

```plaintext
switch# copy tftp://192.10.12.0/ss.10.00.0002.swi primary
The primary image will be deleted.
Continue (y/n)? y

#########################################################################
100.0%
Verifying and writing system firmware...
```

**SFTP download:**

```plaintext
switch# copy sftp://swuser@192.10.12.0/ss.10.00.0002.swi primary
The primary image will be deleted.
Continue (y/n)? y
The authenticity of host '192.10.12.0 (192.10.12.0)' can't be established.
ECDSA key fingerprint is SHA256:L64khLwlyLgX1ARK8MiwcAAK8oRaQ8CDoWP+PkGBXHY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.10.12.0' (ECDSA) to the list of known hosts.
swuser@192.10.12.0's password:
Connected to 192.10.12.0.
Fetching /users/swuser/ss.10.00.0002.swi to ss.10.00.0002.swi.dnld
/users/swuser/ss.10.00.0002.swi 100% 179MB 25.6MB/s 00:07
Verifying and writing system firmware...
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy secondary primary**

**Description**
Copies the firmware image from the secondary to the primary location.

**Examples**
The primary image will be deleted.

Continue (y/n)? y

Verifying and writing system firmware...

The authenticity of host '192.22.1.0 (192.22.1.0)' can't be established.
ECDSA key fingerprint is SHA256:MyI1xbdKnehYut0NLfL69gDpNzCmZqBVvBaRR46m7o8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.22.1.0' (ECDSA) to the list of known hosts.

Verifying and writing system firmware...

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**copy <STORAGE-URL>**

`copy <STORAGE-URL> {primary | secondary}`

**Description**

Copies, verifies, and installs a firmware image from a USB storage device connected to the active management module.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<STORAGE-URL>` | Specifies the name of the firmware file to copy from the storage device. Required.  
USB format:  
`usb:/<FILENAME>` | |
| `{primary | secondary}` | Selects the primary or secondary image profile for receiving the copied firmware.                                                            |

**USB usage**
To specify a file:

- In a USB storage device: `usb:a.txt`
- In a directory of a USB storage device: `usb:dir/a.txt`

**Examples**

```
switch# copy usb:/11.10.00.0002.swi primary
The primary image will be deleted.
Continue (y/n)? y
Verifying and writing system firmware...
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Dynamic Segmentation (DS) is an enterprise network solution that combines AOS-CX security and networking features to dynamically place clients into network segments based on client credentials. The client network segments are dynamically carved out of the enterprise networks when on-boarding secure clients. With dynamic segmentation, there are multiple ways to handle client traffic:

- Locally switched to a VLAN
- User Based Tunnels (UBT).

In both solutions, once authenticated (using MAC-Auth or 802.1X) an enterprise client is bound to a network role and a VLAN is associated with the role. User traffic is then placed on the VLAN (know as the role VLAN) corresponding to the role to which the user belongs. Role association is defined using the individual client authentication mode or using device-profile based authentication.

The administrator must pre-configure all potential role VLANs and VRFs in all access switches (and additional configuration such as IGMP snooping on VLAN, PIM RP, etc.) at the gateway. The switch ensures that the role VLANs and VRFs are instantiated only upon client on-boarding on the target VLAN (using the command `system vlan-client-presence-detect`). This ensures that unnecessary broadcast domain creations and route learning do not occur.

There is no need to provision VLANs on the switch for user-based tunneling. The reserved VLAN is used by default.

### User-based tunneling

User-based tunneling uses GRE to tunnel ingress traffic on a switch interface to a mobility gateway for further processing. User-based tunneling enables a mobility gateway to provide a centralized security policy, using per-user authentication and access control to ensure consistent access and permissions.

Applications of user-based tunneling include:

- **Traffic segmentation**: Enables splitting of traffic based on user credentials, rather than the physical port to which a user is connected. For example, guests on a corporate network can be assigned to a specific VLAN with access and firewall policies defined to protect the network. Traffic from computers/laptops can be tunneled, while allowing VoIP traffic to move freely through the wired network.

- **Authentication of PoE devices**: Many devices that require power over Ethernet (PoE) and network access, such as security cameras, payment card readers, and medical devices, do not have built-in security software. As a result, these devices can pose a risk to networks. User-based tunneling can authenticate these devices and tunnel their traffic to a mobility gateway, harnessing the firewall and policy capabilities to secure the network.
At the most basic level User-Based Tunneling has two components:

- **User-Roles** refers to the ability to assign roles, on the fly, to a wired device/user, based on such things as the access method of a client. When leveraging ClearPass, additional context can be added, such as time-of-day and type-of-machine. As a result, IT staff no longer must pre-configure an access-port to VLAN and uplinks.

- **Tunneling** is the ability to tunnel traffic back to an Aruba Mobility Gateway (previously known as tunneled-node).

User-based tunneling supports two types of gateway deployments:

- Standalone Gateway Support
- Clusters Gateway Support

---

The recommended gateway version for user-based tunneling is 8.5 or greater.

The following commands are required to configure UBT:

- `ip source-interface`  
- `ubt`  
- `ubt-client-vlan`

---

`ubt-client-vlan` is needed for the local vlan or reserved vlan mode, but it is not needed for vlan-extend mode.

---

`ubt-mode vland-extend` is needed for vlan-extend mode.

---

**Components of user-based tunneling**

**Clients and devices**

Traditionally, ports were labeled with a color and a color was assigned to a specific device. With colorless ports, all ports on an access switch are set to authenticate with both 802.1X and MAC Authentication. When a device connects to the network it is authenticated using either MAC Authentication or 802.1X and triggers an enforcement policy from ClearPass, which contains an enforcement profile with a user role configuration.

**Access switches**

Access switches authenticate users connected to the switch. Once a device or user is authenticated, a role is applied to the device or user. A role is a set of attributes and policies that is applied to the device or user. This user role can exist locally on an access switch or on ClearPass as part of an enforcement profile.

**Mobility gateway cluster**

The Aruba Mobility Gateway has many built-in security and application capabilities tailored specifically to wireless traffic. However, this can be extended as well to wired traffic. This is the main reason to tunnel traffic from an Aruba access switch to a gateway, so the wired, tunneled traffic can take advantage of the gateway’s firewall capabilities and client applications.

**Aruba ClearPass Policy Manager**

ClearPass assigns enforcement policies and profiles containing user role information based on profiled devices or authenticated user information.

**How it works**
When first configuring the switch, the tunneling profile must be configured first. This is done using the command ubt zone. Within this context, the primary gateway IP address can be configured, which should be the physical IP of one of the cluster members. Once the gateway information is known on the switch and the UBT service is enabled, the switch then performs a handshake with the gateway to determine its reachability and to discover the version information.

When reachability is confirmed, the switch executes a switch bootstrap, and sends a bootstrap message to the gateway, similar to an AP Hello between an AP and a gateway. This bootstrap control packet contains user role information. Once the gateway receives the message, it replies with an acknowledge message. When acknowledged, the switch updates its local data structures with a bucket map and gateway node list, which is used for mapping users to gateways and client load balancing.

After the bucket map list is downloaded to the switch, a GRE heartbeat is then started between the switch and the gateway, forming a tunnel. A regular heartbeat, using GRE, is exchanged with the gateway, which then serves as the switch anchor gateway (SAC). This is the primary-gateway ip in the ubt zone command. A secondary heartbeat is also established with a standby gateway, acting as a secondary switch anchor gateway (S-SAC).

When a user connects to a secure port, the authentication sub-system on the switch sends a RADIUS request to the RADIUS server (for example, ClearPass Policy Manager), which authenticates the user and returns a user role to the switch in the form of a local user role (LUR) or vendor-specific attribute (VSA).

Aruba utilizes the concept of a user role which contains user policy and access to the network based on the role. A user-role can contain ACL/QoS policy, captive portal, VLAN information (used for locally switched traffic), and device attributes. When the user role VSA, received from the RADIUS server, is applied to the user, a command to redirect traffic to a gateway can be included within the user role. This is defined with the gateway zone command which causes tunneling to be enabled. The authentication sub-system notifies the tunneling subsystem on the switch, providing a gateway or secondary role. The gateway or secondary role is the user role on the gateway where policy will generally exist for tunneled users, and where firewall and security policies are applied. This can also be the same role used for wireless users and can be reused for wired users, if feasible.

The gateway role information sent to the switch tunneling subsystem is an indication to the gateway that it has to enforce additional policies on the user's traffic based on the policy configuration associated with the secondary role and the tunnel. This secondary role can be downloaded directly to the gateway. When the primary gateway or cluster is not reachable, the SAC tunnel is formed with the backup gateway and the clients are tunneled to the backup.

**Points to remember**

- **UBT Mode: Local VLAN**
  - UBT is supported on the default VRF and non-default VRF.
  - Source interface is specified using command `ip source-interface`.
  - VLAN is specified using command `ubt-client-vlan`.
  - `ubt-client-vlan` should not be used on any other feature on the switch except for the client IP address tracking feature.
  - UBT does not support tagged clients.
  - UBT clients and non-UBT clients on same VLAN and same port is not supported.
  - Source interface change: Disable UBT, change the source-interface, enable UBT.

- **UBT Mode: VLAN extend**
  - UBT is supported on the default VRF and non-default VRF.
  - Source interface is specified using command `ip source-interface`.
- UBT client vlan is defined under role.
- DHCP snooping and ND-snooping should not be enabled on a UBT client assigned VLAN.
- IGMP snooping should not be enabled on a UBT client assigned VLAN.
- The VLAN on which UBT clients are placed should not be configured on the switch uplink.
- UBT clients and non-UBT clients on the same VLAN on the same switch is not supported.
- Source interface change: Disable UBT, change the source-interface, enable UBT.

**Gateway DUR**
- Downloadable gateway role is supported with switch VSA only. Mixed mode role configuration is supported ((switch LUR + gateway radius VSA) + gateway DUR). Switch mixed role is used to send other role attributes along with VSA.
  - Use `aaa authentication port-access radius-override enable` to enable.
  - CPPM server FQDN/hostname configuration is supported.

---

Downloadable switch user role and multi-zone are not supported on the 4100i switch.

For information on IP Client Tracker, refer to the IP Client Tracker chapter in the Fundamentals Guide.

**PC behind an IP phone**
- You should not have a PC and phone on the same VLAN on the same port when the PC is a UBT client and the phone is a non-UBT client. If you do, UBT clients broadcast/multicast packets will return to the same port and corrupt the phone MAC table.

**Clients behind an L2 switch on the same VLAN**
- You should not have clients behind an L2 switch in a UBT environment. If UBT and non-UBT clients are behind an L2 switch on the same VLAN, this will cause duplicate packets. Broadcast/multicast packets will be copied to the tunnel and locally, causing the client to receive duplicate packets and network instability.

**Different user role access VLANs on the same port in UBT 1.0 mode for the 4100i switch**
- Two users with different user role access VLANs on the same switch port is not supported. This will lead to a bootstrap failure on the controller for the second user.

---

Connecting the client directly into switch ports or behind VoIP is recommended.

**Comparison between UBT modes**

<table>
<thead>
<tr>
<th>UBT Mode: Local VLAN</th>
<th>UBT Mode: VLAN extend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch unaware of UBT user VLAN</td>
<td>Switch is aware of user VLAN</td>
</tr>
<tr>
<td>Colorless ports: No UBT user VLAN config at switch</td>
<td>Colorless ports: UBT User VLAN config is required on switch</td>
</tr>
<tr>
<td>VLAN assignment by gateway</td>
<td>VLAN assignment by switch</td>
</tr>
<tr>
<td>Supports only untagged UBT users</td>
<td>Supports both tagged/untagged UBT users</td>
</tr>
<tr>
<td>UBT Mode: Local VLAN</td>
<td>UBT Mode: VLAN extend</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gateway replicates the broadcast/multicast traffic (converting bcast/mcast to unicast) and sends it to every UBT client</td>
<td>Single dedicated multicast GRE tunnel will be established between the gateway and switch for Broadcast/Multicast traffic</td>
</tr>
<tr>
<td>Gateway forwards all broadcast/multicast traffic to the UBT clients which are part of the same VLAN</td>
<td>Switch will forward the broadcast/multicast traffic to the UBT clients which are part of the same VLAN</td>
</tr>
<tr>
<td>The unicast/multicast/broadcast traffic from gateway to switch is sent to the clients via the same UAC tunnel</td>
<td>The unicast traffic from gateway to switch is sent through the UAC tunnel and multicast/broadcast traffic via Multicast GRE tunnel</td>
</tr>
<tr>
<td>Multicast traffic will be sent to the client which send join</td>
<td>Multicast traffic will be sent to all UBT clients on the same VLAN</td>
</tr>
</tbody>
</table>

**User-based tunneling commands**

**backup-controller ip**

backup-controller ip <IP-ADDR>

no backup-controller ip <IP-ADDR>

**Description**

Specifies the IP address of the backup controller for the UBT zone.

The no form of this command deletes the IP address of the backup controller.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies the IP address of the backup controller.</td>
</tr>
</tbody>
</table>

**Examples**

Specifying the backup controller ip address for zone1:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# backup-controller ip 10.116.51.11
```

Delete the configured backup controller IP address:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# no backup-controller ip 10.116.51.11
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
### enable

**enable**

**no enable**

**Description**

Enables the UBT zone.
The *no* form of this command disables the UBT zone.

**Examples**

Enabling UBT for zone `zone1`:

```bash
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# enable
```

Disabling UBT for `zone1`:

```bash
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# no enable
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-ubt-&lt;ZONE-NAME&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### ip source-interface (ubt)

**ip source-interface {all | ubt} {interface <IFNAME> | <IPV4-ADDR>} [vrf <VRF-NAME>]
no ip source-interface {all | ubt} {interface <IFNAME> | <IPV4-ADDR>} [vrf <VRF-NAME>]

**Description**

Sets a single source IP address for the UBT zone VRF. This ensures that all traffic sent by UBT zone/VRF has the same source IP address, regardless of how it egresses the switch.

This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The *no* form of this command deletes the single source IP address for UBT.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>When used no other parameters are required.</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the name of the interface from which UBT obtains its source IP address. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.</td>
</tr>
<tr>
<td>&lt;IPV4-ADDR&gt;</td>
<td>Specifies the source IP address to use for UBT. The IP address must be defined on the switch, and it must exist on the specified VRF. Default: default. Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of the VRF from which the UBT zone sets its source IP address.</td>
</tr>
</tbody>
</table>

**Examples**

Setting interface 1/1/7 as the source address for UBT for VRF default:

```
switch(config)# ip source-interface ubt interface 1/1/7 vrf default
```

Deleting the configured source interface 1/1/7 as the source address for UBT for VRF default:

```
switch(config)# no ip source-interface ubt interface 1/1/7 vrf default
```

Specifying the static IP address 1.1.1.1 as the source address for UBT for VRF default:

```
switch(config)# ip source-interface ubt 1.1.1.1 vrf default
```

Deleting the configured ip address as the source address for UBT for VRF default:

```
switch(config)# no ip source-interface ubt 1.1.1.1 vrf default
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**papi-security-key**

```
papi-security-key [[ciphertext <SEC-KEY> | plaintext <SEC-KEY>]]
no papi-security-key
```
**Description**

Specifies the shared security key used to encrypt UBT PAPI messages exchanged between the switch and the controller cluster for the zone.

The no form of this command deletes the shared security key.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciphertext &lt;SEC-KEY&gt;</td>
<td>Specifies an encrypted security key.</td>
</tr>
<tr>
<td>plaintext &lt;SEC-KEY&gt;</td>
<td>Specifies a plaintext security key. Range: 10 to 64 characters.</td>
</tr>
</tbody>
</table>

**NOTE:**
When the security key is not provided on the command line, plaintext security key prompting occurs upon pressing Enter. The entered security key characters are masked with asterisks.

**Examples**

Specifying the PAPI security key for UBT zone zone1 as plaintext:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# papi-security-key plaintext F82#450b
```

Specifying the PAPI security key for UBT zone1 with plaintext prompting:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# papi-security-key
Enter the PAPI security key: **********
Re-Enter the PAPI security key: **********
```

Specifying the PAPI security key for UBT zone1 as ciphertext:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# papi-security-key ciphertext AQBapdAVz5...RmH3+4cpg=
```

Removing the PAPI security key for UBT zone1:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# no papi-security-key
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
### primary-controller ip

**primary-controller ip <IP-ADDR>**

**no primary-controller ip <IP-ADDR>**

**Description**

Specifies the IP address of the primary controller IP address for the zone.

The `no` form of this command deletes the IP address of the primary controller.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies the IP address of the primary controller.</td>
</tr>
</tbody>
</table>

**Examples**

Specify the primary controller IP address for `zone1`:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# primary-controller ip 10.116.51.10
```

Delete the configured primary controller IP address:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# no primary-controller ip 10.116.51.10
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-ubt-&lt;ZONE-NAME&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### sac-heartbeat-interval

**sac-heartbeat-interval <TIME>**

**no sac-heartbeat-interval <TIME>**

**Description**

Specifies the SAC heartbeat refresh time interval in seconds.

The `no` form of this command sets the heartbeat interval to the default value.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TIME&gt;</code></td>
<td>Specifies the SAC heartbeat refresh time interval in seconds. Range: 1 to 8. Default: 1.</td>
</tr>
</tbody>
</table>

**Examples**

Specifying a heartbeat refresh interval of 1 for UBT zone1:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# sac-heartbeat-interval 1
```

Deleting the configured heartbeat refresh interval:

```
switch(config)# ubt zone zone1
switch(config-ubt-zone1)# no sac-heartbeat-interval
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-ubt-&lt;ZONE-NAME&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ip source-interface ubt**

**show ip source-interface ubt**

**Description**

Displays source IP address configuration information for the UBT zone.

**Examples**

Showing source IP address configuration information:

```
switch(config)# show ip source-interface ubt
Source-interface Configuration Information
-----------------------------------------------
Protocol | Src-Interface | Src-IP | VRF     |
----------|---------------|--------|---------|
ubt       | vlan10        | 10.1.1.2| default |
```

**Command History**
Command Information

Platforms | Command context | Authority
--- | --- | ---
4100i | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command.

show capacities ubt

show capacities ubt

Description

Shows the maximum number of UBT clients and zones which can be configured in the system.

Example

Showing maximum number of UBT clients and zones which can be configured:

```
switch# show capacities ubt
System Capacities: Filter UBT Capacities
Name Value
--------------------------------------
Maximum number of UBT clients in a system 768
Maximum number of UBT zones 1
```

On a 24 port 4100i switch, the max number of UBT clients is 768. On a 12 port 4100i switch, the max number of UBT clients is 384.

If TCAM resources are utilized by other features and not available for UBT, UBT user-bootstrap will fail and result in a resource unavailable error message.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
**show ubt**

show ubt [brief]
show ubt zone <ZONE-NAME> [brief]

**Description**

Shows global configuration information for UBT in addition to detailed or brief information for a specific UBT zone.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone &lt;ZONE-NAME&gt;</td>
<td>Specifies the name of a zone. Length: 1 to 64 characters.</td>
</tr>
<tr>
<td>brief</td>
<td>Displays brief information.</td>
</tr>
</tbody>
</table>

**Examples**

Showing global UBT configuration information where local-VLAN mode has been configured:

```plaintext
switch# show ubt
Zone Name                  : zone1
UBT Mode                   : local-vlan
Primary Controller         : 10.116.51.10
Backup Controller          : 10.116.51.11
SAC HeartBeat Interval     : 1
UAC KeepAlive Interval     : 60
Reserved VLAN Identifier   : 4094
VRF Name                   : default
Admin State                : ENABLED
PAPI Security Key          : AQBapdxysvGpvdTl ... bL4FE=
```

Showing global UBT configuration information where VLAN-extend mode has been configured:

```plaintext
switch# show ubt
Zone Name                  : zone1
UBT Mode                   : vlan-extend
Primary Controller         : 10.116.51.10
Backup Controller          : 10.116.51.11
SAC HeartBeat Interval     : 1
UAC KeepAlive Interval     : 60
Reserved VLAN Identifier   : -NA-
VRF Name                   : default
Admin State                : ENABLED
PAPI Security Key          : AQBapdxysvGpvdTlkYn1 ... bL4FE=
```

Showing global UBT configuration information with operational state down failure reason:

```plaintext
switch# show ubt
Zone Name                  : my-zone
UBT Mode                   : local-vlan
Primary Controller         : 10.116.51.10
Backup Controller          : 10.116.51.11
SAC HeartBeat Interval     : 1
```
Showing brief global UBT configuration information where local-VLAN mode has been configured:

```
switch(config)# show ubt brief

<table>
<thead>
<tr>
<th>Zone Name</th>
<th>UBT Mode</th>
<th>Primary Controller Address</th>
<th>VRF Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone1</td>
<td>local-vlan</td>
<td>10.116.51.10</td>
<td>default</td>
<td>Enabled</td>
</tr>
<tr>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone2</td>
<td>local-vlan</td>
<td>20.116.51.20</td>
<td>vrf2</td>
<td>Enabled</td>
</tr>
<tr>
<td>down</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone3</td>
<td>local-vlan</td>
<td>30.116.51.30</td>
<td>vrf3</td>
<td>Enabled</td>
</tr>
<tr>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Showing brief global UBT configuration information where VLAN-extend mode has been configured:

```
switch# show ubt brief

<table>
<thead>
<tr>
<th>Zone Name</th>
<th>UBT Mode</th>
<th>Primary Controller Address</th>
<th>VRF Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone1</td>
<td>vlan-extend</td>
<td>10.116.51.10</td>
<td>default</td>
<td>Enabled</td>
</tr>
<tr>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone2</td>
<td>vlan-extend</td>
<td>20.116.51.20</td>
<td>vrf2</td>
<td>Enabled</td>
</tr>
<tr>
<td>down</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zone3</td>
<td>vlan-extend</td>
<td>30.116.51.30</td>
<td>vrf3</td>
<td>Enabled</td>
</tr>
<tr>
<td>up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Showing brief configuration for UBT zone1 where local-VLAN mode has been configured:

```
switch# show ubt zone zone1 brief
```
Showing brief configuration for UBT zone1 where VLAN-extend mode has been configured:

```
switch# show ubt zone zone1 brief
----------------------------------------
Zone Name  UBT Mode        Primary Controller Address VRF Name Status
----------------------------------------
zoned     local-vlan      10.116.51.10      default  Enabled
----------------------------------------
```

Showing brief global UBT configuration information where VLAN-extend mode has been configured:

```
switch# show ubt zone zone1 brief
----------------------------------------
Zone Name  UBT Mode        Primary Controller Address VRF Name Status
----------------------------------------
zoned     vlan-extend      10.116.51.10      default  Enabled
----------------------------------------
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.09</td>
<td>- Failure Reason field added in the output of show ubt command.</td>
</tr>
<tr>
<td></td>
<td>- Operational State column added in the output of show ubt brief command.</td>
</tr>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt;) or Manager (‡)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ubt information**

`show ubt information`

`show ubt information zone <ZONE-NAME>`

**Description**

Shows SAC and UAC information for UBT. Specifying a zone name displays UBT information for that zone.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZONE-NAME</td>
<td>Specifies UBT zone name. Maximum characters: 64.</td>
</tr>
</tbody>
</table>
Examples

Showing SAC and UAC information for the tunneled node server:

```
switch(config)# show ubt information

=====================================================================  
Zone zone1:
=====================================================================  
SAC Information :
  Active     : 10.1.1.2  
  Standby    : 10.1.1.3  

Node List Information :
  Cluster Name : cluster1  
  Cluster Alias Name :  
  Node List :
    ---------------  
    10.1.1.2  
    10.1.1.3  
    10.1.1.4  

Bucket Map Information :
  Bucket Map Active : [0..255]

  Bucket ID  A-UAC  S-UAC  Connectivity  
              0  10.1.1.2  10.1.1.3  L2  
              1  10.1.1.3  10.1.1.4  L2  
              2  10.1.1.4  10.1.1.2  L2  
      ...  
```

Showing SAC and UAC information for zone1:

```
switch(config)# show ubt information zone zone1

=====================================================================  
Zone zone1:
=====================================================================  
SAC Information :
  Active     : 10.1.1.2  
  Standby    : 10.1.1.3  

Node List Information :
  Cluster Name : cluster1  
  Cluster Alias Name :  
  Node List :
    ---------------  
    10.1.1.2  
    10.1.1.3  
```
10.1.1.4

Bucket Map Information :

Bucket Map Active : [0...255]

<table>
<thead>
<tr>
<th>Bucket ID</th>
<th>A-UAC</th>
<th>S-UAC</th>
<th>Connectivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.1.1.2</td>
<td>10.1.1.3</td>
<td>L2</td>
</tr>
<tr>
<td>1</td>
<td>10.1.1.3</td>
<td>10.1.1.4</td>
<td>L2</td>
</tr>
<tr>
<td>2</td>
<td>10.1.1.4</td>
<td>10.1.1.2</td>
<td>L2</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show ubt state

show ubt state
show ubt state zone <ZONE-NAME>
show ubt state zone <ZONE-NAME> uac-ip <UAC-ADDR>

Description

Shows the global UBT state.
Specifying a zone shows the UBT state of that zone.
Specifying a UAC IP address shows the UBT state of that UAC.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone &lt;ZONE-NAME&gt;</td>
<td>Specifies UBT zone name. Maximum characters: 64.</td>
</tr>
<tr>
<td>uac-ip &lt;UAC-ADDR&gt;</td>
<td>Specifies the IP address of the user anchor controller for which to view user information. Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
</tbody>
</table>

Examples

Showing the UBT state where local-VLAN mode has been configured:

switch# show ubt state
======================================================================
Zone zone1:
==================================================================================================================
Local Conductor Server (LCS) State:
LCS Type    IP Address    State                Role
==================================================================================================================
Primary  : 10.1.1.2    ready_for_bootstrap operational_primary
Secondary: 10.1.1.10   ready_for_bootstrap operational_secondary
Switch Anchor Controller (SAC) State:
IP Address    MAC Address    State
==================================================================================================================
Active  : 10.1.1.2    00:0b:86:b7:62:9f    registered
Standby : 10.1.1.3    00:0b:86:b7:64:0f    registered
User Anchor Controller (UAC): 10.1.1.2
User      Port     State    Bucket ID    Gre Key    VLAN
------------------------------------------------------------------------------------------------------------------
00:00:00:00:00:01   1/1/1    registered    5      13      4094
User Anchor Controller (UAC): 10.1.1.3
User      Port     State    Bucket ID    Gre Key    VLAN
------------------------------------------------------------------------------------------------------------------
00:00:00:00:00:02   1/1/2    registered    4      14      4094

Showing the UBT state where VLAN-extend mode has been configured:

switch# show ubt state
==================================================================================================================
Zone zone1:
==================================================================================================================
Local Conductor Server (LCS) State:
LCS Type    IP Address    State                Role
==================================================================================================================
Primary  : 10.1.1.2    ready_for_bootstrap operational_primary
Secondary: 10.1.1.10   ready_for_bootstrap operational_secondary
Switch Anchor Controller (SAC) State:
IP Address    MAC Address    State
==================================================================================================================
Active  : 10.1.1.2    00:0b:86:b7:62:9f    registered
Standby : 10.1.1.3    00:0b:86:b7:64:0f    registered
User Anchor Controller (UAC): 10.1.1.2
User      Port     State    Bucket ID    Gre Key    VLAN
------------------------------------------------------------------------------------------------------------------
00:00:00:00:00:01   1/1/1    registered    5      13      10
User Anchor Controller (UAC): 10.1.1.3
User      Port     State    Bucket ID    Gre Key    VLAN
------------------------------------------------------------------------------------------------------------------
00:00:00:00:00:02   1/1/2    registered    4      14      20

Showing the UBT state of zone1:

switch# show ubt state zone zone1
==================================================================================================================
Zone zone1:
==================================================================================================================
Local Conductor Server (LCS) State:
Switch Anchor Controller (SAC) State:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>00:0b:86:b7:62:9f</td>
<td>registered</td>
</tr>
<tr>
<td>Standby</td>
<td>00:0b:86:b7:62:64:0f</td>
<td>registered</td>
</tr>
</tbody>
</table>

User Anchor Controller (UAC): 10.1.1.2

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>State</th>
<th>Bucket ID</th>
<th>Gre Key</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:01</td>
<td>1/1/1</td>
<td>registered</td>
<td>5</td>
<td>13</td>
<td>10</td>
</tr>
</tbody>
</table>

User Anchor Controller (UAC): 10.1.1.3

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>State</th>
<th>Bucket ID</th>
<th>Gre Key</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:02</td>
<td>1/1/2</td>
<td>registered</td>
<td>4</td>
<td>14</td>
<td>20</td>
</tr>
</tbody>
</table>

Showing the UBT state of a UAC with IP address 15.212.219.57 where local-VLAN mode has been configured:

```
switch# show ubt state zone zonel uac-ip 15.212.219.57

User Anchor Controller (UAC): 15.212.219.57

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>State</th>
<th>Bucket ID</th>
<th>Gre Key</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:04</td>
<td>1/1/20</td>
<td>registered</td>
<td>4</td>
<td>14</td>
<td>4000</td>
</tr>
</tbody>
</table>
```

Showing the UBT state of a UAC with IP address 15.212.219.55 where VLAN-extend mode has been configured:

```
switch# show ubt state zone zonel uac-ip 15.212.219.55

User Anchor Controller (UAC): 15.212.219.55

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>State</th>
<th>Bucket ID</th>
<th>Gre Key</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:07</td>
<td>1/1/10</td>
<td>registered</td>
<td>40</td>
<td>14</td>
<td>20</td>
</tr>
<tr>
<td>00:00:00:00:00:08</td>
<td>1/1/12</td>
<td>registered</td>
<td>28</td>
<td>14</td>
<td>30</td>
</tr>
</tbody>
</table>
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
Platforms | Command context | Authority
--- | --- | ---
4100i | Operator (>) or Manager(#) | Administrators or local user group members with execution rights for this command.

**show ubt statistics**

`show ubt statistics`

`show ubt statistics zone <ZONE-NAME>`

`show ubt statistics zone <ZONE-NAME> uac-ip <UAC-ADDR>`

**Description**

Displays statistics for UBT.

Specifying a zone shows the UBT statistics for that zone.

Specifying a UAC IP address shows the UBT statistics for that UAC.

**Parameter** | **Description**
--- | ---
`zone <ZONE-NAME>` | Specifies UBT zone name. Maximum characters: 64.
`uac-ip <UAC-ADDR>` | Specifies the IP address of the user anchor controller for which to view user information. Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

**Examples**

Showing UBT statistics where local-VLAN mode has been configured:

```
switch# show ubt statistics
UBT Statistics
===================================================================== Zone zonel:
===================================================================== Control Plane Statistics
Active  : 10.1.1.1
  Bootstrap Tx : 10   Bootstrap Rx : 10
  Nodelist Rx  : 25   Nodelist Ack Rx : 6
  Bucketmap Rx : 21   Bucketmap Ack Rx : 10
  Failover Tx  : 4    Failover Ack Rx : 3
  Unbootstrap Tx : 7   Unbootstrap Ack Rx : 5
  Heartbeat Tx : 5    Heartbeat Rx : 3
Standby : 10.1.1.2
  Bootstrap Tx : 10   Bootstrap Rx : 10
  Nodelist Rx  : 25   Nodelist Ack Rx : 6
  Bucketmap Rx : 21   Bucketmap Ack Rx : 12
  Failover Tx  : 4    Failover Ack Rx : 3
  Unbootstrap Tx : 5   Unbootstrap Ack Rx : 3
  Heartbeat Tx : 7    Heartbeat Rx : 4
UAC : 10.1.1.1
  Bootstrap Tx : 10   Bootstrap Ack Rx : 5
  Unbootstrap Tx : 5   Unbootstrap Ack Rx : 5
  Keepalive Tx : 2    Keepalive Ack Rx : 2
UAC : 10.1.1.2
  Bootstrap Tx : 5    Bootstrap Ack Rx : 5
  Unbootstrap Tx : 0   Unbootstrap Ack Rx : 0
```
Showing UBT statistics where VLAN-extend mode has been configured:

```plaintext
switch# show ubt statistics
UBT Statistics
===================================================================== 
Zone zone1: 
===================================================================== 
Control Plane Statistics 
 Active : 10.1.1.3 
 Bootstrap Tx : 10  Bootstrap Rx : 10 
 Nodelist Rx : 25  Nodelist Ack Rx : 6 
 Bucketmap Rx : 21  Bucketmap Ack Rx : 10 
 Failover Tx : 4  Failover Ack Rx : 3 
 Unbootstrap Tx : 7  Unbootstrap Ack Rx : 5 
 Heartbeat Tx : 5  Heartbeat Rx : 3 
 Standby : 10.1.1.4 
 Bootstrap Tx : 10  Bootstrap Rx : 10 
 Nodelist Rx : 25  Nodelist Ack Rx : 6 
 Bucketmap Rx : 21  Bucketmap Ack Rx : 12 
 Failover Tx : 4  Failover Ack Rx : 3 
 Unbootstrap Tx : 5  Unbootstrap Ack Rx : 3 
 Heartbeat Tx : 7  Heartbeat Rx : 4 
 UAC : 10.1.1.3 
 Bootstrap Tx : 10  Bootstrap Ack Rx : 5 
 Unbootstrap Tx : 5  Unbootstrap Ack Rx : 5 
 Keepalive Tx : 2  Keepalive Ack Rx : 2 
 UAC : 10.1.1.4 
 Bootstrap Tx : 5  Bootstrap Ack Rx : 5 
 Unbootstrap Tx : 0  Unbootstrap Ack Rx : 0 
 Keepalive Tx : 0  Keepalive Ack Rx : 0 
Data Plane Statistics 
 SAC tunnel Rx : 444 
 Standby-SAC tunnel Rx : 0 
 UAC Packets Tx Packets Rx 
---------------------------------------- 
 10.1.1.3  45678  23456 
 10.1.1.4  34567  23457 
User Statistics 
 UAC User Count 
------------------ 
 10.1.1.3  1 
 10.1.1.4  2 
```

Showing UBT statistics for zone1 where local-vlan mode has been configured:
switch# show ubt statistics zone zone1

UBT Statistics

Zone zone1:
Control Plane Statistics

<table>
<thead>
<tr>
<th></th>
<th>Control Plane Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>10.1.1.3</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Tx: 10</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Rx: 10</td>
</tr>
<tr>
<td></td>
<td>Nodelist Rx: 25</td>
</tr>
<tr>
<td></td>
<td>Nodelist Ack Rx: 6</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Rx: 21</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Ack Rx: 12</td>
</tr>
<tr>
<td></td>
<td>Failover Tx: 4</td>
</tr>
<tr>
<td></td>
<td>Failover Ack Rx: 3</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Tx: 7</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Ack Rx: 5</td>
</tr>
<tr>
<td></td>
<td>Heartbeat Tx: 7</td>
</tr>
<tr>
<td></td>
<td>Heartbeat Rx: 3</td>
</tr>
<tr>
<td>Standby</td>
<td>10.1.1.4</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Tx: 10</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Rx: 10</td>
</tr>
<tr>
<td></td>
<td>Nodelist Rx: 25</td>
</tr>
<tr>
<td></td>
<td>Nodelist Ack Rx: 6</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Rx: 21</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Ack Rx: 12</td>
</tr>
<tr>
<td></td>
<td>Failover Tx: 4</td>
</tr>
<tr>
<td></td>
<td>Failover Ack Rx: 3</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Tx: 5</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Ack Rx: 3</td>
</tr>
<tr>
<td></td>
<td>Heartbeat Tx: 7</td>
</tr>
<tr>
<td></td>
<td>Heartbeat Rx: 4</td>
</tr>
<tr>
<td>UAC</td>
<td>10.1.1.3</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Tx: 10</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Ack Rx: 5</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Tx: 5</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Ack Rx: 5</td>
</tr>
<tr>
<td></td>
<td>Keepalive Tx: 2</td>
</tr>
<tr>
<td></td>
<td>Keepalive Ack Rx: 2</td>
</tr>
<tr>
<td>UAC</td>
<td>10.1.1.4</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Tx: 5</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Ack Rx: 5</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Tx: 0</td>
</tr>
<tr>
<td></td>
<td>Unbootstrap Ack Rx: 0</td>
</tr>
<tr>
<td></td>
<td>Keepalive Tx: 0</td>
</tr>
<tr>
<td></td>
<td>Keepalive Ack Rx: 0</td>
</tr>
</tbody>
</table>

Data Plane Statistics

<table>
<thead>
<tr>
<th></th>
<th>UAC</th>
<th>Packets Tx</th>
<th>Packets Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.1.1.3</td>
<td>45678</td>
<td>23456</td>
</tr>
<tr>
<td></td>
<td>10.1.1.4</td>
<td>34567</td>
<td>23457</td>
</tr>
</tbody>
</table>

User Statistics

<table>
<thead>
<tr>
<th></th>
<th>UAC</th>
<th>User Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.1.1.3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>10.1.1.4</td>
<td>2</td>
</tr>
</tbody>
</table>

Showing UBT statistics for zone1 where VLAN-extend mode has been configured:

switch# show ubt statistics zone zone1

UBT Statistics

Zone zone1:
Control Plane Statistics

<table>
<thead>
<tr>
<th></th>
<th>Control Plane Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>10.1.1.3</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Tx: 10</td>
</tr>
<tr>
<td></td>
<td>Bootstrap Rx: 10</td>
</tr>
<tr>
<td></td>
<td>Nodelist Rx: 25</td>
</tr>
<tr>
<td></td>
<td>Nodelist Ack Rx: 6</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Rx: 21</td>
</tr>
<tr>
<td></td>
<td>Bucketmap Ack Rx: 10</td>
</tr>
<tr>
<td></td>
<td>Failover Tx: 4</td>
</tr>
<tr>
<td></td>
<td>Failover Ack Rx: 3</td>
</tr>
</tbody>
</table>

Showing UBT statistics for zone1 where VLAN-extend mode has been configured:
Unbootstrap Tx : 7          Unbootstrap Ack Rx : 5
Heartbeat Tx : 5           Heartbeat Rx : 3

Standby : 10.1.1.4
  Bootstrap Tx : 10           Bootstrap Rx : 10
  Nodelist Rx : 25           Nodelist Ack Rx : 6
  Bucketmap Rx : 21          Bucketmap Ack Rx : 12
  Failover Tx : 4            Failover Ack Rx : 3
  Unbootstrap Tx : 5         Unbootstrap Ack Rx : 3
  Heartbeat Tx : 7           Heartbeat Rx : 4

UAC : 10.1.1.3
  Bootstrap Tx : 10           Bootstrap Ack Rx : 5
  Unbootstrap Tx : 5          Unbootstrap Ack Rx : 5
  Keepalive Tx : 2            Keepalive Ack Rx : 2

UAC : 10.1.1.4
  Bootstrap Tx : 5            Bootstrap Ack Rx : 5
  Unbootstrap Tx : 0          Unbootstrap Ack Rx : 0
  Keepalive Tx : 0            Keepalive Ack Rx : 0

Data Plane Statistics

  SAC tunnel Rx : 444
  Standby-SAC tunnel Rx : 0

<table>
<thead>
<tr>
<th>UAC</th>
<th>Packets Tx</th>
<th>Packets Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.3</td>
<td>45678</td>
<td>23456</td>
</tr>
<tr>
<td>10.1.1.4</td>
<td>34567</td>
<td>23457</td>
</tr>
</tbody>
</table>

User Statistics

<table>
<thead>
<tr>
<th>UAC</th>
<th>User Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.3</td>
<td>1</td>
</tr>
<tr>
<td>10.1.1.4</td>
<td>2</td>
</tr>
</tbody>
</table>

Showing the UBT statistics of a UAC with IP address 101.101.11:

switch# show ubt statistics zone zonel uac-ip 101.101.11

Data Plane Statistics

  SAC tunnel Rx : 6457
  Standby-SAC tunnel Rx : 0

<table>
<thead>
<tr>
<th>UAC</th>
<th>Packets Tx</th>
<th>Packets Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>101.101.101.11 :</td>
<td>145379605</td>
<td>145450113</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
show ubt users

show ubt users [ all | count | down | mac <MAC-ADDR> | (port <IF-NAME> | <IF-RANGE>) | up] zone <ZONE-NAME>

Description
Displays user information for UBT.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display information for all users.</td>
</tr>
<tr>
<td>count</td>
<td>Display the total number of users configured to tunnel traffic.</td>
</tr>
<tr>
<td>down</td>
<td>Display the users that are not able to tunnel traffic.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Display user information based on MAC address.</td>
</tr>
<tr>
<td>port &lt;IF-NAME&gt;</td>
<td>&lt;IF-RANGE&gt;</td>
</tr>
<tr>
<td>up</td>
<td>Display user information that are active.</td>
</tr>
<tr>
<td>zone &lt;ZONE-NAME&gt;</td>
<td>Specifies UBT zone name. Maximum characters: 64.</td>
</tr>
</tbody>
</table>

Examples
Showing information for all users:

```text
switch# show ubt users all
===================================================================== Displaying All UBT Users for Zone: zone1
===================================================================== Downloaded user roles are preceded by *
Port  Mac Address  Tunnel Status  Secondary UserRole  Failure Reason
---------------------------------------------------------------------
1/25  00:00:00:11:12:03  activated  authenticated  ---/---
```

Showing information for users of zone1:

```text
switch# show ubt users all zone zone1
===================================================================== Displaying All UBT Users for Zone: zone1
===================================================================== Downloaded user roles are preceded by *
Port  Mac Address  Tunnel Status  Secondary UserRole  Failure Reason
---------------------------------------------------------------------
1/25  00:00:00:11:12:03  activated  authenticated  ---/---
```
Displaying the number of users that are tunneling traffic:

```
switch# show ubt users count
Total Number of Users using ubt Zone : zone1 is 2
Total Number of Users in all the zones : 2
```

Showing users that are down:

```
switch# show ubt users down

Displaying UBT Users of Zone: zone1 having Tunnel Status DOWN

Downloaded user roles are preceded by *
<table>
<thead>
<tr>
<th>Port</th>
<th>Mac Address</th>
<th>Tunnel Status</th>
<th>Secondary UserRole</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/25</td>
<td>00:00:00:11:12:03 activation_failed</td>
<td>authenticated</td>
<td>User bootstrap has failed</td>
<td></td>
</tr>
</tbody>
</table>
```

Showing information for users of zone1 that are down:

```
switch# show ubt users down zone zone1

Displaying UBT Users of Zone: zone1 having Tunnel Status DOWN

Downloaded user roles are preceded by *
<table>
<thead>
<tr>
<th>Port</th>
<th>Mac Address</th>
<th>Tunnel Status</th>
<th>Secondary UserRole</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/25</td>
<td>00:00:00:11:12:03 activation_failed</td>
<td>authenticated</td>
<td>User bootstrap has failed</td>
<td></td>
</tr>
</tbody>
</table>
```

Showing information for users on port 2/25:

```
switch# show ubt users port 2/25

Displaying UBT Users of Zone: zone1

Downloaded user roles are preceded by *
<table>
<thead>
<tr>
<th>Port</th>
<th>Mac Address</th>
<th>Tunnel Status</th>
<th>Secondary UserRole</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/25</td>
<td>00:00:00:11:12:03</td>
<td>activated</td>
<td>authenticated</td>
<td>---/---</td>
</tr>
</tbody>
</table>
```

Showing information for users that are up:

```
switch# show ubt users up

Displaying UBT Users of Zone: zone1 having Tunnel Status UP

Downloaded user roles are preceded by *
```
Showing information for users of zone 1 that are up:

```
switch# show ubt users up zone zone 1
Displaying UBT Users of Zone: zone 1 having Tunnel Status UP
Downloaded user roles are preceded by *
```

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Mac Address</th>
<th>Tunnel Status</th>
<th>Secondary UserRole</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/25</td>
<td>00:00:00:11:12:03</td>
<td>activated</td>
<td>authenticated</td>
<td>---/---</td>
</tr>
</tbody>
</table>
```

Showing information for the user with MAC address 00:00:00:11:12:03:

```
switch# show ubt users mac 00:00:00:11:12:03
Displaying UBT User of Zone: zone 1 having MAC-Address: 00:00:00:11:12:03
Downloaded user roles are preceded by *
```

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Mac Address</th>
<th>Tunnel Status</th>
<th>Secondary UserRole</th>
<th>Failure Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/25</td>
<td>00:00:00:11:12:03</td>
<td>activated</td>
<td>authenticated</td>
<td>---/---</td>
</tr>
</tbody>
</table>
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**uac-keepalive-interval**

No uac-keepalive-interval <TIME>

**Description**

Specifies the UAC keep alive refresh time interval in seconds for the UBT zone.

The no form of this command sets the keep alive interval to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the UAC keep-alive refresh time interval in seconds. Range: 1 to 60. Default: 60.</td>
</tr>
</tbody>
</table>
Examples

Specifying a keepalive interval of 60 seconds for UBT zone1:

```
switch(config)# ubt zone zonel
switch(config-ubt-zonel)# uac-keepalive-interval 60
```

Deleting the configured UAC keepalive interval:

```
switch(config)# ubt zone zonel
switch(config-ubt-zonel)# no uac-keepalive-interval 60
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-ubt-&lt;ZONE-NAME&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ubt

```
ubt zone <ZONE-NAME> vrf <VRF-NAME>
no ubt zone <ZONE-NAME> vrf <VRF-NAME>
```

Description

Creates a User Based Tunnel (UBT) zone with a specified zone name and VRF name. A UBT name is used to configure all UBT properties advertised by the UBT feature.

The `no` form of this command removes the specified UBT zone.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ZONE-NAME&gt;</td>
<td>Specifies a name for the UBT zone. Length: 1 to 64 characters.</td>
</tr>
<tr>
<td>&lt;VRF-NAME&gt;</td>
<td>Specifies the VRF on which to establish the UBT tunnel.</td>
</tr>
</tbody>
</table>

Examples

Creating UBT zone called zonel associated with a VRF called default:

```
switch(config)# ubt zone zonel vrf default
```

Removing UBT zone zonel on VRF default:

```
switch(config)# no ubt zone zonel vrf default
```
Deleting all UBT configurations:

```bash
switch(config)# no ubt
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ubt-client-vlan**

`ubt-client-vlan <VLAN-ID>`

`no ubt-client-vlan <VLAN-ID>`

**Description**

Specifies the UBT Client VLAN or local VLAN. This VLAN is used in local-VLAN mode only. If the UBT client VLAN is configured in VLAN-extend mode it is ignored, this is the reserved VLAN that all client traffic uses to get to the gateway. At the gateway, VLAN and policy will be assigned to the client traffic. No other feature should be enabled on the UBT client VLAN. The `no` form of this command removes the VLAN to use for tunneled clients.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;VLAN-ID&gt;</code></td>
<td>Specifies the VLAN ID to use for tunneled clients. Range: 1-4094.</td>
</tr>
</tbody>
</table>

**Examples**

Creating VLAN 4000:

```bash
switch(config)# vlan 4000
switch(config-vlan-4000)# no shutdown
```

Specifying UBT client VLAN 4000:

```bash
switch(config)# ubt-client-vlan 4000
```

Removing configured UBT client VLAN 4000:

```bash
switch(config)# no ubt-client-vlan 4000
```
Command Information

Platforms | Command context | Authority
--- | --- | ---
4100i | config | Administrators or local user group members with execution rights for this command.

ubt mode vlan-extend

ubt-mode vlan-extend
no ubt-mode [vlan-extend]

Description
Selects VLAN extended mode. When VLAN-extend mode is enabled clients are assigned to their UBT role-based VLAN in the hardware datapath.

The no form of the command selects the default local-VLAN mode. In local-VLAN mode clients are assigned to a local switch VLAN and associated with their UBT role-based VLAN when client traffic reaches the controller.

The default UBT mode is local-VLAN.

Examples
Setting the UBT mode to VLAN-extend:

```
switch(config)# ubt-mode vlan-extend
```

Setting the UBT mode back to the default of local-VLAN:

```
switch(config)# no ubt-mode
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

Platforms | Command context | Authority
--- | --- | ---
4100i | config | Administrators or local user group members with execution rights for this command.
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.

**Configuring SNMP**

(The SNMP agent provides read-only access.)

**Procedure**

1. Enable SNMP on a VRF using the command `snmp-server vrf default`.
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`
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`.
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`.
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:

- Sets the contact, location, and description for the switch to: `JaniceM, Building2, LabSwitch`.
- Sets the community string to `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.
Aruba Central integration is only available on the 4100i switch.

The Aruba Central network management solution, a software-as-a-service subscription in the cloud, provides streamlined management of multiple network devices. AOS-CX switches are able to talk to Aruba Central and utilize cloud-based management functionality. Cloud-based management functionality allows for the deployment of network devices at sites with no or few dedicated IT personnel (branch offices, retail stores, and so forth). AOS-CX switches utilize secure communication protocols to connect to the Aruba Central cloud portal, and can coexist with corporate security standards, such as those mandating the use of firewalls.

When Aruba Central manages AOS-CX switches, it functions as the single source of truth and the Web UI operates in read-only mode.

This feature provides:

- Zero-touch provisioning
- Network Management/Remote monitoring
- Events/alerts notification
- Switch Configuration using templates
- Firmware management

**Connecting to Aruba Central**

AOS-CX switch downloads the location of Aruba Central server using:

- Command-line interface (CLI).
- Aruba Activate server.
- DHCP options provided during ZTP.

DHCP servers are used to connect to Central on-premise management.

If switch is unable to connect to Activate server, it retries to establish connection in exponential back off of 1s, 2s, 8s, 16s, 32s, 64s, 128s, and 256s. After the maximum back off of 256s, switch retries happen for every 5 minutes.

If the Network Time Protocol (NTP) is not enabled on the switch, it will synchronize the system time with the Activate server.

**Custom CA certificate**

To use custom CA certificate to connect to Aruba Central, AOS-CX switch downloads the certificate from Aruba Activate server.
If there is no custom CA provided by Aruba Activate, the CA certificate present in the device is used.
- Duplicate CA certificates from Aruba Activate server will be ignored.
- If CA certificate is absent in consecutive responses from Aruba Activate server, the installed custom CA certificate in device will be removed.
- Switch will have only one custom CA certificate installed from Aruba Activate Server.
- The certificate installed from Aruba Activate server will not be displayed in the show commands.

### Support mode in Aruba Central

When the AOS-CX switch is managed by Aruba Central, the switch configuration cannot be modified using other interfaces such as CLI or Web UI. The following command categories are blocked:

- auto-confirm
- boot
- checkpoint
- copy-in commands
- erase
- https-server
- mfgread
- mfgwrite
- port-access
- All configuration commands except the aruba-central command

In cases where a maintenance or troubleshooting activity requires configuration updates, aruba-central support-mode can be enabled to allow these operations.

The aruba-central support-mode enable or disable operation is effective only in the CLI session where it is executed and does not impact the other CLI sessions.

If the user tries to execute any command that is not allowed, an **Invalid input:** error message is displayed.

### Aruba Central commands

#### aruba-central

**Applies only to the 4100i switch.**

```
aruba-central
no aruba-central
```

**Description**

Creates or enters the Aruba Central configuration context (config-aruba-central).

**Example**

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

Creating the Aruba Central configuration context:
switch(config)# aruba-central
switch(config-aruba-central)#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

aruba-central support-mode

Applies only to the 4100i switch.

aruba-central support-mode
no aruba-central support-mode

Description

Allows the device to be writable for all operations in Aruba Central lockout mode for troubleshooting. The no form of this command disables this activity.

Support-mode is disabled by default when the switch is managed by Aruba Central. This command is only effective in the CLI session where it is executed.

Examples

Configuring the device to be writable for all operations in Aruba Central lockout mode:

```
switch# aruba-central support-mode
switch#
```

Removing the configuration that allows the device to be writable for all operations in Aruba Central lockout mode:

```
switch# no aruba-central support-mode
switch#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>
configuration-lockout central managed

Applies only to the 4100i switch.

no configuration-lockout central managed

Description
Configures the device to only be writable from Aruba Central. Aruba Central will be the only agent that can add, modify, or delete configurations on the device. The no form of this command disables this feature.

Usage
The no form of this command is only available when the device is disconnected from Aruba Central.

Examples
Configuring the device to only be writable from Aruba Central:

```
switch(config)# configuration-lockout central managed
switch# show configuration-lockout
configuration lockout
-------------------------
central: managed
switch# sh aruba-central
Central admin state :enable
Central location :20.0.0.2:8083
VRF for connection :default
Central connection status :connected

Central source :cli
Central source connection status :connected
Central source last connected on :Tue Feb 9 17:53:13 UTC 2021

Activate Server URL :devices-v2.arubanetworks.com
CLI location :20.0.2:8083
CLI VRF :default
```
switch(config)# end
### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

#### disable

Applies only to the 4100i switch.

**Description**

Disables connection to Aruba Central server.

When the connection is disabled, the switch does not attempt to connect to the Aruba Central server or fetch central location from any of the three sources (CLI/Aruba Activate/DHCP). It also disconnects any active connection to the Aruba Central server.

**Example**

```
switch(config-aruba-central)# disable
switch(config-aruba-central)#
```

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

#### enable (aruba central)

Applies only to the 4100i switch.

**Description**
Enables connection to Aruba Central server. When the connection is enabled, the switch attempts to download the location of the Aruba Central server in one of the following ways at startup and after the connection is lost:

- Using command-line interface (CLI).
- Connecting to Aruba Activate server.
- Using DHCP options provided during ZTP.

DHCP servers provide the options requested by the device to connect to Central, Central On-premise manangement, or the TFTP server.

**Examples**

```bash
switch(config-aruba-central)# enable
switch(config-aruba-central)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-aruba-central</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**location-override**

Applies only to the 4100i switch.

```bash
location-override <location> [vrf <VRF default>]
no location-override
```

**Description**

When `location` and `vrf` are configured, the switch overrides existing connections to Aruba Central. The switch attempts to establish connection to Aruba Central with the specified location and VRF with highest priority.

The `no` form of this command removes location override values from the Aruba Central configuration context.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<location>` | Specifies one of these values:  
- `<FQDN>`: a fully qualified domain name.  
- `<IPV4>`: an IPv4 address.  
- `<IPV6>`: an IPv6 address. |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.</td>
</tr>
</tbody>
</table>

### Examples

Configuring location override with location and VRF:

```bash
switch(config-aruba-central)# location-override aruba-central.com vrf default
switch(config-aruba-central)#
```

Configuring location override with location only:

```bash
switch(config-aruba-central)# location-override aruba-central.com
switch(config-aruba-central)#
```

Removing location override values from the Aruba Central configuration context:

```bash
switch(config-aruba-central)# no location-override
switch(config-aruba-central)#
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-aruba-central</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### show aruba-central

- Applies only to the 4100i switch.

  ```bash
  show aruba-central
  ```

### Description

Shows information about Aruba Central connection and the status of the Activate server connection.

### Examples

Example of a switch that has the Aruba Central connection:
switch# show aruba-central
Central admin state : enabled
Central location : N/A
VRF for connection : N/A
Central connection status : N/A
Central source : dhcp
Central source connection status : connection_failure
Central source last connected on : N/A
System time synchronized from Activate : True
Activate server URL : 172.17.0.1
CLI location : N/A
CLI VRF : N/A
Source IP : N/A
Source IP Overridden : false
Central support mode : disabled

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt;) or Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show running-config current-context**

Applies only to the 4100i switch.

**Description**

Shows the running configuration for the current-context. If user is in the context of Aruba-Central(config-aruba-central), then Aruba Central running configuration is displayed.

**Examples**

Shows the running configuration of Aruba Central:

```
switch(config-aruba-central)# show running-config current-context
aruba-central
disable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>
# Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
Port filtering is a feature in which packets that are ingressed through a source port can be blocked for egressing on a specific set of ports.

**Figure 1  Port Filter Application**

Configuring a port filter to drop traffic received on port 1/1/1 with an outbound destination of port 1/1/2 means that End Nodes A, B, and C cannot send traffic to the server. To block traffic in the opposite direction, you would also configure a port filter to drop traffic received on port 1/1/2 with an outbound destination of port 1/1/1.

---

**Port filtering commands**

**portfilter**

```
portfilter <INTERFACE-LIST>
no portfilter [<INTERFACE-LIST>]
```

**Description**

Configures the specified ports so they do not egress any packets that were received on the source port specified in interface context.

The **no** form of this command removes the port filter setting from one or more ingress ports/LAGs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INTERFACE-LIST&gt;</code></td>
<td>Specifies a list of ports/LAGs to be blocked for egressing. Specify a single interface or LAG, or a range as a comma-separated list, or both. For example: 1/1/1, 1/1/3-1/1/6, lag2, lag1-lag4.</td>
</tr>
</tbody>
</table>

**Usage**

When a port filter configuration is applied on the same ingress physical port/LAG, the configuration is updated with the new sets of egress ports/LAGs that are to be blocked for egressing and that are not a part of its previous configuration. Duplicate updates on an existing port filter configuration are ignored.
When egress ports/LAGs are removed from the existing port filter configuration of an ingress port/LAG, egressing is allowed again on those egress ports/LAGs for all packets originating from the ingress port/LAG. The `no portfilter [<IF-NAME-LIST>]` command removes port filter configurations from the egress ports/LAGs listed in the `<IF-NAME-LIST>` parameter only. All other egress ports/LAGs in the port filter configuration of the ingress port/LAG remain intact.

If no physical ports or LAGs are provided for the `no portfilter` command, the command removes the entire port filter configuration for the ingress port/LAG.

**Examples**

Creating a filter that prevents packets received on port `1/1/1` from forwarding to ports `1/1/3-1/1/6` and to LAGs `1` through `4`:

```
switch(config)# interface 1/1/1
switch(config-if)# portfilter 1/1/3-1/1/6,lag1-lag4
```

Creating a filter that prevents packets received on LAG `1` from forwarding to ports `1/1/6` and LAGs `2` and `4`:

```
switch(config)# interface lag 1
switch(config-lag-if)# portfilter 1/1/6,lag2,lag4
```

Removing filters from an existing configuration that allows back packets received on port `1/1/1` to forward to ports `1/1/6` and LAGs `3` and `4`:

```
switch(config)# interface 1/1/1
switch(config-if)# no portfilter 1/1/6,lag3,lag4
```

Removing all filters from an existing configuration that allows back packets received on LAG `1` to forward to all the ports and LAGs:

```
switch(config)# interface lag 1
switch(config-lag-if)# no portfilter
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-lag-if</td>
<td></td>
</tr>
</tbody>
</table>

**show portfilter**

```
show portfilter [<IFNAME>]
```

**Description**
Displays filter settings for all interfaces or a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IFNAME&gt;</td>
<td>Specifies the ingress interface name. Specifies one of these values:</td>
</tr>
<tr>
<td></td>
<td>- &lt;FQDN&gt;: a fully qualified domain name.</td>
</tr>
<tr>
<td></td>
<td>- &lt;IPV4&gt;: an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>- &lt;IPV6&gt;: an IPv6 address.</td>
</tr>
</tbody>
</table>

**Examples**

Displaying all port filter settings on the switch:

```
switch# show portfilter
Incoming  Blocked
Interface  Outgoing Interfaces
-----------------------------------------------
1/1/1      1/1/3-1/1/6,lag1-lag2
1/1/3      1/1/1,1/1/5,1/1/7,1/1/9,1/1/11,1/1/13,1/1/15,1/1/17,1/1/19,1/1/21,
           1/1/23,1/1/25,1/1/27,1/1/29,1/1/31,1/1/33,1/1/35
lag2       1/1/1,1/1/3-1/1/6
```

Displaying the port filter settings for port **1/1/1**:

```
switch# show portfilter 1/1/1
Incoming  Blocked
Interface  Outgoing Interfaces
-----------------------------------------------
1/1/1      1/1/3-1/1/6,lag1-lag2
```

Displaying the port filter settings for **LAG2**:

```
switch# show portfilter lag2
Incoming  Blocked
Interface  Outgoing Interfaces
-----------------------------------------------
lag2      1/1/1,1/1/3-1/1/6
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; only.</td>
</tr>
</tbody>
</table>
The Domain Name System (DNS) is the Internet protocol for mapping a hostname to its IP address. DNS allows users to enter more readily memorable and intuitive hostnames, rather than IP addresses, to identify devices connected to a network. It also allows a host to keep the same hostname even if it changes its IP address.

Hostname resolution can be either static or dynamic.

- In static resolution, a local table is defined on the switch that associates hostnames with their IP addresses. Static tables can be used to speed up the resolution of frequently queried hosts.
- Dynamic resolution requires that the switch query a DNS server located elsewhere on the network. Dynamic name resolution takes more time than static name resolution, but requires far less configuration and management.

**DNS client**

The DNS client resolves hostnames to IP addresses for protocols that are running on the switch. When the DNS client receives a request to resolve a hostname, it can do so in one of two ways:

- Forward the request to a DNS name server for resolution.
- Reply to the request without using a DNS name server, by resolving the name using a statically defined table of hostnames and their associated IP addresses.

**Configuring the DNS client**

**Procedure**

1. Configure one or more DNS name servers with the command `ip dns server`.
2. To resolve DNS requests by appending a domain name to the requests, either configure a single domain name with the command `ip dns domain-name`, or configure a list of up to six domain names with the command `ip dns domain-list`.
3. To use static name resolution for certain hosts, associate an IP address to a host with the command `ip dns host`.
4. Review your DNS configuration settings with the command `show ip dns`.

**Examples**

This example creates the following configuration:

- Defines the domain `switch.com` to append to all requests.
- Defines a DNS server with IPv4 address of `1.1.1.1`.
- Defines a static DNS host named `myhost1` with an IPv4 address of `3.3.3.3`.
- DNS client traffic is sent on the default VRF (named `default`).
switch(config)# ip dns domain-name switch.com
switch(config)# ip dns server-address 1.1.1.1
switch(config)# ip dns host myhost1 3.3.3.3
switch(config)# exit
switch# show ip dns

VRF Name: default
Domain Name: switch.com
Name Server(s): 1.1.1.1

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>myhost1</td>
<td>3.3.3.3</td>
</tr>
</tbody>
</table>

switch#

### DNS client commands

**ip dns domain-list**

```
ip dns domain-list <DOMAIN-NAME> [vrf default]
no ip dns domain-list <DOMAIN-NAME> [vrf default]
```

**Description**

Configures one or more domain names that are appended to the DNS request. The DNS client appends each name in succession until the DNS server replies. Domains can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF.

The **no** form of this command removes a domain from the list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list &lt;DOMAIN-NAME&gt;</td>
<td>Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.</td>
</tr>
</tbody>
</table>

**Examples**

This example defines a list with two entries: **domain1.com** and **domain2.com**.

```
switch(config)# ip dns domain-list domain1.com
switch(config)# ip dns domain-list domain2.com
```

This example removes the entry **domain1.com**.

```
switch(config)# no ip dns domain-list domain1.com
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
ip dns domain-name

ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]
no ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]

Description

Configures a domain name that is appended to the DNS request. The domain can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF. If a domain list is defined with the command *ip dns domain-list*, the domain name defined with this command is ignored.

The no form of this command removes the domain name.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DOMAIN-NAME&gt;</td>
<td>Specifies the domain name to append to DNS requests. Length: 1 to 256 characters.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>

Examples

Setting the default domain name to domain.com:

```
switch(config)# ip dns domain-name domain.com
```

Removing the default domain name domain.com:

```
switch(config)# no ip dns domain-name domain.com
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ip dns host

ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]
no ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]

Description
Associates a static IP address with a hostname. The DNS client returns this IP address instead of querying a DNS server for an IP address for the hostname. Up to six hosts can be defined. If no VRF is defined, the default VRF is used.

The `no` form of this command removes a static IP address associated with a hostname.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host <code>&lt;HOST-NAME&gt;</code></td>
<td>Specifies the name of a host. Length: 1 to 256 characters.</td>
</tr>
</tbody>
</table>
| `<IP-ADDR>`     | Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx:: xxxx
Configures the DNS name servers that the DNS client queries to resolve DNS queries. Up to six name servers can be defined. The DNS client queries the servers in the order that they are defined. If no VRF is defined, the default VRF is used.

The `no` form of this command removes a name server from the list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP-ADDR&gt;</code></td>
<td>Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>

**Examples**

This example defines a name server at `1.1.1.1`.

```
switch(config)# ip dns server-address 1.1.1.1
```

This example defines a name server at `a::1`.

```
switch(config)# ip dns server-address a::1
```

This example removes a name server at `a::1`.

```
switch(config)# no ip dns server-address a::1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ip dns**

```
show ip dns [vrf `<VRF-NAME>`]
```

**Description**

Shows all DNS client configuration settings or the settings for a specific VRF.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.</td>
</tr>
</tbody>
</table>

**Examples**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
</table>
The switch supports automatic discovery and configuration of other devices on the network.

**Device profiles**

Device profiles rely on role configurations. For information on role configurations, see the Security Guide.

Device profiles are used to dynamically assign port attributes based on the type of devices connected, without having to create a RADIUS infrastructure. You can map device profiles to device groups. A device group contains various match criteria, which can be obtained from multiple sources, such as LLDP, CDP, and local MAC match. Device profiles contain port attributes to be assigned to the port when a connected device matches a device group.

Device profiles are supported on different scenarios. It can be applied on interfaces that are configured with security (802.1X or MAC authentication), or applied based on L2 port (LLDP, CDP), or applied on standalone ports with the block-untill-profile-applied command enabled. All the methods are mutually exclusive of each other. The block-untill-profile-applied mode must be configured only when there is a standalone port where no security has been configured and when you want the port to be offline until at least one client is onboarded based on the match and ignore criteria that you configure. Local MAC match is supported when you configure block-untill-profile-applied command or device profile with security.

Up to eight device profiles can be configured.

See the Security Guide for the following commands:

- The `port-access onboarding-method precedence` command—If you are configuring both security and device profile on the port, and you want to configure the order in which the methods will be executed.
- The `port-access fallback-role` command—If you want to configure a role that must be applied to devices when no other role exists or can be derived for that device.

If you configure a match criteria that matches across multiple device profiles, then the priority considered is LLDP, CDP, and then local MAC match. That is, LLDP precedes over CDP, which in turn precedes over local MAC match.

The following figure displays a simple configuration of device profile and AAA authentication with RADIUS server and Aruba ClearPass Policy Manager. Local MAC match feature is useful when you do not want to afford RADIUS infrastructure or when you want to use local authentication as a backup method in case the RADIUS server is unreachable.
Configuring a device profile for LLDP

Procedure

1. Create an LLDP group with the command `port-access lldp-group`.
2. Define rules for adding devices to an LLDP group with the command `match`.
3. Define rules for ignoring devices so that they are not added to an LLDP group with the command `ignore`.
4. Create a device profile with the command `port-access device-profile`.
5. Add the LLDP group with the command `associate lldp-group`.
6. Add a role to a device profile with the command `associate role`. Make sure that the role is already created. For information on how to create a role, see port access role information in the Security Guide.
7. Enable the device profile with the command `enable`.

Configuring a device profile for CDP

Procedure

1. Create a CDP group with the command `port-access cdp-group`.
2. Define rules for adding devices to a CDP group with the command `match`.
3. Define rules for ignoring devices so that they are not added to a CDP group with the command `ignore`.
4. Create a device profile with the command `port-access device-profile`.
5. Add a CDP group to a device profile with the command `associate cdp-group`.
6. Add a role to a device profile with the command `associate role`. Make sure that the role is already created. For information on how to create a role, see port access role information in the Security Guide.
7. Enable a device profile with the command `enable`.

Configuring a device profile for local MAC match

Procedure
1. Create a MAC group with the `mac-group` command.
2. Define rules for adding devices to a MAC group with the `match` (for MAC groups) command.
3. Define rules for ignoring devices so that they are not added to a MAC group with the `ignore` (for MAC groups) command.
4. Create a device profile with the `port-access device-profile` command.
5. Associate a MAC group with a device profile with the `associate mac-group` command.
6. Add a role to a device profile with the `associate role` command. Make sure that the role is already created. For information on how to create a role, see port access role information in the Security Guide.
7. Enable a device profile with the `enable` command.

**Device profile commands**

**aaa authentication port-access allow-cdp-bpdu**

```
aaa authentication port-access allow-cdp-bpdu
no aaa authentication port-access allow-cdp-bpdu
```

**Description**

Allows all packets related to the CDP (Cisco Discovery Protocol) BPDU (Bridge Protocol Data Unit) on a secure port.

The `no` form of this command blocks the CDP BPDU on a secure port. On a nonsecure port, the command has no effect.

**Examples**

Allowing a CDP BPDU on secure port 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-cdp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!
vlan 1
aaa authentication port-access mac-auth
    enable
aaa authentication port-access dot1x authenticator
    enable
interface 1/1/1
    no shutdown
    vlan access 1
aaa authentication port-access allow-cdp-bpdu
aaa authentication port-access mac-auth
    enable
aaa authentication port-access dot1x authenticator
    enable

switch(config-if)# do show port-access device-profile interface all
Port 1/1/1, Neighbor-Mac 00:0c:29:9e:d1:20
    Profile Name : access_switches
    LLDP Group :  
    CDP Group : aruba-ap_cdp
```
Role: test_ap_role
Status: In Progress
Failure Reason: Blocking LLDP packet on secure port 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access allow-cdp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!vlan 1
aaa authentication port-access mac-auth
  enable
interface 1/1/1
  no shutdown
  vlan access 1
  aaa authentication port-access mac-auth
  enable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

`aaa authentication port-access allow-lldp-bpdu`

`aaa authentication port-access allow-lldp-bpdu`

`no aaa authentication port-access allow-lldp-bpdu`

Description

Allows all packets related to the LLDP BPDU (Bridge Protocol Data Unit) on a secure port.

The `no` form of this command blocks the LLDP BPDU on a secure port. On a nonsecure port, the command has no effect.

Examples

Allowing an LLDP BPDU on secure port 1/1/1:
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
! vlan 1
aaa authentication port-access mac-auth
   enable
interface 1/1/1
   no shutdown
   vlan access 1
   aaa authentication port-access allow-lldp-bpdu
   aaa authentication port-access mac-auth
   enable

switch(config-if)# do show port-access device-profile interface all
Port 1/1/1, Neighbor-Mac 00:0c:29:9e:d1:20
   Profile Name : access_switches
   LLDP Group   : 2920-grp
   CDP Group    :
   Role         : local_2920_role
   Status       : Profile Applied
   Failure Reason :

Blocking LLDP BPDU on secure port 1/1/1:

switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access allow-lldp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000led locator on
!
! vlan 1
aaa authentication port-access mac-auth
   enable
interface 1/1/1
   no shutdown
   vlan access 1
   aaa authentication port-access mac-auth
   enable

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
### associate cdp-group

associate cdp-group <GROUP-NAME>
no associate cdp-group <GROUP-NAME>

**Description**

Associates a CDP (Cisco Discovery Protocol) group with a device profile. A maximum of two CDP groups can be associated with a device profile.

The `no` form of this command removes a CDP group from a device profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;GROUP-NAME&gt;</code></td>
<td>Specifies the name of the CDP group to associate with this device profile. Range: 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Examples**

Associating the CDP group `my-cdp-group` with the device profile `profile01`:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate cdp-group my-cdp-group
```

Removing the CDP group `my-cdp-group` from the device profile `profile01`:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate cdp-group my-cdp-group
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i 6000 6100</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Associates an LLDP group with a device profile. A maximum of two LLDP groups can be associated with a device profile.

The no form of this command removes an LLDP group from a device profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;GROUP-NAME&gt;</code></td>
<td>Specifies the name of the LLDP group to associate with the device profile. Range: 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Examples**

**Associating the LLDP group my-lldp-group with the device profile profile01:**

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate lldp-group my-lldp-group
```

**Removing the LLDP group my-lldp-group from the device profile profile01:**

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate lldp-group my-lldp-group
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**associate mac-group**

```
associate mac-group <GROUP-NAME>
no associate mac-group <GROUP-NAME>
```

**Description**

Associates a MAC group with a device profile. A maximum of two MAC groups can be associated with a device profile.

The no form of this command removes a MAC group from a device profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;GROUP-NAME&gt;</code></td>
<td>Specifies the name of the MAC group to associate with this device profile. Range: 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Examples**
Associating the MAC group **mac01-group** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate mac-group mac01-group
```

Removing the MAC group **mac01-group** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate mac-group mac01-group
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**associate role**

`associate role <ROLE-NAME>`  
`no associate role <ROLE-NAME>`

**Description**

Associates a role with a device profile. Only one role can be associated with a device profile. For information on how to configure a role, see the port access role information in the Security Guide.

The `no` form of this command removes a role from a device profile.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ROLE-NAME&gt;</code></td>
<td>Specifies the name of the role to associate with the device profile. Range: 1 to 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Examples**

Associating the role **my-role** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate role my-role
```

Removing the role **my-role** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate role my-role
```
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**disable (port-access device-profile)**

disable
no disable

**Description**

Disables a device profile.
The no form of this command enables a device profile.

**Examples**

Disabling a device profile:

```bash
switch(config)# port-access device-profile profile01
switch(config-device-profile)# disable
```

Enabling a device profile named profile01:

```bash
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no disable
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**enable**

enable
no enable
Description
Enables a device profile.
The no form of this command disables a device profile.

Examples
Enabling a device profile:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# enable
```

Disabling a device profile named profile01:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no enable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-device-profile</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ignore (for CDP groups)

```
ignore [seq <SEQ-NUM>] {platform <PLATFORM> | sw-version <SWVERSION> | voice-vlan-query <VLAN-ID>}
no ignore [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> | voice-vlan-query <VLAN-ID>}
```

Description
Defines a rule to ignore devices for a CDP (Cisco Discovery Protocol) group. Up to 64 match/ignore rules can be defined for a group.
The no form of this command removes a rule for ignoring devices from a CDP group.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.</td>
</tr>
<tr>
<td>platform &lt;PLATFORM&gt;</td>
<td>Specifies the hardware or model details of the neighbor. Range: 1 to 128 alphanumeric characters.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sw-version &lt;SWVERSION&gt;</td>
<td>Specifies the software version of the neighbor. Range: 1 to 128 alphanumeric characters.</td>
</tr>
<tr>
<td>voice-vlan-query &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN query value of the neighbor. Range: 1 to 65535.</td>
</tr>
</tbody>
</table>

**Examples**

Adding a rule to the CDP group `grp01` that ignores a device that transmits `PLATFORM01` in the platform TLV:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# ignore platform PLATFORM01
```

Adding a rule to the CDP group `grp01` that ignores a device that transmits `SWVERSION` in software version TLV:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# ignore sw-version SWVERSION
```

Removing the rule that matches the sequence number 25 from the CDP group named `grp01`.

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# no ignore seq 25
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-cdp-group</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ignore (for LLDP groups)**

```
ignore [seq <SEQ-ID>] [sys-desc <SYS-DESC>] [sysname <SYS-NAME>] [vendor-oui <VENDOR-OUI>] [type <KEY>] [value <VALUE>]]
no ignore [seq <SEQ-ID>] [sys-desc <SYS-DESC>] [sysname <SYS-NAME>] [vendor-oui <VENDOR-OUI>] [type <KEY>] [value <VALUE>]]
```

**Description**

Defines a rule to ignore devices for an LLDP group. Up to 64 match/ignore rules can be defined for a group. The `no` form of this command removes a rule for ignoring devices from an LLDP group.
## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.</td>
</tr>
<tr>
<td>sys-desc &lt;SYS-DESC&gt;</td>
<td>Specifies the LLDP system description type-length-value (TLV). Range: 1 to 256 alphanumeric characters.</td>
</tr>
<tr>
<td>sysname &lt;SYS-NAME&gt;</td>
<td>Specifies the LLDP system name TLV. Range: 1 to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>vendor-oui &lt;VENDOR-OUI&gt;</td>
<td>Specifies the LLDP system vendor OUI TLV. Range: 1 to 6 alphanumeric characters.</td>
</tr>
<tr>
<td>type &lt;KEY&gt;</td>
<td>Specifies the vendor OUI subtype key. Optional.</td>
</tr>
<tr>
<td>value &lt;VALUE&gt;</td>
<td>Specifies the vendor OUI subtype value. Range: 1 to 256 alphanumeric characters.</td>
</tr>
</tbody>
</table>

### Examples

Adding a rule to the LLDP group `grp01` that ignores a device that transmits `PLATFORM01` in the system description TLV:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# ignore sys-desc PLATFORM01
```

Removing the rule that matches the sequence number **25** from the LLDP group named `grp01`.

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# no match seq 25
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-lldp-group</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ignore (for MAC groups)**

```
[seq <SEQ-ID>] ignore {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}
no [seq <SEQ-ID>] ignore {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}
```

### Description
Defines a rule to ignore devices for a MAC group based on the criteria of MAC address, MAC address mask, or MAC Organizational Unique Identifier (OUI). Up to 64 ignore rules can be defined for a group. The no form of this command removes a rule for ignoring devices from a MAC group.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the entry sequence ID of the rule to create or modify a MAC group. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence. Range: 1 to 4294967295.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Specifies the MAC address of the device to ignore.</td>
</tr>
<tr>
<td>mac-mask &lt;MAC-MASK&gt;</td>
<td>Specifies the MAC address mask to ignore devices in that range. Supported MAC address masks: /32 and /40.</td>
</tr>
<tr>
<td>mac-oui &lt;MAC-OUI&gt;</td>
<td>Specifies the MAC OUI to ignore devices in that range. Supports MAC OUI address of maximum length of 24 bits.</td>
</tr>
</tbody>
</table>

**Usage**

To achieve the required configuration of matches for devices, it is recommended to first ignore the devices that you do not want to add. Then match the criteria for the rest of the devices that you want to add to the MAC group.

For example, if you want to ignore a specific device but add all the other devices that belong to a MAC OUI, then you must first configure the ignore criteria with a lower sequence number. And then configure match criteria with a higher sequence number.

**Examples**

Adding a rule to the MAC group **grp01** to ignore a device based on MAC address, but match all other devices belonging to a MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac 1a:2b:3c:4d:5e:6f
switch(config-mac-group)# match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
ssh server vrf
!
!
!
vlan 1
interface vlan 1
```
Adding a rule to the MAC group **grp01** to ignore devices based on MAC address mask, but match all other devices belonging to a MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac-mask 1a:2b:3c:4d:5e:6f
```

Adding a rule to the MAC group **grp01** that ignores a device based on complete MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac 1a:2b:3c:4d:5e:6f
```

Adding a rule to the MAC group **grp02** that ignores devices based on MAC mask:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac-mask 1a:2b:3c:4d:5e/40
```

Adding a rule to the MAC group **grp03** that ignores devices based on MAC OUI:
Adding a rule to the MAC group `grp01` that ignores devices with a sequence number and based on MAC address:

```bash
switch(config)# mac-group grp03
switch(config-mac-group)# ignore mac-oui 81:cd:93
```

Removing the rule from the MAC group `grp01` based on sequence number:

```bash
switch(config)# mac-group grp01
switch(config-mac-group)# no ignore seq 10
switch(config-mac-group)# exit
```

Adding a rule to the MAC group `grp01` that ignores devices with MAC entry sequence number and based on MAC OUI:

```bash
switch(config)# mac-group grp01
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 ignore mac b2:c3:44:12:78:11
switch(config-mac-group)# exit
```

```
Adding a rule to the MAC group `grp01` that ignores devices with a sequence number and based on MAC address:

```bash
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac-oui 81:cd:93
```

Removing the rule from the MAC group `grp01` based on sequence number:

```bash
switch(config)# mac-group grp01
switch(config-mac-group)# no ignore seq 10
switch(config-mac-group)# exit
```

Adding a rule to the MAC group `grp01` that ignores devices with MAC entry sequence number and based on MAC OUI:

```bash
switch(config)# mac-group grp01
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 ignore mac b2:c3:44:12:78:11
switch(config-mac-group)# exit
```
switch(config)# ^Z

switch#
switch#
switch# show running-config
Current configuration:
!
!Version AOS-CX PL.10.06.0002
!export-password: default
!
!
ssh server vrf default
vlan 1
spanning-tree
mac-group grp01
    seq 10 ignore mac b2:c3:44:12:78:11
    seq 20 ignore mac-oui 1a:2b:3c
    seq 30 ignore mac-mask 71:14:89:42/32
interface 1/1/1
    no shutdown
    vlan access 1
interface 1/1/2
    no shutdown
    vlan access 1
interface 1/1/3
    no shutdown
    vlan access 1
interface 1/1/4
    no shutdown
    vlan access 1
interface 1/1/5
    no shutdown
    vlan access 1
interface 1/1/6
    no shutdown
    vlan access 1
interface 1/1/7
    no shutdown
    vlan access 1
interface 1/1/8
    no shutdown
    vlan access 1
interface 1/1/9
    no shutdown
    vlan access 1
interface 1/1/10
    no shutdown
    vlan access 1
interface 1/1/11
    no shutdown
    vlan access 1
interface 1/1/12
    no shutdown
    vlan access 1
interface 1/1/13
    no shutdown
    vlan access 1
interface 1/1/14
    no shutdown
    vlan access 1
interface 1/1/15
  no shutdown
  vlan access 1
interface 1/1/16
  no shutdown
  vlan access 1
interface vlan 1
  ip dhcp
  
Removing the rule from the MAC group **grp01** based on sequence number and MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no seq 20 ignore mac-oui ia:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
```

```
Current configuration:
  
  !
  !
  !
  vlan 1
  interface vlan 1
    no shutdown
    ip dhcp
    mac-group grp01
      seq 10 ignore mac b2:c3:44:12:78:11
      seq 30 ignore mac-mask 71:14:89:f3/32

```

Removing the rule that matches the sequence number **25** from the MAC group named **grp01**.

```
switch(config)# mac-group grp01
switch(config-mac-group)# no ignore seq 25
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
mac-group

mac-group <MAC-GROUP-NAME>
no mac-group <MAC-GROUP-NAME>

Description

Creates a MAC group or modifies an existing MAC group. A MAC group is used to classify connected devices based on the MAC address details, such as mask or OUI.

A maximum of 32 MAC groups can be configured on the switch. A maximum of 2 MAC groups can be associated with a device profile. Each group accepts 64 match or ignore commands.

The no form of this command removes a MAC group.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC-GROUP-NAME&gt;</td>
<td>Specifies the name of the MAC group to create or modify. The maximum number of characters supported is 32.</td>
</tr>
</tbody>
</table>

Examples

Creating a MAC group named grp01:

```
switch(config)# mac-group grp01
switch(config-mac-group)# exit
```

Removing a MAC group named grp01:

```
switch(config)# no mac-group grp01
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

match (for CDP groups)

match [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> | voice-vlan-query <VLAN-ID>}

Device discovery and configuration | 176
no match [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> | voice-vlan-query <VLAN-ID>}

**Description**

Defines a rule to match devices for a CDP group. A maximum of 32 CDP groups can be configured on the switch. Up to 64 match or ignore rules can be defined for each group.

The `no` form of this command removes a rule for adding devices to a CDP group.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.</td>
</tr>
<tr>
<td>platform &lt;PLATFORM&gt;</td>
<td>Specifies the hardware or model details of the neighbor. Range: 1 to 128 alphanumeric characters.</td>
</tr>
<tr>
<td>sw-version &lt;SWVERSION&gt;</td>
<td>Specifies the software version of the neighbor. Range: 1 to 128 alphanumeric characters.</td>
</tr>
<tr>
<td>voice-vlan-query &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN query value of the neighbor. Range: 1 to 65535.</td>
</tr>
</tbody>
</table>

**Examples**

**Adding rules to match a Cisco device with a specific software version on VLAN 512 to the CDP group **grp01**: 

```bash
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match platform CISCO
switch(config-cdp-group)# match sw-version 11.2(12)P
switch(config-cdp-group)# match voice-vlan-query 512
switch(config-cdp-group)# match seq 50 platform cisco sw-version 11.2(12)P voice-vlan-query 512
switch(config-cdp-group)# exit
switch(config)# do show running-config
```

Current configuration:

```
!
!Version AOS-CX Virtual.10.0X.000
!export-password: default
led locator on
!

vlan 1
port-access cdp-group grp01
  seq 10 match platform CISCO
  seq 20 match sw-version 11.2(12)P
  seq 30 match voice-vlan-query 512
  seq 50 match platform cisco sw-version 11.2(12)P voice-vlan-query 512
```

**Removing a rule that matches the sequence number 25 from the CDP group named **grp01**: 

```bash
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# no match seq 25
```

**Adding a rule that matches the value of vendor-OUI 000b86 to the CDP group named **grp01**: 

```bash
```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match vendor-oui 000b86

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-cdp-group</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

match (for LLDP groups)

match [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> | vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}
no match [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> | vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}

Description

Defines a rule to match devices for an LLDP group. Up to 64 match/ignore rules can be defined for a group. The no form of this command removes a rule.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.</td>
</tr>
<tr>
<td>sys-desc &lt;SYS-DESC&gt;</td>
<td>Specifies the LLDP system description type-length-value (TLV). Range: 1 to 256 alphanumeric characters.</td>
</tr>
<tr>
<td>sysname &lt;SYS-NAME&gt;</td>
<td>Specifies the LLDP system name TLV. Range: 1 to 64 alphanumeric characters.</td>
</tr>
<tr>
<td>vendor-oui &lt;VENDOR-OUI&gt;</td>
<td>Specifies the LLDP system vendor OUI TLV. Range: 1 to 6 alphanumeric characters.</td>
</tr>
<tr>
<td>type &lt;KEY&gt;</td>
<td>Specifies the vendor OUI subtype key.</td>
</tr>
<tr>
<td>value &lt;VALUE&gt;</td>
<td>Specifies the vendor OUI subtype value. Range: 1 to 256 alphanumeric characters.</td>
</tr>
</tbody>
</table>

Examples

Adding rules that match the LLDP system description ArubaSwitch and system name Aruba to the LLDP group named grp01:
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match sys-desc ArubaSwitch
switch(config-lldp-group)# match sysname Aruba
switch(config)# do show running-config

Current configuration:
!
!Version AOS-CX Virtual.10.0X.000
!export-password: default
led locator on
!
!vlan 1
port-access lldp-group grp01
  seq 10 match sys-desc ArubaSwitch
  seq 20 match sysname Aruba

Removing a rule that matches the sequence number 25 from an LLDP group named grp01:

switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# no match seq 25

Adding a rule that matches the value of vendor-OUI 000b86 with type of 1 to the LLDP group named grp01:

switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match vendor-oui 000b86 type 1

Adding a rule that matches the value of vendor-OUI 000c34 to the LLDP group named grp01:

switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match vendor-oui 000c34

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-lldp-group</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

match (for MAC groups)

[seq <SEQ-ID>] match {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}
no [seq <SEQ-ID>] match {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}

Description
Defines a rule to match devices for a MAC group based on the criteria of MAC address, MAC address mask, or MAC Organizational Unique Identifier (OUI). Up to 64 match rules can be defined for a group.

You must not configure the following special MAC addresses:

- Null MAC—For example, 00:00:00:00:00:00 or 00:00:00:00:00/32
- Multicast MAC
- Broadcast MAC—For example, ff:ff:ff:ff:ff:ff
- System MAC

Although the switch accepts these addresses, it will not process these addresses for the local MAC match feature.

The no form of this command removes a rule for adding devices to a MAC group. The number of clients that can onboard based on the match criteria is configured in the `aaa authentication port-access client-limit` command. For information about this command, see the Security Guide for your switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq &lt;SEQ-ID&gt;</td>
<td>Specifies the entry sequence ID of the rule to create or modify a MAC group. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence. Range: 1 to 4294967295.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Specifies the MAC address of the device.</td>
</tr>
<tr>
<td>mac-mask &lt;MAC-MASK&gt;</td>
<td>Specifies the MAC address mask to add devices in that range. Supported MAC address masks: /32 and /40.</td>
</tr>
<tr>
<td>macoui &lt;MAC-OUI&gt;</td>
<td>Specifies the MAC OUI to add devices in that range. Supports MAC OUI address of maximum length of 24 bits.</td>
</tr>
</tbody>
</table>

**Examples**

Adding a device to the MAC group **grp01** based on complete MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# match mac 1a:2b:3c:4d:5e:6f
switch(config-mac-group)# exit
```

Adding devices to the MAC group **grp02** based on MAC mask:

```
switch(config)# mac-group grp01
switch(config-mac-group)# match mac-mask 1a:2b:3c:4d:5e/40
switch(config-mac-group)# match mac-mask 18:e3:ab:73/32
switch(config-mac-group)# exit
```

Adding devices to the MAC group **grp03** based on MAC OUI:
Adding devices to the MAC group **grp01** with MAC entry sequence number and based on MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 match mac b2:c3:44:12:78:11
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 match mac b2:c3:44:12:78:11
```

Removing devices from the MAC group **grp01** based on sequence number:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no match seq 10
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
```

Adding devices to the MAC group **grp01** with MAC entry sequence number and based on MAC address, MAC address mask, and MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 match mac b2:c3:44:12:78:11
switch(config-mac-group)# seq 20 match mac-oui 1a:2b:3c
switch(config-mac-group)# seq 30 match mac-mask 71:14:89:f3/32
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
```
Removing devices from the MAC group **grp01** based on MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no seq 20 match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
```

Adding devices to the MAC group **grp03** with MAC entry sequence number and based on MAC address mask:

```
switch(config)# mac-group grp03
switch(config-mac-group)#  seq 10 match mac-mask 10:14:a3:b7:55/40
switch(config-mac-group)#  exit
switch(config)# do show running-config
```
Removing devices from the MAC group **grp03** based on MAC address mask:

```plaintext
switch(config)# mac-group grp03
switch(config-mac-group)# no seq 10 match mac-mask 10:14:a3:b7:55/40
switch(config-mac-group)# exit
switch(config)# do show running-config
```

Current configuration:
```
! Version AOS-CX Virtual.10.0X.0001
! export-password: default
led locator on
!
! vlan 1
interface vlan1
   no shutdown
   ip dhcp
mac-group grp03
...```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-mac-group</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**port-access cdp-group**

```
port-access cdp-group <CDP-GROUP-NAME>
no port-access cdp-group <CDP-GROUP-NAME>
```

**Description**

Creates a CDP (Cisco Discovery Protocol) group or modifies an existing CDP group. A CDP Group is used to classify connected devices based on the CDP packet details advertised by the device. A maximum of 32 CDP groups can be configured on the switch. Each group accepts 64 match/ignore commands. The **no** form of this command removes a CDP group.
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;CDP-GROUP-NAME&gt;</code></td>
<td>Specifies the name of the CDP group to create or modify. The maximum number of characters supported is 32. Required.</td>
</tr>
</tbody>
</table>

### Examples

Creating a CDP group named grp01:

```bash
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match platform CISCO
switch(config-cdp-group)# match sw-version 11.2(12)P
switch(config-cdp-group)# match voice-vlan-query 512
switch(config-cdp-group)# seq 50 match platform cisco sw-version 11.2(12)P voice-vlan-query 512
switch(config-cdp-group)# exit
switch(config)# do show running-config
```

Current configuration:

```bash
! Version AOS-CX Virtual.10.0X.000
! export-password: default
! led locator on
! vlan 1
port-access cdp-group grp01
  seq 10 match platform CISCO
  seq 20 match sw-version 11.2(12)P
  seq 30 match voice-vlan-query 512
  seq 50 match platform cisco sw-version 11.2(12)P voice-vlan-query 512
```

Removing a CDP group named grp01:

```bash
switch(config)# no port-access cdp-group grp01
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**port-access device-profile**

- `port-access device-profile <DEVICE-PROFILE-NAME>`
- `no port-access device-profile <DEVICE-PROFILE-NAME>`

**Description**
Creates a new device profile and switches to the `config-device-profile` context. A maximum of 32 device profiles can be created.

The `no` form of this command removes a device profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DEVICE-PROFILE-NAME&gt;</code></td>
<td>Specifies the name of a device profile. Range: 1 to 32 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Examples**

Creating a device profile named `profile01`:

```bash
switch(config)# port-access device-profile profile01
switch(config-device-profile)#
```

Removing a device profile named `profile01`:

```bash
switch(config)# no port-access device-profile profile01
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td><code>config</code></td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**port-access device-profile mode block-until-profile-applied**

You must configure this mode in device profile only on standalone ports where there is no security configured and when you not want the port to be offline until one client is onboarded.

`port-access device-profile mode block-until-profile-applied`

`no port-access device-profile mode block-until-profile-applied`

**Description**

Configures the switch to block the port until a profile match occurs for a device. This configuration is required when no security feature is enabled on the port.

You must enable this mode or security on the port for local MAC match feature to operate. You must not enable both features on the same port at the same time.

You must not combine any other AAA configurations with the block-until-profile-applied mode.
The no form of this command removes a rule for adding devices to a MAC group.

**Example**

Configuring block-until-profile applied mode on port 1/1/1:
```
switch(config)# interface 1/1/1
switch(config-if)# port-access device-profile
switch(config-if-deviceprofile)# mode block until-profile-applied
switch(config-if-deviceprofile)# end
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td>config-if-deviceprofile</td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**port-access lldp-group**

<table>
<thead>
<tr>
<th>Command context</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-if</td>
<td>&lt;LLDP-GROUP-NAME&gt;</td>
<td>Specifies the name of the LLDP group to create or modify. The maximum number of characters supported is 32. Required.</td>
</tr>
</tbody>
</table>

**Description**

Creates an LLDP group or modifies an existing LLDP group. An LLDP group is used to classify connected devices based on the LLDP type-length-values (TLVs) advertised by the device. A maximum of 32 LLDP groups can be configured on the switch. Each group accepts 64 match/ignore commands. The no form of this command removes an LLDP group.

**Examples**

Creating an LLDP group named grp01:
```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)#
```

Removing an LLDP group named grp01:
```
switch(config)# no port-access lldp-group grp01
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show port-access device-profile

show port-access device-profile [ [interface { all | <INTERFACE-ID>} ] [ [client-status <MAC-ADDR>] ] | name <DEVICEPROFILE-NAME> ]

Description

Shows the client status for a specific MAC address or profile name.

Parameter | Description
---|---
interface { all | <INTERFACE-ID>} | Select all for all interfaces or specify the name of an interface in the format: member/slot/port.
client-status <MAC-ADDR> | Specifies a MAC address (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F.
name <DEVICEPROFILE-NAME> | Specifies the name of the device profile.

Examples

Showing the applied state of the device profiles:

```yaml
switch# show port-access device-profile

Profile Name : accesspoints
LLDP Groups  : 2920-grp
CDP Groups   :
MAC Groups   : 2920-mac-grp1,2920-iot-grp2
Role         : local_role_1
State        : Enabled

Profile Name : access_switches
LLDP Groups  : 2920-grp
CDP Groups   :
MAC Groups   :
Role         : local_2920_role
State        : Enabled

Profile Name : iot_devices
LLDP Groups  :
CDP Groups   :
MAC Groups   : iot_camera-grp1,iot_sensors-grp1
```
Showing the applied state of the device profile on interface 1/1/3:

```
switch# show port-access device-profile interface 1/1/3 client-status
00:0c:29:9e:d1:20
Port 1/1/3, Neighbor-Mac 00:0c:29:9e:d1:20
  Profile Name  : lobbyaps
  LLDP Group    :
  CDP Group     : aruba-ap_cdp
  MAC Group     :
  Role          : test_ap_role
  Status        : Failed
  Failure Reason : Failed to apply MAC based VLAN
```

Showing the applied state of a specific device profile:

```
switch# show port-access device-profile name lldp-group
Profile Name    : lldp-group
LLDP Groups     :
CDP Groups      :
MAC Groups      : pc-behind-phone, lldp
Role            : auth_role
State           : Enabled
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>4100i</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**LLDP**

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities. An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all interfaces on which outbound
LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports on which inbound LLDP is enabled. Inbound packets from neighbor devices are stored in a special LLDP MIB (management information base). This information can then be queried by other devices through SNMP.

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which interfaces they connect. LLDP operates at layer 2 and requires an LLDP agent to be active on each interface that sends and receives LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device such as: system capabilities, management IP address, device ID, port ID.

**Packet boundaries**

When multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.

An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Therefore, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.

Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

**LLDP-MED**

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to LLDP-MED operation. The show commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED enables:

- Configure Voice VLAN and advertise it to connected MED endpoint devices.
- Power over Ethernet (PoE) status and troubleshooting support via SNMP.

**LLDP agent**

When you enable LLDP on the switch, it is automatically enabled on all data plane interfaces. You can customize this behavior by manually enabling/disabling support on each interface.

**Supported standards**

The LLDP agent supports the following standards: IEEE 802.1AB-2005, Station, and Media Access Control Connectivity Discovery.

**Supported interfaces**

LLDP is supported on interfaces mapped to a physical port. It is not supported on logical interfaces, such as loopback, tunnels, and SVIs.

**Operating modes**

When LLDP is enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions and receives LLDP advertisements on each active port enabled to receive LLDP traffic.

The LLDP agent can operate in one of the following modes:
- Transmit and receive (TxRx): This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets and to store the data from received (inbound) LLDP packets in the switch’s MIB.

- Transmit only (Tx): Enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.

- Receive only (Rx): Enables a port to receive and read LLDP packets from LLDP neighbors and to store the packet data in the switch’s MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.

- Disabled: Disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

An LLDP agent operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes.

**Sending LLDP frames**

Each time the LLDP operating mode of an LLDP agent changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, an LLDP agent must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

**Receiving LLDP frames**

An LLDP agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging timer. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, all saved information ages out.

**TLV support**

By default, the agent sends and receives the following mandatory TLVs on each interface:

- Port ID
- Chassis ID
- TTL

By default, the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED) are enabled on an agent. Sending them depends on the configuration and reception of any MED TLVs:

- MAC/PHY status. Includes the bit rate and auto negotiation status of the link.
- Power Via MDI: Includes Power Over Ethernet related information for supported interfaces.
- Port description
- System name
- System description
- Management address
- System capabilities
- Port VLAN ID

By default, the agent sends and receives the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED):
- Capabilities: Indicates MED TLV capability.
- Power Via MDI: Includes Power Over Ethernet related information.
- Network Policy: Includes the VLAN configuration for voice application.
- Location: Location identification information.
- Extended Power Via MDI: Power Over Ethernet related information

**TLV advertisements**
The LLDP agent transmits the following:

- Chassis-ID: Base MAC address of the switch.
- Port-ID: Port number of the physical port.
- Time-to-Live (TTL): Length of time an LLDP neighbor retains advertised data before discarding it.
- System capabilities: Identifies the primary switch capabilities (bridge, router). Identifies the primary switch functions that are enabled, such as routing.
- System description: Includes switch model name and running software version, and ROM version.
- System name: Name assigned to the switch.
- Management address: Default address selection method unless an optional address is configured.
- Port description: Physical port identifier.
- Port VLAN ID: On an L2 port, contains access or native VLAN ID. Trunk allowed VLANs information are not advertised as part of the Port VLAN ID TLV.

**LLDP MED support**
LLDP-MED inter-operates with directly connected IP telephony (endpoint) clients and provides the following features:

- Advertisement of the voice VLAN configured on the interface which is used by connected IP telephony (endpoint) clients.
- Advertisement of the configured location on the switch that can be used by the connected endpoint.
- Support for the fast-start capability

LLDP-MED is intended for use with VoIP endpoints and is not designed to support links between network infrastructure devices (such as switch-to-switch or switch-to-router links).

**Configuring the LLDP agent**

**Procedure**

1. By default, the LLDP agent is enabled on all active interfaces. If LLDP was disabled, enable it with the command `lldp`.
2. By default, the LLDP agent transmits and receive on all interfaces. To customize LLDP behavior on a specific interface, use the commands `lldp transmit` and `lldp receive`.
3. By default, the LLDP agent sets the management address in all TLVs in the following order:
   a. LLDP management IP address.
   b. SVI.
   c. Base MAC.
4. By default, all supported TLVs are sent and received. To customize the list, use the command `lldp select-tlv`.

5. By default, support for the LLDP-MED TLV is enabled. To customize settings, use the commands `lldp med` and `lldp med-location`.

6. If required, adjust LLDP timer, holdtime, reinitialization delay, and transmit delay from their default values with the commands `lldp timer`, `lldp holdtime`, `lldp reinit`, and `lldp txdelay`.

Example
This example creates the following configuration:

- Enables LLDP support.
- Disables LLDP transmission on interface 1/1/1.

```
switch(config)# lldp
switch(config)# interface 1/1/1
switch(config-copp)# no lldp transmit
```

LLDP commands

clear lldp neighbors
clear lldp neighbors

Description
Cleans all LLDP neighbor details.

Examples
Cleansing all LLDP neighbor details:

```
switch# clear lldp neighbors
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

clear lldp statistics
clear lldp statistics

Description
Cleans all LLDP neighbor statistics.
Examples
Clearing all LLDP neighbor statistics:

```
switch# clear lldp statistics
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

lldp

lldp
no lldp

Description
Enables LLDP support globally on all active interfaces. By default, LLDP is enabled.
The no form of this command disables LLDP support globally on all active interfaces. It does not remove any LLDP configuration settings.

Examples
Enabling LLDP:

```
switch(config)# lldp
```

Disabling LLDP:

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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
### lldp dot3

```
lldp dot3 {poe | macphy}
no lldp dot3 {poe | macphy}
```

#### Description

Sets the 802.3 TLVs to be advertised. By default, advertisement of both POE and MAC/PHY TLVs is enabled. The `no` form of this command disables advertisement of 802.3 TLVs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>poe</td>
<td>Specifies advertisement of power over Ethernet data link classification.</td>
</tr>
<tr>
<td>macphy</td>
<td>Specifies advertisement of media access control and physical layer information.</td>
</tr>
</tbody>
</table>

#### Examples

Enabling advertisement of the POE TLV:

```
switch(config-if)# lldp dot3 poe
```

Disabling advertisement of the POE TLV:

```
switch(config-if)# no lldp dot3 poe
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### lldp holdtime

```
lldp holdtime <TIME>
no lldp holdtime
```

#### Description
Sets the holdtime that is used to calculate the LLDP Time-to-Live value. Time-to-Live defines the length of time that neighbors consider LLDP information sent by this agent as valid. When Time-to-Live expires, the information is deleted by the neighbor. Time-to-live is calculated by multiplying holdtime by the value of lldp timer.

The `no` form of this command sets the holdtime to its default value of 4.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Examples**

Setting the holdtime to 8 seconds:

```
switch(config)# lldp holdtime 8
```

Setting the holdtime to the default value of 4 seconds:

```
switch(config)# no lldp holdtime
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**lldp management-ipv4-address**

`lldp management-ipv4-address <IPV4-ADDR>
no lldp management-ipv4-address`

**Description**

Defines the IPv4 management address of the switch which is sent in the management address TLV. One IPv4 and one IPv6 management address can be configured.

If you do not define an LLDP management address, then LLDP uses one of the following (in order):

- IP address of SVI [interface VLAN <vid>]
- Base MAC address of the switch

The `no` form of this command removes the IPv4 management address of the switch.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV4-ADDR&gt;</code></td>
<td>Specifies the management address of the switch as an IPv4 format (x.x.x.x), where x is a decimal value from 0 to 255.</td>
</tr>
</tbody>
</table>

### Examples

Setting the management address to **10.10.10.2**:

```
switch(config)# lldp management-ipv4-address 10.10.10.2
```

Removing the management address:

```
switch(config)# no lldp management-ipv4-address
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### Description

**lldp management-ipv6-address**

```
lldp management-ipv6-address <IPV6-ADDR>
nolldp management-ipv6-address
```

Defines the IPv6 management address of the switch. The management address is encapsulated in the management address TLV.

If you do not define an LLDP management address, then LLDP uses one of the following (in order):

- IP address of SVI [interface VLAN <vid>]
- Base MAC address of the switch

The `no` form of this command removes the IPv6 management address of the switch.

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV6-ADDR&gt;</code></td>
<td>Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
</tbody>
</table>

### Examples

Setting the management address to **2001:db8:85a3::8a2e:370:7334**:
Removing the management address:

```
switch(config)# no lldp management-ipv6-address
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### lldp med

```
lldp med [poe [priority-override] | capability | network-policy]
nolldp med [poe [priority-override] | capability | network-policy]
```

### Description

Configures support for the LLDP-MED TLV. LLDP-MED (media endpoint devices) is an extension to LLDP developed by TIA to support interoperability between VoIP endpoint devices and other networking end-devices. The switch only sends the LLDP MED TLV after receiving a MED TLV from and connected endpoint device.

The `no` form of this command disables support for the LLDP MED TLV.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>poe [priority-override]</td>
<td>Specifies advertisement of power over Ethernet data link classification. The <code>priority-override</code> option overrides user-configured port priority for Power over Ethernet. When both <code>lldp dot3 poe</code> and <code>lldp med poe</code> are enabled, the <code>lldp dot3 poe</code> setting takes precedence. Default: enabled.</td>
</tr>
<tr>
<td>capability</td>
<td>Specifies advertisement of supported LLDP MED TLVs. The capability TLV is always sent with other MED TLVs, therefore it cannot be disabled when other MED TLVs are enabled. Default: enabled.</td>
</tr>
<tr>
<td>network-policy</td>
<td>Network policy discovery lets endpoints and network devices advertise their VLAN IDs, and IEEE 802.1p (PCP and DSCP) values for voice applications. This TLV is only sent when a voice VLAN policy is present. Default: enabled.</td>
</tr>
</tbody>
</table>

### Examples

Enabling advertisement of the network policy TLV:
Disabling advertisement of the network policy TLV:

```
switch(config-if)# no lldp med network-policy
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

#### lldp med-location

```
lldp med-location {civic-addr | elin-addr}
nno med-location {civic-addr | elin-addr}
```

### Description

Configures support for the LLDP-MED TLV. Supports only civic address and emergency location information number (ELIN). Coordinate-based location is not supported.

The `no` form of this command disables support for the LLDP MED TLV.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>civic-addr</td>
<td>Configures the LLDP MED civic location TLV.</td>
</tr>
<tr>
<td>elin-addr</td>
<td>Configures support for the LLDP MED emergency location TLV.</td>
</tr>
</tbody>
</table>

### Examples

Enabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# lldp med-location elin-addr gher
```

Disabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# no lldp med-location elin-addr gher
```

Enabling support for the LLDP MED civic address TLV:

```
switch(config-if)# lldp med-location civic-addr US 1 4 ret 6 tyu 7 tiyuo
```
Disabling support for the LLDP MED civic address TLV:

```
switch(config-if)# no lldp med-location civic-addr US 1 4 ret 6 tyu 7 tiyuo
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**lldp receive**

*lldp receive*

*no lldp receive*

**Description**

Enables reception of LLDP information on an interface. By default, LLDP reception is enabled on all active interfaces.

The *no* form of this command disables reception of LLDP information on an interface.

**Examples**

Enabling LLDP reception on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp receive
```

Disabling LLDP reception on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp receive
```
lldp reinit

lldp reinit <TIME>
no lldp reinit

Description
Sets the amount of time (in seconds) to wait before performing LLDP initialization on an interface. The no form of this command sets the reinitialization time to its default value of 2 seconds.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the reinitialization time in seconds. Range: 1 to 10. Default: 2 seconds.</td>
</tr>
</tbody>
</table>

Examples
Setting the reinitialization time to 5 seconds:

```
switch(config)# lldp reinit 5
```

Setting the reinitialization time to the default value of 2 seconds:

```
switch(config)# no lldp reinit
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

lldp select-tlv

lldp select-tlv <TLV-NAME>
no lldp select-tlv <TLV-NAME>

Description
Selects a TLV that the LLDP agent will send and receive. By default, all supported TLVs are sent and received. The no form of this command stops the LLDP agent from sending and receiving a specific TLV.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>select-tlv &lt;TLV-NAME&gt;</td>
<td>Specifies the TLV name to send. The following TLV names are supported:</td>
</tr>
</tbody>
</table>
### Examples

Stopping the LLDP agent from sending the **port-description** TLV:

```
switch(config)# no lldp select-tlv port-description
```

Enabling the LLDP agent to send the **port-description** TLV:

```
switch(config)# lldp select-tlv port-description
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### lldp timer

```
lldp timer <TIME>
no lldp timer
```

**Description**

Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices by the LLDP agent. The minimum setting for this timer must be four times the value of `lldp txdelay`.

For example, this is a valid configuration:
lldp timer = 16
lldp txdelay = 4

And, this is an invalid configuration:

lldp timer = 5
lldp txdelay = 2

When copying a saved configuration to the running configuration, the value for lldp timer is applied before the value of lldp txdelay. This can result in a configuration error if the saved configuration has a value of lldp timer that is not four times the value of lldp txdelay in the running configuration. For example, if the saved configuration has the settings:

lldp timer = 16
lldp txdelay = 4

And the running configuration has the settings:

lldp timer = 30
lldp txdelay = 7

Then you will see an error indicating that certain configuration settings could not be applied, and you will have to manually adjust the value of lldp txdelay in the running configuration.

The no form of this command sets the update interval to its default value of 30 seconds.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

Examples

Setting the update interval to 7 seconds:

```
switch(config)# lldp timer 7
```

Setting the update interval to the default value of 30 seconds:

```
switch(config)# no lldp timer
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**lldp transmit**

*lldp transmit*

*no lldp transmit*

**Description**

Enables transmission of LLDP information on specific interface. By default, LLDP transmission is enabled on all active interfaces.

The *no* form of this command disables transmission of LLDP information on an interface.

**Examples**

Enabling LLDP transmission on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp transmit
```

Disabling LLDP transmission on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp transmit
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**lldp txdelay**

*lldp txdelay <TIME>*

*no lldp txdelay*

**Description**

Sets the amount of time (in seconds) to wait before sending LLDP information from any interface. The maximum value for *txdelay* is 25% of the value of *lldp tx timer*.

The *no* form of this command sets the delay time to its default value of 2 seconds.
**Device discovery and configuration**

**Parameter**<br>**Description**<br><br>\(<\text{T I M E}>\) | Specifies the delay time in seconds. Range: 0 to 10. Default: 2.<br><br>**Examples**<br>Setting the delay time to 8 seconds:<br><br>`switch(config)# lldp txdelay 8`<br><br>Setting the delay time to the default value of 2 seconds:<br><br>`switch(config)# no lldp txdelay`<br><br>**Command History**<br><br>**Release** | **Modification**<br>---|---<br>10.07 or earlier | --<br><br>**Command Information**<br><br>**Platforms** | **Command context** | **Authority**<br>---|---|---<br>All platforms | config | Administrators or local user group members with execution rights for this command.<br><br>**lldp trap enable**<br>lldp trap enable<br>no lldp trap enable<br><br>**Description**<br>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.<br>The `no` form of this command disables the LLDP trap generation.<br><br>LLDP trap generation is disabled by default at the global level and must be enabled before any LLDP traps are sent.<br><br>**Examples**<br>Enabling LLDP trap generation on global level:<br><br>`switch(config)# lldp trap enable`<br><br>Enabling LLDP trap generation on interface level:
Disabling LLDP trap generation on global level:

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

Disabling LLDP trap generation on interface level:

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

Displaying LLDP global configuration:

```bash
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
========================
<table>
<thead>
<tr>
<th>PORT</th>
<th>TX-ENABLED</th>
<th>RX-ENABLED</th>
<th>INTF-TRAP-ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>1/1/6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>.......</td>
<td>.......</td>
<td>.......</td>
<td>.......</td>
</tr>
<tr>
<td>mgmt</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Displaying LLDP Configuration for the interface:

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

LLDP Global Configuration
==========================
LLDP Enabled : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
```
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config and config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show lldp configuration

show lldp configuration [INTERFACE-ID]

Description

Shows LLDP configuration settings for all interfaces or a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
Example
Showing configuration settings for all interfaces:
This example shows configuration settings for interface 1/1/1.

```
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
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show lldp local-device**

**Description**

Shows global LLDP information advertised by the switch, as well as port-based data. If VLANs are configured on any active interfaces, the VLAN ID is only shown for trunk native or untagged VLAN IDs on access interfaces.

**Example**

Showing global LLDP information only:

```
switch# show lldp local-device

Global Data
=============
```
Chassis-ID : 88:3a:30:47:c1:c0
System Name : 6100
System Description : Aruba JL679A PL.10.06.0001-346-g56a12a8f4cf15
Management Address : 88:3a:30:47:c1:c0
Capabilities Available : Bridge, Router
Capabilities Enabled : Bridge, Router
TTL : 120

Showing all ports except 1/1/11 as administratively down:

switch# show lldp local-device

Global Data
===========

Chassis-ID : 88:3a:30:47:c1:c0
System Name : 6100
System Description : Aruba JL679A PL.10.06.0001-346-g56a12a8f4cf15
Management Address : 11.11.11.11
Capabilities Available : Bridge, Router
Capabilities Enabled : Bridge, Router
TTL : 120

Port Based Data
===============

Port-ID : 1/1/11
Port-Desc : "1/1/11"
Port Mgmt-Address : 11.11.11.11
Port VLAN ID : 1
Parent Interface : interface 1/1/11

switch#

In this example, all the ports except 1/1/11 are administratively down, and VLAN ID 100 is configured on this access interface.
switch# show lldp local-device

Global Data
=========

Chassis-ID : 1c:98:ec:e3:45:00
System Name : switch
System Description : Aruba
Management Address : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled : Bridge, Router
TTL : 120

Port Based Data
===============

Port-ID : 1/1/1
Port-Desc : "1/1/1"
Port VLAN ID : 100
Parent Interface : interface 1/1/1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show lldp neighbor-info

show lldp neighbor-info [<INTERFACE-NAME>]

Description

Displays information about neighboring devices for all interfaces or for a specific interface. The information displayed varies depending on the type of neighbor connected and the type of TLVs sent by the neighbor.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;INTERFACE-NAME&gt;</td>
<td>Specifies the interface for which to show information for neighboring devices. Use the format member/slot/port (for example, 1/3/1).</td>
</tr>
</tbody>
</table>

Examples

Showing LLDP information for all interfaces:
switch# show lldp neighbor-info

LLDP Neighbor Information
=================================
Total Neighbor Entries : 1
Total Neighbor Entries Deleted : 5
Total Neighbor Entries Dropped : 0
Total Neighbor Entries Aged-Out : 3

<table>
<thead>
<tr>
<th>LOCAL-PORT</th>
<th>CHASSIS-ID</th>
<th>PORT-ID</th>
<th>PORT-DESC</th>
<th>TTL</th>
<th>SYS-NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>38:21:c7:5c:df:40</td>
<td>1/1/2</td>
<td>1/1/2</td>
<td>120</td>
<td>switch</td>
</tr>
<tr>
<td>1/1/3</td>
<td>f8:60:f0:c9:e0:a0</td>
<td>1/1/3</td>
<td>1/1/3</td>
<td>120</td>
<td>switch</td>
</tr>
</tbody>
</table>

Showing information for interface 1/1/3 when it has only one switch connected as a neighbor:

Aruba-6100-Switch2# show lldp neighbor-info 1/1/3

Port : 1/1/3
Neighbor Entries : 1
Neighbor Entries Deleted : 1
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 1
Neighbor Chassis-Name : 6100
Neighbor Chassis-Description : Aruba JL679A PL.10.06.0001
Neighbor Chassis-ID : 88:3a:30:47:d1:c0
Neighbor Management-Address : 88:3a:30:47:d1:c0
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge, Router
Neighbor Port-ID : 1/1/3
Neighbor Port-Desc : 1/1/3
Neighbor Port VLAN ID : 1
TTL : 120
Neighbor Mac-Phy details
Neighbor Auto-neg Supported : True
Neighbor Auto-neg Enabled : True
Neighbor Auto-neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU Type : 1000 BASETFD

Showing neighbor information for interface 1/3/2 when it has EEE enabled and successfully auto-negotiated:

switch# show lldp neighbor-info 1/3/2

Port : 1/3/2
Neighbor Entries : 1
Neighbor Entries Deleted : 1
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 1
Neighbor Chassis-Name : BLDG01-F1-6300
Neighbor Chassis-Description : Aruba JL668A FL.10.07.0001BN
Neighbor Chassis-ID : 88:3a:30:92:a5:c0
Neighbor Management-Address : 10.6.9.15
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge, Router
Neighbor Port-ID : 1/1/1
Neighbor Port-Desc : 1/1/1
Neighbor Port VLAN ID : 1
TTL : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type : 1000 BASETFD

Neighbor EEE information : DOT3
Neighbor TX Wake time : 17 us
Neighbor RX Wake time : 17 us
Neighbor Fallback time : 17 us
Neighbor TX Echo time : 17 us
Neighbor RX Echo time : 17 us

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show lldp neighbor-info detail

Description
Shows detailed LLDP neighbor information for all LLDP neighbor connected interfaces.

Examples
Showing detailed LLDP information for all interfaces:

```bash
switch# show lldp neighbor-info detail

LLDP Neighbor Information
================-----------
Total Neighbor Entries : 6
Total Neighbor Entries Deleted : 2
Total Neighbor Entries Dropped : 0
Total Neighbor Entries Aged-Out : 2

Port : 1/1/1
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
```
<table>
<thead>
<tr>
<th>Neighbor Entries Aged-Out</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Chassis-Name</td>
<td>6300</td>
</tr>
<tr>
<td>Neighbor Chassis-Description</td>
<td>Aruba ...</td>
</tr>
<tr>
<td>Neighbor Chassis-ID</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Neighbor Management-Address</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Chassis Capabilities Available</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Chassis Capabilities Enabled</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Neighbor Port-ID</td>
<td>1/1/4</td>
</tr>
<tr>
<td>Neighbor Port-Desc</td>
<td>1/1/4</td>
</tr>
<tr>
<td>Neighbor Port VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>TTL</td>
<td>120</td>
</tr>
</tbody>
</table>

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type : 1000 BASETFD

<table>
<thead>
<tr>
<th>Port</th>
<th>1/1/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Entries</td>
<td>1</td>
</tr>
<tr>
<td>Neighbor Entries Deleted</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Entries Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Entries Aged-Out</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Chassis-Name</td>
<td>6300</td>
</tr>
<tr>
<td>Neighbor Chassis-Description</td>
<td>Aruba ...</td>
</tr>
<tr>
<td>Neighbor Chassis-ID</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Neighbor Management-Address</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Chassis Capabilities Available</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Chassis Capabilities Enabled</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Neighbor Port-ID</td>
<td>1/1/5</td>
</tr>
<tr>
<td>Neighbor Port-Desc</td>
<td>1/1/5</td>
</tr>
<tr>
<td>Neighbor Port VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>TTL</td>
<td>120</td>
</tr>
</tbody>
</table>

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type : 1000 BASETFD

<table>
<thead>
<tr>
<th>Port</th>
<th>1/1/3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Entries</td>
<td>1</td>
</tr>
<tr>
<td>Neighbor Entries Deleted</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Entries Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Entries Aged-Out</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor Chassis-Name</td>
<td>6300</td>
</tr>
<tr>
<td>Neighbor Chassis-Description</td>
<td>Aruba ...</td>
</tr>
<tr>
<td>Neighbor Chassis-ID</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Neighbor Management-Address</td>
<td>38:11:17:1a:d5:00</td>
</tr>
<tr>
<td>Chassis Capabilities Available</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Chassis Capabilities Enabled</td>
<td>Bridge, Router</td>
</tr>
<tr>
<td>Neighbor Port-ID</td>
<td>1/1/6</td>
</tr>
<tr>
<td>Neighbor Port-Desc</td>
<td>1/1/6</td>
</tr>
<tr>
<td>Neighbor Port VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>TTL</td>
<td>120</td>
</tr>
</tbody>
</table>

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type : 1000 BASETFD

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show lldp statistics**

show lldp statistics [<INTERFACE-ID>]
Shows global LLDP statistics or statistics for a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

### Example

Showing global statistics for all interfaces:

```bash
switch# show copp-policy statistics
switch# show lldp statistics
LLDP Global Statistics
==========================================================================
Total Packets Transmitted : 25
Total Packets Received    : 20
Total Packets Received And Discarded : 0
Total TLVs Unrecognized   : 0

LLDP Port Statistics
==========================================================================
<table>
<thead>
<tr>
<th>PORT-ID</th>
<th>TX-PACKETS</th>
<th>RX-PACKETS</th>
<th>RX-DISCARDED</th>
<th>TLVS-UNKNOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>25</td>
<td>20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/22</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/27</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/28</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Showing statistics for interface 1/1/1:

```bash
switch# show lldp statistics 1/1/1
```
LLDP Statistics
===============

<table>
<thead>
<tr>
<th>Port Name</th>
<th>1/1/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Transmitted</td>
<td>159</td>
</tr>
<tr>
<td>Packets Received</td>
<td>163</td>
</tr>
<tr>
<td>Packets Received And Discarded</td>
<td>0</td>
</tr>
<tr>
<td>Packets Received And Unrecognized</td>
<td>0</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; only).</td>
</tr>
</tbody>
</table>

show lldp tlv

Description
Shows the LLDP TLVs that are configured for send and receive.

Example

```
switch# show lldp tlv

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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a proprietary layer 2 protocol supported by most Cisco devices. It is used to exchange information, such as software version, device capabilities, and voice VLAN information, between directly connected devices, such as a VoIP phone and a switch.

CDP support

By default, CDP is enabled on each active switch port. This is a read-only capability, which means the switch can receive and store information about adjacent CDP devices, but does not generate CDP packets (except when communicating with Cisco IP phones.)

The switch supports CDPv2 only and does not support SNMP MIB traps.

When a CDP-enabled port receives a CDP packet from another CDP device, it enters data for that device into the CDP Neighbors table, along with the port number on which the data was received. It does not forward the packet. The switch also periodically purges the table of any entries that have expired. (The holdtime for any data entry in the switch CDP Neighbors table is configured in the device transmitting the CDP packet and cannot be controlled in the switch receiving the packet.) A switch reviews the list of CDP neighbor entries every three seconds and purges any expired entries.

Support for legacy Cisco IP phones

Autoconfiguration of legacy Cisco IP phones for tagged voice VLAN support requires CDPv2.

On initial boot-up, and sometimes periodically, a Cisco phone queries the switch and advertises information about itself using CDPv2. When the switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone, the switch immediately responds with the voice VLAN ID in a reply packet using the VoIP VLAN Reply TLV (type 0x0e). This enables the Cisco phone to boot properly and send traffic on the advertised voice VLAN ID.

The switch CDP packet includes these TLVs:

- CDP Version: 2
- CDP TTL: 180 seconds
- Checksum
- Capabilities (type 0x04): 0x0008 (is a switch)
- Native VLAN: The PVID of the port
- VoIP VLAN Reply (type 0xe): voice VLAN ID (same as advertised by LLDP-MED)
- Trust Bitmap (type 0x12): 0x00
- Untrusted port CoS (type 0x13): 0x00

CDP commands

cdp
cdp

Description
Configures CDP support globally on all active interfaces or on a specific interface. By default, CDP is enabled on all active interfaces.

When CDP is enabled, the switch adds entries to its CDP Neighbors table for any CDP packets it receives from neighboring CDP devices.

When CDP is disabled, the CDP Neighbors table is cleared and the switch drops all inbound CDP packets without entering the data in the CDP Neighbors table.

The no form of this command disables CDP support globally on all active interfaces or on a specific interface.

**Examples**

Enabling CDP globally:

```
switch(config)# cdp
```

Disabling CDP globally:

```
switch(config)# no cdp
```

Enabling CDP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# cdp
```

Disabling CDP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no cdp
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-if</td>
<td></td>
</tr>
</tbody>
</table>

**clear cdp counters**

clear cdp counters

**Description**

Clears CDP counters.

**Examples**

Clearing CDP counters:
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`clear cdp neighbor-info`

`clear cdp neighbor-info`

**Description**
Clears CDP neighbor information.

**Examples**
Clearing CDP neighbor information:

```plaintext
switch(config) clear neighbor-info
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`show cdp`

`show cdp`

**Description**
Shows CDP information for all interfaces.

**Examples**
Showing CDP information:
switch(config)# show cdp
CDP Global Information
======================
CDP : Enabled
CDP Mode : Rx only
CDP Hold Time : 180 seconds

<table>
<thead>
<tr>
<th>Port</th>
<th>CDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/6</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/7</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/8</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/9</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/10</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show cdp neighbor-info**

**show cdp neighbor-info <INTERFACE-ID>**

**Description**

Shows CDP information for all neighbors or for CDP information on a specific interface.

**Parameter**

<table>
<thead>
<tr>
<th>&lt;INTERFACE-ID&gt;</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies an interface. Format: member/slot/port.</td>
</tr>
</tbody>
</table>

**Examples**

Showing all CDP neighbor information:

```
switch(config)# show cdp neighbor-info
Port    Device ID   Platform     Capability
-------- ----------- ------------ ----------
1/1/1    myswitch   cisco WS-C2950-12  S1
```

Showing CDP information for interface **1/1/1**:
switch(config)# show cdp neighbor-info 1/1/1
Local Port : 1/1/1
MAC : 3c:a8:2a:7b:6b:2b
Device ID : SEPd4adb2a30d6
Address : 2.71.0.230
Platform : Cisco IP Phone 3905
Duplex : full
Capability : host
Voice VLAN Support : Yes
Neighbor Port-ID : Port 1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show cdp traffic**

**show cdp neighbor-info**

**Description**

Shows CDP statistics for each interface.

**Examples**

Showing CDP traffic statistics:

```
switch(config)# show cdp traffic
CDP Statistics
====================
Port | Transmitted Frames | Received Frames | Discarded Frames |
-----|--------------------|-----------------|-----------------|
1/1/1| 0                  | 4               | 0               |
1/1/2| 0                  | 0               | 0               |
1/1/3| 0                  | 2               | 0               |
1/1/4| 0                  | 0               | 0               |
1/1/5| 0                  | 0               | 0               |
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td><code>config</code></td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Zero Touch Provisioning (ZTP) enables the auto-configuration of factory default switches without a network administrator onsite. When a switch is booted from its factory default configuration, ZTP autoprovisions the switch by automatically downloading and installing a firmware file, a configuration file, or both. With ZTP, even a nontechnical user (for example: a store manager in a retail chain or a teacher in a school) can deploy devices at a site.

**ZTP support**

The switch supports standards-based Zero Touch Provisioning (ZTP) operations as follows:

- The switch must be running the factory default configuration.
- ZTP operations are supported over IPv4 connections only. IPv6 connections are not supported for ZTP operations.
- You must configure the DHCP server to provide a standards-based ZTP server solution. Options and features that are specific to Network Management Solution (NMS) tools, such as AirWave, are not supported.
  - Supported DHCP options are:

<table>
<thead>
<tr>
<th>DHCP option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>Vendor Specific Information</td>
</tr>
<tr>
<td>43 suboption 144</td>
<td>Name of the configuration file</td>
</tr>
<tr>
<td>43 suboption 145</td>
<td>Name of the firmware image file</td>
</tr>
<tr>
<td>43 suboption 148</td>
<td>HTTP Proxy FQDN or IPv4 address</td>
</tr>
<tr>
<td>60</td>
<td>Vendor Class Identifier (VCI)</td>
</tr>
<tr>
<td>66</td>
<td>IPv4 address of the TFTP server (Specifying a host name instead of an IP address is not supported.)</td>
</tr>
<tr>
<td>67</td>
<td>Name of the configuration file (Option 43 suboption 144 takes precedence over this option.)</td>
</tr>
</tbody>
</table>

- The configuration file is a text file or JSON file that becomes the startup and running configuration on the switch after the ZTP operation is complete. The configuration can be in CLI or in JSON format.
- When the switch is started using the factory default configuration, the ZTP operation is started automatically and is active until any running configuration of the switch is modified. There is no CLI command required to start the operation.

The switch supports the following standards:
- [RFC 2132](https://tools.ietf.org/html/rfc2132), *DHCP Options and BOOTP Vendor Extensions.* Support is limited to the options listed in the table "Supported DHCP options for ZTP on AOS-CX."

Hewlett Packard Enterprise recommends that you implement ZTP in a secure and private environment. Any public access can compromise the security of the switch, as follows:

- ZTP is enabled only in the factory default configuration of the switch, DHCP snooping is not enabled. The Rogue DHCP server must be manually managed.
- The DHCP offer is in plain data without encryption.

**Setting up ZTP on a trusted network**

The following procedure is an overview of setting up a Zero Touch Provisioning (ZTP) environment to provision newly installed switches automatically. The procedure is intended for network administrators who are familiar with automatically provisioning switches in a network, and does not provide detailed information about configuring or managing switches.

**Procedure**

1. For each switch model to be provisioned using ZTP, do the following:
   a. Obtain the switch firmware image file.
   b. Prepare the switch configuration file. The configuration file becomes the running configuration and the startup configuration on the switch.
2. Set up a TFTP server and record its IP address. The address is required when you set up the DHCP server. The switch must be able to reach the TFTP server and DHCP server on the same subnet. Switches support provisioning through a network connected to a data port or through a network connected to the in-band management interface VLAN 1.
3. Publish the configuration files and image files to the TFTP server. You need to know the locations of the files and the IP address of the TFTP server when you set up the vendor class options on the DHCP server.
4. On the DHCP server, set up vendor classes for each switch model you plan to provision. To do this you need the following information:
   - The IP address of the TFTP server. Using a host name is not supported.
   - The path to the switch configuration and firmware image files on the TFTP server.
   - The vendor class identifier (VCI) for each switch model.
   You can obtain the VCI by entering the `show dhcp client vendor-class-identifier` command from a switch CLI command prompt in the manager context. The VCI is the text string in the response that starts with *Aruba.*
   For example:
   ```
   switch# show dhcp client vendor-class-identifier
   Vendor Class Identifier: Aruba xxxxx xxxx
   ```
   Where x indicates the switch model number.
5. At the installation site, provide the switch installer with a Cat6 network cable connected to the network that includes the DHCP and TFTP servers, and information about the switch port to use. The switch installer plugs the cable into the data port you specify.
The ZTP operation begins when power is applied to the switch after the network cable is installed.

6. Assuming the downloaded configuration includes a way to access the CLI of the switch, you can enter the following command to show the options offered by the DHCP server and the status of the ZTP operation:

   show ztp information

**ZTP process during switch boot**

1. The switch boots up with the factory default configuration.
   
   If the ZTP operation detects that the configuration is different from the factory default configuration, the ZTP operation ends. The switch must be configured at the installation site.

2. The switch sends out a DHCP discovery from the in-band management interface.

   The switch waits to receive DHCP options indefinitely or until the running configuration is modified. If a DHCP IP address is received but no DHCP options are received, the switch waits an additional minute before ending the ZTP operation.

   After the ZTP operation ends, there is no automatic retry. You can either attempt to boot the switch with the factory default configuration again, configure the switch at the installation site, or use the ZTP force-provision CLI to trigger the ZTP process, ignoring the present running configuration of the switch.

   - Once force-provision is enabled, new DHCP requests are sent from the switch. Disabling force-provision does not stop the DHCP already in progress, but only changes the switch configuration status of force-provision.

   - If ZTP fails while force-provision is enabled, there is no automatic retry. To retry, `ztp force-provision` should be disabled and re-enabled to clear the current ZTP state and send a new DHCP request. When `ztp force-provision` is already enabled on the switch, re-enabling it results in no operation.

   - If the DHCP server is configured to provide both ZTP image and configuration options and there is a non-default startup configuration present on the switch, clearing the non-default startup configuration before triggering `ztp force-provision` is recommended. If an image is downloaded via ZTP, the switch reboots once the image download is complete and ZTP force-provision configuration is lost, causing ZTP to enter into a failed state. ZTP force-provision will need to be enabled again to continue the process.

3. The DHCP server responds with an offer containing the following:

   - The IPv4 address of the TFTP server
   - One or both of the following:
     - The name of the firmware image file
     - The name of the configuration file
   - Aruba Central Location (optional)
   - HTTP Proxy Location (optional)

4. If a firmware image file is offered, the ZTP operation downloads the image file from the TFTP server to the switch. If the current switch image and downloaded firmware image version do not match, then the switch boots with the downloaded image:

   - If the image upgrade fails, the switch retains its original firmware image and the ZTP operation ends with a failed status.
If the image upgrade succeeds, the ZTP operation is started again after the switch reboots. Because the downloaded image file matches the image file installed on the switch, the ZTP operation continues, and checks if a configuration file is offered.

5. If a configuration file is offered, the ZTP operation downloads the configuration file copies the file to the running-config and then to the startup-config of the switch:
   - If the startup configuration update fails, the switch retains its factory-default running configuration and the ZTP operation ends with a failed status.
     - If the copy operation fails, the ZTP operation ends with a failed status.
     - If the copy operation succeeds, the ZTP operation ends successfully.

**ZTP commands**

**show ztp information**

*show ztp information*

**Description**
Shows information about Zero Touch Provisioning (ZTP) operations performed on the switch.

**Usage**
When a switch configured to use ZTP is booted from a factory default configuration, the switch contacts a DHCP server, which offers options for obtaining files used to provision the switch:

- The IP address of the TFTP server
- The name of the image file
- The name of the configuration file

The `show ztp information` command shows the options offered by the DHCP server and the status of the ZTP operation.

The status of the ZTP operation is one of the following:

**Success**
The ZTP operation succeeded.

One of the following is true:

- Both the running configuration and the startup configuration were updated.
- The IP address of the TFTP server was received, but the offer did not include a configuration file or a firmware image file.
- Any combination of vendor encapsulated DHCP options are received as configured, along with the firmware image and switch configuration file.
- Only vendor encapsulated DHCP options are configured and are received accordingly.

**Failed - Custom startup configuration detected**
The switch was booted from a configuration that is not the factory default configuration. For example, the administrator password has been set.

**Failed - Timed out while waiting to receive ZTP options**
Either the switch received the DHCP IPv4 address but no ZTP options were received within 1 minute or ZTP force-provision is triggered and no ZTP options are received within 3 minutes.

**Failed - Detected change in running configuration**
The running configuration was modified by a user while the ZTP operation was in progress.

**Failed - TFTP server unreachable**
The TFTP server is not reachable at the specified IP address.

**Failed - TFTP server information unavailable**
The image file name or config file name is provided without the TFTP server location to fetch the files from and ZTP enters failed state.

**Failed - Invalid configuration file received**
Either the file transfer of the configuration file failed, or the configuration file is invalid (an error occurred while attempting to apply the configuration).

**Failed - Invalid image file received**
Either the file transfer of the firmware image file failed, or the firmware image file is invalid (an error occurred while verifying the image).

**Examples**
Showing switch image download in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server : 10.0.0.2
Image File   : TL_10_02_0001.swi
Configuration File : config_file
ZTP Status   : In-progress - Image download and verification
Aruba Central Location : secure.arubanetworks.com
Force-Provision : Disabled
HTTP Proxy Location : http.proxy.arubanetworks.com
```

Showing switch image download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server : 10.0.0.2
Image File   : TL_10_02_0001.swi
Configuration File : config_file
ZTP Status   : Failed - Unable to download image
Aruba Central Location : secure.arubanetworks.com
Force-Provision : Disabled
HTTP Proxy Location : http.proxy.arubanetworks.com
```

Showing switch configuration download in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server : 10.0.0.2
Image File   : TL_10_02_0001.swi
Configuration File : config_file
ZTP Status   : In-progress - Configuration download
Aruba Central Location : secure.arubanetworks.com
Force-Provision : Disabled
HTTP Proxy Location : http.proxy.arubanetworks.com
```

Showing switch configuration download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server : 10.0.0.2
```
Showing switch failure to update start-up configuration after downloading configuration received from ZTP options:

switch# show ztp information
TFTP Server : 10.0.0.2
Image File : TL_10_02_0001.swi
Configuration File : config_file
ZTP Status : Failed - Unable to download configuration
Aruba Central Location : secure.arubanetworks.com
Force-Provision : Disabled
HTTP Proxy Location : http.proxy.arubanetworks.com

In the following example, the ZTP operation succeeded, and both an image file and a configuration file were provided.

switch# show ztp information
TFTP Server : 20.1.1.4
Image File : PL_10_06_0001BT.swi
Configuration File : bristol_maxlimit
Status : Success
Force-Provision : Disabled
switch#

In the following example, the ZTP option succeeded. A configuration file was not provided, but an image file was provided.

switch# show ztp information
TFTP Server : 20.1.1.4
Image File : NA
Configuration File : bristol_maxlimit
Status : Success
Force-Provision : Disabled
switch#

In the following example, the ZTP operation failed because the TFTP server was unreachable.

switch# show ztp information
TFTP Server : 20.1.1.4
Image File : PL_10_06_0001BT.swi
Configuration File : bristol_maxlimit
Status : Failed - TFTP server unreachable
Force-Provision : Disabled
switch#

In the following example, the ZTP operation was stopped because the switch did not receive any options from the DHCP server for ZTP within 1 minute of receiving the IP address from the server.
switch## show ztp information
TFTP Server : NA
Image File : NA
Configuration File : NA
Status : Failed - Timed out while waiting to receive ZTP options
Force-Provision : Disabled
switch#

In the following example, the ZTP operation was stopped because the switch was booted from a configuration that was not the factory default configuration.

switch# show ztp information
TFTP Server : 20.1.1.4
Image File : PL_10_06_0001BT.swi
Configuration File : bristol_maxlimit
Status : Failed - Custom startup configuration detected
Force-Provision : Disabled

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

ztp force provision

ztp force-provision
no ztp force-provision

Description

Starts on-demand ZTP.

Usage

DHCP options received are processed independent of the current state of configuration on the switch. Previous ZTP TFTP Server, Image File, Configuration File, Aruba Central Location, and HTTP Proxy location options are cleared and the switch sends a DHCP request.

Examples

In the following example, force-provision is enabled.

switch# configure terminal
switch(config)# ztp force-provision

In the following example, force-provision status is checked while enabled.
switch# **show ztp information**
TFTP Server: 10.0.0.2
Image File: TL_10_02_0001.swi
Configuration File: ztp.cfg
Status: Success
Aruba Central Location: NA
Force-Provision: Enabled
HTTP Proxy Location: NA

In the following example, force-provision is disabled.

```bash
switch# configure terminal
switch(config)# no ztp force-provision
```

In the following example, force-provision status is checked while disabled.

```bash
switch# show ztp information
TFTP Server: 10.0.0.2
Image File: TL_10_02_0001.swi
Configuration File: ztp.cfg
Status: Success
Aruba Central Location: NA
Force-Provision: Disabled
HTTP Proxy Location: NA
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
clear events

clear events

Description
Clears up event logs. Using the show events command will only display the logs generated after the clear events command.

Examples
Clearing all generated event logs:

```
switch# show events
------------------------------------------------------------------------
show event logs
------------------------------------------------------------------------
2018-10-14:06:53.534384|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 27
2018-10-14:06:58.805504|lldpd|103|LOG_INFO|MSTR|1|Configured LLDP tx-timer to 36
2018-10-14:07:01.577564|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 49

switch# clear events

switch# show events
------------------------------------------------------------------------
show event logs
------------------------------------------------------------------------
2018-10-14:07:03.637544|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource utilization poll interval is changed to 34
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

console baud-rate

close baud-rate <speed>
no console baud-rate <SPEED>

Description
Sets the console serial port speed. The no form of this command resets the console port speed to its default of 115200 bps.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SPEED&gt;</td>
<td>Selects the console port speed in bps, either 9600 or 115200.</td>
</tr>
</tbody>
</table>

Usage
The speed change occurs immediately for the active console session. The console will be inaccessible until the client terminal settings are updated to match the console port speed that you set. After the command is executed you will be prompted to log in again.

Examples
Setting the console port speed to 9600 bps:

```
switch(config)# console baud-rate 9600
```
This command will configure the baud rate immediately for the active serial console session. After the command is executed the user will be prompted to re-login. The serial console will be inaccessible until the terminal client settings are updated to match the baud rate of the switch.
Continue (y/n)? y

Resetting the console port to its default speed 115200 bps:

```
switch(config)# no console baud-rate
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

domain-name
domain-name <NAME>
no domain-name [<NAME>]

Description
Specifies the domain name of the switch.
The no form of this command sets the domain name to the default, which is no domain name.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NAME&gt;</td>
<td>Specifies the domain name to be assigned to the switch. The first character of the name must be a letter or a number. Length: 1 to 32 characters.</td>
</tr>
</tbody>
</table>

**Examples**

Setting and showing the domain name:

```
switch# show domain-name
switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Setting the domain name to the default value:

```
switch(config)# no domain-name
switch(config)# show domain-name
switch(config)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**hostname**

hostname <HOSTNAME>
no hostname [<HOSTNAME>]

**Description**

Sets the host name of the switch.

The no form of this command sets the host name to the default value, which is switch.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;HOSTNAME&gt;</td>
<td>Specifies the host name. The first character of the host name must be a letter or a number. Length: 1 to 32 characters. Default: switch</td>
</tr>
</tbody>
</table>

**Examples**

Setting and showing the host name:

```
switch# show hostname
switch(config)# hostname myswitch
myswitch(config)# show hostname
```

Setting the host name to the default value:

```
myswitch(config)# no hostname
```

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

---

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

---

**show capacities**

```
show capacities <FEATURE>
```

**Description**

Shows system capacities and their values for all features or a specific feature.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;FEATURE&gt;</td>
<td>Specifies a feature. For example, aaa.</td>
</tr>
</tbody>
</table>

**Usage**

Capacities are expressed in user-understandable terms. Thus they may not map to a specific hardware or software resource or component. They are not intended to define a feature exhaustively.

**Examples**
Showing classifier-related capacities on the 6100:

```
switch# show capacities classifier

System Capacities: Filter Classifier
Capacities Name                                                                 Value
-------------------------------------------------------------------------------
Maximum number of Access Control Entries configurable in a system             4096
Maximum number of Access Control Lists configurable in a system               512
Maximum number of class entries configurable in a system                      4096
Maximum number of classes configurable in a system                            512
Maximum number of entries in an Access Control List                           1024
Maximum number of entries in a class                                          1024
Maximum number of entries in a policy                                         64
Maximum number of classifier policies configurable in a system                512
Maximum number of policy entries configurable in a system                     4096

Showing all available capacities on the 6100:

```
switch# show capacities

System Capacities:
Capacities Name                                                                 Value
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Maximum number of Access Control Entries configurable in a system             4096
Maximum number of Access Control Lists configurable in a system               512
Maximum number of class entries configurable in a system                      4096
Maximum number of classes configurable in a system                            512
Maximum number of entries in an Access Control List                           1024
Maximum number of entries in a class                                          1024
Maximum number of entries in a policy                                         64
Maximum number of classifier policies configurable in a system                512
Maximum number of policy entries configurable in a system                     4096
Maximum number of clients supported for tracking the IP address in the system 128
Maximum number of dynamic VLANs that can be allowed using MVRP                256
Maximum number of nexthops per IP ECMP group                                  1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system             1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system    1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system     512
Maximum number of L2 MAC addresses supported in the system                    8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups                    1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
Maximum number of configurable LAG ports 8
Maximum number of members supported by a LAG port 8
Maximum number of VLANs across ports allowed in loop-protect 3328
Maximum number of IGMP/MLD groups supported 512
Maximum number of IGMP/MLD snooping groups supported 512
Maximum number of Mirror Sessions configurable in a system 4
Maximum number of enabled Mirror Sessions in a system 4
Maximum number of mstp instances configurable in a system 16
Maximum number of Clients that can be authenticated on a port 32
Maximum number of Device Profiles allowed to be created on the system 8
Maximum number of Port Access Roles allowed to be created on the system 32
Maximum number of MAC Address that can be authorized on a port 32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system 50
Maximum number of Port Access Role VLAN names allowed to be created on the system 50
Maximum number of RBAC rules per user group 1024
Maximum number of RPVST VLANs configurable on the system 16
Maximum number of RPVST VPORTs supported in a system 512
Maximum number of SVIs supported in the system 16
Maximum number of routes (IPv4+IPv6) on the system 512
Maximum number of IPv4 routes on the system 512
Maximum number of IPv6 routes on the system 512
Maximum number of VLANs supported in the system 512

Showing all available capacities for mirroring:

```
switch# show capacities mirroring
System Capacities: Filter Mirroring
Capacities Name                  Value
Maximum number of Mirror Sessions configurable in a system 4
Maximum number of enabled Mirror Sessions in a system 4
```
Showing all available capacities for MSTP:

```bash
switch# show capacities mstp
```

System Capacities: Filter MSTP
Capacities Name | Value
----------------|--------
Maximum number of mstp instances configurable in a system | 64

Showing all available capacities for VLAN count:

```bash
switch# show capacities vlan-count
```

System Capacities: Filter VLAN Count
Capacities Name | Value
----------------|--------
Maximum number of VLANs supported in the system | 4094

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show capacities-status**

Show capacities-status `<FEATURE>`

**Description**

Shows system capacities status and their values for all features or a specific feature.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;FEATURE&gt;</code></td>
<td>Specifies the feature, for example <code>aaa</code> for which to display capacities, values, and status. Required.</td>
</tr>
</tbody>
</table>

**Examples**

Showing the system capacities status for all features:

```bash
switch# show capacities-status
```
System Capacities Status
Capacities Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td></td>
</tr>
</tbody>
</table>

---

Number of Access Control Entries currently configured 0 4096
Number of Access Control Lists currently configured 0 512
Number of class entries currently configured 0 4096
Number of classes currently configured 0 512
Number of policies currently configured 0 512
Number of policy entries currently configured 0 4096
Number of dynamic VLANs currently learnt using MVRP 0 256
Number of IP neighbor (IPv4+IPv6) entries 1 1024
Number of IPv4 neighbor(ARP) entries 1 1024
Number of IPv6 neighbor(ND) entries 0 512
Number of L3 Groups for IP Tunnels and ECMP Groups currently configured 0 1
Number of L3 Destinations for Routes, Nexthops in ECMP groups and Tunnels currently configured 0 1024
Number of Mirror Sessions currently configured 0 4
Number of Mirror Sessions currently enabled 0 4
Number of mstp instances currently configured 0 16
Number of RPVST VLANs currently configured 0 16
Number of routes (IPv4+IPv6) currently configured 1 512
Number of IPv4 routes currently configured 1 512
Number of IPv6 routes currently configured 0 512
Number of VLANs currently configured 1 512

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show console

Description
Shows the serial console port current speed.

Examples
Showing the console port current speed:

```
switch# show console
Baud Rate: 9600
```

Command History
Release | Modification
--- | ---
10.08 | Command introduced

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show core-dump**

*show core-dump all*

**Description**

Shows core dump information about the specified module. When no parameters are specified, shows only the core dumps generated in the current boot of the management module. When the `all` parameter is specified, shows all available core dumps.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all available core dumps.</td>
</tr>
</tbody>
</table>

**Usage**

When no parameters are specified, the `show core-dump` command shows only the core dumps generated in the current boot of the management module. You can use this command to determine when any crashes are occurring in the current boot.

If no core dumps have occurred, the following message is displayed: **No core dumps are present**

To show core dump information for the standby management module, you must use the `standby` command to switch to the standby management module and then execute the `show core-dump` command.

In the output, the meaning of the information is the following:

- **Daemon Name**
  Identifies name of the daemon for which there is dump information.
- **Instance ID**
  Identifies the specific instance of the daemon shown in the Daemon Name column.
- **Present**
  Indicates the status of the core dump:
  - Yes
    The core dump has completed and available for copying.
  - In Progress
    Core dump generation is in progress. Do not attempt to copy this core dump.
- **Timestamp**
  Indicates the time the daemon crash occurred. The time is the local time using the time zone configured on the switch.
- **Build ID**
  Identifies additional information about the software image associated with the daemon.

**Examples**

Showing core dump information for the current boot of the active management module only:
### show core-dump

```
switch# show core-dump
-----------------------------------------------------------------------------------
Daemon Name    | Instance ID | Present | Timestamp       | Build ID
-----------------------------------------------------------------------------------
hpe-fand      | 1399        | Yes     | 2017-08-04 19:05:34 | 1246d2a
hpe-sysmond   | 957         | Yes     | 2017-08-04 19:05:29 | 1246d2a
------------------------------------------------------------------------------------
Total number of core dumps : 2
-----------------------------------------------------------------------------------
```

Showing all core dumps:

```
switch# show core-dump all
-----------------------------------------------------------------------------------
Management Module core-dumps
-----------------------------------------------------------------------------------
Daemon Name    | Instance ID | Present | Timestamp       | Build ID
-----------------------------------------------------------------------------------
hpe-sysmond   | 513         | Yes     | 2017-07-31 13:58:05 | e70f101
hpe-tempd     | 1048        | Yes     | 2017-08-13 13:31:53 | e70f101
hpe-tempd     | 1052        | Yes     | 2017-08-13 13:41:44 | e70f101
------------------------------------------------------------------------------------
Line Module core-dumps
-----------------------------------------------------------------------------------
Line Module : 1/1
-----------------------------------------------------------------------------------
dune_agent_0  | 18958       | Yes     | 2017-08-12 11:50:17 | e70f101
dune_agent_0  | 18842       | Yes     | 2017-08-12 11:50:09 | e70f101
------------------------------------------------------------------------------------
Total number of core dumps : 5
-----------------------------------------------------------------------------------
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### show domain-name

**show domain-name**

**Description**

Shows the current domain name.

**Usage**

If there is no domain name configured, the CLI displays a blank line.
Example
Setting and showing the domain name:

```
switch# show domain-name
switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show environment fan

show environment fan is not available for JL679A.

show environment fan

Description
Shows the status information for all fans and fan trays (if present) in the system.

Usage
For fan trays, Status is one of the following values:
- **ready**
  - The fan tray is operating normally.
- **fault**
  - The fan tray is in a fault event. The status of the fan tray does not indicate the status of fans.
- **empty**
  - The fan tray is not installed in the system.

For fans:
- **Speed**
  - Indicates the relative speed of the fan based on the nominal speed range of the fan.
  - N/A
    - This value is not applicable to the 6000 or 6100.
- **Direction**
  - The direction of airflow through the fan. Values are:
    - **left-to-right**
      - Air flows from the left of the system to the right of the system.
    - N/A
The fan is not installed.

Status
Fan status. Values are:
uninitialized
   The fan has not completed initialization.
ok
   The fan is operating normally.
fault
   The fan is in a fault state.
empty
   The fan is not installed.

Examples
Showing output for systems with fan trays for 6100 switch series:

```
switch# show environment fan
Fan information
-----------------------------------------------
Mbr/Fan | Product | Serial Number | Speed | Direction | Status | RPM
Name    
-----------------------------------------------
1/1     | N/A     | N/A           | N/A   | left-to-right | ok     | N/A
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show environment led**

**show environment led**

Description
Shows state and status information for all the configurable LEDs in the system.

Example
Showing state and status for LED:

```
switch# show environment led
Mbr/Name       State  Status
-------------------------
1/locator       off    ok
```
show environment power-supply

Description
Shows status information about all power supplies in the switch.

Usage
The following information is provided for each power supply:

- **Mbr/PSU**
  Shows the member and slot number of the power supply.
- **Product Number**
  Shows the product number of the power supply.
- **Serial Number**
  Shows the serial number of the power supply, which uniquely identifies the power supply.
- **PSU Status**
  The status of the power supply. Values are:
    - **OK**
      Power supply is operating normally.
    - **OK***
      Power supply is operating normally, but it is the only power supply in the chassis. One power supply is not sufficient to supply full power to the switch. When this value is shown, the output of the command also shows a message at the end of the displayed data.
    - **Absent**
      No power supply is installed in the specified slot.
    - **Input fault**
      The power supply has a fault condition on its input.
    - **Output fault**
      The power supply has a fault condition on its output.
    - **Warning**
      The power supply is not operating normally.

- **Wattage Maximum**
  Shows the maximum amount of wattage that the power supply can provide.

Example
Showing the output when only one power supply is installed in the switch:
show environment power-supply

<table>
<thead>
<tr>
<th>Product Mbr/PSU</th>
<th>Serial Number</th>
<th>PSU Status</th>
<th>Maximum Wattage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>N/A</td>
<td>OK</td>
<td>500</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show environment temperature

show environment temperature [detail]

Description

Shows the temperature information from sensors in the switch that affect fan control.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Shows detailed information from each temperature sensor.</td>
</tr>
</tbody>
</table>

Usage

Temperatures are shown in Celsius.

Valid values for status are the following:

- normal
- min
- max
- low_critical
- critical
- high_critical
- fault
- emergency
- Over temperature event for this sensor.

Examples

Showing current temperature information for a 6100 switch:
switch# show environment temperature
Temperature information

<table>
<thead>
<tr>
<th>Mbr/Slot-Sensor</th>
<th>Module Type</th>
<th>Current temperature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1-COME-Daughter-Boar</td>
<td>line-card-module</td>
<td>66.45 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/1-PCIE-Switch</td>
<td>line-card-module</td>
<td>95.82 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/1-Processor</td>
<td>line-card-module</td>
<td>00.00 C</td>
<td>fault</td>
</tr>
<tr>
<td>1/1-Switch-ASIC</td>
<td>line-card-module</td>
<td>116.36 C</td>
<td>emergency</td>
</tr>
<tr>
<td>1/1-Switch-ASIC-Internal</td>
<td>line-card-module</td>
<td>108.25 C</td>
<td>critical</td>
</tr>
<tr>
<td>1/2-COME-Daughter-Boar</td>
<td>line-card-module</td>
<td>67.29 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/2-PCIE-Switch</td>
<td>line-card-module</td>
<td>95.82 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/2-Processor-1</td>
<td>line-card-module</td>
<td>72.92 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/2-Processor-2</td>
<td>line-card-module</td>
<td>73.05 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/2-Switch-ASIC</td>
<td>line-card-module</td>
<td>97.41 C</td>
<td>normal</td>
</tr>
<tr>
<td>1/2-Switch-ASIC-Internal</td>
<td>line-card-module</td>
<td>97.62 C</td>
<td>normal</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show events

show events [ -e <EVENT-ID> ]
  -s {emergency | alert | critical | error | warning | notice | info | debug} |
  -r |
  -a |
  -n <COUNT> |
  -i <MEMBER-SLOT> |
  -m {active | standby} |
  -c {lldp | ospf | ...} |
  -d {lldpd | bgpd | fand | ...} |

Description

Shows event logs generated by the switch modules since the last reboot.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-e &lt;EVENT-ID&gt;</td>
<td>Shows the event logs for the specified event ID. Event ID range: 101 through 99999.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>`-s {emergency</td>
<td>Shows the event logs for the specified severity. Select the severity</td>
</tr>
<tr>
<td>alert</td>
<td>critical</td>
</tr>
<tr>
<td>error</td>
<td>warning</td>
</tr>
<tr>
<td>shows event logs with severity emergency only.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity alert and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity critical and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity error and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity warning and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity notice and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with severity info and above.</td>
<td></td>
</tr>
<tr>
<td>shows event logs with all severities.</td>
<td></td>
</tr>
<tr>
<td><code>-r</code></td>
<td>Shows the most recent event logs first.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Shows all event logs, including those events from previous boots.</td>
</tr>
<tr>
<td><code>-n &lt;COUNT&gt;</code></td>
<td>Displays the specified number of event logs.</td>
</tr>
<tr>
<td>`-c {lldp</td>
<td>ospf</td>
</tr>
<tr>
<td>`-d {lldpd</td>
<td>bgpd</td>
</tr>
</tbody>
</table>

**Examples**

**Showing event logs:**

```bash
switch# show events
-----------------------------
show event logs
-----------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
```

**Showing the most recent event logs first:**

```bash
switch# show events -r
-----------------------------
show event logs
-----------------------------
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up for bridge_normal interface
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
```

**Showing all event logs:**

```bash
# Use show event -a for all event logs
```
switch# show events -a
-----------------------------------------------------------
show event logs
-----------------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to up
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1 in Hardware

Showing event logs related to LACP:

switch# show events -c lacp
-----------------------------------------------------------
show event logs
-----------------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c

Showing event logs as per the specified member/slot ID:

switch# show events -i 1/1
-----------------------------------------------------------
show event logs
-----------------------------------------------------------
2017-08-17:22:32:25.743991|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource utilization poll interval is changed to 313
2017-08-17:22:33:01.692860|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource utilization poll interval is changed to 23
2017-08-17:22:33:06.181436|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource utilization poll interval is changed to 512
2017-08-17:22:33:06.181436|systemd-coredump|1201|LOG_CRIT|LC|1/1|hpe-sysmond crashed due to signal:11

Showing event logs as per the specified process:

switch# show events -d lacpd
-----------------------------------------------------------
show event logs
-----------------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to 70:72:cf:51:50:7c

Displaying the specified number of event logs:

switch# show events -n 5
-----------------------------------------------------------
show event logs
-----------------------------------------------------------
2018-03-21:06:12:15.500603|arpmgrd|6101|LOG_INFO|AMM|1|ARPMD daemon has started
2018-03-21:06:12:17.734405|lldpd|109|LOG_INFO|AMM|1|Configured LLDP tx-delay to 2
2018-03-21:06:12:17.743491|vrfmgrp|5401|LOG_INFO|AMM|1|Created a vrf entity 42cc3df7-1113-412f-b5cb-e8227b8c22f2
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor&gt;) only.</td>
</tr>
</tbody>
</table>

**show hostname**

**Description**

Shows the current host name.

**Example**

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
myswitch
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show images**

**Description**

Shows the current images.

**Example**

```
switch# show images
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Description
Shows information about the software in the primary and secondary images.

Example
Showing the primary and secondary images on a 6100 switch:

```
switch(config)# show images
--------------------
AOS-CX Primary Image
--------------------
Version : PL.10.06.0002E
Size : 243 MB
Date : 2020-11-25 22:00:47 PST
SHA-256 : 61fe9233b2c842e8ac1731ad46949bd63e269c5c72d69290932ef19c1ebb0730
--------------------
AOS-CX Secondary Image
--------------------
Version : PL.10.07.0000E-201-gba0c336
Size : 271 MB
Date : 2020-11-25 21:09:08 UTC
SHA-256 : 2fdfc646a8013efc7577958a4bab0fa54604086bad3f46e1c5d4e706b8b30ee
Default Image : primary
Boot Profile Timeout : 2 seconds
--------------------
Management Module 1/1 (Active)
--------------------
Active Image : primary
Service OS Version : PL.01.07.0003-internal
BIOS Version : PL.01.0001
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show module

show module

Description
Shows information about installed line modules and management modules.
Although this switch does not have removable modules, this command will still return information about the switch, referring to management modules and line modules.

Usage

Identifies and shows status information about the line modules and management modules that are installed in the switch.

To show the configuration information—if any—associated with that line module slot, use the `show running-configuration` command.

Status is one of the following values:

- **Active**: This is the active management module.
- **Deinitializing**: The switch is being deinitialized.
- **Diagnostic**: The switch is in a state used for troubleshooting.
- **Down**: The switch is physically present but is powered down.
- **Failed**: The switch has experienced an error and failed.
- **Initializing**: The switch is being initialized.
- **Present**: The switch hardware is installed in the chassis.
- **Ready**: The switch is available for use.
- **Updating**: A firmware update is being applied to the switch.

Examples

Showing all installed modules:

```
switch# show module
Management Modules
=======================
<table>
<thead>
<tr>
<th>Product</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>JL678A</td>
<td>6100F 24G 4SFP+ Swch</td>
<td>SG0ZKW600P</td>
<td>Active (local)</td>
</tr>
</tbody>
</table>

Line Modules
============
<table>
<thead>
<tr>
<th>Product</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>JL678A</td>
<td>6100F 24G 4SFP+ Swch</td>
<td>SG0ZKW600P</td>
<td>Ready</td>
</tr>
</tbody>
</table>
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show running-config**

show running-config [<FEATURE>] [all]

**Description**

Shows the current nondefault configuration running on the switch. No user information is displayed.

**Parameter** | **Description**
---|---
<FEATURE> | Specifies the name of a feature. For a list of feature names, enter the show running-config command, followed by a space, followed by a question mark (?).
all | Shows all default values for the current running configuration.

**Examples**

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX PL.10.06.0001-346-g56a12a8f4cf15
!export-password: default
  ntp enable
  !
  !
  !
  !
  ssh server vrf default
  vlan 1
  spanning-tree
  spanning-tree instance 1 vlan 1,2,4-10
  interface 1/1/1
    no shutdown
    vlan access 1
    portfilter 1/1/2-1/1/3

  interface 1/1/2
    no shutdown
    vlan access 1
  interface 1/1/3
    no shutdown
    vlan access 1
  interface 1/1/4
    no shutdown
    vlan access 1
  interface 1/1/5
    no shutdown
```
vlan access 1
interface 1/1/6
   no shutdown
   vlan access 1
interface 1/1/7
   no shutdown
   vlan access 1
interface 1/1/8
   no shutdown
   vlan access 1
interface 1/1/9
   no shutdown
   vlan access 1
interface 1/1/10
   no shutdown
   vlan access 1
interface 1/1/11
   no shutdown
   vlan access 1
interface 1/1/12
   no shutdown
   vlan access 1
interface 1/1/13
   no shutdown
   vlan access 1
interface 1/1/14
   no shutdown
   vlan access 1
interface 1/1/15
   no shutdown
   vlan access 1
interface 1/1/16
   no shutdown
   vlan access 1
interface vlan 1
   ip dhcp
snmp-server vrf default
snmp-server community public
snmp-server host 1.1.1.1 inform version v2c
snmp-server host 1.1.1.1 trap version v2c
snmpv3 context A vrf default

Showing the current running configuration in json format:

switch> show running-config json
Running-configuration in JSON:
{
   "Monitoring_Policy_Script": {
      "system_resource_monitor_mml.1.0": {
         "Monitoring_Policy_Instance": {
            "system_resource_monitor_mml.1.0/system_resource_monitor_mml.1.0.default": {
               "name": "system_resource_monitor_mml.1.0.default",
               "origin": "system",
               "parameters_values": {
               
```
Show the current running configuration without default values:

```
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX PL.10.06.0001-346-g56a12a8f4cf15
!export-password: default
!
!
ssh server vrf default
vlan 1
spanning-tree
interface 1/1/1
 no shutdown
 vlan access 1
interface 1/1/2
 no shutdown
 vlan access 1
interface 1/1/3
 no shutdown
 vlan access 1
interface 1/1/4
 no shutdown
 vlan access 1
interface 1/1/5
 no shutdown
 vlan access 1
interface 1/1/6
 no shutdown
 vlan access 1
interface 1/1/7
 no shutdown
 vlan access 1
interface 1/1/8
 no shutdown
 vlan access 1
interface 1/1/9
 no shutdown
 vlan access 1
interface 1/1/10
 no shutdown
 vlan access 1
```
interface 1/1/11
  no shutdown
  vlan access 1
interface 1/1/12
  no shutdown
  vlan access 1
interface 1/1/13
  no shutdown
  vlan access 1
interface 1/1/14
  no shutdown
  vlan access 1
interface 1/1/15
  no shutdown
  vlan access 1
interface 1/1/16
  no shutdown
  vlan access 1
interface vlan 1
  ip dhcp

!  !  !  !
https-server vrf default
switch#
switch#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show running-config current-context

Description

Shows the current non-default configuration running on the switch in the current command context.

Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (config) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance. Support for this command is provided for one level below the config context. For example, entering this command for a child of a
child of the **config** context not supported. If you enter the command on a child of the **config** context, the current configuration of that context and the children of that context are displayed.

- The **global configuration** (**config**) context. If you enter this command in the global configuration (**config**) context, it shows the running configuration of the entire switch. Use the `show running-configuration` command instead.

**Examples**

Showing the running configuration for the current interface:

```plaintext
switch(config-if)# show running-config current-context
interface 1/1/1
    no shutdown
description Example interface
vlan access 1
exit
```

Showing the current running configuration for the in-band management interface:

```plaintext
switch(config)# interface vlan 1
switch(config-if-vlan)#description IN-BAND Management Interface
switch(config-if-vlan)#ip dhcp
switch(config-if-vlan)#no shutdown
switch(config-if-vlan)#end
```

Showing the current running configuration for the in-band management interface without DHCP:

```plaintext
switch(config)# interface vlan 1
switch(config-if-vlan)#description IN-BAND Management Interface
switch(config-if-vlan)#no ip dhcp
switch(config-if-vlan)#ip address 192.168.10.1/24
switch(config-if-vlan)#no shutdown
switch(config-if-vlan)#end
```

Showing the running configuration for the external storage share named **nasfiles**:

```plaintext
switch(config-external-storage-nasfiles)# show running-config current-context
external-storage nasfiles
    address 192.168.0.1
    vrf default
    username nasuser
    password ciphertext AQBapalKj+XMsZumHEwIc9Ow5Z6Bh9rV+9ZtKDKzvbAABAAAB1CTrM=
type scp
directory /home/nas
enable
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config or a child of config. See Usage.</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show startup-config**

**show startup-config [json]**

**Description**

Shows the contents of the startup configuration.

Switches in the factory-default configuration do not have a startup configuration to display.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>json</td>
<td>Display output in JSON format.</td>
</tr>
</tbody>
</table>

**Examples**

Showing the startup-configuration in JSON format:

```
switch# show startup-config json
Startup configuration:
{
    "AAA_Server_Group": {
        "local": {
            "group_name": "local"
        },
        "none": {
            "group_name": "none"
        }
    },
    ...
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
**show system**

**Description**
Shows general status information about the system.

**Usage**
CPU utilization represents the average utilization across all the CPU cores. System Contact, System Location, and System Description can be set with the `snmp-server` command.

**Examples**
Showing system information:

```
switch(config)# show system
Hostname : switch
System Description : PL.10.xx.xxxxx
System Contact : 
System Location :
Vendor : Aruba
Product Name : JL678A 6100 24G 4SFP+ Swch
Chassis Serial Nbr : CN9ZKRD058
Base MAC Address : f860f0-c91160
AOS-CX Version : PL.10.xx.xxxxx
Time Zone : UTC
Up Time : 9 hours, 10 minutes
CPU Util (%) : 3
Memory Usage (%) : 15
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (-) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show system resource-utilization**

**Description**
Shows information about the usage of system resources such as CPU, memory, and open file descriptors.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon &lt;DAEMON-NAME&gt;</td>
<td>Shows the filtered resource utilization data for the process specified by &lt;DAEMON-NAME&gt; only.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.</td>
</tr>
</tbody>
</table>

**NOTE:**
For a list of daemons that log events, enter `show events -d ?` from a switch prompt in the manager (＃) context.

**Examples**

Showing all system resource utilization data:

```
switch# show system resource-utilization
System Resources:
 Processes: 147
 CPU usage(%): 12
 Memory usage(%): 13
 Open FD's: 4128
 mmc-type-a: Endurance utilization = 0-10%, Health = normal
 mmc-type-b: Endurance utilization = 0-10%, Health = normal
switch#
```

Showing the resource utilization data for the pmd process:

```
switch# show system resource-utilization daemon pmd
Process CPU Usage Memory Usage Open FD's
-----------------------------------------------
pmd 2 1 14
```

Showing resource utilization data when system resource utilization polling is disabled:

```
switch# show system resource-utilization
System resource utilization data poll is currently disabled
```

Showing resource utilization data for a line module:

```
switch# show system resource-utilization module 1/1
System Resource utilization for line card module: 1/1
 CPU usage(%): 0
 Memory usage(%): 35
 Open FD's: 512
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show tech

show tech [basic | <FEATURE>] [local-file]

Description

Shows detailed information about switch features by automatically running the show commands associated with the feature. If no parameters are specified, the show tech command shows information about all switch features. Technical support personnel use the output from this command for troubleshooting.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic</td>
<td>Specifies showing a basic set of information.</td>
</tr>
<tr>
<td>&lt;FEATURE&gt;</td>
<td>Specifies the name of a feature. For a list of feature names, enter the show tech command, followed by a space, followed by a question mark (?).</td>
</tr>
<tr>
<td>local-file</td>
<td>Shows the output of the show tech command to a local text file.</td>
</tr>
</tbody>
</table>

Usage

To terminate the output of the show tech command, enter Ctrl+C.

If the command was not terminated with Ctrl+C, at the end of the output, the show tech command shows the following:

- The time consumed to execute the command.
- The list of failed show commands, if any.

To get a copy of the local text file content created with the show tech command that is used with the local-file parameter, use the copy show-tech local-file command.

Example

Showing the basic set of system information:

```
switch# show tech basic
====================================================================================================
Show Tech executed on Wed Sep  6 16:50:37 2017
====================================================================================================
[Begin] Feature basic
====================================================================================================
******************************************************************************
Command : show core-dump all
******************************************************************************
no core dumps are present
```
Directing the output of the **show tech basic** command to the local text file:

```
switch# show tech basic local-file
Show Tech output stored in local-file. Please use 'copy show-tech local-file'
to copy-out this file.
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show usb**

**Description**

Shows the USB port configuration and mount settings.

**Examples**

If USB has not been enabled:

```
switch> show usb
Enabled: No
Mounted: No
```

If USB has been enabled, but no device has been mounted:
If USB has been enabled and a device mounted:

```
switch> show usb
Enabled: Yes
Mounted: No
```

```
switch> show usb
Enabled: Yes
Mounted: Yes
```

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

## Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show usb file-system**

```
show usb file-system [<PATH>]
```

### Description

Shows directory listings for a mounted USB device. When entered without the <PATH> parameter the top level directory tree is shown.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;PATH&gt;</td>
<td>Specifies the file path to show. A leading &quot;/&quot; in the path is optional.</td>
</tr>
</tbody>
</table>

### Usage

Adding a leading "/" as the first character of the <PATH> parameter is optional.

Attempting to enter ‘..’ as any part of the <PATH> will generate an invalid path argument error. Only fully-qualified path names are supported.

### Examples

Showing the top level directory tree:

```
switch# show usb file-system
/mnt/usb:
'System Volume Information' dir1
```
Showing available path options from the top level:

```
switch# show usb file-system /
total 64
drwxrwxrwx 2 32768 Jan 22 16:27 'System Volume Information'
drwxrwxrwx 3 32768 Mar  5 15:26 dir1
```

Showing the contents of a specific folder:

```
switch# show usb file-system /dir1
total 32
 drwxrwxrwx 2 32768 Mar  5 15:26 dir2
-rwxrwxrwx 1 0 Feb  5 18:08 test1

switch# show usb file-system dir1/dir2
total 0
-rwxrwxrwx 1 0 Feb  6 05:35 test2
```

Attempting to enter an invalid character in the path:

```
switch# show usb file-system dir1/../../
Invalid path argument
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show version**

show version

**Description**
Shows version information about the network operating system software, service operating system software, and BIOS.

**Example**

Showing version information:

```
switch(config)# show version
```

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**system resource-utilization poll-interval**

`system resource-utilization poll-interval <SECONDS>`

**Description**

Configures the polling interval for system resource information collection and recording such as CPU and memory usage.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Example**

Configuring the system resource utilization poll interval:

```
switch(config)# system resource-utilization poll-interval 20
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**top cpu**

top cpu

**Description**

Shows CPU utilization information.

**Example**

Showing top CPU information:

```
switch# top cpu
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks: 76 total, 2 running, 74 sleeping, 0 stopped, 0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total, 2487508 free, 897040 used, 661948 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 2859196 avail Mem

    PID USER      NI VIRT  RES   SHR S %CPU %MEM    TIME+  COMMAND
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**top memory**

top memory

**Description**
Shows memory utilization information.

Example
Showing top memory:

```
switch> top memory
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks: 76 total, 2 running, 74 sleeping, 0 stopped, 0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 0.4 wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total, 2487508 free, 897040 used, 661948 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 2859196 avail Mem

   PID USER      PRI  NI VIRT  RES  SHR %CPU %MEM    TIME+  COMMAND
...
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**usb**

`usb`

`no usb`

Description
Enables the USB ports on the switch. This setting is persistent across switch reboots and management module failovers. Both active and standby management modules are affected by this setting.
The no form of this command disables the USB ports.

Example
Enabling USB ports:

```
switch(config)# usb
```

Disabling USB ports when a USB drive is mounted:

```
switch(config)# no usb
```

Command History
### usb mount | unmount

**Description**
Enables or disables the inserted USB drive.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mount</td>
<td>Enables the inserted USB drive.</td>
</tr>
<tr>
<td>unmount</td>
<td>Disables the inserted USB drive in preparation for removal.</td>
</tr>
</tbody>
</table>

**Usage**
If USB has been enabled in the configuration, the USB port on the active management module is available for mounting a USB drive. The USB port on the standby management module is not available.
An inserted USB drive must be mounted each time the switch boots or fails over to a different management module.
A USB drive must be unmounted before removal.
The supported USB file systems are FAT16 and FAT32.

**Examples**
Mounting a USB drive in the USB port:

```
switch# usb mount
```

Unmounting a USB drive:

```
switch# usb unmount
```
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Chapter 16
Support and Other Resources

Accessing Aruba Support

<table>
<thead>
<tr>
<th>Support and Other Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba Support Services</td>
</tr>
<tr>
<td>North America telephone</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>International telephone</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Other useful sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airheads social forums and Knowledge Base</td>
</tr>
<tr>
<td><a href="https://community.arubanetworks.com/">https://community.arubanetworks.com/</a></td>
</tr>
<tr>
<td>Software licensing</td>
</tr>
<tr>
<td><a href="https://lms.arubanetworks.com/">https://lms.arubanetworks.com/</a></td>
</tr>
<tr>
<td>End-of-Life information</td>
</tr>
<tr>
<td><a href="https://www.arubanetworks.com/support-services/end-of-life/">https://www.arubanetworks.com/support-services/end-of-life/</a></td>
</tr>
<tr>
<td>Aruba software and documentation</td>
</tr>
<tr>
<td><a href="https://asp.arubanetworks.com/downloads">https://asp.arubanetworks.com/downloads</a></td>
</tr>
<tr>
<td>Aruba Developer Hub</td>
</tr>
<tr>
<td><a href="https://developer.arubanetworks.com/">https://developer.arubanetworks.com/</a></td>
</tr>
</tbody>
</table>

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

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.