AOS-W Instant 8.7.0.x Command-Line Interface

Alcatel·Lucent Enterprise

Reference Guide

Copyright Information

Open Source Code

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

AOS-W Instant Command-Line Interface

The Alcatel-Lucent AOS-W Instant Command-Line Reference Guide allows you to configure and manage OAW-IAPs. The CLI is accessible through a Telnet or SSH session from a remote management console or workstation.

What's New In AOS-W Instant 8.7.0.0

This section lists the commands introduced, modified, or deprecated in Alcatel-Lucent AOS-W Instant 8.7.0.0.

Commands in AOS-W Instant 8.7.0.0

New Commands

The following new commands are introduced in Alcatel-Lucent AOS-W Instant 8.7.0.0:

Table 2: *New Commands in AOS-W Instant 8.7.0.0*

Command	Description
airslice-policy	This command optimizes the quality of communication for applications.
application-monitoring	This command enables traffic monitoring for applications.
ap-poe-power-optimization	This command allows you to enable or disable the low power mode configuration on the AP.
ca-bundle	This command enables the update and reset of CA certificate bundle.
crypto pki-import	This command imports and installs certificates on the AP.
crypto pki-remove	This command removes imported certificates on the AP.
debug-cloud-server	This command is allows you to debug connections between AP and the server.
disable-factory-reset	A new configuration command is introduced to disable the reset to factory default settings function when the AP is operational.
dot1x eap-frag-mtu	This command configures the IP MTU to be considered for EAP fragmentation.
est-activate	This command is used to activate an EST profile on the AP.
est profile	Configures a new EST profile on the AP. The EST profile allows the automatic enrollment and re-enrollment of customized certificates on the OAW-IAP.

Table 2: *New Commands in AOS-W Instant 8.7.0.0*

Command	Description
itm	This command configures Intelligent Thermal Management for the AP.
mesh-cluster	Allows the user to configure multiple mesh cluster profiles on the OAW-IAP and assign a priority to each profile.
mesh-split5g-band-range	This command allows you to configure the 5 GHz radio used for mesh link in dual 5GHz and split 5 GHz enables access points.
show ap debug airslice client-stats	This command displays the application usage statistics of a single client based on its MAC address and DPI ID.
show ap debug ble-input-filter-stats	This command displays the input-filter information in the BLE table.
show ap debug zigbee socket-table	This command displays the zigbee socket information in the BLE table.
show ap mesh link show ap mesh neighbors	The output of these commands includes a new column called **AP Name**.
show app-monitoring	This command lists the applications supported on the OAW-IAP.
show-ca-bundle	This command displays the version details of the CA certificate bundle installed on the AP.
show cert-from-server	This command displays the certificate chain received from the server during SSL handshake.
show cert assignment	This command displays the certificate assignment details of the AP.
show est status	This command displays the EST status of the active EST profiles.
show log ucm	This command displays the log of UCM processes on the AP.
show ucm cdrs	This command displays UCM call data records stored on the AP.
show usb	This command displays the detailed USB device information on an OAW-IAP.
show zigbee service-profile	This command shows the ZigBee service profile.
show zigbee socket-device-profile	This command shows the ZigBee socket device profile(s).
ucm-logging	This command enables logging of UCM processes on the AP.
usb acl-profile	This command is used to create a AP USB ACL profile.

Table 2: *New Commands in AOS-W Instant 8.7.0.0*

Command	Description
usb profile	This command is used to create a AP USB profile.
usb-profile-binding	This command is used to bind the AP USB profile.
wlan mesh-profile	This command allows you to configure mesh profile for the AP.
wlan cert-assignment-profile	This command assigns installed certificates to specific applications running on the AP.
wlan mpsk-local	This command configures a local MPSK profile on the AP.
zigbee service-profile	This command configures or modifies a ZigBee service profile.
zigbee socket-device-profile	This command configures or modifies a ZigBee socket device profile.
zigbee use-service-profile	This commands sets a zigbee service profile on an OAW-IAP

Modified Commands

The following commands are modified in Alcatel-Lucent AOS-W Instant 8.7.0.0:

Table 3: *Modified Commands in Alcatel-Lucent AOS-W Instant 8.7.0.0*

Command	Description
ble-init-action	The following parameters were introduced: ■ input-filter-enable ■ input-filter-disable
hostname	The number of ASCII characters allowed in the OAW-IAP is increased from 32 to 128 characters.
he-min-snr <snr> show arm config show ap client-viewshow ap client-match-ssid-table show ap client-match-ssid-table	The **client-match he-min-snr** parameter is introduced to configure the minimum SNR value required for the targeted HE (802.11ax) steering. The outputs of the relevant show commands have been enhanced to include the HE capability of the AP.
ids	Two new parameters, **ap-max-unseen-timeout** and **valid-ap-max-unseen-timeout**, were added.
iot transportProfile	■ When the meridian asset tracking endpoint is configured and the firmware is upgraded to AOS-W Instant 8.7.0.0, the CA certificate should be uploaded in order to connect to the meridian server. The following parameters were introduced: ■ **ZSDFilter** ■ **data-filter** The following payload content were introduced: ■ **wiliot** ■ **exposure-notification**

Table 3: *Modified Commands in Alcatel-Lucent AOS-W Instant 8.7.0.0*

Command	Description
	- **zsd** - **serial-data**
rf dot11a-radio-profile rf dot11a-secondary-radio-profile rf dot11g-radio-profile	The following parameters to configure ARM settings were added: **backoff-time <secs>** **channel-quality-aware-arm-disable** **channel-quality-threshold** **channel-quality-wait-time** **error-rate-threshold <percent>** **error-rate-wait-time <secs>** **ideal-coverage-index <idx>** **scanning-disable**
show access-rule	The output of this command was modified to include the **CustomApp** column.
show ap checksum	The output of this command was modified to include the number of imported certificates and WebCC certificates on the AP.
show ap debug airwave-config-received	The output of the command was modified to display the last six batches of configurations received from the management platform.
show ap ids show ap debug am-configshow ap debug am-config	The configuration values of **Valid AP Unseen Timeout** and **AP Unseen Timeout** are added to the output of this command.
show ap mesh cluster	A new parameter, **active**, was added and the output of **show ap mesh cluster topology** command was modified to include per-radio topology information.
show ap mesh link show ap mesh neighbors	The output of these commands were modified to include the radio information of mesh APs.
show datapath	The output of the **show datapath session** command was modified to include the following columns: InnerAppID PktsAppMoni
show iot transportProfile	The following parameters were included in the output: - **ZSDFilter** - **DataFilter** The following payload content were included in the output: - **wiliot** - **exposure-notification**
show log ap-debug	The output of this command was modified to include server labels for logs related to server processes.

Table 3: *Modified Commands in Alcatel-Lucent AOS-W Instant 8.7.0.0*

Command	Description
show wifi-uplink	The **IP address**, **Subnet mask**, and **Gateway** information of the layer-3 network are added to the output of this command.
wlan access-rule	The **rule desc <description>** parameter is added to allow users to insert a comment to identify the purpose of the access rule. The **rule markapp <custom1.......custom5>** parameter is added to configure a custom application ID.
wlan access-list session	The **rule markapp <custom1.......custom5>** parameter was added to configure a custom application ID.
wlan ssid-profile	The functionality of **advertise-ap-name** parameter was modified to advertise the ap-name in probe responses. The **radius-interim-accounting-interval <minutes>** parameter was modified to include an additional **{<seconds>}** definition.

About This Guide

This document describes the AOS-W Instant command syntax and provides the following information for each command:

- Command Syntax—The complete syntax of the command.
- Description—A brief description of the command.
- Syntax—A description of the command parameters, the applicable ranges and default values, if any.
- Usage Guidelines—Information to help you use the command, including prerequisites, prohibitions, and related commands.
- Example—An example of how to use the command.
- Command History—The version of AOS-W Instant in which the command was first introduced.
- Command Information—This table describes command modes and platforms for which this command is applicable.

The commands are listed in alphabetical order.

AOS-W Instant CLI

AOS-W Instant supports the use of CLI for scripting purposes. You can access the AOS-W Instant CLI through a SSH.

To enable the SSH access to the AOS-W Instant CLI:

1. From the WebUI, navigate to **System** > **Show advanced options**.
2. Select **Enabled** from the **Terminal access** drop-down list.
3. Click **OK**.

Connecting to a CLI Session

On connecting to a CLI session, the system displays its host name followed by the login prompt. Use the administrator credentials to start a CLI session. For example:

```
(Instant AP)
User: admin
Password: *****
```

If the login is successful, the privileged command mode is enabled and a command prompt is displayed. For example:

```
(Instant AP)#
```

The privileged mode provides access to **show**, **clear**, **ping**, **traceroute**, and **commit** commands. The configuration commands are available in the configuration (config) mode. To move from privileged mode to the configuration mode, enter the following command at the command prompt:

```
(Instant AP)# configure terminal
```

The configure terminal command allows you to enter the basic configuration mode and the command prompt is displayed as follows:

```
(Instant AP)(config)#
```

The AOS-W Instant CLI allows CLI scripting in several other sub-command modes to allow the users to configure individual interfaces, SSIDs, access rules, and security settings.

You can use the question mark (?) to view the commands available in a privileged mode, configuration mode, or sub-mode.

NOTE

Although automatic completion is supported for some commands such as **configure terminal**, the complete **exit** and **end** commands must be entered at command prompt for successful execution.

Applying Configuration Changes

Each command processed by the Virtual Controller is applied on all the slave OAW-IAPs in a cluster. When you make configuration changes on a master OAW-IAP in the CLI, all associated OAW-IAPs in the cluster inherit these changes and subsequently update their configurations. The changes configured in a CLI session are saved in the CLI context.

The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session: therefore, Alcatel-Lucent recommends that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, use the following command in the privileged mode:

```
(Instant AP)# commit apply
```

To apply the configuration changes to the cluster, without saving the configuration, use the following command in the privileged mode:

```
(Instant AP)# commit apply no-save
```

To view the changes that are yet to be applied, use the following command in the privileged mode:

```
(Instant AP)# show uncommitted-config
```

To revert to the earlier configuration, use the following command in the privileged mode.

```
(Instant AP)# commit revert
```

Example:

```
(Instant AP)(config)# rf dot11a-radio-profile

(Instant AP)# show uncommitted-config
```

Configuration Sub-modes

Some commands in configuration mode allow you to enter into a sub-mode to configure the commands specific to that mode. When you are in a configuration sub-mode, the command prompt changes to indicate the current sub-mode.

You can exit a sub-command mode and return to the basic configuration mode or the privileged Exec (enable) mode at any time by executing the **exit** or **end** command.

Deleting Configuration Settings

Use the **no** command to delete or negate previously-entered configurations or parameters.

- To view a list of no commands, type **no** at the prompt in the relevant mode or sub-mode followed by the question mark. For example:

  ```
  (Instant AP)(config) # no?
  ```

- To delete a configuration, use the **no** form of a configuration command. For example, the following command removes a configured user role:

  ```
  (Instant AP)(config) # no user <username>
  ```

- To negate a specific configured parameter, use the **no** parameter within the command. For example, the following command deletes the PPPoE user configuration settings:

  ```
  (Instant AP)(config) # pppoe-uplink-profile
  (Instant AP)(pppoe_uplink_profile)# no pppoe-username
  ```

Using Sequence Sensitive Commands

The AOS-W Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, Alcatel-Lucent recommends that you remove the existing configuration before adding or modifying the configuration details for sequence-sensitive commands. You can either delete an existing profile or remove a specific configuration by using the **no…** commands.

The following table lists the sequence-sensitive commands and the corresponding **no** command to remove the configuration.

Table 4: *Sequence-Sensitive Commands*

Sequence-Sensitive Command	Corresponding no command
rule <dest> <mask> <match> <protocol> <start-port> <end-port> {permit |deny | src-nat | dst-nat {<IP-address> <port>| <port>}}[<option1…option9>]	`no rule <dest> <:mask> <match> <protocol> <start-port> <end-port> {permit | deny | src-nat | dst-nat}`
mgmt-auth-server <auth-profile-name>	`no mgmt-auth-server <auth-profile-name>`

set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <role>| value-of}	`no set-role <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}`
	`no set-role`

set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator> <VLAN-ID>| value-of}	`no set-vlan <attribute>{{equals| not-equals| starts-with| ends-with| contains} <operator>| value-of}`
	`no set-vlan`

auth-server <name>	no auth-server <name>

Saving Configuration Changes

The *running-config* holds the current OAW-IAP configuration, including all pending changes which are yet to be saved. To view the running-config of an OAW-IAP, use the following command:

```
   (Instant AP) # show running-config
```

When you make configuration changes through the CLI, the changes affect the current running configuration only. To save your configuration changes, use the following command in the privileged Exec mode:

```
(Instant AP)# write memory
```

Commands that Reset the OAW-IAP

If you use the CLI to modify a currently provisioned radio profile, the changes take place immediately. A reboot of the OAW-IAP is not required to apply the configuration changes. Certain commands, however, automatically force OAW-IAP to reboot. Verify the current network loads and conditions before executing the commands that enforce a reboot of the OAW-IAP, as they may cause a momentary disruption in service as the unit resets.

The `reload` command resets an OAW-IAP.

Command Line Editing

The system records your most recently entered commands. You can review the history of your actions, or reissue a recent command easily, without having to retype it.

To view items in the command history, use the *up* arrow key to move back through the list and the *down* arrow key to move forward. To reissue a specific command, press **Enter** when the command appears in the command history. You can also use the command line editing feature to make changes to the command prior to entering it. The command line editing feature allows you to make corrections or changes to a command without retyping. The following table lists the editing controls. To use key shortcuts, press and hold the **Ctrl** button while you press a letter key.

Table 5: *Line Editing Keys*

Key	Effect	Description
Ctrl A	Home	Move the cursor to the beginning of the line.
Ctrl B or the left arrow	Back	Move the cursor one character left.
Ctrl D	Delete Right	Delete the character to the right of the cursor.
Ctrl E	End	Move the cursor to the end of the line.
Ctrl F or the right arrow	Forward	Move the cursor one character right.
Ctrl K	Delete Right	Delete all characters to the right of the cursor.
Ctrl N or the down arrow	Next	Display the next command in the command history.
Ctrl P or up arrow	Previous	Display the previous command in the command history.
Ctrl T	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
Ctrl U	Clear	Clear the line.
Ctrl W	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
Ctrl X	Delete Left	Delete all characters to the left of the cursor.

Specifying Addresses and Identifiers in Commands

This section describes addresses and other identifiers that you can reference in CLI commands.

Table 6: *Addresses and Identifiers*

Address or Identifier	Description
IP address	For any command that requires entry of an IP address to specify a network entity, use IPv4 network address format in the conventional dotted decimal notation (for example, 192.0.2.1).
Netmask address	For subnet addresses, specify a subnet mask in dotted decimal notation (for example, 255.255.255.0).
MAC address	For any command that requires entry of a device’s hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
SSID	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).
BSSID	This entry is the unique hard-wireless MAC address of the OAW-IAP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP. Use the same format as for a MAC address.
ESSID	Typically the unique logical name of a wireless network. If the ESSID includes spaces, enclose the name in quotation marks.

Typographic Conventions

The following conventions are used throughout this document to emphasize important concepts:

Table 7: *Typographical Conventions*

Type Style	Description
Italics	This style is used for emphasizing important terms and to mark the titles of books.
Boldface	This style is used for command names and parameter options when mentioned in the text.
`Commands`	This fixed-width font depicts command syntax and examples of commands and command output.
`<angle brackets>`	In the command syntax, text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example, ping <ipaddr> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.
`[square brackets]`	In the command syntax, items enclosed in brackets are optional. Do not type the brackets.
`{Item_A|Item_B}`	In the command examples, single items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.
`{ap-name <ap-name>}|{ipaddr <ip-addr>}`	Two items within curled braces indicate that both parameters must be entered together. If two or more sets of curled braces are separated by a vertical bar, like in the example to the left, enter only one choice. Do not type the braces or bars.

The following informational icons are used throughout this guide:

NOTE

Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION

Indicates a risk of damage to your hardware or loss of data.

WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 8: *Contact Information*

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact Center Telephone	
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

a-channel

```
a-channel <a_channel> <a_tx_power>
```

Description

This command configures 5 GHz radio channels for a specific OAW-IAP.

Syntax

Parameter	Description	Range	Default
`<channel>`	Configures the specified 5 GHz channel.	The valid channels for a band are determined by the OAW-IAP regulatory domain.	—
`<tx-power>`	Configures the specified transmission power values. It also supports 0.1 dBm and negative values.	-51 dBm to 51 dBm	—

Usage Guidelines

Use this command to configure radio channels for the 5 GHz band for a specific OAW-IAP.

Example

The following example configures the 5 GHz radio channel:

```
(Instant AP)# a-channel 44 18
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

a-external-antenna

```
a-external-antenna <gain>
```

Description

This command configures external antenna connectors for an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`<gain>`	Configures the antenna gain. You can configure a gain value in dBi for the following types of antenna: ■ Dipole or Omni ■ Panel ■ Sector	Diploe or Omni - 6 Panel -14 Sector - 14	—

Usage Guidelines

If your OAW-IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the OAW-IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your OAW-IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the OAW-IAP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 9: *Formula Variable Definitions*

Formula Element	Modification
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

For information on antenna gain recommended by the manufacturer, see .

Example

The following example configures external antenna connectors for the OAW-IAP with the 5 GHz radio band.

```
(Instant AP)# a-external-antenna 14
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

aaa test-server

```
aaa test-server <servername> username <username> password <passwd> auth-type <type>
```

Description

This command tests a configured authentication server.

Syntax

Parameter	Description	Range	Default
`<servername>`	Authentication server for which the authentication test must be run.	—	—
`username <username>`	Username to use to test the authentication server.	—	—
`password <passwd>`	Password to use to test the authentication server.	—	—
`auth-type <type>`	Authentication protocol type. Use PAP as the authentication type.	—	—

Usage Guidelines

This command verifies the status of RADIUS authentication between the OAW-IAP and RADIUS or AAA server.

Example

The following example shows the output of the **aaa test-server** command:

```
Authentication is successful
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

aaa dns-query-interval

```
aaa dns-query-interval <interval>
no aaa dns-query-interval
```

Description

This command configures the interval at which the dns server sends out a query.

Syntax

Parameter	Description	Range	Default
`<interval>`	The time interval at which the query must be sent. The interval is ranged in minutes.	0-60 mins	15 mins

Usage Guidelines

Use this command to configure the time interval for sending out dns queries.

Example

The following example shows the output of the **aaa dns-query-interval** command:

```
20:4c:03:24:89:18 (config) # aaa dns-query-interval 15
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

aaa radius-attributes

```
aaa radius-attributes add <attribute> <attribute-id> {date|integer|ipaddr|string} [vendor
<name> <vendor-id>]
```

Description

This command configures RADIUS attributes to statically configure values to be included in RADIUS Access-Requests and Accounting-Requests.

Syntax

Parameter	Description
`add <attribute> <attribute-id>`	Adds the specified attribute name (alphanumeric string), associated attribute ID (integer), and type (date, integer, IP address, or string).
`date`	Adds a date attribute.
`integer`	Adds an `integer` attribute.
`ipaddr`	Adds an IP address attribute.
`string`	Adds a string attribute.
`vendor`	(Optional) Display attributes for a specific vendor name and vendor ID.

Usage Guidelines

Add RADIUS attributes for use in SDRs. Use the **show aaa radius-attributes** command to display a list of the current RADIUS attributes recognized by the Mobility Master. To add a RADIUS attribute to the list, use the **aaa radius-attributes** command.

Example

The following command adds the VSA AOS-W Instant-User-Role:

```
(host) (config)# aaa radius-attributes add AOS-W Instant-User-Role 1 string vendor AOS-W
Instants 14823
```

Command History

Release	Modification
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

aaa radius modifier

```
aaa radius-attributes modifier <profile_name>
```

Description

This command configures the RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server.

Syntax

Parameter	Description
`<profle_name>`	The specified RADIUS modifier profile name
`clone`	Copy data from another Radius Modifier Profile
`exclude`	Attribute to be excluded in RADIUS request
`include`	Attribute/Value to be included in RADIUS request
`no`	Delete Command

Usage Guidelines

Use the **show aaa radius modifier** command to display a list of RADIUS modifier profiles . To create a RADIUS modifier profile with customized attributes, use the **aaa radius-attributes** command.

Example

Example for Included attribute

```
(host) [md](config) #aaa radius-attributes add BW-Area-Code 18 integer vendor Boingo 22472
   (host) [md](Radius Modifier Profile "radmodifier1") # include BW-Area-Code static "212"
   (host) [md](Radius Modifier Profile "radmodifier1") # no include BW-Area-Code
```

Example for excluded attribute

```
(host) (config) #aaa radius-attributes add BW-Area-Code 18 integer vendor Boingo 22472
   (host) (Radius Modifier Profile "radmodifier1") # exclude BW-Area-Code
   (host) (Radius Modifier Profile "radmodifier1") # no exclude BW-Area-Code
```

Example for modified attribute

Default attributes to carry to radius server can be modified with include option.

```
(host) Radius Modifier Profile "radmodifier1") # include "Aruba-location-id" static "Shim-
office"
```

Command History

Version	Modification
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

aeroscout-rtls

```
aeroscout-rtls <addr> <Port> [include-unassoc-sta]
no…
```

Description

This command configures the Aeroscout RTLS settings for AOS-W Instant and sends the RFID tag information to an Aeroscout RTLS server.

Syntax

Parameter	Description	Range	Default
`<addr>`	IP address of the Aeroscout RTLS server to which the location reports are sent.	—	—
`<Port>`	Port number of the Aeroscout RTLS server to which the location reports are sent..	—	—
`include-unassoc-stas`	Includes the client stations not associated to any OAW-IAP when mobile unit reports are sent to the Aeroscout RTLS server.	—	Disabled
`no`	Removes the Aeroscout RTLS configuration.	—	—

Usage Guidelines

This command allows you to integrate Aeroscout RTLS server with AOS-W Instant by specifying the IP address and port number of the Aeroscout RTLS server. When enabled, the RFID tag information for the stations associated with an OAW-IAP are sent to the AeroScout RTLS. You can also send the RFID tag information for the stations that are not associated with any OAW-IAP.

Example

The following example configures the Aeroscout RTLS server:

```
(Instant AP)(config)# aeroscout-rtls 192.0.2.2 3030 include-unassoc-sta
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

a-ant-pol

```
a-ant-pol <pol>
```

Description

This command configures the antenna polarization value for 5 GHz radio channels.

Syntax

Parameter	Description	Range	Default
`<pol>`	Denotes the antenna polarization value for 5 GHz radio channel. ■ 0: Co-Polarized radio ID ■ 1: Cross-Polarized radio ID	0 or 1	—

Usage Guidelines

Use this command to set the antenna polarization value for 5 GHz radio channel.

Example

The following example configures the antenna polarization value for a 5 GHz radio channel:

```
(Instant AP)# a-ant-pol 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.2.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

activate-disable

```
activate-disable
no…
```

Description

This command disables all communication between OAW-IAP and Activate during initial provisioning.

Syntax

Parameter	Description	Range	Default
`activate-disable`	Disables communication between the OAW-IAP and Activate.	—	Disabled
`no…`	Removes the configuration and enables communication between the AP and Activate.	–	–

Usage Guidelines

This is primarily used by customers who do not use Activate because of their security policy or because it is a new site and they do not have internet connectivity when the OAW-IAP is initially brought up.

Example

The following command disables communication between the OAW-IAP and Activate:

```
(Instant AP)(config)# activate-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

advanced-zone

```
advanced-zone
no...
```

Description

This command is used to enable or disable the advanced zone feature that can configure up to 32 SSIDs. Since the mapping method of the WLAN index and BSSID index are different, when you change the advanced zone configuration, the BSSID is removed and created again.

When advanced zone is enabled:

- The WLAN SSID profile will remain inactive without the zone.
- Configure the OAW-IAP zone. Otherwise, keep the WLAN SSIDs inactive.
- A zone can be assigned to a maximum of up to 16 SSIDs. However, if the extended SSID is disabled, a zone can be assigned to a maximum of up to 14 SSIDs wherein the first two virtual APs are reserved for mesh.

Example

```
(Instant AP)(config)# advanced-zone
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

airgroup

```
airgroup
   cppm
   cppm-query-interval
   cppm-server
   disable
   enable
   enable-guest-multicast
   multi-swarm
   no
```

Description

This command configures the AirGroup settings on an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`cppm`	Enforces the discovery of the ClearPass Policy Manager registered devices. When enabled, only devices registered with ClearPass Policy Manager will be discovered by Bonjour® or DLNA devices, based on the ClearPass Policy Manager policy configured.	—	Enabled
`cppm-query-interval <interval>`	Configures a time interval at which AOS-W Instant sends a query to ClearPass Policy Manager for mapping the access privileges of each device to the available services.	1-24	10 hours
`cppm-server <server-name>`	Configures the ClearPass Policy Manager server information for AirGroup policy.	—	—
`disable`	Disables the AirGroup feature.	—	—
`enable [dlna-only| mdns-only]`	Enables the mDNS or DLNA or both. When **dlna-only** command is executed with **enable**, the DLNA support is enabled for AirGroup enabled devices. When **mdns-only** command is executed with **enable**, the Bonjour support is enabled for AirGroup enabled devices.	—	—
`enable-guest-multicast`	Allows the users to use the Bonjour or DLNA services enabled in a guest VLAN. When enabled, the Bonjour or DLNA devices will be visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.	—	—

Parameter	Description	Range	Default
`multi-swarm`	Enables inter cluster mobility. When enabled, the OAW-IAP shares the mDNS database information with the other clusters. The AirGroup records in the Virtual Controller can be shared with all the Virtual Controllers specified for L3 Mobility.	—	Disabled
`no…`	Removes the configuration settings for parameters under the **airgroup** command.	—	—
`no airgroup`	Removes the AirGroup configuration.	—	—

Usage Guidelines

Use this command to configure the AirGroup, the availability of the AirGroup services, and ClearPass Policy Manager servers.

Example

The following example configures an AirGroup profile:

```
(Instant AP)(config)# airgroup
(Instant AP)(airgroup)# enable
(Instant AP)(airgroup)# cppm enforce-registration
(Instant AP)(airgroup)# cppm-server Test
(Instant AP)(airgroup)# cppm-query-interval 10
(Instant AP)(airgroup)# enable-guest-multicast
(Instant AP)(airgroup)# multi-swarm
(Instant AP)(airgroup)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and AirGroup configuration sub-mode.

airgroupservice

```
airgroupservice <airgroupservice>
   description <description>
   disable
   disallow-role <role>
   disallow-vlan <VLAN-ID>
   enable
   id <AirGroupservice-ID>
   no
```

Description

This command configures the availability of AirGroup services for the OAW-IAP clients.

Syntax

Parameter	Description	Range	Default
`<airgroupservice>`	Specifies the AirGroup service to configure. The following pre-configured services are available for OAW-IAP clients: ■ AirPlay™— Apple® AirPlay allows wireless streaming of music, video, and slideshows from your iOS device to Apple TV® and other devices that support the AirPlay feature. ■ AirPrint™— Apple® AirPrint allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint compatible printers. ■ iTunes— iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple® devices. ■ RemoteMgmt— Use this service for remote login, remote management, and FTP utilities on Apple® devices. ■ Sharing— Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple® devices. ■ ChromeCast—ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high definition television by streaming content through Wi-Fi from the Internet or local network. ■ DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device. ■ DLNA Print—This service is used by printers that support DLNA. You can allow all services or add custom services. Up to 10 services can be configured on an OAW-IAP.	–	—

Parameter	Description	Range	Default
`description <description>`	Adds a description to the AirGroup service profile.	–	—
`disable`	Disables AirGroup services for the profile.	–	—
`disallow-role <role>`	Restricts the user roles specified for role from accessing the AirGroup service.	–	Disabled
`disallow-vlan <VLAN-ID>`	Restricts the AirGroup servers connected on the specified VLANs from being discovered.	–	Disabled
`enable`	Enables the AirGroup service for the profile.	–	—
`id <airgroupserviceid>`	Allows you to specify the AirGroup service ID corresponding to the service that you are trying to configure. **NOTE:** The service IDs cannot be added for the pre-configured services.	–	—
`no…`	Removes the AirGroup service configuration.	–	—

Usage Guidelines

Use this command to enforce AirGroup service policies and define the availability of a services for an AirGroup profile. When configuring AirGroup service for an AirGroup profile, you can also restrict specific user roles and VLANs from availing the AirGroup services.

Example

The following example configures AirGroup services:

```
(Instant AP)(config)# airgroupservice AirPlay
(Instant AP)(airgroup-service)# description AirPlay Service
(Instant AP)(airgroup-service)# disallow-role guest
(Instant AP)(airgroup-service)# disallow-vlan 200
(Instant AP)(airgroup-service)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	The AirGroup chat service was deprecated.
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and AirGroup services configuration sub-mode.

airslice-policy

```
airslice-policy
```

Description

This command optimizes the quality of communication for applications.

Example

The following example configures airslice policy on an OAW-IAP:

```
(Instant AP)(config)# airslice-policy
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-530 Series and OAW-AP555 access points	Configuration mode.

airwave-rtls

```
airwave-rtls <addr> <Port> <key> <frequency> [include-unassoc-sta]
no…
```

Description

This command integrates OmniVista 3600 Air Manager RTLS settings for AOS-W Instant and sends the RFID tag information to an OmniVista 3600 Air Manager RTLS server with the RTLS feed to accurately locate the wireless clients.

Syntax

Parameter	Description	Range	Default
`<addr>`	Configures the IP address of the OmniVista 3600 Air Manager RTLS server.	—	—
`<Port>`	Configures the port for the OmniVista 3600 Air Manager RTLS server.	—	—
`<key>`	Configures key for service authorization.	—	—
`<frequency>`	Configures the frequency at which packets are sent to the RTLS server in seconds.	—	5
`include-unassoc-sta`	When enabled, this option sends mobile unit reports to the OmniVista 3600 Air Manager RTLS server for the client stations that are not associated to any OAW-IAP (unassociated stations).	—	Disabled
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to send the RFID tag information to OmniVista 3600 Air Manager RTLS. Specify the IP address and port number of the OmniVista 3600 Air Manager server, to which the location reports must be sent. You can also send reports of the unassociated clients to the RTLS server for tracking purposes.

Example

The following command enables OmniVista 3600 Air Manager RTLS:

```
(Instant AP)(config) # airwave-rtls ams-ip 192.0.2.3 3030 pass@1234 5 include-unassoc-sta
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ale-report-interval

```
ale-report-interval <seconds>
no…
```

Description

This command configures the interval at which an OAW-IAP sends data to the ALE server.

Syntax

Parameter	Description	Range	Default
`ale-report-interval <seconds>`	Configures an interval at which the Virtual Controller can report the OAW-IAP and client details to the ALE server.	6–60 seconds	30
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to specify an interval for OAW-IAP and ALE server communication.

Example

The following example configures the ALE server details:

```
(Instant AP)(config)# ale-report-interval 60
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ale-server

```
ale-server <server>
  no…
```

Description

This command configures ALE server details for OAW-IAP integration with ALE.

Syntax

Parameter	Description	Range	Default
`ale-server <server>`	Allows you to specify the FQDN or IP address of the ALE server.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to enable an OAW-IAP for ALE support.

Example

The following example configures the ALE server details:

```
(Instant AP)(config)# ale-server AleServer1
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

alg

```
alg
  sccp-disable
  sip-disable
  ua-disable
  vocera-disable
  no…
```

Description

This command allows you to modify the configuration settings for ALG protocols enabled on an OAW-IAP. An application-level gateway consists of a security component that augments a firewall or NAT used in a network.

Syntax

Parameter	Description	Range	Default
`sccp-disable`	Disables the SCCP.	—	Enabled
`sip-disable`	Disables the SIP for VOIP and other text and multimedia sessions.	—	Enabled
`ua-disable`	Disables the Alcatel-Lucent NOE protocol.	—	Enabled
`vocera-disable`	Disables the VOCERA protocol.	—	Enabled
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to functions such as SIP, Vocera, and Cisco Skinny protocols for ALG.

Example

The following example configures the ALG protocols:

```
(Instant AP)(config)# alg
(Instant AP)(ALG)# sccp-disable
(Instant AP)(ALG)# no sip-disable
(Instant AP)(ALG)# no ua-disable
(Instant AP)(ALG)# no vocera-disable
(Instant AP)(ALG)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and ALG configuration sub-mode.

allow-new-aps

```
allow-new-aps
no…
```

Description

This command allows the new access points to join the OAW-IAP cluster.

Syntax

Parameter	Description	Range	Default
`allow-new-aps`	Allows new access points in the domain.	—	—
`no`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to allow the new access points to join the OAW-IAP cluster. When this command is enabled, only the licensed slave OAW-IAPs can join the cluster.

Example

The following command allows the new OAW-IAPs to join the cluster.

```
(Instant AP)(config)# allow-new-aps
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

allowed-ap

```
allowed-ap <MAC-address>
no…
```

Description

This command allows an OAW-IAP to join the OAW-IAP cluster.

Syntax

Parameter	Description	Range	Default
`allowed-ap <MAC-address>`	Specifies the MAC address of the OAW-IAP that is allowed to join the cluster.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to allow an OAW-IAP to join the cluster.

Example

The following command configures an allowed OAW-IAP:

```
(Instant AP)(config)# allowed-ap 01:23:45:67:89:AB
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

a-max-clients

```
a-max-clients <ssid_profile> <max-clients>
```

Description

This command configures the maximum number of clients allowed for an SSID profile on a 5 GHz radio channel.

Syntax

Parameter	Description	Range	Default
`<ssid_profile>`	Denotes the SSID profile for which the maximum clients limit is to be configured.	—	—
`<max-clients>`	Denotes the maximum number of clients that can be configured on the 5 GHz radio channel of the OAW-IAP.	1 to 255	—

Usage Guidelines

Use this command to set the maximum number of clients allowed to connect to 5 GHz radio channels for a specific SSID profile. This is a per-AP and per-Radio configuration.

Example

The following example configures the maximum number of clients for a 5 GHz radio channel:

```
(Instant AP)# a-max-clients test1 35
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.0.0-4.3.0.0	**ssid_profile** parameter added.
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

ams-backup-ip

```
ams-backup-ip <IP-address or domain name>
no…
```

Description

This command adds the IP address or domain name of the backup OmniVista 3600 Air Manager Management server.

Syntax

Parameter	Description	Range	Default
`<IP-address or domain name>`	Configures the IP address or domain name of the secondary OmniVista 3600 Air Manager Management Server.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to add the IP address or domain name of the backup OmniVista 3600 Air Manager Management Server. The backup server provides connectivity when the OmniVista 3600 Air Manager primary server is down. If the OAW-IAP cannot send data to the primary server, the Virtual Controller switches to the backup server automatically.

Example

The following command configures an OmniVista 3600 Air Manager backup server.

```
(Instant AP)(config)# ams-backup-ip 192.0.2.1
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ams-identity

```
ams-identity <Name>
```

Description

This command uniquely identifies the group of OAW-IAPs managed or monitored by the OmniVista 3600 Air Manager Management console. The name can be a location, vendor, department, or any other identifier.

Syntax

Parameter	Description	Range	Default
`ams-identity <Name>`	Configures a name that uniquely identifies the OAW-IAP on the OmniVista 3600 Air Manager Management server. The name defined for this command will be displayed under the **Groups** tab in the OmniVista 3600 Air Manager UI.	—	—

Usage Guidelines

Use this command to assign an identity for the OAW-IAPs monitored or managed by the OmniVista 3600 Air Manager Management Server.

Example

The following command configures an OmniVista 3600 Air Manager identifier:

```
(Instant AP)(config)# ams-identity alcatel
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ams-ip

```
ams-ip <IP-address or domain name>
no…
```

Description

This command configures the IP address or domain name of the OmniVista 3600 Air Manager Management console for an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`<IP-address or domain name>`	Configures the IP address or domain name of an OmniVista 3600 Air Manager Management server for an OAW-IAP.	—	—

Usage Guidelines

Use this command to configure the IP address or domain name of the AMS console for an OAW-IAP.

Example

The following command configures the OmniVista 3600 Air Manager Management Server.

```
(Instant AP)(config)# ams-ip 192.0.1.2
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ams-key

```
ams-key <key>
no…
```

Description

This command assigns a shared key for service authorization.

Syntax

Parameter	Description	Range	Default
`<key>`	Authorizes the first Virtual Controller to communicate with the OmniVista 3600 Air Manager server.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to assign a shared key for service authorization. This shared key is used for configuring the first OAW-IAP in the OAW-IAP network.

Example

The following command configures the shared key for the OmniVista 3600 Air Manager management server.

```
(Instant AP)(config)# ams-key key@789
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ap1x

```
ap1x {peap|tls {tpm|user}} [validate-server]
no…
```

Description

This command sets the 802.1X authentication type on the uplink ports of OAW-IAP.

Syntax

Parameter	Description	Range	Default
`peap`	Configures PEAP based 802.1X authentication type.	—	—
`tls`	Configures TLS based 802.1X authentication type.	—	—
`tpm`	Configures a factory-installed TPM certificate for OAW-IAP authentication.	—	—
`validate-server`	Validates the authentication server credentials against the CA certificate in the OAW-IAP database.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to configure 802.1X authentication on uplink ports of an OAW-IAP, so that the OAW-IAPs can authenticate as 802.1X supplicant against the wired ports.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ap-frequent-scan

```
ap-frequent-scan <band>
```

Description

This command enables an OAW-IAP to search for a new environment, triggering the ARM profile to perform frequent scanning of transmission signals in a short span of time. Once the frequent scanning is complete, the ARM selects a valid channel of transmission.

Syntax

Parameter	Description	Range	Default
`band`	Sets a frequency band of the transmission signal during frequent scanning. **NOTE:** Client connection is impacted for a few seconds when the frequent scanning is in progress. The connection is re-established after the scanning is complete. Typically, a frequent scanning session lasts for less than 10 seconds.	2.4, 5.0, all	—

Usage Guidelines

Execute this command to enable the OAW-IAP to perform frequent scanning of transmission signals, and to select a valid channel for transmission.

The following checks must be performed before scanning:

- The DFS channels are skipped.
- The OAW-IAP is on stand-alone mode.
- The **client-aware** parameter is disabled by executing the **arm** command.

Example

The following example triggers the ARM to perform frequent scanning on a 2.4 GHz frequency band radio profile:

```
(Instant AP)# ap-frequent-scan 2.4
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.0.0-4.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ap-installation

```
ap-installation default|indoor|outdoor
```

Description

This command allows you to select the installation type you prefer for the OAW-IAP.

Syntax

Parameter	Description	Range	Default
`ap-installation`	Specify the type of installation (indoor or outdoor). The default parameter automatically selects an installation mode based upon the OAW-IAP model type	default indoor outdoor	default

Usage Guidelines

Use this command to provision an outdoor OAW-IAP into an indoor OAW-IAP or vice versa. The OAW-IAP needs to be rebooted for the configuration to take effect.

Example

The following example changes the installation type of the OAW-IAP from default to outdoor:

```
(Instant AP)# ap-installation outdoor
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.1.0-4.3.1.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

application-monitoring

```
application-monitoring
```

Description

This command enables traffic monitoring for applications. Use this command to monitor traffic generated on each application by a client.

Example

The following example configures application monitoring on an OAW-IAP:

```
(Instant AP)(config)# application-monitoring
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-530 Series and OAW-AP555 access points	Configuration mode.

ap1x-peap-user

```
ap1x-peap-user <ap1xuser> <password>
no…
```

Description

This command configures the user name and password variables to set the OAW-IAP as a 802.1X supplicant to authenticate against the wired ports.

Syntax

Parameter	Description	Range	Default
`<ap1xuser>`	Configures the user name variable for OAW-IAP to authenticate against the wired uplink ports with 802.1X authentication enabled.	—	—
`<password>`	Configures the password variable for OAW-IAP to authenticate against the wired uplink ports with 802.1X authentication enabled.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to configure and store the user name and password variables in OAW-IAP flash. This configuration is required for OAW-IAP to authenticate as 802.1X supplicant against the wired ports that are configured to use 802.1X protocols for authenticating clients.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ap2xx-prestandard-poe-detection

```
ap2xx-prestandard-poe-detection
no…
```

Description

This command enables pre-standard POE+ detector on OAW-AP200 Series, OAW-AP210 Series, OAW-AP 220 Series, OAW-AP270 Series OAW-IAPs.

Usage Guidelines

Configure this command on the OAW-IAP and then reload it when the switch is using pre-standard or Legacy POE+.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.3.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-IAP207 OAW-IAP214/OAW-IAP215 OAW-IAP224/OAW-IAP225 OAW-IAP274/OAW-IAP275 OAW-IAP277	Privileged EXEC mode

ap debug eapol-debug

```
ap debug eapol-debug
   enable client-mac <mac>
   disable
```

Description

This command enables and disables the EAPoL debugging for the specified client device.

Parameter	Description
`enable client mac`	Enables EAPoL debugging for the specified client device.
`   <mac>`	Enter the MAC address of the client.
`disable`	Disables EAPoL debugging for the OAW-IAP.

Usage Guidelines

Use this command to enable or disable EAPoL debugging for the specified client device. To view the current status of EAPoL debugging, use the **show ap debug eapol-debug status** command. To view the EAPoL debug logs, use the **show log driver** command.

Example

The following example shows the configuration of **ap debug eapol-debug** command:

```
(InstantAP)# ap debug eapol-debug enable client-mac 34:36:3b:70:37:ac
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-300 Series access points except OAW-340 Series	Privileged EXEC mode

apply

```
apply {cplogo-install| cplogo-uninstall| debug-command| delta-config}
```

Description

This command is used to save or apply the configuration settings on the OAW-IAP.

Syntax

Parameter	Description	Range	Default
`cplogo-install`	Installs the captive portal logo on the OAW-IAP.	—	—
`cplogo-uninstall`	Uninstalls the captive portal logo on the OAW-IAP.	—	—
`debug-command`	Applies the configuration settings from the **debug command**.	—	—
`delta-config`	Applies the configuration settings from the **delta-config** command.	—	—

Usage Guidelines

Use this command to apply the current configuration settings on the OAW-IAP.

Example

The following example installs the captive portal logo on an OAW-IAP.

```
(Instant AP)(config)# apply cplogo-inistall http://cp.logo.com
```

The following example uninstalls the captive portal logo on an OAW-IAP.

```
(Instant AP)(config)# apply cplogo-inistall http://cp.logo.com
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

ap-poe-power-optimization

```
ap-poe-power-optimization [enable | disable]
no..
```

Description

Enabling optimization minimizes the POE draw of the AP and may disable some parts of the AP. The USB and Ethernet port (eth1) are shut down on the AP when this option is enabled. The AP will operate in the full power mode when this option is disabled. This command is disabled by default on the AP.

Example

The following CLI command enables the low power mode on the AP:

```
(Instant AP)# ap-poe-power-optimization enable
```

The following CLI command disables the low power mode on the AP:

```
(Instant AP)# ap-poe-power-optimization disable
```

The following CLI command deletes the low power mode configuration on the AP:

```
(Instant AP)# no ap-poe-power-optimization
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

arm

```
arm
   80mhz-support
   a-channels <channel>
   air-time-fairness-mode {<default-access>| <fair-access>| <preferred-access>}
   backoff-time <secs>
   band-steering-mode {balance-bands|prefer-5ghz| force-5ghz| disable}
   channel-quality-aware-arm-disable
   channel-quality-threshold
   channel-quality-wait-time
   client-aware
   client-match [bad-snr <snr> | [calc-interval <interval>| calc-threshold <thresh>| client-
   thresh  <thresh> | debug <level>| good-snr <snr> | he-min-snr <snr> | holdtime <second> |
   key <key> | max-adoption <adopt>| max-request <req>| nb-matching <percentage> |report-
   interval <interval>| restriction-timeout  slb-mode <mode>|snr-thresh <snr>| sta-entry-age
   <age> | vbr-entry-age <age>]
   error-rate-threshold <percent>
   error-rate-wait-time <secs>
   free-channel-index <idx>
   g-channels <channel>
   ideal-coverage-index <idx>
   max-tx-power
   min-tx-power
   scanning
   spectrum-load-balancing [calc-interval <Seconds> |calc-threshold <threshold> | nb-matching
   <Percentage>]
   wide-bands {<none>| <all>| <2.4>| <5>}
   no…
```

Description

This command assigns an ARM profile for an OAW-IAP and configures ARM features such as band steering, spectrum load balancing, airtime fairness mode, and access control features.

Syntax

Parameter	Description	Range	Default
`80mhz-support`	Enables the use of 80 MHz channels on OAW-IAPs with 5 GHz radios, which support a VHT. **NOTE:** Only the OAW-IAPs that support 802.11ac can be configured with 80 MHz channels.	—	—
`a-channels <a-channel>`	Configures 5 GHz channels.	—	—
`air-time-fairness-mode {<default-access>| <fair-access>| <preferred-access>}`	Allows equal access to all clients on the wireless medium, regardless of client type, capability, or operating system and prevents the clients from monopolizing resources. You can configure any of the following modes: ■ default-access—To provide access based on client requests. When this mode is configured, the	default-access,fair-access, preferred-access	default-access

Parameter	Description	Range	Default
	per user and per SSID bandwidth limits are not enforced. ■ fair-access—To allocate Airtime evenly across all the clients. ■ preferred-access—To set a preference where 802.11n clients are assigned more airtime than 802.11a or 802.11g. The 802.11a or 802.11g clients get more airtime than 802.11b. The ratio is 16:4:1.		
`backoff-time <secs>`	Configures the time when an OAW-IAP backs off after requesting a new channel or power.	10-3600	240
`band-steering-mode {<balance-bands>|<prefer-5ghz>|<force-5ghz>|<disable>}`	Assigns the dual-band capable clients to the 5 GHz band on dual-band. It reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. You can configure any of the following band-steering modes: ■ prefer-5ghz—To allow the OAW-IAP to steer the client to 5 GHz band (if the client is 5 GHz capable). However, the OAW-IAP allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association. ■ force-5ghz—To enforce 5 GHz band steering mode on the OAW-IAPs, so that the 5 GHz capable clients are allowed to use only the 5 GHz channels. ■ balance-bands—To allow the OAW-IAPs to balance the clients across the two 2.4 GHz and 5 GHz radio and to utilize the available bandwidth. ■ disable—To allow the clients to select the bands.	balance-bands, prefer-5ghz, force-5ghz, disable	balance-bands
`channel-quality-aware-arm-disable`	With this parameter, ARM ignores the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value.	—	Disabled
`channel-quality-threshold <thresh>`	Specifies the channel quality percentage below which ARM initiates a channel change.	0-100	70
`channel-quality-wait-time <secs>`	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change.	1-3600	120

Parameter	Description	Range	Default
	NOTE: If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.		
`client-aware`	Enables the client aware feature. When enabled, the OAW-IAP will not change channels for the Access Points when clients are active, except for high priority events such as radar or excessive noise. The client aware feature must be enabled in most deployments for a stable WLAN.	—	Enabled
`client-match`	Enables enable the client match feature on OAW-IAPs. When the client match feature is enabled on an OAW-IAP, the OAW-IAP measures the RF health of its associated clients. If the client's RSSI is less than 18dB but has a good RSSI with another OAW-IAP having an RSSI of more than 30db or atleast 10db more than its current RSSI, the client will be moved to the OAW-IAP with the higher RSSI for better performance and client experience. In the current release, the client match feature is supported only within the OAW-IAPs within the swarm.	—	—
`bad-snr <snr>`	The clients with an SNR value below the threshold value will be moved to a potential target OAW-IAP.	0-100	18
`calc-interval<seconds>`	Configures an interval at which client match is calculated.	1-600 in seconds	3
`calc-threshold <threshold>`	Configures a threshold that takes acceptance client count difference among all the channels of Client match into account. When the client load on an OAW-IAP reaches or exceeds the threshold in comparison, client match is enabled on that OAW-IAP.	1-255	5
`client-thresh <thresh>`	When the number of clients on a radio exceeds the value, SLB algorithm will be triggered.	0-255	30
`debug <level>`	Displays information required for debugging client match issues.	0-4 0—none, 1—error, 2—information, 3—debug, 4—dump	1— error

Parameter	Description	Range	Default
`good-snr <snr>`	The OAW-IAPs with a RSSI higher than the specified good-snr value will be considered as a potential target OAW-IAP.	0-100	30
`he-min-snr <snr>`	Configures the minimum SNR value required for the targeted HE (802.11ax) steering.	0-100	40
`holdtime <number>`	Configures the hold time for the next client match action on the same client.	1—1800	300
`key <key>`	Configures the client match key of an OAW-IAP.	1–2147483646	VC key generated
`max-adoption <count>`	Configure a maximum number for adopting clients.	0-100	10
`max-request <count>`	Configures the maximum number of requests for client match.	0-100	10
`nb-matching <percentage>`	Configures a percentage value to be considered in the same virtual RF neighborhood of Client match.	20-100%	60%
`report-interval <interval>`	Configures the report interval of VBR on each OAW-IAP.	0-3600	30
`restriction-timeout`	Configures the timeout interval during which non-target OAW-IAP will not respond to a specific client.	1—255	10
`slb-mode <mode>`	Configures a balancing strategy for client match. The applicable values are: ■ 1—Channel-based ■ 2—Radio-based ■ 3—Channel and Radio based	1—3	1
`snr-thresh <snr>`	The snr value of the Client RSSI must be higher than the current OAW-IAP for a potential target OAW-IAP.	0-100	10
`sta-entry-age <age>`	Denotes the aging time of stale STA entries.	—	1000
`vbr-entry-age <age>`	Denotes the aging time for stable VBR entries	1-3600	300
`error-rate-threshold <percent>`	Configures the minimum percentage of errors in the channel that triggers a channel change.	0-100	70
`error-rate-wait-time <secs>`	Configures the time that the error rate has to be at least equal to the error rate threshold to trigger a channel change. The error rate must be equal to or more than the error rate threshold to trigger a channel change.	1-3600	90

Parameter	Description	Range	Default
`free-channel-index <idx>`	Checks the difference in threshold in the channel interference index between the new channel and the existing channel. An OAW-IAP will only move to a new channel if the new channel has a lower interference index value than the current channel. This parameter specifies the required difference between the two interference index values before the OAW-IAP moves to the new channel. The lower this value, the more likely it is that the OAW-IAP will move to the new channel.		25
`g-channels <g-channel>`	Configures 2.4 GHz channels.	—	—
`ideal-coverage-index`	Specifies the ideal coverage index that an OAW-IAP tries to achieve on its channel. The denser the OAW-IAP deployment, the lower this value should be.	2-20	10
`max-tx-power <power>`	Sets the highest transmit power levels for the OAW-IAP. If the maximum transmission EIRP configured on an OAW-IAP is not supported by the OAW-IAP model, the value is reduced to the highest supported power setting. **NOTE:** Higher power level settings may be constrained by local regulatory requirements and OAW-IAP capabilities.	0-127 dBm	127
`min-tx-power <power>`	Sets the minimum transmission power. This indicates the minimum EIRP. If the minimum transmission EIRP setting configured on an OAW-IAP is not supported by the OAW-IAP model, this value is reduced to the highest supported power setting.	0-127 dBm	9
`scanning`	Allows the OAW-IAPs to scan other channels for RF Management and WIPS enforcement.	—	Enabled
`spectrum-load-balancing {<calc-interval>|<calc-threshold>|<nb-matching>}`			

Parameter	Description	Range	Default
`wide-bands {<none>| <all>| <2.4>| <5>}`	Allows administrators to configure 40 MHz. channels in the 2.4 GHz and 5 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channels double the frequency bandwidth available for data transmission. For high performance, enter 5 GHz. If the OAW-IAP density is low, enter 2.4 GHz.	none, all, 2.4, and 5	5ghz
`no…`	Removes the current value for that parameter and return it to its default setting	—	—

Usage Guidelines

Use this command to configure ARM features on an OAW-IAP. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11ac, a, b, g, and n client types to inter-operate at the highest performance levels.

Example

The following example configures an ARM profile:

```
(Instant AP)(config)# arm
(Instant AP)(ARM)# 80mhz-support
(Instant AP)(ARM)# a-channels 44
(Instant AP)(ARM)# min-tx-power 18
(Instant AP)(ARM)# max-tx-power 127
(Instant AP)(ARM)# band-steering-mode prefer-5ghz
(Instant AP)(ARM)# air-time-fairness-mode fair-access
(Instant AP)(ARM)# backoff-time 600
(Instant AP)(ARM)# scanning
(Instant AP)(ARM)# client-aware
(Instant AP)(ARM)# client-match
(Instant AP)(ARM)# error-rate-threshold 80
(Instant AP)(ARM)# error-rate-wait-time 120
(Instant AP)(ARM)# free-channel-index 75
(Instant AP)(ARM)# ideal-coverage-index 7
(Instant AP)(ARM)# channel-quality-threshold 50
(Instant AP)(ARM)# channel-quality-wait-time 180
(Instant AP)(ARM)# wide-bands 5
(Instant AP)(ARM)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The **client-match he-min-sn**r parameter was introduced.
AOS-W Instant 8.4.0.0	■ The **key <key>** parameter was introduced. ■ The default values of the following parameters were updated to stay aligned with the AOS-W default values:

Release	Modification
	min-tx-power **channel-quality-aware-arm-disable**
Alcatel-Lucent AOS-W Instant 8.3.0.0	The following parameters were added: ▪ **backoff-time** ▪ **error-rate-threshold** ▪ **error-rate-wait-time** ▪ **free-channel-index** ▪ **ideal-coverage-index** ▪ **channel-quality-aware-arm-disable** ▪ **channel-quality-threshold** ▪ **channel-quality-wait-time**
Alcatel-Lucent AOS-W Instant 6.4.3.2-4.2.1.0	The **restriction-timeout** parameter was added to the **client-match** command.
Alcatel-LucentAOS-W Instant 6.3.1.1-4.0.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration and ARM configuration sub-mode.

attack

```
attack
   drop-bad-arp-enable
   fix-dhcp-enable
   no…
   poison-check-enable
```

Description

This command enables firewall settings to protect the network against wired attacks, such as ARP attacks or malformed DHCP packets, and notify the administrator when these attacks are detected.

Syntax

Parameter	Description	Range	Default
`drop-bad-arp-enable`	Enables the OAW-IAP to block the bad ARP request.	—	—
`fix-dhcp-enable`	Enables the OAW-IAP to fix the malformed DHCP packets.	—	—
`poison-check-enable`	Enables the OAW-IAP to trigger an alert to the user about the ARP poisoning that may have been caused by the rogue OAW-IAPs. Enabling this parameter triggers alerts when a known client on the OAW-IAP spoofs the base MAC address of the OAW-IAP.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Usage Guidelines

Use this command to block ARP attacks and to fix malformed DHCP packets.

Example

The following example configures firewall settings to protect the network from Wired attacks:

```
(Instant AP)(config)# attack
(Instant AP)(ATTACK)# drop-bad-arp-enable
(Instant AP)(ATTACK)# fix-dhcp-enable
(Instant AP)(ATTACK)# poison-check-enable
(Instant AP)(ATTACK)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration and Attack configuration sub-mode

auth-failure-blacklist-time

```
auth-failure-blacklist-time <seconds>
```

Description

This command allows the OAW-IAPs to dynamically blacklist the clients when they exceed the authentication failure threshold.

Syntax

Parameter	Description	Range	Default
`auth-failure-blacklist-time <seconds>`	Configures the duration in seconds for which the clients that exceed the maximum authentication failure threshold are blacklisted.	—	3600

Usage Guidelines

Use this command to dynamically blacklist the clients that exceed the authentication failure threshold configured for a network profile.

Example

The following example blacklists the clients dynamically:

```
(Instant AP)(config)# auth-failure-blacklist-time 60
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

auth-survivability cache-time-out

```
auth-survivability cache-time-out <time-out>
```

Description

This command configures an interval after which the authenticated credentials of the clients stored in the cache expire. When the cache expires, the clients are required to authenticate again.

Syntax

Parameter	Description	Range	Default
`auth-survivability cache-time-out`	Indicates the duration after which the authenticated credentials in the cache expire.	1-99 hours	24 hours

Usage Guidelines

Use this command when the authentication survivability is enabled on a network profile, to set a duration after which the authentication credentials stored in the cache expires. To enable the authentication survivability feature, use the **auth-survivability** in WLAN SSID profile sub-mode.

Example

```
(Instant AP) (config)# auth-survivability cache-time-out 60
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

banner

```
banner motd <motd_text>
no…
```

Description

This command defines a text banner to be displayed at the login prompt when a user is on a Telnet or SSH session of an OAW-IAP. The banner you define is displayed at the login prompt of the OAW-IAP. The banner is specific to the OAW-IAP on which you configure it. The configured banner is displayed at the CLI login prompt of the OAW-IAP. AOS-W Instant supports up to 16 lines text, and each line accepts a maximum of 255 characters including spaces.

Parameter	Description	Range	Default
`<motd_text>`	Indicates the text message that you define.	—	—
`no…`	Removes the banner configuration.	—	—

Example

The following example configures a banner:

```
(Instant AP)(config)# banner motd "######welcome to login instant###########"
(Instant AP)(config)# banner motd "####please start to input admin and password#########"
(Instant AP)(config)# banner motd "###Don't leak the password###"
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

bcn-rpt-req-profile

```
bcn-rpt-req-profile <profile-name>
   bssid <mac>
   channel <channel>
   include-ssid-disable
   last-beacon-rpt-indication
   measure-duration <measure-duration>
   measure-mode
   no
   random-interval <random-interval>
   reg-class {1|12|81|115}
   request-info <request-info>
   rpt-detail
   ssid <ssid>
```

Description

Configures a Beacon Report Request Profile to provide the parameters for the Beacon Report Request frames. The Beacon Report Request profile is configured under the 802.11K profile.

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`bssid <mac address>`	Set the the BSSID to be included in the beacon request frame.	—	FF:FF:FF:FF:FF:FF
`channel <channel>`	This option is used to set the Channel field in the Beacon Report Request frame. The Channel value can be set to one of the following: ■ The channel of the AP (when Measurement Mode is set to either 'Passive' or 'Active-All channels') ■ 0 (when Measurement Mode is set to 'Beacon Table') ■ 255 (when Measurement Mode is set to 'Active-Channel Report')	For 802.11b/g band: 1 to 14 For 802.11a band: 36 to 165	255
`include-ssid-disable`	The SSID information element will not included in the Beacon Report request if configured.	—	Disabled
`last-beacon-rpt-indication`	Enables the last beacon request indication sub-element in the beacon report request.	—	Disabled
`measure-duration <measure-duration>`	This value is used to set the Measurement Duration field in the Beacon Report Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs.	0 – 65535	0
`measure-mode`	Indicates the mode used for the measurement. The valid measurement modes are:	–	beacon-table

Parameter	Description	Range	Default
	■ **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ■ **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ■ **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table		
`no`	Negates any configured parameter.	—	—
`random-interval <random-interval>`	This value is used to set the Randomization Interval field in the Beacon Report Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units). A Randomization Interval of 0 in a measurement request indicates that no random delay is to be used.	0 – 65535	0

Parameter	Description	Range	Default
`reg-class {1|12|81|85}`	This option is used to specify the Regulatory Class field in the Beacon Report Request frame.	For 802.11b/g bands, 12. For 802.11a, use 1	12
`request-info <request-info>`	This option is used to indicate the contents of the Request Information IE that could be present in the Beacon Report Request frame. The Request Information IE is present for all Measurement Modes except the Beacon Table mode. It consists of a list of Element IDs that should be included by the client in the response frame.	Any valid element ID in the x/y/z format. For example, 0/21/22.	—
`rpt-detail`	This option is used to indicate the value for the Detail field in the Reporting Detail sub-element present in the Beacon Report Request frame.	—	Disabled
`ssid <ssid>`	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN- 01).	—	—

Example

The following commands configure the parameters under the bcn-rpt-req-profile.

```
(Instant AP)(config) #wlan bcn-rpt-req-profile default
(Instant AP)(Beacon Report Request Profile "default") #channel 9
(Instant AP)(Beacon Report Request Profile "default") #measure-duration 100
(Instant AP)(Beacon Report Request Profile "default") #measure-mode active-all-ch
(Instant AP)(Beacon Report Request Profile "default") #random-interval 100
(Instant AP)(Beacon Report Request Profile "default") #reg-class 12
(Instant AP)(Beacon Report Request Profile "default") #no rpt-detail
(Instant AP)(Beacon Report Request Profile "default") #request-info 0/21/22
(Instant AP)(Beacon Report Request Profile "default") #ssid aruba-ap
```

Command History

Release	Modification
AOS-W Instant 8.6.0.0	Command introduced

Command Information

Platforms	Command Mode
All platforms	Configuration mode

blacklist-client

```
blacklist-client <MAC-address>
no…
```

Description

This command allows you to manually blacklist the clients by using MAC addresses of the clients.

Parameter	Description	Range	Default
`blacklist-client <MAC-address>`	Adds the MAC address of the client to the blacklist.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Example

The following command blacklists an OAW-IAP client:

```
(Instant AP)(config)# blacklist-client 01:23:45:67:89:AB
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

blacklist-time

```
blacklist-time <seconds>
```

Description

This command sets the duration in seconds for which the clients can be blacklisted due to an ACL rule trigger. Use this command to configure the duration in seconds for which the clients can be blacklisted when the blacklisting rule is triggered.

Parameter	Description	Range	Default
`blacklist-time <seconds>`	Sets the duration in seconds for blacklisting clients due to an ACL rule trigger.	—	3600

Examples

The following command configures the duration for blacklisting clients:

```
(Instant AP) (config) # blacklist-time 30
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ble-init-action

```
ble-init-action
   add-log-level-str <level_str>
   ap-sleep-duration-min <duration>
   apb-power-reset
   ble_relay {send-sync-iotcfg|set-attr}
   clear-all-beacons
   clear-all-log-mac-filters
   clear-log-mac-filter <mac_address>
   input-filter-disable
   input-filter-enable
   log-level <level>
   log-level-str <level_str>
   log-mac-filter <mac_address>
   msg-select <msgselect>
   ota-fw-upgrade {disable|enable}
   remove-beacon-mac <mac_address>
   send-apb-update
   send-update <profile_name>
   start-log
   stop-log
```

Description

This command initiates BLE action for APs.

Parameter	Description
`add-log-level-str`	This parameter adds a new BLE daemon log level.
`ap-sleep-duration-min`	This parameter configuration a sleep duration.
`apb-power-reset`	This parameter will power-on reset for the on-board BLE radio.
`ble_relay`	Denotes the Bluetooth Low Energy (BLE) relay on devices. Configure one of the following options: ■ **send_sync_iotcfg**—Sends synchronized IoT configurations to the APs. ■ **set-attr**—Sets the attribute value. ●br-loglvl– ●tag-logging–Initiates or terminates the tag report logging. This action is completed using binary numbers, for example 1: initiate, 0: terminate. ●ws-connect–Initiates or terminates the web-socket connection. This action is completed using binary numbers, for example 1: initiate, 0: terminate. ●ws-loglvl–Provides the log levels to debug a web-socket connection.
`clear-all-beacons`	This parameter will delete all beacon data.
`clear-all-log-mac-filters`	This parameter will clear all the BLE daemon log MAC filters.
`clear-log-mac-filter`	This parameter will clear the BLE daemon log MAC filter.
`input-filter-enable`	This parameter will enable input filter for storing devices in the BLE table.
`input-filter-disable`	This parameter will enable input filter for storing devices in the BLE table.
`log-level`	BLE daemon log level specified as a number.
`log-level-str`	BLE daemon log levels specified as comma-separated values (without quotes). Possible values:'info','warning','error','ageout','bmreq','fw-upgrade',' fw-upgradeerr','cfgupdate,'cfgupdateerr','beacon','bcntl v','bcnerr','apb','tags','zf','amon','iot_gw','at-httpsjson',' at-websocket-protobuf'.
`log-mac-filter`	BLE daemon log MAC filter.
`msg-select`	Set bits to enable specific messages from APB to controller BLE Daemon - refer to BLE config CLI cmd.
`ota-fw-upgrade`	Over the Air firmware upgrade for onboard BLE.
`remove-beacon-mac`	Delete beacon with matching MAC address.
`send-apb-update`	Send APB info update to BLE Relay on controller.
`send-update`	Send IoT payload message to BMC immediately.
`start-log`	Enable BLE Daemon logging.
`stop-log`	Disable BLE Daemon logging.

Example

The following command enables input filter on the OAW-IAP:

```
(Instant AP)# ble-init-action input-filter-enable
```

The following command disables input filter on the OAW-IAP:

```
(Instant AP)# ble-init-action input-filter-disable
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The following parameters were introduced: - **input-filter-enable** - **input-filter-disable**
Alcatel-Lucent AOS-W Instant 8.3.0.0	This command is introduced.

Command Information

Platforms	Command Mode
OAW-AP-303, OAW-AP-303P OAW-AP365/OAW-AP367 OAW-AP303H OAW-IAP304/OAW-IAP305 OAW-AP203R/OAW-AP203RP OAW-IAP207 OAW-IAP334/OAW-IAP335 OAW-IAP314/OAW-IAP315 OAW-APAP-324/OAW-IAP325 OAW-AP-344/OAW-AP-345 OAW-AP515 OAW-530 Series OAW-500 Series	Privileged EXEC mode.

branch-name

```
branch-name
   master-mac
   string <string>
   vc-name
```

Description

This command configures the VPN branch key name. Use this command to enter a custom name for the branch key name. If a branch key name is not configured the VC-Key will be used as default.

Parameter	Description
`master-mac`	Configures the MAC address of the master OAW-IAP as the branch key name.
`string`	Configure a custom name for the VPN branch key.
`<string>`	Enter the custom string. Maximum of 64 characters.
`vc-name`	Configures the cluster name as the branch key name.

Example

The following example shows a sample configuration of **branch-name** command with the MAC of the master OAW-IAP:

```
(Instant AP)(config) # branch-name master-mac
(Instant AP)(config) # end
(Instant AP)# commit apply
committing configuration...
configuration committed.
```

The following example shows a sample configuration of **branch-name** command with a custom name:

```
(Instant AP)(config) # branch-name string test-setup-1
(Instant AP)(config) # end
(Instant AP)# commit apply
committing configuration...
configuration committed.
```

The following example shows a sample configuration of **branch-name** command with the name of the virtual cluster:

```
(Instant AP)(config) # branch-name vc-name
(Instant AP)(config) # end
(Instant AP)# commit apply
committing configuration...
configuration committed.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ca-bundle

```
ca-bundle
  reset
  update {download-url <download url>}
```

Description

This command updates the trusted CA certificate bundle installed on the AP.

Parameter	Description
`reset`	Resets CA certificate bundle to the factory default version.
`update`	Downloads the trusted CA certificate bundle from Activate.
`{download-url <download url>}`	Downloads the trusted CA certificate bundle from the specified URL. Only supports **https**. This parameter is optional.

Example

The following command downloads the CA certificate bundle from Activate:

```
(Instant AP)# ca-bundle update
```

The following command resets the CA certificate bundle on the AP to the factory default version:

```
(Instant AP)# ca-bundle reset
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

calea

```
calea
   encapsulation-type <gre>
   gre-type <type>
   ip <IP-address>
   ip mtu <size>
   no…
no calea
```

Description

This command creates a CALEA profile to enable OAW-IAPs for LI compliance and CALEA integration.

Syntax

Parameter	Description	Range	Default
`calea`	Enables **calea** configuration sub-mode for CALEA profile configuration.	—	—
`encapsulation-type <gre>`	Specifies the encapsulation type for GRE packets.	GRE	GRE
`gre-type`	Specifies GRE type.	—	25944
`ip <IP-address>`	Configures the IP address of the CALEA server on an OAW-IAP.	—	—
`ip mtu <size>`	Configures the MTU size to use.	68—1500	1500
`no…`	Disables the parameters configured under the **calea** command.	—	—
`no calea`	Removes the CALEA configuration	—	—

Usage Guidelines

Use this command to configure an OAW-IAP to support LI. LI allows the LEA to conduct an authorized electronic surveillance. Depending on the country of operation, the service providers are required to support LI in their respective networks.

In the United States, SPs are required to ensure LI compliance based on CALEA specifications. LI compliance in the United States is specified by the CALEA.

For more information on configuring OAW-IAPs for CALEA integration, see *Alcatel-Lucent AOS-W Instant User Guide*.

Example

The following example configures a CALEA profile:

```
(Instant AP)(config)# calea
(Instant AP)(calea)# ip 192.0.8.29
(Instant AP)(calea)# ip mtu 1500
(Instant AP)(calea)# encapsulation-type gre
(Instant AP)(calea)# gre-type 25944
(Instant AP)(calea)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and access rule configuration sub-mode.

cellular-uplink-profile

```
cellular-uplink-profile <profile>
   4g-usb-type <4G-usb-type>
   modem-country <modem-country>
   modem-isp <modem_isp>
   usb-auth-type <usb_authentication_type>
   usb-dev <usb-dev>
   usb-dial <usb-dial>
   usb-init <usb-init>
   usb-modeswitch <usb-modeswitch>
   usb-passwd <usb-passwd>
   usb-tty <usb-tty>
   usb-type <usb-type>
   usb-user <usb-user>
   no...
no cellular-uplink-profile
```

Description

This command provisions the cellular (3G or 4G) uplink profiles on an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`cellular-uplink-profile <profile>`	Configures a 3G or 4G cellular profile for an OAW-IAP.	—	—
`4g-usb-type <4G-usb-type>`	Indicates the selection of a specific 4G modem driver operation. This parameter represents different dialling modes. **NOTE:** This parameter is used only in modem UML290 and modem MC551L in an OAW-IAP.	ether-lte, pantech-lte, pantech-auto, none	—
`modem-country <modem-country>`	Specifies the country for the deployment.	—	—
`modem-isp <modem_isp>`	Specifies the name of the ISP to connect.	—	—
`usb-auth-type <usb_authentication_type>`	Specifies the authentication type for USB.	PAP, CHAP	PAP

Parameter	Description	Range	Default
`usb-dev <usb-dev>`	Specifies the device ID of the USB modem.	—	—
`usb-dial <usb-dial>`	Specifies the parameter to dial the cell tower.	—	—
`usb-init <usb-init>`	Specifies the parameter name to initialize the modem.	—	—
`usb-passwd  <usb-passwd>`	Specifies the password for the account associated with the subscriber of the selected ISP.	—	—
`usb-modeswitch <usb-modeswitch>`	Specifies the parameter used to switch modem from storage mode to modem mode.	—	—
`usb-type <usb-type>`	Indicates the device driver required for the 3G or 4G modem.	acm, airprime, hso, option, pantech-3g, sierra-evdo, sierra-gsm,none, ether-3g, sierra-net, option, sierra-gobi, rndis-uml295, rndis-u770, huawei-cdc, rndis-l800, novatel-u620	—
`usb-tty <usb-tty>`	Specifies the modem tty port.	—	—
`usb-user <usb-user>`	Specifies the username of subscriber of the selected ISP.	—	—
`no...`	Removes the configuration settings of parameters under the **cellular-uplink-profile** command.	—	—
`no cellular-uplink-profile`	Removes the cellular uplink configuration profile.	—	—

Usage Guidelines

Use this command to configure a cellular uplink profile on an OAW-IAP and modem parameters 3G or 4G uplink provisioning. AOS-W Instant supports the use of 3G or 4G USB modems to provide Internet backhaul to an AOS-W Instant network. The 3G or 4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the OAW-IAPs to automatically choose the available network in a specific region.

Most modems using a 4G driver will automatically select the best available cellular network coverage based on the RSSI value.

NOTE

When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Example 1

The following example configures a cellular uplink profile:

```
(Instant AP)(config) # cellular-uplink-profile
(Instant AP)(cellular-uplink-profile)# usb-type sierra-net
(Instant AP)(cellular-uplink-profile)# usb-dev 0x0f3d68aa
(Instant AP)(cellular-uplink-profile)# usb-init 3,broadband
(Instant AP)(cellular-uplink-profile)# end
(Instant AP)# commit apply
```

Example 2

The following example configures a cellular uplink profile for UML295 Country US and ISP Pantech:

```
(Instant AP)(config) # cellular-uplink-profile
(Instant AP)(cellular-uplink-profile)# usb-type rndis-uml295
(Instant AP)(cellular-uplink-profile)# usb-dev 0x10a96064
(Instant AP)(cellular-uplink-profile)# usb-tty ttyACM0
(Instant AP)(cellular-uplink-profile)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 6.5.0.0-4.3.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.4.3.4-4.2.1.0	The **pin-enable**, **pin-puk**, and **pin-renew** parameters were removed. These parameters are available as commands in the privileged Exec mode.
Alcatel-Lucent AOS-W Instant 6.4.3.1-4.2.0.0	The **pin-enable**, **pin-puk**, and **pin-renew** parameters were added.
Alcatel-LucentAOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and cellular uplink profile configuration sub-mode

clarity

```
clarity
   inline-auth-stats
   inline-dhcp-stats
   inline-dns-stats
   inline-sta-stats
   no…
```

Description

This command enables inline monitoring statistics for the OAW-IAP. The information is collected and forwarded to OmniVista 3600 Air Manager to debug client connectivity issues.

Syntax

Parameter	Description	Range	Default
`inline-auth-stats`	Enables the client authentication statistics on the OAW-IAP.	—	Disabled
`inline-dhcp-stats`	Enables the DHCP statistics on the OAW-IAP.	—	Disabled
`inline-dns-stats`	Enables the DNS statistics on the OAW-IAP.	—	Disabled
`inline-sta-stats`	Enables the station passive monitor statistics on the OAW-IAP.	—	Disabled
`no…`	Removes the configuration and returns the values to its default setting	—	—

Usage Guidelines

Use this command to configure the OAW-IAP to generate authentication, dhcp, dns, and station passive monitor statistics by using inline monitoring. These statistics are sent to OmniVista 3600 Air Manager to derive conclusions on the client connectivity issues.

Example

The following example configures a clarity profile:

```
(Instant AP)(config)# clarity
(Instant AP)(clarity)# inline-auth-stats
(Instant AP)(clarity)# inline-dhcp-stats
(Instant AP)(clarity)# inline-dns-stats
(Instant AP)(clarity)# inline-sta-stats
(Instant AP)(clarity)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.1.0-4.3.1.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration and clarity configuration sub-mode.

clear airgroup state statistics

```
clear airgroup state statistics
```

Description

This command removes the AirGroup statistics.

Usage Guidelines

Use this command to remove AirGroup details from the OAW-IAP database.

Example

The following command clears AirGroup statistics:

```
(Instant AP)(config)# clear airgroup state statistics
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clear

```
clear
   airgroup {blocked-queries|blocked-service-id}
   ap-env-backup
   ap-env-current
   arp <ip>
   captive-portal <logo>
   cluster-security {connections|peers|stats}
   core-file
   datapath {session|session-all|statistics}
   debug <ap>
   trace {ip|mac}
```

Description

This command clears various user-configured values from the running configuration on an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`airgroup {blocked-queries|blocked-service-id}`	Clears all AirGroup blocked queries and service IDs.	—	—
`ap-env-backup`	Clears all information from a backup AP.	—	—
`ap <ip-address>`	Clears all OAW-IAP related information.	—	—
`arp <ip-address>`	Clears all ARP table information for an OAW-IAP.	—	—
`client <mac>`	Clears all information pertaining to an OAW-IAP client.	—	—
`datapath {session-all| statistics}`	Clears all configuration information and statistics for datapath modules and user sessions.	—	—

Usage Guidelines

Use the clear command to clear the current information stored in the running configuration of an OAW-IAP.

Example

The following command clears all information related to an OAW-IAP:

```
(Instant AP)# clear ap 192.0.2.3
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clear-cert

```
clear-cert
   airwaveca
   ap1x
   ap1xca
   ca
   clearpassca
   cp
   datatunnel
   datatunnelca
   default [clearpassca]
   radsec
   radsecca
   server
   ui
```

Description

This command clears client and server, customized CA certificates from the OAW-IAP database.

Syntax

Parameter	Description	Range	Default
`airwaveca`	Clears the Airwave CA certificate on the OAW-IAP.	—	—
`ap1x`	Clears the user certificate used for TLS based 802.1x authentication of the OAW-IAP.	—	—
`ap1xca`	Clears CA certificate used for 802.1x authentication of the OAW-IAP against its uplink wired ports.	—	—
`ca`	Clears the CA certificates.	—	—
`clearpassca`	Clears the ClearPass Policy Manager CA.	—	—
`cp`	Clears the captive portal server certificate.	—	—
`default [clearpassca]`	Clears all the default ClearPass Policy Manager CA.	—	—

Parameter	Description	Range	Default
`radsec`	Clears the RadSec server certificate.	—	—
`radsecca`	Clears the RadSec CA certificate.	—	—
`server`	Clears all server certificates.	—	—
`ui`	Clears the WebUI certificate.	—	—

Usage Guidelines

Use this command to clear the certificates from the OAW-IAP database.

Example

The following command shows an example for clearing server certificates:

```
(Instant AP)# clear-cert server
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.4.0.0	The **airewaveca**, **default**, and **clearpassca** parameters were introduced.
Alcatel-Lucent AOS-W Instant 6.5.2.0	The **ui** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	The **ap1x** and **ap1xca** parameters were introduced.
Alcatel-Lucent AOS-W Instant 6.4.3.1-4.2.0.0	The **radsec** and **radsecca** parameters were introduced.
Alcatel-Lucent AOS-W Instant 6.3.1.0-4.0.0.0	The **cp** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clear datapath subnet

```
clear datapath subnet
   all
   vlan <id>
   vlan <id> ip <ip-address>
```

Description

This command clears entries in the datapath subnet table.

Syntax

Parameter	Description
`all`	Clears all dynamically learned IP and MAC addresses.
`vlan <id>`	Clears dynamically learned IP and MAC addresses in this VLAN.
`vlan <id> ip <ip>`	Clears a specific IP and MAC address in this VLAN.

Usage Guidelines

Use the clear datapath subnet command to clear dynamically learned and configured entries in the subnet table.

Example

The following command clears all entries in the datapath subnet table:

```
(Instant AP)# clear datapath subnet all
```

The following command clears dynamically learned IP and MAC in a particular VLAN:

```
(Instant AP)# clear datapath subnet vlan <id>
```

The following command clears a specific IP and MAC address in this VLAN:

```
(Instant AP)# clear datapath subnet vlan <id> ip <ip>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clock set

```
clock set <year> <month> <day> <hour> <min> <sec>
```

Description

This command sets the date and time on the OAW-IAP system clock.

Syntax

Parameter	Description	Range	Default
`<year>`	Sets the year. Requires all 4 digits.	Numeric	—
`<month>`	Sets the month.	1–12	—
`<day>`	Sets the day.	1–31	—
`<time>`	Sets the hour. Specify hours, minutes, and seconds separated by spaces. <hour> <min> <sec>	Numeric	—

Usage Guidelines

You can configure the year, month, day, and time. Specify the time using a 24-hour clock with hours, minutes and seconds separated by spaces.

Example

The following example sets the clock to 21 May 2013, 1:03:52 AM:

```
(Instant AP)# clock set 2013 5 21 1 3 52
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clear-dhcpoption82

```
clear-dhcpoption82 [xml]
```

Description

This command is used to delete the DHCP option 82 XML file from the OAW-IAP. This command must be executed only from the master OAW-IAP. Further, this will be allowed only if the XML file is disabled from the configure terminal.

Syntax

Parameter	Description	Range	Default
`xml`	This is used to specify that the DHCP Option82 XML file is deleted from the OAW-IAP flash.	—	—

The following command shows an example for clearing DHCP option 82:

```
(Instant AP)# clear-dhcpoption82 xml
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

cluster-security

```
cluster-security
   allow-low-assurance-devices
   disallow-non-dtls-slaves
   dtls
   no…
```

Description

This command enables cluster security in DTLS mode and also provides an option for users to allow or deny a DTLS connection for low assurance OAW-IAPs.

Syntax

Parameter	Description	Range	Default
`allow-low-assurance-devices`	Enables DTLS connection for low assurance OAW-IAPs.	—	Allow
`disallow-non-dtls-slaves`	Blocks non-DTLS slave OAW-IAPs from joining a DTLS enabled cluster.	—	—
`dtls`	Enables cluster security on the OAW-IAP using DTLS and secures the control plane messages between OAW-IAPs in the cluster.	—	Disabled
`no…`	Removes the configuration and returns the values to its default setting	—	—

Usage Guidelines

Use this command to configure cluster security using DTLS for securing control plane messages exchanged between the OAW-IAPs in a cluster.

Example

The following example configures a cluster-security profile:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# dtls
(Instant AP)(cluster-security)# end
(Instant AP)# commit apply
```

The following example configures DTLS connection for low assurance PKIs:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# allow-low-assurance-devices
(Instant AP)(cluster-security)# end
(Instant AP)# commit apply
```

The following example allows a non-DTLS slave OAW-IAP to join a DTLS enabled cluster:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# no disallow-non-dtls-slaves
(Instant AP)(cluster-security)# end
(Instant AP)# commit apply
```

The following example prevents a non-DTLS slave OAW-IAP from joining a DTLS enabled cluster:

```
(Instant AP)(config)# cluster-security
(Instant AP)(cluster-security)# disallow-non-dtls-slaves
(Instant AP)(cluster-security)# end
```

```
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **disallow-non-dtls-slaves** parameter was introduced.
Alcatel-LucentAOS-W Instant 6.5.3.0	The **allow-low-assurance-devices** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.5.1.0-4.3.1.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration and configuration sub-modes.

cluster-security logging

```
cluster-security logging module <module_name> log-level <level>
```

Description

This command allows you to set per module logging levels and retrieve the debugging logs on a one-time basis.

Syntax

Parameter	Description	Range	Default
`cluster-security logging`	Allows you to change the per module logging level for cluster security	—	—
`module <module_name>`	Allows you to set the following core modules for debugging. ■ **peer**—The peer module helps in logging the connection initiation, renegotiation, collision, and active connection updates. ■ **conn**—The connection module helps in logging connection creation, establishment, data transfer, and maintenance logs. ■ **mcap**—The message capture module logs the messages received and sent to the socket.	peer conn mcap	—
`log-level <level>`	Allows you to set a log level. Set the log-level to **debug** to log only the control messages. Set the log level to **debug1** to log both control and data messages.	debug debug1	—

Usage Guidelines

Use this command to change the per module logging level of cluster security

Example

The following example creates a log for the peer module:

```
(Instant AP)# cluster-security logging module peer log-level-individual debug1
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.1.0-4.3.1.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

clock summer-time

```
clock summer-time <timezone> recurring <start-week> <start-day> <start-month> <start-hour>
<eweek> <eday> <emonth> <ehour>
no…
```

Description

This command configures daylight saving for the time zones that support DST.

Syntax

Parameter	Description	Range	Default
`clock summer-time <timezone>`	Configures DST.	Timezones that support daylight saving configuration	—
`recurring`	Indicates the recurrences.	—	—
`<start-week>`	Indicates the week from which the daylight saving configuration is effective.	—	—
`<start-day>`	Indicates the day from which the daylight saving configuration applies.	—	—
`<start-month>`	Indicates the month from which the daylight saving configuration applies.	—	—
`<start-hour>`	Indicates the hour from which the daylight saving configuration applies.	1-24	—
`<eweek>`	Indicates the week in which the daylight saving configuration ends.	—	—
`<eday>`	Indicates the day on which daylight saving configuration ends.	—	—
`<emonth>`	Indicates the month in which daylight saving configuration ends.	—	—
`<ehour>`	Indicates the hour at which daylight saving configuration ends.	1-24	—
`no…`	Removes the configuration	—	—

Usage Guidelines

Use this command to configure daylight saving for the timezones that support daylight saving. When enabled, the DST ensures that the OAW-IAPs reflect the seasonal time changes in the region they serve.

Example

The following example configures daylight saving for a timezone:

```
(Instant AP)(config)# clock summer-time PST recurring 7 10 March 9PM 38 10 October 9PM
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

clock timezone

```
clock timezone <name> <hour-offset> <minute-offset>
no…
```

Description

This command sets the timezone on an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`clock timezone <name>`	Configures the required timezone.	All supported timezones	—
`<hour-offset>`	Specifies the hours offset from the UTC.	—	—
`<minute-offset>`	Specifies the hours offset from the UTC.	—	—
`no…`	Removes the timezone configuration.	—	—

Usage Guidelines

Use this command to set the timezone on an OAW-IAP.

Example

The following example configures the PST timezone:

```
(Instant AP) (config)# clock timezone PST -8 0
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

commit

```
commit {apply [no-save]| revert}
```

Description

This command allows you to commit configuration changes performed during a user session. You can also revert the changes that are already committed.

Syntax

Parameter	Description	Range	Default
`apply`	Applies and saves the OAW-IAP configuration changes.	—	—
`no-save`	Applies the configuration changes to the cluster, but does not save the configuration. To save the configuration, run the **write memory** or **commit apply** command.	—	—
`revert`	Reverts the changes committed to the current configuration of an OAW-IAP.	—	—

Usage Guidelines

Each command processed by the Virtual Controller is applied on all the slave OAW-IAPs in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session: therefore, Alcatel-Lucent recommends that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes, use the **commit apply** command. To apply the configuration changes without saving the configuration, use the **commit apply no-save** command.

Example

The following command allows you to commit the configuration changes:

```
(Instant AP) # commit apply
```

The following command reverts the already committed changes.

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 6.3.1.1-4.0.0.0	This command was modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

configure terminal

```
configure terminal
```

Description

This command allows you to enter configuration commands.

Syntax

No parameters.

Usage Guidelines

Upon entering this command, the enable mode prompt changes to:

```
(Instant AP)(config)#
To return to EXEC mode, enter Ctrl-Z, end or exit.
```

Example

The following command allows you to enter configuration commands:

```
(Instant AP) # configure terminal
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

console

```
console
  enable
  disable
no console
```

Description

This command enables console access to an OAW-IAP through the serial port.

Syntax

Parameter	Description	Range	Default
`console`	Allows you to enter the console configuration mode.	—	—
`enable`	Enables console access to the OAW-IAP.	—	—
`disable`	Disables console access to the OAW-IAP.	—	—
`no…`	Removes the console access settings.	—	—

Usage Guidelines

Use this command to enable or disable access to the OAW-IAP console and thus allow users to configure OAW-IAP settings or debug system errors. By default, the console access to the OAW-IAP is enabled.

Example

The following example disables console access to the OAW-IAP:

```
(Instant AP)(config)# console
(Instant AP)(console)# disable
(Instant AP)(console)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Console configuration sub mode

content-filtering

```
content-filtering
no…
```

Description

This command enables content filtering feature. When content filtering is enabled on an SSID, all DNS requests to non-corporate domains on this wireless network are sent to the configured DNS server.

Syntax

Parameter	Description	Range	Default
`content-filtering`	Enables content filtering.	—	—
`no`	Removes the configuration.	—	—

Usage Guidelines

Use this command to enable content filter. With content filter feature enabled, you can:

- Prevent known malware hosts from accessing your wireless network.
- Improve employee productivity by limiting access to certain websites.
- Reduce bandwidth consumption significantly.

You can enable content filtering on an SSID. When enabled, all DNS requests to non-corporate domains on this SSID are sent to the configured DNS server.

Example

The following example enables content filtering:

```
ac:a3:1e:cd:7b:d6 (config) # content-filtering
ac:a3:1e:cd:7b:d6 (config) # end
ac:a3:1e:cd:7b:d6# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

convert-aos-ap

```
convert-aos-ap <mode> <name>
```

Description

This command allows you to provision an OAW-IAP as a Campus AP or Remote AP in a switch-based network.

Syntax

Parameter	Description	Range	Default
`<mode>`	Provisions the OAW-IAP as remote AP or campus AP in a switch-based network.	RAP, CAP.	—
`<name>`	Allows you to specify the IP address of the switch to which the Remote AP or Campus AP will be connected.	—	—

Usage Guidelines

Before converting an OAW-IAP, ensure that both the OAW-IAP and switch are configured to operate in the same regulatory domain. An OAW-IAP can be converted to a Campus AP and Remote AP only if the switch is running AOS-W 6.1.4 or later versions.

For more information, see the *Converting an* OAW-IAP *to a Remote AP and Campus AP* topic in *Alcatel-Lucent AOS-W Instant User Guide*.

Example

The following command allows you to convert an OAW-IAP to a remote AP:

```
(Instant AP)# convert-aos-ap RAP 192.0.2.5
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

copy

```
copy
   config tftp <ip-address> <filename>
   core-file tftp <ip-address>
   flash tftp <ip-address> <filename>
   tftp <ip-address> <filename> {ap1x {ca|cert} <password> format pem}| cpserver cert
   <password> format {p12|pem}| clearpassca | portal logo| radsec {ca|cert <password>} format
   pem| system {1xca [format {der|pem}]|1xcert <passsword>[format {p12|pem}]|config|flash} |
   uiserver cert <password> format pem}
```

Description

This command copies files to and from the OAW-IAP.

Syntax

Parameter	Description	Range	Default
`config`	Copies a configuration file to the TFTP server.	—	—
`core-file`	Copies a core file to the TFTP server.	—	—
`flash`	Copies a file from flash to the TFTP server or to flash from a TFTP server.	—	—
`tftp`	Copies files and certificates to the OAW-IAP database from a TFTP server.	—	—
`<ip-address>`	Copies files to the specified TFTP server IP address.	—	—
`<filename>`	Indicates the name of the file to be copied.	—	—
`ap1x {ca |cert}`	Copies user or CA certificate required for 802.1X authentication of the OAW-IAP.	—	—
`cpserver cert <password>`	Copies internal captive portal server certificate.	—	—
`clearpassca`	Copies the ClearPass Policy Manager certificate from the TFTP server to the OAW-IAP.	—	—

Parameter	Description	Range	Default
`uiserver cert <password>`	Copies the customized WebUI server certificate.	—	—
`portal` `logo`	Copies customized logo for the internal captive portal server.	—	—
`radsec {ca | cert <password>`	Copies RadSec server or CA certificates.	—	—
`system`	Copies the file to the system partition.	—	—
`1xca`	Copies the CA certificate used for 802.1X authentication from the TFTP server.	—	—
`der` `pem`	Indicates the system partition file extensions.	—	—
`1xcert`	Copies the server certificate used for 802.1X authentication from the TFTP server.	—	—
`<passsword>`	Indicates the password for certificate authentication.	—	—
`p12` `pem`	Indicates the certificate file extensions.	—	—

Usage Guidelines

Use this command to save backup copies of the configuration file to a TFTP server, or to load a certificate file and customized logo from a TFTP server to the OAW-IAP database.

Example

The following example copies a configuration file to the TFTP server:

```
(Instant AP)# copy config tftp 10.0.0.1 filename.cfg
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **clearpassca** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.5.2.0	The**uiserver** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	The **ap1x** parameter was introduced.

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.3.1-4.2.0.0	The **radsec** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	The **cpserver** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

crypto pki-import

```
crypto pki-import format {pem|der|pkcs12|pfx|pkcs7} cert-type { PublicCert| ServerCert|
TrustedCA|ClientCert} <url> certname <certname> [ psk <passphrase>]
```

Description

This command allows you to import certificates to the OAW-IAP. In AOS-W Instant clusters, certificates can only be imported on the master AP. The imported certificates are saved in the flash memory of the AP.

Parameter	Description	Range
`format { pem|der}`	Specify the format of the certificate. The supported file formats are .pem and .der.	per, der
`cert-type { PublicCert| ServerCert| TrustedCA| ClientCert}`	Specify the certificate type.	PublicCert, ServerCert, TrustedCA, ClientCert
`<url>`	Specify the download URL of the certificate.	—
`certname <certname>`	Specify the name of the certificate. This name will be used to assign the certificate to an application.	—
`[ psk <passphrase>]`	Enter the passphrase for the certificate. This is an optional parameter. Use this parameter only if the certificate includes a passphrase.	—

Example

The following command uploads a trusted CA certificate with a passphrase on the OAW-IAP:

```
(Instant AP)# crypto pki-import format dem cert-type TrustedCA ftp://192.2.0.7/xxx.crt
certname PrimaryRadius psk secure123
```

Related Commands

Command	Description
crypto pki-remove	Removes certificates installed on the AP.

Command	Description
show ap checksum	Displays the number of certificates installed on the AP.
show cert assignment	Displays the list of certificates assigned to applications on the AP.
wlan cert-assignment-profile	Configures installed certificates for specific applications.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced

Command Information

Instant AP Platform	Command Mode
All platforms	Privileged EXEC mode

crypto pki-remove

```
crypto pki-remove
   cert all
   cert-type < PublicCert| ServerCert| TrustedCA| ClientCert> certname <certname>
```

Description

This command allows you to remove certificates on the OAW-IAP. In AOS-W Instant clusters, certificates can only be removed on the master AP. Certificates cannot be removed on the AP if they are assigned to an application. Therefore, ensure that the certificate is disassociated from the application before attempting to remove it.

Parameter	Description	Range
`cert all`	Removes all certificates on the AP. This command will not take effect if any of the certificate is assigned to an application.	—
`cert-type { PublicCert| ServerCert| TrustedCA| ClientCert}`	Specify the certificate type.	PublicCert, ServerCert, TrustedCA, ClientCert
`certname <certname>`	Specify the name of the certificate. This name will be used to assign the certificate to an application.	—

Example

The following command removes the server certificate named PrimaryRadius on the OAW-IAP:

```
(Instant AP)# crypto pki-remove cert-type ServerCert certname PrimaryRadius
```

Related Commands

Command	Description
crypto pki-import	Imports and installs certificates on the AP.
show ap checksum	Displays the number of certificates installed on the AP.
show cert assignment	Displays the list of certificates assigned to applications on the AP.
wlan cert-assignment-profile	Configures installed certificates for specific applications.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Instant AP Platform	Command Mode
All platforms	Privileged EXEC mode.

custom_var

```
custom_var <text>
no...
```

Description

This command is used to set the custom string length. The string length that is set will be valid until the OAW-IAP is factory reset.

Syntax

Parameter	Description	Range	Default
`<text>`	Indicates the custom variable string.	1-32	—
`no…`	Disables the custom string length that has been set.	—	—

Example

The following example sets the custom string length:

```
(Instant AP)# custom_var 12
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.4.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

debug-cloud-server

```
debug-cloud-server
  <server> websocket
  cert-verify-disable
  cert-verify-enable
  domain-name-verify-disable
  domain-name-verify-enable
```

Description

This command is used for debugging connections between the OAW-IAP and the server. Use this command to manually establish websocket connections to servers and toggle verification processes for SSL handshakes.

When certificate and domain name verification is enabled or disabled on the AP, manually reset the websocket connection for the setting to take effect. The websocket connection can be reset by connecting the AP to 0.0.0.0 and re-connecting it back to the server.

NOTE

If certificate and domain name verification is disabled, the connection between the AP and the server is unsecure. Use these commands for debugging purposes only.

Parameter	Description
`<server>`	URL of the server
`websocket`	Establishes a websocket connection to the server.
`cert-verify-disable`	Disables certificate verification during SSL handshake between the AP and the server.
`cert-verify-enable`	Enables certificate verification during SSL handshake between the AP and the server.
`domain-name-verify-disable`	Disables domain name verification during SSL handshake between the AP and the server.
`domain-name-verify-enable`	Enables domain name verification during SSL handshake between the AP and the server.

Example

The following example establishes a websocket connection between the AP and a server at **central.arubanetworks.com**:

```
(Instant AP) #debug-cloud-server-cert central.arubanetworks.com websocket
```

The following example shows how to reset a websocket connection on the AP:

```
(Instant AP) #debug-cloud-server-cert 0.0.0.0 websocket
(Instant AP) #debug-cloud-server-cert <server> websocket
```

The following example enables certificate verification during SSL handshake between the AP and the server:

```
(Instant AP) #debug-cloud-server-cert cert-verify-enable
(Instant AP) #debug-cloud-server-cert 0.0.0.0 websocket
(Instant AP) #debug-cloud-server-cert <server> websocket
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

debug-rtls-logs

```
debug-rtls-logs
no…
```

Description

This command generates debugging logs for the RTLS tags.

Usage Guidelines

Use this command to generate debugging logs for the RTLS tags. The generated logs can be viewed by using the **show rtls-logs** command.

Example

The following example disables the default provisioning SSID:

```
(Instant AP)# debug-rtls-logs
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

debug pkt

```
debug pkt
   dump
   match { any | dev | ip | ipv6 | mac | port | proto | vlan }
   mirror <ip>
   reset
   type {arp | pppoe | apmsg | icmp | icmpv6 | igmp | tcp | udp | gre | dhcp | dhcpv6 | dns |
   radius | http | https | echo | nd | rd | mld | mobility | beacon | all }
```

Description

This command is a packet debugging utility used to debug packets handled by the OAW-IAP.

Syntax

Parameter	Description
`debug pkt`	Packet debugging utility to troubleshoot data packets.
`dump`	Displays data packets of the selected type on the console.
`match`	Filter packets based on the following parameters: **any, dev, ip, ipv6, mac, port, proto** and **vlan**.
`mirror <ip>`	This command mirrors the specified packets to the network device at the mentioned IP address.
`reset`	Resets the **debug pkt** configuration.
`type`	Selects the packet type for debugging. Debugging packet types include the following packet types: **arp, pppoe, apmsg, icmp, icmpv6, igmp, tcp, udp, gre, dhcp, dhcpv6, dns, radius, http, https, echo, nd, rd, mld, mobility, beacon** and **all**.

Usage Guidelines

Use this command to troubleshoot data packets at the OAW-IAP. Configure the **debug pkt** utility using the **debug pkt type** and **debug pkt match** to select the packet data type and filter respectively. Use the **debug pkt dump** command to view the selected data packets and **debug pkt mirror <ip>** command to mirror the data packets to a network device. The **debug pkt reset** command clears the debug pkt configuration.

Example

The following example shows the partial output of **debug pkt** command:

```
(Instant AP)# debug pkt type icmp
(Instant AP)# debug pkt match ip 10.20.102.208
(Instant AP)# debug pkt dump
(Instant AP)# debug pkt dump
If source, destination or target IP is 10.20.102.208
AND packet is of type ICMP
Press 'q' to quit.

Received packet from bond0 (timestamp (2019-3-25 16:38:22:890734))
[asap_firewall_forward(7119):firewall entry] len 74, vlan 0, egress CP, ingress bond0:
#mac: etype 0800 smac 00:0b:86:6c:b6:80 dmac 70:3a:0e:cc:ee:3e
#ip: sip 10.20.102.208, dip 10.65.18.2, proto 1 hdr len 20
len 60, id 6421, cksum a285, ttl 114, dscp 0
fragment ok, last fragment, frag off 0
```

```
#icmp: type echo-request(8) code 0 id 1 seq 488
[asap_firewall_forward(7335):vlan decision, tags 0] len 74, vlan 1, egress CP, ingress bond0:
[asap_firewall_forward(7858):looking up pkt ingress/src bridge entry 00:0b:86:6c:b6:80] len
74, vlan 1, egress CP, ingress bond0:
[asap_firewall_forward(7907):Found ingress/src bridge entry 00:0b:86:6c:b6:80 rechable via
bond0] len 74, vlan 1, egress CP, ingress bond0:
[asap_firewall_forward(8243):bridge section, looking for dst bridge entry 70:3a:0e:cc:ee:3e]
len 74, vlan 1, egress CP, ingress bond0:
[asap_firewall_forward(8524):session section] len 74, vlan 1, egress CP, ingress bond0:
[asap_firewall_forward(8798):fastpath session returned 1 opcode 4, snat none] len 74, vlan 1,
egress CP, ingress bond0:
[asap_firewall_forward(8813):slowpath section: opcode 4] len 74, vlan 1, egress CP, ingress
bond0:
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

debug ap log enable

```
debug ap log enable
```

Description

This command enables debug logging for the OAW-IAP.

Usage Guidelines

Use this command to enable debug logging for the OAW-IAP.

Example

The following example shows how to configure **debug ap log enable**:

```
(Instant AP) #debug ap log enable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

deny-inter-user-bridging

```
deny-inter-user-bridging
no…
```

Description

This command disables bridging traffic between two clients of an OAW-IAP on the same VLAN. Bridging traffic between the clients will be sent to the upstream device to make the forwarding decision.

Syntax

Parameter	Description	Range	Default
`deny-inter-user-bridging`	Prevents the inter-user bridging.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command if you have security and traffic management policies defined for upstream devices.

Example

The following command disables inter-user bridging:

```
(Instant AP)(config)# deny-inter-user-bridging
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

deny-local-routing

```
deny-local-routing
no…
```

Description

This command disables routing traffic between two clients of an OAW-IAP on different VLANs. Routing traffic between the clients will be sent to the upstream device to make the forwarding decision.

Syntax

Parameter	Description	Range	Default
`deny-local-routing`	Disables local routing of traffic.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to prevent the local routing of traffic if you have security and traffic management policies defined for upstream devices.

Example

The following command disables local routing:

```
(Instant AP)(config)# deny-local-routing
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

device-id

```
device-id <device>
```

Description

This command assigns an ID for the OAW-IAP device.

Syntax

Parameter	Description	Range	Default
`device-id <device>`	Configures an ID for the OAW-IAP device.	—	—

Usage Guidelines

Use this command to configure a device identification.

Example

The following example configures a device ID:

```
(Instant AP)(config)# device-ID Device1
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dhcp

```
dhcp
   option82-xml <string>
   no…
```

Description

This command is used to configure the DHCP option 82 parameters present in the XML file into the datapath.

Syntax

Parameter	Description	Range	Default
`option82-xml <mydhcpoption82.xml>`	Indicates the XML file from which DHCP option 82 needs to be configured.	—	—
`no…`	Removes the DHCP option 82 XML based configuration.	—	—

Example

The following command configures DPI support:

```
(Instant AP)(config)# dhcp option82-xml file
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

disable-factory-reset

```
disable-factory-reset
no…
```

Description

This command disables the factory reset function on the OAW-IAP. Use this command to prevent the manual hard reset to factory default by pressing down reset button for 5 seconds.

Syntax

Parameter	Description	Range	Default
`disable-factory-reset`	Disables the factory reset function when the OAW-IAP is operational.	—	Disabled
`no…`	Removes the configuration and allows the OAW-IAP to be reset to factory default again.	**NOTE:** —	**NOTE:** —

Example

The following CLI command disables the AP factory reset feature while the AP is operational:

```
(Instant AP)(Config)# disable-factory-reset
```

The following CLI command enables the AP factory reset feature while the AP is operational:

```
(Instant AP)(Config)# no disable-factory-reset
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

disable-prov-ssid

```
disable-prov-ssid
no…
```

Description

This command disables the default provisioning SSID enabled in the OAW-IAP factory default settings.

Usage Guidelines

The default provisioning SSID is used during the initial configuration of the OAW-IAP if the automatic provisioning of the OAW-IAP fails and if OmniVista 3600 Air Manager is not reachable.

Example

The following example disables the default provisioning SSID:

```
(Instant AP)# disable-prov-ssid
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

disconnect-user

```
disconnect-user {<addr>|all|mac <mac>| network <name>}
```

Description

This command disconnects the clients from an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`<addr>`	Allows you to disconnect a client by specifying the IP address of the client.	—	—
`all`	Disconnects all users associated with anOAW-IAP.	—	—
`mac <mac>`	Allows you to disconnect a client by specifying the MAC address of the client.	—	—
`network <name>`	Allows you to disconnect the clients connected to a specific network.	—	—

Example

The following example disconnects all clients associated with an OAW-IAP:

```
(Instant AP)# disconnect-user
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

dot1x eap-frag-mtu

dot1x eap-frag-mtu <ipmtu>

```
no ...
```

Description

This command configures the IP MTU to be considered for EAP fragmentation.

Parameter	Description	Default	Range
`<ipmtu>`	The OAW-IAP receives the EAP packet with certificate from the client and fragments it into smaller EAP fragments based on the eap-frag-mtu configured.	—	576 to 1300
`no`	Removes the configuration.	—	—

Example

The following CLI command configures EAP-TLS fragmentation in an 802.1X authentication profile:

```
(Instant AP)(config) #dot1x eap-frag-mtu 600
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced

Command Information

Platforms	Command Mode
All platforms	Configuration mode

dot11a-radio-disable

```
dot-11a-radio-disable
no…
```

Description

This command disables the 5 GHz or 802.11a radio profile for an OAW-IAP. Disabling the radio profile using this command will not delete the SSID profiles.

Syntax

Parameter	Description	Range	Default
`dot11a-radio-disable`	Disables the 5 GHz or 802.11a radio profile	—	—
`no…`	Removes the radio profile from the disabled mode.	—	—

Usage Guidelines

Use this command to disable a 5 GHz radio profile on an OAW-IAP.

Example

The following example disables the 5 GHz radio profile:

```
(Instant AP)# dot11a-radio-disable
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

dot11g-radio-disable

```
dot-11g-radio-disable
no…
```

Description

This command disables the 2.4 GHz or 802.11g radio profile for an OAW-IAP. Disabling the radio profile using this command will not delete the SSID profiles.

Syntax

Parameter	Description	Range	Default
`dot11g-radio-disable`	Disables the 2.4 GHz or 802.11g radio profile	—	—
`no…`	Removes the radio profile from the disabled mode.	—	—

Usage Guidelines

Use this command to disable a 2.4 GHz radio profile on an OAW-IAP.

Example

The following example disables the 2.4 GHz radio profile:

```
(Instant AP)# dot11g-radio-disable
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

dot11k-profile

```
dotllk-profile <profile-name>
   ap-chan-rpt-11a <ap-chan-rpt-11a>
   ap-chan-rpt-11bg <ap-chan-rpt-11bg>
   bcn-req-chan-11a <bcn-req-chan-11a>
   bcn-req-chan-11bg <bcn-req-chan-11bg>
   bcn-req-time <bcn-req-time>
   bcn-rpt-req-profile <profile-name>
   dot11k-enable
   no ...
   rrm-ie-profile <profile-name>
```

Description

Configures a 802.11k radio profile.

Syntax

Parameter	Description	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	"default"
`ap-chan-rpt-11a <ap-chan-rpt-11a>`	This value is sent in the Channel field of the AP channel reports on the 'A' radio. You can specify values in the range 34 to 165.	36
`ap-chan-rpt-11bg <ap-chan-rpt-11bg>`	This value is sent in the Channel field of the AP channel reports on the 'BG' radio. You can specify values in the range 1 to 14.	1
`bcn-req-chan-11a <bcn-req-chan-11a>`	This value is sent in the Channel field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165.	36
`bcn-req-chan-11bg <bcn-req-chan-11bg>`	This value is sent in the Channel field of the Beacon Requests on the BG radio. You can specify values in the range 1 to 14 or 0 to 255.	1
`bcn-req-time <bcn-req-time>`	This option configures the time duration between two consecutive beacon requests sent to a802.11k client. By default, the beacon requests are sent to a802.11k client every 60 seconds. However, if a different value is required, the `bcn-req-time` option can be used. This permits values in the range from 10 seconds to 200 seconds.	60 seconds
bcn-rpt-req-profile <profile-name>	Beacon Report Request Settings for the selected profile.	—
`dot11k-enable`	Enables the 802.11K feature. This feature is disabled by default.	Disabled
`no`	Negates or removes any configured parameter.	
`rrm-ie-profile <profile-name>`	RRM IE Settings Profile.	

Usage Guidelines

In a 802.11k network, if the AP with the strongest signal is reaches its maximum capacity, clients may connect to an under utilized AP with a weaker signal. A 802.11k profile can assigned to each AP. The dot11k-profile must be attached to the WLAN SSID using the **dot11k-profile <profile name>** parameter under **wlan ssid-profile** command.

Example

The following command enables the 802.11k feature on the 802.11k profile.

```
(Instant AP)(config) #wlan dot11k-profile default
(Instant AP)(802.11K Profile "default") #dot11k-enable
(Instant AP)(802.11K Profile "default") #bcn-measurement-mode beacon-table
(Instant AP)(802.11K Profile "default") #bcn-req-time 60
```

Command History

Release	Modification
AOS-W 8.6.0.0	Command introduced

Command Information

Platforms	Command Mode
All platforms	Configuration mode

download-cert

```
download-cert
   ap1x <url> format pem [psk <psk>]
   ap1xca <url> format pem
   ca <url> format {der|pem}
   clearpassca <url> format pem
   cp <url> format pem [psk <psk>]
   radsec <url> format pem [psk <psk>]
   radsecca <url> format pem [psk <psk>]
   server <url> format pem [psk <psk>]
   ui <url> format pem [psk <psk>]
```

Description

This command allows you to download the authentication, captive portal and RadSec server certificates, and CA certificates from an FTP or TFTP server, or through an HTTP URL.

Syntax

Parameter	Description	Range	Default
`ap1x`	Downloads user certificate for TLS based 802.1X authentication of the OAW-IAP.	—	—
`ap1xca`	Downloads CA certificates.	—	—
`ca`	Downloads CA certificates for validating the identity of the client.	—	—
`clearpassca <url> format pem`	Downloads the customized ClearPass Policy Manager CA.	—	—
`cp`	Downloads captive portal server certificates for validating the identity of the internal captive portal server identity to the client.	—	—
`radsec`	Downloads RadSec certificates for mutual authentication between the OAW-IAP and the client.	—	—
`radsecca`	Downloads RadSec CA certificates for authentication between the OAW-IAP and the client.	—	—
`server`	Downloads authentication server certificates for validating the identity of the server to the client.	—	—
`ui`	Downloads the WebUI certificates.	—	—
`<url>`	Allows you to specify the FTP, TFTP, or HTTP URL.	—	—
`format`	Allows you to specify the certificate format. The following types of certificate formats are supported:	–	–

Parameter	Description	Range	Default
	■ CA certificate—PEM or DER format ■ Authentication server—PEM format with PSK ■ Captive portal certificate—PEM format with PSK ■ RadSec—PEM format with PSK		
`psk <psk>`	Allows you to specify the passphrase for server, captive portal, and RadSec certificates.	—	—

Usage Guidelines

Use this command to download certificates.

Example

The following command shows an example for downloading CA client certificates:

```
(Instant AP)# download-cert ca ftp://192.0.2.7
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.4.0.0	The **clearpassca** parameter was introduced.
Alcatel-LucentAOS-W Instant 6.5.2.0	The **ui** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	The **ap1x** and **ap1xca** parameters were introduced.
Alcatel-LucentAOS-W Instant 6.4.3.1-4.2.0.0	The **radsec** and **radsecca** parameters were introduced.
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	The **cp** parameter was introduced.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

download-dhcpopt82

```
download-dhcpopt82
  xml <url>
```

Description

This command allows you to download the XML file using HTTP, FTP or TFTP URL.

Syntax

Parameter	Description	Range	Default
`xml <url>`	Allows you to specify the FTP, TFTP, or HTTP URL of the XML file. For example, if the URL is in HTTP format, the XML file's URL will be addressed as http://<ip address>/filename.xml.	—	—

Usage Guidelines

Use this command to download the DHCP option 82 XML file in the **mydhcpopt82.xml** format regardless of what name is given to the XML file. The OAW-IAP validates if the XML file is in correct format and load it into OAW-IAP flash. If the validation fails, the error type is displayed in the output of the **show dhcp opt82 xml-config**.

The maximum size limit of the XML buffer is 1 KB. The XML buffer will be filled from the downloaded XML file omitting any whitespace characters in the file. This command must be executed only from master OAW-IAP.

Example

The following command shows an example for downloading DHCP option 82:

```
(Instant AP)# download-dhcpopt82 xml http://10.20.52.131/googledhcp.xml
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

dpi

```
dpi
no…
```

Description

This command enables visualization of traffic from wired and wireless clients associated with an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`dpi`	Enables AppRF feature.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to enable AppRF visibility for wired and wireless clients associated with an OAW-IAP. AppRF supports an application and web-filtering service that allows creating firewall policies based on types of application. AppRF includes the following capabilities:

- Access control, QoS, and bandwidth contract rules based on application and application categories.
- Content filters based on web categories and reputation scores (security ratings).

For more information access rule configuration and web-filtering options, see the *Alcatel-Lucent AOS-W Instant User Guide* and the wlan access-rule command page.

Example

The following command configures DPI support:

```
(Instant AP)(config)# dpi
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.0.0-4.3.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dpi-error-page-url

```
dpi-error-page-url <idx> <url>
no…
```

Description

This command allows you to create a custom list of URLs to which users can be redirected. The URLs configured by using the **wlan access-rule <rule> dpi-error-page-url** command are used for defining an access rule to redirect users to a specific URL when they access a blocked website.

Parameter	Description	Range	Default
`<idx>`	Index number of the URL.	—	—
`<url>`	URL of the website.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example shows how to add a URL:

```
(Instant AP)(config)# dpi-error-page-url 0 http://www.NoExample.com
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dual-5GHz-mode

```
dual-5GHz-mode {<enable><disable>}
```

Description

This command is used to configure dual 5 GHz mode on OAW-AP-344/OAW-AP-345 access points. Dual 5 GHz mode enables both radio channels on the OAW-IAP to run 5 GHz band.

Parameter	Description	Range
<enable>	Enables dual 5 GHz mode on the AP. Both Radio 0 and Radio 1 use dot11a-radio-profile configuration settings under this configuration and run 5 GHz on both Radio 0 and Radio 1.	—
<disable>	Disabled dual 5 GHz mode. In this mode, Radio 0 is in 5 GHz mode and Radio 1 is in 2.4 GHz mode.	—

Example

The following example enables dual 5 GHz mode:

```
345#c8:b5:ad:c3:af:a0# dual-5GHz-mode enable
345#c8:b5:ad:c3:af:a0# show ap-env
Antenna Type:Internal
Need USB field:Yes
name:345#c8:b5:ad:c3:af:a0
radio0_channel:165
radio0_power_10x:15.0
standalone_mode:1
iap_master:1
uap_controller_less:1
iap_rf_zone:33
dual_5g_mode:enable
345#c8:b5:ad:c3:af:a0#
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344/OAW-AP-345	Privileged EXEC mode.

dynamic-cpu-mgmt

```
dynamic-cpu-mgmt {auto| disable| enable}
```

Description

This command enables or disables the dynamic CPU management feature, to manage resources across different functions performed by an OAW-IAP.

Parameter	Description	Range	Default
`auto`	Configures the OAW-IAP to automatically enable or disable CPU management feature during run-time. When configured, the OAW-IAP determines the need for enabling or disabling CPU management, based on the real-time load calculations taking into account all different functions that the CPU needs to perform. The **auto** option is the default and recommended setting.	—	—
`disable`	Disables CPU management on all OAW-IAPs, typically for small networks. This setting protects the user experience.	—	—
`enable`	Enables the CPU management feature. When configured, the client and network management functions are protected. This setting helps in large networks with a high client density.	—	—

Example

The following example enables the automatic enabling or disabling of CPU management:

```
(Instant AP)(config)# dynamic-cpu-mgmt auto
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

dynamic-dns

```
dynamic-dns {<dns_action> <dns_server> <dns_domain> <dns_hostname> <dns_host>} [key <algo-name:keyname:keystring>]
```

Description

This command makes a one time dynamic update of the DNS records of the OAW-IAP and its clients after the user has manually configured the dns values.

Parameter	Description	Example
`dynamic-dns`	Updates the DNS records of the OAW-IAP and its clients dynamically on the DNS server.	—
`<dns_action>`	Allows you to add or delete the DNS record from the DNS server.	—
`<dns_server>`	Denotes the IP address of the DNS server.	10.17.132.85
`<dns_domain>`	Denotes the domain name of the client that is updated on the DNS server.	test.dns
`<dns_hostname>`	Denotes the hostname of the client or OAW-IAP that is updated on the DNS server.	host-anand
`<dns_host>`	Denotes the IP address of the OAW-IAP or the client.	10.17.132.85
`key <algo-name:keyname:keystring>`	Configures a TSIG shared secret key to secure the dynamic updates. The following algorithm names are supported: ■ hmac-md5 (used by default if algo-name is not specified) ■ hmac-sha1 ■ hmac-sha256 **NOTE:** When a **key** is configured, the update is successful	hmac-sha1:arubaddns: 16YuLPdH21rQ6PuK9udsVLtJw3Y=

Parameter	Description	Example
	only if OAW-IAP and DNS server clocks are in sync.	

Example

The following example manually adds the SOA record:

```
(Instant AP)# dynamic-dns add 10.1.1.23 test.dns host-anand 10.3.2.11  key hmac-
sha1:arubaddns:16YuLPdH21rQ6PuK9udsVLtJw3Y=
(Instant AP)# commit apply
```

The following example manually deletes the SOA record.

```
(Instant AP)# dynamic-dns delete 10.17.132.7 test.ddns host-anand 10.17.132.85 key hmac-
sha1:arubaddns:16YuLPdH21rQ6PuK9udsVLtJw3Y=
(Instant AP)# commit apply
```

NOTE

The colon (:) functions as an input separator in the shared secret key entry.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

dynamic-dns-ap

```
dynamic-dns-ap [key <algo-name:keyname:keystring>] [server <ddns_server>]
```

Description

This command enables the OAW-IAP and clients to dynamically update the DNS server. Dynamic DNS configuration is allowed only on Master OAW-IAPs.

Parameter	Description	Example
`dynamic-dns-ap`	Updates the DNS records of the OAW-IAP and its clients dynamically on the DNS server.	—
`key <algo-name:keyname:keystring>`	Configures a TSIG shared secret key to secure the dynamic updates. The following algorithm names are supported: ■ hmac-md5 (used by default if algo-name is not specified) ■ hmac-sha1 ■ hmac-sha256 **NOTE:** When a **key** is configured, the update is successful only if OAW-IAP and DNS server clocks are in sync.	hmac-sha1:ddns-key: asdafsdfasdfsgdsgs=
`server <ddns_server>`	Denotes the IP address of the DNS server.	10.17.132.85

Example

The following example enables the dynamic dns feature:

```
(Instant AP)(config)# dynamic-dns-ap
(Instant AP)(config)# dynamic-dns-ap key hmac-sha1:arubaddns:16YuLPdH21rQ6PuK9udsVLtJw3Y=
(Instant AP)(config)# dynamic-dns-ap server 10.1.1.23
(Instant AP)(config)# end
(Instant AP)# commit apply
```

NOTE

The colon (:) functions as an input separator in the shared secret key entry.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dynamic-dns-interval

```
dynamic-dns-interval <ddns_interval>
```

Description

This command configures a time interval at which the DNS updates are synched with the server.

Parameter	Description	Range	Default
`dynamic-dns-interval <ddns_interval>`	Configures the time interval (in seconds) at which the DNS updates are synced to the server. The default value is 12 hours.	—	—

Example

The following example configures a DDNS time interval:

```
(Instant AP)(config)# dynamic-dns-interval 900
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dynamic-radius-proxy

```
dynamic-radius-proxy
no…
```

Description

This command enables the use of IP Address of the Virtual Controller for communication with external RADIUS servers. Ensure that you set the Virtual Controller IP address as a NAS client in the RADIUS server when Dynamic RADIUS proxy is enabled.

Parameter	Description	Range	Default
`dynamic-radius-proxy`	Enables dynamic RADIUS proxy feature to allow the Virtual Controller network to use the IP address of the Virtual Controller when communicating with the external RADIUS servers.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables the dynamic RADIUS proxy feature:

```
(Instant AP)(config)# dynamic-radius-proxy
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

dynamic-tacacs-proxy

```
dynamic-tacacs-proxy
no…
```

Description

This command enables the Virtual Controller network to use the IP Address of the Virtual Controller for communication with external TACACS servers. The command channels all TACACS related traffic from the slave OAW-IAPs to the external TACACS server

Parameter	Description	Range	Default
`dynamic-tacacs-proxy`	Allows the Virtual Controller network to use the IP address of the Virtual Controller when communicating with the external TACACS servers. **NOTE:** When dynamic-tacacs-proxy is enabled on the OAW-IAP, the TACACS server cannot identify the slave OAW-IAP that generates the TACACS traffic as the source IP address is changed.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables the dynamic TACACS proxy feature:

```
(Instant AP)(config)# dynamic-tacacs-proxy
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet-vlan

```
enet-vlan <vlan-ID>
no…
```

Description

This command configures a VLAN for Ethernet connections. Use this command to configure VLAN settings for upstream switch to which the is connected. By default, the value is set to 1. The VLAN setting configured by this command is used for restricting the from sending out tagged frames to clients connected on

Parameter	Description	Range	Default
`enet-vlan <vlan-ID>`	Configures VLAN for the upstream switch to which the OAW-IAP is connected.	1–4093	1
`no…`	Removes the configuration.	—	—

Example

The following example configures a non-default VLAN value for the Ethernet ports:

```
(Instant AP)(config)# enet-vlan 200
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet0-bridging

```
enet0-bridging
```

Description

This command allows you to use all ports on the OAW-IAPs as downlink ports. Use this command for OAW-IAP models that have only one Ethernet port enabled. When Ethernet 0 bridging is configured, ensure that the uplink for each OAW-IAP is mesh link, Wi-Fi, or 3G or 4G.

Example

The following command enables Ethernet 0 bridging:

```
(Instant AP)# enet0-bridging
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

enet0-port-profile

```
enet0-port-profile <profile>
```

Description

This command assigns a wired profile to the ENET 0 port on an OAW-IAP.

Syntax

Parameter	Description	Range	Default
`enet0-port-profile <profile>`	Assigns a wired profile to the ENET 0 interface port.	—	—

Usage Guidelines

Use this command to assign a wired profile to the ENET 0 port to activate the wired profile.

Example

The following command assigns a wired profile to the ENET 0 port:

```
(Instant AP)(config)# enet0-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet1-port-profile

```
enet1-port-profile <profile>
```

Description

This command assigns a wired profile to the ENET 1 port on an OAW-IAP.

Parameter	Description	Range	Default
`enet1-port-profile <profile>`	Assigns a wired profile to the ENET 1 interface port.	—	—

Example

The following command assigns a wired profile to the ENET 1 port:

```
(Instant AP)(config)# enet1-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet2-port-profile

```
enet2-port-profile <profile>
```

Description

This command assigns and activates a wired profile on the Ethernet 2 port on an OAW-IAP.

Parameter	Description	Range	Default
`enet2-port-profile <profile>`	Assigns a wired profile to the Ethernet 2 interface port.	—	—

Example

The following command assigns a wired profile to the Ethernet 2 port:

```
(Instant AP)(config)# enet2-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet3-port-profile

```
enet3-port-profile <profile>
```

Description

This command assigns and activates a wired profile on the Ethernet 3 port on an OAW-IAP.

Parameter	Description	Range	Default
`enet3-port-profile <profile>`	Assigns a wired profile to the Ethernet 3 interface port.	—	—

Example

The following command assigns a wired profile to the Ethernet 3 port:

```
(Instant AP)(config)# enet3-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet4-port-profile

```
enet4-port-profile <profile>
```

Description

This command assigns and activates a wired profile on the Ethernet 4 port on an OAW-IAP.

Parameter	Description	Range	Default
`enet4-port-profile <profile>`	Assigns a wired profile to the Ethernet 4 interface port.	—	—

Example

The following command assigns a wired profile to the Ethernet 4 port:

```
(Instant AP)(config)# enet4-port-profile <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enet-usb-port-profile

```
enet-usb-port-profile <profile>
```

Description

This command configures the USB port on the AP as a wired Ethernet port.

Parameter	Description	Range	Default
`<profile>`	Denotes the wired port profile.	—	—

Example

The following command onfigures the USB port on the AP as a wired Ethernet port:

```
(Instant AP)(config)# enet-usb-port-profile <profile>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enhanced-mesh-role-detect

```
enhanced-mesh-role-detect
no…
```

Description

This command enables mesh role detection during OAW-IAP boot up and OAW-IAP running time.

Parameter	Description	Range	Default
`no…`	Removes the enhanced mesh role detection configuration.	—	—

Example

The following example enables the configuration of **enhanced mesh-role-detect** command:

```
(Instant AP)(config)# enhanced-mesh-role-detect
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

enhanced-voice-tracking-traps-disable

```
enhanced-voice-tracking-traps-disable
no enhanced-voice-tracking-traps-disable
```

Description

This command is used to disable SNMP traps messages sent for voice calls. By default, it is enabled.

Parameter	Description
`enhanced-voice-tracking-traps-disable`	Disables the sending of SNMP traps messages for voice calls.
`no enhanced-voice-tracking-traps-disable`	Enables the sending of SNMP traps messages for voice calls.

Example

The following example disables the sending of SNMP traps messages for voice calls:

```
(Instant AP)(config)# enhanced-voice-tracking-traps-disable
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

est-activate

```
est-activate <profile_name>
```

Description

This command is used to activate an existing EST profile on the OAW-IAP.

Parameter	Description
`<profile_name>`	Denotes the profile name of the EST profile to be activated.

Example

The following command activates an EST profile:

```
(Instant AP)(config)# est-activate est-test-profile
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Configuration mode.

est profile

```
est profile <profile_name>
  arbitrary-label <arbitrary-label>
  arbitrary-label-enrollment <arbitrary-label-enrollment>
  arbitrary-label-reenrollment <arbitrary-label-reenrollment>
  challenge-password <challenge-password>
  organizational-unit-name <name>
  server-host <server-host>
  server-port <server-port>
  trust-anchor<trustanchor-name>
  username <username>
  password <password>
  no..
```

Description

This command configures an EST profile on the OAW-IAP. Use this command to configure an EST profile and setup automatic enrollment and re-enrollment of custom certificates on the OAW-IAP.

Parameter	Description
`profile <profile_name>`	Denotes the profile name of the EST profile.
`arbitrary-label <arbitrary-label>`	Sets an arbitrary label for the EST URI to distinguish it from the other EST profiles running on the EST server.
`arbitrary-label-enrolment <arbitrary-label-enrollment>`	Sets an arbitrary enrollment label for EST URI.
`arbitrary-label-reenrolment <arbitrary-label-reenrollment>`	Sets an arbitrary re-enrollment label for EST URI.
`challenge-password <challenge-password>`	Sets a challenge password used in CSR.
`organizational-unit-name <name>`	Sets the organizational unit name. String length: 1 to 63
`server-host <server-host>`	Denotes the IPv4 address or the hostname of the EST server.
`server-port <server-port>`	Indicates the port value of the EST server. The default value is 443.
`trust-anchor <trustanchor-name>`	Denotes the server's trust anchor.

Parameter	Description
`username <username>`	Sets an username for the EST Client.
`password <password>`	Sets a password for the EST Client.
`no..`	Deletes the configuration.

Example

The following command configures an EST profile:

```
(Instant AP)(config)# est profile est-new
(Instant AP)(est profile "est-new" )# server-host 10.15.33.232
(Instant AP)(est profile "est-new" )# server-port 443
(Instant AP)(est profile "est-new" )# arbitrary-label /ca:2
(Instant AP)(est profile "est-new" )#arbitrary-label-enrollment /ca:7
(Instant AP)(est profile "est-new" )#arbitrary-label-reenrollment /ca:7
(Instant AP)(est profile "est-new" )# challenge-password pass123
(Instant AP)(est profile "est-new" )# trust-anchor trust456
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Config mode and config submode of **est profile** command.

extended-ssid

```
extended-ssid
no…
```

Description

This command allows you to configure additional WLAN SSIDs. Extended SSID is enabled in the factory default settings of OAW-IAPs. You cannot disable the extended SSID in the factory default mode.

By default, you can create up to six WLAN SSIDs. With the Extended SSID option enabled, you can create up to 16 WLANs. However, if more than 16 SSIDs are assigned to a zone, you will receive an error message when you disable extended zone.

Parameter	Description	Range	Default
`extended-ssid`	Enables the users to configure additional SSIDs.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables the configuration of extended SSIDs:

```
(Instant AP)(config)# extended-ssid
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

facebook

```
facebook <id> <secret>
```

Description

This command saves the Facebook ID and secret text that are generated after registering an OAW-IAP with Facebook.

Parameter	Description	Range	Default
`<id>`	Indicates the ID generated after an OAW-IAP is successfully registered with Facebook.	—	—
`<secret>`	Indicates the secret key that is returned after a successful registration of an OAW-IAP with Facebook.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

factory-ssid-enable

```
factory-ssid-enable
```

Description

This command resets the OAW-IAP to use the factory default SSID.

Parameter	Description	Range	Default
`factory-ssid-enable`	Enables factory SSID configuration.	—	—

Example

The following example enables factory default configuration:

```
(Instant AP)(config)# factory-ssid-enable
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

firewall

```
firewall
   disable-auto-topology-rules
   no…
```

Description

This command allows control over the ACEs that are automatically programmed due to expansion of the ACLs. Use this command to remove the default auto topology rules created for predefined ACLs and WLAN Access Rules. When **disable-auto-topology-rules** is configured on the OAW-IAP and the Inbound Firewall rule is set using the AOS-W Instant UI, the user rules take precedence over the guest VLAN ACL expansion and overrides the auto-expanded rules. However, the corporate and local VLAN expansions will continue to take precedence over the user rules.

Parameter	Description	Range	Default
`firewall`	Opens the firewall configuration mode.	—	—
`disable-auto-topology-rules`	Disables the default auto topology rule that is created for predefined ACLs and WLAN Access Rules.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Example

The following example disables the default auto topology rules on an OAW-IAP:

```
(Instant AP)(config)# firewall
(Instant AP)(firewall)# disable-auto-topology-rules
(Instant AP)(firewall)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and firewall sub-mode.

firewall-external-enforcement

```
firewall-external-enforcement pan
   disable
   domain-name <name>
   enable
   ip <address>
   port <port>
   user <name> <password>
   no…
```

Description

This command configures external firewall details such as PAN firewall to enable integration with the OAW-IAP. The PAN firewall is based on user ID, which provides many methods to connect to the sources of identity information and associate them with firewall policy rules. This feature requires information from the network. OAW-IAP maintains the network and user information such as IP address mapping of the clients in the network, and provides the required information for the user ID feature on PAN firewall.

To enable OAW-IAP integration with PAN firewall, configure a global profile on OAW-IAP with PAN firewall information such as IP address, port, user name, password, firewall enabled or disabled status.

Parameter	Description	Range	Default
`firewall-external-enforcement pan`	PAN firewall configuration sub-mode.	—	—
`disable`	Disables PAN firewall.	—	—
`enable`	Enables PAN firewall.	—	—
`ip <address>`	Configures PAN firewall IP address on the OAW-IAP	—	—
`port <port>`	Configures a port for the PAN firewall.	1—65535	443
`user <name> <password>`	Configures administrator user credentials of PAN firewall on an OAW-IAP.	—	—
`domain-name <name>`	Configures a static domain name to be prefixed with the client user id sent to the PAN firewall.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Example

The following example configures PAN firewall information on an OAW-IAP:

```
(Instant AP)(config)# firewall-external-enforcement pan
(Instant AP)(firewall-external-enforcement pan)# enable
(Instant AP)(firewall-external-enforcement pan)# domain-name domain@xyz
(Instant AP)(firewall-external-enforcement pan)# ip 192.0.2.11
(Instant AP)(firewall-external-enforcement pan)# port 443
(Instant AP)(firewall-external-enforcement pan)# user admin1 admin1
(Instant AP)(firewall-external-enforcement pan)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and firewall-external-enforcement sub-mode.

flex-radio-mode

```
flex-radio-mode <mode>
```

Description

This action command is used to configure the flexible radio mode on OAW-AP203R/OAW-AP203RP access points.

Parameter	Description	Range	Default
`flex-radio-mode`	Specifies the flexible radio mode configured on the OAW-IAP.	—	—
`<mode>`	Denotes the type of radio mode configured on the OAW-IAP. The flexible radio can be configured in one of the following modes: ■ 2.4ghz—Acts as a single radio operating on 2.4 GHz band. ■ 5ghz—Acts as a single radio operating on 5 GHz band. ■ 2.4ghz-and-5ghz—Acts as two radios (interfaces), one operating on 5 GHz band, and the other on the 2.4 GHz band. By default, the flexible radio is set to this mode.	2.4ghz, 5ghz, 2.4ghz-and-5ghz.	2.4ghz-and-5ghz

Example

The following example enables the factory default configuration:

```
(Instant AP)# flex-radio-mode 5ghz
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP203R/OAW-AP203RP	Privileged EXEC mode.

flow-offload

```
flow-offload
no...
```

Description

This command configures hardware offloading for the OAW-IAP.

Parameter	Description
`flow-offload`	Offloads some data processing flows from the software to the hardware of the AP.
`no...`	Removes the configuration.

Example

The following example enables hardware offloading on the OAW-IAP:

```
(Instant AP)#config
(Instant AP)(config)#flow-offload
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-AP535 and OAW-AP555 access points	Configuration mode

g-channel

```
g-channel <channel> <tx-power>
```

Description

This command configures 2.4 GHz radio channels for a specific OAW-IAP.

Parameter	Description	Range	Default
`<channel>`	Configures the specified 2.4 GHz channel.	The valid channels for a band are determined by the OAW-IAP regulatory domain.	—
`<tx-power>`	Configures the specified transmission power values. It also supports 0.1 dBm and negative values.	-51 dBm to 51 dBm.	—

Example

The following example configures the 2.4 GHz radio channel:

```
(Instant AP)# g-channel 11 18
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

g-external-antenna

```
g-external-antenna <gain>
```

Description

This command configures external antenna connectors for an OAW-IAP.

If your OAW-IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the OAW-IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your OAW-IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the OAW-IAP device.

Parameter	Description	Range	Default
<gain>	Configures the antenna gain. You can configure gain value in dBi for the following types of antenna: ■ Dipole or Omni ■ Panel ■ Sector	Diploe or Omni - 6 Panel -12 Sector - 12	—

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 10: *Formula Variable Definitions*

Formula Element	Modification
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

For information on antenna gain recommended by the manufacturer, see .

Example

The following example configures external antenna connectors for the OAW-IAP with the 2.4 GHz radio band.

```
(Instant AP)# g-external-antenna 12
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

g-ant-pol

```
g-ant-pol <pol>
```

Description

This command configures the antenna polarization value for 2.4 GHz radio channels.

Parameter	Description	Range	Default
`<pol>`	Denotes the antenna polarization value for 2.4 GHz radio channel. ■ 0: Co-Polarized radio ID ■ 1: Cross-Polarized radio ID	0 or 1	—

Example

The following example configures the antenna polarization value for a 2.4 GHz radio channel:

```
(Instant AP)# g-ant-pol 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

g-max-clients

```
g-max-clients <ssid_profile> <max-clients>
```

Description

This command configures the maximum number of clients allowed for an SSID profile on a 2.4 GHz radio channel. This is a per-AP and per-Radio configuration.

Parameter	Description	Range	Default
`<ssid_profile>`	Denotes the SSID profile for which the maximum clients limit is to be configured.	—	—
`<max-clients>`	Denotes the maximum number of clients that can be configured on the 2.4 GHz radio channel of the OAW-IAP.	1–255	—

Example

The following example configures the maximum number of clients for a 2.4 GHz radio channel:

```
(Instant AP)# g-max-clients test1 77
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **ssid_profile** parameter is added.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

gre

```
gre
   primary <name>
   backup <name>
   disable-preemption
   disable-reconnect-user-on-failover
   hold-time <hold_time>
   per-ap-tunnel
   ping-frequency <freq>
   ping-retry-count <new_count>
   reconnect-time-on-failover <down_time>
   type <type>
no…
```

Description

This command allows you to manually configure an IPv4 or IPv6 GRE tunnel on an OAW-IAP.

Parameter	Description	Range	Default
`primary <name>`	Denotes the primary GRE tunnel IP address or domain name.	—	—
`backup <name>`	Denotes the secondary GRE tunnel IP address or domain name.	—	—
`disable-preemption`	Disables the hold on timer from running on the OAW-IAP.	—	—
`disable-reconnect-user-on-failover`	Prevents the SSIDs from being disabled when a GRE tunnel failover occurs.	—	—
`hold-time <hold_time>`	Configures the hold time for the GRE tunnel failover. When preemption is enabled, and the primary GRE tunnel is UP, the GRE tunnel connection will switch to the primary tunnel after the specified hold time.	30-900 seconds.	600 seconds

Parameter	Description	Range	Default
`per-ap-tunnel`	Enables allOAW-IAPs in a cluster to form individual GRE tunnels to the endpoints. The tunnel failover will be determined by the Master AP in the cluster. The slave APs will sync its GRE tunnel endpoint to the same endpoint as the master AP to ensure uniformity in the tunnel endpoint across the cluster.	—	—
`ping-frequency <freq>`	Denotes the ping interval.	10-60 seconds	15 seconds
`ping-retry-count <new_count>`	Denotes the number of ping packets missed to mark the tunnel down status.	2-10	3
`reconnect-time-on-failover <down_time>`	Denotes the time to disable SSIDs.	—	—
`type <type>`	Configures the protocol number for the GRE type.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a IPv4 or IPv6 GRE tunnel :

```
(Instant AP)(config)# gre primary pendpoint@arubanetworks.com
(Instant AP)(config)# gre backup sendpoint@arubanetworks.com
(Instant AP)(config)# gre disable-preemption
(Instant AP)(config)# gre disable-reconnect-user-on-failover
(Instant AP)(config)# gre hold-time 600
(Instant AP)(config)# gre per-ap-tunnel
(Instant AP)(config)# gre ping-frequency 15
(Instant AP)(config)# gre ping-retry-count <new_count>
(Instant AP)(config)# gre reconnect-time-on-failover <down_time>
(Instant AP)(config)# gre type 25944
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.4.0.0	The following parameters were introduced:

Release	Modification
	■ backup <name> ■ disable-reconnect-user-on-failover ■ reconnect-time-on-failover <down_time> ■ ping-retry-count <new_count> ■ ping-frequency <freq> ■ disable-preemption ■ hold-time <hold_time>
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

hash-mgmt-password

```
hash-mgmt-password
```

Description

This command enables hashing of the management user password.

When this command is configured, the **mgmt-user** command will not longer be available to add, modify, or remove management users. You will be redirected to the **hash-mgmt-user** command to add, modify, or remove management users.

Example

The following example enables password hashing for management users:

```
(Instant AP)(config) # hash-mgmt-password
(Instant AP)(config) # end
(Instant AP) # commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

hash-mgmt-user

```
hash-mgmt-user <username> password {{cleartext <cleartext_password>} | {hash <hash_password>
}} [usertype <type>]
no...
```

Description

This command is used to configure management users by using clear text or hash as the password input.

After you configure the **hash-mgmt-password** command, the **mgmt-user** command will no longer be valid. You will be directed to this command for management user configuration.

Parameter	Description	Range	Default
`<username>`	Indicates the username of the management user.	—	—
`password`	Indicates the management user password.	—	—
`cleartext`	Indicates if a user will enable clear text as the password input format.	—	—
`<cleartext_password>`	Indicates the password in plain text format.	—	—
`hash`	Indicates that the input password is in hash format.	—	—
`<hash_password>`	Indicates the password in hash format.	—	—
`usertype`	Indicates the type of management user.	—	—
`<type>`	Indicates the type of management user. For example, users with guest-management, local, or read-only privilege.	—	—
`no`	Removes the management user configuration.	—	—

Example

The following example adds a management user with read-only privilege:

```
(Instant AP)(config) # hash-mgmt-user john password cleartext password01 usertype read-only
(Instant AP)(config) # end
(Instant AP) # commit apply
```

The following examples removes a management user with read-only privilege:

```
(Instant AP)(config) # no hash-mgmt-user read-only
(Instant AP)(config) # end
(Instant AP) # commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

help

```
help
```

Description

This command displays keyboard editing commands that allow you to make corrections or changes to the command without retyping.

You can also enter the question mark (?) to get various types of command help:

- When typed at the beginning of a line, the question mark lists all commands available in the current mode.
- When typed at the end of a command or abbreviation, the question mark lists possible commands that match.
- When typed in place of a parameter, the question mark lists available options.

Example

The following example shows the output of the **help** command.

```
HELP:
Special keys:
BS       .... delete previous character
Ctrl-A   .... go to beginning of line
Ctrl-E   .... go to end of line
Ctrl-F   .... go forward one character
Ctrl-B   .... go backward one character
Ctrl-D   .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K   .... delete to end of line
Ctrl-W   .... delete previous word
Ctrl-T   .... transpose previous character
Ctrl-P   .... go to previous line in history buffer
Ctrl-N   .... go to next line in history buffer
Ctrl-Z   .... return to root command prompt
Tab      .... command-line completion
exit     .... go to next lower command prompt
?        .... list choices
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show w?'.)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

hostname

```
hostname <system_name>
```

Description

This command changes the hostname of the Virtual Controller.

The hostname is used as the default prompt. You can use any alphanumeric character, punctuation, or symbol characters. When spaces, plus symbols (+), question marks (?), or asterisks (*) are used, enclose the text in quotes.

NOTE

As a best practice, It is recommended to configure the hostname by using only **a-z**, **A-Z**, **0-9**, '**.**', '**-**', '**:**', '_' , but not special characters such as "**#$%**".

Parameter	Description	Range	Default
`<system_name>`	Configures a hostname for the Virtual Controller.	1-128 ASCII characters	—

Example

The following example configures host name for an OAW-IAP.

```
(Instant AP)# hostname IAP1
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The number of ASCII characters allowed in the OAW-IAP hostname was increased to 128 characters.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

hotspot anqp-3gpp-profile

```
hotspot anqp-3gpp-profile <profile-name>
   3gpp-plmn1…3gpp-plmn6 <PLMN-ID>
   enable
   no…
```

Description

This command configures a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.

The IE defined in this profile will be sent in a GAS query response from an OAW-IAP in a cellular network hotspot. The 3GPP MCC and the 12-bit Mobile Network Code data in the IE can help the client select a 3GPP network when associated with a hotspot profile and enabled on a WLAN SSID profile.

Parameter	Description	Range	Default
`hotspot anqp-3gpp-profile <profile-name>`	Creates a 3GPP profile.	—	—
`3gpp-plmn1…3gpp-plmn6 <PLMN-ID>`	Configures the PLMN value of the network. The PLMN value can be specified for first, second, third, fourth, fifth, and sixth highest priority network. The PLMN ID consists of a 12-bit MCC and the 12-bit MNC.	—	—
`enable`	Activates the configuration profile.	—	—
`no…`	Removes the configuration	—	—

Example

The following command configures a 3GPP profile:

```
(Instant AP)(config)# hotspot anqp-3gpp-profile cellcorp1
(Instant AP)(3gpp "cellcorp1")# 3gpp-plmn1 310026
(Instant AP)(3gpp "cellcorp1")# 3gpp_plmn2 208000
(Instant AP)(3gpp "cellcorp1")# 3gpp_plmn3 208001
(Instant AP)(3gpp "cellcorp1")# enable
(Instant AP)(3gpp "cellcorp1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the 3GPP hotspot profile configuration sub-mode

hotspot anqp-domain-name-profile

```
hotspot anqp-domain-name-profile <profile-name>
   domain-name <domain-name>
   enable
   no…
```

Description

This command defines the domain name to be sent in an ANQP information element in a GAS query response.

If a client uses the GAS to post an ANQP query to an OAW-IAP, the OAW-IAP will return an ANQP Information Element with the domain name when this profile is associated with a hotspot profile and enabled on a WLAN SSID profile.

Parameter	Description	Range	Default
`hotspot anqp-domain-name-profile <profile-name>`	Creates a domain profile.	—	—
`domain-name <domain-name>`	Configures a domain name of the hotspot operator.	—	—
`enable`	Enables the configuration profile.	—	—
`no…`	Removes the existing configuration	—	—

Example

The following command defines a domain name for the ANQP domain name profile:

```
(Instant AP)(config)# hotspot anqp-domain-name-profile domain1
(Instant AP)(domain-name "domain1")# domain-name example.com
(Instant AP)(domain-name "domain1")# enable
(Instant AP)(domain-name "domain1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the ANQP domain profile configuration sub-mode

hotspot anqp-ip-addr-avail-profile

```
hotspot anqp-ip-addr-avail-profile <profile-name>
   enable
   ipv4-addr-avail <ipv4>
   ipv6-addr-avail <ip46>
   no…
```

Description

This command defines the available IP address types to be sent in an ANQP information element in a GAS query response.

Parameter	Description		
`hotspot anqp-ip-addr-avail-profile <profile-name>`	Creates an ANQP IP Address availability profile.	—	—
`enable`	Enables the IP address availability profile.	—	—
`ipv4-addr-avail <ipv4>`	Indicates the availability of an IPv4 network. It can take one of the following values: ■ public ■ port-restricted ■ single-nated-private ■ double-nated- private ■ port-restricted-single-nated-private ■ port-restricted-double-nated-private ■ not-available	—	—
`ipv6-addr-avail <ipv6>`	Indicates the availability of an IPv6 network. This can take one of the following values: ■ available ■ not-available	—	—
`no…`	Removes the existing configuration.	—	—

Example

The following command configures an OAW-IAP using this profile to advertise a public IPv4 network.

```
(Instant AP)(config)# hotspot anqp-ip-addr-avail-profile default
```

```
(Instant AP)(IP-addr-avail "default")# ipv4-addr-avail
(Instant AP)(IP-addr-avail "default")# ipv6-addr-avail
(Instant AP)(IP-addr-avail "default")# enable
(Instant AP)(IP-addr-avail "default")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the ANQP IP address availability profile configuration sub-mode

hotspot anqp-nai-realm-profile

```
hotspot anqp-nai-realm-profile <profile-name>
   enable
   nai-home-realm
   nai-realm-auth-id-1 <auth-ID>
   nai-realm-auth-id-2 <auth-ID>
   nai-realm-auth-value-1 <auth-value>
   nai-realm-auth-value-2 <auth-value>
   nai-realm-eap-method <eap-method>
   nai-realm-encoding <encoding>
   nai-realm-name <name>
   no…
```

Description

This command defines a NAI realm information that can be sent as an ANQP information element in a GAS query response.

The settings configured in this profile determine the NAI realm elements that are included as part of a GAS Response frame.

Parameter	Description	Range	Default
`hotspot anqp-nai-realm-profile <profile-name>`	Configures a NAI realm hotspot profile.	—	—
`enable`	Enables the NAI realm profile.	—	—
`nai-home-realm`	Sets the realm in this profile as the NAI Home Realm.	—	—
`nai-realm-auth-id-1` `nai-realm-auth-id-2`	Configures the NAI realm authentication ID. Use the **nai-realm-auth-id-1** command to send the one of the following authentication methods for the primary NAI realm ID. Use the **nai-realm-auth-id-2** command to send the one of the following authentication methods for the secondary NAI realm ID.	—	—
`<auth-id>`	Configures any of the following types of authentication ID: ■ **credential**— Uses credential authentication. ■ **eap-inner-auth**— Uses EAP inner authentication type.	credential eap-inner-auth exp-inner-auth expanded-eap non-eap-inner-auth reserved	—

Parameter	Description	Range	Defau-lt
	■ **exp-inner-eap**—Uses the expanded inner EAP authentication method. ■ **expanded-eap**—Uses the expanded EAP authentication method. ■ **non-eap-inner-auth**—Uses non-EAP inner authentication type. ■ **reserved**—Uses the reserved authentication method.		
`nai-realm-auth-value-1` `nai-realm-auth-value-2`	Configures a value for NAI realm authentication. Use the **nai-realm-auth-value-1** command to select an authentication value for the authentication method specified by **nai-realm-auth-id-1**. Use the**nai-realm-auth-value-2** command to select the authentication value for the authentication method specified by**nai-realm-auth-id-2**.	—	—
`<auth-value>`	Configures any of following types of authentication values for the specified <auth-id>: ■ For **credential** <auth-ID>, specify the following values: ■ sim ■ usim ■ nfc-secure ■ hw-token ■ softoken ■ certificate ■ uname-passward ■ none ■ reserve	sim, usim. nfc-secure, hw-token, softoken, certificate, uname-password, none, reserved, vendor-specific reserved, pap chap, mschap, mschapv2, exp-inner-eap, expanded-eap, reserved	—

Parameter	Description	Range	Default
	d ■ vendor-specific ■ For **eap-inner-auth** <aut- ID>, specify the following values: ■ reserved ■ pap ■ chap ■ mschap ■ mschapv2 ■ For **exp-inner-eap** <auth-ID>, specify **exp-inner-eap** as the authentication value. ■ For **expanded-eap**<auth-ID>, specify **expanded-eap** as the authentication value ■ For **non-eap-inner-auth**<auth-ID> specify any of the following values: ■ reserved ■ pap ■ chap ■ mschap ■ mschapv2		
`nai-realm-eap-method`	Configures an EAP method for NAI realm.		—
`<eap-method>`	Configures any of the following EAP methods: ■ **crypto-card**—Crypto card authentication ■ **eap-aka**—EAP for UMTS Authentication and Key Agreement ■ **eap-sim**—EAP for GSM SIMs ■ **eap-tls**—EAP-Transport Layer Security ■ **eap-ttls**—EAP-Tunneled Transport	crypto-card, eap-aka, eap-sim, eap-tls, eap-ttls, generic-token-card, identity notification, one-time-password, peap, peapmschapv2	—

Parameter	Description	Range	Defau-lt
	Layer Security ■ **generic-token-card**—EAP-Generic Token Card ■ **identity**— EAP Identity type ■ **notification**—The hotspot realm uses EAP Notification messages for authentication. ■ **one-time-password**—Authentication with a single-use password ■ **peap**—Protected EAP ■ **peapmschapv2**—Protected EAP with Microsoft CHAP version 2		
`nai-realm-encoding <encoding>`	Configures a UTF-8 or rfc4282 formatted character string for NAI realm encoding.	rfc4282, utf8	—
`nai-realm-name <nai-realm-name>`	Configures a name for the NAI realm. The realm name is often the domain name of the service provider.	—	—
`no…`	Removes any existing configuration.	—	—

Example

The following example creates an NAI realm profile:

```
(Instant AP)(config)# hotspot anqp-nai-realm-profile home
(Instant AP)(nai-realm "home")# nai-realm-name home-hotspot.com
(Instant AP)(nai-realm "home")# nai-realm-encoding utf8
(Instant AP)(nai-realm "home")# nai-realm-eap-method eap-sim
(Instant AP)(nai-realm "home")# nai-realm-auth-id-1 non-eap-inner-auth
(Instant AP)(nai-realm "home")# nai-realm-auth-value-1 mschapv2
(Instant AP)(nai-realm "home")# nai-home-realm
(Instant AP)(nai-realm "home")# enable
(Instant AP)(nai-realm "home")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the NAI realm profile configuration sub-mode

hotspot anqp-nwk-auth-profile

```
hotspot anqp-nwk-auth-profile <profile-name>
  enable
  nwk-auth-type <auth-type>
  url <url>
  no...
```

Description

This command configures an ANQP network authentication profile to define authentication type being used by the hotspot network.

When the **asra** option is enabled in the hotspot profile associated with a WLAN SSID, the settings configured for the network authentication profile are sent in the GAS response to the client.

Parameter	Description	Range	Default
`hotspot anqp-nwk-auth-profile <profile-name>`	Configures an ANQP network authentication profile.	—	—
`enable`	Enables the network authentication profile.	—	—
`nwk-auth-type`	Defines the network Authentication type being used by the hotspot network.	—	—
`<auth-type>`	Allows you to specify any of the following values: ■ **accept-term-and-cond**—When configured, the network requires the user to accept terms and conditions. **NOTE:** This option requires you to specify a redirection URL string as an IP address, FQDN or URL. ■ **online-enrollment**—When configured, the network supports the online enrollment. ■ **http-redirect**—When configured, additional information on the network is provided through HTTP or HTTPS redirection. ■ **dns-redirect**—When configured, additional information on the network is provided through DNS redirection. **NOTE:** This option requires you to specify a redirection URL string as an IP address, FQDN or URL.	accept-term-and-cond, online-enrollment, http-redirect, dns-redirect	—

Parameter	Description	Range	Default
url	Configures URL, IP address, or FQDN used by the hotspot network for the **accept-term-and-cond** or **dns-redirect** network authentication types.	—	—
no…	Removes any existing configuration.	—	—

Example

The following command configures a network authentication profile for DNS redirection.

```
(Instant AP)(config)# hotspot anqp-nwk-auth-profile default
(Instant AP)(network-auth "default")# nwk-auth-type dns-redirection
(Instant AP)(network-auth "default")# url http://www.example.com
(Instant AP)(network-auth "default")# enable
(Instant AP)(network-auth "default")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the ANQP network authentication profile configuration sub-mode

hotspot anqp-roam-cons-profile

```
hotspot anqp-roam-cons-profile <profile-name>
   enable
   roam-cons-oi <roam-cons-oi>
   roam-cons-oi-len <roam-cons-oi-len>
   no…
```

Description

This command configures the Roaming Consortium OI information to be sent in an ANQP information element in a GAS query response.

The Roaming Consortium Information Elements contain information about the network and service provider, whose security credentials can be used to authenticate with the OAW-IAP transmitting this IE.

Parameter	Description	Range	Default
`hotspot anqp-roam-cons-profile <profile-name>`	Creates roaming consortium profile.	—	—
`enable`	Enables the roaming consortium profile.	—	—
`roam-cons-oi <roam-cons-oi>`	Sends the specified roaming consortium OI in a GAS query response. The OI must be a hexadecimal number 3-5 octets in length.	Hexadecimal number 3-5 octets in length	—
`roam-cons-oi-len <roam-cons-oi-len>`	Indicates the length of the OI. The value of the **roam-cons-oi-len** parameter must equal upon the number of octets of the **roam-cons-oi** field. ■ **0**: 0 Octets in the OI (Null) ■ **3**: OI length is 24-bit (3 Octets) ■ **5**: OI length is 36-bit (5 Octets)	—	—
`no…`	Removes any existing configuration.	—	—

Example

The following command defines the roaming consortium OI and OI length in the ANQP roaming consortium profile:

```
(Instant AP)(config)# hotspot anqp-roam-cons-profile profile1
(Instant AP)(roaming-consortium "profile1")# roam-cons-oi 506F9A
(Instant AP)(roaming-consortium "profile1")# roam-cons-oi-len 3
(Instant AP)(roaming-consortium "profile1")# enable
(Instant AP)(roaming-consortium "profile1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the ANQP roaming consortium profile configuration sub-mode

hotspot anqp-venue-name-profile

```
hotspot anqp-venue-name-profile <profile-name>
   enable
   venue-group <group>
   venue-lang-code <language>
   venue-name <name>
   venue-type <type>
   no…
```

Description

This command defines venue information be sent in an ANQP information element in a GAS query response.

If a client uses the GAS to post an ANQP query to an Access Point, the OAW-IAP will return ANQP Information Elements with the values configured in this profile.

Parameter	Description	Range	Default
`hotspot anqp-venue-name-profile <profile-name>`	Creates a ANQP venue name profile.	—	—
`enable`	Enables the ANQP venue name profile.	—	—
`venue-group <group>`	Configures one of the following venue groups to be advertised in the IEs from OAW-IAPs associated with this hotspot profile. ■ assembly ■ business ■ educational ■ factory-and-industrial ■ institutional ■ mercantile ■ outdoor ■ residential ■ storage ■ utility-and-misc ■ vehicular **NOTE:** This parameter only defines the venue group advertised in the IEs from hotspot OAW-IAPs. To define the venue group to be included in ANQP responses, use **anqp-venue-name-profile <profile-name>** command.	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	unspecified

Parameter	Description	Range	Default
`venue-lang-code <language>`	Configures an ISO 639 language code that identifies the language used in the Venue Name field.	—	—
`venue-name <name>`	Configures the venue name to be advertised in the ANQP IEs. If the venue name includes spaces, the name must be enclosed in quotation marks, e.g. “Midtown Shopping Center”.	—	—
`venue-type <type>`	Specifies the venue type to be advertised in the IEs.	The complete list of supported venue types is described in hotspot anqp-venue-name-profile on page 195.	unspecified
`no…`	Removes any existing configuration.	—	—

Venue Types

The following list describes the different venue types for each venue group:

Venue Group	Associated Venue Type Value
`assembly`	■ arena ■ stadium ■ passenger-terminal ■ amphitheater ■ amusement-park ■ place-of-worship ■ convention-center ■ library ■ museum ■ restaurant ■ theater ■ bar ■ coffee-shop ■ zoo-or-aquarium ■ emergency-cord-center ■ unspecified
`business`	■ doctor ■ bank ■ fire-station ■ police-station ■ post-office ■ professional-office ■ research-and-dev-facility ■ attorney-office ■ unspecified
`educational`	■ school-primary

Venue Group	Associated Venue Type Value
	■ school-secondary ■ univ-or-college ■ unspecified
`factory-and-industrial`	■ factory ■ unspecified
`institutional`	■ hospital ■ long-term-care ■ alc-drug-rehab ■ group-home ■ prison-or-jail ■ unspecified
`mercantile`	■ retail-store ■ grocery-market ■ auto-service-station ■ shopping-mall ■ gas-station ■ unspecified
`outdoor`	■ muni-mesh-network ■ city-park ■ rest-area ■ traffic-control ■ bus-stop ■ kisok ■ unspecified
`residential`	■ private-residence ■ hotel ■ dormitory ■ boarding-house ■ unspecified
`storage`	unspecified
`utility-and-misc`	unspecified
`vehicular`	■ unspecified ■ automobile-or-truck ■ airplane ■ bus ■ ferry ■ ship ■ train ■ motor-bike

Example

The following command defines an ANQP Venue Name profile for a shopping mall:

```
(Instant AP)(config)# hotspot anqp-venue-name-profile Mall1
(Instant AP)(venue-name "Mall1")# venue-name ShoppingCenter1
(Instant AP)(venue-name "Mall1")# venue-group mercantile
(Instant AP)(venue-name "Mall1")# venue-type shopping-mall
(Instant AP)(venue-name "Mall1")# venue-lang-code EN
(Instant AP)(venue-name "Mall1")# enable
(Instant AP)(venue-name "Mall1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the ANQP venue name profile configuration sub-mode

hotspot h2qp-conn-cap-profile

```
hotspot h2qp-conn-cap-profile <profile-name>
   enable
   esp-port
   icmp
   tcp-ftp
   tcp-http
   tcp-pptp-vpn
   tcp-ssh
   tcp-tls-vpn
   tcp-voip
   udp-ike2
   udp-ipsec-vpn
   udp-voip
   no...
```

Description

This command configures a H2QP profile that advertises hotspot protocol and port capabilities.

Parameter	Description	Range	Default
`hotspot h2qp-conn-cap-profile<profile-name>`	Creates a connection capability profile.	—	—
`enable`	Enables the connection capability H2QP profile.	—	—
`esp-port`	Enables the ESP port used by IPsec VPNs. (port 0)	—	—
`icmp`	Indicates that the ICMP port is enabled and available. (port 0)	—	—
`tcp-ftp`	Enables the FTP port. (port 20)	—	—
`tcp-http`	Enables the HTTP port. (port 80)	—	—
`tcp-pptp-vpn`	Enables the PPTP port used by IPsec VPNs. (port 1723)	—	—
`tcp-ssh`	Enables the SSH port. (port 22)	—	—
`tcp-tls-vpn`	Enables the TCP TLS port used by VPNs. (port 80)	—	—

Parameter	Description	Range	Default
tcp-voip	Enables the TCP VoIP port. (port 5060)	—	—
udp-ike2	Enables the IKEv2 port.	—	—
udp-ipsec-vpn	Enables the IPsec VPN port. (ports 500, 4500 and 0)	—	—
udp-voip	Enables the UDP VoIP port. (port 5060)	—	—
no…	Removes any existing configuration.	—	—

Example

The following example allows the H2QP connection capability profile to advertise the availability of ICMP and HTTP ports.

```
(Instant AP)(config) # hotspot h2qp-conn-cap-profile Wan1
(Instant AP)(connection-capabilities "Wan1")# icmp
(Instant AP)(connection-capabilities "Wan1")# tcp-http
(Instant AP)(connection-capabilities "Wan1")# enable
(Instant AP)(connection-capabilities "Wan1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the H2QP connection capability profile configuration sub-mode

hotspot h2qp-oper-name-profile

```
hotspot h2qp-oper-name-profile <profile>
   enable
   op-fr-name <name>
   op-lang-code <language>
   no…
```

Description

This command configures a H2QP operator-friendly name profile.

Parameter	Description	Range	Default
`hotspot h2qp-oper-name-profile <profile>`	Creates an operator-friendly name profile.	—	—
`enable`	Enables the operator-friendly name profile.	—	—
`op-fr-name <name>`	Configures an operator-friendly name to be sent by devices using this profile. If the name includes quotation marks (“), include a backslash character (\) before each quotation mark. (e.g. \"example\")	1-64 alphanumeric characters	—
`op-lang-code <language>`	Configures an ISO 639 language code that identifies the language used in the **op-fr-name** command.	—	—
`no…`	Removes any existing configuration.	—	—

Example

The following example configures an operator friendly profile:

```
(Instant AP)(config)# hotspot h2qp-oper-name-profile Profile1
(Instant AP)(operator-friendly-name "Profile1")# op-fr-name hotspot1
(Instant AP)(operator-friendly-name "Profile1")# op-lang-code EN
(Instant AP)(operator-friendly-name "Profile1")# enable
(Instant AP)(operator-friendly-name "Profile1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the H2QP operator friendly name profile configuration sub-mode

hotspot h2qp-oper-class-profile

```
hotspot h2qp-oper-class-profile <profile>
   enable
   op-class <class>
   no…
```

Description

This command configures a H2QP profile that defines the Operating Class to be sent in the H2QP IE.

Parameter	Description	Range	Default
`hotspot h2qp-oper-class-profile <profile>`	Creates operating class profile.	—	—
`enable`	Enables the operating class profile.	—	—
`op-class <class>`	Configures the operating class for the devices' BSS.	1-255	1
`no…`	Removes any existing configuration.	—	—

Example

The following example configures and enables a profile with the default operating class value.

```
(Instant AP)(config) # hotspot h2qp-oper-class-profile Profile1
(Instant AP)(operator-class"Profile1")# op-class 1
(Instant AP)(operator-class"Profile1")# enable
(Instant AP)(operator-class"Profile1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the H2QP operating class profile configuration sub-mode

hotspot h2qp-osu-provider-profile

```
hotspot h2qp-osu-provider-profile <profile>
   disable
   enable
   frnd-name-count <count>
   frnd-name1 <OSU Friendly name>
   frnd-name1-hex <OSU Friendly name>
   frnd-name1-lang-code <lang code>
   frnd-name2 <OSU Friendly name>
   frnd-name2-hex <OSU Friendly name>
   frnd-name2-lang-code <lang code>
   icon1-file <idx> <File Name>
   icon1-height <height>
   icon1-lang-code <lang code>
   icon1-type <file type>
   icon1-width <width>
   icon2-file <idx> <File Name>
   icon2-height <height>
   icon2-lang-code <lang code>
   icon2-type <file type>
   icon2-width <width>
   iconfile-count <count>
   no
   osu-method <OSU method>
   osu-server-uri <OSU server URI>
   srvc-desc1 <description>
   srvc-desc1-hex <description>
   srvc-desc1-lang-code <lang code>
   srvc-desc2 <description>
   srvc-desc2-hex <description>
   srvc-desc2-lang-code <lang code>
   srvcdesc-count <count>
```

Description

This command configures a H2QP profile that defines the Open Sign-Up(OSU) provider details to be sent in the H2QP IE.

Parameter	Description	Range	Default
`disable`	Disables the OSU provider profile.	—	—
`enable`	Enables the OSU provider profile. This is enabled by default.	—	—
`frnd-name-count`	Number of OSU friendly names to be configured.	1-2	—
`frnd-name1`	The first OSU friendly name if you selected the language code as English. A string value of maximum 64 characters.	—	—
`frnd-name1-hex`	The first OSU friendly name in hexadecimal format for language codes other than English.	—	—

Parameter	Description	Range	Default
`frnd-name1-lang-code`	The language code used for configuring the first OSU friendly name.	—	—
`frnd-name2`	The second OSU friendly name if the language code chosen is English. A string value of maximum 64 characters.	—	—
`frnd-name2-hex`	The second OSU friendly name in hexadecimal format for language codes other than English.	—	—
`frnd-name2-lang-code`	The language code used for configuring the second OSU friendly name.	—	—
`icon1-file`	The index and name of the first icon image file. **NOTE:** The index value and the filename value must match the file downloaded to OAW-IAP. For more information on downloading the icon file, refer to hs2-osu-icon-download.	—	—
`icon1-height`	Height of the first icon image file.	1-256	—
`icon1-lang-code`	Indicates the language used in the first icon image.	—	—
`icon1-type`	Type of the image file used as first icon.	—	—
`icon1-width`	Width of the first icon image file.	1-256	—
`icon2-file`	The index and name of the second icon image file. **NOTE:** The index value and the filename value must match the file downloaded to OAW-IAP. For more information on downloading the icon file, refer to hs2-osu-icon-download.	—	—
`icon2-height`	Height of the second icon image file.	—	—
`icon2-lang-code`	Indicates the language used in the second icon image.	—	—
`icon2-type`	Type of the image file used as second icon.	—	—
`icon2-width`	Width of the second icon image file.	—	—
`iconfile-count`	Number of icon files to be used for the OSU provider.	1-2	—
`no`	Deletes the command.	—	—
`osu-method`	Indicates the method used by OSU to provision the HS2 client.	■ OMA-DM ■ SOAP-	–

Parameter	Description	Range	Default
		XML	
osu-server-uri	The URI of the OSU Server that is used for OSU with the service provider configured in the **frnd-name1** parameter.	—	—
srvc-desc1	The first service description if you selected the language code as English.	—	—
srvc-desc1-hex	The first service description in hexadecimal format for language codes other than English.	—	—
srvc-desc1-lang-code	The language code used for the first description.	—	—
srvc-desc2	The second service description if you selected the language code as English.	—	—
srvc-desc2-hex	The second service description in hexadecimal format for language codes other than English.	—	—
srvc-desc2-lang-code	The second service description if you selected the language code as English.	—	—
srvcdesc-count	Number of descriptions to be provided for the OSU provider.	—	—

Example

The following example creates and configures an OSU provider profile:.

```
(Instant AP) (config) # hotspot h2qp-osu-provider-profile OSU
(Instant AP) (osu-provider OSU) # frnd-name-count 2
(Instant AP) (osu-provider OSU) # frnd-name1-lang-code "eng"
(Instant AP) (osu-provider OSU) # frnd-name1 "SP Red Test Only"
(Instant AP) (osu-provider OSU) # frnd-name1-hex
(Instant AP) (osu-provider OSU) # frnd-name2-lang-code "kor"
(Instant AP) (osu-provider OSU) # frnd-name2 ""
(Instant AP) (osu-provider OSU) # frnd-name2-hex
535020ebb9a8eab09520ed858cec8aa4ed8ab820eca084ec9aa9
(Instant AP) (osu-provider OSU) # iconfile-count 2
(Instant AP) (osu-provider OSU) # icon1-width 128
(Instant AP) (osu-provider OSU) # icon1-height 61
(Instant AP) (osu-provider OSU) # icon1-lang-code zxx
(Instant AP) (osu-provider OSU) # icon1-type image/png
(Instant AP) (osu-provider OSU) # icon1-file 1 "icon_red_zxx.png"
(Instant AP) (osu-provider OSU) # icon2-width 160
(Instant AP) (osu-provider OSU) # icon2-height 76
(Instant AP) (osu-provider OSU) # icon2-lang-code eng
(Instant AP) (osu-provider OSU) # icon2-type image/png
(Instant AP) (osu-provider OSU) # icon2-file 2 "icon_red_eng.png"
(Instant AP) (osu-provider OSU) # srvcdesc-count 2
(Instant AP) (osu-provider OSU) # srvc-desc1-lang-code eng
(Instant AP) (osu-provider OSU) # srvc-desc1 "Free service for test purpose"
(Instant AP) (osu-provider OSU) # srvc-desc1-hex
(Instant AP) (osu-provider OSU) # srvc-desc2-lang-code kor
(Instant AP) (osu-provider OSU) # srvc-desc2 ""
```

```
(Instant AP) (osu-provider OSU) # srvc-desc2-hex
ed858cec8aa4ed8ab820ebaaa9eca081ec9cbceba19c20ebacb4eba38c20ec849cebb984ec8aa4
(Instant AP) (osu-provider OSU) # osu-server-uri https://osu-server.r2-testbed-aru.wi-
fi.org:443/guest/HotSpot2OnlineSignUp.php
(Instant AP) (osu-provider OSU) # osu-method SOAP-XML
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the H2QP OSU provider profile configuration sub-mode

hotspot h2qp-wan-metrics-profile

```
hotspot h2qp-wan-metrics-profile <profile-name>
   at-capacity
   downlink-load <load>
   downlink-speed <speed>
   enable
   load-duration <duration>
   symm-link
   no
   uplink-load <load>
   uplink-speed <speed>
   wan-metrics-link-status <status>
```

Description

This command configures a H2QP profile that specifies the hotspot WAN status and link metrics.

Parameter	Description	Range	Default
`hotspot h2qp-wan-metrics-profile <profile-name>`	Creates a H2QP WAN metric profile	—	—
`at-capacity`	Indicates if the WAN Link has reached its maximum capacity. If this parameter is enabled, no additional mobile devices will be permitted to associate to the hotspot OAW-IAP.	—	—
`downlink-load <load>`	Configures the percentage of the WAN downlink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	1-100	0 (unspecified)

Parameter	Description	Range	Default
`downlink-speed <speed>`	Indicates the current WAN backhaul downlink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	0 - 2,147,483,647 Kbps	0 (unspecified)
`enable`	Enables the H2QP WAN metrics profile.	—	—
`load-duration <duration>`	Configures a duration at which the downlink load is measured, in tenths of a second.	0 and 65535	—
`symm-link`	Indicates that the WAN Link has same speed in both the uplink and downlink directions.	—	—
`no`	Removes any existing configuration.	—	—
`uplink-load <speed>`	The percentage of the WAN uplink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	1-100	0 (unspecified)

Parameter	Description	Range	Default
`uplink-speed <speed>`	Use the **uplink <speed>** parameter to indicate the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified.	0 - 2,147,483,647 kbps	0 (unspecified)
`wan-metrics-link-status`	Define the status of the WAN Link by configuring one of the following values.	—	—
`<status>`	Configures any of the following states: ■ **link-up**—Indicates if WAN link is up. ■ **link-down**—Indicates if WAN link is down ■ **link-under-test**—Indicates if WAN link is currently in a test state.	link-down, link-under-test, link-up	unspecified

Examples

The following example configures a WAN metric profile:

```
(Instant AP)(config)# hotspot h2qp-wan-metrics-profile Wan1
(Instant AP)(WAN-metrics "Wan1")# at-capacity
(Instant AP)(WAN-metrics "Wan1")# downlink-load 5
(Instant AP)(WAN-metrics "Wan1")# downlink-speed 147
(Instant AP)(WAN-metrics "Wan1")# load-duration 60
```

```
(Instant AP)(WAN-metrics "Wan1")# symm-link
(Instant AP)(WAN-metrics "Wan1")# uplink-load 10
(Instant AP)(WAN-metrics "Wan1")# uplink-speed 147
(Instant AP)(WAN-metrics "Wan1")# wan-metrics-link-status link_up
(Instant AP)(WAN-metrics "Wan1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the H2QP WAN metrics profile configuration sub-mode

hotspot hs-profile

```
hotspot hs-profile <profile-name>
   access-network-type <type>
   addtl-roam-cons-ois <addtl-roam-cons-ois>
   advertisement-profile
      {anqp-3gpp-profile
      |anqp-domain-name-profile
      |anqp-ip-addr--profile
      |anqp-nai-realm-profile
      |anqp-nwk-auth-profile
      |anqp-roam-cons-profile
      |anqp-venue-name-profile
      |h2qp-conn-cap-profile
      |h2qp-oper-class-profile
      |h2qp-osu-provider-profile
      |h2qp-oper-name-profile
      |h2qp-wan-metrics-profile
      } <profile-name>
   asra
   comeback-mode
   enable
   gas-comeback-delay <delay>
   group-frame-block
   hessid <id>
   internet
   no
   osen
   osu-nai <osu-nai>
   osu-ssid <ssid>
   p2p-cross-connect
   p2p-dev-mgmt
   pame-bi
   qos-map-excp
   qos-map-range
   query-response-length-limit <len>
   release-number
   roam-cons-len-1 0|3|5
   roam-cons-len-2 0|3|5
   roam-cons-len-3 0|3|5
   roam-cons-oi-1 <roam-cons-oi-1>
   roam-cons-oi-2 <roam-cons-oi-1>
   roam-cons-oi-3 <roam-cons-oi-1>
   venue-group <venue-group>
   venue-type <venue-type>
   no
```

Description

This command configures a hotspot profile for an 802.11u public access service provider.

Parameter	Description	Range	Default
`access-network-type <type>`	Configures any of the following access network (802.11u network type) type: ■ **private**—This network is accessible for authorized users only. For example, home networks or enterprise networks that require user authentication. The corresponding integer value for this network type is 0. ■ **private-with-guest**—This network is accessible to guest users based on guest authentication methods. For example, enterprise networks that allow guest users with captive portal authentication. The corresponding integer value for this network type is 1. ■ **chargeable-public**— This network provides access to the Internet based on payment. For example, a subscription-based Internet access in a coffee shop or a hotel offering chargeable in-room Internet access service. The corresponding integer value for this network type is 2. ■ **free-public**—This network is accessible to all without any charges applied. For example, a hotspot in airport or other public places that provide Internet access with no additional cost. The corresponding integer value for this network type is 3. ■ **personal-device**—This network is accessible for personal devices. For example, a laptop or camera configured with a printer for the purpose of printing. The corresponding integer value for this network type is 4. ■ **emergency-services**—This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5. ■ **test**—This network is used for test purposes only. The corresponding integer value for this network type is 14. ■ **wildcard**—This network indicates a wildcard network. The corresponding integer value for this network type is 15.	private, private-with-guest,chargeable-public, free-public, personal-device, emergency-services, test, wildcard	chargeable-public

Parameter	Description	Range	Default
`addtl-roam-cons-ois <addtl-roam-cons-ois>`	Configures the number of additional roaming consortium OIs advertised by the OAW-IAP. This feature supports up to three additional OIs, which are defined using the roam-cons-oi-1, roam-cons-oi-2 and roam-cons-oi-3 parameters.	—	—
`advertisement-profile {anqp-3gpp-profile |anqp-domain-name-profile |anqp-ip-addr--profile |anqp-nai-realm-profile |anqp-nwk-auth-profile |anqp-roam-cons-profile |anqp-venue-name-profile |h2qp-conn-cap-profile |h2qp-oper-class-profile |h2qp-osu-provider-profile |h2qp-oper-name-profile |h2qp-wan-metrics-profile }`	Associates an advertisement profile with the hotspot profile. You can associate any of the following advertisement profiles: ■ anqp-3gpp-profile ■ anqp-domain-name-profile ■ anqp-ip-addr--profile ■ anqp-nai-realm-profile ■ anqp-nwk-auth-profile ■ anqp-roam-cons-profile ■ anqp-venue-name-profile ■ h2qp-conn-cap-profile ■ h2qp-oper-class-profile ■ h2qp-osu-provider-profile ■ h2qp-oper-name-profile ■ h2qp-wan-metrics-profile	—	—
`<profile-name>`	Allows you to associate a specific advertisement profile to the hotspot profile.	—	—
asra	Indicates if any additional steps are required for network access.	—	—
`comeback-mode`	By default, ANQP information is obtained from a GAS Request and Response. If you enable the comeback-mode option, advertisement information is obtained using a GAS Request and Response. as well as a Comeback-Request and Comeback-Response. This option is disabled by default.	—	—
`enable`	Enables the hotspot profile.	—	—

Parameter	Description	Range	Default
`gas-comeback-delay <delay>`	Configures a GAS comeback delay interval after which the client can attempt to retrieve the query response using a Comeback Request Action frame.	100—2000 milliseconds	100
`group-frame-block`	Configures the DGAF Disabled Mode. This feature ensures that the OAW-IAP does not forward downstream group-addressed frames. It is disabled by default, allowing the OAW-IAP to forward downstream group-addressed frames.	—	—
`hessid`	Configures a homogenous ESS identifier.	MAC address in colon-separated hexadecimal format	–
`internet`	Allows the OAW-IAP to send an Information Element indicating that the network allows the Internet access. By default, a hotspot profile does not advertise network internet access.	—	—
`no`	Removes any existing configuration.	—	—
`osen`	Uses the OSEN information element to advertise and select an OSEN capable network. **NOTE:** When OSU ESS is encypted, create a separate hotspot profile with only **osen** enabled and attach it to an SSID that broadcasts OSEN capable network. Then, choose the operation mode to WPA2-AES.	—	Disabled
`osu-nai`	Indicates the Network Access Identifier(NAI) that is used for OSU with the service provider configured in the OSU provider profile. When the OSU NAI is configured, the OSU ESS employs a link-layer encryption. For open OSU ESS, this parameter is not applicable.	—	—
`osu-ssid`	Configures the SSID that the wireless devices use for OSU with all the OSU providers.	—	—
`p2p-cross-connect`	Advertises support for P2P Cross Connections.	—	Disabled
`p2p-dev-mgmt`	Advertises support for P2P device management.	—	Disabled

Parameter	Description	Range	Default
`pame-bi`	Enables the PAME-BI bit, which is used by an OAW-IAP to indicate whether the OAW-IAP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.	—	—
`qos-map-excp`	Includes the DSCP exceptions in the QoS map set. You can configure a maximum of 21 sets of DSCP exception fields. It must be entered in Hexadecimal format. It is in the format, <value>-<up> separated by ',' where <value> can be 0-3F or FF, and user priority <up> can be 0-7)	—	—
`qos-map-range`	Configures the DSCP range value between 0 and 63 inclusive, or 255. It must be entered in Hexadecimal format. You must configure 8 sets each corresponding to a user priority. The format is <low>-<high> separated by a ',' where low and high are 0-3F and FF. For Example: 08-0F,00-07,FF-FF,10-1F,20-27,FF-FF,28-2F,30-3F	—	—
`query-response-length-limit <len>`	Configures the maximum length of the GAS query response. GAS enables advertisement services that allow the clients to query multiple 802.11 networks at once, while also allowing the client to learn more about a network's 802.11 infrastructure before associating. If a client transmits a GAS Query using a GAS Initial Request frame, the responding OAW-IAP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame.	1-6	1
`release-number`	Indicates the release number of Hotspot.	1-2	1
`roam-cons-len-1`	Configures the length of the OI. The value of the **roam-cons-len-1**parameter is based upon the number of octets of the **roam-cons-oi-1** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—
`roam-cons-len-2`	Length of the OI. The value of the **roam-cons-len-2**parameter is based upon the number of octets of the **roam-cons-oi-2** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—

Parameter	Description	Range	Default
`roam-cons-len-3`	Length of the OI. The value of the **roam-cons-len-3**parameter is based upon the number of octets of the **roam-cons-oi-3** field.	**0**: Zero Octets in the OI (Null), **3**: OI length is 24-bit (3 Octets), **5**: OI length is 36-bit (5 Octets)	—

`roam-cons-oi-1`
`roam-cons-oi-2`
`roam-cons-oi-3`
	Configures the roaming consortium OI to assign to one of the service provider’s top three roaming partners. This additional OI will only be sent to a client if the **addtl-roam-cons-<oisaddtl-roam-cons-ois>** parameter is set to 1 or higher.
	NOTE: The service provider’s own roaming consortium OI is configured using the **hotspot anqp-roam-cons-profile** command.
		—	—

`venue-group <venue-group>`	Configures one of the following venue groups to be advertised in the IEs from OAW-IAPs associated with this hotspot profile. ■ assembly ■ business ■ educational ■ factory-and-industrial ■ institutional ■ mercantile ■ outdoor ■ residential ■ storage ■ unspecified ■ utility-and-misc ■ vehicular **NOTE:** This parameter only defines the venue group advertised in the IEs from hotspot OAW-IAPs. To define the venue group to be included in ANQP responses, use **anqp-venue-name-profile <profile-name>** command.	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	business
`venue-type <venue-type>`	Specifies the venue type to be advertised in the IEs from OAW-IAPs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 219 This parameter only defines the venue type advertised in the IEs from hotspot OAW-IAPs. To define the venue type to be included in ANQP responses, use the **hotspot anqp-venue-name-profile <profile-name>** command.	—	—

Hotspot 2.0 is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request and association response), connect to networks, and roam between networks without additional authentication.

The Hotspot 2.0 provides the following services:

- Network discovery and selection— Allows the clients to discover suitable and available networks by advertising the access network type, roaming consortium, and venue information through the management frames. For network discovery and selection, GAS and ANQP are used.
- QOS Mapping— Provides a mapping between the network-layer QoS packet marking and over- the-air QoS frame marking based on user priority.

When a hotspot is configured in a network:

- The clients search for available hotspots using the beacon management frame.
- When a hotspot is found, the client sends queries to obtain information about the type of network authentication and IP address, and IP address availability using the GAS action frames.
- Based on the response of the advertisement Server (response to the GAS Action Frames), the relevant hotspot is selected and the client attempts to associate with it.
- Based on the authentication mode used for mobility clients, the client authenticates to access the network.

GAS Queries

An OI is a unique identifier assigned to a service provider when it registers with the IEEE registration authority. An OAW-IAP can include its service provider OI in beacons and probe responses to clients. If a client recognizes the OI, it will attempt to associate to the OAW-IAP using the security credentials corresponding to that service provider.

If the client does *not* recognize the OI, that client can send a GAS query to the OAW-IAP to request more information more about the network before associating.

ANQP Information Elements

ANQP Information Elements are additional data that can be sent from the OAW-IAP to the client to identify the network and service provider of the OAW-IAP. If a client requests this information through a GAS query, the hotspot OAW-IAP then sends the ANQP Capability list in the GAS Initial Response frame indicating support for the following IEs:

- **Venue Name** - Defined using the **hotspot anqp-venue-name-profile** command.
- **Domain Name**: Defined using the **hotspot anqp-domain-name-profile** command.
- **Network Authentication Type**: Define using the **hotspot anqp-nwk-auth-profile** command.
- **Roaming Consortium List**: Defined using the **hotspot anqp-roam-cons-profile** command.
- **NAI Realm**: Defined using the **hotspot anqp-nai-realm-profile** command.
- **Cellular Network Data**: Defined using the **hotspot anqp-3gpp-nwk-profile** command.
- **Connection Capability**: Defined using the **hotspot h2qp-conn-capability-profile** command.
- **Operator Class**: Defined using the **hotspot h2qp-op-cl-profile** command.
- **Operator Friendly Name**: Defined using the **hotspot h2qp-operator-friendly-name-profile** command.
- **WAN Metrics**: Defined using the **hotspot h2qp-wan-metrics-profile** command.

Roaming Consortium OIs

OIs are assigned to service providers when they register with the IEEE registration authority. You can specify the OI for the hotspot's service provider in the ANQP Roaming Consortium profile using the **hotspot anqp-**

roam-cons-profile command. This Hotspot profile also allows you to define and send up to three additional roaming consortium OIs for the service provider's top three roaming partners. To send this additional data to clients, you must specify the number of roaming consortium elements a client can query using the **addtl-roam-cons-ois <1-3>** parameter, then define those elements using the following parameters:

- **roam-cons-oi-1** and **roam-cons-len 1**
- **roam-cons-oi-2** and **roam-cons-len 2**
- **roam-cons-oi-3** and **roam-cons-len 3**

The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Venue Types

The following list describes the different venue types for each venue group:

Table 11: *Venue Types*

Venue Group	Associated Venue Type Value
unspecified The associated numeric value is **0**.	—
assembly The associated numeric value is **1**.	unspecified—The associated numeric value is **0**. arena—The associated numeric value is **1**. stadium—The associated numeric value is **2**. passenger-terminal—The associated numeric value is **3**. amphitheater—The associated numeric value is **4**. amusement-park—The associated numeric value is **5**. place-of-worship—The associated numeric value is **6**. convention-center—The associated numeric value is **7**. library—The associated numeric value is **8**. museum—The associated numeric value is **9**. restaurant—The associated numeric value is **10**. theater—The associated numeric value is **11**. bar—The associated numeric value is **12**. coffee-shop—The associated numeric value is **13**. zoo-or-aquarium—The associated numeric value is **14**. emergency-cord-center—The associated numeric value is **15**.
business The associated numeric value is **2**.	unspecified—The associated numeric value is **0**. doctor—The associated numeric value is **1** bank—The associated numeric value is **2** fire-station—The associated numeric value is **3** police-station—The associated numeric value is **4** post-office—The associated numeric value is **6** professional-office—The associated numeric value is **7** research-and-dev-facility—The associated numeric value is **8** attorney-office—The associated numeric value is **9**
educational The associated numeric value is **3**.	unspecified—The associated numeric value is **0**. school-primary—The associated numeric value is **1**. school-secondary—The associated numeric value is **2**. univ-or-college—The associated numeric value is **3**.
factory-and-industrial The associated numeric value is **4**.	unspecified—The associated numeric value is **0**. factory—The associated numeric value is **1**.
institutional	unspecified—The associated numeric value is **0**. hospital—The associated numeric value is **1**.

Venue Group	Associated Venue Type Value
The associated numeric value is **5**.	long-term-care—The associated numeric value is **2**. alc-drug-rehab—The associated numeric value is **3**. group-home—The associated numeric value is **4**. prison-or-jail—The associated numeric value is **5**.
mercantile The associated numeric value is **6**.	unspecified—The associated numeric value is **0**. retail-store—The associated numeric value is **1**. grocery-market—The associated numeric value is **2**. auto-service-station—The associated numeric value is **3**. shopping-mall—The associated numeric value is **4**. gas-station—The associated numeric value is **5**
residential The associated numeric value is **7**.	unspecified—The associated numeric value is **0**. private-residence—The associated numeric value is **1**. hotel—The associated numeric value is **3** dormitory—The associated numeric value is **4** boarding-house—The associated numeric value is **5**.
storage The associated numeric value is **8**.	unspecified—The associated numeric value is **0**.
utility-misc The associated numeric value is **9**.	unspecified—The associated numeric value is **0**.
vehicular The associated numeric value is **10**	unspecified—The associated numeric value is **0**. automobile-or-truck—The associated numeric value is **1**. airplane—The associated numeric value is **2**. bus—The associated numeric value is **3**. ferry—The associated numeric value is **4**. ship—The associated numeric value is **5**. train—The associated numeric value is **6**. motor-bike—The associated numeric value is **7**.
outdoor The associated numeric value is **11**.	unspecified—The associated numeric value is **0** muni-mesh-network—The associated numeric value is **1**. city-park—The associated numeric value is **2**. rest-area—The associated numeric value is **3**. traffic-control—The associated numeric value is **4** bus-stop—The associated numeric value is **5** kiosk—The associated numeric value is **6**

Example

The following commands configure a hotspot profile:

```
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0 "hs1")# enable
(Instant AP)(Hotspot2.0 "hs1")# comeback-mode
(Instant AP)(Hotspot2.0 "hs1")# gas-comeback-delay 10
(Instant AP)(Hotspot2.0 "hs1")# no asra
(Instant AP)(Hotspot2.0 "hs1")# no internet
(Instant AP)(Hotspot2.0 "hs1")# query-response-length-limit 5
(Instant AP)(Hotspot2.0 "hs1")# access-network-type chargeable-public
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-1 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-1 123456
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-len-2 3
(Instant AP)(Hotspot2.0 "hs1")# roam-cons-oi-2 223355
(Instant AP)(Hotspot2.0 "hs1")# addtl-roam-cons-ois 0
(Instant AP)(Hotspot2.0 "hs1")# venue-group business
(Instant AP)(Hotspot2.0 "hs1")# venue-type research-and-dev-facility
```

```
(Instant AP)(Hotspot2.0 "hs1")# pame-bi
(Instant AP)(Hotspot2.0 "hs1")# group-frame-block
(Instant AP)(Hotspot2.0 "hs1")# p2p-dev-mgmt
(Instant AP)(Hotspot2.0 "hs1")# p2p-cross-connect
(Instant AP)(Hotspot2.0 "hs1")# end
(Instant AP)# commit apply
```

The following commands associate **anqp-3gpp** advertisement profile with a hotspot profile:

```
(Instant AP)(config)# hotspot hs-profile hs1
(Instant AP)(Hotspot2.0"hs1")# advertisement-protocol anpp
(Instant AP)(Hotspot2.0"hs1")# advertisement-profile anqp-3gpp 3gpp1
(Instant AP)(Hotspot2.0"hs1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.4.0.0	■ The following parameters were introduced ● **h2qp-osu-provider-profile** ● **osen** ● **osu-nai** ● **osu-ssid** ● **qos-map-excp** ● **qos-map-range** ■ The range of the **query-response-length-limit** parameter was changed to 1–6 from 1–127.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except 5xx series platforms	Configuration mode and the hotspot profile configuration sub-mode

hs2-osu-icon-delete

```
hs2-osu-icon-delete <idx>
```

Description

This command deletes the specified OSU icon file downloaded in the OAW-IAP.

Parameter	Description	Range	Default
`<idx>`	Deletes the file referenced by the specified index ID.	—	—

Example

The following command deletes a downloaded icon file:

```
(Instant AP)# hs2-osu-icon-delete 5
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

hs2-osu-icon-download

```
hs2-osu-icon-download <idx> <ftp/tftp/http URL syntax>
```

Description

This command downloads the OSU provider's icon file to the OAW-IAP.

The icon file is downloaded from the specified location and stored in flash with the specified index as reference.

Parameter	Description	Range	Default
`<idx>`	Indicates the index of the file which can take values from 1 to 10	1-10	—
`<url>`	The location from which the icon file can be downloaded. The location can be FTP, TFTP, or HTTP.	—	—

Example

To download the icon file to the OAW-IAP, execute the following command:

```
(Instant AP)# hs2-osu-icon-download <idx> <ftp/tftp/http URL syntax>
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

iap-master

```
iap-master
no…
```

Description

This command provisions an OAW-IAP as a master OAW-IAP.

Syntax

Parameter	Description	Range	Default
`iap-master`	Provisions the OAW-IAP as a master OAW-IAP.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to manually provision an OAW-IAP as a master OAW-IAP.

Example

The following example provisions a master OAW-IAP:

```
(Instant AP)# iap-master
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ids

```
ids
   ap-max-unseen-timeout <seconds>
   client-detection-level <type>
   client-protection-level <type>
   detect-adhoc-network
   detect-adhoc-using-valid-ssid
   detect-ap-flood
   detect-ap-impersonation
   detect-ap-spoofing
   detect-bad-wep
   detect-beacon-wrong-channel
   detect-block-ack-attack
   detect-chan-based-mitm
   detect-chopchop-attack
   detect-client-flood
   detect-cts-rate-anomaly
   detect-disconnect-sta
   detect-eap-rate-anomaly
   detect-fatajack
   detect-hotspotter-attack
   detect-ht-40mhz-intolerance
   detect-ht-greenfield
   detect-invalid-addresscombination
   detect-invalid-mac-oui
   detect-malformed-assoc-req
   detect-malformed-frame-auth
   detect-malformed-htie
   detect-malformed-large-duration
   detect-omerta-attack
   detect-overflow-eapol-key
   detect-overflow-ie
   detect-power-save-dos-attack
   detect-rate-anomalies
   detect-rts-rate-anomaly
   detect-tkip-replay-attack
   detect-unencrypted-valid
   detect-valid-clientmisassociation
   detect-valid-ssid-misuse
   detect-windows-bridge
   detect-wireless-bridge
   detect-wpa-ft-attack
   infrastructure-detection-level <type>
   infrastructure-protection-level <type>
   no
   protect-adhoc-network
   protect-ap-impersonation
   protect-ssid
   protect-valid-sta
   protect-windows-bridge
   rogue-containment
   signature-airjack
   signature-asleap
   signature-deassociation-broadcast
   signature-deauth-broadcast
   valid-ap-max-unseen-timeout <seconds>
   wired-containment
   wired-containment-ap-adj-mac
   wired-containment-susp-l3-rogue
   wireless-containment <type>
```

```
no ids
```

Description

This command configures an IDS policy for an OAW-IAP. Use this command to configure IDS detection and protection policies. The IDS feature monitors the network for the presence of unauthorized OAW-IAPs and clients and enables you to detect rogue OAW-IAPs, interfering OAW-IAPs, and other devices that can potentially disrupt network operations. It also logs information about the unauthorized OAW-IAPs and clients, and generates reports based on the logged information.

WIP offers a wide selection of intrusion detection and protection features to protect the network against wireless threats. Like most other security-related features of the Alcatel-Lucent network, the WIP can be configured on the OAW-IAP.

You can configure the following policies:

- Infrastructure Detection Policies— Specifies the policy for detecting wireless attacks on access points
- Client Detection Policies— Specifies the policy for detecting wireless attacks on clients
- Infrastructure Protection Policies— Specifies the policy for protecting access points from wireless attacks.
- Client Protection Policies— Specifies the policy for protecting clients from wireless attacks.
- Containment Methods— Prevents unauthorized stations from connecting to your AOS-W Instant network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly. The following levels of detection can be configured:

- Off
- Low
- Medium
- High

Parameter	Description	Range	Default
`ids`	Creates an IDS policy	—	—
`ap-max-unseen-timeout <seconds>`	Configures the ageout time for interfering AP entries in the **Unknown Access Points Detected** table of the AOS-W Instant network. The entry of the interfering AP will be deleted if it is not seen by the OAW-IAP after the configured duration is elapsed. For interfering APs operating in a different channel, the ageout time is twice the duration configured. The value is configured in seconds.	5-360000	600
`client-detection-level <type>`	Sets the client detection level.	off, low, medium, high	off

Parameter	Description	Range	Default
`client-protection-level <type>`	Sets the client protection level.	off, low, medium, high	off
`detect-adhoc-network`	Enables detection of ad hoc networks.	—	—
`detect-adhoc-using-valid-ssid`	Enables or disables detection of ad hoc networks using valid or protected SSIDs.	—	—
`detect-ap-flood`	Enables detection of flooding with fake OAW-IAP beacons to confuse the legitimate users and to increase the amount of processing needed on client operating systems.	—	—
`detect-ap-impersonation`	Enables detection of OAW-IAP impersonation. In OAW-IAP impersonation attacks, the attacker sets up an OAW-IAP that assumes the BSSID and ESSID of a valid OAW-IAP or a neighboring OAW-IAP. OAW-IAP impersonation attacks can be done for man-in-the-middle attacks, a rogue OAW-IAPs attempting to bypass detection, or a honeypot attack.	—	—
`detect-ap-spoofing`	Enables OAW-IAP Spoofing detection.	—	—
`detect-bad-wep`	Enables detection of WEP initialization vectors that are known to be weak or repeating. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and search for implementations that are still used by many legacy devices.	—	—
`detect-beacon-wrong-channel`	Enables detection of beacons advertising the incorrect channel.	—	—
`detect-block-ack-attack`	Enables detection of attempts to reset traffic receive windows using the forged Block ACK Add messages.	—	—
`detect-chan-based-mitm`	Enables or disables channel-based man-in-the-middle attack detection.	—	—
`detect-chopchop-attack`	Enables detection of ChopChop attack.	—	—
`detect-client-flood`	Enables detection of client flood attack.	—	—

Parameter	Description	Range	Default
`detect-cts-rate-anomaly`	Enables detection of CTS rate anomaly.	—	—
`detect-disconnect-sta`	Enables a station disconnection attack. In a station disconnection, attacker spoofs the MAC address of either an active client or an active OAW-IAP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association.	—	—
`detect-eap-rate-anomaly`	Enables EAP handshake analysis to detect an abnormal number of authentication procedures on a channel and generate an alarm when this condition is detected.	—	—
`detect-fatajack`	Enables detection of fatjack attacks.	—	—
`detect-hotspotter-attack`	Enables detection of hotspot attacks.	—	—
`detect-ht-40mhz-intolerance`	Enables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and OAW-IAPs advertising 40 MHz intolerance will be reported.	—	—
`detect-ht-greenfield`	Enables detection of HT devices advertising greenfield preamble capability.	—	—
`detect-invalid-addresscombination`	Enables detection of invalid address combinations.	—	—
`detect-invalid-mac-oui`	Enables checking of the first three bytes of a MAC address, known as the OUI, assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI checking causes an alarm to be triggered if an unrecognized MAC address is in use.	—	—
`detect-malformed-assoc-req`	Enables detection of malformed association requests.	—	—
`detect-malformed-frame-auth`	Enables detection of malformed authentication frames	—	—
`detect-malformed-htie`	Enables detection of malformed HT information elements.	—	—

Parameter	Description	Range	Default
`detect-malformed-large-duration`	Enables detection of unusually large durations in frames.	—	—
`detect-omerta-attack`	Enables detection of Omerta attack.	—	—
`detect-overflow-eapol-key`	Enables detection of overflow EAPOL key requests.	—	—
`detect-overflow-ie`	Enables detection of overflow Information Elements.	—	—
`detect-power-save-dos-attack`	Enables detection of Power Save DoS attack.	—	—
`detect-rate-anomalies`	Enables detection of rate anomalies.	—	—
`detect-rts-rate-anomaly`	Enables detection of RTS rate anomaly.	—	—
`detect-tkip-replay-attack`	Enables detection of TKIP replay attack.	—	—
`detect-unencrypted-valid`	Enables detection of unencrypted valid clients.	—	—
`detect-valid-clientmisassociation`	Enables detection of misassociation between a valid client and an unsafe OAW-IAP. This setting can detect the following misassociation types: ■ MisassociationToRogueAP ■ MisassociationToExternalAPI ■ MisassociationToHoneypotAP ■ MisassociationToAdhocAP ■ MisassociationToHostedAP	—	—
`detect-valid-ssid-misuse`	Enables detection of interfering or Neighbor APs using valid or protected SSIDs.	—	—
`detect-windows-bridge`	Enables detection of Windows station bridging.	—	—
`detect-wireless-bridge`	Enables detection of wireless bridging.	—	—
`detect-wpa-ft-attack`	Enables or disables detection of WPA FT attacks.	—	—
`infrastructure-detection-level <type>`	Sets the infrastructure detection level.	off, low, medium, high	off
`infrastructure-protection-level <type>`	Sets the infrastructure protection level.	off, low, medium, high	off

Parameter	Description	Range	Default
`protect-adhoc-network`	Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a DoS attack	—	—
`protect-ap-impersonation`	Enables protection from OAW-IAP impersonation attacks. When OAW-IAP impersonation is detected, both the legitimate and impersonating OAW-IAP are disabled using a DoS attack.	—	—
`protect-ssid`	Enables use of SSID by valid OAW-IAPs only.	—	—
`protect-valid-sta`	Enables protection of valid stations. When enabled valid stations are not allowed to connect to an invalid OAW-IAP.	—	—
`protect-windows-bridge`	Enables protection of a windows station bridging	—	—
`rogue-containment`	Controls Rogue OAW-IAPs. When rogue OAW-IAPs are detected, they are not automatically disabled. This option automatically shuts down rogue OAW-IAPs. When this option is enabled, clients attempting to associate to an OAW-IAP classified as a rogue are disconnected through a DoS attack.	—	—
`signature-airjack`	Enables signature matching for the AirJack frame type.	—	—
`signature-asleap`	Enables signature matching for the ASLEAP frame type.	—	—
`signature-deassociation-broadcast`	Configures signature matching for the deassociation broadcast frame type.	—	—
`signature-deauth-broadcast`	Configures signature matching for the deauth broadcast frame type.	—	—
`valid-ap-max-unseen-timeout <seconds>`	Configures the ageout time for valid AP entries in the **Unknown Access Points Detected** table of the AOS-W Instant network. The entry of the valid AP will be deleted if it is not seen by the OAW-IAP after the configured duration is elapsed.	5-360000	7200

Parameter	Description	Range	Default
	For valid APs operating in a different channel, the ageout time is twice the duration configured. The value is configured in seconds.		
`wired-containment`	Controls Wired attacks.	—	—
`wired-containment-ap-adj-mac`	Enables a wired containment to Rogue OAW-IAPs whose wired interface MAC address is offset by one from its BSSID.	—	—
`wired-containment-susp-l3-rogue`	Enables the user to identify and contain an OAW-IAP with a preset wired MAC address that is different from the BSSID of the OAW-IAP if the MAC address that the OAW-IAP provides to wireless clients as the Gateway MAC is offset by one character from its wired MAC address. **NOTE:** Enable this feature only when the specific containment is needed, to avoid a false alarm.	—	—
`wireless-containment <type>`	Enable wireless containment including Tarpit Shielding. Tarpit shielding works by steering a client to a tarpit so that the client associates with it instead of the OAW-IAP that is being contained. ■ deauth-only— Enables Containment using deauthentication only . ■ none— Disables wireless containment. ■ tarpit-all-sta—Enables wireless containment by tarpit of all stations. ■ tarpit-non-valid-sta— Enables wireless containment by tarpit of non-valid clients	deauth-only, none, tarpit-all-sta, tarpit-non-valid-sta	deauth-only
`no…`	Removes configuration settings for parameters under the **ids** command.	—	—
`no ids`	Removes IDS configuration.	—	—

Example

The following example configures detection and protection policies:

```
(Instant AP)(config)# ids
(Instant AP)(IDS)# infrastructure-detection-level low
(Instant AP)(IDS)# client-detection-level low
(Instant AP)(IDS)# infrastructure-protection-level low
(Instant AP)(IDS)# client-protection-level low
(Instant AP)(IDS)# wireless-containment deauth-only
```

```
(Instant AP)(IDS)# wired-containment
(Instant AP)(IDS)# detect-ap-spoofing
(Instant AP)(IDS)# detect-windows-bridge
(Instant AP)(IDS)# signature-deauth-broadcast
(Instant AP)(IDS)# signature-deassociation-broadcast
(Instant AP)(IDS)# detect-adhoc-using-valid-ssid
(Instant AP)(IDS)# detect-malformed-large-duration
(Instant AP)(IDS)# detect-ap-impersonation
(Instant AP)(IDS)# detect-adhoc-network
(Instant AP)(IDS)# detect-valid-ssid-misuse
(Instant AP)(IDS)# detect-wireless-bridge
(Instant AP)(IDS)# detect-ht-40mhz-intolerance
(Instant AP)(IDS)# detect-ht-greenfield
(Instant AP)(IDS)# detect-ap-flood
(Instant AP)(IDS)# detect-client-flood
(Instant AP)(IDS)# detect-bad-wep
(Instant AP)(IDS)# detect-cts-rate-anomaly
(Instant AP)(IDS)# detect-rts-rate-anomaly
(Instant AP)(IDS)# detect-invalid-addresscombination
(Instant AP)(IDS)# detect-malformed-htie
(Instant AP)(IDS)# detect-malformed-assoc-req
(Instant AP)(IDS)# detect-malformed-frame-auth
(Instant AP)(IDS)# detect-overflow-ie
(Instant AP)(IDS)# detect-overflow-eapol-key
(Instant AP)(IDS)# detect-beacon-wrong-channel
(Instant AP)(IDS)# detect-invalid-mac-oui
(Instant AP)(IDS)# detect-valid-clientmisassociation
(Instant AP)(IDS)# detect-disconnect-sta
(Instant AP)(IDS)# detect-omerta-attack
(Instant AP)(IDS)# detect-fatajack
(Instant AP)(IDS)# detect-block-ack-attack
(Instant AP)(IDS)# detect-hotspotter-attack
(Instant AP)(IDS)# detect-unencrypted-valid
(Instant AP)(IDS)# detect-power-save-dos-attack
(Instant AP)(IDS)# detect-eap-rate-anomaly
(Instant AP)(IDS)# detect-rate-anomalies
(Instant AP)(IDS)# detect-chopchop-attack
(Instant AP)(IDS)# detect-tkip-replay-attack
(Instant AP)(IDS)# signature-airjack
(Instant AP)(IDS)# signature-asleap
(Instant AP)(IDS)# protect-ssid
(Instant AP)(IDS)# rogue-containment
(Instant AP)(IDS)# protect-adhoc-network
(Instant AP)(IDS)# protect-ap-impersonation
(Instant AP)(IDS)# protect-valid-sta
(Instant AP)(IDS)# protect-windows-bridge
(Instant AP)(IDS)# ap-max-unseen-timeout 3600
(Instant AP)(IDS)# valid-ap-max-unseen 5000
(Instant AP)(IDS)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	**ap-max-unseen-timeout** and **valid-ap-max-unseen-timeout** parameters were added.
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and IDS configuration sub-mode.

ignore-image-check

```
ignore-image-check
```

Description

This command ignores the automatic image check feature. The automatic image check feature automatically checks for a new version of AOS-W Instant on the image server, once after the OAW-IAP boots up and every week thereafter.

Usage Guidelines

Use this command to disable the automatic image check feature:

Example

The following example disables the image check feature:

```
(Instant AP)# ignore-image-check
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

inactivity-ap-timeout

```
inactivity-ap-timeout <seconds>
no…
```

Description

This command configures the timeout interval for inactive user sessions.

Syntax

Parameter	Description	Range	Default
`inactivity-ap-timeout <seconds>`	Configures the inactivity timeout interval in seconds.	1-1000	1000
`no…`	Removes any existing configuration.	—	—

Usage Guidelines

Use this command to configure an inactivity timeout interval for an OAW-IAP.

Example

The following example configures the inactivity timeout interval:

```
(Instant AP)(config)# inactivity-ap-timeout 180
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

inbound-firewall

```
inbound-firewall
  rule <subnet> <smask> <dest> <mask> <match/invert> <protocol> <sport> <eport>
  {permit|deny|src-nat|dst-nat ip <IP-address> <port>}[{log | blacklist | disable-scanning |
  tos <0-63> | dot1p-priority <0-7>}]
  no…
```

Description

This command configures inbound firewall rules based on the source subnet.

Syntax

Parameter	Description	Range	Default
`inbound-firewall`	Opens the inbound firewall configuration mode.	—	—
`rule`	Creates an access rule. You can create up to 128 access rules. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
`<subnet>`	Allows you to specify the source subnet IP address	—	—
`<smask>`	Specifies the subnet mask of the source IP address.	—	—
`<dest>`	Allows you to specify the destination IP address.	—	—
`<mask>`	Specifies the subnet mask for the destination IP address.	—	—
`<match/invert>`	■ **match**—Indicates if the rule specific to the destination IP address and subnet mask matches the value specified for protocol. ■ **invert**— Indicates if the rule allows or denies traffic with an exception to the specified destination IP address and subnet mask.	match invert	—
`<protocol>`	Configures any of the following: ■ Protocol number between 0-255 ■ any: any protocol ■ tcp: Transmission Control Protocol ■ udp: User Datagram Protocol	1-255	—
`<sport>`	Specifies the starting port number from which the rule applies.	1-65534	—
`<eport>`	Specifies the ending port number until which the rule applies	1-65534	—

Parameter	Description	Range	Default
`dst-nat`	Allows the OAW-IAP to perform destination NAT on packets.	—	—
`src-nat`	Allows the OAW-IAP to perform source NAT on packets. When configured, the source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool).	—	—
`ip <IP-addr>`	Specifies the destination NAT IP address for the specified packets when dst-nat action is configured.	—	—
`<port>`	Specifies the destination NAT port for the specified packets when dst-nat action is configured.	—	—
`deny`	Creates a rule to reject the specified packets	—	—
`<option1-option9>`	Allows you to specify any of the following options:	—	—
`log`	Creates a log entry when this rule is triggered.	—	—
`blacklist`	Blacklists the client when this rule is triggered.	—	—
`disable-scanning`	Disables ARM scanning when this rule is triggered.	—	—
`tos <tos value>`	Specifies a DSCP value to prioritize traffic when this rule is triggered.	0-63	—
`dot1p-priority <priority>`	Sets an 802.1p priority.	0-7	—
no...	Removes the configuration	—	—

Usage Guidelines

Use this command to configure inbound firewall rules for the inbound traffic coming through the uplink ports of an OAW-IAP. The rules defined for the inbound traffic are applied if the destination is not a user connected to the OAW-IAP. If the destination already has a user role assigned, the user role overrides the actions or options specified in inbound firewall configuration. However, if a deny rule is defined for the inbound traffic, it is applied irrespective of the destination and user role. Unlike the ACL rules in a WLAN SSID or wired profile, the inbound firewall rules can be configured based on the source subnet.

For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default.

Management access to the OAW-IAP is allowed irrespective of the inbound firewall rule. For more information on configuring restricted management access, see restricted-mgmt-access.

The inbound firewall is not applied to traffic coming through GRE tunnel.

Example

The following example configures inbound firewall rules:

```
(Instant AP)(config)# inbound-firewall
(Instant AP)(inbound-firewall)# rule 192.0.2.1 255.255.255.255 any any match 6 631 631 permit
(Instant AP)(inbound-firewall)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and inbound firewall configuration sub-mode.

interface vlan

```
interface vlan <vlan_id>
   ip <IP address or domain name>
   no
```

Description

This command allows you to configure an interface VLAN.

Syntax

Parameter	Description	Default
`interface vlan <vlan-id>`	Configures an Interface VLAN.	—
`ip <ip-address>`	Denotes the IP address or domain name of the server.	—
`no`	Deletes the configuration.	—

Usage Guidelines

Use this command to configure an interface VLAN between the AP and a custom server.

Example

The example below shows how to configure an interface VLAN:

```
(Instant AP)(config)# interface vlan <vlan_id>
(Instant AP)("interface vlan <vlan-id>")# ip <ip address>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode and Interface VLAN sub-mode on the Instant Access Point.

internal-domains

```
internal-domains
  domain-name <domain-name>
  no…
```

Description

This command configures valid domain names for the enterprise network.

Syntax

Parameter	Description	Range	Default
`internal-domains`	Enables the internal-domain configuration sub-mode	—	—
`domain-name <domain-name>`	Defines the valid domain names	—	—
`no…`	Removes any existing configuration	—	—

Usage Guidelines

Use this command to configure the DNS domain names that are valid on the enterprise network. This list is used for determining how the client DNS requests should be routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the configured DNS server.

Example

The following example configures the internal domains for a network:

```
(Instant AP)(config)# internal-domains
(Instant AP)(domain)# domain-name www.example.com
(Instant AP)(domain)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and domains configuration sub-mode

intra-vlan-traffic-profile

```
intra-vlan-traffic-profile
   no
   wired-server-ip <ip>
   wired-server-mac <mac>
```

Description

This command allows you to configure an intra VLAN traffic profile and add trusted wired servers to the network.

Syntax

Parameter	Description	Default
`no`	Deletes the configuration.	—
`wired-server-ip <ip>`	Configures a wired server using its IP address.	—
`wired-server-mac <mac>`	Configures a wired server using its MAC address.	–

Usage Guidelines

Use this command to configure wired servers to the intra VLAN traffic profile by either their IP or MAC addresses.

Example

The example below shows how to configure a wired server to the intra VLAN traffic profile:

```
(Instant AP)(config) #intra-vlan-traffic-profile
(Instant AP)(intra-vlan-traffic) #wired-server-ip <ip>
(Instant AP)(intra-vlan-traffic) #wired-server-mac <mac>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Instant Access Point.

iot radio-profile

```
iot radio-profile <profile-name>
  ble-console {dynamic|off|on}
  ble-opmode {beaconing|scanning}
  ble-txpower <ble-txpower>
  no
  radio-instance {external | internal}
  radio-mode {ble | zigbee}
  zigbee-channel {auto|11|12|13|14|15|16|17|18|19|20|21|22|23|24|25|26}
  zigbee-opmode coordinator
```

Description

This command configures or modifies an IoT radio profile.

Parameter	Description	Range	Default
`ble-console`	Set the BLE console mode. Configure one of the following: ■ **dynamic**: The built-in BLE chip of the OAW-IAP functions in the beaconing mode and dynamically enables access to OAW-IAP console over BLE when the link to the LMS is lost. The dynamic console mode performs special error checks when the OAW-IAP experiences connectivity issues and decides if the BLE Console needs to be enabled. ■ **off**—Disables the BLE console. ■ **on**—Enables the BLE console.	on, off, or dynamic.	off
`ble-opmode`	Set the BLE operation mode. Configure one of the following: ■ **beaconing**: The built-in BLE chip of the OAW-IAP functions as an iBeacon combined with the beacon management functionality. ■ **scanning**—Enables BLE scanning on the OAW-IAP. ■ **both**—Enables both BLE beaconing and scanning options.	beaconing, scanning, or both.	—
`ble-txpower`	Set the BLE transmission power in dBm.	—	—
`no...`	Removes any existing configuration.	—	—

Parameter	Description	Range	Default
radio-instance	Enables external or internal radio instance.	—	—
radio-mode	Enables BLE or ZigBee radio mode.	—	—
zigbee-channel	Set the ZigBee scanning channel.	—	—
zigbee-opmode	Set the ZigBee coordinator operation mode.	—	—

Example

The following example configures an IoT Radio profile.

```
(host) [mynode] (config) #iot radio-profile Sample-Zigbee
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #radio-mode zigbee
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #zigbee-channel auto
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #zigbee-opmode coordinator
```

Command History

Version	Modification
AOS-W Instant 8.6.0.0	The following parameters were removed: ■ radio-enable ■ zigbee-panid ■ zigbee-panid-type ■ zigbee-permit joining ■ zigbee-permit-joining-duration The following parameters were introduced: ■ ble-console ■ ble-opmode ■ ble-txpower
AOS-W Instant 8.4.0.0	Command introduced

Command Information

Platforms	Command Mode
All platforms	Configuration mode.

iot transportProfile

```
iot transportProfile <profile>
   ZSDFilter <Zigbee_Socket_Device_Filter>
   accessID <accessID>
   ageFilter <ageout>
   authenticationURL <url>
   cellSizeFilter <cellsize>
   customFadingFactor <type>
   data-filter <filter>
   deviceCountOnly
   endpointID <id>
   endpointToken <token>
   endpointType {Meridian-Asset-Tracking|Meridian-Beacon-Management|ZF|telemetry-
   https|telemetry-websocket|Assa-Abloy}
   endpointURL <url>
   environmentType <type>
   movementFilter <threshold>
   password <password>
   payloadContent {managed-beacons|managed-tags|zf-tags|all|enocean-sensors/enocean-
   switches|ibeacon|eddystone|assa-abloy|unclassified|aruba-sensors|mysphera|wifi-tags|wifi-
   assoc-sta|wifi-unassoc-sta|ability-smart-sensor|sbeacon|wiliot|zsd|serial-data|exposure-
   notification}
   proxyserver <host> <port> [<username>|<password>]
   rssiReporting <type>
   rtlsDestMAC <mac_address>
   uidNamespaceFilter <filter>
   transportInterval <interval>
   uuidFilter <filter>
   urlFilter <filter>
   username <user>
   vendorFilter
   vlan <vlan_id>
   no…
```

Description

This command configures an IoT transport profile on an AOS-W Instant network. An IoT transport profile is a global profile that is created for transporting BLE information from an OAW-IAP to an endpoint server. Use this command to create or modify an IoT transport profile.

Parameter	Description	Range	Default
`ZSDFilter <filter>`	A list of Zigbee socket devices to filter the packets fro m Zigbee.	—	—
`accessID`	An access ID can grant extended access	—	—
`ageFilter <ageout>`	Devices without recent activity will not be reported.	0 to 3600 seconds	0
`authenticationURL <url>`	Denotes the server URL used for authentication.	—	—

Parameter	Description	Range	Default
`cellSizeFilter <cellsize>`	This is a proximity filter. Devices outside the cell will not be reported. Size is specified in meters. Setting to 0 disables the cell size filter .	0 to 255 meters	0
`customFadingFactor <type>`	When environment type is custom, you can define a fading factor to get the most accurate distance according to your environment.	10 to 40	—
`data-filter <filter>`	A list of numbers to filter the data before reporting to a server. The numbers correspond to protobuf files. For more information, see DataFilter Values.	—	—
`deviceCountOnly`	Send only the aggregated device counts per configured device class	—	—
`endpointID <id>`	Endpoint ID of the IoT management server.	—	—
`endpointToken <token>`	Configures a text string of text string of 1-255 characters as the BLE endpoint authorization token. The authorization token is used by the BLE devices in the HTTPS header when communicating with the BMC.	1 to 255 characters	—
`endpointType`	This parameter registers the WebSocket endpoint of a management server for BLE data on the OAW-IAP. The WebSocket endpoint allows the management server to receive messages from the BLE relay process on the OAW-IAP. **NOTE:** Only one endpoint configuration is supported at a given time. A new endpoint configuration will overwrite the existing configuration. The following endpoint types are supported: ■ **Meridian-Asset-Tracking**—Stream data to meridian WebSocket server. **NOTE:** When the meridian asset tracking endpoint is configured and the firmware is upgraded to AOS-W Instant 8.7.0.0, the CA certificate should be uploaded in order to	—	Meridian-Beacon-Management

Parameter	Description	Range	Default
	connect to the meridian server. ■ **Meridian-Beacon-Management**—Sends a POST request on a REST meridian API. ■ **ZF**—ZF deTagtive server. ■ **telemetry-https**—Sends a POST request on a REST meridian API. However, the payload encoding adheres to the published Aruba Telemetry JSON schema. ■ **telemetry-websocket**—Stream data to meridian WebSocket server. However. the payload encoding adheres to the published Alcatel-Lucent Telemetry.proto format. ■ **Assa-Abloy**: Sends Assa Abloy data.		
`movementFilter <threshold>`	Filters devices that do not change distance. Specified in meters. Applicable only if a cell size is set. Setting to 0 disables the movement filter.	0 to 255 meters	0
`endpointURL <url>`	Configures the URL of the IoT management server to which the BLE monitoring data is sent.	—	—
`environmentType <type>`	Configures the working environment type.	—	—
`uuidFilter`	Denotes the universal unique identifiers (UUIDs) through comma separated strings.	—	—
`vendorFilter`	A list of list of vendor IDs and vendor names. You can specify a maximum of 5 vendor IDs or vendor names.	—	—
`password <password>`	Endpoint password.	—	—
`payloadContent <payload>`	Content of the messages sent to the IoT management server. The following payload options are supported: ■ **ability-smart-sensor**—ABB ability smart sensor data. ■ **managed-beacons**—Beacon management data. ■ **managed-tags**—Asset tag RSSI data. ■ **zf-tags**—ZF tag data ■ **all**—All the BLE device data	—	—

Parameter	Description	Range	Default
	■ **enocean-sensors**—EnOcean sensor device data ■ **enocean-switches**—EnOcean switch device data ■ **ibeacons**—iBeacon device data ■ **assa-abloy**—Assa Abloy dor lock data ■ **unclassified**—Raw data of the BLE chip ■ **exposure-notification**—Exposure notification based on the presence of service UUID 0xFD6F and service data 0xFD6F. ■ **eddystone**—Eddystone device data. ■ **aruba-sensors**—Alcatel-Lucent sensor data. ■ **mysphera**—MySphera data. ■ **sbeacon**—sbeacon data. ■ **wiliot**—Wiliot data. ■ **wifi-assoc-sta**—Data of Wi-Fi associated stations. ■ **wifi-tags**—WiFi RTLS tag data. ■ **wifi-unassoc-sta**—Data of WiFi unassociated stations. ■ **zsd**—Zigbee Socket Device. ■ **serial-data**—Serial data.		
`proxyserver <host> <port> [<username>|<password>]`	Denotes the proxy server to which the IoT data is sent. ■ **host**—IP address or domain name of the proxy server. ■ **port**—Port number through which the connection to the proxy server is established. ■ **username**—Username to log in to the proxy server. This parameter is optional. ■ **password**—Password to log in to the proxy server. This parameter is optional.	—	—
`transportInterval <interval>`	OAW-IAP IoT data interval in seconds.	5 to 3600 seconds	300 seconds
`rssiReporting <type>`	Sets the preferred format for RSSI reporting.	—	average
`rtlsDestMAC <mac_address>`	Set the destination MAC address filter for RTLS tags.	—	—

Parameter	Description	Range	Default
`uidNamespaceFilter <filter>`	A list of UID namespaces to filter devices included in the reports. Applies only Eddystone-UID devices. You can specify a maximum of 10 namespaces	—	—
`urlFilter <filter>`	A list of URL strings to filter devices included in the reports. Applies only to Eddystone-URL devices. The string listed here can be partial URL strings. You can specify a maximum of 10 URL strings.	—	—
`username <user>`	Endpoint user name.	—	—
`vlan <vlan_id>`	Configures a client specific VLAN to transport IoT telemetry data	—	—
`no…`	Removes any existing configuration.	—	—

DataFilter Values

Value	Description
#2	reporter
2.1	name
2.3	ipv4
2.4	ipv6
2.5	hwType
2.6	swVersion
2.7	swBuild
2.8	time
#3	reported
3.2	deviceClass
3.3	model
3.4	firmware
3.5	assetId
3.6	publicKey
3.7	lastSeen

Value	Description
3.9	bevent
3.10	rssi
3.11	cell
3.12	beacons
3.13	txpower
3.14	sensors
3.14.1	accelerometer
3.14.2	battery
3.14.3	temperatureC
3.14.4	humidity
3.14.5	voltage
3.14.6	illumination
3.14.7	motion
3.14.8	current
3.14.9	CO
3.14.10	CO2
3.14.11	VOC
3.14.12	resistance
3.14.13	pressure
3.14.14	alarm
3.14.15	contact
3.14.16	occupancy
3.14.17	mechanicalHandle
3.14.18	distance
3.14.19	capacitance
3.16	stats
3.16.1	uptime
3.16.2	adv_cnt
3.16.3	seq_nr
3.17	inputs

Value	Description
3.18	vendorData
3.19	vendorName
3.20	sensorTimestamp
3.21	flags
3.22	localName
3.23	identity

Example

The following example configures an IoT transport profile:

```
(Instant AP)(config)# iot transportProfile sample
(Instant AP)(IoT Data Profile "sample")# endpointURL
https://edit.meridianapps.com/api/beacons/manage
(Instant AP)(IoT Transport Profile "sample")# endpointType Meridian-Beacon-Management
(Instant AP)(IoT Transport Profile "sample")# payloadContent managed-beacons
(Instant AP)(IoT Transport Profile "sample")# transportInterval 300
(Instant AP)(IoT Transport Profile "sample")# endpointToken
MzkxMTZlMWYtYTgzYS00YWUxLTkzYWEtYjQyNzE1MGMyMjAxOjBiZWJjYWViLTRjNjItNGEwNC1hMGIyLWYzZTM5ZDFlN
GVkNg==
(Instant AP)(IoT Transport Profile "sample")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The following parameters were introduced: - **ZSDFilter** - **data-filter** The following payload content were introduced: - **wiliot** - **exposure-notification** - **zsd** - **serial-data**
AOS-W Instant 8.6.0.0	The following parameters were introduced: - **proxyserver** - **vendorFilter** - **vlan <vlan_id>** The following payloadContent were introduced: - **mysphera** - **ability-smart-sensor** - **sbeacon** - **wifi-assoc-sta** - **wifi-tags** - **wifi-unassoc-sta**

Release	Modification
AOS-W Instant 8.5.0.0	The **aruba-sensors** payload content was introduced.
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were introduced: ■ **uuidFilter** ■ **rssiReporting** The following endpoint types were introduced: ■ **telemetry-https** ■ **telemetry-websocket** The following payload contents were introduced: ■ **unclassified** ■ **enocean-sensors** ■ **enocean-switches** ■ **ibeacons**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and IoT transport profile configuration sub-mode.

iot use-radio-profile

```
iot use-radio-profile <profile>
```

Description

This command sets an IoT radio profile on an AOS-W Instant network.

Syntax

Parameter	Description	Range	Default
`<profile>`	Type of IoT radio profile.	—	—

Example

The following example sets an IoT radio profile:

```
(Instant AP)(config)# iot use-radio-profile sample
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

iot useTransportProfile

```
iot useTransportProfile <profile>
```

Description

This command sets an IoT management server profile on an AOS-W Instant network. You can set up to two management server profiles.

Syntax

Parameter	Description	Range	Default
`<profile>`	Type of IoT management server profile.	—	—

Example

The following example sets an IoT transport profile:

```
(Instant AP)(config)# iot useTransportProfile sample
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Syntax was modified to from iot usetransportProfile to iot useTransportProfile.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

ip-address

```
ip-address <ip-address> <subnet-mask> <nexthop-ip-address> <dns-ip-address> <domain-name>
```

Description

This command configures an IP address for the OAW-IAP.

Syntax.

Parameter	Description	Range	Default
`<ip-address>`	Assigns an IP address to the OAW-IAP.	—	—
`<subnet-mask>`	Specifies the subnet mask.	—	—
`<nexthop-ip-address>`	Specifies the gateway IP address.	—	—
`<dns-ip-address>`	Specifies the DNS server IP address. You can configure up to two DNS servers separated by a comma. If the first DNS server goes down, the second DNS server will take control of resolving the domain name.	—	—
`<domain-name>`	Specifies the domain name.	—	—

Usage Guidelines

Use this command to assign a static IP address to the OAW-IAP.

Example

The following example configures an IP address for the OAW-IAP.

```
(Instant AP)# ip-address 10.65.72.126 255.255.255.240 10.65.72.113 10.65.7.5,10.65.6.15
example.com
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	The **<dns-ip-address>** parameter allows you to configure up to two DNS servers separated by a comma.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

ipm

```
ipm
  disable
  enable
  ipm-power-reduction-step-prio
  no
```

Description

This command configures IPM. It also helps set IPM power reduction steps and specify their priorities. IPM is disabled by default.

IPM cannot be disabled if ITM is enabled. Disabling IPM when ITM is enabled will display the following error message: **Reject: Cannot disable ipm when itm is enabled, please disable itm first**

Parameter	Description
`ipm`	IPM system on 300 Series, 310 Series, and 330 Series access points. IPM is a feature that actively measures the power utilization of an OAW-IAP and dynamically adapts to the power resources.
`enable`	Enables IPM on the OAW-IAP.
`disable`	Disables IPM on the OAW-IAP. Turn off ITM before disabling IPM.
`ipm-power-reduction-step-prio`	Sets IPM power reduction steps and specifies their priorities. A prioirity between 1-16 can be assigned to a reduction step.
`no`	Removes the IPM configuration.

The following table lists the reduction steps available for IPM and ITM:

Reduction Step	Description
`cpu_throttle_25`	Reduces CPU frequency to 25%
`cpu_throttle_50`	Reduces CPU frequency to 50%
`cpu_throttle_75`	Reduces CPU frequency to 75%
`disable_alt_eth`	Disables 2nd Ethernet port
`disable_pse`	Disables PSE
`disable_usb`	Disables USB
`radio_2ghz_chain_1x1`	Reduces 2 GHz chains to 1x1
`radio_2ghz_chain_2x2`	Reduces 2 GHz chains to 2x2
`radio_2ghz_chain_3x3`	Reduces 2 GHz chains to 3x3
`radio_2ghz_power_3dB`	Reduces 2 GHz radio power by 3dB from maximum
`radio_2ghz_power_6dB`	Reduces 2 GHz radio power by 6dB from maximum

Reduction Step	Description
radio_5ghz_chain_1x1	Reduces 5 GHz chains to 1x1
radio_5ghz_chain_2x2	Reduces 5 GHz chains to 2x2
radio_5ghz_chain_3x3	Reduces 5 GHz chains to 3x3
radio_5ghz_power_3dB	Reduces 5 GHz radio power by 3dB from maximum
radio_5ghz_power_6dB	Reduces 5 GHz radio power by 6dB from maximum

Example

The following example enables IPM:

```
(Instant AP)(config)# ipm
(Instant AP)(ipm)# enable
(Instant AP)(ipm)# end
(Instant AP)# commit apply
```

The following example alters the IPM priority list:

```
(Instant AP) #configure terminal
(Instant AP)(config) # ipm
(Instant AP)(ipm) # ipm-power-reduction-step-prio ipm-step radio_5ghz_power_3dB priority 1
(Instant AP)(ipm) # exit
(Instant AP)(config) # exit
(Instant AP)# commit apply
committing configuration...
```

Related Commands

Command	Description
itm	Configures ITM on the AP.
show running-config	Displays the status of IPM configuration and the priority of reductions steps.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and IPM configuration sub-mode.

ip dhcp

```
ip dhcp <dhcp_profile>
   bid <bid>
   client-count <idx>
   default-router <default_router>
   dhcp-relay
   dhcp-server <dhcp_server>
   disable-split-tunnel
   dns-cache
   dns-server <dns_server>
   domain-name <domain-name>
   dynamic-dns [key <algo-name:keyname:keystring>]
   exclude-address <exclude_address>
   host <mac>
   ip-range <start_IP> <end_IP>
   lease-time <lease_time>
   option <option_type> <option_value>
   option82 {alu|xml}
   reserve {first <count>| last <count>}
   server-type <server_type>
   server-vlan <idx>
   subnet <subnet>
   subnet-mask <Subnet-Mask>
   vlan-ip <VLAN_IP> mask <VLAN mask>
   no…
```

Description

This command configures DHCP assignment modes and scopes for an AOS-W Instant network.

Syntax

Parameter	Description	Range	Default
`ip dhcp <profile>`	Creates a DHCP profile with a unique name.	—	—
`bid <bid>`	Defines the branch ID. **NOTE:** You can allocate multiple BID per subnet. The OAW-IAP generates a subnet name from the DHCP IP configuration, which the switch can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.	—	—

Parameter	Description	Range	Default
`client-count <idx>`	Defines the number of clients allowed per DHCP branch. **NOTE:** The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The OAW-IAP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.	—	—
`default-router <default_ router>`	Defines the IP address of the default router for the Distributed, L2 , Local, Local, L2, and Local, L3 DHCP scopes.	—	—
`dhcp-relay`	Enables the OAW-IAPs to intercept the broadcast packets and relay DHCP requests directly to corporate network.	—	—

Parameter	Description	Range	Default
	The DHCP relay is enabled for the centralized DHCP scopes to reduce network traffic caused by the broadcasting of DHCP requests to the corporate network. With a centralized DHCP scope, the clients in the branch are in the same subnet as clients in the corporate network. Normally the DHCP request goes through the VPN tunnel and is broadcast into the corporate network. This feature allows it to succeed without requiring to broadcast and thus reduces the network traffic.		
`dhcp-server <dhcp_server>`	Defines the IP address of the corporate DHCP server for DHCP request relay.	—	—
`dynamic-dns`	Enables dynamic dns updates for this pool.	—	Disabled
`dynamic-dns [key <algo-name:keyname:keystring>]`	You can optionally choose to configure a TSIG shared secret key to secure the dynamic updates. The following algorithm names are supported: ■ hmac-md5 (used by default if algo-name is not specified) ■ hmac-sha1 ■ hmac-sha256 **NOTE:** When a **key** is configured, the update is successful only if OAW-IAP and DNS server clocks are in sync.	—	hmac-sha1:arubaddns: 16YuLPdH21rQ6PuK9udsVLtJw3Y=
`disable-split-tunnel`	Disables split tunnel functionality for Centralized, L2 subnets.	—	—

Parameter	Description	Range	Default
	Split tunneling allows a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. When split-tunnel is disabled, all the traffic including the corporate and Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped.		
`dns-cache`	Enables DNS caching on the OAW-IAP, which allows the OAW-IAP to respond to DNS requests from cache or deny the request immediately if the upstream DNS server is not reachable.	—	—
`dns-server <dns_server>`	Defines the DNS server IP address. You can configure up to 4 DNS servers for a DHCP scope.	—	—
`domain-name <domain-name>`	Defines the domain name.	—	—
`host <mac>`	Allows you to specify the host MAC address.	1–25	—
`exclude-address <exclude_address>`	Defines the IP address to exclude for the Local, L3 DHCP scope. The value entered in the field determines the exclusion range of the subnet. Based on the size of the subnet, the IP addresses that come before or after the IP address value specified in this field are excluded.	—	—

Parameter	Description	Range	Default
`ip-range <start_IP> <end_IP>`	Defines a range of IP addresses to use in the Distributed, L2 and Distributed, L3 DHCP scopes. You can configure a range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically. You can configure up to four different ranges of IP addresses ■ For **Distributed, L2** mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. ■ For **Distributed, L3** mode, you can configure any discontiguous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.	—	—
`lease-time <lease_time>`	Defines a lease time for the client in seconds.	120–86400 seconds	43200 seconds (720 minutes)
`option <option_type> <option_value>`	Defines the type and a value for the DHCP option to use.	—	—

Parameter	Description	Range	Default
	You can configure up to eight DHCP options supported by the DHCP server and enter the option value in "" not exceeding 255 characters.		
`option82 {alu|xml}`	Enables the DHCP Option 82 for the Centralized L2 DHCP scope to allow clients to send DHCP packets with the Option 82 string. To enable ALU based DHCP option82, ensure that **dhcp-option82-xml** is disabled.	—	—
`reserve {first <count>| last <count>}`	Reserves the first few and last few IP addresses in the subnet.	—	—
`server-type <server_type>`	Defines any of the following DHCP assignment modes: ■ **Distributed, L2** ■ **Distributed, L3** ■ **Local** ■ **Local, L2** ■ **Local, L3** ■ **Centralized, L2** ■ **Centralized, L3**	Distributed, L2; Distributed, L3; Local; Local, L2; Local, L3; Centralized, L2; Centralized, L3	Local
`server-vlan <idx>`	Configures a VLAN ID for the DHCP scope. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile.	1-4093	—
`subnet <subnet>`	Defines the network IP address	—	—
`subnet-mask <subnet_mask>`	Defines the subnet mask for Local; Local, L3; and Distributed, L3 DHCP scopes. The subnet mask and the network determine the size of subnet.	—	—

Parameter	Description	Range	Default
`vlan-ip <VLAN_IP> mask <VLAN mask>`	Defines the IP address and subnet mask for the DHCP server VLAN for Local, Local, L3, and Centralized, L3 servers.	—	—
`no…`	Removes any existing configuration.	—	—

Usage Guidelines

Use this command to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the following types of DHCP profiles.

- **Distributed, L2—**In this mode, the Virtual Controller acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller controls a scope that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.
- **Distributed, L3**—In this mode, the Virtual Controller acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the Virtual Controller is configured with a unique subnet and a corresponding scope.
- **Local**—In this mode, the Virtual Controller acts as both the DHCP Server and the default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other OAW-IAP clusters. The Virtual Controller assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the Virtual Controller acts as a DHCP server with data center as the gateway. When Local, L2 DHCP scope is selected, the NAT for client IPs is not carried out at the source.
- **Local, L3**— In this mode, the Virtual Controller acts as a DHCP server and the gateway, and assigns an IP address from the local subnet. The OAW-IAP routes the packets sent by clients on its uplink. This mode does not provide corporate access through the IPsec tunnel. This DHCP assignment mode is used with the L3 forwarding mode.
- **Centralized, L2**—When a Centralized, L2 DHCP scope is configured, the Virtual Controller bridges the DHCP traffic to the switch over the VPN or GRE tunnel. The IP address is obtained from the DHCP server behind the switch serving the VLAN or GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the switch.
- **Centralized, L3**—For Centralized, L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located either in the corporate or local network. The Centralized, L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

Example

The following example configures a Distributed, L2 DHCP scope:

```
(Instant AP)(config)# ip dhcp corpNetwork1
(Instant AP)(DHCP Profile"corpNetwork1")# ip dhcp server-type distributed,l2
(Instant AP)(DHCP Profile"corpNetwork1")# server-vlan 1
(Instant AP)(DHCP Profile"corpNetwork1")# subnet 192.0.1.0
(Instant AP)(DHCP Profile"corpNetwork1")# subnet-mask 255.255.255.0
(Instant AP)(DHCP Profile"corpNetwork1")# default-router 192.0.1.1
```

```
(Instant AP)(DHCP Profile"corpNetwork1")# client-count 0
(Instant AP)(DHCP Profile"corpNetwork1")# dns-server 192.0.1.2
(Instant AP)(DHCP Profile"corpNetwork1")# domain-name www.example.com
(Instant AP)(DHCP Profile"corpNetwork1")# lease-time 1200
(Instant AP)(DHCP Profile"corpNetwork1")# ip-range 192.0.1.0 192.0.1.17
(Instant AP)(DHCP Profile"corpNetwork1")# reserve first 2
(Instant AP)(DHCP Profile"corpNetwork1")# option 176
"MCIPADD=10.72.80.34,MCPORT=1719,TFTPSRVR=10.80.0.5,L2Q=1,L2QVLAN=2,L2QAUD=5,L2QSIG=3"
(Instant AP)(DHCP Profile"corpNetwork1")# end
(Instant AP)# commit apply
```

The following example configures a Distributed,L3 DHCP scope:

```
(Instant AP)(DHCP Profile <profile-name>)# ip dhcp server-type <Distributed,L3>
(Instant AP)(DHCP Profile <profile-name>)# server-vlan <vlan-ID>
(Instant AP)(DHCP Profile <profile-name>)# client-count <number>
(Instant AP)(DHCP Profile <profile-name>)# dns-server <dns_server>
(Instant AP)(DHCP Profile <profile-name>)# dynamic-dns key <algo-name:keyname:keystring>
(Instant AP)(DHCP Profile <profile-name>)# domain-name <domain-name>
(Instant AP)(DHCP Profile <profile-name>)# lease-time <seconds>
(Instant AP)(DHCP Profile <profile-name>)# ip-range <start-IP> <end-IP>
(Instant AP)(DHCP Profile <profile-name>)# reserve {first | last} <count>
(Instant AP)(DHCP Profile <profile-name>)# option <type> <value>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure VLAN in a Local DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# vlan-ip <VLAN_IP> mask <VLAN mask>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

To configure a default router in a Local DHCP profile:

```
(Instant AP)(config)# ip dhcp <profile-name>
(Instant AP)(DHCP Profile <profile-name>)# default-router <default_router>
(Instant AP)(DHCP Profile <profile-name>)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **xml** option was introduced in the **option82** parameter.
Alcatel-Lucent AOS-W Instant 6.5.4.0	This command was enhanced to configure the VLAN IP address and default router settings in a DHCP profile.
Alcatel-Lucent AOS-W Instant 6.4.4.4-4.2.3.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	Command modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and IP DHCP profile configuration sub-mode.

ip dhcp pool

```
ip dhcp pool
   dns-cache
   dns-server  <IP-address>
   domain-name <domain-name>
   lease-time <minutes>
   subnet <IP-address-subnet>
   subnet-mask <Subnet_Mask>
   no…
```

Description

This command configures a DHCP pool on the Virtual Controller.

Syntax

Parameter	Description	Range	Default
`dns-cache`	Enables DNS caching on the OAW-IAP, which allows the OAW-IAP to respond to DNS requests from cache or deny the request immediately if the upstream DNS server is not reachable. When DNS caching is enabled, the DNS server configuration details are ignored.	—	—
`dns-server <address>`	Defines the IP address of the DNS server. You can specify up to eight IP addresses as a comma separated list.	—	—
`domain-name <domain-name>`	Defines the name of domain to which the client belongs.	—	—
`lease-time <minutes>`	Configures the duration of the DHCP lease in minutes.	2–43200 minutes	720 minutes
`subnet <IP-address-subnet>`	Defines IP address of the subnet.	—	—
`subnet-mask <Subnet_Mask>`	Defines the subnet mask of the IP address,	—	—
`no…`	Removes any existing configuration	—	—

Usage Guidelines

Use this command to configure a DHCP pool. The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the Virtual Controller. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The pool can support up to 2048 addresses. The default size of the IP address pool is 512. When an OAW-IAP receives a DHCP request from a client, it examines the origin of the request to determine if it a response must be sent. If the IP address of the VLAN matches a configured DHCP pool, the OAW-IAP answers the request.

Example

The following command configures a DHCP pool:

```
(Instant AP)(config)# ip dhcp pool
(Instant AP)(DHCP)# domain-name example.com
(Instant AP)(DHCP)# dns-cache
(Instant AP)(DHCP)# dns-server 192.0.2.1
```

```
(Instant AP)(DHCP)# lease-time 20
(Instant AP)(DHCP)# subnet 192.0.2.0
(Instant AP)(DHCP)# subnet-mask 255.255.255.0
(Instant AP)(DHCP)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and IP DHCP configuration sub-mode.

ip-mode

```
ip-mode {v4-only|v4-prefer}
no…
```

Description

This command configures the IP mode to enable the processing of IPv4 packets globally.

Syntax

Parameter	Description	Range	Default
`ip-mode`	Configures the IP mode to process IPv6 or IPv4 packets.	—	—
`v4-only`	Enables global processing of IPv4 packets.	—	—
`v4-prefer`	TBU	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to configure IP modes to enable global processing of IPv4 packets.

Example

The following example configures the IPv4 mode:

```
(Instant AP)(config)# ip-mode v4-only
(Instant AP)(config)# end
(Instant AP )# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.0.0-4.3.0.0	Command introduced.

Command Information

Platform	Command Mode
OAW-IAP214/OAW-IAP215, OAW-IAP224/OAW-IAP225, OAW-IAP274/OAW-IAP274, OAW-IAP314/OAW-IAP315, OAW-APAP-324/OAW-IAP325, OAW-IAP334/OAW-IAP335.	Privileged EXEC mode

ip radius

```
ip radius rfc-3576-server udp-port <port>
```

Description

This command configures global parameters for configured RADIUS servers.

Syntax

Parameter	Description	Default	Range
`rfc-3576-server`	Configures the UDP port to receive requests from a RADIUS server. **NOTE:** This parameter can only be used on AOS-W Instant Virtual switch.	—	—
`udp-port`	Indicates the UDP port to receive server requests.	3799	1–65535
`<port>`	Indicates the port number.	—	—

Usage Guidelines

This command configures global RADIUS server parameters. The `rfc3576` parameter must be enabled in the **wlan auth-server** command for the global RADIUS server configuration to take effect.

Example

The following example configures the UDP port:

```
(Instant AP)(config)# ip radius rfc-3576-server udp-port 1700
(Instant AP)(config)# end
(Instant AP )# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.3.0	Command introduced.

Command Information

Platform	Command Mode
All platforms	Configuration mode

itm

```
itm
   no
```

Description

This command enables Intelligent Thermal Management on the AP. When enabled, certain operations of the AP will be throttled down to reduce its internal temperature. The limitations of AP operations is defined by the priority assigned for reduction steps configured in **ipm** command.

IPM must be enabled for ITM to function. Turning on ITM when IPM is disabled will display the following error message: **Reject: Cannot enable itm because ipm is disabled.**

Parameter	Description
`itm`	Enables ITM on the AP
`no itm`	Disables ITM on the AP.

Example

The following command enables thermal management on the AP:

```
(Instant AP)(config)# itm
```

The following command disables thermal management on the AP:

```
(Instant AP)(config)# no itm
```

Related Commands

Command	Description
ipm	Configures IPM settings.
show running-config	Displays the status of ITM configuration and the priority of reductions steps.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-570 Series, OAW-570EX Series, and OAW-AP518 access points	Configuration mode

l3-mobility

```
l3-mobility
  home-agent-load-balancing
  subnet <IP-address-subnet> <subnet-mask> <vlan> <virtual-controller-IP-address>
  virtual-controller <IP-address>
  no…
```

Description

This command configures Layer-3 mobility domains on an OAW-IAP.

Parameter	Description	Range	Default
`l3-mobility`	Enables Layer-3 mobility configuration sub-mode.	—	—
`home-agent-load-balancing`	Enables home agent load balancing. When enabled, the Virtual Controller assigns the home OAW-IAP for roamed clients by using a round robin policy. With this policy, the load for the OAW-IAPs acting as Home Agents for roamed clients is uniformly distributed across the OAW-IAP cluster.	—	Disabled
`<IP-address>`	Configures the IP address for the subnets support in an OAW-IAP cluster.	—	—
`subnet <subnet-mask>`	Specifies the subnet mask.	—	—
`<vlan>`	Assigns the VLAN applicable to the OAW-IAP cluster.	1-4093	—
`<virtual-controller IP>`	Specifies the IP address of the Virtual Controller in an OAW-IAP cluster.	—	—
`virtual-controller <IP-address>`	Adds the IP address of a Virtual Controller to the mobility domain. In a typical deployment scenario, all the OAW-IAPs are configured in one subnet and all the clients in another subnet. You can also deploy OAW-IAPs across different subnets, in which case the OAW-IAPs in each subnet will form a cluster with its own Virtual Controller IP address. To allow clients to roam seamlessly among all the OAW-IAPs, the Virtual Controller IP for each of the foreign subnets must be configured for each OAW-IAP cluster.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures L3-mobility:

```
(Instant AP)(config)# l3-mobility
(Instant AP)(L3-mobility)# home-agent-load-balancing
(Instant AP)(L3-mobility)# virtual-controller 192.0.2.1
(Instant AP)(L3-mobility)# subnet 192.0.2.2 255.255.255.0 1 192.0.2.1
(Instant AP)(L3-mobility)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and L3 mobility configuration sub-mode.

lacp-mode

```
lacp-mode {enable|disable}
no..
```

Description

Use this command to enable, disable, and remove the static LACP configuration. When an OAW-IAP boots up, it forms the LACP according to the static configuration.

Parameter	Description	Range	Default
`enable`	This parameter enables the static LACP configuration. The OAW-IAP will work on LACP mode irrespective of whether or not the peer switch works on the LACP mode.	—	—
`disable`	This parameter disables the static LACP configuration. The OAW-IAP will not work on LACP mode even it detects any LACP PDUs from the peer switch.	—	—
`no`	Removes the static LACP configuration	—	—

Example

The following example configures the static LACP for the OAW-IAP.

```
(Instant AP)# lacp-mode enable
(Instant AP)# lacp-mode disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-IAP- 225, OAW-IAP-325, OAW-IAP275	Privileged EXEC mode

led-off

```
led-off
no…
```

Description

This command disables LED display on an OAW-IAP.

Parameter	Description	Range	Default
`led-off`	Disables LED display.	—	—
`no…`	Re-enables LED display.	—	—

Example

The following example disables LED display on an OAW-IAP:

```
(Instant AP)(config)# led-off
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

loginsession

```
loginsession timeout <val>
```

Description

This command configures the management session (Telnet or SSH) to remain active without any user activity. The management user must re-login to the OAW-IAP after a Telnet or SSH session times out. If you set the timeout value to 0, sessions do not time out.

Parameter	Description	Range	Default
`timeout`	Number of seconds or minutes that a management session remains active without any user activity.	5-60 minutes or 1-3600 seconds, 0 to disable	5 minutes

Example

The following example configures management sessions on the OAW-IAP to not time out:

```
(Instant AP)(config) # loginsession timeout 0
(Instant AP)(config) # end
(Instant AP) # commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

logout

```
logout
```

Description

This command logs you out of the current CLI session and return to the user login prompt.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

managed-mode-profile

```
managed-mode-profile
   automatic
   config-filename <filename>
   debug-managed-mode
   download-method <method>
   retry-poll-period <time-in-sync>
   server <server name>
   sync-time day <dd> | hour <hh> | min <mm> | window <window>
   username <username>
   password <password>
   no…
```

Description

Use this command to enable automatic configuration of the OAW-IAPs in the management mode.

The following checks must be performed before the configuration:

- Ensure that the OAW-IAPs running AOS-W Instant 8.7.0.x Command-Line Interface or later release version.
- When the OAW-IAPs are in the management mode, ensure that the OAW-IAPs are not managed by OmniVista 3600 Air Manager.

Parameter	Description	Rang-e	Defaul-t
`managed-mode-profile`	Configures the managed-mode-profile for automatic configuration.	—	—
`automatic`	Enabled the automatic mode to automatically generate the user credentials based on OAW-IAP MAC address.	—	—
`config-filename  <file_name>`	Filename—Indicates filename within the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.	—	—
`download-method <method>`	Denotes the method used for downloading configuration files (FTP or FTPS).	—	—

Parameter	Description	Rang-e	Defaul-t
`server <server_name>`	Denotes the name of the server or the IP address of the server from which the configuration file must be downloaded.	—	—
`sync-time day <dd> hour <hh> min <mm> window <window>`	Configures the day and time at which the OAW-IAPs can poll the configuration files from the server. ■ `day <dd>`—Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, enter 00. ■ `hour <hh>`—Indicates hour within the range of 0-23. ■ `min <mm>`—Indicates minutes within the range of 0-59. ■ `window <hh>`—Defines a window for synchronization of the configuration file. The default value is 3 hours.	—	—
`retry-poll-period <time-in-sync>`	Configures the time interval in minutes between two retries, after which OAW-IAPs can retry downloading the configuration file	—	—

Parameter	Description	Rang-e	Defaul-t

`username <username>`
`password <password>`
	Denotes the user credentials set by the user to enable automatic configuration.	—	—

`no…`	Removes the configuration.	—	—

Example

The following example configures an OAW-IAP for automatic configuration:

```
(Instant AP)(config)# managed-mode-profile
(Instant AP)(managed-mode-profile)# username <username>
(Instant AP)(managed-mode-profile)# password <password>
(Instant AP)(managed-mode-profile)# config-filename instant.cfg
(Instant AP)(managed-mode-profile)# download-method ftps
(Instant AP)(managed-mode-profile)# sync-time day 00 hour 03 min 30 window 02
(Instant AP)(managed-mode-profile)# retry-poll-period 10
(Instant AP)(managed-mode-profile)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

managed-mode-sync-server

```
managed-mode-sync-server
```

Description

This command is used to retrieve a new set of configuration from the server ahead of the next scheduled sync-time. Use this command for a real-time retrieve and apply of the configuration from the server, even before its actual set sync-time.

Parameter	Description	Range	Default
`managed-mode-sync-server`	Initiates the fetching of a new set of configuration from the server for the OAW-IAPs in the management mode.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

mesh-cluster

```
mesh-cluster-key <key>
mesh-cluster-name <name>
no…
```

Description

This command configures name and key details in a mesh network. After you execute this command, ensure to reboot the OAW-IAP for the mesh cluster functionality to take effect. Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned OAW-IAP that has a valid uplink (wired or 3G) functions as a mesh portal, and the OAW-IAP without an Ethernet link functions as a mesh point. The mesh portal can also act as a Virtual Controller. A mesh portal uses its uplink connection to reach the Virtual Controller, a mesh point, or establishes an all wireless path to the mesh portal. Mesh portals and mesh points are also known as mesh nodes, a generic term used to describe OAW-IAPs configured as mesh.

Mesh OAW-IAPs detect the environment when they boot up and locate and associate with their nearest neighbor to determine the best path to the mesh portal.

AOS-W Instant mesh functionality is supported only on dual radio OAW-IAPs only. On dual-radio OAW-IAPs, the 5 GHz radio is always used for both mesh-backhaul and client traffic, while the 2.4 GHz radio is always used for client traffic.

The mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on OAW-IAP ROWs like any other regulatory domain.

Parameter	Description	Range	Default
`<key>`	Enables key values in a mesh network.	8–64	—
`<name>`	Enables mesh name in a mesh network.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables mesh network key on an OAW-IAP:

```
(Instant AP)# mesh-cluster-key 12345678
```

The following example enables mesh network name on an OAW-IAP:

```
(Instant AP)# mesh-cluster-name Hallmark
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

mesh-cluster

```
mesh-cluster <cluster_name> wpa2-psk <cluster_key> priority <cluster_priority>
```

Description

This command configures a new mesh cluster profile on the OAW-IAP with a passphrase and a priority. In the configuration mode, you can create up to 16 mesh cluster profiles, including the default mesh cluster profile. Use this command when you choose to configure multiple mesh cluster profiles on an OAW-IAP to enable failover to the next high priority cluster.

Parameter	Description	Range	Default
`<cluster_name>`	Configures a mesh cluster profile. Enter a name for the mesh cluster profile. The name must be 8–32 characters long.	8–32 characters	—
`<wpa2-psk>`	Configures a WPA2 PSK passphrase as the cluster key.	8–64 characters	—
`<priority>`	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The supported range of values is 1–16. The lower the number, the higher the priority.	1—15	—

Example

The following example configures multiple mesh cluster profiles on an OAW-IAP

```
(Instant AP)(config)# mesh-cluster cluster_1 wpa2-psk ade23d343 priority 1
(Instant AP)(config)# mesh-cluster cluster_2 wpa2-psk sidq87dqu priority 2
(Instant AP)(config)# mesh-cluster cluster_3 wpa2-psk sdygeg28g priority 3
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration Mode

mesh-disable

```
mesh-disable
no…
```

Description

This command disables the mesh functionality in an OAW-IAP.

Parameter	Description	Range	Default
`no…`	Removes the mesh disable configuration.	—	—

Example

The following example disables the mesh functionality OAW-IAP:

```
(Instant AP)# mesh-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

mesh-mobility

```
mesh-mobility [high|low|<number>]
no…
```

Description

This command configures enabled fast roaming on a mesh point.

Syntax

Parameter	Description	Range	Default
`high`	Enables mesh roaming function and RSSI threshold less than or equal to 22	—	—
`low`	Enables mesh roaming function and RSSI threshold less than or equal to 15.	—	—
`<number>`	Enables mesh roaming function and RSSI is set as a definite value	10-50	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to configure fast roaming on mesh points.

Example

The following example enables fast roaming on an mesh point::

```
(Instant AP)# mesh-mobility high
(Instant AP)# mesh-mobility low
(Instant AP)# mesh-mobility 30
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

mesh-split5g-band-range

```
mesh-split5g-band-range {full| lower | upper | first}
```

Description

This command configures the 5 GHz radio used for the mesh link. Use this command to configure the 5 GHz radio that should be used as the mesh link. This setting only takes effect when split 5 GHz or dual 5 GHz radio is enabled on the AP. The AP must be reboot for the configuration to take effect.

Parameter	Description
`full`	Configures both the sub bands of the 5 GHz radio as the mesh link. The radio assignment however depends on factors such as hop count to the mesh portal, availability of neighboring mesh APs, and preferred uplink radio setting of the mesh profile. This is the default setting.
`lower`	Configures the lower 5 GHz radio as the mesh link.
`upper`	Configures the upper 5 GHz radio as the mesh link
`first`	Configures radio 0 as the mesh link.

The radio assignment and operating band information is listed in the following table:

Radio Mode	Radio	Operating Band
Dual 5 GHz (OAW-340 Series access points)	Radio 0	Lower 5 GHz band
	Radio 1	Upper 5 GHz band
Split 5 GHz (OAW-AP555 access point)	Radio 0	Upper 5 GHz band
	Radio 2	Lower 5 GHz band

Example

The following example configures the lower band of the 5 GHz radio to serve as the mesh link:

```
(Instant AP)(config) #mesh-split5g-band-range lower
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-340 Series and OAW-AP555 access points	Configuration mode

mgmt-accounting

```
mgmt-accounting command all
no…
```

Description

This command is used to enable accounting privileges on TACACS+ servers for management users. Use this command to record the user name of the management users and the respective IP address sending the request to account for the usage of the authorized network services.

Parameter	Description	Range	Default
`mgmt-accounting command all`	Configures TACACS+ servers to enable accounting for management users.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a TACACS+ server for management accounting

```
(Instant Access Point)(config)# mgmt-accounting command all tacacs1
(Instant Access Point)(config)# end
(Instant Access Point)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

mgmt-auth-server

```
mgmt-auth-server <server>
no…
```

Description

This command is used to configure a management authentication server for administrator users of a Virtual Controller.

Parameter	Description	Range	Default
`mgmt-auth-server <server>`	Configures a server for management user authentication.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures an authentication server for the management UI:

```
(Instant AP)(config)# mgmt-auth-server server1
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

mgmt-auth-server-load-balancing

```
mgmt-auth-server-load-balancing
no…
```

Description

This command enables load balancing when two authentication servers are configured for management user authentication.

Parameter	Description	Range	Default
`mgmt-auth-server-load-balancing`	Enables load balancing between the primary and the backup authentication servers	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables load-balancing between two authentication servers.

```
(Instant AP)(config)# mgmt-auth-server-load-balancing
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

mgmt-auth-server-local-backup

```
mgmt-auth-server-local-backup
no…
```

Description

Configures a secondary internal authentication server that will validate the management interface user credentials at runtime.

Parameter	Description	Range	Default
`mgmt-auth-server-local-backup`	Configures a backup internal server for management user authentication. When enabled, the authentication switches to Internal if there is no response from the RADIUS server (RADIUS server timeout).	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a backup internal authentication server:

```
(Instant AP)(config)# mgmt-auth-server-local-backup
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

mgmt-login-blacklist-period

```
mgmt-login-blacklist-period <10-65535>
no…
```

Description

This command configures the time for which an unauthorized users will be blacklisted.

Parameter	Description	Range
`mgmt-login-blacklist-period`	Configures the time period for which the unauthorized users will be blacklisted. The value is measured in seconds.	10-65535
`no…`	Removes the configuration.	—

Example

The following example configures a backup internal authentication server:

```
(Instant AP)(config)# mgmt-login-blacklist-period 210
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

mgmt-login-threshold

```
mgmt-login-threshold <1-65535>
no…
```

Description

This command configures the number of invalid login attempts allowed before the user is blocked out of the system.

Parameter	Description	Range
`mgmt-login-threshold`	Configures the number of invalid login attempts before a user is block out of the system.	1-65535
`no…`	Removes the configuration.	—

Example

The following example configures a backup internal authentication server:

```
(Instant AP)(config)# mgmt-login-threshold 10
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

mgmt-user

```
mgmt-user <username> [<password>][<type>]
no..
```

Description

This command configures user credentials for access to the Virtual Controller Management UI.

Parameter	Description	Range	Default
`mgmt-user`	Configures administrator credentials.	—	—
`<username>`	Creates a User name for the administrator user.	—	—
`<password>`	Creates a password for the administrator user.	—	—
`<type>`	Indicates the type of the user. For example, users with read-only privilege or the guest management user.	—	—
`no..`	Removes the configuration.	—	—

Example

The following example configures administrator login credentials for the OAW-IAP management interface:

```
(Instant AP)(config)# mgmt-user User1 Password123 guest-mgmt
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command modified.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

mtu

```
mtu <size>
no…
```

Description

This command configures the MTU size for tunnel and br0 interfaces, and uplink interfaces such as 3G or 4G. The configured MTU size is applied when the uplink changes.

Parameter	Description	Range	Default
`mtu <size>`	Configures MTU size.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example sets the MTU size to 1200 bytes:

```
(Instant AP)(config)# mtu <1200>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

name

```
name <name>
```

Description

This command configures a unique name for the OAW-IAP.

Parameter	Description	Range	Default
`name <name>`	Configures a name for the OAW-IAP or the Virtual Controller.	—	—

Example

The following example configures a name for the OAW-IAP:

```
(Instant AP)# hostname <system-name>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

netservice

```
netservice svc-sip <port> <proto> <timeout>
no…
```

Description

This command configures port, protocol, and timeout values for NAT sessions. You can configure a maximum of up to 10 netservice port entries. This command is introduced to help SIP work across NAT. SIP sessions over UDP may age out when an OAW-IAP is performing NAT for its clients. If there are no keepalives in the session, the session ages out and reverse traffic flowing from the destination to the client connected to the OAW-IAP may fail. The above command ensures that the sessions are kept alive for longer duration even though there are no keep alives.

Parameter	Description	Range	Default
`<port>`	Configures the port value for the SIP server port on which the SIP server is configured to listen.	—	—
`<proto>`	Configures UDP or TCP as the protocol.	UDP or TCP	—
`<timeout>`	Configures a timeout value between 15 to 30 minutues	15-30 minutes	—

Example

The following command configures the SIP Net Service for an OAW-IAP:

```
(Instant AP)(config)# netservice svc-sip 5080 udp 15
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

ntp-server

```
ntp-server <name1>,<name2>,<name3>,<name4>
no…
```

Description

This command configures NTP servers for an OAW-IAP. The NTP helps obtain the precise time from a server and regulate the local time in each network element. If NTP server is not configured in the AOS-W Instant network, an OAW-IAP reboot may lead to variation in time data. Upto 4 ntp servers can be configured for an AP.

Parameter	Description	Range	Default
`ntp-server <name1>,<name2>,<name3>,<name4>`	Configures the IP address or the URL (domain name) of the NTP server.	—	pool.ntp.org
`no`	Removes the configuration	—	—

Example

The following command configures an NTP server for an OAW-IAP:

```
(Instant AP)(config)# ntp-server <name1>,<name2>,<name3>,<name4>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Configuration of up to 4 NTP servers supported.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

organization

```
organization <name>
no…
```

Description

This command configures an organization string for OAW-IAPs managed or monitored by the OmniVista 3600 Air Manager Management console. Use this command to specify an organization string for integrating the OmniVista 3600 Air Manager Management Server with the OAW-IAP. The organization is a set of colon-separated strings created by the OmniVista 3600 Air Manager administrator to accurately represent the deployment of each OAW-IAP. This string is defined by the installation personnel on the site.

Parameter	Description	Range	Default
`organization <name>`	Specifies the name of your organization.	You can use any of the following strings: ■ AMP Role— "Org Admin" (initially disabled) ■ AMP User— "Org Admin" (assigned to the role "Org Admin") ■ Folder— "Org" (under the Top folder in AMP) ■ Configuration Group— "Org" You can also assign additional strings to create a hierarchy of sub folders under the folder named "Org": For example: ■ subfolder1 for a folder under the "Org" folder ■ subfolder2 for a folder under subfolder1	—
`no…`	Removes the configuration settings.	—	—

Example

The following command configures an OmniVista 3600 Air Manager organization string:

```
(Instant AP)(config)# organization alcatel
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

out-of-service-hold-on-time

```
out-of-service-hold-on-time <time>
no…
```

Description

This command configures a hold on time in seconds, after which out-of-service operation is triggered. For example, if the VPN is down, the effect of this out-of-service state impacts the SSID availability after the configured hold on time.

Parameter	Description	Range	Default
`<time>`	Configures the hold on time of out-of-service operations.	30–300 seconds	30 seconds
`no…`	Removes the configuration	—	—

Example

The following example sets the out of service hold on interval to 45 seconds:

```
(Instant AP)(config)# out-of-service-hold-on-time 45
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

pcap

```
pcap {start <bssid> <ip> <port> <format> <maxlen> [<channel>]|stop <bssid> <id>}
```

Description

This command configures the wireless packet capture on an OAW-IAP and send the packets to a client packet analyzer utility like Airmagnet, Wireshark and so on, on a remote client.

Before using this command, you need to start the packet analyzer utility on the client and open a capture window for the port from which you are capturing packets. The packet analyzer cannot be used to control the flow or type of packets sent from the OAW-IAPs.

The packet analyzer processes all packets. However, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the timestamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the OAW-IAP.

Parameter	Description	Range	Default
`start`	Starts the packet capture configuration.	—	—
`<bssid>`	Indicates the basic bssid.	—	—
`<ip>`	Indicates the IP address of the client running the packet analyzer.	—	—
`<port>`	indicates the UDP port number on the client station where the captured packets are sent.	—	—
`<format>`	Indicates the number assigned to each format for captured packets.	—	—
`<maxlen>`	Indicates the maximum length of 802.11 frames to include in the capture.	—	—
`<channel>`	Indicates the number of a radio channel to tune into to capture packets.	—	—
`stop`	Stops the packet capture configuration.	—	—
`<id>`	Indicates the ID of the PCAP session.	—	—

Example

The following example starts the packet capture configuration:

```
(Instant AP)# pcap start ac:a3:1e:57:bd:60 10.163.148.35 5555 0 1518
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

per-ap-ssid

```
per-ap-ssid <essid>
no…
```

Description

This command configures the SSID settings to every OAW-IAP in a cluster.

Parameter	Description	Range	Default
`<essid>`	Denotes the environment variable configured in apboot.	—	—
`no…`	Removes the environment variable.	—	—

Example

The following example sets the environment variable:

```
(Instant AP)# per-ap-ssid <essid>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

per-ap-vlan

```
per-ap-vlan <vlan>
no…
```

Description

This command assigns a VLAN to a given SSID profile.

Parameter	Description	Range	Default
`<vlan>`	Denotes the environment variable configured in apboot.	—	—
`no…`	Removes the environment variable.	—	—

Example

The following example sets the environment variable:

```
(Instant AP)# per-ap-vlan <vlan>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-enable

```
pin-enable <pin_current_used>
no…
```

Description

This command enables locking of the SIM PIN for the 3G or 4G modems.

Parameter	Description	Range	Default
`pin-enable <pin_current_used>`	Enables locking of the SIM. To enable SIM PIN lock, the PIN code should be same as the PIN code that is currently used.	—	—
`no…`	Disables SIM PIN locking.	—	—

Example

The following example enables SIM PIN locking:

```
(host)# pin-enable 12345678
```

The following example disables SIM PIN locking:

```
(host)# pin-enable 12345678
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-puk

```
pin-puk <pin_puk>
```

Description

This command unlocks the cellular modems using the PUK code. The SIM PIN of a modem is locked if a user enters incorrect PIN code for three consecutive attempts.

Parameter	Description	Range	Default
`pin-puk <pin_puk> <pin_new>`	Unlocks the SIM PIN using the PUK code provided by the ISP and by entering a new PIN code.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

pin-renew

```
pin-renew <pin_current> <pin_new>
```

Description

This command renews PIN for the SIM card of the 3G or 4G modem.

Parameter	Description	Range	Default
`pin-renew`	Renews the SIM PIN of the modem.	—	—
`<pin-current>`	Allows you to enter the current PIN of the modem SIM.	—	—
`<pin_new>`	Allows you to specify a new SIM PIN for the modem.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

ping

```
ping <host>[count <count> | packet-size <size> | interface <interface> | source-address
<address>]
```

Description

This command sends ICMP echo packets, frame count, packet-size, source-address, and interface information to the specified IP address.

The OAW-IAP times out after two seconds.

Parameter	Description	Range	Default
`<host>`	Indicates the host name.	—	—
`<count>`	Indicates the frame count.	—	—
`<packet-size>`	Indicates the packet-size data in bytes.	—	56
`<interface>`	Indicates the interface through which data is sent.	—	—
`<address>`	Indicates the source IP address to send the ping.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **count**, **packet-size**, **source-address**, and **interface** parameters were introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode

pppoe-uplink-profile

```
pppoe-uplink-profile <profile>
   pppoe-username <username>
   pppoe-passwd <password>
   pppoe-svcname <svcname>
   pppoe-chapsecret <password>
   pppoe-unnumbered-local-l3-dhcp-profile <dhcp-profile>
   no…
```

Description

Use this command to configure PPPoE uplink profile.

Parameter	Description	Range	Default
`pppoe-uplink-profile <profile>`	Creates an uplink profile and enables the PPPoE uplink profile configuration mode.	—	—
`pppoe-username <username>`	Configures a user name to allow a user to log into the DSL network.	—	—
`pppoe-passwd <password>`	Configures a password for the user to log into the DSL network.	—	—
`pppoe-svcname <svcname>`	Specifies the PPPoE service provided by your service provider.	—	—
`pppoe-chapsecret <password>`	Configures a secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.	—	—

Parameter	Description	Range	Default
`pppoe-unnumbered-local-l3-dhcp-profile <dhcp-profile>`	Configures the Local, L3 DHCP gateway IP address as the local IP address of the PPPoE interface. When configured, the local interface acts as an unnumbered PPPoE interface and allows the entire Local, L3 DHCP subnet to be allocated to clients.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures the PPPoE uplink on an OAW-IAP:

```
(Instant AP)(config) # pppoe-uplink-profile
(Instant AP)(pppoe-uplink-profile)# pppoe-username User1
(Instant AP)(pppoe-uplink-profile)# pppoe-passwd Password123
(Instant AP)(pppoe-uplink-profile)# pppoe-svcname internet03
(Instant AP)(pppoe-uplink-profile)# pppoe-chapsecret 8e87644deda9364100719e017f88ebce
(Instant AP)(pppoe-uplink-profile)# pppoe-unnumbered-local-l3-dhcp-profile dhcpProfile1
(Instant AP)(pppoe-uplink-profile)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and PPPoE uplink profile configuration sub-mode.

preferred-uplink

```
preferred-uplink <0,1>
```

Description

This command configures the active uplink for the OAW-IAP.

This command is a per-AP setting and should be configured manually on individual APs through the CLI. Reboot the AP after configuration for the settings to take effect.

Parameter	Description	Range	Default
`preferred uplink`	Configures the uplink port for the AP.	0,1	1
`0`	Configures the eth0 port as the preferred uplink.	—	—
`1`	Configures the eth1 port as the prefferred uplink.	—	—

Example

The following example configures the eth1 port as the preferred uplink:

```
(Instant AP)# preferred-uplink 1
(Instant AP)# write memory
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

proxy

```
proxy {exception <host>| server <host> <port> [<username> <password>]}
```

Description

This command configures HTTP proxy settings to download the image from the cloud server. This command also configures the HTTP proxy settings in an OAW-IAP to route the web classification queries through the proxy server.

Parameter	Description	Range	Default
`exception <hostname>`	Sets the IP address or the domain name of the host to be added under the exception list.	—	—
`server <hostname> <port number> [<username> <password>]`	Sets the HTTP proxy server's IP address or domain name and the port number. You can optionally configure a username and password to authenticate the proxy server. **NOTE:** The `username` and `password` options are applicable only to configure proxy support for web classification.	—	—

Example

The following example configures an HTTP proxy settings in an OAW-IAP:

```
(Instant AP)(config)# proxy exception 10.15.107.214
(Instant AP)(config)# proxy server 10.15.107.210 1337 user1 passwd1
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were added: ■ **username** ■ **password**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

radio-0-5ghz-ant-gain

```
radio-0-5ghz-ant-gain <gain>
```

Description

This command configures external antenna connectors for an OAW-IAP. If your OAW-IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the OAW-IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your OAW-IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the OAW-IAP device. This command is supported only in dual 5GHz mode.

Parameter	Description	Range	Default
`<gain>`	Configures the antenna gain. You can configure a gain value in dBi for the following types of antenna: ■ Dipole or Omni ■ Panel ■ Sector	Diploe or Omni - 6 Panel -14 Sector - 14	—

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 12: *Formula Variable Definitions*

Formula Element	Modification
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

For information on antenna gain recommended by the manufacturer, see .

Example

The following example configures external antenna connectors for the OAW-IAP with the 5 GHz radio band.

```
(Instant AP)# radio-0-5ghz-ant-gain 14
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-0-5ghz-ant-pol

```
radio-0-5ghz-ant-pol <pol>
no radio-0-5ghz-ant-pol
```

Description

This command configures the antenna polarization value for 5 GHz radio 0 channel. Use this command to set the antenna polarization value for 5 GHz radio 0 channel. This command is supported only in dual 5GHz mode.

Parameter	Description	Range	Default
`<pol>`	Denotes the antenna polarization value for 5 GHz radio channel. ■ 0: Co-Polarized radio ID ■ 1: Cross-Polarized radio ID	0 or 1	—

Example

The following example configures the antenna polarization value for a 5 GHz radio channel:

```
(Instant AP)# radio-0-5ghz-ant-pol 1
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-1-5ghz-ant-gain

```
radio-1-5ghz-ant-gain <gain>
```

Description

This command configures external antenna connectors for an OAW-IAP. If your OAW-IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the OAW-IAP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your OAW-IAP device supports external antenna connectors, see the *Install Guide* that is shipped along with the OAW-IAP device. This command is supported only in dual 5GHz mode.

Parameter	Description	Range	Default
`<gain>`	Configures the antenna gain. You can configure gain value in dBi for the following types of antenna: ■ Dipole or Omni ■ Panel ■ Sector	Diploe or Omni - 6 Panel -12 Sector - 12	—

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

EIRP = Tx RF Power (dBm)+GA (dB) - FL (dB)

The following table describes this formula:

Table 13: *Formula Variable Definitions*

Formula Element	Modification
EIRP	Limit specific for each country of deployment
Tx RF Power	RF power measured at RF connector of the unit
GA	Antenna gain
FL	Feeder loss

For information on antenna gain recommended by the manufacturer, see .

Example

The following example configures external antenna connectors for the OAW-IAP with the 5 GHz radio band.

```
(Instant AP)# radio-1-5ghz-ant-gain 12
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-1-5ghz-ant-pol

```
radio-1-5ghz-ant-pol <pol>
no radio-1-5ghz-ant-pol
```

Description

This command configures the antenna polarization value for 5 GHz radio 1 channel.

Syntax

Parameter	Description	Range	Default
`<pol>`	Denotes the antenna polarization value for 5 GHz radio channel. ■ 0: Co-Polarized radio ID ■ 1: Cross-Polarized radio ID	0 or 1	—

Example

The following example configures the antenna polarization value for a 5 GHz radio channel:

```
(Instant AP)# radio-1-5ghz-ant-pol 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-0-channel

```
radio-0-channel <channel> <tx-power>
```

Description

This command configures 5 GHz radio channels for an OAW-IAP. When split-5GHz radio mode is enabled, this command configures the radio channels for the primary 5GHz radio of the OAW-IAP.

Syntax

Parameter	Description	Range	Default
`<channel>`	Configures the specified 5 GHz channel.	The valid channels for a band are determined by the OAW-IAP regulatory domain.	—
`<tx-power>`	Configures the specified transmission power values. It also supports 0.1 dBm and negative values.	-51dBm to 51dBm	—

Example

The following example configures the 5 GHz radio-0 channel:

```
c8:b5:ad:c3:ab:dc# radio-0-channel 149E 20
c8:b5:ad:c3:ab:dc#
c8:b5:ad:c3:ab:dc#
c8:b5:ad:c3:ab:dc# radio-
radio-0-5ghz-ant-gain
radio-0-5ghz-ant-pol
radio-0-channel          only needed for APs support Dual 5G, channel range 100-161
radio-0-disable
radio-1-5ghz-ant-gain
radio-1-5ghz-ant-pol
radio-1-channel          only needed for APs support Dual 5G, channel range 36-64
radio-1-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344/OAW-AP-345	Privileged EXEC mode

radio-0-disable

```
radio-0-disable
```

Description

This command disables the radio-0 profile in the dual 5 GHz radio channel for OAW-AP-344 and OAW-AP-345 access points. Disabling the radio profile using this command will not delete the SSID profiles.

Example

The following example disables the 5 GHz radio-0 channel:

```
radio-0-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-1-channel

```
radio-1-channel <channel> <tx-power>
```

Description

This command configures 60 GHz radio channels for a specific OAW-IAP.

Parameter	Description	Range	Default
`<channel>`	Configures the specified 60 GHz channel. The valid channels for a band are determined by the OAW-IAP regulatory domain.	1 to 4	—
`<tx-power>`	Configures the specified transmission power values. It also supports 0.1 dBm and negative values.	-51dBm to 51dBm	—

Example

The following example configures the 60 GHz radio-1 channel:

```
c8:b5:ad:c3:ab:dc# radio-1-channel 36E 18
c8:b5:ad:c3:ab:dc#
c8:b5:ad:c3:ab:dc#
c8:b5:ad:c3:ab:dc# show ap bss-table
Aruba AP BSS Table
------------------
bss                ess         port  ip             phy    type  ch/EIRP/max-EIRP  cur-cl  ap
name            in-t(s)  tot-t     flags
---                ---         ----  --             ---    ----  ----------------  ------  --
-----           -------  -----    -----
c8:b5:ad:ba:bd:c3  0_ybu_tkip  ?/?   192.168.1.114  a      ap    36/18.0/18.7      0
c8:b5:ad:c3:ab:dc  0        3h:1m:3s  K
c8:b5:ad:ba:bd:d2  ybu_345     ?/?   192.168.1.114  a-VHT  ap    149E/20.0/20.2    0
c8:b5:ad:c3:ab:dc  0        3h:1m:5s  K
c8:b5:ad:ba:bd:d3  0_ybu_tkip  ?/?   192.168.1.114  a      ap    149/20.0/20.2     0
c8:b5:ad:c3:ab:dc  0        3h:1m:4s  K
c8:b5:ad:ba:bd:c2  ybu_345     ?/?   192.168.1.114  a-VHT  ap    36E/18.0/18.7     0
c8:b5:ad:c3:ab:dc  0        3h:1m:4s  K
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

radio-1-disable

```
radio-1-disable
```

Description

This command disables the radio-1 profile in the dual 5 GHz radio channel for OAW-AP-344 and OAW-AP-345 access points. Disabling the radio profile using this command will not delete the SSID profiles. This command is applicable only when the dual 5 GHz mode is enabled in OAW-AP-340 series access points.

Example

The following example disables the 5 GHz radio-1 channel:

```
(Instant AP)# radio-0-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344 and OAW-AP-345 access points	Privileged EXEC mode

radio-2-channel

```
radio-2-channel <channel> <tx-power>
```

Description

This command configures the radio channels for the secondary 5GHz radio of an OAW-IAP. Use this command to configure radio channels for the secondary 5GHz radio when split 5GHz is enabled for a specific OAW-IAP.

Parameter	Description	Range	Default
`<channel>`	Configures the specified 5GHz channel. The valid channels for a band are determined by the OAW-IAP regulatory domain.	The valid channels for a band are determined by the OAW-IAP regulatory domain.	—
`<tx-power>`	Configures the specified transmission power values. It also supports 0.1 dBm and negative values.	-51dBm to 51dBm	—

Example

The following example configures the 60 GHz radio-1 channel:

```
c8:b5:ad:c3:ab:dc# radio-2-channel 149E 20
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-550 Series access points	Privileged EXEC mode

radio-2-disable

```
radio-2-disable
```

Description

This command disables the radio2, the secondary 5GHz radio, of an OAW-IAP. Use this command to disable the secondary 5GHz radio of the OAW-IAP when split 5GHz radio is enabled

Example

The following command disables the radio0 of the OAW-IAP:

```
(Instant AP)# radio-2-disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-550 Series access points	Privileged EXEC mode

radius-vsa-redirect-url

```
radius-vsa-redirect-url {add| clear} <client MAC-address> <URL> [count]
```

Description

This command allows the user to manually add the VSA redirect URL for debugging purpose.

Parameter	Description	Range	Default
`add`	Adds radius redirect url on the AP for debug.	—	—
`clear`	Clears radius redirect url on the AP for debug.	—	—
`<client MAC-address>`	Enter the MAC address of the client to the Instant AP.	—	—
`<URL>`	Enter the URL of the website.	—	—
`<count>`	Allows you to add the number of clients.	—	—

Example

The following output is displayed for **radius-vsa-redirect-url add <client MAC-address> <URL> [count]** command:

```
c8:b5:ad:c3:af:16# radius-vsa-redirect-url add 0e:00:32:f8:ef:10 https://172.10.10.10/guest 1
c8:b5:ad:c3:af:16# sh radius-redirect-url
Radius VSA Redirect URL
-----------------------
MAC                URL
---                ---
0e:00:32:f8:ef:10  https://172.10.10.10/guest
```

The following output is displayed for **radius-vsa-redirect-url clear** command:

```
c8:b5:ad:c3:af:16# radius-vsa-redirect-url clear
c8:b5:ad:c3:af:16# sh radius-redirect-url
Radius VSA Redirect URL
-----------------------
MAC  URL
---  ---
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

reload

```
reload <all>
```

Description

This command performs a reboot of the Virtual Controller. Use this command to reboot an OAW-IAP after making configuration changes or under the guidance of Alcatel-Lucent Networks customer support. The reload command powers down the OAW-IAP, making it unavailable for configuration. After the OAW-IAP reboots, you can access it through a local console connected to the serial port, or through an SSH, Telnet, or UI session. If you need to troubleshoot the OAW-IAP during a reboot, use a local console connection.

After you use the reload command, the OAW-IAP prompts you to confirm this action. If you have not saved your configuration, the OAW-IAP returns the following message:

```
Do you want to save the configuration (y/n):
```

- Enter **y** to save the configuration.
- Enter **n** to not save the configuration.
- Press [Enter] to exit the command without saving changes or rebooting the OAW-IAP.

If your configuration has already been saved, the OAW-IAP returns the following message:

```
Do you really want to reset the system(y/n):
```

- Enter **y** to reboot the OAW-IAP.
- Enter **n** to cancel this action.

The command will timeout if you do not enter **y** or **n**.

Parameter	Description	Range	Default
`<all>`	Reloads all OAW-IAPs in a cluster.	—	—

Example

The following command assumes you have already saved your configuration and you must reboot the OAW-IAP:

The OAW-IAP returns the following messages:

```
Do you really want to reset the system(y/n): y
System will now restart!
...
Restarting system.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

remove-blacklist-client

```
remove-blacklist-client <MAC_address> <AP_name>
```

Description

This command allows you to delete the clients that are blacklisted. Use this command to remove the entries for the clients that are dynamically blacklisted.

Parameter	Description	Range	Default
`MAC-address`	Adds the MAC address of the blacklisted client.	—	—
`AP_name`	Adds the access point name to which the client is connected to.	—	—
`no…`	Removes the specified configuration parameter.	—	—

Example

The following command deletes the blacklisted OAW-IAP client entries:

```
(Instant AP)# remove-blacklist-client d7:a:b2:c3:45:67 AP125
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

reset drt

```
reset drt
```

Description

This command resets the DRT version on an OAW-IAP. Use this command to clear the upgraded DRT file and enable the OAW-IAP cluster to use the default DRT file.

Example

The following command shows how to reset the DRT version:

```
(Instant AP)# reset drt
```

The OAW-IAP returns the following message if the OAW-IAP is using the default DRT version:

```
DRT is already in default status.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

reset drt

```
reset drt
```

Description

This command resets the DRT version on an OAW-IAP. Use this command to clear the upgraded DRT file and enable the OAW-IAP cluster to use the default DRT file.

Example

The following command shows how to reset the DRT version:

```
(Instant AP)# reset drt
```

The OAW-IAP returns the following message if the OAW-IAP is using the default DRT version:

```
DRT is already in default status.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

restrict-corp-access

```
restrict-corp-access
no…
```

Description

This command configures restricted access to the corporate network. Use this command to configure restricted corporate to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master OAW-IAP, including clients connected to a slave OAW-IAP.

Parameter	Description	Range	Default
`no…`	Removes the configuration.	—	—

Example

The following example enables restricted access to the corporate network;

```
(Instant AP)(config) # restrict-corp-access
(Instant AP)(config) # end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

restricted-mgmt-access

```
restricted-mgmt-access <subnet> <mask>
no…
```

Description

This command configures management subnet on an OAW-IAP. Use this command to configure management subnets. This ensures that the OAW-IAP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.

Parameter	Description	Range	Default
subnet	Configures a management subnet address.	—	—
mask	Configures the subnet mask for the management subnet address.	—	—
no…	Removes the configuration.	—	—

Example

The following example configures a management subnet;

```
(Instant AP)(config) # restricted-mgmt-access 192.0.2.13 255.255.255.255
(Instant AP)(config) # end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

rf dot11a-radio-profile

```
rf dot11a-radio-profile <profile_name>
   40MHZ-intolerance
   backoff-time <secs>
   beacon-interval <interval>
   bss-color <0-63>
   cell-size-reduction <reduction>
   channel-quality-aware-arm-disable
   channel-quality-threshold
   channel-quality-wait-time
   csa-count <count>
   csd-override
   disable-arm-wids-functions
   dot11h
   error-rate-threshold <percent>
   error-rate-wait-time <secs>
   honor-40MHZ-intolerance-disable
   ideal-coverage-index <idx>
   interference-immunity <level>
   free-channel-index <idx>
   legacy-mode
   max-distance <count>
   max-tx-power <power>
   min-tx-power <power>
   scanning-disable
   smart-antenna
   spectrum-band <type>
   spectrum-monitor
   very-high-throughput-disable
   zone <zone>
   no…
```

Description

This command configures a 5 GHz or 802.11a radio profile for an OAW-IAP. The following ARM settings defined in this radio profile will take precedence over the settings in the ARM profile:

- **backoff-time <secs>**
- **channel-quality-aware-arm-disable**
- **channel-quality-threshold**
- **channel-quality-wait-time**
- **error-rate-threshold <percent>**
- **error-rate-wait-time <secs>**
- **ideal-coverage-index <idx>**
- **scanning-disable**

Parameter	Description	Range	Default
`rf dot11a-radio-profile`	Enables the 5 GHz RF configuration sub-mode	—	—

Parameter	Description	Range	Default
`40MHZ-intolerance`	Controls whether or not OAW-IAPs using this radio profile will advertise intolerance of 40 MHz operation.	—	Disabled
`backoff-time <secs>`	Configures the time when an OAW-IAP backs off after requesting a new channel or power.	10-3600	240
`beacon-interval <interval>`	Enter the Beacon period for the OAW-IAP in milliseconds. When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.	60-500	100
`bss-color <0-63>`	Configures BSS color for the BSSIDs broadcast by the radio. The value range is 0-63, where 0 configures automatic BSS coloring. The default value is 0.	0-63	0
`channel-quality-aware-arm-disable`	With this parameter, ARM ignores the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value.	—	Disabled
`channel-quality-threshold <thresh>`	Specifies the channel quality percentage below which ARM initiates a channel change.	0-100	70
`channel-quality-wait-time <secs>`	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. **NOTE:** If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.	1-3600	120
`cell-size-reduction <reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an OAW-IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB.	1-55	0

Parameter	Description	Range	Default
	NOTE: This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's Tx power to match its new Rx power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.		
`csa-count <count>`	Configures the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.	0-10	2
`csd-override`	Most transmissions to HT stations are sent through multiple antennas using CSD. When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. This option is disabled by default, and should only be enabled under the supervision of Alcatel-Lucent technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). **NOTE:** Enabling this feature can reduce overall throughput rates.	—	—

Parameter	Description	Range	Default
`disable-arm-wids-functions`	By default, WIDS protection is on dynamic mode. If an OAW-IAP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. When **disable-arm-wids-functions** is on, the OAW-IAP will stop process frames for WIDS purposes regardless of whether the OAW-IAP is heavily loaded or not. The WIDS functionality will not take effect. When **disable-arm-wids-functions** is off, the OAW-IAP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. The WIDS functionality will always take effect.	Dynamic, off, on	Dynamic
`dot11h`	Allows the OAW-IAP to advertise its 802.11d (country information) and 802.11h TPC capabilities.	—	Disabled
`error-rate-threshold <percent>`	Configures the minimum percentage of errors in the channel that triggers a channel change.	0-100	70
`error-rate-wait-time <secs>`	Configures the time that the error rate has to sustain to trigger a channel change. The error rate must be equal to or more than the error rate threshold for the duration of this time period to trigger a channel change.	1-3600	90
`honor-40MHZ-intolerance-disable`	When this parameter is set, the radio will still use the 40 MHz channels even if the 40 MHz intolerance indication is received from another OAW-IAP or station.	—	Disabled
`ideal-coverage-index`	Specifies the ideal coverage index that an OAW-IAP tries to achieve on its channel. The denser the OAW-IAP deployment, the lower this value should be.	2-20	10

Parameter	Description	Range	Default
`interference-immunity <level>`	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: ■ Level 0— no ANI adaptation. ■ Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4— Level 3 settings, and FIR immunity. At this level, the OAW-IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5— The OAW-IAP completely disables PHY error reporting, improving performance by eliminating the time the OAW-IAP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the OAW-IAP to lose a small amount of range.	0-5	2
`legacy-mode`	Enables the OAW-IAPs to run the radio in non-802.11n mode.	—	Disabled

Parameter	Description	Range	Default
`max-distance <count>`	Configures the maximum distance between a client and an OAW-IAP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies the default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.	0-100000	0
`max-tx-power <power>`	Configures the maximum transmit power value for the 5 GHz radio profile.	3-max	18 dBm
`min-tx-power <power>`	Configures the minimum transmit power value for the 5 GHz radio profile.	3-max	12 dBm
`free-channel-index <idx>`	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	25
`scanning-disable`	Disables the radio from scanning other channels for RF Management and WIPS enforcement.	—	Disabled

Parameter	Description	Range	Default
`smart-antenna`	OAW-IAP335 access points support the smart antenna feature. This feature helps optimize the selection of antenna polarization values based on the data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the OAW-IAP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the OAW-IAP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using SU or MU transmit beamforming, and will use default polarization values for these clients.	—	Disabled
`spectrum-band <type>`	Allows you to specify the portion of the channel to monitor for 5 GHz configuration.	—	—
`spectrum-monitor`	Allows the OAW-IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring OAW-IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	—	—
`very-high-throughput-disable`	Disables VHT for clients connecting on the 5 GHz band.	—	—
`zone <zone>`	Configures a zone name for the radio profile. **NOTE:** This parameter cannot be configured on a default radio profile.	—	—

Parameter	Description	Range	Default
no…	Removes the current value for that parameter and return it to its default setting	—	—

Example

The following example configures the 5 GHz radio profile:

```
(Instant AP)(config)# rf dot11a-radio-profile
(Instant AP)(RF dot11a Radio Profile)# beacon-interval 100
(Instant AP)(RF dot11a Radio Profile)# legacy-mode
(Instant AP)(RF dot11a Radio Profile)# dot11h
(Instant AP)(RF dot11a Radio Profile)# interference-immunity 3
(Instant AP)(RF dot11a Radio Profile)# max-tx-power 33
(Instant AP)(RF dot11a Radio Profile)# min-tx-power 10
(Instant AP)(RF dot11a Radio Profile)# max-distance 600
(Instant AP)(RF dot11a Radio Profile)# csa-count 2
(Instant AP)(RF dot11a Radio Profile)# free-channel-index 40
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11a Radio Profile)# end
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The following parameters were added: ■ **backoff-time <secs>** ■ **channel-quality-aware-arm-disable** ■ **channel-quality-threshold** ■ **channel-quality-wait-time** ■ **error-rate-threshold <percent>** ■ **error-rate-wait-time <secs>** ■ **ideal-coverage-index <idx>** ■ **scanning-disable**
Alcatel-Lucent AOS-W Instant 8.6.0.0	The following parameter was added: ■ **bss-color**
Alcatel-Lucent AOS-W Instant 8.4.0.0	The default values for the following parameters were modified: ■ **max-distance** ■ **max-tx-power** ■ **min-tx-power** ■ **disable-arm-wids-functions** A new parameter was introduced: ■ **free-channel-index <idx>**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and RF dot11a Radio Profile configuration sub-mode

rf dot11a-secondary-radio-profile

```
rf dot11a-radio-profile <profile_name>
   40MHZ-intolerance
   backoff-time <secs>
   beacon-interval <interval>
   bss-color <0-63>
   cell-size-reduction <reduction>
   channel-quality-aware-arm-disable
   channel-quality-threshold
   channel-quality-wait-time
   csa-count <count>
   csd-override
   disable-arm-wids-functions
   dot11h
   error-rate-threshold <percent>
   error-rate-wait-time <secs>
   honor-40MHZ-intolerance-disable
   ideal-coverage-index <idx>
   interference-immunity <level>
   free-channel-index <idx>
   legacy-mode
   max-distance <count>
   max-tx-power <power>
   min-tx-power <power>
   scanning-disable
   smart-antenna
   spectrum-band <type>
   spectrum-monitor
   very-high-throughput-disable
   zone <zone>
   no…
```

Description

This command configures the secondary 5GHz radio profile for an OAW-IAP. This profile is only used when **split-5ghz-radio** is enabled on the access point. When **split-5ghz-radio** is enabled, the secondary radio profile is created based on the **rf-dot11a-radio-profile** settings.

The following ARM settings defined in this radio profile will take precedence over the settings in the ARM profile:

- **backoff-time <secs>**
- **channel-quality-aware-arm-disable**
- **channel-quality-threshold**
- **channel-quality-wait-time**
- **error-rate-threshold <percent>**
- **error-rate-wait-time <secs>**
- **ideal-coverage-index <idx>**
- **scanning-disable**

Parameter	Description	Range	Default
`rf dot11a-secondary-radio-profile`	Enables the 5 GHz RF configuration sub-mode	—	—

Parameter	Description	Range	Default
`40MHZ-intolerance`	Controls whether or not OAW-IAPs using this radio profile will advertise intolerance of 40 MHz operation.	—	Disabled
`backoff-time <secs>`	Configures the time when an OAW-IAP backs off after requesting a new channel or power.	10-3600	240
`beacon-interval <interval>`	Enter the Beacon period for the OAW-IAP in milliseconds. When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.	60-500	100
`bss-color <0-63>`	Configures BSS color for the BSSIDs broadcast by the radio. The value range is 0-63, where 0 configures automatic BSS coloring. The default value is 0.	0-63	0
`channel-quality-aware-arm-disable`	With this parameter, ARM ignores the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value.	—	Disabled
`channel-quality-threshold <thresh>`	Specifies the channel quality percentage below which ARM initiates a channel change.	0-100	70
`channel-quality-wait-time <secs>`	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. **NOTE:** If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.	1-3600	120
`cell-size-reduction <reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an OAW-IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB.	1-55	0

Parameter	Description	Range	Default
	NOTE: This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's Tx power to match its new Rx power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.		
`csa-count <count>`	Configures the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.	0-10	2
`csd-override`	Most transmissions to HT stations are sent through multiple antennas using CSD. When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. This option is disabled by default, and should only be enabled under the supervision of Alcatel-Lucent technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). **NOTE:** Enabling this feature can reduce overall throughput rates.	—	—

Parameter	Description	Range	Default
`disable-arm-wids-functions`	By default, WIDS protection is on dynamic mode. If an OAW-IAP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. When **disable-arm-wids-functions** is on, the OAW-IAP will stop process frames for WIDS purposes regardless of whether the OAW-IAP is heavily loaded or not. The WIDS functionality will not take effect. When **disable-arm-wids-functions** is off, the OAW-IAP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. The WIDS functionality will always take effect.	Dynamic, off, on	Dynamic
`dot11h`	Allows the OAW-IAP to advertise its 802.11d (country information) and 802.11h TPC capabilities.	—	Disabled
`error-rate-threshold <percent>`	Configures the minimum percentage of errors in the channel that triggers a channel change.	0-100	70
`error-rate-wait-time <secs>`	Configures the time that the error rate has to sustain to trigger a channel change. The error rate must be equal to or more than the error rate threshold for the duration of this time period to trigger a channel change.	1-3600	90
`honor-40MHZ-intolerance-disable`	When this parameter is set, the radio will still use the 40 MHz channels even if the 40 MHz intolerance indication is received from another OAW-IAP or station.	—	Disabled
`ideal-coverage-index`	Specifies the ideal coverage index that an OAW-IAP tries to achieve on its channel. The denser the OAW-IAP deployment, the lower this value should be.	2-20	10

Parameter	Description	Range	Default
`interference-immunity <level>`	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: ■ Level 0— no ANI adaptation. ■ Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ Level 3— Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4— Level 3 settings, and FIR immunity. At this level, the OAW-IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5— The OAW-IAP completely disables PHY error reporting, improving performance by eliminating the time the OAW-IAP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the OAW-IAP to lose a small amount of range.	0-5	2
`legacy-mode`	Enables the OAW-IAPs to run the radio in non-802.11n mode.	—	Disabled

Parameter	Description	Range	Default
`max-distance <count>`	Configures the maximum distance between a client and an OAW-IAP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies the default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.	0-100000	0
`max-tx-power <power>`	Configures the maximum transmit power value for the 5 GHz radio profile.	3-max	18 dBm
`min-tx-power <power>`	Configures the minimum transmit power value for the 5 GHz radio profile.	3-max	12 dBm
`free-channel-index <idx>`	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	25
`scanning-disable`	Disables the radio from scanning other channels for RF Management and WIPS enforcement.	—	Disabled

Parameter	Description	Range	Default
`smart-antenna`	OAW-IAP335 access points support the smart antenna feature. This feature helps optimize the selection of antenna polarization values based on the data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the OAW-IAP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the OAW-IAP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using SU or MU transmit beamforming, and will use default polarization values for these clients.	—	Disabled
`spectrum-band <type>`	Allows you to specify the portion of the channel to monitor for 5 GHz configuration.	—	—
`spectrum-monitor`	Allows the OAW-IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring OAW-IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	—	—
`very-high-throughput-disable`	Disables VHT for clients connecting on the 5 GHz band.	—	—
`zone <zone>`	Configures a zone name for the radio profile. **NOTE:** This parameter cannot be configured on a default radio profile.	—	—

Parameter	Description	Range	Default
no…	Removes the current value for that parameter and return it to its default setting	—	—

Example

The following example configures the 5 GHz radio profile:

```
(Instant AP)(config)# rf dot11a-secondary-radio-profile
(Instant AP)(RF dot11a Radio Profile)# beacon-interval 100
(Instant AP)(RF dot11a Radio Profile)# legacy-mode
(Instant AP)(RF dot11a Radio Profile)# dot11h
(Instant AP)(RF dot11a Radio Profile)# interference-immunity 3
(Instant AP)(RF dot11a Radio Profile)# max-tx-power 33
(Instant AP)(RF dot11a Radio Profile)# min-tx-power 10
(Instant AP)(RF dot11a Radio Profile)# max-distance 600
(Instant AP)(RF dot11a Radio Profile)# csa-count 2
(Instant AP)(RF dot11a Radio Profile)# free-channel-index 40
(Instant AP)(RF dot11a Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11a Radio Profile)# end
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The following parameters were added: ■ **backoff-time <secs>** ■ **channel-quality-aware-arm-disable** ■ **channel-quality-threshold** ■ **channel-quality-wait-time** ■ **error-rate-threshold <percent>** ■ **error-rate-wait-time <secs>** ■ **ideal-coverage-index <idx>** ■ **scanning-disable**
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-550 Series access points	Configuration mode and rf dot11a secondary radio profile configuration sub-mode

rf dot11g-radio-profile

```
rf dot11g-radio-profile [<profile_name>]
   40MHZ-intolerance
   backoff-time <secs>
   bss-color <0-63>
   beacon-interval <interval>
   cell-size-reduction <reduction>
   channel-quality-aware-arm-disable
   channel-quality-threshold
   channel-quality-wait-time
   csa-count <count>
   csd-override
   disable-arm-wids-functions
   dot11h
   error-rate-threshold <percent>
   error-rate-wait-time <secs>
   free-channel-index <idx>
   honor-40MHZ-intolerance-disable
   ideal-coverage-index <idx>
   interference-immunity <level>
   legacy-mode
   max-distance <count>
   max-tx-power <power>
   min-tx-power <power>
   scanning-disable
   smart-antenna
   spectrum-monitor
   zone <zone>
no…
```

Description

This command configures a 2.4.GHz or 802.11g radio profile for an OAW-IAP. The following ARM settings defined in this radio profile will take precedence over the settings in the ARM profile:

- **backoff-time <secs>**
- **channel-quality-aware-arm-disable**
- **channel-quality-threshold**
- **channel-quality-wait-time**
- **error-rate-threshold <percent>**
- **error-rate-wait-time <secs>**
- **ideal-coverage-index <idx>**
- **scanning-disable**

Parameter	Description	Range	Default
`rf dot11g-radio-profile`	Enables the 2.4 GHz RF configuration sub-mode	—	—
`40MHZ-intolerance`	Controls whether or not OAW-IAPs using this radio profile will advertise intolerance of 40 MHz operation.	—	Disabled

Parameter	Description	Range	Default
`backoff-time <secs>`	Configures the time when an OAW-IAP backs off after requesting a new channel or power.	10-3600	240
`bss-color <0-63>`	Configures BSS color for the BSSIDs broadcast by the radio. The value range is 0-63, where 0 configures automatic BSS coloring. The default value is 0.	0-63	0
`cell-size-reduction <reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an OAW-IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB. **NOTE:** This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's Tx power to match its new Rx power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.	1-55	0
`channel-quality-aware-arm-disable`	With this parameter, ARM ignores the internally calculated channel quality metric and initiates channel changes based on thresholds defined in the profile. ARM chooses the channel based on the calculated interference index value.	—	Disabled
`channel-quality-threshold <thresh>`	Specifies the channel quality percentage below which ARM initiates a channel change.	0-100	70

Parameter	Description	Range	Default
`channel-quality-wait-time <secs>`	Specifies the time that the channel quality is below the channel quality threshold value to initiate a channel change. **NOTE:** If current channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.	1-3600	120
`beacon-interval <interval>`	Enter the Beacon period for the OAW-IAP in milliseconds. When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.	60-500	100
`cell-size-reduction <reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an OAW-IAPs receive coverage area. It helps to minimize co-channel interference and optimizes channel reuse. The possible range of values for this feature are 0-55 dB. **NOTE:** This value should be changed if the network is experiencing performance issues. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's Tx power to match its new Rx power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.	1-55	0
`csa-count <count>`	Configures the number of channel switching announcements that must be sent before switching to a new channel. This allows associated clients to recover gracefully from a channel change.	0-10	2

Parameter	Description	Range	Default
`csd-override`	Most transmissions to HT stations are sent through multiple antennas using CSD. When you enable the CSD Override parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n CDD data. This option is disabled by default, and should only be enabled under the supervision of Alcatel-Lucent technical support. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). **NOTE:** Enabling this feature can reduce overall throughput rates.	—	—
`disable-arm-wids-functions`	By default, WIDS protection is on dynamic mode. If an OAW-IAP is heavily loaded with client traffic and the CPU utilization exceeds the threshold limit, the WIDS processing is suspended. This causes more CPU cycles to handle the client traffic. When the CPU utilization is within the the threshold limit, the WIDS processing is resumed. When **disable-arm-wids-functions** is on, the OAW-IAP will stop process frames for WIDS purposes regardless of whether the OAW-IAP is heavily loaded or not. The WIDS functionality will not take effect. When **disable-arm-wids-functions** is off, the OAW-IAP will always process frames for WIDS purposes even when it is heavily loaded with client traffic. The WIDS functionality will always take effect.	Dynamic, off, on	Dynamic
`dot11h`	Allows the OAW-IAP to advertise its 802.11d (country information) and 802.11h capabilities.	—	Disabled

Parameter	Description	Range	Default
`error-rate-threshold <percent>`	Configures the minimum percentage of errors in the channel that triggers a channel change.	0-100	70
`error-rate-wait-time <secs>`	Configures the time that the error rate has to sustain to trigger a channel change. The error rate must be equal to or more than the error rate threshold for the duration of this time period to trigger a channel change.	1-3600	90
`free-channel-index <idx>`	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	40
`honor-40MHZ-intolerance-disable`	When this parameter is set, the radio will still use the 40 MHz channels even if the 40 MHz intolerance indication is received from another OAW-IAP or station.	—	Disabled
`ideal-coverage-index`	Specifies the ideal coverage index that an OAW-IAP tries to achieve on its channel. The denser the OAW-IAP deployment, the lower this value should be.	2-20	10
`interference-immunity <level>`	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: ■ Level 0— no ANI adaptation. ■ Level 1— Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2— Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. l Level 3— Level 2 settings and	0-5	2

Parameter	Description	Range	Default
	weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4— Level 3 settings, and FIR immunity. At this level, the OAW-IAP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5— The OAW-IAP completely disables PHY error reporting, improving performance by eliminating the time the OAW-IAP would spend on PHY processing. **NOTE:** Increasing the immunity level makes the OAW-IAP to lose a small amount of range.		
`legacy-mode`	Enables the OAW-IAPs to run the radio in non-802.11n mode.	—	Disabled
`max-tx-power <power>`	Configures the maximum transmit power value for the 2.4 GHz radio profile.	3-max	9 dBm
`min-tx-power <power>`	Configures the minimum transmit power value for the 2.4 GHz radio profile.	3-max	6 dBm
`max-distance <count>`	Configures the maximum distance between a client and an OAW-IAP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies the default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16 km.	0-100000	0

Parameter	Description	Range	Default
scanning-disable	Disables the radio from scanning other channels for RF Management and WIPS enforcement.	—	Disabled
spectrum-monitor	Allows the OAW-IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring OAW-IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	—	Disabled
smart-antenna	OAW-IAP335 access points support the smart antenna feature. This feature helps optimize the selection of antenna polarization values based on the data collected from the training of polarization pattern combinations. This feature identifies the clients most likely to benefit from smart antenna polarization, based on the average RSSI of the received frames and the number of streams. This feature uses frame-based antenna training, which allows the OAW-IAP to cycle through training combinations and collect statistics without causing any impact on the client. At the end of the training sequence, the OAW-IAP selects the best antenna polarization based on these collected statistics. The smart antenna feature does not support optimized antenna polarization for clients using SU or MU transmit beamforming, and will use default polarization values for these clients.	—	disabled
zone <zone>	Configures a zone name for the radio profile. **NOTE:** This parameter cannot be configured on a default radio profile.	—	—
no...	Removes the configuration.	—	—

Example

The following example configures the 2.4 GHz radio profile:

```
(Instant AP)(config)# rf dot11g-radio-profile
(Instant AP)(RF dot11g Radio Profile)# beacon-interval 200
(Instant AP)(RF dot11g Radio Profile)# no legacy-mode
(Instant AP)(RF dot11g Radio Profile)# dot11h
(Instant AP)(RF dot11g Radio Profile)# interference-immunity 3
(Instant AP)(RF dot11g Radio Profile)# max-tx-power 33
(Instant AP)(RF dot11g Radio Profile)# min-tx-power 10
(Instant AP)(RF dot11g Radio Profile)# max-distance 600
(Instant AP)(RF dot11g Radio Profile)# csa-count 2
(Instant AP)(RF dot11g Radio Profile)# free-channel-index 40
(Instant AP)(RF dot11g Radio Profile)# spectrum-monitor
(Instant AP)(RF dot11g Radio Profile)# end
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The following parameters were added: ■ **backoff-time <secs>** ■ **channel-quality-aware-arm-disable** ■ **channel-quality-threshold** ■ **channel-quality-wait-time** ■ **error-rate-threshold <percent>** ■ **error-rate-wait-time <secs>** ■ **ideal-coverage-index <idx>** ■ **scanning-disable**
Alcatel-Lucent AOS-W Instant 8.6.0.0	The following parameter was added: ■ **bss-color**
Alcatel-Lucent AOS-W Instant 8.4.0.0	The default value for the following parameters have been updated to stay aligned with the AOS-W default values: ■ **max-distance** ■ **max-tx-power** ■ **min-tx-power** ■ **disable-arm-wids-functions** A new parameter was introduced: ■ **free-channel-index <idx>**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and RF dot11g Radio Profile sub-mode

rf-band

```
rf-band {2.4| 5.0| all}
```

Description

This command configures the RF band for an OAW-IAP.

Parameter	Description	Range	Default
`rf-band {2.4| 5| all}`	Configures a RF band for an OAW-IAP. You can configure any of the following options: ■ 2.4 - For 2.4 GHz band or 802.11g configuration ■ 5 - For 5 GHz and 802.11a configuration ■ all - For a mixed configuration of 2.4.GHz and 5 GHz. If you do not specify any value, by default both 5 GHz and 2.4 GHz bands are selected.	2.4, 5.0, all	all

Example

The following example configures the 5 GHz RF band for an OAW-IAP.

```
(Instant AP)(config)# rf-band 5
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

rf-zone

```
rf-zone <zone>
no…
```

Description

This command configures the RF zone for an OAW-IAP.

Parameter	Description	Range	Default
`<zone>`	Configures the RF zone and maps the RF zone to a radio profile.	—	—
`no`	Removes the RF zone configuration.	—	—

Example

The following example configures the RF zone of a guest SSID.

```
(Instant AP)# rf-zone guest
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged Exec mode

routing-profile

```
routing-profile
   route <destination> <mask> <gateway> {<metric>}
   no…
no routing profile
```

Description

This command configures a routing profile for a specific destination address or destination subnet.

Parameter	Description	Range	Default
`routing-profile <profile>`	Creates a routing profile for routing traffic into a specific destination address or destination subnet.	—	—
`route`	Configures route parameters.	—	—
`<destination>`	Configures the destination network that is reachable through the VPN tunnel.	—	—
`<mask>`	Specify the subnet mask of network that is reachable through the VPN tunnel.	—	—
`<gateway>`	Specify the gateway to which traffic must be routed. This IP address must be the switch IP address on which the VPN connection is terminated.	—	—
`<metric>`	This is an optional field and is configures a metric for the datapath route from source to destination. The default metric value is 15.	—	—
`no…`	Removes configuration settings for parameters under the **routing-profile** command.	—	—
`no routing-profile`	Removes the routing profile configuration.	—	—

Example

The following example configures a routing profile:

```
(Instant AP)(config)# routing-profile
(Instant AP)(Routing-profile)# route 192.0.1.0 255.255.255.0 192.0.2.0 15
(Instant AP)(Routing-profile)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and routing profile configuration sub-mode.

rrm-ie-profile

```
rrm-ie-profile <profile-name>
   country-ie-disable
   enabled-capabilities-ie-disable
   no
```

Description

This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled. All IEs are sent by default.

Parameter	Description
`country-ie-disable`	The AP will not advertise the country information element in beacon and probe responses.
`enabled-capabilities-ie-disable`	The AP will not advertise the enabled capabilities in beacon and probe responses.
`no ...`	Disables the transmission of an IE in this profile.

Example

The following command prevents the AP from advertising the country IE:

```
(Instant AP)(config) #wlan rrm-ie-profile default
(Instant AP)(RRM IE Profile "default") #country-ie-disabled
```

Command History

Release	Description
AOS-W Instant 8.6.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Configuration mode.

sesimagotag-esl-channel

```
sesimagotag-esl-channel <channel>
```

Description

This command is used to configure the static channel number of the ESL radio on an OAW-IAP.

Parameter	Description	Range	Default
`sesimagotag-esl-channel <channel>`	Configures the static channel number of the ESL radio.	0–10	—

Example

The following example configures a static ESL radio channel number:

```
(Instant AP)# sesimagotag-esl-channel 6
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP303H, OAW-IAP304, OAW-IAP305, OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-IAP334, and OAW-IAP335	Privileged EXEC mode.

sesimagotag-esl-profile

```
sesimagotag-esl-profile
   sesimagotag-esl-server <name>
   sesimagotag-esl-channel <channel>
   sesimagotag-esl-serverip <addr>
no...
```

Description

This command is used to configure SES-imagotag's Electronic Shelf Label system details.

Parameter	Description	Range	Default
`sesimagotag-esl-server <name>`	Sets the FQDN of SES-imagotag ESL Server. Configured server name takes priority over configured IP address of SES-imagotag ESL Server. If server name is not configured, IP address of SES-imagotag Server takes effect.	—	—
`sesimagotag-esl-serverip <addr>`	Sets the IP Address of SES-imagotag ESL Server. Adding server IP addresses allows bulk management and control of multiple servers at the same time.	—	—
`sesimagotag-esl-channel <channel>`	Sets the channel of SES-imagotag ESL Radio. **NOTE:** There are 11 pre-defined, independent radio channels that you can configure. The recommended channels are 3, 5, 8, 9, and 10 as they connect faster. These channels do not correspond to standard 802.11 channels.	0–10	—
`no`	Removes the configuration.	—	—

Example

The following example shows how to configure SES-imagotag:

```
(Instant AP)(config) # sesimagotag-esl-profile
(Instant AP)(sesimagotag-esl-profile) # sesimagotag-esl-serverip 10.62.39.210
(Instant AP)(sesimagotag-esl-profile) # sesimagotag-esl-channel 9
(Instant AP)(sesimagotag-esl-profile) # end
```

Command History

Release	Modification
AOS-W Instant 8.6.0.0	The **sesimagotag-esl-server <name>** command was introduced.
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-AP303H, OAW-IAP304, OAW-IAP305, OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-IAP334, OAW-IAP335 OAW-AP-344, OAW-AP-345, OAW-AP514, and OAW-AP515	Configuration mode and sesimagotag-esl-profile sub configuration mode.

show 1xcert

```
show 1xcert
```

Description

This command displays the details about the external server certificate, which is used by the OAW-IAP for client authentication.

Example

The following example shows the output of **show 1xcert** command:

```
Default Server Certificate:
Release       :3
Serial Number :01:DA:52
Issuer        :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA
Subject       :0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com,
OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Doma
                in Control Validated - QuickSSL(R) Premium, CN=securelogin.arubanetworks.com
Issued On     :2011-05-11 01:22:10
Expires On    :2017-08-11 04:40:59
Signed Using  :SHA1
RSA Key size  :2048 bits
```

The output of this command describes details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the certificates uploaded to the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show aaa

```
show aaa
  dns-query-interval
  fqdn-server-names
  radius modifier <radius_modifier>
```

Description

This command displays the AAA profile details. Use this command to view the time interval range set for a dns query, FQDN server details, and the RADIUS modifier profiles.

Parameter	Description	Range	Default
`dns-query-interval <minutes>`	Displays the time interval at which the query must be sent. The interval is ranged in minutes.	0–60 minutes	15
`fqdn-server-names`	Displays the host name of a RADIUS server profile, IP address, and mapping details.	—	—
`radius modifier <radius_modifier>`	Displays a list of RADIUS modifier profiles.	—	—

Example

The following example shows the output of **show aaa dns-query-interval** command.

```
20:4c:03:24:89:18# show aaa dns-query-interval
DNS QUERY Interval:15
```

The following example shows the output of **show aaa fqdn-server-names** command.

```
20:4c:03:24:89:18# show aaa fqdn-server-names
Auth Server FQDN names
----------------------
FQDN  IP Address  IPv6 Address  Refcount
----  ----------  ------------  --------
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show about

```
show about
```

Description

This command displays information about AOS-W Instant version, build time and OAW-IAP model.

Example

The **show about** command displays the Build Time, OAW-IAP model number, the Instant version, website address of organization, and Copyright information. The following example shows the **show about** command output:

```
Name                    :Alcatel-Lucent Operating System-Wireless
Type                    :OAW-AP105
Build Time              :2015-08-05 02:11:11 PDT
Version                 :6.4.3.1-4.2.0.0_51112
Website                 :http://enterprise.alcatel-lucent.com/
Legal                   :All Rights Reserved (c) 2005-2015, Alcatel-Lucent.
Cloud Activation Key:
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show access-rule

```
show access-rule [<name>]
```

Description

This command displays the details of access rules configured for the wired or wireless clients associated with an OAW-IAP.

Parameter	Description	Range	Default
`<name>`	Displays the access rule configuration details based the name specified for this parameter.	—	—

Example

The following example shows the output displayed for the **show access-rule** command:

```
Access Rules
------------
Dest IP  Dest Mask  Eth Type  Dest Match  Protocol (id:sport:eport)  Application
-------  ---------  --------  ----------  -------------------------  -----------
any      any        IPv4/6    match       sips
any      any        IPv4/6    match       https
any      any        IPv4/6    match       any

Action  Log  TOS  802.1P  Blacklist  App Throttle (Up:Down)  Mirror  DisScan
------  ---  ---  ------  ---------  ----------------------  ------  -------
permit
permit
permit

time-range  CustomApp
---------   ---------

Vlan Id           :0
ACL Captive Portal:disable
ACL ECP Profile   :default
CALEA             :disable
Redirect Blocked HTTPS Traffic  :disable
DPI error page URL:
Bandwidth Limit   :downstream disable upstream disable
```

The output of this command displays information about the access rule parameters configured for a specific wired or wireless profile. It indicates whether a particular type of traffic is allowed to a particular destination, and the service and protocol in use and if options such as logging and prioritizing traffic are enabled when the rule is triggered. If the DPI access rules are configured, it displays the list of rules configured to allow or deny access to certain applications, application categories, web categories, and websites based on their reputation score.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of this command was modified to include the **CustomApp** column.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show access-rule-all

```
show access-rule-all
```

Description

This command displays the details of the access rules configured for all wired and wireless profiles on the OAW-IAP.

Example

The following example shows the partial output of the **show access-rule-all** command:

```
Access Rule Name :default_wired_port_profile
In Use           :Yes
Access Rules
------------
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport)  Application
-------  ---------  ----------  -------------------------  -----------
any      any        match       any
masterip 0.0.0.0    match       http
masterip 0.0.0.0    match       6:4343:4343
any       any       match       dhcp

Action  Log  TOS  802.1P  Blacklist  App Throttle (Up:Down)  Mirror  DisScan
------  ---  ---  ------  ---------  ----------------------  ------  -------
permit
permit
permit

Vlan Id           :0
ACL Captive Portal:disable
ACL ECP Profile   :default
CALEA             :disable
Bandwidth Limit   :downstream disable upstream disable
Access Rule Name :NewRole17
In Use           :No
Access Rules
------------
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport)  Application
-------  ---------  ----------  -------------------------  -----------
10.17.88.188  255.255.255.255  match       http
10.17.88.188  255.255.255.255  match       6:4343:4343
any           any              match       dhcp
any           any              match       dns

Action  Log  TOS  802.1P  Blacklist  App Throttle (Up:Down)  Mirror  DisScan
------  ---  ---  ------  ---------  ----------------------  ------  -------
permit
permit
permit
permit

Vlan Id           :0
ACL Captive Portal:disable
ACL ECP Profile   :default
CALEA             :disable
Bandwidth Limit   :downstream disable upstream disable
Access Rule Name :NewRole18
In Use           :No
```

The output of this command includes the following parameters:

Parameter	Description	Range	Default
`Access Rule Name`	Displays the name of the access rule.	—	—
`In use`	Indicates if the access rules are in use.	—	—
`Access Rules`	Displays the access rules parameter for each rule configured for the SSID or Wired profile users.	—	—
`VLAN Id`	Indicates the VLAN ID associated with the SSID or wired profile access rules.	—	—
`ACL Captive Portal`	Indicates if the ACL rules are applicable to the captive portal users.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show acl

```
show acl [domains]
```

Description

This command displays the ACL configuration details.

Parameter	Description	Range	Default
`domains`	Displays the domains configured with an ACL.	—	—

Example

The following example shows the output of the **show acl** command:

```
(Instant AP)# show acl
role-domain
-----------
role-domain  inused
-----------  ------
d8:c7:c8:c4:42:98#
```

The output of this command displays information about the role-domain.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show activate status

```
show activate status
```

Description

This command displays the status of the Alcatel-Lucent Activate cloud-based services.

Example

The following example shows the output displayed for the **show activate status** command:

```
IAP MAC Address          :38:17:c3:c0:58:06
IAP Serial Number        :CNFDK5148D
Cloud Activation Key     :II6JSV1X
Activate Server          :device.arubanetworks.com
Activate Status          :admin-disabled-by-dhcp-option
Provision interval       :0 minutes
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show airgroup

```
show airgroup {blocked-queries [dlna| mdns]| blocked-service-id [dlna| mdns]| cache {<MAC-address> |
entries [dlna| mdns]} | cppm {auth  server [coa-capable | non-coa-only] | entries | query-interval |
server}| cppm-entry <MAC-address> | debug statistics| internal-state statistics | servers
[dlna| mdns| verbose]|
status | swarm-info| users [dlna| mdns| verbose]}
```

Description

This command displays the AirGroup configuration details for an OAW-IAP client.

Parameter	Description	Range	Default
`blocked-queries [dlna |mdns]`	Displays blocked queries if any.	—	—
`blocked-service-id [dlna| mdns]`	Displays blocked services and service IDs if any.	—	—
`cache <MAC-address> cache entries [dlna| mdns]`	Displays AirGroup cache details for a specific OAW-IAP or for the OAW-IAP clients in a cluster.	—	—
`cppm {auth server [coa-capable	non-coa-only] entries	query-interval	server}`	Displays ClearPass Policy Manager server details associated with AirGroup configuration.	—	—
`cppm-entry <MAC-address>`	Displays ClearPass Policy Manager server details for an AirGroup client.	—	—
`debug statistics`	Displays debug statistics for AirGroup enabled OAW-IAPs.	—	—
`internal-state statistics`	Displays statistical details of queries and responses, and RADIUS client messages.	—	—
`servers [dlna| mdns| verbose]`	Displays AirGroup server details.	—	—
`status`	Indicates the AirGroup feature activation status.	—	—

Parameter	Description	Range	Default
`swarm-info`	Displays information about the AirGroup cluster.	—	—
`users [dlna| mdns| verbose]`	Displays the list of AirGroup users.	—	—

Example

Example outputs for some of the **show airgroup** commands are as follows:

show airgroup blocked-queries

The **show airgroup blocked-queries** command output displays the blocked queries if any:

```
AirGroup dropped Query IDs
--------------------------
Service ID  #query-hits
----------  -----------
Num dropped Query IDs:0
```

show airgroup blocked-service-id

The **show airgroup blocked-service-id** command output displays the blocked AirGroup service IDs if any:

```
AirGroup Blocked Service IDs
----------------------------
Origin  Service ID  #response-hits
------  ----------  --------------
Num Blocked Service-ID:0
```

show airgroup cache entries

The following output is displayed for the **show airgroup cache entries** command:

```
Cache Entries
-------------
Name                                           Type        Class  TTL   Origin        Expiry
 Last Update
----                                           ----        -----  ---   ------        ------
 -----------
_airplay._tcp.local                            PTR         IN     4500  10.16.94.236  3696.00
 Tue May 13 19:32:11 2014
_raop._tcp.local                               PTR         IN     4500  10.16.94.236  3794.31
 Tue May 13 19:32:11 2014
BLR-DPARASAR-T4._airplay._tcp.local            SRV/NBSTAT  IN     120   10.16.94.236  311.38
 Tue May 13 19:32:11 2014
2577037A8680@BLR-DPARASAR-T4._raop._tcp.local  SRV/NBSTAT  IN     120   10.16.94.236  134.14
 Tue May 13 19:32:11 2014
BLR-DPARASAR-T430S.local                       A           IN     120   10.16.94.236  255.07
 Tue May 13 19:32:11 2014
BLR-DPARASAR-T430S.local                       AAAA        IN     120   10.16.94.236  393.69
 Tue May 13 19:32:11 2014
BLR-DPARASAR-T4._airplay._tcp.local            TXT         IN     4500  10.16.94.236  3784.51
 Tue May 13 19:32:11 2014
2577037A8680@BLR-DPARASAR-T4._raop._tcp.local  TXT         IN     4500  10.16.94.236  3840.38
 Tue May 13 19:32:11 2014
urn:schemas-upnp-org:device:MediaRenderer:1    N/A         N/A    1800  10.16.94.236  N/A
 Tue May 13 19:33:51 2014
```

The output of this command includes the following information:

Column	Description
Name	Indicates the name of AirGroup server.
Type	Indicates the AirGroup model.
Class	Indicates the class of the mDNS record.
TTL	Indicates the duration after which the cache entries expire.
Origin	Indicates the origin IP address of the cache entries.
Expiry	Indicates the expiration details.
Last Update	Indicates when the entries were last updated.

show airgroup cppm auth server non-coa-only

The following output is displayed for the **show airgroup cppm auth server non-coa-only** command:

```
All Airgroup Non-CoA-only Servers known to MDNS
-----------------------------------------------
Server   IP-Address  Port  timeout  rfc3576   rfc3576-only  rfc3576-port
------   ----------  ----  -------  -------   ------------  ------------
test     192.0.2.0    1812  5        Disabled  Disabled      5999
test123  192.0.2.1    1812  5        Disabled  Disabled      5999
```

show airgroup cppm auth server coa-capable

The following output is displayed for the **show airgroup cppm auth server coa-capable** command:

```
All Airgroup CoA-capable Servers known to MDNS
----------------------------------------------
Server   IP-Address  Port  timeout  rfc3576  rfc3576-only  rfc3576-port
------   ----------  ----  -------  -------  ------------  ------------
server1  192.0.1.1    1812  5        Enabled  Enabled       5999
```

show airgroup cppm server

The following output is displayed for the **show airgroup cppm server** command:

```
CPPM Servers
------------
Server   IP-Address  Port  timeout  rfc3576   rfc3576-only  rfc3576-port
------   ----------  ----  -------  -------   ------------  ------------
test     192.0.2.0   1812  5        Disabled  Disabled      5999
test123  192.0.2.1   1812  5        Disabled  Disabled      5999
```

The output of these commands provide the following information:

Column	Description
Server	Indicates the name of the ClearPass Policy Manager server.
IP address	Indicates the IP address of the ClearPass Policy Manager server.
Port	Indicates the authorization port number of the ClearPass Policy Manager server.
timeout	Indicates timeout value in seconds for one RADIUS request.
rfc3576	Indicates if the OAW-IAPs are configured to process RFC 3576-compliant CoA.

Column	Description
`rfc3576-only`	Indicates if OAW-IAPs are configured to be RFC 3576 compliant only.
`rfc3576-port`	Indicates the port number used for sending AirGroup CoA.

show airgroup cppm entries

The following output is displayed for the **show airgroup cppm entries** command:

```
swarm id = fc6520ad018ee6eb13bdc6b985e0fe6361bd37f7d25212a77e
--------------------------------------------------------------------
ap id = d8:c7:c8:c4:42:98       ap ip = 192.0.2.0    update no = 0
-------------------------------------
Device device-owner shared location-id AP-name shared location-id AP-FQLN
------  ------------  --------------------------  --------------------------
shared location-id AP-group shared user-list shared role-list
------------------  ----------------  ----------------
Num CPPM Entries:0
```

The output of this command provides the following information:

Column	Description
`swarm id`	Indicates the cluster ID of the OAW-IAP.
`ap id`	Displays the MAC address of the OAW-IAP on which AirGroup is configured.
`ap ip`	Displays the IP address of the OAW-IAP on which AirGroup is configured.
`update no`	Indicates the number of configuration updates if any.
`Device`	Indicates the device for which AirGroup is configured.
`device-owner`	Indicates the device owner's identity.
`shared location-id AP-name`	Indicates the shared location ID associated with the OAW-IAP name.
`shared location-id AP-FQLN`	Indicates the shared location ID associated with the FQDN of the OAW-IAP.
`shared location-id AP-group`	Indicates the shared location ID associated with the OAW-IAP group.
`shared user-list`	Indicates the list of shared users.
`shared role-list`	Indicates the list of shared user roles.
`Num CPPM Entries`	Indicates the number of ClearPass Policy Manager entries.

show airgroup debug statistics

The following output is displayed for the **show airgroup debug statistics** command:

```
Airgroup slave status       :TRUE
Airgroup master status      :TRUE
Airgroup multi swarm status :TRUE
status value                :0x7f
My ip address               :192.168.10.251
My VC address               :192.168.10.2
Peer VC address             :192.168.10.2
Peer VC address            :192.168.20.2
Peer VC address            :192.168.30.2
Peer VC address            :192.168.40.2
Peer VC address            :0.0.0.0
Peer VC address            :0.0.0.0
Peer VC address            :0.0.0.0
Peer VC address            :0.0.0.0
AirGroup Debug Statistics
--------------------------
Key                                  Value
---                                  -----
network cache init counter           2(2)
mdns apdb init counter               7(7)
mdns apdb destroy counter            1(1)
user timed out                       1(1)
airgroup restore count               1(1)
mdns mac move counter                4(4)
mdns master to vc hello rx           2060(2060)
mdns slave to slave hello rx         8240(8240)
mdns ap to ap mac sync resp rx       57(57)
mdns master to vc mac req rx         1580(1580)
swarm update counter rx              1(1)
mdns recieved valid swarm packet     11978(11978)
mdns recieved dlna pkt from device   177704(177704)
mdns partial hello tx                2059(2059)
mdns ap update tx                    80(80)
mdns master to vc mac sync resp tx   232(232)
mdns ap to ap mac sync resp tx       1348(1348)
dropped init not done tx             6(6)
master to vc hello tx                2059(2059)
master to my swarm hello tx          2354(2354)
mdns ap to swarm hello tx            4118(4118)
mdns slave to slave mac sync req tx  57(57)
mdns total pkt sent to asap tx       112563(112563)
hello ap verification fail count     1(1)
```

The output of this command provides the following information:

Column	Description
`Airgroup slave status`	Indicates the AirGroup configuration status on the slave OAW-IAP.
`Airgroup master status`	Indicates the AirGroup configuration status on the slave OAW-IAP.
`Airgroup multi swarm status`	Indicates the status of the inter cluster mobility.
`status value`	Indicates the status value.
`Key and Value`	Displays details of AirGroup counters.

show airgroup internal-state statistics

The following output is displayed for the **show airgroup internal-state statistics** command:

```
Time: Fri May 16 09:30:22 2014
RADIUS Client Messages
----------------------
Type                         Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----                         --------------------  ----------  --------------------  ----------
Auth Req/Resp                0                     0           0                     0
RFC3576                      N/A                   N/A         0                     0
CPPM Device-Entry Added      N/A                   N/A         0                     0
CPPM Device-Entry Deleted    N/A                   N/A         0                     0
```

```
Internal MDNS Statistics
------------------------
Functionality                     Hit Count Since Last Read  Hit Count Total  Average Time in
microsec (since last read)  Average Time in microsec (alltime)
-------------                     -------------------------  ---------------  ---------------
---------------------------  ----------------------------------
Response - Cache Update           0                          0                0
                            0
Response                          0                          0                0
                            0
Query - prepare records + Policy  0                          0                0
                            0
Query - Policy                    0                          0                0
                            0
Query - resp pkt gen & send       0                          0                0
                            0
Query - Response packet send      0                          0                0
                            0
Query                             0                          0                0
                            0
Internal DLNA Statistics
------------------------
Functionality                     Hit Count Since Last Read  Hit Count Total  Average Time in
microsec (since last read)  Average Time in microsec (alltime)
-------------                     -------------------------  ---------------  ---------------
---------------------------  ----------------------------------
Response - Cache Update           0                          0                0
                            0
Response                          0                          0                0
                            0
Query - prepare records + Policy  0                          0                0
                            0
Query - Policy                    0                          0                0
                            0
Query - resp pkt gen & send       0                          0                0
                            0
Query - Response packet send      0                          0                0
                            0
Query                             0                          0                0
                            0
```

The output of this command displays information about queries and responses, and RADIUS client messages.

show airgroup servers

The following output is displayed for the **show airgroup servers** command:

```
AirGroup Servers
----------------
MAC  IP  Type  Host Name  Service  VLAN  Wired/Wireless  Role  Group  Username  AP-Name
---  --  ----  ---------  -------  ----  --------------  ----  -----  --------  -------
Num Servers: 0, Max Servers: 80.
```

The output of this command provides the following information:

Column	Description
MAC	Indicates the MAC address of the AirGroup servers.
IP	Indicates the IP address of the AirGroup servers.

Column	Description
`Type`	Indicates the type of server.
`Hostname`	Indicates the hostname of the AirGroup servers.
`Service`	Indicates if AirGroup services such as AirPlay or AirPrint are configured.
`VLAN`	Displays VLAN details of the AirGroup servers.
`Wired/Wireless`	Displays if the AirGroup server is connected to a wired or wireless interface.
`Role`	Displays the user role details.
`Group`	Displays the server group.
`Username`	Displays the username details.
`AP-name`	Displays the name of the OAW-IAP.
`Num servers`	Displays the total number of servers.
`Max Servers`	Displays the maximum number of servers that are supported.

show airgroup status

The following output is displayed for the **show airgroup status** command:

```
AirGroup Feature
----------------
Status
------
Disabled
AirGroup- MDNS Feature
----------------------
Status
------
Disabled
AirGroup- DLNA Feature
----------------------
Status
------
Disabled
AirGroup Multi Swarm
--------------------
Status
------
Disabled
AirGroup Guest Multicast
------------------------
Status
------
Disabled
CPPM Parameters
---------------
Parameter                   Value
---------                   -----
CPPM Enforce Registration   Disabled
CPPM Server query interval  10 Hours
CPPM Server dead time       100 Seconds
AirGroup Service Information
----------------------------
Service     Status
```

```
-------      ------
airplay      Disabled
airprint     Disabled
itunes       Disabled
remotemgmt   Disabled
sharing      Disabled
Chromecast   Disabled
DLNA Media   Disabled
DLNA Print   Disabled
allowall     Disabled
```

The output of this command provides the following information:

Column	Description
`Airgroup feature status`	Indicates if the AirGroup feature such as DLNA or MDNS support is enabled.
`AirGroup Multi Swarm status`	Indicates if the inter cluster mobility is enabled.
`AirGroup Guest Multicast`	Indicates if a guest VLAN is used for Bonjour services.
`CPPM Parameters`	Displays ClearPass Policy Manager configuration parameters associated with the AirGroup configuration.
`AirGroup Service Information`	Displays information about the status of the AirGroup services configuration.

show airgroup swarm-info

The following output is displayed for **show airgroup swarm-info** command:

```
AirGroup Swarm info
--------------------
Swarm id
--------
ef7501af01cd098223100f6d02733552765515ffcd7712c41c
AirGroup Swarm AP info
-----------------------
Ap MAC             Ap Name            Ap Ip          Update no
------             -------            -----          ---------
6c:f3:7f:c3:5c:12  6c:f3:7f:c3:5c:12  10.17.141.140  0x3
d8:c7:c8:cb:d3:b8  d8:c7:c8:cb:d3:b8  10.17.141.138  0x0
d8:c7:c8:cb:d3:9c  d8:c7:c8:cb:d3:9c  10.17.141.139  0x0
d8:c7:c8:cb:d4:20  d8:c7:c8:cb:d4:20  10.17.141.137  0x0

AirGroup Swarm AP's Client info
--------------------------------
Mac                Ip             Update no  Record Hash  APs Mac
---                --             ---------  -----------  -------
9c:20:7b:df:3e:8a  10.17.141.141  0x1        0x12cc1003   6c:f3:7f:c3:5c:12
```

The output of this command displays the AirGroup cluster information.

show airgroup users

The following output is displayed for the **show airgroup users** command:

```
AirGroup Users
--------------
MAC  IP  Host Name  VLAN  Wired/Wireless  Role  Username  AP-Mac  Query/Resp
---  --  ---------  ----  --------------  ----  --------  ------  ----------
Num Users:0
```

The output of this command provides the following information:

Column	Description
`MAC`	Indicates the MAC address of the AirGroup clients.
`IP`	Indicates the IP address of the AirGroup clients.
`Host Name`	Indicates the hostname of the AirGroup clients.
`VLAN`	Displays VLAN details of the AirGroup clients.
`Wired/Wireless`	Displays if the AirGroup user is connected to a wired or wireless interface.
`Role`	Indicates the AirGroup user role.
`Username`	Displays the username of the AirGroup user.
`AP-Mac`	Displays the MAC address of the OAW-IAP to which the user is connected.
`Query/Resp`	Displays information query and response details exchanged between the AirGroup user and the AirGroup server.
`Num Users`	Indicates the number of AirGroup users.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show airgroupservice

```
show airgroupservice [disallow {role [servers|users] | vlan [servers|users]}]
```

Description

This command displays the AirGroup service configured on an OAW-IAP.

Parameter	Description	Range	Default
`show airgroupservice`	Displays a summary of the configuration details for AirGroup services.	—	—
`disallow {role [servers|users] |vlan}`	Displays the user roles or VLANs that are restricted from accessing AirGroup services. When the access to AirGroup services is restricted, the clients that are assigned with a specific role or VLAN will not be able to use the AirGroup service.	—	—

Examples

The following output is displayed for the **show airgroupservice** command:

```
AirGroupService Details
-----------------------
Service     Description        status     Disallowed-Role  Disallowed-VLAN  ID
-------     -----------        ------     ---------------  ---------------  --
airplay     AirPlay            Disabled                                     _airp
     lay._tcp
_raop                   ._tcp
_appl                   etv-v2._tcp
airprint    AirPrint           Disabled                                     _ipp.
     _tcp
_pdl-                   datastream._tcp
_prin                   ter._tcp
_scan                   ner._tcp
_univ                   ersal._sub._ipp._tcp
_univ                   ersal._sub._ipps._tcp
_prin                   ter._sub._http._tcp
_http                   ._tcp
_http                   -alt._tcp
_ipp-                   tls._tcp
_fax-                   ipp._tcp
_riou                   sbprint._tcp
_cups                   ._sub._ipp._tcp
_cups                   ._sub._fax-ipp._tcp
_ica-                   networking._tcp
_ptp.                   _tcp
_cano                   n-bjnp1._tcp
_ipps                   ._tcp
_ica-                   networking2._tcp
itunes      iTunes             Disabled                                     _home
     -sharing._tcp
```

```
_appl                  e-mobdev._tcp
_daap                  ._tcp
_dacp                  ._tcp
remotemgmt  Remote management  Disabled                                   _ssh.
     _tcp
_sftp                  -ssh._tcp
_ftp.                  _tcp
_teln                  et._tcp
_rfb.                  _tcp
_net-                  assistant._tcp
AirGroupService Details
-----------------------
Service     Description         status    Disallowed-Role  Disallowed-VLAN  ID
-------     -----------         ------    ---------------  ---------------  --
sharing     Sharing             Disabled                                    _odi
     sk._tcp
_afp                  overtcp._tcp
_xgr                  id._tcp
Chromecast  Chromecast          Disabled                                    urn:
     dial-multiscreen-org:service:dial:1
urn:                  dial-multiscreen-org:device:dial:1
DLNA Media  Media               Disabled                                    urn:
     schemas-upnp-org:device:MediaServer:1
urn:                  schemas-upnp-org:device:MediaServer:2
urn:                  schemas-upnp-org:device:MediaServer:3
urn:                  schemas-upnp-org:device:MediaServer:4
urn:                  schemas-upnp-org:device:MediaRenderer:1
urn:                  schemas-upnp-org:device:MediaRenderer:2
urn:                  schemas-upnp-org:device:MediaRenderer:3
urn:                  schemas-upnp-org:device:MediaPlayer:1
DLNA Print  Print               Disabled                                    urn:
     schemas-upnp-org:device:Printer:1
urn:                  schemas-upnp-org:service:PrintBasic:1
urn:                  schemas-upnp-org:service:PrintEnhanced:1
allowall    Remaining-Services  Disabled
Num Services:10
Num Service-ID:49
```

The following example shows the partial output displayed for the **show airgroupservice disallow role** command:

```
airplay
-------
default_wired_port_profile
port
airprint
--------
default_wired_port_profile
port
```

The following example shows the partial output displayed for the **show airgroupservice disallow vlan** command:

```
airplay
-------
1
100
200
airprint
--------
1
100
200
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show airgroupservice-ids

```
show airgroupservice-ids <service>
```

Description

This command displays the AirGroup service IDs configured on an OAW-IAP for its AirGroup clients.

Parameter	Description	Range	Default
`service`	Indicates the name of the service and displays the service ID details of specified AirGroup service.	—	—

Examples

The following output is displayed for the **show airgroupservice-ids** command for the AirPlay service:

```
(Instant AP)# show airgroupservice-ids airplay
airplay
-------
Service ids
-----------
_airplay._tcp
_raop._tcp
_appletv-v2._tcp
```

The output of this command displays the service IDs associated with the AirGroupservice.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ale

```
show ale {config | stats | status}
```

Description

This command displays the ALE configuration details.

Parameter	Description	Range	Default
`config`	Displays the ALE configuration details.	—	—
`stats`	Displays the number of times a specific message type such as AppRF statistics, and uplink bandwidth report was sent to the ALE server.	—	—
`status`	Displays the status of ALE server.	—	—

Example

The following example shows the output of the **show ale config** command:

```
(Instant AP)# show ale config
ALE Config
----------
Type                 Value
----                 -----
ale-server           AleServer1
ale-report-interval  60
```

The output of this command displays the ALE server details and the reporting interval at which the Virtual Controller sends data to the ALE server.

The following example shows the output of the **show ale stats** command:

```
(Instant AP)# show ale stats
ALE Stats
---------
Type               Value
----               -----
VC package         0
RSSI package       0
APPRF package      0
URLv package       0
STATE package      0
STAT package       0
UPLINK BW package  0
Total              0
```

The following example shows the output of the **show ale status** command:

```
(Instant AP)# show ale status
ALE Status
----------
Type                     Value
----                     -----
ale login status         False
ale login status code
ale fail times           0
ale request state        Idle
```

The output of this command displays information about the ALE server status and data request status.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show alert global

```
show alert global [count]
```

Description

This command displays the list of client alerts for an OAW-IAP. The client alerts occur when clients are connected to the AOS-W Instant network. Alerts are generated when a client encounters problems while accessing or connecting to the OAW-IAP network.

Parameter	Description	Range	Default
`<count>`	Filters client alerts based on the specified number.	—	—

Example

The **show alerts global** command displays information about the clients for which alerts (if any) are generated. The following example shows the output for the **show alerts global** command.

```
Client Alerts
-------------
Timestamp  Type  MAC Address  Description  Access Point
---------  ----  -----------  -----------  ------------
10:45:42   5     80:86:f2:85:51:6f  11           rno04-api-2
10:54:15   5     bc:3b:af:3d:32:bf  11           rno04-api-4
```

The output of this command provides the following information:

Column	Description	Range	Default
`Timestamp`	Displays the time at which the client alert was recorded.	—	—
`Type`	Displays the numeric value to indicate the type of event that triggered the alert. For more information, see .	—	—
`MAC Address`	Displays the MAC address of the client that caused the alert.	—	—
`Description`	Displays the description code for the alert. For example, Type 5 and Description 11 indicates that the DHCP request has timed out and the client did not receive a response to its DHCP request in time. For more information, see .	—	—
`Access Point`	Displays the IP address of the OAW-IAP to which the client is connected.	—	—

Table 14: *Client Alert —Type and Description Codes*

Type code	Description Code	Detailed Description
1	1	**Internal error**

Table 14: *Client Alert —Type and Description Codes*

Type code	Description Code	Detailed Description
		The OAW-IAP has encountered an internal error for this client.
	2	**Unknown SSID in association request.** The OAW-IAP cannot allow this client to associate because the association request received contains an unknown SSID.
	3	**Mismatched authentication/encryption setting** The OAW-IAP cannot allow this client to associate because its authentication or encryption settings do not match the configuration of the OAW-IAP.
	4	**Unsupported 802.11 rate** The OAW-IAP cannot allow this client to associate because it does not support the 802.11 rate requested by this client.
	5	**Maximum capacity reached on OAW-IAP** The OAW-IAP has reached maximum capacity and cannot accommodate any more clients.
2	6	**Invalid MAC Address** The OAW-IAP cannot authenticate this client because its MAC address is not valid.
3	7	**Client blocked due to repeated authentication failures** The OAW-IAP is temporarily blocking the 802.1x authentication request from this client because the credentials provided have been rejected by the RADIUS server too many times.
	8	**Authentication server timeout** The OAW-IAP cannot authenticate this client using 802.1x because the RADIUS server did not respond to the authentication request. If the OAW-IAP is using the internal RADIUS server, recommend checking the related configuration as well as the installed certificate and passphrase.
	9	**RADIUS server authentication failure** The OAW-IAP cannot authenticate this client using 802.1x because the RADIUS server rejected the authentication credentials provided by the client.
4	10	**Integrity check failure in encrypted message** The OAW-IAP cannot receive data from this client because the integrity check of the received MIC has failed. Recommend checking the encryption setting on the client and on the OAW-IAP.
5	11	**DHCP request timed out** This client did not receive a response to its DHCP request in time. Recommend checking the status of the DHCP server in the network.
10	12	**Wrong Client VLAN** VLAN mismatch between the OAW-IAP and upstream device. Upstream device can be upstream switch or RADIUS server.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show alg

```
show alg
```

Description

This command displays the ALG protocol information configured on an OAW-IAP. An application-level gateway consists of a security component that augments a firewall or NAT used in a network.

Example

The following output is displayed for the **show alg** command:

```
Current ALG
-----------
ALG     Status
---     ------
sccp    Enabled
sip     Enabled
ua      Enabled
vocera  Enabled
```

The output of this command displays if the ALG protocols such as SCCP, SIP, Alcatel-Lucent NOE (UA), and VOCERA are enabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show allowed-aps

```
show allowed-aps
```

Description

This command displays the list of OAW-IAPs that are allowed to join the OAW-IAP cluster.

Example

The following example shows the output of the **show allowed-aps** command:

```
Allow New APs  :enable
AP Whitelist
------------
MAC Address
-----------
d8:c7:c8:cb:d4:20
d8:c7:c8:cb:d3:98
d8:c7:c8:cb:d3:b4
d8:c7:c8:cb:d3:d4
```

The output of this command provides the following information:

Column	Description	Range	Default
`Allow New APs`	Indicates if the new OAW-IAPs are allowed to join the network.	—	—
`MAC Address`	Displays the MAC address of the OAW-IAPs that are allowed to join the network.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show a-max-clients

```
show a-max-clients [<ssid_profile>]
```

Description

This command displays the maximum number of clients allowed for an SSID profile on a 5 GHz radio channel.

Parameter	Description	Range	Default
`<ssid_profile>`	Denotes the SSID profile for which the maximum clients limit is set.	—	—

Example

The following **show a-max-clients** command output displays the maximum number of clients allowed to connect to the each SSID:

```
(Instant AP)# show a-max-clients
test1 : 30
test2 : 200
test3 : 64
```

The following **show a-max-clients <ssid_profile>** command output displays the maximum number of clients allowed to connect to the **test1** SSID:

```
(Instant AP)# show a-max-clients test1
a-max-clients: 30
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

show all monitor

```
show all monitor active-laser-beams
```

Description

This command shows information for Alcatel-Lucent AOS-W Instant AMs.

Parameter	Description	Range	Default
`active-laser-beams`	Show active laser beam generators. The output of this command shows a list of all OAW-IAPs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which OAW-IAP is sending out deauthorization frames, although it does not specify which OAW-IAP is being contained.	—	—

Example

The following example shows the output of **show all monitor** command.

```
Swarm Active Laser Beam Sources
-------------------------------
bssid  channel  rssi  ap name  lms ip  master ip  inactive time  reported by
-----  -------  ----  -------  ------  ---------  -------------  -----------
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show amp-audit

```
show amp-audit
```

Description

This command displays the set of configurations on the OmniVista 3600 Air Manager Management Platform.

Example

The following example shows the output of the **show amp-audit** command:

```
rule any any match any any any deny
wlan access-rule ssid1
   index 3
   rule any any match any any any deny
hotspot anqp-nai-realm-profile "name1"
   enable
   nai-realm-name ""
   nai-realm-eap-method eap-ttls
   nai-realm-auth-id-1 non-eap-inner-auth
   nai-realm-auth-value-1 mschapv2
   nai-realm-auth-id-2 credential
   nai-realm-auth-value-2 uname-password
   nai-realm-encoding utf8
   no nai-home-realm
hotspot anqp-nai-realm-profile "nr1"
   enable
   nai-realm-name "name1"
   nai-realm-eap-method eap-sim
   nai-realm-auth-id-1 non-eap-inner-auth
   nai-realm-auth-value-1 mschapv2
   nai-realm-auth-id-2 credential
   nai-realm-auth-value-2 uname-password
   nai-realm-encoding utf8
   nai-home-realm
hotspot anqp-venue-name-profile "Vn1"
   enable
   venue-group business
   venue-type research-and-dev-facility
   venue-lang-code en
   venue-name ""
hotspot anqp-venue-name-profile "vn1"
   enable
   venue-group business
   venue-type research-and-dev-facility
   venue-lang-code eng
   venue-name "vn1"
hotspot anqp-nwk-auth-profile "na1"
   enable
   nwk-auth-type accept-term-and-cond
   url "www.nwkauth.com"
hotspot anqp-roam-cons-profile "rc1"
   enable
   roam-cons-oi-len 3
   roam-cons-oi "888888"
hotspot anqp-3gpp-profile "3g"
   enable
   3gpp-plmn1 "40486"
   3gpp-plmn2 ""
   3gpp-plmn3 ""
   3gpp-plmn4 ""
   3gpp-plmn5 ""
   3gpp-plmn6 ""
hotspot anqp-ip-addr-avail-profile "ip1"
   enable
   ipv4-addr-avail
   no ipv6-addr-avail
   hotspot anqp-domain-name-profile "dn1"
   enable
   domain-name "DomainName"
hotspot h2qp-oper-name-profile "on1"
   enable
   op-lang-code eng
   op-fr-name "FriendlyName"
hotspot hs-profile "hs1"
   enable
   comeback-mode
   no asra
   no internet
   pame-bi
   group-frame-block
   p2p-dev-mgmt
   no p2p-cross-connect
   addtl-roam-cons-ois 0
   gas-comeback-delay 10
   query-response-length-limit 5
   access-network-type chargeable-public
   venue-group business
   venue-type research-and-dev-facility
   roam-cons-len-1 3
   roam-cons-oi-1 "123456"
   roam-cons-len-2 3
   roam-cons-oi-2 "223355"
   roam-cons-len-3 0
   roam-cons-oi-3 ""
   advertisement-profile anqp-nai-realm "nr1"
wlan ssid-profile test
   enable
   index 0
   type employee
   essid instant
   opmode opensystem
   max-authentication-failures 0
   rf-band all
   captive-portal disable
   dtim-period 1
   inactivity-timeout 1000
   broadcast-filter none
   dmo-channel-utilization-threshold 90
   local-probe-req-thresh 0
   max-clients-threshold 64
   dot11k
   dot11v
wlan ssid-profile ssid1
   enable
   index 1
   type employee
   essid hsProf
   opmode wpa2-aes
   max-authentication-failures 0
   vlan 200
   rf-band all
   captive-portal disable
   mac-authentication
   l2-auth-failthrough
   dtim-period 1
   inactivity-timeout 1000
   broadcast-filter none
   radius-accounting
   blacklist
   dmo-channel-utilization-threshold 90
   local-probe-req-thresh 0
   max-clients-threshold 64
   hotspot-profile "hs1"
auth-survivability cache-time-out 24
wlan external-captive-portal
   server localhost
   port 80
   url "/"
   auth-text "Authenticated"
   auto-whitelist-disable
   https
blacklist-time 3600
auth-failure-blacklist-time 3600
ids
   wireless-containment none
wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
wired-port-profile default_wired_port_profile
   switchport-mode trunk
   allowed-vlan all
   native-vlan 1
   shutdown
   access-rule-name default_wired_port_profile
   speed auto
   duplex full
   no poe
   type employee
   captive-portal disable
   no dot1x
enet0-port-profile default_wired_port_profile
uplink
   preemption
   enforce none
   failover-internet-pkt-lost-cnt 10
   failover-internet-pkt-send-freq 30
   failover-vpn-timeout 180
airgroup
   disable
airgroupservice airplay
   disable
   description AirPlay
airgroupservice airprint
   disable
   description AirPrint
per-ap-settings d8:c7:c8:c4:42:98
   hostname d8:c7:c8:c4:42:98
```

```
ip-address 10.17.161.254 255.255.255.0 10.17.161.1 10.13.6.110 ""
swarm-mode cluster
wifi0-mode access
wifi1-mode access
g-channel 0 0
a-channel 0 0
uplink-vlan 0
g-external-antenna 0
a-external-antenna 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap-alert

```
show ap-alert <count>
```

Description

This command displays all the alerts received for the specified OAW-IAPs.

Example

The following example shows the output of **show ap-alert** command.

```
AP Alerts
---------
Timestamp  Type  MAC Address  IP Address  Description
---------  ----  -----------  ----------  -----------
```

The output of this command includes the following information:

Column	Description	Range	Default
`Timestamp`	Indicates the time at which the alert was received.	—	—
`Type`	Indicates the type of alert received for the OAW-IAP.	—	—
`MAC Address`	Indicates the MAC address of the OAW-IAP clients.	—	—
`IP Address`	Indicates the IP address associated with the OAW-IAP.	—	—
`Description`	Displays a brief description of the alert received.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap-env

```
show ap-env [<addr>]
```

Description

This command displays all provisioned OAW-IAP parameters such as the type of antenna used by an OAW-IAP. The output of this command indicates if the OAW-IAP is configured to use an external or integrated antenna and if the OAW-IAP is configured as a master OAW-IAP.

Example

The following output is displayed for the **show ap-env** command:

```
# show ap-env
Antenna Type:External
Need USB field:Yes
name:344
radio_0_5ghz_ant_gain:5.0
radio_1_5ghz_ant_gain:5.0
radio_0_5ghz_ant_pol:1
radio_1_5ghz_ant_pol:1
uap_controller_less:1
dual_5g_mode:enable
344#
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap1x

```
show ap1x {config|debug-logs|status}
```

Description

This command shows the status and the details of 802.1X supplicant configuration on an OAW-IAP.

Parameter	Description	Range	Default
`config`	Shows the 802.1X supplicant configuration details.	—	—
`debug-logs`	Displays debug logs pertaining to the 802.1X supplicant configuration.	—	—
`status`	Shows the status of the 802.1X supplicant configuration.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap1xcert

```
show ap1xcert
```

Description

This command displays the details of certificates used for 802.1X authentication with wired ports.

Usage Guidelines

Use this command to view information server and CA certificates used for validating the authentication server to which OAW-IAP authenticates as a 802.1X supplicant.

Example

The following example shows the output of the **show ap1xcert** command:

```
Current ap1x CA Certificate:
Version       :3
Serial Number :AB:C1:1E:06:77:69:20:4F
Issuer        :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant/CN=Feng
Ding
Subject       :/C=CN/ST=Beijing/O=Aruba Networks/O=an HP company/OU=Aruba Instant/CN=Feng
Ding
Issued On     :Jan 26 08:48:16 2016 GMT
Expires On    :Jan 23 08:48:16 2026 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show aps

```
show aps [scanning]][sync]
```

Description

This command displays all active OAW-IAPs, OAW-IAP scanning, and OAW-IAP synchronization status.

Parameter	Description	Range	Default
`aps`	Displays the list of all active OAW-IAPs in the cluster.	—	—
`scanning`	Displays OAW-IAP scanning details.	—	—
`sync`	Displays OAW-IAP synchronization details.	—	—

Example

The following output is displayed for the **show aps** command:

```
c8:b5:ad:c3:ac:5c# show aps
1 Access Point
--------------
Name IP Address Mode Spectrum Clients Type IPv6 Address
Mesh Role Zone Serial # 2.4 Channel 2.4 Power (dB) 2.4 Utilization (%) 2.4
Noise Floor (dBm) 5.0 Channel 5.0 Power (dB) 5.0 Utilization (%) 5.0 Noise Floor (dBm)
Need Antenna Config From Port Config Id Config Csum Ext SSID Active Age Link
Local IP Address
---- ---------- ---- --------- -------- ---- ------------
--------- ---- --------- ----------- -------------- ------------------- --------
------------- ----------- -------------- ------------------- --------------------- ------
------------- --------- --------- ----------- --------------- --- --------------
-------
c8:b5:ad:c3:ac:5c 192.168.1.128* access disable 1 345(indoor)
fe80::cab5:adff:fec3:ac5c N/A - CNDBK5106R 149E 19 51(ok)
-90(good) 52E 12 51(ok) -88(good)
No none 0 12495 enable
20h:22m:48s fe80::cab5:adff:fec3:ac5c
```

The output of this command includes the following parameters:

Column	Description
`Name`	Name of the OAW-IAPs.
`IP address`	IP address of the OAW-IAPs.
`Mode`	Operating mode. For example, access, monitor, or spectrum monitor modes.
`Spectrum`	Indicates if spectrum monitoring is enabled or disabled.
`Clients`	Indicates the number of client associated with the OAW-IAP.
`Type`	Displays the OAW-IAP model.
`IPv6 Address`	IPv6 address of the OAW-IAP.

Column	Description
`Mesh Role`	Indicates if the OAW-IAP is functioning as Mesh Point or mesh Portal.
`Zone`	Zone name of the OAW-IAP.
`Serial#`	Serial number of the OAW-IAP.
`2.4 Channel`	Channels used by the OAW-IAP in the 2.4 GHz band.
`2.4 Power(dB)`	Transmission power allocated for 2.4 Ghz band channels.
`2.4 Utilization`	Percentage of utilization of 2.4 GHz channels.
`2.4 Noise Floor`	Noise floor of the 2.4 GHz channels.
`5.0 Channel`	Channels used by the OAW-IAP in the 5 GHz band.
`5.0 Power(dB)`	Transmission power allocated for 5 GHz band channels.
`5.0 Utilization`	Percentage of utilization of 5 GHz channels.
`5.0 Noise Floor`	Noise floor of the 5 GHz channels.
`Need antenna config`	Indicates if antenna configuration is required.
`From port`	Indicates the port details if any.
`Config Id`	Indicates the configuration ID.
`Config Csum`	Checksum that is used for configuration sync between master and slave access points.
`Ext SSID Active`	Extended SSID flag that indicates if mesh is enabled.
`Age`	Active time of the current master OAW-IAP.
`Link Local IP Address`	IPv6 link local IP address of the OAW-IAP.

The following output is displayed for the **show aps scanning** command:

```
AP Scanning Stats
-----------------
Name              IP Address   2.4 Reqs 2.4 Voice Rejs 2.4 Video Rejs 5.0 Reqs
----              ----------   -------- --------------  --------------  -----
d8:c7:c8:cb:d4:20 10.17.88.188 5665     0                   0           5675

5.0 Voice Rejs  5.0 Video Rejs
--------------  --------------
         0              0
```

The output of this command includes the following parameters:

Column	Description
`Name`	Displays the name of the OAW-IAP.
`IP address`	Displays the IP address of the OAW-IAP.
`2.4 Reqs`	Displays the counters that indicate channel scanning requirements.

Column	Description
5.0 Reqs	
2.4 Voice Rejs 5.0 Voice Rejs	Displays the counters that indicate the number of scanning rejects due to voice traffic.
2.4 Video Rejs 5.0 Video Rejs	Displays the counters that indicate the number of scanning rejects due to voice traffic.

The following output is displayed for the **show aps sync** command:

```
AP Sync List
------------
MAC  IP Address  Class  Current Version
---  ----------  -----  ---------------
```

The output of this command includes the following parameters:

Column	Description
MAC	Indicates MAC address of the OAW-IAP with which the current OAW-IAP is synchronized.
IP address	Displays the IP address of the OAW-IAP.
Class	Indicates if the OAW-IAP is serving as master or slave.
Current Version	Displays the Instant version currently running on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
■ All platforms.	Privileged EXEC mode

show ap allowed-channels

```
show ap allowed-channels
```

Description

This command displays a list of allowed channels for an OAW-IAP. Specify the country code for your OAW-IAP during the initial setup. Changing the country code causes the valid channel lists to be reset to the defaults for that country.

Example

The following example shows the output of the **show ap allowed-channels US** command for the OAW-IAP215 device:

```
Allowed Channels for AP Type 215 Country Code US
------------------------------------------------
PHY Type                   Allowed Channels
--------                   ----------------
802.11g (indoor)           1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)           36 40 44 48 149 153 157 161 165
802.11g (outdoor)          1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)          149 153 157 161 165
802.11g 40MHz (indoor)     1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)     36-40 44-48 149-153 157-161
802.11g 40MHz (outdoor)    1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)     149-153 157-161
802.11a 80MHz (indoor)     36-48 149-161
802.11a 80MHz (outdoor)     149-161
802.11a (DFS)
```

The output of this command includes the following information:

Column	Description
`PHY Type`	Indicates the PHY type.
`Allowed Channels`	Displays the list of allowed channels for a specific regulatory domain.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap allowed-max-EIRP

```
show ap allowed-max-EIRP
```

Description

This command displays the maximum EIRP settings for the country in which the OAW-IAP is currently operational. You can also view the maximum EIRP settings for a specific country.

Example

The following example shows the output of the **show ap allowed-max-EIRP** command:

```
Max EIRP setting for Country Code US Country United States and AP type AP-105
-----------------------------------------------------------------------------
Channel  1   2   3   4   5   6   7   8   9   10  11  12  13  14  36  40  44  48

-------  -   -   -   -   -   -   -   -   -   --  --  --  --  --  --  --  --  --

b        20  20  20  20  20  20  20  20  20  20  20  *   *   *   *   *   *   *

g/a      22  22  22  22  22  22  22  22  22  22  22  *   *   *   22  22  22  22

HT 20    22  22  22  22  22  22  22  22  22  22  22  *   *   *   21  21  21  21

HT 40    19  19  20  21  22  23  22  22  22  21  21  *   *   *   20  20  20  20



Max EIRP setting for Country Code US Country United States and AP type AP-105
-----------------------------------------------------------------------------
Channel  52  56  60  64  100  104  108  112  116  120  124  128  132  136  140  149  153

-------                                                 ---  ---  ---

b         *   *   *   *   *    *    *    *    *    *    *    *    *    *    *    *    *

g/a      24  24  24  24  22   22   22   22   22   *    *    *    22   22   22   23   23

HT 20    24  24  24  24  22   22   22   22   22   *    *    *    22   22   22   22   23

HT 40    23  23  23  23  22   22   22   22   *    *    *    *    22   22   22   22   22


Max EIRP setting for Country Code US Country United States and AP type AP-105
-----------------------------------------------------------------------------
Channel  157  161  165
-------  ---  ---  ---
b        *    *    *
g/a      23   23   23
HT 20    24   24   24
HT 40    22   20   17
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap arm

```
show ap arm {bandwidth-management | history | neighbors |rf-summary | scan-times}
```

Description

This command displays information about bandwidth management, historical statistics, OAW-IAP neighbors, RF summary, and scanning details for the OAW-IAP.

Parameter	Description	Range	Default
`bandwidth management`	Displays ARM bandwidth details for anOAW-IAP.	—	—
`history`	Displays detailed information about the ARM configuration changes over a period of time.	—	—
`neighbors`	Displays details about the ARM neighbors.	—	—
`rf-summary`	Displays a summary of RF configuration information for anOAW-IAP	—	—
`scan-times`	Displays ARM channel scanning details for anOAW-IAP.	—	—

Example

show ap arm bandwidth-management

The following example shows the output of **show ap arm bandwidth-management** command:

```
Interface :wifi0
Shaping Table
-------------
Client  Tx Pkt  Tx Byte (KB)  Tx Alloc (ms)  Tx Time (ms) Rx Time (ms) Active Time (ms) -----
-  ------  ------------  -------------  ------------  ------------ --------------
Tx Rate (mbps)
---------
Interface :wifi1
Shaping Table
-------------
Client  Tx Pkt  Tx Byte (KB)  Tx Alloc (ms)  Tx Time (ms) Rx Time (ms) Active Time (ms) -----
-  ------  ------------  -------------  ------------ ------------ --------------
Tx Rate (mbps)
---------
```

The output of this command includes the following information:

Column	Description
`Interface`	Displays the Wi-F interface configured on the OAW-IAP.
`Shaping table`	Displays information on the ARM configuration details for the clients associated with the OAW-IAP.
`Client`	Displays the list of OAW-IAP clients connected through the Wi-Fi interface.

Column	Description
`Tx Pkt`	Displays the transmission packet details associated with the interface.
`Tx Byte`	Displays the number of bytes in the transmission packets associated with the interface.
`Tx Alloc (ms)`	Indicates the time allocated for transmission in milliseconds.
`Tx Time (ms)`	Indicates the transmission time in milliseconds.
`Rx Time (ms)`	Indicates the reception time in milliseconds.
`Active time (ms)`	Indicates duration until which the Wi-Fi devices are active.
`Tx Rate (Mbps)`	Indicates the current speed at which data is transmitted through the Wi-Fi interface.

show ap arm history

For each interface on an OAW-IAP, the **show ap arm history** command shows the history of channel and power changes due to ARM. ARM can automatically change channel and power levels based on a number of factors such as noise levels and radio interference.

The following example shows the output of the **show ap arm history** command:

```
Interface :wifi0
ARM History
-----------
Time of Change       Old Channel  New Channel  Old Power  New Power  Reason
--------------       -----------  -----------  ---------  ---------  ------
2013-05-11 04:24:31  149+         161-         27         27         I
2013-05-11 02:54:34  157+         149+         27         27         I
2013-05-11 02:46:13  153-         157+         27         27         I
2013-05-11 02:27:11  157+         153-         27         27         I
2013-05-11 02:22:18  149+         157+         27         27         I
2013-05-11 01:35:00  161-         149+         27         27         I
2013-05-11 01:28:58  149+         161-         27         27         I
2013-05-10 22:46:33  161-         149+         27         27         I
2013-05-10 22:38:09  153-         161-         27         27         I
2013-05-10 22:02:10  161-         153-         27         27         I
2013-05-10 21:55:21  153-         161-         27         27         I
2013-05-10 16:47:15  157+         153-         27         27         I
2013-05-10 16:28:16  149+         157+         27         27         I
2013-05-10 15:19:59  161-         149+         27         27         I
2013-05-10 15:14:29  149+         161-         27         27         I
2013-05-10 13:10:55  161-         149+         27         27         I
2013-05-10 13:03:47  149+         161-         27         27         I
2013-05-10 12:17:34  157+         149+         27         27         I
2013-05-10 12:10:21  153-         157+         27         27         I
2013-05-10 11:12:04  157+         153-         27         27         I
2013-05-10 11:00:07  149+         157+         27         27         I
2013-05-10 10:54:39  157+         149+         27         27         I
2013-05-10 10:49:33  149+         157+         27         27         I
2013-05-10 10:44:34  157+         149+         27         27         I
2013-05-10 10:39:51  149+         157+         27         27         I
2013-05-10 10:33:07  157+         149+         27         27         I
2013-05-10 10:25:35  149+         157+         27         27         I
2013-05-10 09:18:11  157+         149+         27         27         I
2013-05-10 09:04:24  149+         157+         27         27         I
2013-05-10 06:08:59  157+         149+         27         27         I
2013-05-10 05:55:10  153-         157+         27         27         I
2013-05-10 05:11:21  157+         153-         27         27         I
```

```
Interface :wifi1
ARM History
-----------
Time of Change       Old Channel  New Channel  Old Power  New Power  Reason
--------------       -----------  -----------  ---------  ---------  ------
2013-05-11 04:16:28  6            1            24         24         I
2013-05-11 03:58:53  11           6            24         24         I
2013-05-11 03:13:44  1            11           24         24         I
2013-05-11 01:23:32  6            1            24         24         I
2013-05-11 01:04:29  11           6            24         24         I
2013-05-11 00:26:16  1            11           24         24         I
2013-05-10 23:13:30  6            1            24         24         I
2013-05-10 23:04:49  11           6            24         24         Q
2013-05-10 22:51:10  6            11           24         24         I
2013-05-10 22:45:01  1            6            24         24         I
2013-05-10 21:52:39  6            1            24         24         I
2013-05-10 21:44:37  1            6            24         24         Q
2013-05-10 21:29:52  6            1            24         24         I
2013-05-10 21:19:16  11           6            24         24         I
2013-05-10 21:12:53  6            11           24         24         I
2013-05-10 20:52:07  1            6            24         24         I
2013-05-10 19:28:09  6            1            24         24         I
2013-05-10 19:02:08  11           6            24         24         I
2013-05-10 18:23:32  1            11           24         24         I
2013-05-10 17:40:55  6            1            24         24         I
2013-05-10 17:28:40  11           6            24         24         I
2013-05-10 17:01:24  1            11           24         24         I
2013-05-10 15:10:19  6            1            24         24         I
2013-05-10 15:03:41  11           6            24         24         I
2013-05-10 14:45:39  6            11           24         24         I
2013-05-10 14:19:32  11           6            24         24         I
2013-05-10 13:37:30  1            11           24         24         I
2013-05-10 11:34:27  6            1            24         24         I
2013-05-10 11:19:52  11           6            24         24         I
2013-05-10 10:30:51  1            11           24         24         I
2013-05-10 09:18:51  6            1            24         24         I
2013-05-10 09:06:31  11           6            24         24         I
I: Interference, R: Radar detection, N: Noise exceeded, Q: Bad Channel Quality E: Error
threshold exceeded, INV: Invalid Channel, G: Rogue AP Containment, M: Empty Channel, P+:
Increase Power, P-: Decrease Power, 40INT: 40MHZ intol detected on 2.4G, NO40INT: 40MHz intol
cleared on 2.4G, OFF: Turn off Radio, ON: Turn on Radio
```

The output of this command includes the following information:

Column	Description
`Time of change`	Indicates the timestamp of the channel changes for each interface.
`Old Channel`	Displays the channel number used by the OAW-IAP before the ARM change.
`New channel`	Displays the channel number used by the OAW-IAP after the ARM change.
`Old Power`	Indicates power values configured on the OAW-IAP before the ARM change.
`New Power`	Indicates power values configured on the OAW-IAP after the ARM change.
`Reason`	Indicates the reason for changes in channels. For more information about the reason, see the description below the command output.

show ap arm neighbors

The **show ap arm neighbors** command displays the ARM settings on the OAW-IAP neighbors.

The following example shows the output of the **show ap arm neighbors** command:

```
ARM Neighbors
-------------
bssid              essid        channel  rssi  tx-power  PL (dB)  AP Flags  Last Update
-----              -----        -------  ----  --------  -------  --------  ------------
6c:f3:7f:45:57:20  7SPOT        1        8     0         0        Passive
6c:f3:7f:56:7e:a0  7SPOT        1        9     0         0        Passive
6c:f3:7f:56:7e:a1  NTT-SPOT     1        12    0         0        Passive
00:24:6c:80:77:c1  NTT-SPOT     1        9     0         0        Passive
6c:f3:7f:45:57:21  NTT-SPOT     1        8     0         0        Passive
6c:f3:7f:44:91:11  NTT-SPOT     1        9     0         0        Passive
00:24:6c:2b:fd:e8  qa-mv-vap3   161      5     9         98       Passive
00:24:6c:80:4d:62  docomo       1        10    0         0        Passive

(Total updates)
---------------
Neighbor Summary:One hop 232 Two hop 0 Current Time: 2013-05-11 04:31:33
```

The output of this command includes the following information:

Column	Description
`bssid`	Indicates the BSSID of the OAW-IAP neighbors.
`essid`	Indicates the ESSID of the OAW-IAP neighbors.
`Channel`	Indicates the channels assigned to the OAW-IAP neighbors
`rssi`	Indicates the RSSI values associated with the ARM channels to which OAW-IAP neighbors are connected.
`tx power`	Indicates the transmission power.
`PL`	Indicates power loss.
`AP Flags`	Indicates the status of OAW-IAP neighbors.
`Last Update`	Displays details of last updates if any.
`Total updates`	Displays a summary of updates.

show ap arm rf-summary

The **show ap arm rf-summary** command shows the statistics for all channels monitored by an OAW-IAP.

The following example shows the output of the **show ap arm rf-summary** command:

```
Channel Summary
---------------
channel  retry  phy-err  mac-err  noise  util(Qual)  cov-idx(Total)  intf_idx(Total)
-------  -----  -------  -------  -----  ----------  --------------  ---------------
36       0      0        0        97     1/0/0/0/99  0/0(0)          25/28//0/0(53)
40       0      0        0        97     1/0/0/0/99  0/0(0)          52/0//0/0(52)
44       0      0        0        97     1/0/0/0/99  0/0(0)          19/41//0/0(60)
48       0      0        0        97     1/0/0/0/99  0/0(0)          40/0//0/0(40)
52       0      0        0        97     1/0/0/0/99  0/0(0)          0/13//0/0(13)
56       0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
60       0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
64       0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
100      0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
104      0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
108      0      0        0        97     1/0/0/0/99  0/0(0)          0/0//0/0(0)
112      0      0        0        97     1/0/0/0/99  0/0(0)          0/18//0/0(18)
```

```
116      0      0        0        97     1/0/0/0/99   10/0(10)        103/0//0/0(103)
120      0      0        0        97     1/0/0/0/99   0/0(0)          27/18//0/0(45)
124      0      0        0        97     1/0/0/0/99   0/0(0)          0/0//0/0(0)
128      0      0        0        97     1/0/0/0/99   0/0(0)          0/0//0/0(0)
1        0      0        0        97     6/4/2/0/100  12/0(12)        133/0//0/0(133)
Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality

HT Channel Summary
------------------
channel_pair  Pairwise_intf_index
------------  -------------------
116-120       148
100-104       0
124-128       0
108-112       18
Interface Name           :wifi0
Current ARM Assignment   :100+/6
Covered channels a/g     :2/0
Free channels a/g        :6/0
Last check channel/pwr   :3m:17s/5m:4s
Last change channel/pwr  :1h:18m:38s/1h:18m:38s
Next Check channel/pwr   :4m:21s/1m:6s
Assignment Mode          :Single Band
Interface Name           :wifi1
Current ARM Assignment   :1/3
Covered channels a/g     :0/1
Free channels a/g        :0/0
ARM Edge State           :disable
Last check channel/pwr   :3m:12s/5m:13s
Last change channel/pwr  :3h:16m:53s/1h:32m:33s
Next Check channel/pwr   :3m:17s/10s
Assignment Mode          :Single Band

Channel quality history:wifi0
36 :Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99 100 100 100
100     100 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   0   0   0   0
        0   0
40 :Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99
99      99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
        1   1
44 :Q:  99  99  99  99  99  99  99 100 100 100 100  99  99  99 100  99  99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   1   1   0   0   0   0   1   1   1   0   1   1   1
48 :Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99
99      99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
         0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
        1   1
52 :Q:  99  99  99  99 100 100 100 100 100 100  99 100 100   0   0   0
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97   0 * 0 * 0
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0 100 100 100
   :U:  1   1   1   1   0   0   0   0   0   0   1   0   0   0   0   0
56 :Q:  99  99  99  99  99  99 100 100 100  99  99  99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   1   0   0   0   1   1   1   1
60 :Q:  99  99  99  99  99 100 100 100  99 100 100  99  99 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   0   0   0   1   0   0   1   1   0
64 :Q:  99  99  99  99  99 100 100 100 100 100 100 100 100 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   0   0   0   0   0   0   0   0   0
100:Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99
99      99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N: 97 97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97
        *97 *97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
        1   1
   :R:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
104:Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99 100 100 100
100     100 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   0   0   0   0
        0   0
108:Q:  99  99  99  99  99  99  99  99  99  99 100 100  99 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   1   1   1   1   1   0   0   1   0
112:Q:  99  99  99  99  99  99  99  99  99  99 100  99  99 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   1   1   1   1   1   1   1   0   1   1   0
116:Q:  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99  99
99      99  99
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
```

```
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
        1   1
120:Q:  99  99  99  99  99  99  99  99  99  99  99 100 100 100 100 100  99 100 100 100  99
100     100 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97  97
97      97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
        0   0
   :U:  1   1   1   1   1   1   1   1   1   1   1   0   0   0   0   0   1   0   0   0   1   0
        0   0
124:Q:  99  99  99  99  99  99  99  99  99 100 100 100 100   0
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97   0
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0 100
   :U:  1   1   1   1   1   1   1   1   1   0   0   0   0   0
128:Q:  99  99  99 100 100 100 100  99  99  99  99  99  99 100
   :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :N:  97  97  97  97  97  97  97  97  97  97  97  97  97  97
   :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0
   :U:  1   1   1   0   0   0   0   1   1   1   1   1   1   0

Channel quality history:wifi1
1:Q:  99  98 100 100 100 100  99 100  99  99  99 100  99 100 100 100  99  98 100 100  99  99
       100  99
 :c:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
       0   0
 :N: *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97 *97
      *97 *97
 :s:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
       0   0
 :U:  1   2   0   0   0   0   1   0   1   1   1   0   1   0   0   0   1   2   0   0   1   1
       0   1
 :R:  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
       0   0
```

The output of this command includes the following information:

Column	Description
`channel`	Displays the list of channels enabled on anOAW-IAP.
`retry`	Indicates the number of retry attempts.
`Phy-err`	Indicates the PHY errors on the current channels of anOAW-IAP.
`Mac-err`	Indicates the MAC errors on the current channels of anOAW-IAP.
`noise`	Displays the current noise level on each channel.
`Util (Qual)`	Displays the percentage of the channel being used and the current relative quality of selected channels.
`cov-idx(Total)`	Displays RF coverage details. The OAW-IAP uses this metric to measure RF coverage. The coverage index is calculated as x+y, where “x” is the OAW-IAP’s weighted calculation of the SNR on all valid OAW-IAPs on a specified 802.11 channel, and “y” is the weighted calculation of the OAW-IAPs SNR detected by the neighboring OAW-IAPs on that channel.

Column	Description
`intf_idx(Total)`	Displays channel interference details. The OAW-IAP uses this metric to measure co-channel and ACI. The Interference Index is calculated as a,b,c, or d where: ■ Metric value “a” is the channel interference the OAW-IAP sees on its selected channel. ■ Metric value “b” is the interference the OAW-IAP sees on the adjacent channel. ■ Metric value “c” is the channel interference the neighbors of the OAW-IAP see on the selected channel. ■ Metric value “d” is the interference the neighbors of the OAW-IAP see on the adjacent channel. ■ To calculate the total Interference Index for a channel add “a+b+c+d”.
`channel_pair`	Displays the list of paired channels.
`Pairwise_intf_index`	Displays the pairwise interference index.
`Interface Name`	Displays the interface name.
`Current ARM Assignment`	Displays the current ARM assignment details.
`Covered channels`	Displays the number of channels being used by the OAW-IAP's BSSID in the 2.4 GHz and 5 GHz bands.
`Free channels`	Displays the number of available channels in the 2.4 GHz and 5 GHz bands.
`ARM Edge State`	Displays the ARM Edge status. If ARM edge status is enabled, the ARM-enabled OAW-IAPs on the network edge will not function as AMs.
`Last check channel/pwr`	Indicates the time since the channel and power assignment was verified.
`Last change channel/pwr`	Indicates the time since the channel and power assignment was updated.
`Next Check channel/pwr`	Indicates the next interval at which the channel and power assignment will be verified.
`Assignment Mode`	Indicates if the ARM is assignment is applicable to a single band or dual band.
`Q`	Indicates the current channel quality for Wi-Fi transmission.
`c`	Indicates the duration of the channel quality. The OAW-IAP changes its channel when the value hits 120.
`N`	Indicates the noise floor.
`s`	Indicates the noise floor scale.
`U`	Indicates the non Wi-Fi utilization rate.
`R`	Indicates the retry rate.

show ap arm scan-times

The **show ap arm scan-times** command shows the AM channel scan times for an OAW-IAP. The following example shows the output of the **show ap arm scan-times** command:

```
Channel Scan Time
-----------------
channel  assign-time(ms) scans-attempted  scans-rejected  dos-scans  flags   timer-tick
-------  --------------- ---------------  --------------  ---------  -----   ----------
36       2483300          1530             0               0          DVACFT  172120
```

```
40       576170           1547             0               0          DVACPT  172139
44       9945940          1454             0               0          DVACFT  172145
48       170500           1550             0               0          DVACPT  172158
52       167420           1522             0               0          DVACT   172046
56       65450            595              0               0          DVCT    171880
60       169840           1544             0               0          DVACT   172052
64       170390           1549             0               0          DVACT   172063
149      68631720         952              0               0          DVACFT  172074
153      32278480         1268             0               0          DVACPT  172088
157      38634770         1207             0               0          DVACFT  172132
161      20620710         1361             0               0          DVACPT  172161
165      170280           1548             0               0          DVACT   172110
1        86424330         903              0               0          DVACFT  172161
2        53570            487              0               0          DC      171936
3        55660            506              0               0          DC      171980
4        88550            805              0               0          DC      172030
5        327140           2974             0               0          DVACP   172124
6        40459820         2562             0               0          DVACT   172110
7        334620           3042             0               0          DVACF   172137
8        89210            811              0               0          DC      171627
9        92620            842              0               0          DC      171684
10       192940           1754             0               0          DAC     172144
11       45787400         1340             0               0          DVACPT  172159
12       132550           1205             0               0          DAC     172051
13       51260            466              0               0          DC      171890
Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present
L: Scan 40MHz Lower, U: Scan 40MHz Upper, Z: Rare Channel
V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel, P: Valid 40MHZ Channel Pair
O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower
R: Radar detected in last 30 min, X: DFS required

WIF Scanning State
-------------------
Scan mode  channel  current-scan-channel  last-dos-channel  timer-milli-tick
---------  -------  --------------------  ----------------  ----------------
Default    161-     48-                   0                 172161700
Default    1        11-                   0                 172161700

next-scan-milli-tick (jitter)  scans (Tot:Rej:Eff(%):Last intvl(%))
--------------------           ------------------------------------
172172520(4420)                    17627:0:100:100
172164890(-4108)                   17697:0:100:100
```

The output of this command includes the following information:

Column	Description
`channel`	Displays the list of channels configured on the OAW-IAP.
`assign-time(ms)`	Displays the time since OAW-IAP is assigned a channel.
`scans-attempted`	Indicates the number times anOAW-IAP has attempted to scan another channel.
`scans-rejected`	Displays the number of times anOAW-IAP was unable to scan a channel, because the scan was halted due to other ARM settings.
`dos-scans`	Indicates the number of times services to a rogue device on a channel were denied by anOAW-IAP.

Column	Description
`flags`	Indicates channel flags. For more information on channel flags, see the flag description below the channel scan time table.
`timer-tick`	Indicates the time interval since the last scan.
`Scan mode`	Indicates if the scan mode enabled on the Wi-Fi interface.

`channel`
`(under WIFI Scanning State)`
	Indicates the channels available on the Wi-Fi interface.

`current-scan-channel`	Indicates the current channel scanned.
`last-dos-channel`	Indicates the last channel on which was detected.
`timer-milli-tick`	Indicates the time in milliseconds since the Wi-Fi interface channels were scanned.
`next-scan-milli-tick (jitter)`	Indicates the next interval at which the scanning will begin.
`scans (Tot:Rej:Eff(%):Last intvl(%))`	Provides a summary of the Wi-Fi scanning details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap association

```
show ap association
```

Description

This command displays the association table for anOAW-IAP group or for an individual OAW-IAP.

Example

The following example shows the output of **show ap association** command.

```
The phy column shows client's operational capabilities for current association
Flags: A: Active, B: Band Steerable, H: Hotspot(802.11u) client, K: 802.11K clie
                      nt, R: 802.11R client, W: WMM client, w: 802.11w client
PHY Details: HT   : High throughput;      20: 20MHz;  40: 40MHz
VHT  : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz +
          80MHz
<n>ss: <n> spatial streams
Association Table
-----------------
Name  bssid  mac  auth  assoc  aid  l-int  essid  vlan-id  tunnel-id  phy assoc.time num
assoc ----  -----  ---  ----  -----  ---  -----  -----  -------  ---------  ---  -----------
------
Flags
-----
Num Clients:0
```

The output of this command includes the following information:

Column	Description
Name	Indicates the Name of anOAW-IAP or the OAW-IAP group.
bssid	Indicates BSSID associated with the OAW-IAP. The BSSID is usually the MAC address of the OAW-IAP.
mac	Indicates the MAC address of the OAW-IAP clients.
auth	Displays the status of client authentication. Indicates **y** if the OAW-IAP is configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
assoc	Displays the status of user association. Indicates **y** if the OAW-IAP is configured for 802.11 association frame types. Otherwise, it displays an **n**.
aid	Indicates 802.11 association ID. A client receives a unique 802.11 association ID when it associates to an OAW-IAP.
1-int	Indicates the number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listening interval time of 1 second.
essid	Indicates the name that uniquely identifies the OAW-IAP's ESSID.
vlan-id	Indicates the VLAN ID associated with the OAW-IAP.
tunnel-id	Indicates the identification number of the OAW-IAP tunnel.
assoc. time	Indicates the amount of time the client has been associated with the OAW-IAP, in the hours: minutes: seconds format.

Column	Description
`num assoc`	Indicates the number of clients associated with the OAW-IAP.
`flags`	Displays flags for this OAW-IAP if any. For information on flag abbreviations, see the flag description at beginning of the output.
`Num Clients`	Indicates the number of clients associated with the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap bss-table

```
show ap bss-table
```

Description

This command displays the BSS of anOAW-IAP. The output of the show ap bss-table command shows the Alcatel-Lucent OAW-IAP BSS table for all OAW-IAPs. To filter this information and view BSS table data for an individual OAW-IAP or a specific port and slot number, include the ap-name, bssid, essid, ip-addr or port keywords.

Example

The following example shows the output of **show ap bss-table** command:

```
 Alcatel-Lucent AP BSS Table

------------------
bss                ess                      port  ip      phy    type
---                ---                       ----  --     ---    ----
d8:c7:c8:3d:42:12  example1  ?/?            10.17.88.188  a-HT   ap
d8:c7:c8:3d:42:13  example-local-nw ?/?     10.17.88.188  a-HT   ap
d8:c7:c8:cb:d4:21  __wired__eth1   ?/?      10.17.88.188  b      ap
d8:c7:c8:3d:42:02  example1  ?/?            10.17.88.188  g-HT   ap
d8:c7:c8:3d:42:03  example-local-nw   ?/?   10.17.88.188  g-HT   ap

ch/EIRP/max-EIRP  cur-cl  ap name            in-t(s)  tot-t
----------------  ------  -------            -------  -----
149+/20/22.5      1       d8:c7:c8:cb:d4:20  0        18h:13m:58s
149+/20/22.5      0       d8:c7:c8:cb:d4:20  0        18h:13m:58s
0/0/0             0       d8:c7:c8:cb:d4:20  0        18h:13m:59s
7/21.5/21.5       0       d8:c7:c8:cb:d4:20  0        18h:13m:58s
7/21.5/21.5       0       d8:c7:c8:cb:d4:20  0        18h:13m:58s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Num APs:5
Num Associations:1
```

The output of this command includes the following information:

Column	Description
bss	Displays the OAW-IAPBSSID. This is usually the MAC address of the OAW-IAP.
ess	Displays the OAW-IAP ESSID.
port	Displays port used by the OAW-IAP.
ip	Displays the IP address of an OAW-IAP.
phy	Displays an OAW-IAP radio type. Possible values are: ■ a—802.11a ■ a-HT—802.11a high throughput ■ g—802.11g ■ g-HT—802.11g high throughput

Column	Description
`type`	Shows whether the OAW-IAP is working as an access point or AM.
`ch/EIRP/max-EIRP`	Displays the radio channel used by the OAW-IAP or current EIRP or maximum EIRP.
`cur`	Displays the current number of clients on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap cacert

```
show ap cacert
```

Description

This command displays the details of the CA certificate on the OAW-IAP.

Example

The following example shows the certificate details displayed in the output of the **show ap cacert** command:

```
Local CA Certificates:
Version       :3
Serial Number :16:90:C3:29:B6:78:06:07:51:1F:05:B0:34:48:46:CB
Issuer        :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Subject       :/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO High-
Assurance Secure Server CA
Issued On     :Apr 16 00:00:00 2010 GMT
Expires On    :May 30 10:48:38 2020 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
Version       :3
Serial Number :01
Issuer        :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Subject       :/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA
Root
Issued On     :May 30 10:48:38 2000 GMT
Expires On    :May 30 10:48:38 2020 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
Version       :3
Serial Number :02:34:56
Issuer        :/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
Subject       :/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
Issued On     :May 21 04:00:00 2002 GMT
Expires On    :May 21 04:00:00 2022 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
Version       :3
Serial Number :6E:CC:7A:A5:A7:03:20:09:B8:CE:BC:F4:E9:52:D4:91
Issuer        :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Subject       :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at
https://www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3
Issued On     :Feb  8 00:00:00 2010 GMT
Expires On    :Feb  7 23:59:59 2020 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
Version       :3
Serial Number :18:DA:D1:9E:26:7D:E8:BB:4A:21:58:CD:CC:6B:3B:4A
Issuer        :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Subject       :/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. -
For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5
Issued On     :Nov  8 00:00:00 2006 GMT
Expires On    :Jul 16 23:59:59 2036 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
```

```
Version       :3
Serial Number :
Issuer        :/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Subject       :/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
Issued On     :Jun 29 17:06:20 2004 GMT
Expires On    :Jun 29 17:06:20 2034 GMT
Signed Using  :SHA1-RSA
RSA Key size  :2048 bits
```

The output of this command displays details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information of the CA certificates uploaded on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap checksum

```
show ap checksum
```

Description

This command displays the checksums if they are the same between master AP and the slave AP.

Example

The following example shows the output of **show ap checksum** command:

```
(Instant AP)# show ap checksum
Cfg                 :1559083477
Radius Cert         :0
Radius Psk          :0
Radius CA           :0
Radsec Cert         :0
Radsec Psk          :0
Radsec CA           :0
Web UI cert         :0
Web UI key          :0
CP cert             :0
CP key              :0
CP logo             :0
Datatunnel Cert     :0
Datatunnel Psk      :0
Datatunnel CA       :0
DHCP Option82 XML :0
Custom AWC CA from Activate      :4064146648
Custom AWC CA from Airwave       :0
Default ClearPass CA             :0
ClearPass CA        :0
WebCC CA            :0
Resource files      :0
Checksum            :26667
Audit Checksum      :0
Download role       :0
Import cert         :0
CA bundle           :0
Calc time           :2020-05-17 19:51:01
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The number of imported certificates and WebCC certificates on the AP were added to the output of this command.
AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-history

```
show ap client-match-history [client-mac <mac-address>]
```

Description

This command displays a historical record of the client match events and actions for the clients associated with an OAW-IAP.

Parameter	Description	Range	Default
`client-mac <mac-address>`	Allows you to filter the output based on a client MAC address. When the client MAC address is specified and the command is executed, the client match actions pertaining to the specified client is displayed.	—	—

Example

The following example shows the output of **show ap client-match-history** command:

```
Client Match Action Table
-------------------------
Station            Old State  New State  Reason                  Radio  Time
-------            ---------  ---------  ------                  -----  ----
00:db:df:0a:57:4e  Normal     Normal     Client associated       1      18h:32m:5s
00:db:df:0a:57:4e  Normal     Normal     Client associated       0      15h:20m:1s
00:db:df:0a:57:4e  Normal     Normal     Client associated       0      9h:48m:57s
00:db:df:0a:57:4e  Normal     Target     I am the better AP      0      7m:9s
00:db:df:0a:57:4e  Normal     Deny       I am not the better AP  1      7m:9s
a0:88:b4:41:64:18  Normal     Deny       I am not the better AP  0      5m:20s
a0:88:b4:41:64:18  Normal     Deny       I am not the better AP  1      5m:20s
00:db:df:0a:57:4e  Target     Adopted    Client match succeed    0      5m:17s
00:db:df:0a:57:4e  Deny       Normal     Client match succeed    1      5m:17s
a0:88:b4:41:64:18  Deny       Normal     State aged out          0      2m:27s
a0:88:b4:41:64:18  Deny       Normal     State aged out          1      2m:23s

Total 11 Records
00:24:6c:c8:74:4c# show ap client-match-his client-mac 00:db:df:0a:57:4e
Client Match History for 00:db:df:0a:57:4e
------------------------------------------
Old State  New State  Reason                  Radio  Time
---------  ---------  ------                  -----  ----
Normal     Normal     Client associated       1      18h:32m:5s
Normal     Normal     Client associated       0      15h:20m:1s
Normal     Normal     Client associated       0      9h:48m:57s
Normal     Target     I am the better AP      0      7m:9s
Normal     Deny       I am not the better AP  1      7m:9s
Target     Adopted    Client match succeed    0      5m:17s
Deny       Normal     Client match succeed    1      5m:17s

Total 7 Records
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-live

```
show ap client-match-live
```

Description

This command displays the current client match events and actions for clients associated with an OAW-IAP.

Example

The following example shows the output of the **show ap client-match-live** command.

```
Client Match Table
------------------
Station            CM State  RSSI  Radio  Home AP  Target AP  Time
-------            --------  ----  -----  -------  ---------  ----
00:db:df:0a:57:4e  Adopted   47    0      -        -          5m:17s

Total 1 Client Matches
00:24:6c:c8:74:4c# show ap client-match-his
Client Match Action Table
-------------------------
Station            Old State  New State  Reason                  Radio  Time
-------            ---------  ---------  ------                  -----  ----
00:db:df:0a:57:4e  Normal     Normal     Client associated       1      18h:32m:5s
00:db:df:0a:57:4e  Normal     Normal     Client associated       0      15h:20m:1s
00:db:df:0a:57:4e  Normal     Normal     Client associated       0      9h:48m:57s
00:db:df:0a:57:4e  Normal     Target     I am the better AP      0      7m:9s
00:db:df:0a:57:4e  Normal     Deny       I am not the better AP  1      7m:9s
a0:88:b4:41:64:18  Normal     Deny       I am not the better AP  0      5m:20s
a0:88:b4:41:64:18  Normal     Deny       I am not the better AP  1      5m:20s
00:db:df:0a:57:4e  Target     Adopted    Client match succeed    0      5m:17s
00:db:df:0a:57:4e  Deny       Normal     Client match succeed    1      5m:17s
a0:88:b4:41:64:18  Deny       Normal     State aged out          0      2m:27s
a0:88:b4:41:64:18  Deny       Normal     State aged out          1      2m:23s

Total 11 Records
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-refused

```
show ap client-match-refused [<radio>]
```

Description

This command displays the list of clients for which the channel allocation is refused based on the client match configuration parameters. When the client match feature is enabled on anOAW-IAP, the OAW-IAP measures the RF health of its associated clients. If spectrum load balancing is triggered and a client's RSSI is or less than 20 dB, clients are moved from one OAW-IAP to another for better performance and client experience.

Parameter	Description	Range	Default
`<radio>`	Allows you to filter the output based the ID number of the radio (for example, 0 or 1).	—	—

Example

The following example shows the output of the **show ap client-match-refused** command.

```
Client Match Status:: RUNNING  BALANCING
Associated:1, Threshold:1
Leaving:0, Coming:0
Last Refused Clients Table
--------------------------
MAC                RSSI  Refused Count  Last Refused Time
---                ----  -------------  -----------------
02:99:00:00:01:33  27    2              3
7e:17:7b:2c:f5:e2  5     4              6
00:27:10:c5:96:54  22    1              0
18:3d:a2:0a:48:3c  33    2              1
02:21:00:00:00:14  28    2              5
00:27:10:cf:ef:b4  32    2              7
7e:17:7b:27:6b:af  6     2              3
00:db:df:0a:6a:db  21    2              4

00:24:6c:c8:74:4c# show ap client-match-ref 1
Client Match Status:: RUNNING
Associated:0, Threshold:1
Leaving:0, Coming:0
Last Refused Clients Table
--------------------------
MAC                RSSI  Refused Count  Last Refused Time
---                ----  -------------  -----------------
02:99:00:00:01:33  35    2              3
00:db:df:0a:6a:db  29    3              10
fc:75:16:03:40:d9  41    10             3
18:3d:a2:09:79:ac  27    2              11
00:db:df:05:1f:d6  37    2              6
02:21:00:00:00:14  23    3              3
00:27:10:cf:ef:b4  27    2              5
00:27:10:cf:f2:4c  18    1              6
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-ssid-table

```
show ap client-match-ssid-table [radio-mac <mac-address>]
```

Description

This command displays the SSID table list over a specific radio for the current OAW-IAP and all other neighboring OAW-IAPs.

Parameter	Description	Range	Default
`<mac address>`	Enter a specific radio belonging to the current OAW-IAP and all its neighboring OAW-IAPs.	—	—

Example

The following example shows the output of the **show ap client-match-ssid-table** command:

```
(Instant AP)# show ap client-match-ssid-table
Client Match SSID Table
-----------------------
MAC                SSID Count  SSID Name   Clients  Threshold   HE Enable
---                ----------  ---------   -------  ---------   ---------
40:e3:d6:7f:4c:70  2           CM_zone_b   0        64          0
CM2_zone_b  0        64
40:e3:d6:7f:4c:60  2           CM_zone_b   0        64          1
CM2_zone_b  0        64
f0:5c:19:1c:92:40  2           CM_zone_a   0        64          0
CM1_zone_a  0        64
f0:5c:19:1c:92:50  2           CM_zone_a   0        64          0
CM1_zone_a  0        64
9c:1c:12:3a:e8:e0  2           CM_zone_a   0        64          1
CM1_zone_a  0        64
9c:1c:12:3a:e8:f0  2           CM_zone_a   0        64          0
CM1_zone_a  0        64
Total 6 Radios
```

The following example shows the output of the **show ap client-match-ssid-table radio-mac** command:

```
(Instant AP)# show ap client-match-ssid-table radio-mac f0:5c:19:1c:92:50
Client Match SSID Table
-----------------------
MAC                SSID Count  SSID Name   Clients  Threshold   HE Enable
---                ----------  ---------   -------  ---------   ---------
f0:5c:19:1c:92:50  2           CM_zone_a   0        64          1
CM1_zone_a  0      64
Total 1 Radios
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of this command has been enhanced to include the **HE capable** status column.
Alcatel-Lucent AOS-W Instant 8.3.1.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-match-triggers

```
show ap client-match-triggers
```

Description

This command displays the configuration conditions that trigger client match events and actions for the clients associated with an OAW-IAP. When the client match feature is enabled on an IAP, the OAW-IAP measures the RF health of its associated clients. Based on the following trigger conditions, the clients are moved from one OAW-IAP to another for better performance and client experience.

For more information on client match and client match trigger conditions, see *Alcatel-Lucent AOS-W Instant User Guide*.

Example

The following example shows the output of the **show ap client-match-triggers** command:

```
Client Match Triggers
---------------------
Station            PHY  Target_AP          Reason
-------            ---  ---------          ------
A_CCNT  Time
---  ----
00:15:00:5e:7e:3c  0    9c:1c:12:3a:e9:70  Dynamic Load Balancing
5a:15:00:00:00:16  1    9c:1c:12:3a:e9:10  Sticky Client
00:15:00:5e:77:c8  0    9c:1c:12:3a:e9:10  Dynamic Load Balancing
a4:4e:31:97:da:74  0    9c:1c:12:3a:e9:10  Dynamic Load Balancing
00:15:00:5b:72:1c  1    9c:1c:12:3a:e9:60  Sticky Client
5a:12:00:00:00:11  0    9c:1c:12:3a:e6:70  Dynamic Load Balancing

STA_CAP  rssi  chan  ccnt  cutil  g_ccnt  RSSI  CHAN  CCNT  ROOM  CUTIL
-------  ----  ----  ----  -----  ------  ----  ----  ----  ----  -----  ---
-        25    36+   12    -      -       44    44+   2     -     -      -       3h:11m:19s
-        17    6     -     -      -       34    40-   -     -     -      -       2h:11m:40s
-        36    48-   19    -      -       38    40-   0     -     -      -       2h:11m:34s
-        31    48-   19    -      -       42    40-   0     -     -      -       2h:11m:34s
-        24    5     -     -      -       35    6     -     -     -      -       1h:29m:37s
-        15    44+   9     -      -       35    40-   9     -     -      -       1h:9m:41s
Total 6 Records
```

The output of this command displays client match trigger records with details such as station MAC, target AP MAC, trigger condition and so on.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-probe-report

```
show ap client-probe-report [<radio>]
```

Description

This command displays the client probe report for an OAW-IAP.

Parameter	Description	Range	Default
`<radio>`	Allows you to filter the output based the ID number of the radio (for example, 0 or 1).	—	—

Example

The following example shows the output of the **show ap client-probe-report** command.

```
AP Client Probe Report for Wifi0 (5G)
-------------------------------------
MAC                RSSI  In Swarm  Flags  Matched          Received
---                ----  --------  -----  -------          --------
00:27:10:a9:98:60  12    No        4      -                1m:5s
60:f8:1d:ad:7f:f0  18    No        N      -                4s
24:77:03:8f:78:30  24    No        4      -                40s
24:77:03:f7:6d:20  20    No        4      -                17s
00:15:00:5b:3a:50  28    No        4      -                15s
02:36:00:00:00:30  58    No        4      -                45s
0c:84:dc:3b:63:f1  16    No        4      -                3m:27s
6a:10:00:00:00:01  43    No        8      -                2m:33s
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap client-view

```
show ap client-view
```

Description

This command displays information about the clients in an OAW-IAP's neighborhood.

Example

The following example shows the output of **show ap client-view** command:

```
Client Match Neighbor Table
---------------------------
MAC                Channel  RSSI  Clients  Threshold  Channel Util (%)
---                -------  ----  -------  ---------  ----------------
d8:c7:c8:44:50:c0  6        13    1        -          -
d8:c7:c8:44:50:d0  40       8     2        -          -
d8:c7:c8:44:51:b0  44       40    10       -          -
d8:c7:c8:44:61:a0  1        36    3        -          -
d8:c7:c8:44:61:b0  48       24    3        -          -
d8:c7:c8:44:51:a0  11       50    4        -          -
d8:c7:c8:44:62:a0  6        19    2        -          -
6c:f3:7f:ef:12:c0  1        28    0        1          0
6c:f3:7f:ef:12:d0  149E     72    0        1          0
6c:f3:7f:ef:03:00  6        24    0        0          0
d8:c7:c8:44:63:90  153      9     2        -          -
6c:f3:7f:ee:f7:80  3        76    0        1          0
6c:f3:7f:ee:f7:90  52E      62    0        1          0
d8:c7:c8:44:4a:30  161      7     2        -          -
d8:c7:c8:44:4b:80  6        10    3        -          -
d8:c7:c8:44:4b:90  48       17    2        -          -
6c:f3:7f:ee:dc:20  11       32    2        3          0
d8:c7:c8:44:4c:80  6        24    1        -          -
d8:c7:c8:44:4c:90  36       20    11       -          -
6c:f3:7f:e7:5d:40  1        59    1        3          0

VC Key    Flags  Received   HE Capable
------    -----  --------   ----------
-                8m:27s     Yes
-         V      1s         Yes
-         VR     2m:49s     Yes
-         VR     58s        Yes
-         V      1s         No
-         VR     1s         No
-         V      20s        Yes
271d9383  VRIC   4s
271d9383  VRIC   13s
-                9m:8s
847face0  B      5m:7s
-         V      19s
271d9383  VRIC   6s
271d9383  VRIC   6s
-         S      12m:43s
-         VR     1m:24s
-         VR     2m:34s
847face0         3m:6s
-         VR     2m:27s
-         VR     2m:34s
847face0         14m:24s

Neighbor Flags:      V - Valid;       R - In RF Neighborhood;      S - Same Channel;
```

```
B - Balancing;   C - Client Match Enabled;    I - In Same Swarm
Total 21 Neighbors
00:24:6c:c8:74:4c# show ap client-match-live
Client Match Table
------------------
Station            CM State  RSSI  Radio  Home AP  Target AP  Time
-------            --------  ----  -----  -------  ---------  ----
00:db:df:0a:57:4e  Adopted   47    0      -        -          5m:17s

Total 1 Client Matches
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of this command includes the **HE Capable** column.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airslice client-stats

```
show ap debug airslice client-stats <mac> <dpiid>
```

Description

This command displays the application usage statistics of a single client based on its MAC address and DPI ID.

Example

The following example shows the partial output of **show ap debug airslice client-stats**:

```
(Instant AP)# show ap debug airslice client-stats 3c:a9:f4:42:73:14 20004

Airslice client 3c:a9:f4:42:73:14 dpi 20004 stats table
-------------------------------------------------------
Index Avg Jitter Avg Delay Loss pkts TX pkts
----- ---------- --------- --------- -------
0         2493           29551           0               60
1         3460           29116           0               75
2          483           10169           0               20
3         4165           20568           0               90
4          613           10265           0               18
5         1429           26830           0               4
6          128           4383            0               11
7          323           26397           0               7
8         1129           9651            0               27
9          425           11068           0               10
10         236           9679            0               4
11         325           15691           0               8
12         568           11262           0               8
13           0           5409            0               1
14        1330           27422           0               8
15        3081           21221           0               234
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-530 Series and OAW-AP555 access points	Privileged EXEC mode

show ap debug airwave

```
show ap debug airwave
```

Description

This command displays the list of OmniVista 3600 Air Manager servers configured on an OAW-IAP.

Example

The following example shows the output of **show ap airwave** command:

```
Airwave Server List
-------------------
Domain/IP Address              Type     Mode  Config-only  Rapids-mode  Status
-----------------              ----     ----  -----------  -----------  ------

securelogin.arubanetworks.com  Primary  -     -            No           Not connected
70:3a:0e:cc:ee:b2# show ap debug airwave
Airwave Server List
-------------------
Domain/IP Address  Type  Mode  Config-only  Rapids-mode  Status
-----------------  ----  ----  -----------  -----------  ------
70:3a:0e:cc:ee:b2#
70:3a:0e:cc:ee:b2# show ap debug am-config
Radio Configuration for wifi0
-----------------------------
Parameter          Value
---------          -----
Preferred Channel  108
Tx Power           27.0
VHT Enabled        1
Radio Configuration for wifi1
-----------------------------
Parameter          Value
---------          -----
Preferred Channel  1
Tx Power           24.0
VHT Enabled        0
ARM Configuration for wifi0
----------------------------
Parameter                                         Value
---------                                         -----
Assignment                                        0
Client Aware                                      1
Mode Aware                                        0
OTA Updates                                       0
Scanning                                          1
Scan Interval                                     10
Rogue AP Aware                                    0
Max Tx Power (cfg/internal)                       12/10
Min Tx Power (cfg/internal)                       1/1
Scan Mode                                         reg-domain
40 MHz/80 MHz                                     1/1
Channel Quality aware/qual thresh/qual wait time  0/70/120
Error rate thresh/error rate wait time            70/90
Noise thresh/noise wait time                      75/120
Aggressive scans                                  0
Frequent scan action                              0
Client Match/Upd intvl                            0/0
Sticky (Intvl/SNR/SNR thr/Min Sig)                0/0/0/0
```

```
Bandsteer (g max sig/a min sig)                  0/0
Ideal Coverage Index                             10
Acceptable Coverage Index                        4
Free Channel Index                               25
Backoff Time                                     240
Intf AP Weight                                   25
ARM Configuration for wifi1
----------------------------
Parameter                                        Value
---------                                        -----
Assignment                                       0
Client Aware                                     1
Mode Aware                                       0
OTA Updates                                      0
Scanning                                         1
Scan Interval                                    10
Rogue AP Aware                                   0
Max Tx Power (cfg/internal)                      12/[282208.333178] __ieee80211_smart_ant_
init: Smart Antenna is not supported
8
Min Tx Power (cfg/internal)                      1/1
Scan Mode                                        reg-domain
40 MHz/80 MHz                                    1/0
Channel Quality aware/qual thresh/qual wait time  0/70/120
Error rate thresh/error rate wait time           70/90
Noise thresh/noise wait time                     75/120
Aggressive scans                                 0
Frequent scan action                             0
Client Match/Upd intvl                           0/0
Sticky (Intvl/SNR/SNR thr/Min Sig)               0/0/0/0
Bandsteer (g max sig/a min sig)                  0/0
Ideal Coverage Index                             10
Acceptable Coverage Index                        4
Free Channel Index                               25
Backoff Time                                     240
Intf AP Weight                                   25
Scanning Configuration for wifi0
---------------------------------
Parameter                             Value
---------                             -----
Scan-mode                             all-reg-domain
Dwell Time: Active Channel            500
Dwell Time: Reg-Domain Channel        250
Dwell Time: Other Reg-Domain Channel  200
Dwell Time: Rare Channel              100
Scanning Configuration for wifi1
---------------------------------
Parameter                             Value
---------                             -----
Scan-mode                             all-reg-domain
Dwell Time: Active Channel            500
Dwell Time: Reg-Domain Channel        250
Dwell Time: Other Reg-Domain Channel  200
Dwell Time: Rare Channel              100
Regulatory Domain Configuration
-------------------------------
Parameter     Value
---------     -----
Country Code  67
G-Band 20MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
```

```
Reg Domain Profile
Downloadable Reg Table        1 6 11
AP Cert Info                  1 2 3 4 5 6 7 8 9 10 11
Valid (Assignment) Channels   1 6 11
A-Band 20MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161 165
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161 165
Valid (Assignment) Channels   36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161 165
G-Band 40MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        1 7
AP Cert Info                  1 2 3 4 5 6 7
Valid (Assignment) Channels   1 7
A-Band 40MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 44 52 60 100 108 116 124 132 140 149 157
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161
Valid (Assignment) Channels   36 44 52 60 100 108 116 124 132 140 149 157
A-Band 80MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 52 100 116 132 149
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161
Valid (Assignment) Channels   36 52 100 116 132 149
A-Band 160MHz Channels
------------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 100
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128
Valid (Assignment) Channels   36 100
AP System Configuration
-----------------------
Parameter        Value
---------        -----
AM Scan RF Band  all
Flex Radio Mode  2g_plus_5g
RF Behavior Configuration
-------------------------
Parameter               Value
---------               -----
Station Handoff Assist  Disable
RSSI Falloff Wait Time  0
Low RSSI Threshold      0
RSSI Check Frequency    0
```

```
Event Thresholds Configuration
------------------------------
Parameter                                Value
---------                                -----
Detect Frame Rate Anomalies              Disable
Bandwidth Rate High Watermark            0
Bandwidth Rate Low Watermark             0
Frame Error Rate High Watermark          0
Frame Error Rate Low Watermark           0
Frame Fragmentation Rate High Watermark  0
Frame Fragmentation Rate Low Watermark   0
Frame Low Speed Rate High Watermark      0
Frame Low Speed Rate Low Watermark       0
Frame Non Unicast Rate High Watermark    0
Frame Non Unicast Rate Low Watermark     0
Frame Receive Error Rate High Watermark  0
Frame Receive Error Rate Low Watermark   0
Frame Retry Rate High Watermark          0
Frame Retry Rate Low Watermark           0
Interference Configuration
--------------------------
Parameter                        Value
---------                        -----
Detect Interference              Disable
Interference Increase Threshold  0
Interference Increase Timeout    0
Interference Wait Time           0
IDS General Configuration
-------------------------
Parameter                                Value
---------                                -----
Stats Update Interval                    60
Monitored Device Stats Update Interval   60
AP Inactivity Timeout                    20
Adhoc AP Inactivity Timeout              5
AP Unseen Timeout                        600
Adhoc AP Unseen Timeout                  180
STA Inactivity Timeout                   120
STA Unseen Timeout                       600
Min Potential AP Beacon Rate             25
Min Potential AP Monitor Time            2
Signature Quiet Time                     900
Containment Confirmation                 Disable
Wireless Containment                     none
Debug Wireless Containment               Disable
Wired Containment                        Disable
Wired Containment of AP's Adj MACs       Disable
Wired Containment of Suspected L3 Rogue  Disable
Mobility Manager RTLS                    Disable
AP Event Generation                      traps-only
Send Adhoc Info to Controller            Disable
WMS Client Monitoring                    none
Packet SNR Threshold                     0
Frame Type for RSSI calculation          ba pr dlow mgmt ctrl null
Max Monitored Devices                    1024
Max Unassociated Stations                256
Unclassified AP Updates                  Disable
Unclassified STA Updates                 Disable
Unclassified Device Update Interval      60
Client Detection Mode                    normal
Station RSSI Message                     Disable
Station RSSI Message Interval            0
AP Neighbors Message                     Disable
AP Neighbors Message Interval            0
IDS DOS Configuration
---------------------
Parameter                                           Value
---------                                           -----
Detect Disconnect Station Attack                    Disable
Disconnect STA Detection Assoc Resp Threshold       5
Disconnect STA Detection Deauth-Disassoc Threshold  8
Disconnect STA Detection Quiet Time                 900
Detect AP Flood Attack                              Enable
AP Flood Threshold                                  50
AP Flood Increase Time                              3
AP Flood Quiet Time                                 900
Detect Client Flood Attack                          Disable
Client Flood Threshold                              150
Client Flood Increase Time                          3
Client Flood Quiet Time                             900
Detect EAP Rate Anomaly                             Disable
EAP Rate Threshold                                  60
EAP Rate Time Interval                              3
EAP Rate Quiet Time                                 900
Detect CTS Rate Anomaly                             Disable
CTS Rate Threshold                                  5000
CTS Rate Time Interval                              5
CTS Rate Quiet Time                                 900
Detect RTS Rate Anomaly                             Disable
RTS Rate Threshold                                  5000
RTS Rate Time Interval                              5
RTS Rate Quiet Time                                 900
Detect Rate Anomalies                               Disable
Detect 802.11n 40MHz Intolerance                    Disable
Client 40MHz Intolerance Quiet Time                 900
Detect Omerta Attack                                Disable
Omerta Attack Rate Threshold                        10
Omerta Quiet Time                                   900
Detect FATA-Jack Attack                             Disable
FATA-Jack Quiet Time                                900
Detect TKIP Replay Attack                           Disable
TKIP Replay Quiet Time                              900
Detect ChopChop Attack                              Disable
ChopChop Quiet Time                                 900
Detect Invalid Address Combination                  Disable
Invalid Address Combination Quiet Time              900
Detect Malformed Assoc Request                      Disable
Malformed Assoc Request Quiet Time                  900
Detect Malformed HT IE                              Disable
Malformed HT IE -Jack Quiet Time                    900
Detect Overflow EAPOL Key                           Disable
Overflow EAPOL key Quiet Time                       900
Detect Malformed Auth Frame                         Disable
Malformed Auth Frame Quiet Time                     900
Detect Overflow IE                                  Disable
Overflow IE Quiet Time                              900
Detect Malformed Large Duration                     Disable
Malformed Large Duration Quiet Time                 900
Detect Block ACK DoS                                Disable
Block ACK DoS Quiet Time                            900
Detect Power Save DoS Attack                        Disable
Power Save DoS Threshold                            80
Power Save DoS Quiet Time                           900
Detect WPA FT Attack                                Disable
WPA FT Attack Detection Time Interval               60
WPA FT Attack Detection Threshold                   45
WPA FT Attack Detection Quiet Time                  900
IDS Rate Parameters
--------------------
FrameType       ChThreshold  ChTime  ChQuietTime  NodeThreshold  NodeTime  NodeQuietTime
---------       -----------  ------  -----------  -------------  --------  -------------
assoc           300          15      900          200            15        900
disassoc        300          15      900          200            15        900
deauth          300          15      900          200            15        900
probe-request   300          15      900          200            15        900
probe-response  300          15      900          200            15        900
auth            300          15      900          200            15        900
IDS Impersonation Configuration
-------------------------------
Parameter                                     Value
---------                                     -----
Detect AP Impersonation                       Disable
Protect from AP Impersonation                 Disable
Beacon Diff Threshold                         50
Beacon Increase Wait Time                     3
Detect AP Spoofing                            Disable
AP Spoofing Quiet Time                        900
Detect Channel Based MitM(Man in the Middle)  Disable
Channel Based MitM Quiet Time                 900
Detect Beacon on Wrong Channel                Disable
Beacon on Wrong Channel Quiet Time            900
Detect Hotspotter Attack                      Disable
Hotspotter Quiet Time                         900
IDS Unauthorized Device Profile Configuration
---------------------------------------------
Parameter                                           Value
---------                                           -----
Detect Adhoc Networks                               Disable
Protect from Adhoc Networks                         Disable
Detect Windows Bridge                               Disable
Protect Windows Bridge                              Disable
Detect Wireless Bridge                              Disable
Wireless Bridge detection Quiet Time                900
Detect Devices with an Invalid MAC OUI              Disable
MAC OUI detection Quiet Time                        900
Rogue AP Classification                             Enable
Overlay Rogue AP Classification                     Disable
OUI-based Rogue AP Classification                   Disable
Propagated Wired MAC based Rogue AP Classification  Disable
Rogue Containment                                   Disable
Suspected Rogue Containment                         Disable
Suspect Rogue Confidence Level                      100
Allow Well Known MACs
Protect Valid Stations                              Disable
Detect Bad WEP                                      Disable
Detect Misconfigured AP                             Disable
Protect Misconfigured AP                            Disable
Protect SSID                                        Disable
Privacy                                             Disable
Require WPA                                         Disable
Detect Unencrypted Valid Clients                    Disable
Unencrypted Valid Clients Quiet Time                900
Protect 802.11n High Throughput Devices             Disable
Protect 802.11n High Throughput 40MHz Devices       Disable
Detect 802.11n Greenfield Activity                  Disable
Detect Adhoc Using Valid SSID                       Disable
Adhoc Using Valid SSID Quiet Time                   900
Protect Adhoc Using Valid SSID                      Disable
Detect Valid Client Misassociation                  Disable
Detect STA Assoc To Rogue                           Disable
Detect Wireless Hosted Network                      Disable
Wireless Hosted Network Quiet Time                  0
Protect From Wireless Hosted Network                Disable
Valid 802.11b channel
Valid 802.11a channel
Config Wired MAC Table
-----------------------
mac
---
Valid OUIs
-----------
OUI
---
Valid and Protected SSIDs
--------------------------
SSID
----
334-Mesh
70:3a:0e:cc:ee:b2#
```

The following output of the **show ap debug airwave** command to displays the WebSocket debug information:

```
Airwave Server List
-------------------

Domain/IP Address  Type    Mode Config-only     Rapids-mode     Status
-----------------  ----    ----  -----------    -----------     ------
10.65.6.213        Primary Manage   -            Yes            Login done

Aruba Airwave server        :10.65.6.213
Aruba Airwave proxy server  :None
Aruba Airwave Protocol  :wss
Aruba Airwave uptimes   :3s
Aruba Airwave status    :Login done

Server Debug Statistics
------ ----- ----------
Key                                         Value
---                                         -----

Connect establish success                     3(3)
Authentication failed                         3(3)
Login done times                              1(1)
Connect retry times                           3(3)


Last connect status
-------------------

Last connect ID                             :3
Last connect time                           :2018-01-25 07:12:36
Last connect trigger                        :retry auth

Last connect fail status
------------------------

Last fail server
Last fail time
Last fail reason

Last login done status
```

```
----------------------
Last connect done                            :2018-01-25 07:12:37
```

The output of this command includes the following information:

Column	Description
`Domain/IP Address`	Displays the IP address or domain name of the OmniVista 3600 Air Manager server.
`Type`	Displays the type of the OmniVista 3600 Air Manager server. For example, backup or primary server.
`Mode`	Indicates the mode of OmniVista 3600 Air Manager operation. **NOTE:** OmniVista 3600 Air Manager can be configured to operate in the Manage Read/Write or Monitor-only+ Firmware Upgrades modes.
`Config-only`	Indicates whether OmniVista 3600 Air Manager is in the configuration mode. If yes, the OAW-IAP simplifies the report for OmniVista 3600 Air Manager.
`Rapids-mode`	Indicates whether OmniVista 3600 Air Manager is in RAPIDS mode. RAPIDS is a powerful tool used for monitoring and managing security on wireless networks. The OAW-IAP can perform different actions when RAPIDS mode is enabled.
`Status`	Indicates the OmniVista 3600 Air Manager login status.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-config-received

```
show ap debug airwave-config-received
```

Description

This command displays the list of configurations received by the OAW-IAP from the OmniVista 3600 Air Manager server. The output displays the last six batches of configurations received from OmniVista 3600 Air Manager. The log of configurations received from the OmniVista 3600 Air Manager server is cleared when there is a reboot or image upgrade.

The command will return the following error messages based on the scenario:

- If the AP is managed using Central???, the command returns the result **Current manage mode is athena, please use command "show ap debug cloud-config-received"**.
- If the AP did not receive configuration from the OmniVista 3600 Air Manager server, the command returns the result **No configuration received from OmniVista 3600 Air Manager yet**.

Example

The following example shows the output of the **show ap debug airwave-config-received** command:

```
(Instant AP)show ap debug airwave-config-received

timestamp: 2020-03-26 09:19:41
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname lau-test: OK
swarm-mode standalone: OK
exit: OK

timestamp: 2020-03-26 09:24:05
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname lau-1234: OK
swarm-mode standalone: OK
exit: OK

timestamp: 2020-03-26 09:33:08
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname lau-123456788: OK

timestamp: 2020-03-26 09:34:49
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname 70:3a:0e:cc:ee:8c : OK

timestamp: 2020-03-26 09:35:58
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname 70:3a:0e:cc:ee:8c--01 : OK

timestamp: 2020-03-26 13:24:35
per-ap-settings 70:3a:0e:cc:ee:8c : OK
hostname 70:3a:0e:cc:ee:8c--02 : OK
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The output of the command was modified to include the number of imported certificates and WebCC certificates on the AP.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-data-sent

```
show ap debug airwave-data-sent
```

Description

This command displays information about data exchange between the OmniVista 3600 Air Manager server and the OAW-IAP.

Example

The following example shows the output of the **show ap debug airwave-data-sent** command:

```
cat: /tmp/awc_buf.txt: No such file or directory
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-events-pending

```
show ap debug airwave-events-pending
```

Description

This command displays the pending OmniVista 3600 Air Manager server events.

Example

The following example shows the partial output of the **show ap debug airwave-events-pending** command:

```
<t11>
<e61>1106</e61>
<e62>654</e62>
<e1005>6c:f3:7f:56:7f:60</e1005>
<e1006>7SPOT</e1006>
<e1001>d8:c7:c8:cb:d4:20</e1001>
<e1056>2</e1056>
<e1017>d8:c7:c8:cb:d4:20</e1017>
<e1018>1</e1018>
<e1058>Varbind deprecated</e1058>
</t11>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-pingpong-stats

```
show ap debug airwave-pingpong-stats
```

Description

This command shows the ping pong count statistics between the OAW-IAP and OmniVista 3600 Air Manager.

Example

The following example shows the output of **show ap debug airwave-pingpong-stats** command:

```
ping statistics    1657(2448)
pong statistics    1657(2444)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-restore-status

```
show ap debug airwave-restore-status
```

Description

This command displays information about the status of the OAW-IAP configuration restoration on the OmniVista 3600 Air Manager server. If the OAW-IAPs managed by OmniVista 3600 Air Manager are not able to connect to the OmniVista 3600 Air Manager server, OAW-IAP can load the backed up configuration received by OmniVista 3600 Air Manager after five minutes. This command displays the restoration status of the OAW-IAP configuration for the OAW-IAPs managed by OmniVista 3600 Air Manager.

Example

The output of the **show ap debug airwave-restore-status** command displays the restoration flag and time. The following example shows the output of this command:

```
Airwave Config Restore
----------------------
Restore flag  Time
------------  ----
No            N/A
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-signon-key

```
show ap debug airwave-signon-key
```

Description

This command displays the OmniVista 3600 Air Manager sign on key used by the used by the administrator to manually authorize the first virtual switch for an organization.

Example

The following example shows the output of the **show ap debug airwave-signon-key** command:

```
awc_ui_key_new : 8adf05e0013cb69393335b32627b02db7b49af0705da9fbda6
awc_ui_key_old : 9418cf5e0137b6b2d99e78c64e8604522948881d78fd7781e2
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-state

```
show ap debug airwave-state [<def>]
```

Description

This command displays the configuration details and status of OmniVista 3600 Air Manager events associated with an OAW-IAP.

Example

The following example shows the output of the **show ap debug airwave-state** command:

```
<t1>
<e1>fc6520ad018ee6eb13bdc6b985e0fe6361bd37f7d25212a77e</e1>
<e2>Instant-C4:42:98</e2>
<e3></e3>
<e5>0.0.0.0</e5>
<e8>6.2.0.0-3.3.0.0_37557</e8>
<e60>Alcatel-Lucent</e60>
<e79>c3abebcd0138eb8997a5ee52abf418883ee1356fbf0befba81</e79>
<e63></e63>
<e64></e64>
</t1>
<t4>
<e25>test</e25>
<e26>2</e26>
<e27></e27>
<e28>64</e28>
<e29>1</e29>
<e30>2</e30>
</t4>
<t4>
<e25>test123</e25>
<e26>3</e26>
<e27></e27>
<e28>64</e28>
<e29>1</e29>
<e30>2</e30>
</t4>
<t2>
<e1>d8:c7:c8:c4:42:98</e1>
<e6>BE0000315</e6>
<e2>d8:c7:c8:c4:42:98</e2>
<e7>1.3.6.1.4.1.14823.1.2.34</e7>
<e18></e18>
<e5>10.17.88.59</e5>
<e15>10</e15>
<e16>129183744</e16>
<e17>71094272</e17>
<e13>1</e13>
<e14>257137</e14>
<e65>0</e65>
<t3>
<e1>d8:c7:c8:c4:29:88</e1>
<e23>48-</e23>
<e24>22</e24>
<e10>0</e10>
<e11>1</e11>
<e47>93</e47>
<e46>3</e46>
</t3>
```

```
<t3>
<e1>d8:c7:c8:c4:29:80</e1>
<e23>1</e23>
<e24>22</e24>
<e10>1</e10>
<e11>0</e11>
<e47>80</e47>
<e46>61</e46>
</t3>
</t2>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug airwave-stats

```
show ap debug airwave-stats [<def>]
```

Description

This command displays the configuration statistics associated with an OAW-IAP managed or monitored by the OmniVista 3600 Air Manager server.

Example

The following example shows the partial output of the **show ap debug airwave-stats** command:

```
<t7>
<e1>d8:c7:c8:3d:3a:83</e1>
<e25>test_wep</e25>
<e23>1</e23>
<e22>1</e22>
<e21>1</e21>
<e19>2</e19>
<e20>1</e20>
</t7>
<t7>
<e1>6c:f3:7f:a5:df:32</e1>
<e25>sw-san-rapng-13</e25>
<e23>153</e23>
<e22>1</e22>
<e21>1</e21>
<e19>1</e19>
<e20>1</e20>
</t7>
<t7>
<e1>d8:c7:c8:3d:46:d2</e1>
<e25>test_1x_term</e25>
<e23>48</e23>
<e22>1</e22>
<e21>1</e21>
<e19>1</e19>
<e20>2</e20>
</t7>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug am-config

```
show ap debug am-config
```

Description

This command displays the information required for debugging an OAW-IAP.

Example

The following example shows the partial output of **show ap debug am-config** command:

```
# show ap debug am-config
…
IDS General Configuration
-------------------------
Parameter                                 Value
---------                                 -----
Stats Update Interval                     60
Monitored Device Stats Update Interval    60
AP Inactivity Timeout                     20
Adhoc AP Inactivity Timeout               5
Valid AP Unseen Timeout                   7200
AP Unseen Timeout                         600
Adhoc AP Unseen Timeout                   180
STA Inactivity Timeout                    120
STA Unseen Timeout                        600
Min Potential AP Beacon Rate              25
Min Potential AP Monitor Time             2
Signature Quiet Time                      900
Containment Confirmation                  Enable
Wireless Containment                      deauth-only
Debug Wireless Containment                Disable
Wired Containment                         Disable
Wired Containment of AP's Adj MACs        Disable
Wired Containment of Suspected L3 Rogue   Disable
Mobility Manager RTLS                     Disable
AP Event Generation                       traps-only
Send Adhoc Info to Controller             Disable
WMS Client Monitoring                     none
Packet SNR Threshold                      0
Frame Type for RSSI calculation           ba pr dlow mgmt ctrl null
Max Monitored Devices                     1024
Max Unassociated Stations                 512
Unclassified AP Updates                   Disable
Unclassified STA Updates                  Disable
Unclassified Device Update Interval       60
Client Detection Mode                     normal
Valid 802.11b channel
Valid 802.11a channel
Config Wired MAC Table
-----------------------
mac
---
Valid OUIs
-----------
OUI
---
Valid and Protected SSIDs
--------------------------
SSID
----
```

```
8eb3ef208a601c64298ff2561359756
8.3-L2-ACL
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The configuration values of **Valid AP Unseen Timeout** was added to the output of this command.
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug anul-sta-entries

```
show ap debug anul-sta-entries
```

Description

This command shows the list of available BSSIDs on the OAW-IAP and the number of clients connected to the SSID.

Example

The following example shows the output of **show ap debug anul-sta-entries** command:

```
ANUL BSS State for radio 0
--------------------------
bssid              num_stas  data ready drops
-----              --------  ----------------
6C:F3:7F:EE:EF:50  0         0
6C:F3:7F:EE:EF:51  0         0
6C:F3:7F:EE:EF:52  0         0
6C:F3:7F:EE:EF:53  0         0
6C:F3:7F:EE:EF:54  0         0
6C:F3:7F:EE:EF:55  0         0
6C:F3:7F:EE:EF:56  0         0
6C:F3:7F:EE:EF:57  0         0
6C:F3:7F:EE:EF:58  0         0
6C:F3:7F:EE:EF:59  0         0
6C:F3:7F:EE:EF:5A  0         0
6C:F3:7F:EE:EF:5B  0         0
6C:F3:7F:EE:EF:5C  1         0
6C:F3:7F:EE:EF:5D  0         0

ANUL STA State
--------------
mac                bssid              aid  data ready  bss  Drops not Rdy  LAG  LAG drops
---                -----              ---  ----------  ---  -------------  ---  ---------
38:53:9C:6A:F7:6E  6C:F3:7F:EE:EF:5C  1    No          B    0              n/a  0
UAC   Tun Dest  Pkts to Tun  Pkts from Tun  Drops
---   --------  -----------  -------------  -----
null  null      0            0              31,0

ANUL BSS State for radio 1
--------------------------
bssid              num_stas  data ready drops
-----              --------  ----------------
6C:F3:7F:EE:EF:40  0         0
6C:F3:7F:EE:EF:41  0         0
6C:F3:7F:EE:EF:42  0         0
6C:F3:7F:EE:EF:43  0         0
6C:F3:7F:EE:EF:44  0         0
6C:F3:7F:EE:EF:45  0         0
6C:F3:7F:EE:EF:46  0         0
6C:F3:7F:EE:EF:47  0         0
6C:F3:7F:EE:EF:48  0         0
6C:F3:7F:EE:EF:49  0         0
6C:F3:7F:EE:EF:4A  0         0
6C:F3:7F:EE:EF:4B  0         0
6C:F3:7F:EE:EF:4C  0         0
6C:F3:7F:EE:EF:4D  0         0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug auth-trace-buf

```
show ap debug auth-trace-buf <count> [<mac>]
```

Description

This command displays the trace buffer for authentication events associated with the OAW-IAP. Use the output of this command to troubleshoot authentication errors. Include the <MAC> parameter to filter data by the MAC address of the client to view specific details.

Parameter	Description	Range	Default
`<count>`	Displays the count of trace buffer authentication events.	—	—
`<mac>`	Displays the authentication trace information for a specific MAC address.	—	—

Example

The following example shows the output of **show ap debug auth-trace-buf <count>** command:

```
Auth Trace Buffer
-----------------
May 10 13:05:09  station-up *  ac:81:12:59:5c:12 d8:c7:c8:3d:42:13 -   -  wpa2 psk aes
May 10 13:05:09  wpa2-key1  <- ac:81:12:59:5c:12 d8:c7:c8:3d:42:13 - 117
May 10 13:06:30  station-up *  08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 -   -  wpa2 psk aes
May 10 13:06:30  wpa2-key1  <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:06:30  wpa2-key2  -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:06:30  wpa2-key3  <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 151
May 10 13:06:30  wpa2-key4  -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 -  95
May 10 13:07:03  station-up *  08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 -   -  wpa2 psk aes
May 10 13:07:03  wpa2-key1  <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:07:03  wpa2-key2  -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:07:03  wpa2-key3  <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 151
May 10 13:07:03  wpa2-key4  -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 -  95
```

The command output displays the most recent ten trace buffer entries for the OAW-IAP. Each row in the output of this table may include some or all of the following information:

- A timestamp that indicates when the entry was created.
- The type of exchange that was made.
- The direction the packet was sent.
- The source MAC address.
- The destination MAC address.
- The packet number.
- The packet length.
- Additional information such as encryption and WPA type.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug ble-config

```
show ap debug ble-config
```

Description

This command displays the BLE configuration details and information such as the update interval for sending beacon management requests to the BMC, BLE token, and the operation mode.

Examples

The following example shows the output of the **show ap debug ble-config** command:

```
(host)# show ap debug ble-config
BLE Configuration
-----------------
Item                               Value
----                               -----
BLE Supported                      USB
BLE HW Type                        LS-BT1USB
Master IP                          10.65.66.14
Authorization Token
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJsIjo1NzQxMzEyNTI3NTY0ODAwLCJ0IjoxNDk4MTE0MTEzfQ.071Ud
a25uzup9w61wJUgsJVuC8qOrMBH3KHbwhlktPE
Endpoint URL                       https://edit.meridianapps.com/api/beacons/manage
BLE Ready                          Yes
Beacon Mgmt Update Intvl (in sec)  60
APB Info Update Intvl (in sec)     103 (3092/3010)
BLE debug log                      Enabled
Operational Mode                   Beaconing (APB: Beaconing)
AP USB Power Override              Disabled (-1)
Uplink Status                      Up (APB: Dynamic Console)
APB Connection Status              0
Last BLE Device Update Attempted   8c:8b:83:3d:72:6c
Last AP to APB Message Time        2017-09-06 03:07:59
Last Update to Endpoint Time       No Update Sent
Log Levels Available               { All(0xffff), Info(0x04), Warning(0x02), Error(0x01),
Ageout(0x08), BMReq(0x10), FW-Upgrade(0x20), FW-UpgradeErr(0x40), CfgUpdate(0x80),
CfgUpdateErr(0x100), Beacon(0x200), BcnTLV(0x400), BcnErr(0x800), APB(0x1000), AssetUpdate
(0x2000), None(0x00) }
Current Log Level                  { 0x61 : Error(0x0001), FW-Upgrade(0x0020), FW-UpgradeErr
(0x0040) }
Log Mac Filter                     None
Bundled BluOS Images               Bank A(/aruba/bin/UpgradeImage_Nano_OAD-A_1.2-19.bin) Bank
B(/aruba/bin/Beacon_Nano_OAD-B_1.2-19.bin)
-----------------
BLE IoT Transport Context Configuration #0 Config ID: 4
-------------------------------------------------------
Item           Value
----           -----
Endpoint Type  0 (Meridian Beacon Management)
Interval       30
Content        0 (Managed Beacons)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-APAP-324/325 OAW-IAP214/215 OAW-IAP224/225	Privileged EXEC mode

show ap debug ble-counters

```
show ap debug ble-counters
```

Description

This command displays a log showing the BLE counter details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-APAP-324/OAW-AP325 OAW-IAP214/OAW-IAP215 OAW-IAP224/OAW-IAP225	Privileged EXEC mode

show ap debug ble-daemon

```
show ap debug ble-daemon
```

Description

This command displays the BLE daemon log messages.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-APAP-324/OAW-AP325 OAW-IAP214/OAW-IAP215 OAW-IAP224/OAW-IAP225	Privileged EXEC mode

show ap debug ble-database

```
show ap debug ble-database
```

Description

This command shows the details of the AP beacon clusters associated with the master OAW-IAP.

Example

The following example shows the output of **show ap debug ble-database** command:

```
BLE APB Information
-------------------
AP Name            AP Group  BLE MAC            BLE Cur. Bank  BLE Opp. Bank
-------            --------  -------            -------------  -------------
                        AP Eth MAC         AP IP        Reported at          ConfigID  Status
                        ----------         -----        -----------          --------  ------
20:4c:03:0e:bf:01            f4:5e:ab:da:4b:1a  OAD B 1.2-30   OAD A 1.2-30
                        20:4c:03:0e:bf:01  10.65.18.23  2019-03-19 09:45:04   4         Current
70:3a:0e:c1:15:1a            80:30:dc:de:19:d1  OAD B 1.2-30   OAD A 1.2-30
                        70:3a:0e:c1:15:1a  10.65.18.26  2019-03-19 09:45:36   4         Current
38:17:c3:c7:ff:1e            64:cf:d9:24:44:08  OAD B 1.2-30   OAD A 1.2-30
                        38:17:c3:c7:ff:1e  10.65.18.21  2019-03-19 09:45:08   4         Current
94:b4:0f:c1:bf:62            7c:ec:79:6c:59:55  OAD B 1.2-30   OAD A 1.2-30
                        94:b4:0f:c1:bf:62  10.65.18.20  2019-03-19 09:43:57   4         Current
a8:bd:27:c9:84:6c            a8:bd:27:c9:84:6d  OAD A 0.0-0    OAD A 0.0-0
                        a8:bd:27:c9:84:6c  10.65.18.13  2019-03-19 09:44:27   4         Current
b4:5d:50:c3:18:92            20:91:48:31:c9:2b  OAD B 1.2-30   OAD A 1.2-30
                        b4:5d:50:c3:18:92  10.65.18.10  2019-03-19 09:44:52   4         Current
a8:bd:27:cf:f8:a2            50:f1:4a:f1:fe:1b  OAD B 1.2-30   OAD A 1.2-30
                        a8:bd:27:cf:f8:a2  10.65.18.30  2019-03-19 09:45:17   4         Current
38:17:c3:c0:56:a8            44:ea:d8:46:e6:67  OAD B 1.2-30   OAD A 1.2-30
                        38:17:c3:c0:56:a8  10.65.18.27  2019-03-19 09:44:23   4         Current
44:48:c1:cb:b6:bc            98:7b:f3:7b:46:5b  OAD B 1.2-30   OAD A 1.2-30
                        44:48:c1:cb:b6:bc  10.65.18.11  2019-03-19 09:45:32   4         Current
40:e3:d6:cf:f3:e2            88:c2:55:b9:62:41  OAD B 1.2-30   OAD A 1.2-30
                        40:e3:d6:cf:f3:e2  10.65.18.4   2019-03-19 09:45:00   4         Current
a8:bd:27:cf:fa:ee            50:f1:4a:f2:6c:18  OAD B 1.2-30   OAD A 1.2-30
                        a8:bd:27:cf:fa:ee  10.65.18.19  2019-03-19 09:45:52   4         Current
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except IAP-155	Privileged EXEC mode

show ap debug ble-database long

```
show ap debug ble-database long
```

Description

This command shows extended details of the AP beacon clusters associated with the master OAW-IAP.

Example

The following example shows the output of **show ap debug ble-database long** command:

```
BLE APB Information
-------------------
AP Name            AP Group  BLE MAC            BLE Cur. Bank  BLE Opp. Bank
-------            --------  -------            -------------  -------------
        AP Eth MAC         AP IP        Reported at          ConfigID  Status   Bank A UI Sta
        ----------         -----        -----------          --------  ------   -------------
        Bank B UI Sta
        -------------
20:4c:03:0e:bf:01            f4:5e:ab:da:4b:1a  OAD B 1.2-30   OAD A 1.2-30
        20:4c:03:0e:bf:01  10.65.18.23  2019-03-19 09:45:04   4         Current  no need
        no need
70:3a:0e:c1:15:1a            80:30:dc:de:19:d1  OAD B 1.2-30   OAD A 1.2-30
        70:3a:0e:c1:15:1a  10.65.18.26  2019-03-19 09:45:36   4         Current  no need
        no need
38:17:c3:c7:ff:1e            64:cf:d9:24:44:08  OAD B 1.2-30   OAD A 1.2-30
        38:17:c3:c7:ff:1e  10.65.18.21  2019-03-19 09:45:08   4         Current  no need
        no need
94:b4:0f:c1:bf:62            7c:ec:79:6c:59:55  OAD B 1.2-30   OAD A 1.2-30
        94:b4:0f:c1:bf:62  10.65.18.20  2019-03-19 09:45:56   4         Current  no need
        no need
a8:bd:27:c9:84:6c            a8:bd:27:c9:84:6d  OAD A 0.0-0    OAD A 0.0-0
        a8:bd:27:c9:84:6c  10.65.18.13  2019-03-19 09:44:27   4         Current  na
        na
b4:5d:50:c3:18:92            20:91:48:31:c9:2b  OAD B 1.2-30   OAD A 1.2-30
        b4:5d:50:c3:18:92  10.65.18.10  2019-03-19 09:44:52   4         Current  no need
        no need
a8:bd:27:cf:f8:a2            50:f1:4a:f1:fe:1b  OAD B 1.2-30   OAD A 1.2-30
        a8:bd:27:cf:f8:a2  10.65.18.30  2019-03-19 09:45:17   4         Current  no need
        no need
38:17:c3:c0:56:a8            44:ea:d8:46:e6:67  OAD B 1.2-30   OAD A 1.2-30
        38:17:c3:c0:56:a8  10.65.18.27  2019-03-19 09:46:10   4         Current  no need
        no need
44:48:c1:cb:b6:bc            98:7b:f3:7b:46:5b  OAD B 1.2-30   OAD A 1.2-30
        44:48:c1:cb:b6:bc  10.65.18.11  2019-03-19 09:45:32   4         Current  no need
        no need
40:e3:d6:cf:f3:e2            88:c2:55:b9:62:41  OAD B 1.2-30   OAD A 1.2-30
        40:e3:d6:cf:f3:e2  10.65.18.4   2019-03-19 09:46:14   4         Current  no need
        no need
a8:bd:27:cf:fa:ee            50:f1:4a:f2:6c:18  OAD B 1.2-30   OAD A 1.2-30
        a8:bd:27:cf:fa:ee  10.65.18.19  2019-03-19 09:45:52   4         Current  no need
        no need
Total AP BLE devices reported:11
Note:   'Status' column indicates whether information received for an AP's
        : BLE radio is 'Current' (message received in the last 10 minutes)
        : or 'OutOfDate' (message received more than last 10 minutes ago and/or AP might be down).
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except IAP-155	Privileged EXEC mode

show ap debug ble-firmware-upgrade-info

```
show ap debug ble-firmware-upgrade-info
```

Description

This command shows information about the upgrade status of the AP beacons associated with the master OAW-IAP.

Example

The following example shows the output of **show ap debug ble-firmware-upgrade-info** command:

```
-------------------------
IoT Firmware Upgrade Info
-------------------------
Item           Value
----           -----
BLE Supported  ONBOARD
BLE HW Type    BT-AP300H
MAC Address    c4:f3:12:1f:65:4a
APB UI:[0/NO_UPGRADE_REQD]:65535(0xffff) blks:0/0 rep:0  total:0(0x0)
APB UI:upg_b_status-next:0x00/ooo:0x00/next2:0x00/upg_
b:0x00/allrx:0x00/oooBlk:0x00/oooBlk:0x00/oooBlk:0x00
APB UI:upg_b_status_errs-inv_upg:0x00/inv_cmd:0x00/inv_op:0x00/buf_tl:0x00/good:0x00
APB UI:acks/ka-From APB:0x00/0x00 From app:0x00,0x00/0x00
APB UI Clock:Start:1970-01-01 00:00:00  End:1970-01-01 00:00:00  Current:2019-03-18 17:27:09
APB Info:Opp. Bank[A]:1.2-30 Reset Reason:0x2 BIM Ver:1.0-2
APB Info:Bank A[3]: CRC:0x5147 Shadow:0x5147 --- Bank B[3]: CRC:0xb41a Shadow:0xb41a
--------------------------
No remote device is currently being upgraded
--------------------------
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except IAP-155	Privileged EXEC mode

show ap debug ble-input-filter-stats

```
show ap debug ble-input-filter-stats
```

Description

This command displays the input-filter information in the BLE table.

Examples

The following example shows the output of the **show ap debug ble-input-filter-stats** command:

```
(Instant AP)# show ap debug ble-input-filter-stats
BLE Table Input Filter Stats
----------------------------
Input Filtering: Disabled
Filtered Devices
----------------
MAC Address  Last Updated
-----------  ------------
List Size:     0 entries
List Capacity: 64 entries
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-AP-303, OAW-AP-303P OAW-AP365/OAW-AP367 OAW-AP303H OAW-IAP304/OAW-IAP305 OAW-AP203R/OAW-AP203RP OAW-IAP207 OAW-IAP334/OAW-IAP335 OAW-IAP314/OAW-IAP315 OAW-APAP-324/OAW-IAP325 OAW-AP-344/OAW-AP-345 OAW-AP515 OAW-530 Series OAW-500 Series	Privileged EXEC mode

show ap debug ble-relay

```
show ap debug ble-relay [disp-attr | iot-profile | jobs [<profile>] | report [<profile>] |
tag-report [<profile>] | ws-log [<profile>]]
```

Description

This command displays the BLE process logs.

Examples

The following command displays the values of various settings related to an asset tag reporting:

```
(Instant AP)# show ap debug ble-relay disp-attr
WebSocket Connect Request               : Yes
WebSocket Connect Status                : 3
WebSocket Connection Established        : Yes
WebSocket LogLevel                      : 0
Tag Logging                             : Off
Websocket Address                       : beacons.meridianapps.com
WebSocket Host                          : beacons.meridianapps.com
WebSocket Path                          : /ingestion/ingest
=============================
Note: Websocket Loglevel List: Error (0x1), Warn (0x2), Notice (0x4), Info (0x8),
Debug (0x10), Parser (0x20), Header (0x40), Ext (0x80), Client (0x100), Latency (0x200).
```

The following command displays the BLE tag data for the OAW-IAP:

```
(Instant AP)# show ap debug ble-relay tag-report
Incoming Tag messages                   : 65102
Tag messages processed                  : 5114
Tag messages dropped                    : 59988
Tag messages WS queue success           : 5114
Tag messages WS queue unavailable       : 4359
Tag messages WS not connected           : 55629
Tag messages WS sent                    : 5114
```

The following command displays the WebSocket logs of the OAW-IAP:

```
(Instant AP)# show ap debug  ble-relay ws-log
WS: 2017-03-03 08:17:18: Initial logging level 65535
WS: 2017-03-03 08:17:18: Library version: 1.3 unknown-build-hash
WS: 2017-03-03 08:17:18:  LWS_MAX_HEADER_LEN: 1024
WS: 2017-03-03 08:17:18:  LWS_MAX_PROTOCOLS: 5
WS: 2017-03-03 08:17:18:  LWS_MAX_EXTENSIONS_ACTIVE: 3
WS: 2017-03-03 08:17:18:  SPEC_LATEST_SUPPORTED: 13
WS: 2017-03-03 08:17:18:  AWAITING_TIMEOUT: 5
WS: 2017-03-03 08:17:18:  SYSTEM_RANDOM_FILEPATH: '/dev/urandom'
WS: 2017-03-03 08:17:18:  LWS_MAX_ZLIB_CONN_BUFFER: 65536
WS: 2017-03-03 08:17:18:  Started with daemon pid 0
WS: 2017-03-03 08:17:18:  static allocation: 4448 + (12 x 1024 fds) = 16736 bytes
WS: 2017-03-03 08:17:18:  canonical_hostname = 10.65.65.238
WS: 2017-03-03 08:17:18:   Protocol: http-only
WS: 2017-03-03 08:17:18: libwebsocket_client_connect: direct conn
WS: 2017-03-03 08:17:18: libwebsocket_client_connect_2
WS: 2017-03-03 08:17:18: libwebsocket_client_connect_2: address tags.meridianapps.com
WS: 2017-03-03 08:17:48: Unable to get host name from tags.meridianapps.com
WS: 2017-03-03 08:18:04: Initial logging level 65535
WS: 2017-03-03 08:18:04: Library version: 1.3 unknown-build-hash
WS: 2017-03-03 08:18:04:  LWS_MAX_HEADER_LEN: 1024
WS: 2017-03-03 08:18:04:  LWS_MAX_PROTOCOLS: 5
WS: 2017-03-03 08:18:04:  LWS_MAX_EXTENSIONS_ACTIVE: 3
WS: 2017-03-03 08:18:04:  SPEC_LATEST_SUPPORTED: 13
```

```
WS: 2017-03-03 08:18:04:  AWAITING_TIMEOUT: 5
WS: 2017-03-03 08:18:04:  SYSTEM_RANDOM_FILEPATH: '/dev/urandom'
WS: 2017-03-03 08:18:04:  LWS_MAX_ZLIB_CONN_BUFFER: 65536
WS: 2017-03-03 08:18:04:  Started with daemon pid 0
WS: 2017-03-03 08:18:04:  static allocation: 4448 + (12 x 1024 fds) = 16736 bytes
WS: 2017-03-03 08:18:04:  canonical_hostname = 10.65.65.238
WS: 2017-03-03 08:18:04:   Protocol: http-only
WS: 2017-03-03 08:18:04: libwebsocket_client_connect: direct conn
WS: 2017-03-03 08:18:04: libwebsocket_client_connect_2
WS: 2017-03-03 08:18:04: libwebsocket_client_connect_2: address tags.meridianapps.com
WS: 2017-03-03 08:18:34: Unable to get host name from tags.meridianapps.com
```

The following command displays the IoT profile details:

```
(Instant AP)# show ap debug ble-relay iot-profile
---------------------------Profile[test]---------------------------
EndpointURL                             : https://edit.meridianapps.com/api/beacons/manage
EndpointType                            : Meridian Beacon Management
PayloadContent                          : Managed Beacons
TransportInterval                       : 300s
Token                                   :
MzkxMTZlMWYtYTgzYS00YWUxLTkzYWEtYjQyNzE1MGMyMjAxOjBiZWJjYWViLTRjNjItNGEwNC1hMGIyLWYzZTM5ZDFlN
GVkNg==
TransportContext                        : Spawn
SpawnThread                             : 4100
TransType                               : Https(Meridian Beacon Management-Managed Beacons)
```

The following command displays the BLE relay job queue status:

```
(Instant AP)# show ap debug ble-relay jobs
---------------------------Profile[test]---------------------------
Pending Jobs
------------
Slot#  AP IP      Payload Size  Status     Last Updated
-----  -----      ------------  ------     ------------
0    127.0.0.1  226           DO_POST    1506485394
1    127.0.0.1  226           SUBMITTED  1506485394
2    127.0.0.1  226           REUSE      1506485394
3    127.0.0.1  226           REUSE      1506485394
4    127.0.0.1  226           REUSE      1506485394
5    127.0.0.1  226           REUSE      1506485394
6    127.0.0.1  226           REUSE      1506485394
7    127.0.0.1  226           REUSE      1506485394
8    127.0.0.1  226           REUSE      1506485394
9    127.0.0.1  226           REUSE      1506485394
10    127.0.0.1  226           REUSE      1506485394
...
|                Total |     Last 10s |     Last 60s |    Last 600s |   Last 3600s |
Slots requested      |                 6413 |            2 |           12 |         3220 |
     2864 |
Slots utilized       |                 6244 |            2 |           12 |         3170 |
     2814 |
Slots unavailable    |                  169 |            0 |            0 |           50 |
       50 |
Slots recycled       |                    0 |            0 |            0 |            0 |
        0 |
Num. stats rollover  |                    0
```

The following command displays the BLE relay report:

```
(Instant AP)# show ap debug ble-relay report
---------------------------Profile[test]---------------------------
Sent report to Endpoint server (2s) ago: success 6059, failed 301, last curl result code 1
Timeout(-1):20 Jobs added: 6360
```

```
Request to Server:
Last Curl logs:
*   Trying 54.255.165.205...
* TCP_NODELAY set
* Connected to edit.meridianapps.com (54.255.165.205) port 443 (#0)
* SSL connected
> POST /api/beacons/manage HTTP/1.1
Host: edit.meridianapps.com
Content-Type: application/json
Authorization: MERIDIAN
MzkxMTZlMWYtYTgzYS00YWUxLTkzYWEtYjQyNzE1MGMyMjAxOjBiZWJjYWViLTRjNjItNGEwNC1hMGIyLWYzZTM5ZDFlN
GVkNg==
Accept: application/vnd.meridian.v1+json
Content-Length: 10559
Expect: 100-continue
< HTTP/1.1 100 Continue
* We are completely uploaded and fine
< HTTP/1.1 200 OK
< Date: Wed, 27 Sep 2017 04:05:22 GMT
< Content-Type: application/json; application/vnd.meridian.v1+json;
< Content-Length: 112
* Connection #0 to host edit.meridianapps.com left intact
Server response:
{"next_sync":60,"updates":[{"mac":"987BF358E010","firmware":{"B":
{"url":null,"version":""}},"type":"location"}]}
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-APAP-324/325 OAW-IAP214/215 OAW-IAP224/225	Privileged EXEC mode

show ap debug ble-table

```
show ap debug ble-table [all | assettags | generic | mac-addr <mac>]
```

Description

This command displays beacon details for the BLE devices detected by the OAW-IAP.

Example

The following example shows the output of the **show ap debug ble-table** command:

```
BLE Device Table
----------------
MAC  HW_Type  FW_Ver  Flags  Status  Batt(%)  RSSI  Major#  Minor#  UUID  Tx_Power  Last
Update  Uptime
---  -------  ------  -----  ------  -------  ----  ------  ------  ----  --------  ---------
--  ------
Total beacons:0
Note: Battery level for LS-BT1USB devices is indicated as USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Status Flags:L:AP's local beacon; I:iBeacon; A: Aruba Beacon; H: Aruba HiPower Beacon
:U:Image Upgrade Pending
```

The following example shows the output of the **show ap debug ble-table assettags** command:

```
(host)# show ap debug ble-table assettags
BLE Device Table [Asset Tags]
------------------------------
MAC                HW_Type  FW_Ver          Flags   Status  Batt(%)  RSSI  Asset_Tag_Id
Last Update  Uptime
---                -------  ------          -----   ------  -------  ----  ------------    --
---------  ------
a0:e6:f8:38:1b:46  AT-BT10  OAD E 7.5-7     0x0001  T       82       -81   0000-0000-0000
12s          2h:50m:15s
a0:e6:f8:2c:09:b8  AT-BT10  OAD E 7.14-254  0x0001  T       100      -78   0000-0000-0000
21s          2h:57m:30s
a0:e6:f8:38:1b:4c  AT-BT10  OAD E 7.5-7     0x0001  T       87       -91   0000-0000-0000  1s
          2h:50m:0s
a0:e6:f8:38:11:0e  AT-BT10  OAD E 7.5-7     0x0001  T       100      -75   0000-0000-0000  4s
          1h:47m:0s
a0:e6:f8:2c:0e:1a  AT-BT10  OAD E 7.14-254  0x0001  T       100      -71   0000-0000-0000
16s          19m:30s
a0:e6:f8:2c:0d:52  AT-BT10  OAD E 7.14-254  0x0001  T       100      -82   0000-0000-0000
12s          23h:59m:30s
a0:e6:f8:38:1d:54  AT-BT10  OAD E 7.5-7     0x0001  T       100      -76   0000-0000-0000
25s          1h:46m:30s
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-APAP-324/325 OAW-IAP214/215 OAW-IAP224/225	Privileged EXEC mode

show ap debug ble-update-status

```
show ap debug ble-update-status
```

Description

This command shows information on pending configuration updates for AP beacons and Bluetooth devices associated with the OAW-IAP.

Usage Guidelines

Use this command to view the status of configuration updates waiting to be applied to AP beacons and Bluetooth devices associated with the OAW-IAP. The table is cleared once configuration changes are applied.

Example

The following example shows the output of **show ap debug ble-update-status** command:

```
(Instant AP) #show ap debug ble-update-status ap-name openble325
BLE Device Table
----------------
BLE Device MAC     Attribute  Actual/Observed                       Desired/Pending
--------------     ---------  ---------------                       ---------------
6c:ec:eb:40:3d:da  Tx Power   15                                    14
6c:ec:eb:40:3d:da  Major      5000                                  4000
6c:ec:eb:40:3d:da  Minor      5                                     4
6c:ec:eb:40:3d:da  UUID       5152554E-F99B-4A3B-86D0-947070693A78  4152554E-F99B-4A3B-86D0-
                                                                            947070693A78
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug client-match

```
show ap debug client-match <radio>
```

Description

This command displays the information about the client match configuration status on anOAW-IAP radio interface.

Parameter	Description	Range	Default
`<radio>`	Allows you to specify the ID number of the radio (for example, 0 or 1) for which you want to view client match configuration status.	—	—

Example

The following example shows the output of **show ap debug client-match <radio ID>** command:

```
Client Match Status:: RUNNING
Associated:0, Threshold:MAX
Leaving:0, Coming:0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug client-mgmt-counters

```
show ap debug client-mgmt-counters
```

Description

This command shows the client management packet counters for clients associated with the OAW-IAP.

Example

The following example shows the output of **show ap debug client-mgmt-counters** command:

```
Counters
--------
Name                                                                  Value
----                                                                  -----
LED Update                                                            13
Tunnel VLAN Membership                                                18
Tunnel DACL                                                           13
AP Radio and Client Stats Update                                      3764
STA Up/Down Protobuf Requests                                         38
3233                                                                  1
ARM Update                                                            3786
ARM Propagate                                                         678
ARM Neighbor Assigned                                                 14
802.11 Management Message                                             4
STM Restart Notification to Auth                                      1
AP Ethernet Stats Update Message                                      3725
AP Stats Update Message                                               1742
sapcp                                                                 24
Associations Dropped Due to Auth Throttling                           0
PubSub Messages Rcvd                                                  1141
User Mon Messages                                                     0
Auth .1x Queue: High, Pending                                         70, 0
Reg timer calls                                                       3277
BSS publish Failures                                                  0
Tunnel Timeouts                                                       24
Unreg/Wipeout Requests                                                24 17
Auth Resp for unknown sap                                             0
Auth enet Resp Tout                                                   0
VAP Wipeout Requests                                                  0
SOS Rx Msg Count: tunop ctrl dtun_data tun_data non_dtun misc         0 40 0 2 0 0 0 0 0 0 0 0
Received Client Ageout Messages from APs)                             0
Received stale Entries                                                0
Received stale Entries in Deauth (Deauths from clients)               0
Processed stale Entries in Deauth                                     0
Stale entry error - BSS not found                                     0
Stale entry error - STA not found in Deauth                           0
Stale entry error - failed to clear STA in Deauth                     0
Stale entry error - Deauth bad length                                 0
Stale entry error - special handling                                  0
Sta down: total flag_unmatch not_assoc papi_send papi_ok papi_fail    16 0 0 8 8 0
Sta up: total flag_unmatch not_assoc papi_send papi_ok papi_fail      22 11 0 11 11 0
AMSDU Updates sent to SOS from STM                                    1
Invalid tunnel-id (0)                                                 0
HBT tunnel not found on timeout                                       0
AID-MAC mismatch                                                      0
Stats for unknown AP                                                  0
Channel stats for unknown AP                                          0
Channel stats for unknown radio                                       0
Missing SAP for Radio                                                 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug client-stats

`show ap debug client-stats {<mac>} | {<bssid>}`

Description

This command displays detailed statistics for packets received from and transmitted to the specified client of the OAW-IAP.

Parameter	Description	Range	Default
`<mac>`	Displays data based on the client MAC address.	—	—
`<bssid>`	Displays data based on the client's BSSID.	—	—

Example

The following example displays the output of the **show ap debug client-stats <mac> <bssid>** command. displays statistics for packets received from and transmitted to the specified client:

```
Station Stats
-------------
Parameter            Value
----------------                 General Per-radio Statistics
Last TX Antenna                  0
Last RX Antenna                  0
----------------                 Transmit Specific Statistics
Tx Frames Rcvd                   948
Tx Frames Dropped                200
Tx Frames Transmitted            948
Tx Bytes Rcvd                    0
Tx Bytes Transmitted             287317
Tx Time Frames Rcvd              349004
Tx Time Frames Dropped           15376
Tx Time Frames Transmitted       333628
Tx PS Unicast                    0
Tx Success With Retry            88
Tx Multiple Retries              0
Tx Mgmt Frames                   236
Tx Probe Responses               121
Tx Data Transmitted Retried      74
Tx Data Transmitted              1027
Tx Data Frames                   948
Tx Data Bytes Transmitted        255754
Tx Data Bytes                    79315
Tx Time Data Transmitted         260084
Tx Time Data dropped             15376
Tx Time Data                     275460
Tx Time Data (Ideal)             97360
Client Health Samples            923
Tx DMO Replicated                0
Tx CTS Frames                    0
Tx Powersave Queue Timeouts      0
Tx Dropped After Retry           0
Tx Dropped No Buffer             0
Tx Missed ACKs                   0
Tx Long Preamble                 367
Tx Short Preamble                0
Tx EAPOL Frames                  18
TX STBC Frames                   0
TX LDPC Frames                   0
TX OFDMA Frames                  0
Tx AGGR Good                     860
Tx AGGR Unaggr                   141
Tx AGGR Retry                    60
Tx Data Priority [BE]            1027
Tx Data Frames  12 Mbps  (Mon)   18
Tx Data Frames  24 Mbps  (Mon)   883
Tx Data Frames  36 Mbps  (Mon)   99
Tx Data Frames  54 Mbps  (Mon)   8
Tx Data Frames  72 Mbps  (Mon)   0
Tx Data Frames 108 Mbps  (Mon)   11
Tx Data Frames 300 Mbps  (Mon)   8
Tx Data Frames 450 Mbps  (Mon)   0
Tx Data Frames 1300 Mbps  (Mon)  0
Tx Data Frames 1300 Mbps+ (Mon)  0
Tx Data Bytes   12 Mbps  (Mon)   4577
Tx Data Bytes   24 Mbps  (Mon)   216157
Tx Data Bytes   36 Mbps  (Mon)   26594
Tx Data Bytes   54 Mbps  (Mon)   2177
Tx Data Bytes   72 Mbps  (Mon)   0
Tx Data Bytes  108 Mbps  (Mon)   3915
Tx Data Bytes  300 Mbps  (Mon)   2334
Tx Data Bytes  450 Mbps  (Mon)   0
Tx Data Bytes  1300 Mbps  (Mon)  0
Tx Data Bytes  1300 Mbps+ (Mon)  0
Tx 6 Mbps                        367
Tx HT 13 Mbps                    376
Tx HT 14.4 Mbps                  491
Tx HT 19.5 Mbps                  16
Tx HT 26 Mbps                    54
Tx HT 28.9 Mbps                  45
Tx HT 39 Mbps                    2
Tx HT 52 Mbps                    6
Tx HT 78 Mbps                    8
Tx HT 104 Mbps                   3
Tx HT 117 Mbps                   3
Tx HT 130 Mbps                   5
Tx WMM [BE]                      1027
Tx WMM [BE] Dropped              79
Tx UAPSD OverflowDrop            0
Tx AMSDU pkt count               0
Tx EAPOL Frames Rcvd             0
Tx EAPOL Frames Dropped          0
Tx Data Frames MCS 0 :           885
Tx Data Frames MCS 1 :           93
Tx Data Frames MCS 2 :           18
Tx Data Frames MCS 3 :           12
Tx Data Frames MCS 4 :           8
Tx Data Frames MCS 5 :           3
Tx Data Frames MCS 6 :           3
Tx Data Frames MCS 7 :           5
Tx Data Frames Legacy :          18
Tx Data Frames MCS :             1009
Tx Data Frames NSS1 :            40
Tx Data Frames NSS2 :            987
Tx Data Frames GI(0.4) :         536
Tx Data Frames GI(0.8) :         473
Tx Data Frames BW 20 :           1027
----------------                 Receive Specific Statistics
Rx Last SNR                      52
Rx Last SNR CTL0                 52
Rx Last SNR CTL1                 52
Rx Last SNR CTL2                 98
Rx Last SNR EXT0                 52
Rx Last SNR EXT1                 52
Rx Last SNR EXT2                 98
Rx Last ACK SNR                  61
Rx Frames Received               5701
Rx Data Frames Retried           91
Rx Data Frames                   1860
Rx Data Bytes                    359623
Rx Time Data                     155876
Rx Duplicate Frames              0
Rx Null Data Frames              0
Rx Mgmt Frames                   236
Rx Frames To Me                  5701
Rx Bytes To Me                   476305
Rx Time To Me                    404264
Rx PS Poll Frames                0
Rx EAPOL Frames                  16
Rx STBC Frames                   0
Rx LDPC Frames                   0
Rx Data Priority [BE]            1860
Rx Data Frames  12 Mbps  (Mon)   29
Rx Data Frames  54 Mbps  (Mon)   1275
Rx Data Frames 108 Mbps  (Mon)   556
Rx Data Frames 300 Mbps  (Mon)   0
Rx Data Frames 450 Mbps  (Mon)   0
Rx Data Frames 1300 Mbps  (Mon)  0
Rx Data Frames 1300 Mbps+ (Mon)  0
Rx Data Bytes   12 Mbps  (Mon)   3825
Rx Data Bytes   54 Mbps  (Mon)   244496
Rx Data Bytes  108 Mbps  (Mon)   111302
Rx Data Bytes  300 Mbps  (Mon)   0
Rx Data Bytes  450 Mbps  (Mon)   0
Rx Data Bytes  1300 Mbps  (Mon)  0
Rx Data Bytes  1300 Mbps+ (Mon)  0
Rx HT 6.5 Mbps                   1
Rx HT 13 Mbps                    22
Rx HT 19.5 Mbps                  44
Rx HT 21.7 Mbps                  39
Rx HT 26 Mbps                    55
Rx HT 28.9 Mbps                  85
Rx HT 39 Mbps                    41
Rx HT 43.3 Mbps                  728
Rx HT 52 Mbps                    182
Rx HT 57.8 Mbps                  529
Rx HT 65 Mbps                    27
Rx WMM [BE]                      1860
Max Negotiated Tx Rate (Kbps)    144400
SLB: Probe Requests Sent         0
SLB: Probe Responses Sent        0
SLB: Probe Requests Received     0
SLB: Probe Response Received     0
SLB: Probe Requests Ignored      0
SLB: Auth Requests Refused       0
SLB: Assoc Requests Refused      0
Hotspot2 Action Frame From STM   0
Hotspot2 Action TX Prepare       0
Hotspot2 Action Skip Crypto      0
Hotspot2 Action Process Action   0
Hotspot2 Action TXOP ok          0
Hotspot2 Action DMA ok           0
```

```
Hotspot2 Action Frame Drop 1      0
Hotspot2 Action Frame Drop 2      0
Hotspot2 Action Frame Drop 3      0
Hotspot2 Action Frame Drop 4      0
Hotspot2 Action Frame Drop 5      0
Hotspot2 Action Frame Drop 6      0
Hotspot2 Action Frame Drop 7      0
Hotspot2 Action Frame Drop 8      0
Smart Antenna Status              0
Smart Antenna Last-train time     0
Smart Antenna Re-train by time    0
Smart Antenna Re-train by PER     0
Smart Antenna Current Pattern     0
```

The output of this command includes the following information:

Column	Description
`Frames Rcvd For TX`	Shows the number of frames received for transmission.
`Tx Frames Dropped`	Shows the number of transmission frames that were dropped.
`Frames Transmitted`	Shows the number of frames successfully transmitted.
`Success With Retry`	Shows the number of frames that were transmitted after being retried.
`Tx Mgmt Frames`	Shows the number of management frames transmitted.
`Tx Probe Responses`	Shows the number of transmitted probe responses.
`Tx Data Frames`	Shows the number of transmitted data frames.
`Tx CTS Frames`	Shows the number of CTS frames transmitted.
`Dropped After Retry`	Shows the number of frames dropped after an attempted retry.
`Dropped No Buffer`	Shows the number of frames dropped because the buffer of the OAW-IAP was full.
`Missed ACKs`	Shows the number of missed acknowledgments.
`Long Preamble`	Shows the number of frames sent with a long preamble.
`Short Preamble`	Shows the number of frames sent with a short preamble.
`Tx EAPOL Frames`	Shows the number of EAPOL frames transmitted.
`Tx <n> Mbps`	Shows the number of frames transmitted at <n> Mbps, where <n> is a value between 6 and 300.
`Tx WMM`	Shows the number of WMM packets transmitted for the following access categories. If the OAW-IAP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. **`Tx WMM [BE]`**: Best Effort **`Tx WMM [BK]`**: Background **`Tx WMM [VO]`**: VoIP **`Tx WMM [VI]`**: Video
`UAPSD OverflowDrop`	Shows the number of packets dropped due to U-APSD overflow.
`Last SNR`	Indicates the last recorded SNR.

Column	Description
`Last SNR CTL0`	Indicates the SNR for the last received data packet on the primary (control) channel 0. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last SNR CTL1`	Indicates the SNR for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for OAW-IAPs operating in 40 Mhz mode.
`Last SNR CTL2`	Indicates the SNR for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last ACK SNR`	Indicates the SNR for the last received ACK packet.
`Last ACK SNR CTL0`	Indicates the SNR for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last ACK SNR CTL1`	Indicates the SNR for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last ACK SNR CTL2`	Indicates the SNR for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last ACK SNR EXT0`	Indicates the SNR for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Last ACK SNR EXT1`	Indicates the SNR for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for OAW-IAPs operating in 40 MHz mode.
`Frames Received`	Shows the number of frames received.
`Rx Data Frames`	Shows the number of data frames received.
`Null Data Frames`	Shows the number of null data frames received.
`Rx Mgmt Frames`	Shows the number of management frames received.
`PS Poll Frames`	Shows the number of power save poll frames received.
`Rx <n> Mbps`	Shows the number of frames received at <n> Mbps, where <n> is a value between 6 and 300.
`Tx WMM`	Shows the number of WMM packets transmitted for the following access categories. If the OAW-IAP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. **`Tx WMM [BE]`:** Best Effort **`Tx WMM [BK]`:** Background **`Tx WMM [VO]`:** VoIP **`Tx WMM [VI]`:** Video

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug client-table

```
show ap debug client-table
```

Description

This command shows the clients associated with an OAW-IAP.

Example

The following example shows the output of **show ap debug client-table** command:

```
Client Table
------------
MAC               ESSID     BSSID             Assoc_State  HT_State  AID  PS_State        ---
-----              -----   -----------     --------  ---  --------
08:ed:b9:e1:51:7d example1  d8:c7:c8:3d:42:12 Associated   WSsM     0x1   Awake

UAPSD          Tx_Pkts  Rx_Pkts PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate  Last_ACK_SNR
-----           ------   ------- -------  ----------  -------  -------  ------------
(0,0,0,0,N/A,0)  101      12888    0        0          300      300       45
 -----------
 Last_Rx_SNR TX_Chains   Tx_Timestamp             Rx_Timestamp         MFP Status (C,R)
---------   ------------ ----------             ----------------       ----------------
  50          3[0x7]  Sun May 12 07:41:25 2013  Sun May 12 07:42:13 2013  (0,0)

UAPSD:(VO,VI,BK,BE,Max SP,Q Len)
HT Flags: A - LDPC Coding; W - 40Mhz; S - Short GI HT40; s - Short GI HT20
D - Delayed BA; G - Greenfield; R - Dynamic SM PS
Q - Static SM PS; N - A-MPDU disabled; B - TX STBC
b - RX STBC; M - Max A-MSDU; I - HT40 Intolerant
```

The output of this command includes the following information:

Column	Description
`MAC`	Indicates the MAC address of the OAW-IAP.
`ESSID`	Indicates the ESSID used by the client. An ESSID is a user-defined name for a wireless network.
`BSSID`	Filters the OAW-IAP Config table by BSSID. The BSSID is usually the MAC address of the OAW-IAP.
`Assoc_State`	Shows whether or not the client is currently authorized and/or associated with the OAW-IAP.
`HT_State`	Shows the client's high-throughput (802.11n) transmission type: none: OAW-IAP is a legacy access point that does not support the 802.11n standard. ■ 20Mhz: A high-throughput OAW-IAPs using a single 20 Mhz channel. ■ 40Mhz: A high-throughput OAW-IAPs using two 20 Mhz channels.
`AID`	Indicates the 802.11 association ID. A client receives a unique 802.11 association ID when it associates to anOAW-IAP.
`UAPSD`	Shows the following values for UAPSD in comma-separated format: VO, VI, BK, BE, Max SP, Q Len.

Column	Description
	VO: If 1, UAPSD is enabled for the VoIP AC. If UAPSD is disabled for this AC, this value is 0. VI: If 1, UAPSD is enabled for the Video AC. If UAPSD is disabled for this AC, this value is 0. BK: If 1, UAPSD is enabled for the Background AC. If UAPSD is disabled for this AC, this value is 0. BE: If 1, UAPSD is enabled for the Best Effort AC. If UAPSD is disabled for this AC, this value is 0. Max SP: The maximum service period is the number of frame sent per trigger packet. This value is value can be 0, 2, 4 or 8. Q Len: The number of frames currently queued for the client, from 0 to 16 frames.
`Tx_Pkts`	Shows the number of packets transmitted to the client.
`Rx_Pkts`	Shows the number of packets received from the client.
`PS_Qlen`	Shows power save queue length, in bytes.
`Tx_Rate`	Shows the packet rate from the OAW-IAP to client.
`Rx_Rate`	Show the packet rate from the client to OAW-IAP.
`Tx_Retries`	Shows the number of packets that the client had to resend due to an initial transmission failure.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug client-frame-history

```
show ap debug client-frame-history {client-mac <mac-address} | {radio {0|1}}
```

Description

This command displays the latest RSSI information about the incoming packets for a client connected to an OAW-IAP. Use this command to verify if the RSSI information is frequently updated. If the RSSI information is not frequently updated, a client may be steered to an improper new OAW-IAP in the cluster.

Parameter	Description	Range	Default
`client-mac <mac-address>`	Allows you to filter the output based on a client MAC address.	—	—
`radio {0|1}`	Allows you to specify the OAW-IAP radio ID to which the client is associated.	—	—

Example

The following example shows the output of **show ap debug client-frame-history** command:

```
Frame History count: 5
Client Frame History Report
---------------------------
Received Time RSSI Previous RSSI
------------- ---- -------------
1s 42 42
1s 42 42
1s 42 42
1s 42 42
1s 42 42
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug core-info

```
show ap debug core-info
```

Description

This command displays the core file history running on an OAW-IAP.

Example

The following example shows the output of the **show ap debug core-info** command:

```
325#f0:5c:19:ca:1a:92# show ap debug core-info
The build information:
Compiled on 2017-11-14 at 07:27:21 UTC (build 62273) by p4build
This time core files:
-----------------------------------------------------------
Previous core files:
-----------------------------------------------------------
core.20171122_182111.f05c19ca1a92.meshd.4193.Hercules_62273.1.tgz
core.20171122_182213.f05c19ca1a92.meshd.8525.Hercules_62273.2.tgz
core.20171122_182303.f05c19ca1a92.meshd.8793.Hercules_62273.3.tgz
core.20171122_182352.f05c19ca1a92.meshd.8974.Hercules_62273.4.tgz
core.20171122_182442.f05c19ca1a92.meshd.9084.Hercules_62273.5.tgz
core.20171122_182532.f05c19ca1a92.meshd.9280.Hercules_62273.6.tgz
core.20171122_182621.f05c19ca1a92.meshd.9460.Hercules_62273.7.tgz
core.20171122_182711.f05c19ca1a92.meshd.9647.Hercules_62273.8.tgz
core.20171122_184400.f05c19ca1a92.sapd.4091.Hercules_62273.9.tgz
core.20171123_145733.f05c19ca1a92.meshd.4193.Hercules_62273.10.tgz
core.20171123_145822.f05c19ca1a92.meshd.17677.Hercules_62273.11.tgz
core.20171123_145912.f05c19ca1a92.meshd.18013.Hercules_62273.12.tgz
core.20171123_150001.f05c19ca1a92.meshd.18355.Hercules_62273.13.tgz
core.20171123_150051.f05c19ca1a92.meshd.18694.Hercules_62273.14.tgz
core.20171123_150140.f05c19ca1a92.meshd.19028.Hercules_62273.15.tgz
Core file URL: http://10.65.120.185/core/
325#f0:5c:19:ca:1a:92#
```

The output of this command provides the following information:

Column	Description
`This time core files`	Indicates the core file history of the current running session.
`Previous core files`	Indicates the core file history of the previous session.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug crash-info

```
show ap debug crash-info
```

Description

This command displays log information for an OAW-IAP that crashed. The stored crash information is cleared from the flash after the OAW-IAP reboots.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug curpower

```
show ap debug curpower [radio]
```

Description

This command displays the dump status of the Tx power stored in the static ROM.

Parameter	Description	Range	Default
`radio`	Indicates the polarization value of the radio channel.	0 or 1	0

Example

The following example displays the output of the **show ap debug curpower** command:

```
Power Control:          On, HW
Current Channel:        36/80
BSS Channel:            36/80
BSS Local Max:          0.0 dBm
BSS Local Constraint:   0.0 dB
Channel Width:          80MHz
User Target:            10.50 dBm
SROM Antgain 2G:        0.0 dB
SROM Antgain 5G:        4.50 dB
SAR:                    -
Open loop:              Off
Current rate:           [VHT9SS3] vht mcs 9 Nss 3 Tx Exp 0 BW 80
Regulatory Limits:
Rate                  Chains 20in80 40in80 80MHz
DSSS                    1     -      -      -
OFDM                    1     30.0   30.0   30.0
MCS0_7                  1     30.0   30.0   30.0
VHT8_9SS1               1     30.0   30.0   30.0
DSSS_MULTI1             2     -      -      -
OFDM_CDD1               2     30.0   30.0   30.0
MCS0_7_CDD1             2     30.0   30.0   30.0
VHT8_9SS1_CDD1          2     30.0   30.0   30.0
MCS0_7_STBC             2     30.0   30.0   30.0
VHT8_9SS1_STBC          2     30.0   30.0   30.0
MCS8_15                 2     30.0   30.0   30.0
VHT8_9SS2               2     30.0   30.0   30.0
DSSS_MULTI2             3     -      -      -
OFDM_CDD2               3     30.0   30.0   30.0
MCS0_7_CDD2             3     30.0   30.0   30.0
VHT8_9SS1_CDD2          3     30.0   30.0   30.0
MCS0_7_STBC_SPEXP1      3     30.0   30.0   30.0
VHT8_9SS1_STBC_SPEXP1   3     30.0   30.0   30.0
MCS8_15_SPEXP1          3     30.0   30.0   30.0
VHT8_9SS2_SPEXP1        3     30.0   30.0   30.0
MCS16_23                3     30.0   30.0   30.0
VHT8_9SS3               3     30.0   30.0   30.0
OFDM_TXBF1              2     30.0   30.0   30.0
MCS0_7_TXBF1            2     30.0   30.0   30.0
VHT8_9SS1_TXBF1         2     30.0   30.0   30.0
MCS8_15_TXBF0           2     30.0   30.0   30.0
OFDM_TXBF2              3     30.0   30.0   30.0
MCS0_7_TXBF2            3     30.0   30.0   30.0
VHT8_9SS1_TXBF2         3     30.0   30.0   30.0
MCS8_15_TXBF1           3     30.0   30.0   30.0
```

```
VHT8_9SS2_TXBF1         3     30.0   30.0   30.0
MCS16_23_TXBF0          3     30.0   30.0   30.0
Core Index:             0
Board Limits:
Rate                  Chains 20in80 40in80 80MHz
DSSS                    1     -      -      -
OFDM                    1     10.50  10.50  10.50
MCS0_7                  1     10.50  10.50  10.50
VHT8_9SS1               1     10.50  10.50  10.50
DSSS_MULTI1             2     -      -      -
OFDM_CDD1               2     10.50  10.50  10.50
MCS0_7_CDD1             2     10.50  10.50  10.50
VHT8_9SS1_CDD1          2     10.50  10.50  10.50
MCS0_7_STBC             2     10.50  10.50  10.50
VHT8_9SS1_STBC          2     10.50  10.50  10.50
MCS8_15                 2     10.50  10.50  10.50
VHT8_9SS2               2     10.50  10.50  10.50
DSSS_MULTI2             3     -      -      -
OFDM_CDD2               3     10.50  10.50  10.50
MCS0_7_CDD2             3     10.50  10.50  10.50
VHT8_9SS1_CDD2          3     10.50  10.50  10.50
MCS0_7_STBC_SPEXP1      3     10.50  10.50  10.50
VHT8_9SS1_STBC_SPEXP1   3     10.50  10.50  10.50
MCS8_15_SPEXP1          3     10.50  10.50  10.50
VHT8_9SS2_SPEXP1        3     10.50  10.50  10.50
MCS16_23                3     10.50  10.50  10.50
VHT8_9SS3               3     10.50  10.50  10.50
OFDM_TXBF1              2     10.50  10.50  10.50
MCS0_7_TXBF1            2     10.50  10.50  10.50
VHT8_9SS1_TXBF1         2     10.50  10.50  10.50
MCS8_15_TXBF0           2     10.50  10.50  10.50
OFDM_TXBF2              3     10.50  10.50  10.50
MCS0_7_TXBF2            3     10.50  10.50  10.50
VHT8_9SS1_TXBF2         3     10.50  10.50  10.50
MCS8_15_TXBF1           3     10.50  10.50  10.50
VHT8_9SS2_TXBF1         3     10.50  10.50  10.50
MCS16_23_TXBF0          3     10.50  10.50  10.50
Power Targets:
Rate                  Chains 20in80 40in80 80MHz
DSSS                    1     -      -      -
OFDM                    1      9.0    9.0    9.0
MCS0_7                  1      9.0    9.0    9.0
VHT8_9SS1               1      9.0    9.0    9.0
DSSS_MULTI1             2     -      -      -
OFDM_CDD1               2      9.0    9.0    9.0
MCS0_7_CDD1             2      9.0    9.0    9.0
VHT8_9SS1_CDD1          2      9.0    9.0    9.0
MCS0_7_STBC             2      9.0    9.0    9.0
VHT8_9SS1_STBC          2      9.0    9.0    9.0
MCS8_15                 2      9.0    9.0    9.0
VHT8_9SS2               2      9.0    9.0    9.0
DSSS_MULTI2             3     -      -      -
OFDM_CDD2               3      9.0    9.0    9.0
MCS0_7_CDD2             3      9.0    9.0    9.0
VHT8_9SS1_CDD2          3      9.0    9.0    9.0
MCS0_7_STBC_SPEXP1      3      9.0    9.0    9.0
VHT8_9SS1_STBC_SPEXP1   3      9.0    9.0    9.0
MCS8_15_SPEXP1          3      9.0    9.0    9.0
VHT8_9SS2_SPEXP1        3      9.0    9.0    9.0
MCS16_23                3      9.0    9.0    9.0
VHT8_9SS3               3      9.0    9.0    9.0
OFDM_TXBF1              2      9.0    9.0    9.0
MCS0_7_TXBF1            2      9.0    9.0    9.0
```

```
VHT8_9SS1_TXBF1        2       9.0     9.0     9.0
MCS8_15_TXBF0          2       9.0     9.0     9.0
OFDM_TXBF2             3       9.0     9.0     9.0
MCS0_7_TXBF2           3       9.0     9.0     9.0
VHT8_9SS1_TXBF2        3       9.0     9.0     9.0
MCS8_15_TXBF1          3       9.0     9.0     9.0
VHT8_9SS2_TXBF1        3       9.0     9.0     9.0
MCS16_23_TXBF0         3       9.0     9.0     9.0
Maximum Power Target among all rates:    9.00    9.00    9.00
Last est. power                     :    8.75    8.75    8.25
Power Target for the current rate   :    9.00    9.00    9.00
Last adjusted est. power            :    8.75    8.75    8.25
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-IAPs running the Broadcom chipset: OAW-IAP224, OAW-IAP225, OAW-IAP274, OAW-IAP275, OAW-IAP214, OAW-IAP215, OAW-IAP228, OAW-IAP277, OAW-IAP207, OAW-AP203R, OAW-AP203RP, OAW-AP203H	Privileged EXEC mode

show ap debug dhcp-packets

```
show ap debug dhcp-packets [<mac>]
```

Description

This command displays information about the DHCP packets sent or received by an OAW-IAP. You can view DHCP information only when the **dhcp-option** parameter is configured with the **set-vlan** or **set-role** rule.

Parameter	Description	Range	Default
`<mac>`	Indicates the OAW-IAP's MAC address.	—	—

Example

The following example shows the output of **show ap debug dhcp-packets** command:

```
Traced Dhcp Packets
-------------------
Timestamp  Mtype  Htype  Hops  TID  Cip  Yip  Sip  Gip  Cmac
---------  -----  -----  ----  ---  ---  ---  ---  ---  ----
```

The output of this command includes the following parameters:

Column	Description
`Timestamp`	Displays the timestamp for DHCP packets.
`Mtype`	Indicates the message type.
`Htype`	Indicates the hardware address type.
`Hops`	Shows the number of hops.
`TID`	Shows the transaction ID.
`Cip`	Indicates the client IP address.
`Yip`	Indicates the IP address of the OAW-IAP.
`Sip`	Indicates the source IP address from which the DHCP packets originated.
`Gip`	Indicates the Gateway IP address.
`Cmac`	Indicates the MAC address of the client.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug dot1x-statistics

```
show ap debug dot1x-statistics
```

Description

This command displays the aggregate 802.11X debug statistics for an OAW-IAP.

Example

The following output is displayed for the **show ap debug dot1x-statistics** command:

```
802.1X Statistics
-----------------
Mac         Name     AP         Auth-Succs  Auth-Fails Auth-Tmout  Re-Auths

----------  ------ ---- ----------  --------  ---------  -------  -------
08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12  0           0           0           0

Total:                               0           0           0           0

Supp-Naks  UKeyRot  MKeyRot
---------- -------- --------
       0          0        0
       0          0        0
802.1x Counters
WPA2
Message-1......................3
Message-2......................2
Message-3......................2
Message-4......................2
```

The output of this command includes the following parameters:

Parameter	Description
Mac	Displays the MAC address of the authenticated client.
Name	Displays the name of the client device.
AP	Displays the OAW-IAP device details to which the client is connected.
Auth-Succs	Displays the number of times the client authenticated successfully.
Auth-Fails	Displays the number of times the client failed to authenticate.
Auth-Timeout	Displays if client authentication timeout details.
Reauths	Displays the reauthentication attempts if any.
Supp-Naks	Displays the number of supplementary NAKs.
UkeyRot	Displays the unicast key rotation details.
MkeyRot	Displays the multicast key rotation details.
802.1X counters	Displays the 802.1X authentication counters.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug driver-config

```
show ap debug driver-config
```

Description

This command displays OAW-IAP driver configuration. Use this command to review configuration changes made since the OAW-IAP driver was last reset.

Example

The **show ap debug driver-config** command displays the BSSID, SSID, and radio configuration details associated with the OAW-IAP driver. The following output is displayed for the **show ap debug driver-config** command:

```
Downloaded Config for WIFI 0
----------------------------
Item                                                                    Value
----                                                                    -----
BSSID                                                                   d8:c7:c8:3d:42:12
LMS IP
Master IP                                                               0.0.0.0
Mode                                                                    AP Mode
Group Key Received                                                      Yes
QBSS Probe Response                                                     Allow Access
Native VLAN ID                                                          1
LED operating mode (11n APs only)                                       normal
SAP MTU                                                                 1500 bytes
Heartbeat DSCP                                                          0
High throughput enable (radio)                                          Enabled
Channel                                                                 44+
Transmit EIRP                                                           24 dBm
Non-Wi-Fi Interference Immunity                                         2
Enable CSA                                                              Disabled
CSA Count                                                               4
Advertise 802.11d and 802.11h Capabilities                              Disabled
TPC Power                                                               0 dBm
Spectrum Load Balancing                                                 Disabled
Spectrum Load Balancing Mode                                            channel
Spectrum Load Balancing Update Interval (sec)                           30 seconds
Spectrum Load Balancing Threshold (%)                                   2 percent
Infrastructure assisted client association management                   Disabled
Beacon Period                                                           100 msec
Beacon Regulate                                                         Disabled
Advertized regulatory max EIRP                                          0
ARM/WIDS Override                                                       Dynamic
Reduce Cell Size (Rx Sensitivity)                                       0 dB
Management Frame Throttle interval                                      0 sec
Management Frame Throttle Limit                                         0
Maximum Distance                                                        600 meters
RX Sensitivity Threshold                                                0 dB
RX Sensitivity Tuning Based Channel Reuse                               disable
Active Scan                                                             Enabled
ARM Over the Air Updates                                                Disabled
VoIP Aware Scan                                                         Enabled
Power Save Aware Scan                                                   Disabled
Video Aware Scan                                                        Enabled
Load aware Scan Threshold                                               1048576 Bps
40 MHz intolerance                                                      Disabled
Honor 40 MHz intolerance                                                Enabled
CSD override                                                            Enabled
```

```
Advertise 802.11K Capability                                            Disabled
Measurement Mode for Beacon Reports                                     passive
Channel for Beacon Requests in 'A' band                                 0
Channel for Beacon Requests in 'BG' band                                0
Channel for AP Channel Reports in 'A' band                              0
Channel for AP Channel Reports in 'BG' band                             0
Time duration between consecutive Beacon Requests                       0 sec
Time duration between consecutive Link Measurement Requests             0 sec
Time duration between consecutive Transmit Stream Measurement Requests  0 sec
Enable Handover Trigger feature                                         Disabled
Advertise Enabled Capabilities IE                                       Disabled
Advertise Country IE                                                    Disabled
Advertise Power Constraint IE                                           Disabled
Advertise TPC Report IE                                                 Disabled
Advertise QBSS Load IE                                                  Disabled
Advertise BSS AAC IE                                                    Disabled
Advertise Quiet IE                                                      Disabled
Advertise Fast-BSS Transition (802.11r) Capability                      Disabled
Fast-BSS Transition Mobility Domain ID                                  0
Country Code                                                            IN
ESSID                                                                   example1
Encryption                                                              wpa2-psk-aes
WPA2 Pre-Auth                                                           Disabled
Enable Management Frame Protection                                      Disabled
Require Management Frame Protection                                     Disabled
DTIM Interval                                                           1 beacon periods
802.11a Basic Rates                                                     6 12 24
802.11a Transmit Rates                                                  6 9 12 18 24 36 48 54
Station Ageout Time                                                     1000 sec
Max Transmit Attempts                                                   16
RTS Threshold                                                           2333 bytes
Max Associations                                                        64
Wireless Multimedia (WMM)                                               Enabled
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave                        Enabled
WMM TSPEC Min Inactivity Interval                                       0 msec
DSCP mapping for WMM voice AC                                           N/A
DSCP mapping for WMM video AC                                           N/A
DSCP mapping for WMM best-effort AC                                     N/A
DSCP mapping for WMM background AC                                      N/A
Hide SSID                                                               Disabled
Deny_Broadcast Probes                                                   Disabled
Local Probe Response                                                    Enabled
Local Probe Request Threshold (dB)                                      0
Disable Probe Retry                                                     Enabled
Maximum Transmit Failures                                               0
BC/MC Rate Optimization                                                 Disabled
Rate Optimization for delivering EAPOL frames                           Enabled
Strict Spectralink Voice Protocol (SVP)                                 Disabled
802.11a Beacon Rate                                                     0
Advertise QBSS Load IE                                                  Enabled
Advertise Location Info                                                 Disabled
Advertise AP Name                                                       Disabled
40 MHz channel usage                                                    Enabled
BA AMSDU Enable                                                         Disabled
Temporal Diversity Enable                                               Enabled
High throughput enable (SSID)                                           Enabled
Low-density Parity Check                                                Enabled
Maximum number of spatial streams usable for STBC reception             1
Maximum number of spatial streams usable for STBC transmission          1
MPDU Aggregation                                                        Enabled
Max received A-MPDU size                                                65535 bytes
Max transmitted A-MPDU size                                             65535 bytes
Min MPDU start spacing                                                  16 usec
```

```
Short guard interval in 20 MHz mode                                     Enabled
Short guard interval in 40 MHz mode                                     Enabled
Supported MCS set
Explicit Transmit Beamforming                                           Disabled
Transmit Beamforming Compressed Steering                                Disabled
Transmit Beamforming non Compressed Steering                            Disabled
Transmit Beamforming delayed feedback support                           Disabled
Transmit Beamforming immediate feedback support                         Disabled
Transmit Beamforming Sounding Interval                                  0 sec
40 MHz channel usage                                                    Enabled
BA AMSDU Enable                                                         Disabled
Temporal Diversity Enable                                               Enabled
High throughput enable (SSID)                                           Enabled
Low-density Parity Check                                                Enabled
Maximum number of spatial streams usable for STBC reception             1
Maximum number of spatial streams usable for STBC transmission          1
MPDU Aggregation                                                        Enabled
Max received A-MPDU size                                                65535 bytes
Max transmitted A-MPDU size                                             65535 bytes
Min MPDU start spacing                                                  16 usec
Short guard interval in 20 MHz mode                                     Enabled
Short guard interval in 40 MHz mode                                     Enabled
Supported MCS set
Explicit Transmit Beamforming                                           Disabled
Transmit Beamforming Compressed Steering                                Disabled
Transmit Beamforming non Compressed Steering                            Disabled
Transmit Beamforming delayed feedback support                           Disabled
Transmit Beamforming immediate feedback support                         Disabled
Transmit Beamforming Sounding Interval                                  0 sec
Forward mode                                                            bridge
Band Steering                                                           Enabled
Steering Mode                                                           prefer-5ghz
Dynamic Multicast Optimization (DMO)                                    Disabled
Dynamic Multicast Optimization (DMO) Threshold                          0

VAP on radio 1 : is not created and is not enabled
--------------------------------------------------
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug eapol-debug status

```
show ap debug eapol-debug status
```

Description

This command shows the status of EAPoL debug logs for the OAW-IAP.

Example

The following example shows the output of **show ap debug eapol-debug status** command:

```
[radio 0]:ap eapol debug log is disabled
[radio 1]:ap eapol debug log is disabled
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug facebook-token-log

```
show ap debug facebook-token-log
```

Description

This command shows the user authentication log of clients accessing the internet using Facebook Wi-Fi . This command will only show the authentication log of active clients using the feature.

Example

The following example shows the output of **show ap debug facebook-token-log** command:

```
DEBUG output created by Wget 1.10.2 (Red Hat modified) on linux-gnu.
--12:14:38--  https://graph.facebook.com/2228603190737192/wifiauth/316257032411974
=> `/tmp/facebook_access_token_14652'
Resolving graph.facebook.com... 157.240.22.19, 2a03:2880:f031:12:face:b00c:0:2
Caching graph.facebook.com => 157.240.22.19 2a03:2880:f031:12:face:b00c:0:2
Connecting to graph.facebook.com|157.240.22.19|:443... connected.
Created socket 6.
Releasing 0x01695750 (new refcount 1).
Initiating SSL handshake.
Handshake successful; connected socket 6 to SSL handle 0x01695a50
certificate:
subject: /C=US/ST=CA/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
issuer:  /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
X509 certificate successfully verified and matches host graph.facebook.com
---request begin---
POST /2228603190737192/wifiauth/316257032411974 HTTP/1.0
User-Agent: Wget/1.10.2 (Red Hat modified)
Accept: */*
Host: graph.facebook.com
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
---request end---
[POST data: secret=Dk_Zmu1abqsSFyjYobf8fkUTVZ_2DcAW-KENb-xZekc]
HTTP request sent, awaiting response...
---response begin---
HTTP/1.1 200 OK
Vary: Accept-Encoding
x-app-usage: {"call_count":0,"total_cputime":0,"total_time":0}
Content-Type: application/json; charset=UTF-8
facebook-api-version: v2.8
Strict-Transport-Security: max-age=15552000; preload
Pragma: no-cache
x-fb-rev: 1000557895
Access-Control-Allow-Origin: *
Cache-Control: private, no-cache, no-store, must-revalidate
x-fb-trace-id: AHUBZqwa8PR
x-fb-request-id: AYCtIV3MMZWQomQiRtKemNq
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-FB-Debug:
ddR86kvMSJ80794wD9eFYtL9YvCF08mMAz0nDf/O2Ll0CtvrCArSdvrZ6kX8LVZlmJQlIITxE6W9+2Em74coIg==
Date: Tue, 02 Apr 2019 19:14:38 GMT
Connection: keep-alive
Content-Length: 14
---response end---
200 OK
Registered socket 6 for persistent reuse.
Length: 14 [application/json]
0K                                                       100%  273.44 KB/s
```

```
12:14:38 (273.44 KB/s) - `/tmp/facebook_access_token_14652' saved [14/14]
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug lldp

```
show ap debug lldp {counters | neighbor [interface <name> detail] | state}
```

Description

This command displays LLDP information for a specific OAW-IAP, or all OAW-IAPs sending or receiving LLDP PDUs.

Parameter	Description	Range	Default
`counters`	Displays LLDP counters for a specific OAW-IAP, or all OAW-IAPs sending or receiving LLDP PDUs.	—	—
`neighbor`	The LLDP protocol allows switches, routers, and WLAN access points to advertise information about themselves such as identity, capabilities, and neighbors to other nodes on the network. Use this command to display information about LLDP peers and OAW-IAPs. By default, this command displays LLDP neighbors for the entire list of LLDP interfaces. Include the IP address of an to display neighbor information only for that one device.	—	—
`interface <name>`	Displays the name of the OAW-IAP interface sending or receiving LLDP PDUs.	—	—
`detail`	Displays details about the interface and number of neighbors.	—	—
`state`	This command displays the LLDP interfaces information sending or receiving LLDP PDUs.	—	—

Examples

The following example shows the output of **show ap debug lldp counters** command.

```
(Instant AP)# show ap debug lldp counters
Interface  Received  Unknown TLVs  Malformed  Overflow  Transmitted
---------  --------  ------------  ---------  --------  -----------
eth0       3259      0             0          0         3255
eth1       0         0             0          0         0
```

The output of this command includes the following information:

Column	Description
`Interface`	Name of the OAW-IAP interface sending or receiving LLDP PDUs.
`Received`	Number of packets received on the specified interface.

Column	Description
`Unknown TLVs`	Number of LLDP PDUs with an unknown TLV.
`Malformed`	Number of malformed packets received on that interface.
`Overflow`	Number of times that an LLDP neighbor could not be added to the neighbor table (there is a limit of 8 per port).
`Transmitted`	Number of packets transmitted from that interface.

The following example shows the output of **show ap debug lldp neighbor** command.

```
(Instant AP)# show ap debug lldp neighbor
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-------------------------
Interface  Neighbor ID        Capabilities  Remote Interface  Expiry-Time (Secs)
---------  -----------        ------------  ----------------  ------------------
eth0       00:0b:86:6b:57:80  B:R           GE0/0/22          93
```

The output of this command includes the following information:

Column	Description
`Interface`	Indicates the interface on the OAW-IAP sending or receiving LLDP PDUs.
`Neighbor ID`	Indicates the LLDP neighbor number.
`Capabilities`	This data column can list any of the following data codes to indicate LLDP neighbor capabilities. ■ R: Router ■ B: Bridge ■ A: Access Point ■ P: Phone ■ O: Other
`Remote Interface`	Indicates the interface name on a peer device to which the OAW-IAP port is connected.
`Expiry-Time (Secs)`	Indicates the maximum time limit for sending and receiving LLDP PDUs.

The following example shows the output of **show ap debug lldp state** command.

```
(Instant AP)# show ap debug lldp state
LLDP Interface Information
--------------------------
Interface  LLDP TX  LLDP RX  LLDP-MED  TX interval  Hold Timer
---------  -------  -------  --------  -----------  ----------
eth0       Enabled  Enabled  Disabled  30           120
eth1       Enabled  Enabled  Disabled  30           120
```

The output of this command includes the following information:

Column	Description
`Interface`	Indicates the LLDP interface name.

Column	Description
`LLDP TX`	Shows if LLDP PDU transmission is enabled or disabled.
`LLDP RX`	Shows if the OAW-IAP has enabled or disabled processing of received LLDP PDUs.
`LLDP-MED`	Shows if LLDP MED protocol is enabled or disabled.
`TX interval`	Indicates the LLDP transmit interval in seconds.
`Hold Timer`	Indicates the LLDP transmit hold multiplier.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug message-ids

```
show ap debug message-ids <id>
```

Description

This command shows the field ID and the locator information for a specified message type. The list of message IDs can be viewed by executing the **show ap debug message-list** command.

Parameter	Description
`<id>`	Specify the message id for which you want to view the field ID and locator information.

Example

The following example shows the output of **show ap debug message-ids** command:

```
(InstantAP)# show ap debug message-ids 2
Message Dictionary ID Table
---------------------------
Field ID  Locator
--------  -------
1         /iap/ap/state/ClusterInfo/vc_key(32)
2         /iap/ap/state/ClusterInfo/vc_name(33)
3         /iap/ap/state/ClusterInfo/organization(38)
4         /iap/ap/state/ClusterInfo/vc_ip(31)
5         /iap/ap/state/ClusterInfo/image_version(39)
6         /iap/ap/state/ClusterInfo/oem(29)
7         /iap/ap/state/ClusterInfo/single_signon_key(43)
8         /iap/ap/state/ClusterInfo/cert_sn_server(40)
9         /iap/ap/state/ClusterInfo/cert_sn_ca(36)
10        /iap/ap/state/ClusterInfo/config_rcv(36)
11        /iap/ap/state/ClusterInfo/upgrade_state(39)
12        /iap/ap/state/ClusterInfo/facebook_id(37)
13        /iap/ap/state/ClusterInfo/master_ip(35)
14        /iap/ap/state/ClusterInfo/master_ip_mask(40)
15        /iap/ap/state/ClusterInfo/master_gateway_ip(43)
16        /iap/ap/state/ClusterInfo/master_nameserver_ip(46)
17        /iap/ap/state/ClusterInfo/drt_version(37)
18        /iap/ap/state/ClusterInfo/ext(29)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug message-list

```
show ap debug message-list
```

Description

This command shows the list of all message data locators supported by the OAW-IAP.

Example

The following example shows the partial output of **show ap debug message-list** command:

```
Message Dictionary Table
------------------------
Msg ID  Msg Name                             Locator
------  --------                             -------
1       State message                        /iap/ap/state(13)
2       AP cluster Info                      /iap/ap/state/ClusterInfo(25)
3       AP Info                              /iap/ap/state/ApInfo(20)
4       WLAN Info                            /iap/ap/state/WlanInfo(22)
5       Radio Info                           /iap/ap/state/ApInfo/radios(27)
6       VAP Info                             /iap/ap/state/ApInfo/radios/vaps(32)
7       User Info                            /iap/ap/state/ClientInfo(24)
8       Rssi Info                            /iap/ap/state/ApInfo/radios/rssi(32)
9       Tags                                 /iap/ap/state/tag(17)
10      VPN Tunnel Info                      /iap/ap/state/VpnTunnelInfo(27)
11      Dynamic black client Info            /iap/ap/state/DynamicBlackedClientsInfo(39)
12      AP Ethernet Info                     /iap/ap/state/ApInfo/ports(26)
13      AP power Info                        /iap/ap/state/ApInfo/power(26)
14      Stats message                        /iap/ap/stats(13)
15      Radio Stats                          /iap/ap/stats/RadioStat(23)
16      VAP Stats                            /iap/ap/stats/VapStat(21)
17      STA Stats                            /iap/ap/stats/ClientStat(24)
18      Airmonitor Info                      /iap/ap/stats/AirMonitorInfo(28)
19      Rough AP Info                        /iap/ap/stats/AirMonitorInfo/am_rouge(37)
20      Spec Dev Details                     /iap/ap/stats/SpectrumInfo(26)
21      Active Laser Beam Info               /iap/ap/stats/AirMonitorActiveLaserBeamInfo(43)
22      AP Ethernet Stats                    /iap/ap/stats/PortStat(22)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug mgmt-frames

```
show ap debug mgmt-frames [<mac>]
```

Description

This command displays the trace information for the 802.11 management frames.

Parameter	Description	Range	Default
`<mac>`	Displays trace information for an OAW-IAP based on MAC address.	—	—

Example

The following example shows the partial output of **show ap debug mgmt-frames** command:

```
Traced 802.11 Management Frames
-------------------------------
Timestamp      stype     SA                  DA                 BSS           signal Misc
---------      -----    -------            ------  ----
May 9 23:09:42 deauth   d8:c7:c8:c4:29:82 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:82 15     -
May 9 23:09:42 disassoc d8:c7:c8:c4:29:82 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:82 15     -
May 9 23:09:03assoc-respd8:c7:c8:c4:29:82 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:82 15Success
May 9 22:02:40 auth     d8:c7:c8:c4:29:8b c4:85:08:de:06:d4 d8:c7:c8:c4:29:8b 15Success
May 9 01:25:51 auth     08:ed:b9:e1:51:87 d8:c7:c8:c4:29:8a d8:c7:c8:c4:29:8a 60     -
```

The output of this command includes the following information:

Column	Description
`Timestamp`	Indicates timestamp for the authentication management frame.
`stype`	Indicates the type of the packet.
`SA`	Indicates the source of the packets.
`DA`	Indicates the destination to which the packets are intended.
`BSS`	Indicates the BSSID.
`Signal`	Indicates the signal level.
`Misc`	Indicates miscellaneous information such as status and other relevant details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug msghandler-stats

```
show ap debug msghandler-stats
```

Description

This command shows PAPI message counters between the master OAW-IAP and the slave OAW-IAPs.

Example

The following example shows the output of **show ap debug msghandler-stats** command:

```
MsgHandlerStats
FalseSelect     : 0
MsgHandlerError : 0
PacketNotForMe  : 0
ForwardFailed   : 0
BadPacketType   : 0
BadPacket       : 0
BadSignature    : 0
Rx_Count        : 2232951
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug msg-subscription

```
show ap debug msg-subscription
```

Description

This command shows the status of message subscriptions of the OAW-IAP with OmniVista 3600 Air Manager and ALE servers.

Example

The following example shows the output of **show ap debug msg-subscription** command:

```
Subscription modules List
-------------------------
message type  Central  Airwave  ALE
------------  -------  -------  ---
state         TRUE     FALSE    FALSE
stat          TRUE     FALSE    FALSE
trap          TRUE     FALSE    FALSE
speedtest     TRUE     FALSE    FALSE
telemetry     TRUE     FALSE    FALSE
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug network-bssid

```
show ap debug network-bssid [<mac> | all]
```

Description

This command displays the mapping of WLAN index and BSSID for an OAW-IAP. When this command is executed on a master OAW-IAP, it displays the mapping details of the slave OAW-IAP.

Parameter	Description	Range	Default
`<mac>`	Displays the mapping of WLAN index and BSSID along with the MAC address.	—	—
`all`	Displays the virtual AP status that includes all types of status details.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode

show ap debug pan-key

```
show ap debug pan-key
```

Description

This command shows the PAN negotiation key used between the OAW-IAP and the PAN server.

Example

The following example shows the output of **show ap debug pan-key** command:

```
(Instant AP)# show ap debug pan-key
pan_firewall_key :  ajkdlfajdlkf197921ofsjfsfa
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug pan-sent

```
show ap debug pan-sent
```

Description

This command shows the client information sent to the PAN server. Use the output of this command to view the client information including the client name, IP address, MAC Adress, network name and also the access point.

Example

The following example shows the output of **show ap debug pan-sent** command:

```
(Instant AP)# show ap debug pan-sent
Client List
-----------
Name          IP Address     MAC Address        Network                 Access Point
----          ----------     -----------        -------                 ------------
                        DEL  Offline  Roam Away  Pan Login
                        ---  -------  ---------  ---------
Admin-PC      172.31.99.140  70:1c:e7:6f:a1:c1  ChinaNet                38:17:c3:c8:02:60-303
                        no   no       no         no
Admin-2       172.99.99.3    68:64:4b:f0:7f:f5  Branch Net              40:e3:d6:cf:f5:18-305
                        no   yes      yes        no
Litt          10.64.153.166  54:9f:13:08:cd:1e  Pearson Specter         40:e3:d6:cf:f5:18-305
                        no   yes      no         no
Testbed       172.31.98.170  38:53:9c:79:3f:2f  Employee only           40:e3:d6:cf:f5:18-305
                        no   no       no         no
Harvey-PC     172.31.99.224  90:32:4b:2d:ea:0d  SL Zane                 c8:b5:ad:c3:ab:2c-345
                        no   no       no         no
Guest         172.31.99.57   b4:ef:fa:c6:8e:ee  Aruba net               c8:b5:ad:c3:ab:2c-345
                        no   yes      yes        no
Donna-PC      172.31.99.177  b8:8d:12:23:1e:1a  Corp Net                c8:b5:ad:c3:ab:2c-345
                        no   yes      yes        no
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug persistent-clients

```
show ap debug persistent-clients
```

Description

This command displays the information about the persistent OAW-IAP clients. Use the output of this command to view information about the clients that are persistently connected to anOAW-IAP.

Example

The following example shows the output of **show ap debug persistent-clients** command:

```
Persistent Clients
------------------
MAC Address  ESSID  State  Expired  Update Time  Expiration Time
-----------  -----  -----  -------  -----------  ---------------
```

The output of this command includes the following information:

Column	Description
`MAC Address`	Shows the MAC address of the client.
`ESSID`	Shows the ESSID used by the client.
`State`	Indicates the connection status of the client.
`Expired`	Indicates if the client session is expired.
`Update Time`	Indicates the update time.
`Expiration Time`	Indicates the time at which the client session expires.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug power-table

```
show ap debug power-table [<radio>]
```

Description

This command displays the following information for a specific radio:

- Power limit table based on regulatory powers, user configured power, and override powers.
- Board limit table.
- A combination of all the above fields to calculate the actual transmit power of the packets.

Parameter	Description	Range	Default
`<radio>`	Denotes the polarization value for the radio channel.	0 or 1	—

Example

The following example shows the output of the **show ap debug power-table** command.

```
(Instant AP)# show ap debug power-table 1
Combined CONDUCTED Limits(dBm) 11
#Antenna 1:
#NSS 1:
CCK:
CDD     18.0     18.0     18.0     18.0
CDD+CRPOL     18.0     18.0     18.0     18.0
TXBF        *        *        *        *
TXBF+CRPOL        *        *        *        *
OFDM:
CDD     18.0     18.0     18.0     18.0     18.0     18.0     18.0     18.0
CDD+CRPOL     18.0     18.0     18.0     18.0     18.0     18.0     18.0     18.0
TXBF        *        *        *        *        *        *        *        *
TXBF+CRPOL        *        *        *        *        *        *        *        *
Mode HT/VHT 20:
CDD     18.0     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0     15.0
CDD+CRPOL     18.0     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0
 15.0
TXBF     18.0     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0
15.0
TXBF+CRPOL     18.0     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0
  15.0
Mode HT/VHT 40:
CDD     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0     15.0     14.0
CDD+CRPOL     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0     15.0
 14.0
TXBF     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0     15.0
14.0
TXBF+CRPOL     18.0     18.0     18.0     18.0     18.0     18.0     17.0     16.0     15.0
  14.0
Note:
NSS: Number of Spatial Streams
CDD: Cyclic Diversity Delay
TXBF: Transmit Beamforming
MCS: Modulation and Coding Index
Combined Conducted limits = Min(Board limits, User configured conducted power(floored to min
conducted power), override board limit, regulatory limits)
Combined EIRP Limits = Combined Conducted Limited + Effective Antenna Gain + Power gain +
correlation gain
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug radar-logs

```
show ap debug radar-logs
```

Description

This command shows the radar event logs of the OAW-IAP. Use the output of this command to view the debugging logs of radar events of the OAW-IAP.

Example

The following example shows the output of **show ap debug radio-logs** command:

```
The latest 4 radar event logs
Radar logs:
dfs_print_radar_events:Total radar events detected=21, entries in the radar queue follows:
ts=3276926874 diff_ts=89 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=-100, freq_offset=-
31.200MHz, peak_mag=75, total_gain=86, mb_gain=48, relpwr_db=27
ts=3276927875 diff_ts=1001 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=-112, freq_offset=-
34.944MHz, peak_mag=80, total_gain=72, mb_gain=31, relpwr_db=30
ts=3276930031 diff_ts=2156 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=-72, freq_offset=-
22.464MHz, peak_mag=99, total_gain=84, mb_gain=31, relpwr_db=15
ts=3276931228 diff_ts=1197 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=36, freq_
offset=11.232MHz, peak_mag=100, total_gain=83, mb_gain=27, relpwr_db=28
ts=3276931586 diff_ts=358 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=36, freq_
offset=11.232MHz, peak_mag=76, total_gain=76, mb_gain=25, relpwr_db=25
ts=3276934903 diff_ts=3317 rssi=20 dur=1, is_chirp=0, seg_id=0, sidx=0, freq_offset=0.0MHz,
peak_mag=74, total_gain=130, mb_gain=74, relpwr_db=0
Time of detection: UTC 2019-03-18 05:21:50
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug radio-info

```
show ap debug radio-info
```

Description

This command shows the radio debug messages of the AP driver. Use the output of this command to view radio debug messages of the AP driver.

Example

The following example shows the output of **show ap debug radio-info** command:

```
Radio Info Script
------------------
Script Output
-------------
aruba_dbg_radio_info_0 Start time: Tue Mar 19 09:44:38 UTC 2019
wifi0-drop-list:
wmi_htc_tx_complete(903): 11237524/11237524 0/0
htt_rx_desc_frame_free(1207): 319663891/319663891 0/0
wmi_unified_event_rx(365): 102544161/102544161 0/0
dbglog_deferred_work(1173): 99/99 0/0
HTCRxCompletionHandler(391): 3/3 0/0
DestroyHTCTxCtrlPacket(41): 3/3 0/0
wmi_control_rx(541): 3/3 0/0
pre_service_ready_event(4974): 1/1 0/0
htt_h2t_send_complete_free_netbuf(62): 3/3 0/0
htt_pkt_buf_list_del(156): 511401/511401 0/0
aruba_am_rx_pkt_handler_data_ol(10122): 202799667/202799667 0/0
aruba_am_rx_pkt_handler_data_ol(10400): 187791816/187791816 0/0
osif_receive(4233): 181763999/181763999 0/0
ieee80211_release_wbuf_internal(415): 1611941/1611941 0/0
ieee80211_input_all(2113): 9658638/9658638 0/0
ieee80211_input(1657): 789660/789660 0/0
aruba_am_rx_pkt_handler_data_ol(10117): 38235922/38235922 0/0
wmi_unified_beacon_send(150): 24/24 0/0
wifi0-anul-dump:
assert_list (both wifi0 and wifi1):
No VAP found.
No VAP found.
aruba_dbg_radio_info_0 Finished time: Tue Mar 19 09:44:38 UTC 2019
aruba_dbg_radio_info_0: Read 1079 bytes in 31 lines. Truncated:FALSE
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug radio-stats

```
show ap debug radio-stats [<radio>]
```

Description

This command displays the aggregate radio debug statistics of an OAW-IAP. Use the output of this command to view the general radio debug statistics and also statics transmitted and received frames for anOAW-IAP. Use the <radio-ID> parameter customize the radio statistics.

Parameter	Description	Range	Default
`<radio-ID>`	Allows you to specify the ID number of the radio (for example, 0 or 1) for which you want to view statistics.	—	—

Example

The output of this command displays general statistics for the radio, as well as statistics for transmitted and received frames.

```
RADIO Stats
-----------
Parameter                     Value
---------                     -----
Tx Powersave Queue Timeouts   0
Tx Dropped After Retry        158551
Tx Dropped No Buffer          0
Tx Missed ACKs                158581
Tx Failed Beacons             1
Tx Multi-Beacon Fail          0
Tx Long Preamble              557658
Tx Short Preamble             0
Tx Beacon Interrupts          2597365
Tx Interrupts                 780044
Tx FIFO Underrun              0
Tx Allocated Desc             557660
Tx Freed Desc                 557660
Tx EAPOL Frames               15
TX STBC Frames                0
TX LDPC Frames                0
Tx AGGR Good                  0
Tx AGGR Unaggr                0
Tx Data Priority [BE]         125
Tx Data 6 Mbps (Mon)          125
Tx Data 12 Mbps (Mon)         0
Tx Data 24 Mbps (Mon)         0
Tx Data 36 Mbps (Mon)         0
Tx Data 54 Mbps (Mon)         0
Tx Data 108 Mbps (Mon)        0
Tx Data 108 Mbps+ (Mon)       0
Tx Data Bytes 6 Mbps (Mon)    16648
Tx Data Bytes 12 Mbps (Mon)   0
Tx Data Bytes 24 Mbps (Mon)   0
Tx Data Bytes 36 Mbps (Mon)   0
Tx Data Bytes 54 Mbps (Mon)   0
Tx Data Bytes 108 Mbps (Mon)  0

RADIO Stats
```

```
-----------
Parameter                      Value
---------                      -----
Tx Data Bytes 108 Mbps+ (Mon)  0
Tx 6 Mbps                      557650
Tx WMM [BE]                    125
Tx WMM [VO]                    557532
Tx WMM [BE] Dropped            158561
Tx UAPSD OverflowDrop          0
TX Timeouts                    36
Lost Carrier Events            8
Tx HT40 Hang Detected          0
Tx HT40 Hang Stuck             0
Tx HT40 Hang Possible          0
Tx HT40 Dfs IMM WAR            0
Tx HT40 Dfs HT20 WAR           0
Tx MAC/BB Hang Stuck           0
Tx Mgmt Bytes                  1434583125
Tx Beacons Bytes               1202571538
-------------------            Receive Specific Statistics
Rx Last SNR                    16
Rx Last SNR CTL0               14
Rx Last SNR CTL1               13
Rx Last ACK SNR                0
Rx Frames Received             5622989
Rx Good Frames                 4517471
Rx Bad Frames                  1105518
Rx Total Data Frames Recvd     518806
Rx Total Mgmt Frames Recvd     3261635
Rx Total Control Frames Recvd  736829
Rx Total Bytes Recvd           755424522
Rx Total Data Bytes Recvd      78179450
Rx Total RTS Frames Recvd      230212
Rx Total CTS Frames Recvd      204854
Rx Total ACK Frames            2344801
```

The output of this command provides the following information:

Column	Description
`Parameter`	Displays the transmission and reception parameters.
`Value`	Displays the values associated with the transmission and reception parameters.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug radius-attributes

```
show ap debug radius-attributes
```

Description

This command shows the RADIUS attributes for authentication servers configured on the OAW-IAP. Use the output of this command to view the radio debug attributes for anOAW-IAP.

Example

The following example shows the partial output of **show ap debug radius-attributes** command:

```
Dictionary
----------
Attribute                         Value  Type         Vendor     Id
---------                         -----  ----         ------     --
MS-CHAP-NT-Enc-PW                 6      String       Microsoft  311
Suffix                            1004   String
fw_mode                           321    Integer
Revoke-Text                       316    String
Acct-Output-Packets               48     Integer
WISPr-Session-Term-End-Of-Day     10     Integer      WISPr      14122
Aruba-Mdps-Device-Version         21     String       Aruba      14823
Aruba-Mdps-Max-Devices            18     Integer      Aruba      14823
Location-Information              127    String
WISPr-Redirection-URL             4      String       WISPr      14122
Menu                              1001   String
Acct-Session-Time                 46     Integer
Framed-AppleTalk-Zone             39     String
RTTS-Reest-Below-Throughput       5      Integer      RTTS       10923
Requested-Location-Info           132    Integer
Framed-Interface-Id               96     IF ID
Connect-Info                      77     String
Aruba-Location-Id                 6      String       Aruba      14823
Service-Type                      6      Integer
Nomadix-Group-Max-Up              20     Integer      Nomadix    3309
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug radius-statistics

```
show ap debug radius-statistics [termination]
```

Description

This command displays the RADIUS statistics for the authentication servers configured on an OAW-IAP. Use the output of this command to view the authentication server details.

Example

The following example displays the output of the **show ap debug radius-statistics** command:

```
RADIUS Statistics
-----------------
Statistics                   TerminationServer  InternalServer  testserver  test1234
----------                   -----------------  --------------  ----------  --------
In Service: Management Auth  Not used           Not used        Not used    Not used
In Service: Example1         Not used           Up 67920s       Not used    Not used
Accounting Requests          0                  0               0           0
Raw Requests                 0                  0               0           0
PAP Requests                 0                  0               0           0
CHAP Requests                0                  0               0           0
MS-CHAP Requests             0                  0               0           0
MS-CHAPv2 Requests           0                  0               0           0
Mismatch Response            0                  0               0           0
Invalid Secret               0                  0               0           0
Access-Accept                0                  0               0           0
Access-Reject                0                  0               0           0
Accounting-Response          0                  0               0           0
Access-Challenge             0                  0               0           0
Unknown Response code        0                  0               0           0
Timeouts                     0                  0               0           0
AvgRespTime (ms)             0                  0               0           0
Total Qequests               0                  0               0           0
Total Response               0                  0               0           0
Read Error                   0                  0               0           0
SEQ first/last/free          0/0/0              0/0/0           0/0/0       0/0/0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug received-reg-table

```
show ap debug received-reg-table
```

Description

This command shows the regulatory table downloaded to the OAW-IAP. Use the output of this command to view the regulatory information of the OAW-IAP.

Example

The following example shows the output of **show ap debug received-reg-table** command:

```
Country reg-info for Country Code "IN"
---------------------------------------
PHY Type                        Allowed Channels
--------                        ----------------
802.11g (indoor)                1 2 3 4 5 6 7 8 9 10 11 12 13
802.11a (indoor)                36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
                                140 144 149 153 157 161 165
802.11g (outdoor)               1 2 3 4 5 6 7 8 9 10 11 12 13
802.11a (outdoor)               36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
                                140 144 149 153 157 161 165
802.11g 40MHz (indoor)          1-5 2-6 3-7 4-8 5-9 6-10 7-11 8-12 9-13
802.11a 40MHz (indoor)          36-40 44-48 52-56 60-64 100-104 108-112 116-120 124-128 132-136
                                        140-144 149-153 157-161
802.11g 40MHz (outdoor)         1-5 2-6 3-7 4-8 5-9 6-10 7-11 8-12 9-13
802.11a 40MHz (outdoor)         36-40 44-48 52-56 60-64 100-104 108-112 116-120 124-128 132-136
                                        140-144 149-153 157-161
802.11a 80MHz (indoor)          36-48 52-64 100-112 116-128 132-144 149-161
802.11a 80MHz (outdoor)         36-48 52-64 100-112 116-128 132-144 149-161
802.11a 160MHz (indoor)         36-64 100-128
802.11a 160MHz (outdoor)        36-64 100-128
802.11a (DFS)                   52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 144

Certificate reg-info for AP-345 Country Code "IN"
---------------------------------------------------
PHY Type                  Allowed Channels
--------                  ----------------
802.11g (indoor)          1 2 3 4 5 6 7 8 9 10 11 12 13
802.11a (indoor)          36 40 44 48 52 56 60 64 149 153 157 161 165
802.11g (outdoor)         1 2 3 4 5 6 7 8 9 10 11 12 13
802.11a (outdoor)         36 40 44 48 52 56 60 64 149 153 157 161 165
802.11g 40MHz (indoor)    1-5 2-6 3-7 4-8 5-9 6-10 7-11 8-12 9-13
802.11a 40MHz (indoor)    36-40 44-48 52-56 60-64 149-153 157-161
802.11g 40MHz (outdoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11 8-12 9-13
802.11a 40MHz (outdoor)   36-40 44-48 52-56 60-64 149-153 157-161
802.11a 80MHz (indoor)    36-48 52-64 149-161
802.11a 80MHz (outdoor)   36-48 52-64 149-161
802.11a 160MHz (indoor)   36-64
802.11a 160MHz (outdoor)  36-64
802.11a (DFS)             52 56 60 64

Max EIRP settings for AP-345 Country Code "IN"
------------------------------------------------
Channel     1     2     3     4     5     6     7     8     9     10    11    12    13    14
-------     -     -     -     -     -     -     -     -     -     --    --    --    --    --
b           27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  *
g/a         27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  *
HT 20       27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  *
HT 40       27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  27.4  *
VHT 80      *     *     *     *     *     *     *     *     *     *     *     *     *     *
VHT 160     *     *     *     *     *     *     *     *     *     *     *     *     *     *
country     36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  36.0  *
DFS         *     *     *     *     *     *     *     *     *     *     *     *     *     *
PSD         *     *     *     *     *     *     *     *     *     *     *     *     *     *
MaxAntGain  6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   *
Corr        n     n     n     n     n     n     n     n     n     n     n     n     n     *

Max EIRP settings for AP-345 Country Code "IN"
------------------------------------------------
Channel         36    40    44    48    52    56    60    64    100  104  108  112  116  120
-------         --    --    --    --    --    --    --    --    ---  ---  ---  ---  ---  ---

                124  128  132  136  140  144  149   153   157   161   165   169  173
                ---  ---  ---  ---  ---  ---  ---   ---   ---   ---   ---   ---  ---
b               *     *     *     *     *     *     *     *     *    *    *    *    *    *
                *     *      *    *    *    *    *     *     *     *     *     *    *
g/a             23.0  23.0  23.0  23.0  23.0  23.0  23.0  23.0  *    *    *    *    *    *
                *     *    *    *    *    *    23.0  23.0  23.0  23.0  23.0  *    *
HT 20           23.0  23.0  23.0  23.0  23.0  23.0  23.0  23.0  *    *    *    *    *    *
                *    *    *    *    *    *    23.0  23.0  23.0  23.0  23.0  *    *
HT 40           23.0  23.0  23.0  23.0  23.0  23.0  23.0  23.0  *    *    *    *    *    *
                *    *    *    *    *    *    23.0  23.0  23.0  23.0  23.0  *    *
VHT 80          23.0  23.0  23.0  23.0  23.0  23.0  23.0  23.0  *    *    *    *    *    *
                *    *    *    *    *    *    23.0  23.0  23.0  23.0  23.0  *    *
VHT 160         23.0  23.0  23.0  23.0  23.0  23.0  23.0  23.0  *    *    *    *    *    *
                *    *    *    *    *    *    *     *     *     *     *     *    *
country         36.0  36.0  36.0  36.0  30.0  30.0  30.0  30.0  *    *    *    *    *    *
                *    *    *    *    *    *    36.0  36.0  36.0  36.0  36.0  *    *
DFS             *     *     *     *     FCC   FCC   FCC   FCC   *    *    *    *    *    *
                *    *    *    *    *    *    *     *     *     *     *     *    *
PSD             17.0  17.0  17.0  17.0  11.0  11.0  11.0  11.0  *    *    *    *    *    *
                *    *    *    *    *    *    33.0  33.0  33.0  33.0  33.0  *    *
MaxAntGain      6.0   6.0   6.0   6.0   6.0   6.0   6.0   6.0   *    *    *    *    *    *
                *    *    *    *    *    *    6.0   6.0   6.0   6.0   6.0   *    *
Corr            y     y     y     y     y     y     y     y     *    *    *    *    *    *
                *    *    *    *    *    *    y     y     y     y     y     *    *
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug rfc3576-radius-statistics

```
show ap debug rfc3576-radius-statistics [termination]
```

Description

This command displays the CoA statistics for the servers configured on an OAW-IAP. Use the output of this command to view the CoA details for debugging authentication and authorization related issues.

Parameter	Description	Range	Default
`termination`	Displays termination details.	—	—

Example

The following example shows the output of the **show ap debug rfc3576-radius-statistics** command:

```
RADIUS RFC3576 Statistics
-------------------------
Statistics                   InternalServer  test      testServer
----------                   --------------  ----      ----------
In Service: Management Auth  Not used        Not used  Not used
In Service: Test1            Up 699292s      Not used  Not used
In Service: ssid1            Up 699292s      Not used  Not used
Disconnect Requests          0               0         0
Disconnect Accepts           0               0         0
Disconnect Rejects           0               0         0
No Secret                    0               0         0
No Session ID                0               0         0
Bad Authenticator            0               0         0
Invalid Request              0               0         0
Packets Dropped              0               0         0
Unknown service              0               0         0
CoA Requests                 0               0         0
CoA Accepts                  0               0         0
CoA Rejects                  0               0         0
No permission                0               0         0
SEQ first/last/free          0/0/0           0/0/0     0/0/0
Packets received from unknown clients ::0
Packets received with unknown request ::0
Total RFC3576 packets Received        ::0
```

The following example shows the output of the **show ap debug rfc3576-radius-statistics termination** command:

```
RADIUS RFC3576 Statistics
-------------------------
Statistics                   t_cppm    t_HOVCLEARPASS  LDAP-none  free-LDAP
----------                   ------    --------------  ---------  ---------
In Service: OCSPTEST         Not used  Not used        Not used   Not used
In Service: Management Auth  Not used  Not used        Not used   Not used
In Service: IPFHUNTV         Not used  Not used        Not used   Not used
In Service: __wired__eth1    Not used  Not used        Not used   Not used
In Service: IPFHUN           Not used  Not used        Not used   Not used
In Service: IPFHUNGuest      Not used  Not used        Not used   Not used
In Service: booth-psk-225    Not used  Not used        Not used   Not used
In Service: booth-open-205   Not used  Not used        Not used   Not used
In Service: IPFNET           Not used  Not used        Not used   Not used
In Service: booth-cp-225     Not used  Not used        Up 90490s  Up 90490s
In Service: booth-dot1x-225  Not used  Not used        Not used   Not used
In Service: aaa              Not used  Not used        Not used   Not used
```

```
Disconnect Requests          0         0               0          0
Disconnect Accepts           0         0               0          0
Disconnect Rejects           0         0               0          0
No Secret                    0         0               0          0
No Session ID                0         0               0          0
Bad Authenticator            0         0               0          0
Invalid Request              0         0               0          0
Packets Dropped              0         0               0          0
Unknown service              0         0               0          0
CoA Requests                 0         0               0          0
CoA Accepts                  0         0               0          0
CoA Rejects                  0         0               0          0
No permission                0         0               0          0
SEQ first/last/free          0/0/0     0/0/0           0/0/0      0/0/0
Packets received from unknown clients ::0
Packets received with unknown request ::0
Total RFC3576 packets Received        ::0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug sa-status

```
show ap debug sa-status
```

Description

This command shows the smart antenna training information for all non-TXBF clients. Use the output of this command to view the smart antenna training details.

Example

The following example shows the output of **show ap debug sa-status** command:

```
SA Status
---------
MAC                ESSID    BSSID              AID   Current Polarization
---                -----    -----              ---   --------------------
            Last Train Cost Time  SA   Last Train PER                       Last Train RATE
            --------------------  --   --------------                       ---------------
0a:19:5f:32:f0:29  IAP_SM   18:64:72:7e:89:52  0x3   0x5
            0                     0x2  00000000-00000000-00000000-00000000  00000000-00000000-
00000000-00000000
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP335	Privileged EXEC mode

show ap debug shaping-table

```
show ap debug shaping-table
```

Description

This command displays the shaping information for clients associated to an OAW-IAP.

Example

The following output is displayed for the **show ap debug shaping-table** command:

```
Interface :wifi1
VAP aruba102
in     out     drop   fail   q    cmn[C:O:H]             Numcl   TotCl  BWmgmt
28     28      0      0      0    328787-328787-328787   0-0-0   0      1
                                -0
d1     d2      d3     d4     d5   d6      d7      d8     d9
0      28      0      28     0    28      0       0      0

idx   tokens    last-t bw-t in   out   drop  fail   q     tx-t   rx-t   al-t  rate
idx   d1        d2     d3   d4   d5    d6    d7     d8      d9      d10
0    2147483647 0      0    0    0     0     0      0      0      0
VAP aruba103
in    out   drop  fail  q    cmn[C:O:H]              Numcl   TotCl  BWmgmt
0      0      0     0     0    328787-328787-328787    0-0-0   0      1
                           -0
d1    d2    d3    d4     d5      d6      d7      d8      d9
0     0     0     0      0       0       0       0       0

idx   tokens last-t bw-t  in   out   drop  fail   q    tx-t   rx-t     al-t    rate
idx   d1         d2      d3      d4      d5      d6      d7      d8      d9     d10
0  2147483647     0       0       0       0       0       0       0        0      0
```

The output of this command provides the following information:

Column	Description
`in`	Shows the number of packets received by the OAW-IAP.
`out`	Shows the number of packets sent by the OAW-IAP.
`drop`	Shows the number of packets dropped by the OAW-IAP.
`fail`	Shows the number of packets failed.
`Numcl`	Shows the number of CCK (802.11b) and OFDM (802.11a or 802.11g) packets dropped.
`TotCl`	Shows the total number of clients associated with the OAW-IAP.
`Bwmgmt`	Displays 1 if the bandwidth management feature has been enabled. Otherwise, it displays a 0.
`idx`	Shows the association index value.
`tokens`	Represents the credits the station has to transmit tokens.
`last-t`	Shows the number of tokens that were allocated to the station last time token allocation algorithm ran.

Column	Description
in	Shows the number of packets received.
out	Shows the number of packets sent.
drop	Shows the number of dropped packets.
q	Shows the number of queued packets.
tx-t	Shows the total time spent transmitting data.
rx-t	Shows the total time spent receiving data.
al-t	Shows the total time allocated for transmitting data to this station.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug spanning-tree

```
show ap debug spanning-tree
```

Description

This command displays the STP information for an OAW-IAP. Use the output of this command to view STP details on anOAW-IAP. STP is enabled for a wired port profile to ensure that there are no loops in any bridged Ethernet network. STP operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on OAW-IAPs with three or more ports.

Example

The following example shows the output displayed for the **show ap debug spanning-tree** command when there are no STP devices found:

```
stpdev
bridge id               f000.000000000000
designated root         f000.000000000000
root port                 0                       path cost                  0
max age                  20.00                    bridge max age            18.08
hello time                2.00                    bridge hello time         10.00
forward delay            34.04                    bridge forward delay      15.00
ageing time              13.29
hello timer               0.82                    tcn timer                  0.00
topology change timer     0.00                    gc timer                  22.55
flags
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug spectrum-channel-details

```
show ap debug spectrum-channel-details
```

Description

This command displays the all the spectrum channels from AM modules. Use the output of this command to view the details of all the spectrum channels.

Example

The following example is an output of the **show ap debug spectrum-channel-details** command:

<please provide an example output for this command>.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug stm-config

```
show ap debug stm-config
```

Description

This command displays the OAW-IAP STM configuration information.

Example

The following output is displayed for the **show ap debug stm-config** command:

```
SSID:
Server Load Balancing:disable
MAC Authentication:disable
RADIUS Accounting:disable
SSID:__wired__eth1
Server Load Balancing:disable
MAC Authentication:disable
RADIUS Accounting:disable
SSID:wireless-local-nw
Server Load Balancing:disable
MAC Authentication:disable
RADIUS Accounting:disable
Associated RADIUS Server:InternalServer
```

The output of this command provides the following information for each SSID:

Column	Description
`SSID`	Indicates the name of the SSID.
`Server Load Balancing`	Indicates if server load balancing is enabled.
`MAC Authentication`	Indicates if MAC authentication is enabled.
`RADIUS Accounting`	Indicates if RADIUS accounting is enabled.
`Associated RADIUS Server`	Displays the authentication server details configured for an SSID.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug stm-role

```
show ap debug stm-role
```

Description

This command displays the STM user roles configured for the SSIDs in an OAW-IAP. Use the output of this command to view the user roles configured for the OAW-IAP STM. This includes details of the VLANs assigned to each SSID and also shows if the Calea feature is enabled or disabled.

Example

The following example shows the output of **show ap debug stm-role** command:

```
User Role
---------
Name                         Index  Vlan  Calea
----                         -----  ----  -----
Test                         4      0     OFF
wired-instant                2      0     OFF
ssid1                        3      0     OFF
default_wired_port_profile   1      0     OFF
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug system-status

```
show ap debug system-status
```

Description

This command displays the detailed system configuration information for an OAW-IAP. Use this command under the guidance of Alcatel-Lucent technical support to troubleshoot network issues. The output of this command displays the following types of information if any for the selected OAW-IAP:

■ Bootstrap information	■ Per-radio statistics	■ Ethernet duplex or speed settings
■ Descriptor Usage	■ Encryption statistics	■ Tunnel heartbeat stats
■ Interface counters	■ OAW-IAP uptime	■ Boot version
■ MTU discovery	■ memory usage	■ LMS information
■ ARP cache	■ Kernel slab statistics	■ Power status
■ Route table	■ Interrupts	■ CPU type
■ Interface Information	■ Crash Information	■ CPU usage statistics

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug tacacs-statistics

```
show ap debug tacacs-statistics
```

Description

This command displays the TACACS statistics for the authentication servers configured on an OAW-IAP.

Example

The output of this command displays general statistics of the authentication servers configured on an OAW-IAP.

```
Tacacs Statistics
-----------------
Statistics
----------
In Service: Management Auth
In Service: Test1
In Service: ssid1
Accounting Requests
Authen Requests
Author Requests
Authen Response Pass
Authen Response Fail
Author Response Pass
Author Response Fail
Accounting Response Pass
Accounting Response Fail
Login Success
Login Failure
Timeouts
AvgRespTime (ms)
Outstanding Auths
SEQ first/last/free
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap debug zigbee socket-table

```
show ap debug zigbee socket-table
```

Description

This command displays the zigbee socket information in the BLE table.

Examples

The following example shows the output of the **show ap debug zigbee socket-table** command:

```
(Instan AP)# show ap debug zigbee socket-table
Zigbee Socket Table
-------------------
Source Endpoint Endpoint Cluster ID Profile ID Direction Options Client Num Radio Bound
Transport DevClass RX Packets RX Bytes RX Errors RX Dropped TX Packets TX Bytes TX Errors TX
Dropped
--------------- -------- ---------- ---------- --------- -------- ---------- ----------- -----
---- -------- ---------- -------- --------- ---------- ---------- -------- --------- --------
--
1 1 0001 c0fb inbound ar 0 all n/a assaAbloy 0 0 0 0 0 0 0 0
1 1 0003 c0fb outbound arn 0 all n/a assaAbloy 0 0 0 0 0 0 0 0
1 1 5678 1234 inbound ar 0 all atw ZSD 0 0 0 0 0 0 0 0
1 1 fc00 7abc outbound ar 0 all atw ZSD 0 0 0 0 0 0 0 0
Flags:
a - raw socket, r - E2PC reused, n - no APS ack
-----------------
Total Zigbee Socket(s):7
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
OAW-AP-303, OAW-AP-303P OAW-AP365/OAW-AP367 OAW-AP303H OAW-IAP304/OAW-IAP305 OAW-AP203R/OAW-AP203RP OAW-IAP207 OAW-IAP334/OAW-IAP335 OAW-IAP314/OAW-IAP315 OAW-APAP-324/OAW-IAP325 OAW-AP-344/OAW-AP-345 OAW-AP515 OAW-530 Series OAW-500 Series	Privileged EXEC mode

show ap dot11k-beacon-report

```
show ap dot11k-beacon-report <mac>
```

Description

This command displays the beacon report details for the 802.11k clients of an OAW-IAP.

Parameter	Description	Range	Default
`<mac>`	Allows you to specify the MAC address of the client for which you want to view the beacon report details.	—	—

Example

The following example shows the output of the **show ap dot11k-beacon-report <mac>** command:

```
(Instant AP)# show ap dot11k-beacon-report 70:11:24:56:02:72
Client:  70:11:24:56:02:72
Status: Success
Nbr count: 4
Last received: 31s
Client 11k Beacon Report
------------------------
BSSID                 Channel       RSSI       Antenna
-----                 ------        -------    -------
6c:f3:7f:b6:62:f0       38                 92  0
6c:f3:7f:b6:69:30        38                94  0
6c:f3:7f:4a:43:d0       46            94       0
6c:f3:7f:b6:66:30       46                92   0
```

The output of this command displays information on the number of 802.11k neighbors, connection status, and the channel, RSSI and antenna details for the specified MAC address.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap dot11k-nbrs

```
show ap dot11k-nbrs
```

Description

This command displays the neighboring details of the 802.11k clients connected to an OAW-IAP.

Example

The following example shows the output of the **show ap dot11k-nbrs** command:

```
 Radio: 0
 Nbr count: 3
 11k Neighbours
 --------------
BSSID                 Channel  Last Update
-----                 ------   -------
6c:f3:7f:b6:62:f0      292      1s
6c:f3:7f:b6:69:30      816      6s
6c:f3:7f:b6:66:30      808      5s
 Radio: 1
 Nbr count: 3
 11k Neighbours
 --------------
BSSID                 Channel  Last Update
-----                 ------   -----------
6c:f3:7f:b6:62:e0      1       13s
6c:f3:7f:b6:66:20      6       33s
6c:f3:7f:b6:69:20      6       33s
```

The output of this command displays information on the number of 802.11k neighbors on each radio of the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap flash-config

```
show ap flash-config
```

Description

This command shows the statistics of the OAW-IAP configuration stored in flash memory. Use the output of this command to view the configuration details in the flash memory.

Example

The following example shows the output of **show ap flash-config** command:

```
IP Address: 10.15.20.252
Network Mask:10.15.22.257
Gateway IP:10.15.20.255
DNS Server: 92.168.1.10
Domain Name: floor1.test.com
Name:Undefined
```

The output of this command includes the following information:

Column	Description
IP Address	Displays the IP address of the OAW-IAP.
Network Mask	Displays the Network mask of the network.
Gateway IP	Displays the Gateway IP address to which traffic is sent.
DNS Server	Displays the IP address of the DNS server.
Domain Name	Displays the Domain name of the server.
Name	Displays the name of the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap ids

```
show ap ids {config | radio}
```

Description

This command displays the IDS configuration and radio whitelist table of the access point.

Parameter	Description
`config`	Displays the IDS configuration of the AP.
`radio`	Displays the list of white-listed radios in the network.

Example

The following extract shows the output of the **show ap ids config** command:

```
90:4c:81:c3:28:1e# show ap ids config

Radio Configuration for wifi0
-----------------------------
Parameter           Value
---------           -----
Preferred Channel   132
Tx Power            18.0
VHT Enabled         1
Radio Configuration for wifi1
-----------------------------
Parameter           Value
---------           -----
Preferred Channel   6
Tx Power            9.0
VHT Enabled         0

ARM Configuration for wifi0
----------------------------
Parameter                                        Value
---------                                        -----
Assignment                                       0
Client Aware                                     1
Mode Aware                                       0
OTA Updates                                      0
Scanning                                         1
Scan Interval                                    10
Rogue AP Aware                                   0
Max Tx Power (cfg/internal)                      6/6
Min Tx Power (cfg/internal)                      4/4
Scan Mode                                        reg-domain
40 MHz/80 MHz                                    1/1
Channel Quality aware/qual thresh/qual wait time 0/70/120
Error rate thresh/error rate wait time           70/90
Noise thresh/noise wait time                     75/120
Aggressive scans                                 0
Frequent scan action                             0
Client Match/Upd intvl                           0/0
Sticky (Intvl/SNR/SNR thr/Min Sig)               0/0/0/0
Bandsteer (g max sig/a min sig)                  0/0
Ideal Coverage Index                             10
Acceptable Coverage Index                        4
Free Channel Index                               25
Backoff Time                                     240
Intf AP Weight                                   25
```

```
HE min sig)                                         0

ARM Configuration for wifi1
----------------------------
Parameter                                           Value
---------                                           -----
Assignment                                          0
Client Aware                                        1
Mode Aware                                          0
OTA Updates                                         0
Scanning                                            1
Scan Interval                                       10
Rogue AP Aware                                      0
Max Tx Power (cfg/internal)                         3/3
Min Tx Power (cfg/internal)                         2/2
Scan Mode                                           reg-domain
40 MHz/80 MHz                                       1/0
Channel Quality aware/qual thresh/qual wait time  0/70/120
Error rate thresh/error rate wait time              70/90
Noise thresh/noise wait time                        75/120
Aggressive scans                                    0
Frequent scan action                                0
Client Match/Upd intvl                              0/0
Sticky (Intvl/SNR/SNR thr/Min Sig)                  0/0/0/0
Bandsteer (g max sig/a min sig)                     0/0
Ideal Coverage Index                                10
Acceptable Coverage Index                           4
Free Channel Index                                  40
Backoff Time                                        240
Intf AP Weight                                      25
HE min sig)                                         0

Scanning Configuration for wifi0
---------------------------------
Parameter                           Value
---------                           -----
Scan-mode                           all-reg-domain
Dwell Time: Active Channel          500
Dwell Time: Reg-Domain Channel      250
Dwell Time: Other Reg-Domain Channel  200
Dwell Time: Rare Channel            100

Scanning Configuration for wifi1
---------------------------------
Parameter                           Value
---------                           -----
Scan-mode                           all-reg-domain
Dwell Time: Active Channel          500
Dwell Time: Reg-Domain Channel      250
Dwell Time: Other Reg-Domain Channel  200
Dwell Time: Rare Channel            100
Regulatory Domain Configuration
-------------------------------
Parameter     Value
---------     -----
Country Code  21

 G-Band 20MHz Channels
-----------------------
Reg Info Type                 Channels
-------------                 --------
Reg Domain Profile
Downloadable Reg Table         1  6  11
AP Cert Info                   1  2  3  4  5  6  7  8  9  10  11
Valid (Assignment) Channels    1  6  11

 A-Band 20MHz Channels
```

```
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        34 36 38 40 42 44 46 48 52 56 60 64 100 104 108 11

                                                 2 116 120 124 128 132 136 140 144 149 153
157 161 165 169 173
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 12

                                                 4 128 132 136 140 144 149 153 157 161 165
Valid (Assignment) Channels   36 40 44 48 52 56 60 64 100 104 108 112 116 120 12

                                                 4 128 132 136 140 144 149 153 157 161 165

 G-Band 40MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        1 7
AP Cert Info                  1 2 3 4 5 6 7
Valid (Assignment) Channels   1 7

 A-Band 40MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 44 52 60 100 108 116 124 132 140 149 157
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 12

                                                 4 128 132 136 140 144 149 153 157 161
Valid (Assignment) Channels   36 44 52 60 100 108 116 124 132 140 149 157

 A-Band 80MHz Channels
-----------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 52 100 116 132 149
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 12

                                                 4 128 132 136 140 144 149 153 157 161
Valid (Assignment) Channels   36 52 100 116 132 149

 A-Band 160MHz Channels
------------------------
Reg Info Type                Channels
-------------                --------
Reg Domain Profile
Downloadable Reg Table        36 100
AP Cert Info                  36 40 44 48 52 56 60 64 100 104 108 112 116 120 12

                                                 4 128
Valid (Assignment) Channels   36 100
AP System Configuration
-----------------------
Parameter        Value
---------        -----
AM Scan RF Band  all
Flex Radio Mode  2g_plus_5g
RF Behavior Configuration
-------------------------
Parameter               Value
---------               -----
Station Handoff Assist  Disable
```

```
RSSI Falloff Wait Time  0
Low RSSI Threshold      0
RSSI Check Frequency    0
Event Thresholds Configuration
------------------------------
Parameter                                Value
---------                                -----
Detect Frame Rate Anomalies              Disable
Bandwidth Rate High Watermark            0
Bandwidth Rate Low Watermark             0
Frame Error Rate High Watermark          0
Frame Error Rate Low Watermark           0
Frame Fragmentation Rate High Watermark  0
Frame Fragmentation Rate Low Watermark   0
Frame Low Speed Rate High Watermark      0
Frame Low Speed Rate Low Watermark       0
Frame Non Unicast Rate High Watermark    0
Frame Non Unicast Rate Low Watermark     0
Frame Receive Error Rate High Watermark  0
Frame Receive Error Rate Low Watermark   0
Frame Retry Rate High Watermark          0
Frame Retry Rate Low Watermark           0
Interference Configuration
--------------------------
Parameter                        Value
---------                        -----
Detect Interference              Disable
Interference Increase Threshold  0
Interference Increase Timeout    0
Interference Wait Time           0
IDS General Configuration
-------------------------

IDS Unauthorized Device Profile Configuration
---------------------------------------------
Parameter                                           Value
---------                                           -----
Detect Adhoc Networks                               Disable
Protect from Adhoc Networks                         Disable
Detect Windows Bridge                               Disable
Protect Windows Bridge                              Disable
Detect Wireless Bridge                              Disable
Wireless Bridge detection Quiet Time                900
Detect Devices with an Invalid MAC OUI              Disable
MAC OUI detection Quiet Time                        900
Rogue AP Classification                             Enable
Valid AP Unseen Timeout                             7200
AP Unseen Timeout                                   600
Overlay Rogue AP Classification                     Disable
OUI-based Rogue AP Classification                   Disable
Propagated Wired MAC based Rogue AP Classification  Disable
Rogue Containment                                   Disable
Suspected Rogue Containment                         Disable
Suspect Rogue Confidence Level                      100
Allow Well Known MACs
Protect Valid Stations                              Disable
Detect Bad WEP                                      Disable
Detect Misconfigured AP                             Disable
Protect Misconfigured AP                            Disable
Protect SSID                                        Disable
Privacy                                             Disable
Require WPA                                         Disable
Detect Unencrypted Valid Clients                    Disable
Unencrypted Valid Clients Quiet Time                900
Protect 802.11n High Throughput Devices             Disable
Protect 802.11n High Throughput 40MHz Devices       Disable
Detect 802.11n Greenfield Activity                  Disable
Detect Adhoc Using Valid SSID                       Disable
Adhoc Using Valid SSID Quiet Time                   900
Protect Adhoc Using Valid SSID                      Disable

Detect Valid Client Misassociation                  Disable
Detect STA Assoc To Rogue                           Disable
Detect Wireless Hosted Network                      Disable
Wireless Hosted Network Quiet Time                  0
Protect From Wireless Hosted Network                Disable
Valid 802.11b channel
Valid 802.11a channel

Config Wired MAC Table
-----------------------
mac
---

Valid OUIs
-----------
OUI
---

Valid and Protected SSIDs
--------------------------
SSID
----
test
```

The following example shows the output of the **show ap ids radio** command:

```
(Instant AP)# show ap ids radio

Swarm Radio Whitelist
---------------------
Radio MAC Address  AP MAC Address
-----------------  --------------
90:4c:81:b2:81:f0  90:4c:81:c3:28:1e
90:4c:81:b2:81:e0  90:4c:81:c3:28:1e
```

The output of the **show ap ids radio** command includes the following information:

Column	Description
`Radio MAC Address`	Displays the MAC address of the radio.
`AP MAC Address`	Displays the MAC address of the AP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The configuration values of **Valid AP Unseen Timeout** and **AP Unseen Timeout** were added to the output of **show ap ids config** command.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap mesh cluster

```
show ap mesh cluster
   active
   configuration
   stats <IP address>
   status
   topology
```

Description

This command shows the mesh cluster details of the AP.

Parameter	Description
`active`	Displays the cluster information of mesh APs in the cluster.
`configuration`	Displays the mesh cluster configuration details of the AP.
`stats <IP address>`	Displays the radio and mesh statistics of the mesh AP at the defined IP address.
`status`	Displays the mesh cluster status and mesh role details of the AP.
`topology`	Displays the topology information of the mesh APs in the cluster.

Example

The following example shows the output of **show ap mesh cluster active** command:

```
Mesh Cluster name: cb02b6b95b8e92c86ad18dea27bfaa3
--------------------------------------------------
Name            AP Type  Mesh Role  IP Address  Portal AP       Parent AP       RSSI  Last
Update  Uplink Age  Children Num  Children List
----            -------  ---------  ----------  ---------       ---------       ----  -------
----  ----------  ------------  -------------
IAP387_mmdev_2  AP-387   Point      3.3.0.127   IAP387_mmdev_1  IAP387_mmdev_1  64    1m:0s
     7m:18s      0             -
IAP387_mmdev_1  AP-387   Portal     3.3.0.126   IAP387_mmdev_1                  0     1m:58s
     11m:52s     1             IAP387_mmdev_2

Total APs: 2
(N): 11N Enabled. (AC): 11AC Enabled. (AD): 11AD Enabled. (AX): 11AX Enabled. For Portals
'Uplink Age' equals uptime.
```

The following example shows the output of **show ap mesh cluster configuration** command:

```
Mesh cluster name :mesh_cluster1
Mesh cluster key  :Manual
```

The following example shows the output of **show ap mesh cluster stats** command:

```
Radio ID : 0
Mesh link on radio : Yes
Mesh link band : 5G
Children Num : 0
Children List : -
Metrics stats:
--------------
Timestamp  RSSI  Channel Utilization (%)  Goodput [Tx] (bps)  Goodput [Rx] (bps)  Throughput
[Tx] (bps)  Throughput [Rx] (bps)
---------  ----  -----------------------  ------------------  ------------------  -----------
----------  ---------------------
```

```
00:12:59   55    35                       21454545            23507208            2047
           2358
00:12:28   84    31                       19994865            24501726            2047
           2799
00:11:58   38    47                       19750623            23037894            2082
           2877
00:11:27   48    33                       21728395            26358381            2082
           2398
00:10:57   41    33                       20127064            24952120            2082
           2398
00:10:26   38    39                       20152671            23505154            2082
           2398
00:09:56   44    34                       21149171            23891598            2012
           2317
00:09:26   44    34                       20124031            25193370            2047
           2398
00:08:55   21    33                       20924702            22237849            2082
           2826
00:08:25   25    32                       21120000            23048231            2082
           2826
00:07:55   39    33                       21405405            24816326            2082
           2398
00:07:24   27    34                       20842105            23812010            2082
           2398
00:06:53   18    33                       27040871            28174570            2674
           11047

Radio ID : 1
Mesh link on radio : Yes
Mesh link band : 60G
Children Num : 0
Children List : -
Metrics stats:
--------------
Timestamp  RSSI  Channel Utilization (%)  Goodput [Tx] (bps)  Goodput [Rx] (bps)  Throughput
[Tx] (bps)  Throughput [Rx] (bps)
---------  ----  -----------------------  ------------------  ------------------  -----------
----------  ---------------------
00:12:59   34    -                        -                   -                   1397
           1538
00:12:28   34    -                        -                   -                   1282
           702
00:11:58   34    -                        -                   -                   1560
           786
00:11:27   34    -                        -                   -                   1355
           1531
00:10:57   34    -                        -                   -                   1340
           1537
00:10:26   34    -                        -                   -                   1282
           1015
00:09:56   34    -                        -                   -                   1414
           1172
00:09:26   34    -                        -                   -                   1469
           1173
00:08:55   34    -                        -                   -                   1323
           1034
00:08:25   34    -                        -                   -                   1281
           716
00:07:55   34    -                        -                   -                   1397
           1118
00:07:24   34    -                        -                   -                   1282
           1456
00:06:53   34    -                        -                   -                   1952
           6152
```

```
Radio ID : 2
Mesh link on radio : No
```

The following example shows the output of **show ap mesh cluster status** command:

```
Mesh cluster      :Enabled
Mesh cluster name :mesh_clusterl
Mesh role         :Mesh Portal
```

The following example shows the output of **show ap mesh cluster topology** command:

```
Mesh Cluster name: cb02b6b95b8e92c86ad18dea27bfaa3
--------------------------------------------------
Name            AP Type  Mesh Role  IP Address  Portal AP       Radio ID  Radio Mode  BSSID
           Parent AP       Path Cost  Node Cost  Link Cost  Hop Count  Rate Tx/Rx  RSSI  Last
Update  Uplink Age  Children Num  Children List
----            -------  ---------  ----------  ---------       --------  ----------  -----
           ---------       ---------  ---------  ---------  ---------  ----------  ----  ----
-------  ----------  ------------  -------------
IAP387_mmdev_2  AP-387   Point      3.3.0.127   IAP387_mmdev_1  0         MPC (AC)
90:4c:81:82:01:50  IAP387_mmdev_1  1          0          0          1          526/468     64
   1m:8s        7m:26s      0             -
1         MPC (AD)    90:4c:81:82:01:01  IAP387_mmdev_1  0          0          0          1
       27/385      34    1m:8s        9m:6s       0             -
IAP387_mmdev_1  AP-387   Portal     3.3.0.126   IAP387_mmdev_1  0         MPP (AC)
90:4c:81:82:26:d0  -               0          1          0          0          -           -
   2m:6s        12m:0s      1             IAP387_mmdev_2
1         MPP (AD)    90:4c:81:82:26:00  -               0          0          0          0
       -           -     2m:6s        12m:0s      1             IAP387_mmdev_2
```

The output of the above commands include the following information:

Column	Description
Mesh cluster	Indicates whether the mesh cluster is enabled or disabled.
Mesh cluster name	Name of the mesh cluster.
Name	Indicates the AP name.
AP Type	Indicates the AP model.
Mesh Role	Indicates the mesh role of the AP.
Parent	Indicates the parent name of the mesh point.
IP Address	IP address of the AP.
Path Cost	Path cost is calculated by analyzing the other components in this command output, adding the link cost, the mesh parent's path cost, and the parent's node cost. Mesh portals typically advertise a path cost of 0, but high-throughput portals add an offset penalty if they are connected to a 10/100 mbps port that is too slow for the high throughput link capacity.
Node Cost	A relative measure of the quality of the node, where a lower number of is more favorable than a higher number. This cost is related to the number of children on the specified node.

Column	Description
`Link Cost`	Represents the quality of the link to an active neighbor. The higher the RSSI, the better the path to the neighbor and the mesh portal. If the RSSI value is below the configured threshold, the link cost is penalized to filter marginal links. A less direct, higher quality link may be preferred over the marginal link. The following factors also affect mesh link metrics: ■ High-throughput APs add a high cost penalty for links as compared to non-high-throughput APs. ■ Multi-stream high-throughput APs add proportional cost penalties for links to high throughput. ■ APs that support fewer streams.
`Hop Count`	Indicates the number of hops it takes for the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0 for a mesh portal and a hop count of 1 or 2 for a mesh point, while all other mesh nodes advertise a cumulative count based on the parent mesh node. The range is 0-8.
`RSSI`	Indicates the RSSI values associated with the mesh networks to which APs are connected.
`Rate Tx/Rx`	Indicates the rate of data frames transmitted and received.
`Last Update`	Indicates when the entries were last updated.
`Uplink`	Indicates the AP's current active uplink.
`Age`	indicates the uptime of the mesh link.
`Children`	Indicates the number of downward mesh point connected to a mesh AP. The range is 0-8
`Children List`	Indicates a string contains all children’s AP name of Mesh AP.
`Parent AP`	Indicates AP name of mesh AP’s parent.
`Portal AP`	Indicates AP Name of mesh AP’s portal.
`Goodput Tx/Rx`	Indicates ratio of the data bytes transmitted and received to the actual air time on mesh AP’s uplink.
`Throughput Tx/Rx`	Indicates ratio of data bytes transmitted and received to the sample period on mesh AP’s uplink.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	■ **active** parameter was added. ■ The output of the **show ap mesh cluster topology** command was modified to include per-radio topology information.
Alcatel-Lucent AOS-W Instant 8.6.0.0	**stats** parameter was added.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap mesh counters

```
show ap mesh counters
```

Description

This command displays the mesh counters for an OAW-IAP. Use the output of this command to view a list of mesh counters available for anOAW-IAP.

Example

The following example shows the output of **show ap mesh counters** command.

```
Mesh Packet Counters
--------------------
Interface  Echo Sent  Echo Recv  Probe Req  Probe Resp   Assoc Req
---------  ---------  ---------  ---------  ----------   ---------
Parent     0          0          770        770(770 HT)  0

Assoc Resp   Assoc Fail  Link up/down  Resel.  Switch  Other Mgmt
----------   ----------  ------------  ------  ------  ----------
0            0           0             -       -       0

Received Packet Statistics: Total 7013859, Mgmt 7013859 (dropped non-mesh 0),
Data 0 (dropped unassociated 0)HT: pns=770 ans=0 pnr=0 ars=0 arr=0 anr=0

Recovery Profile Usage Counters
-------------------------------
Item                         Value
----                         -----
Enter recovery mode          0
Exit recovery mode           0
Total connections to switch  0
Mesh loop-prevention Sequence No.:370765
Mesh timer ticks:370764
d8:c7:c8:c4:42:98# show ap mesh counters
Mesh Packet Counters
--------------------
Interface  Echo Sent  Echo Recv  Probe Req  Probe Resp   Assoc Req
---------  ---------  ---------  ---------  ----------   ---------
Parent     0          0          770        770(770 HT)  0

Assoc Resp  Assoc Fail  Link up/down  Resel.  Switch  Other Mgmt
----------  ----------  ------------  ------  ------  ----------
0           0           0             -       -       0

Received Packet Statistics: Total 7016747, Mgmt 7016747 (dropped non-mesh 0),
Data 0 (dropped unassociated 0)HT: pns=770 ans=0 pnr=0 ars=0 arr=0 anr=0

Recovery Profile Usage Counters
-------------------------------
Item                         Value
----                         -----
Enter recovery mode          0
Exit recovery mode           0
Total connections to switch  0
Mesh loop-prevention Sequence No.:370891
Mesh timer ticks:370890
```

Column	Description
`Interface`	Indicates whether the mesh interface connects to a Parent OAW-IAP or a Child OAW-IAP. Each row of data in the Mesh Packet Counters table shows counter values for an individual interface.
`Echo Sent`	Number of echo packets sent.
`Echo Recv`	Number of echo packets received.
`Probe Req`	Number of probe request packets sent from the interface specified in the Mesh-IF parameter.
`Probe Resp`	Number of probe response packets sent to the interface specified in the Interface parameter.
`Assoc Req`	Number of association request packets from the interface specified in the Interface parameter.
`Assoc Resp`	Number of association response packets from the interface specified in the Interface parameter. This number includes valid responses and fail responses.
`Assoc Fail`	Number of fail responses received from the interface specified in the Interface parameter.
`Link up/down`	Number of times the link up or link down state has changed.
`Resel`	Number of times a mesh point attempted to reselect a different mesh portal.
`Switch`	Number of times a mesh point successfully switched to a different mesh portal.
`Other Mgmt`	Management frames of any type other than association and probe frames, either received on child interface, or sent on parent interface.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap mesh link

```
show ap mesh link
```

Description

This command shows the mesh link information of the OAW-IAP.

Example

The following example shows the output of **show ap mesh link** command:

```
Neighbor list
-------------
Radio  MAC                Portal  Channel  Age  Hops  Cost  Relation                 Flags
RSSI  Rate Tx/Rx  A-Req  A-Resp  A-Fail  HT-Details        Cluster ID
-----  ---                ------  -------  ---  ----  ----  -----------------        -----   -
---  ----------  -----  ------  ------  ----------        ----------
2      20:a6:cd:71:59:f0  Yes     149E     0    0     5.00  P 2m:42s                 VLK
61    48/1733     1      1       0       VHT-80MHzsgi-4ss  7d1e081541800e8b7a6d9b94b570836

Total count: 1, Children: 0
Relation: P = Parent; C = Child; N = Neighbor; B = Blacklisted-neighbor
Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure;
H = High Throughput; V = Very High Throughput, E= High efficient, L = Legacy allowed
K = Connected; U = Upgrading; G = Descendant-upgrading; Z = Config pending; Y = Assoc-
resp/Auth pending
a = SAE Accepted; b = SAE Blacklisted-neighbour; e = SAE Enabled; u = portal-unreachable; o =
opensystem
```

The output of this command includes the following information:

Column	Description
`Radio`	Radio used for the mesh link.
`MAC`	MAC address of the mesh node.
`Portal`	By default, this column displays the BSSID of the mesh point. If you include the optional names parameter, this column will display OAW-IAP names, if available. The OAW-IAP names will include [p] (parent), or [c] (child) suffixes to indicate the role of the mesh BSSID.
`Channel`	Number of a radio channel used by the OAW-IAP.
`Age`	Number of seconds elapsed since the OAW-IAP heard from the neighbor.
`Hops`	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node.
`Cost`	A relative measure of the quality of the path from the OAW-IAP to the switch. A lower number indicates a better quality path, where a higher number indicates a less favorable path (For example, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
`Relation`	Shows the relationship between the specified OAW-IAP and the OAW-IAP on the neighbor list and the amount of time that relationship has existed. ▪ P = Parent ▪ C = Child

Column	Description
	- N = Neighbor - B = Blacklisted-neighbor
`Flags`	This parameter shows additional information about the mesh neighbor. The key describing each flag is displayed at the bottom of the neighbor list.
`RSSI`	The RSSI value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
`Rate Tx/Rx`	The rate, in Mbps, that a neighbor transmits data to or receives data from the mesh-node specified by the command.
`A-Req`	Number of association requests from clients.
`A-Resp`	Number of association responses from the mesh node.
`A-Fail`	Number of association failures.
`Cluster ID`	Name of the Mesh cluster that includes the specified OAW-IAP or BSSID.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of the command was modified to include the radio information of the AP.
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap mesh neighbors

```
show ap mesh neighbors
```

Description

This command shows all mesh neighbors for anOAW-IAP.

Example

The following example shows the output of **show ap mesh neighbors** command:

```
(Instant AP)# show ap mesh neighbours

Neighbor list
-------------
Radio  MAC                Portal             Channel  Age  Hops  Cost   Relation
   Flags  RSSI  Rate Tx/Rx  A-Req  A-Resp  A-Fail  HT-Details        Cluster ID
-----  ---                ------             -------- ---  ----  ----   ------------------
   -----  ----  ----------  -----  ------  ------  ----------        ----------
0      b4:5d:50:d4:67:50  Yes                36E      45   0     7.00   N 45s
   VLK    12    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
0      48:4a:e9:7c:d2:b1  Yes                48       70   0     33.00  N 1m:10s
   ELK    45    -           0      0       0       HE-20MHzsgi-2ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      b4:5d:50:d4:63:70  Yes                36E      45   0     7.00   N 45s
   VLK    23    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
0      b4:5d:50:d4:63:f0  Yes                36E      45   0     6.00   N 45s
   VLK    23    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
0      9c:8c:d8:23:d3:d1  Yes                64       56   0     34.00  N 56s
   SELK   7     -           0      0       0       HE-20MHzsgi-4ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      40:e3:d6:56:a1:b0  Yes                40E      43   0     6.00   N 43s
   VLK    24    -           0      0       0       VHT-80MHzsgi-4ss  Sun_mesh1
0      48:4a:e9:7c:d5:d1  Yes                36       45   0     33.00  N 45s
   ELK    25    -           0      0       0       HE-20MHzsgi-2ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      48:4a:e9:7c:cb:f1  Yes                40       43   0     33.00  N 43s
   ELK    27    -           0      0       0       HE-20MHzsgi-2ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      48:4a:e9:7c:e2:11  Yes                40       43   0     48.00  N 43s
   SELK   8     -           0      0       0       HE-20MHzsgi-2ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      b4:5d:50:d4:63:d0  Yes                36E      45   0     6.00   N 45s
   VLK    33    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
0      b4:5d:50:d4:9e:d0  Yes                52E      69   0     6.00   N 1m:9s
   VLK    14    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
0      9c:8c:d8:23:cf:11  Yes                52       69   0     30.00  N 1m:9s
   SELK   9     -           0      0       0       HE-20MHzsgi-4ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
0      b4:5d:50:d4:6e:70  b4:5d:50:d4:63:70  36       45   1     24.00  N 45s
   VLK    17    -           0      0       0       VHT-20MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
2      20:a6:cd:71:59:f0  Yes                149E      0   0     4.00   P 39s
   VLK    59    1300/1733   1      1       0       VHT-80MHzsgi-4ss
7d1e081541800e8b7a6d9b94b570836
2      38:17:c3:00:07:b0  Yes                149E      0   0     6.00   N 4m:11s
   VLoK   50    -           0      0       0       VHT-80MHzsgi-2ss  aruba-mesh-yinzhi
```

```
2      38:17:c3:91:d4:91  f0:5c:19:1c:7d:f1  153E     52   1     9.00   N 52s
   VLK    41    -           0      0       0       VHT-80MHzsgi-4ss  xzhang2_mon_1
2      38:17:c3:91:fb:71  38:17:c3:91:fb:61  149E     85   0     4.00   N 1m:14s
   VLK    61    -           1      1       0       VHT-80MHzsgi-4ss
7d1e081541800e8b7a6d9b94b570836
2      d0:15:a6:ba:ae:11  Yes                161      50   0     17.00  N 50s
   ELK    30    -           0      0       0       HE-20MHzsgi-2ss
76bbbd2dd7bc0f4a6c52dec7cb3628f
2      b4:5d:50:d4:64:10  Yes                149E      0   0     4.00   N 4m:11s
   VLK    33    -           0      0       0       VHT-80MHzsgi-4ss
ff6c4c436b49c4e4d958cfee28748b2
2      34:fc:b9:2f:51:f0  34:fc:b9:2f:71:50  149E      0   2     7.00   N 4m:11s
   VLK    24    -           0      0       0       VHT-80MHzsgi-3ss
6b6fd5e60177ba0ce6e2b9f7d903d36
2      90:4c:81:73:ee:f1  a8:bd:27:7f:63:20  149E      0   1     7.00   N 4m:11s
   ELK    51    -           0      0       0       HE-80MHz-4ss      mesh-5

Total count: 36, Children: 0
Relation: P = Parent; C = Child; N = Neighbor; B = Blacklisted-neighbor
Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure;
H = High Throughput; V = Very High Throughput, E= High efficient, L = Legacy allowed
K = Connected; U = Upgrading; G = Descendant-upgrading; Z = Config pending; Y = Assoc-
resp/Auth pending
a = SAE Accepted; b = SAE Blacklisted-neighbour; e = SAE Enabled; u = portal-unreachable; o =
opensystem
```

The output of this command includes the following information:

Column	Description
`Radio`	Radio information of the mesh neighbor AP.
`MAC`	MAC address of the mesh node.
`Portal`	By default, this column displays the BSSID of the mesh point. If you include the optional names parameter, this column will display OAW-IAP names, if available. The OAW-IAP names will include [p] (parent), or [c] (child) suffixes to indicate the role of the mesh BSSID.
`Channel`	Number of a radio channel used by the OAW-IAP.
`Age`	Number of seconds elapsed since the OAW-IAP heard from the neighbor.
`Hops`	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node.
`Cost`	A relative measure of the quality of the path from the OAW-IAP to the Virtual Controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
`Relation`	Shows the relationship between the specified OAW-IAP and the OAW-IAP on the neighbor list and the amount of time that relationship has existed. ■ P = Parent ■ C = Child ■ N = Neighbor ■ B = Blacklisted-neighbor

Column	Description
`Flags`	This parameter shows additional information about the mesh neighbor. The key describing each flag is displayed at the bottom of the neighbor list.
`RSSI`	The RSSI value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
`Rate Tx/Rx`	The rate, in Mbps, that a neighbor transmits data to or receives data from the mesh-node specified by the command.
`A-Req`	Number of association requests from clients.
`A-Resp`	Number of association responses from the mesh node.
`A-Fail`	Number of association failures.
`Cluster ID`	Name of the Mesh cluster that includes the specified OAW-IAP or BSSID.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	The output of the command was modified to include the radio information of the AP.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap monitor

```
show ap monitor {active-laser-beams|ap-list|ap-wired-mac <mac>|arp-cache| arp-vlan-cache |
containment-info|
enet-wired-mac <mac>| ids-state <type>| pot-ap-list | pot-sta-list| rogue-ap <mac>| routers|
scan-info| sta-list|
state <mac>| stats  <mac>| status| swarm-radio-list}
```

Description

This command shows information for OAW-IAP AMs.

Parameter	Description	Range	Default
`active-laser-beams`	Shows active laser beam generators. The output of this command shows a list of all OAW-IAPs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which OAW-IAP is sending out deauthorization frames, although it does not specify which OAW-IAP is being contained.	—	—
`ap-list`	Shows list of OAW-IAPs being monitored.	—	—
`ap-wired-mac`	Shows the MAC address of the wired OAW-IAP.	—	—
`arp-cache`	Shows ARP Cache of learned IP to MAC binding.	—	—
`arp-vlan-cache`	Shows ARP cache that contains VLAN tags.	—	—
`containment-info`	Shows containment events and counters triggered by the wired containment and wireless containment features configured in the ids. The output of this command shows device and target data for wired containment activity, as well as data for the following counters. Wireless Containment Counters: ■ Last Deauth Timer Tick ■ Deauth frames to OAW-IAP ■ Deauth frames to Client ■ Last Tarpit Timer Tick ■ Tarpit Frames: Probe Response ■ Tarpit Frames: Association Response ■ Tarpit Frames: Authentication ■ Tarpit Frames: Data from OAW-IAP ■ Tarpit Frames: Data from Client ■ Last Enhanced ad hoc Containment Timer Tick ■ Enhanced ad hoc Containment: Frames To Data Sender ■ Enhanced ad hoc Containment: Frames To Data Receiver ■ Enhanced ad hoc Containment:	—	—

Parameter	Description	Range	Default
	Response to Request Enhanced Ad Hoc Containment: Replay Response Wired Containment Counters: ■ Last Wired Containment Timer Tick ■ Last Tagged Wired Containment Timer Tick ■ Spoof frames sent ■ Spoof frames sent on tagged VLAN		
`enet-wired-mac`	Shows Wired MAC Addresses learned.	—	—
`ids-state <type>`	Shows IDS State.	—	—
`pot-ap-list`	Display the Potential OAW-IAP table. The Potential OAW-IAP table shows the following data: ■ bssid: The BSSID of the OAW-IAP. ■ channel: The current radio channel of the OAW-IAP. ■ phy type: The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b or 802.11g, 802.11b or 802.11g-HT-20. ■ num-beacons: Number of beacons seen during a 10-second scan ■ tot-beacons: Total number of beacons seen since the last reset. ■ num-frames: Total number of frames seen since the last rest. ■ mt: Monitor time; the number of timer ticks elapsed since the first OAW-IAP is recognized. ■ at: Active time, in timer ticks. ■ ibss: Shows if ad hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad hoc BSS (an ibss bit in an 802.11 frame). ■ rssi: The RSSI value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.	—	—
`pot-sta-list`	Shows the Potential client table. The Potential Client table shows the following values: ■ last-bssid: the Last BSSID to which the client associated. ■ from-bssid, ■ to-bssid ■ mt:Monitor time; the number of timer ticks elapsed since the first client is recognized. ■ it: Client Idle time, expressed as a number of timer ticks.	—	—
`rogue-ap <mac>`	Displays rogue OAW-IAPs information for the current OAW-IAP.	—	—

Parameter	Description	Range	Default
routers	Shows the Router MAC Addresses that were learned. The output of this command includes the router’s MAC address, IP address and uptime.	—	—
scan-info	Shows scanned information for the OAW-IAP.	—	—
sta-list	Shows the configuration and status of monitor information of the OAW-IAP.	—	—
state	Shows the OAW-IAP monitoring state.	—	—
stats	Shows the OAW-IAP monitoring statistics.	—	—
status	Shows the status of the OAW-IAP monitoring.	—	—

Examples

show ap monitor active-laser-beams

The following example shows the output of **show ap monitor active-laser-beams** command:

```
Active Laser Beam Sources
-------------------------
bssid  channel  rssi  ap name  lms ip  master ip  inactive time

-----  -------  ----  -------  ------  ---------  -------------
```

show ap monitor ap-list

The following example shows the output of **show ap monitor ap-list** command:

```
Monitored AP Table
------------------
bssid              essid                            chan  ap-type      transition-type
-----              -----                            ----  -------      ---------------
c8:b5:ad:ba:f9:80  345                              1     valid        valid
f0:5c:19:1e:39:e0  345                              36E   valid        valid
ac:a3:1e:dd:c7:f0  UCC-Campus                       36    interfering  interfering
ac:a3:1e:dd:c7:f4  UCC-Employee                     36    interfering  interfering
ac:a3:1e:dd:c7:f5  UCC-Student                      36    interfering  interfering
ac:a3:1e:dd:c7:f7  225                              36    interfering  interfering
6c:f3:7f:77:b6:d2  155                              36    interfering  interfering
f0:5c:19:1d:b6:b2  207mesh                          36    interfering  interfering
f0:5c:19:1d:b6:b3  2200                             36    interfering  interfering
f0:5c:19:1d:b6:b4  222                              36    interfering  interfering
6c:f3:7f:78:60:92  155                              36    interfering  interfering
6c:f3:7f:78:60:82  155                              6     interfering  interfering
f0:5c:19:1f:9c:60  zefeng325psk                     1     interfering  interfering
f0:5c:19:1f:9c:61  hm                               1     interfering  interfering
f0:5c:19:1f:9c:62  hm1                              1     interfering  interfering
f0:5c:19:1d:b6:a4  222                              11    interfering  interfering

f0:5c:19:1d:b6:a3  2200                             11    interfering  interfering

f0:5c:19:1d:b6:a2  207mesh                          11    interfering  interfering
f0:5c:19:1e:39:f0  345                              6     interfering  interfering
ac:a3:1e:d2:a6:e0  rfcage1                          6     interfering  interfering

6c:f3:7f:77:b6:c2  155                              1     interfering  interfering
```

```
d0:bf:9c:3d:1f:0e  HP-Print-0E-Deskjet 4640 series  11    interfering  interfering
c8:b5:ad:ba:f9:90  345                              36E   valid        valid
ac:a3:1e:d2:a6:f0  rfcage1                          132E  interfering  interfering

confirmed  phy-type        dos      dt/mt        ut/it  encr
---------  --------        ---      -----        -----  ----
no         80211b/g-HT-20  disable  12182/12182  0/0    open
yes        80211a-VHT-80   disable  12177/12177  0/0    open
no         80211a-VHT-20   disable  12177/12177  0/0    wpa2-8021x-aes
no         80211a-VHT-20   disable  12177/12177  0/0    wpa2-psk-aes
no         80211a-VHT-20   disable  12177/12177  0/0    wpa2-8021x-aes
no         80211a-VHT-20   disable  12177/12177  0/0    open
no         80211a-HT-20    disable  12177/12177  0/0    open
no         80211a-VHT-20   disable  12177/12177  0/0    wpa2-8021x-aes
no         80211a-VHT-20   disable  12177/12177  0/0    open
no         80211a-VHT-20   disable  12177/12177  0/0    open
no         80211a-HT-20    disable  12177/12177  0/3    open
no         80211b/g-HT-20  disable  12176/5813   1/0    open
no         80211b/g-HT-20  disable  12176/10093  0/0    wpa2-psk-aes
no         80211b/g-HT-20  disable  12176/10093  0/0    wpa2-psk-aes
no         80211b/g-HT-20  disable  12176/10093  0/0    wpa2-psk-aes
no         80211b/g-HT-20  disable  12176/1936   4/0    open
no         80211b/g-HT-20  disable  12174/1933   3/0    open
no         80211b/g-HT-20  disable  12174/1934   1/0    wpa2-8021x-aes
no         80211b/g-HT-20  disable  12146/543    0/0    open
no         80211b/g-HT-20  disable  12117/387    11/0   wpa2-psk-aes
no         80211b/g-HT-20  disable  12098/5402   32/31  open
no         80211b/g        disable  11897/2280   47/1   wpa2-psk-aes
no         80211a-VHT-80   disable  7640/7640    0/0    open
no         80211a-VHT-80   disable  2834/63      22/0   wpa2-psk-aes

 nstas  avg-snr  curr-snr  avg-rssi  curr-rssi  wmacs  ibss  cl-delay
 -----  -------  --------  --------  ---------  -----  ----  --------
 0      45       45        50        50         0      no    0
 0      64       64        30        31         2      no    0
 1      55       56        39        39         0      no    0
 0      55       55        39        40         0      no    0
 0      55       55        39        40         0      no    0
 0      55       56        39        39         0      no    0
 0      56       55        38        40         0      no    0
 0      71       71        23        24         0      no    0
 0      71       71        24        24         0      no    0
 0      70       71        24        24         0      no    0
 0      52       52        42        43         0      no    0
 0      59       58        35        37         0      no    0
 0      62       55        32        40         0      no    0
 0      62       55        32        40         0      no    0
 0      62       55        32        40         0      no    0
 0      0        73        0         22         0      no    0
 0      0        73        0         22         0      no    0
 0      0        73        0         22         0      no    0
 0      0        46        0         49         0      no    0
 0      51       52        44        43         0      no    0
 0      69       69        25        26         0      no    0
 0      0        57        0         38         0      no    0
 1      25       25        70        70         2      no    0
 0      59       59        36        36         0      no    0

Start:0
Length:24
Total:24
345--c8:b5:ad:c3:af:98#
```

show ap monitor ap-wired-mac <mac>

The following example shows the output of **show ap monitor ap-wired-mac <mac>** command:

```
Wired MAC Table
---------------
mac  age
```

show ap monitor arp-cache

The following example shows the output of **show ap monitor arp-cache** command:

```
br0:10.17.88.188
ARP Cache Table
mac                ip            vlanid  age
---                --            ------  ---
d8:c7:c8:cb:d4:20  10.17.88.188  0       1s
d8:c7:c8:cb:d3:d4  10.17.88.186  0       1s
00:0b:86:40:1c:a0  10.17.88.129  0       1m:18s
```

show ap monitor arp-vlan-cache

The following example shows the output of **show ap monitor arp-vlan-cache** command:

```
br0:10.65.130.92
ARP VLAN Cache Table
--------------------
mac                ip             vlanid  age
---                --             ------  ---
00:1a:1e:01:94:e8  10.65.128.1    128     50s
18:64:72:c6:d5:fe  10.65.134.202  128     3m:36s
f0:1f:af:27:5d:64  10.65.128.241  128     57s
20:4c:03:05:e0:80  10.65.128.248  128     8m:27s
00:07:85:3a:5d:20  10.65.128.58   128     9m:21s
00:1a:1e:01:93:b0  10.65.128.249  128     5m:52s
00:1a:1e:01:bf:48  10.65.128.250  128     9m:21s
d4:ae:52:ca:15:82  192.168.0.120  128     4s
d4:ae:52:d2:01:a5  192.168.0.120  128     17s
00:1a:1e:15:86:00  10.65.128.92   128     9m:12s
```

show ap monitor containment-info

The following example shows the output of **show ap monitor containment-info** command:

```
br0:10.17.88.188
ARP Cache Table
---------------
mac                ip            vlanid  age
---                --            ------  ---
d8:c7:c8:cb:d4:20  10.17.88.188  0       1s
d8:c7:c8:cb:d3:d4  10.17.88.186  0       1s
00:0b:86:40:1c:a0  10.17.88.129  0       1m:18s
```

show ap monitor enet-wired-mac

The following example shows the output of **show ap monitor enet-wired-mac** command:

```
Wired MAC Table
---------------
mac  age
```

show ap monitor ids-state

Use this command to view information about the IDS the following detection polices:

- Detect Block ACK DOS
- Disconnect station attack
- Intrusion event Type

- Intrusion rate parameters
- Detect Omerta attack
- Detect Power Save DOS Attack
- Detect Rate Anomaly
- Sequence
- IDS Signature— Deauthentication Broadcast and Deassociation Broadcast
- Detect AP Spoofing
- Valid and Protected SSIDs (from IDS Unauthorized Device Profile)

The following example shows the output of **show ap monitor ids-state valid-ssid** command.

```
System Generated (using WLAN SSID profile configuration)
---------------------------------------------------------
SSID
----
Valid and Protected SSIDs (from IDS Unauthorized Device Profile)
------------------------------------------------------------------
SSID
----
example1
example-local-nw
a36534e02ee1f3a7edeb0c247d07c9b
```

show ap monitor pot-ap-list

The following example shows the output of **show ap monitor pot-ap-list** command.

```
Potential AP Table
------------------
bssid              channel  phy     num-beacons  tot-beacons
-----              -------  ---     -----------  -----------
d8:c7:c8:3d:3b:13  161      80211a  0            9
d8:c7:c8:3d:3b:03  1        80211b  0            9
00:24:6c:81:64:a8  36       80211a  0            9
00:24:6c:81:64:a9  36       80211a  0            9
00:24:6c:80:7a:a2  6        80211b  0            0

num-frames  mt  it   at  ibss     rssi
----------  --  --   --  ----     ----
0           3   352  1   disable  26
0           4   363  1   disable  43
0           3   185  2   disable  17
0           1   45   1   disable  17
0           1   1    1   disable  30

Num Potential APs:5
```

show ap monitor pot-sta-list

The following example shows the output of **show ap monitor pot-sta-list** command.

```
Potential Client Table
----------------------
mac                last-bssid         from-bssid
---                ----------         ----------
00:24:d7:40:bb:b0  00:1a:1e:17:dc:62  00:00:00:00:00:00
60:67:20:5f:e1:94  00:1a:1e:17:d4:a0  00:00:00:00:00:00
58:94:6b:a0:47:74  00:1a:1e:17:d4:a1  00:00:00:00:00:00
b0:ec:71:98:da:44  00:24:6c:80:55:b0  00:00:00:00:00:00
00:27:10:2a:c6:ac  00:1a:1e:17:d4:a1  00:00:00:00:00:00
b0:65:bd:dc:51:8a  00:24:6c:80:03:4e  00:00:00:00:00:00
74:e1:b6:15:1b:5f  d8:c7:c8:3d:42:13  00:00:00:00:00:00
60:67:20:5b:33:28  00:1a:1e:17:d4:a1  00:00:00:00:00:00
```

```
00:27:10:5c:23:78  00:24:6c:80:fd:72  00:00:00:00:00:00
00:24:d6:9d:7c:28  00:24:6c:80:a3:90  00:00:00:00:00:00
58:94:6b:b3:14:a8  00:24:6c:80:03:4e  00:00:00:00:00:00
24:77:03:d0:0a:d8  00:1a:1e:17:dc:62  00:00:00:00:00:00
24:77:03:7a:7f:40  6c:f3:7f:94:63:80  00:00:00:00:00:00
24:77:03:ce:a5:fc  00:24:6c:80:4f:80  00:00:00:00:00:00
00:23:14:9d:ba:f0  00:1a:1e:17:d4:a1  00:00:00:00:00:00
24:77:03:cf:09:2c  00:24:6c:80:4f:81  00:00:00:00:00:00
24:77:03:d1:05:b0  00:1a:1e:17:dc:62  00:00:00:00:00:00
24:77:03:7a:89:50  00:24:6c:80:a3:91  00:00:00:00:00:00

       to-bssid           mt   it   channel  rssi
       --------           --   --   -------  ----
      00:00:00:00:00:00  133  50   7        44
      00:00:00:00:00:00  6    43   7        0
      00:00:00:00:00:00  217  104  7        0
      00:00:00:00:00:00  37   2    7        0
      00:00:00:00:00:00  72   50   7        30
      00:00:00:00:00:00  217  10   149      11
      00:00:00:00:00:00  164  19   149      10
      00:00:00:00:00:00  6    5    7        0
      00:00:00:00:00:00  56   53   7        27
      00:00:00:00:00:00  97   96   7        28
      00:1c:b0:eb:d7:00  154  1    7        14
      00:00:00:00:00:00  19   14   7        16
      00:00:00:00:00:00  42   41   7        0
      00:00:00:00:00:00  143  16   7        0
      00:00:00:00:00:00  158  36   7        0
      00:00:00:00:00:00  117  57   7        22
      00:00:00:00:00:00  169  33   7        37
      00:24:6c:80:a3:9a  248  20   7        37
```

show ap monitor routers

The following example shows the output of **show ap monitor routers** command.

```
Wired MAC of Potential Wireless Devices
----------------------------------------
mac  ip  age
---  --  ---
```

show ap monitor scan-info

The following example shows the output of **show ap monitor scan-info** command.

```
WIF Scanning State: wifi0: d8:c7:c8:3d:42:10
---------------------------------------------
Parameter                      Value
---------                      -----
Probe Type                     m-portal
Phy Type                       80211a-HT-40
Scan Mode                      reg-domain
Scan Channel                   no
Disable Scanning               yes
RegDomain Scan Completed       yes
DOS Channel Count              0
Current Channel                149+
Current Scan Channel           153-
Current Channel Index          9
Current Scan Start Milli Tick  232927000
Current Dwell Time             110
Current Scan Type              active
Scan-Type-Info
---------------
```

```
Info-Type          Active  Reg-domain  All-reg-domain  Rare  DOS
---------          ------  ----------  --------------  ----  ---
Dwell Times        500     250         200             100   500
Last Scan Channel  153-    44+         0               0     0
```

show ap monitor state

The following example shows the output of **show ap monitor state <mac>** command.

```
DoS State
----------
tx  old-tx  rx  old-rx  last-dos-time  ap-ev-time
--  ------  --  ------  -------------  ----------
0   0       0   0       0              0

sta-ev-time  last-enhanced-cm-time  enhanced-cm-ev-time
-----------  ---------------------  -------------------
0            0                      0
```

show ap monitor stats

The following example shows the output of **show ap monitor stats** command.

```
(Instant AP)# show ap monitor stats d8:c7:c8:cb:d4:22
Aggregate Stats
---------------
retry  low-speed  non-unicast  recv-error  frag  bwidth
-----  ---------  -----------  ----------  ----  ------
0      0          0            0           0     0
RSSI
----
avg-signal  low-signal  high-signal  count  duration (sec)
----------  ----------  -----------  -----  --------------
40          40          40           748    70
AP Impersonation State
----------------------
beacons  prev-beacons  exp-beacons  beacon-interval  imp-time  imp-active  wait-time
-------  ------------  -----------  ---------------  --------  ----------  ---------
0        11            11.00        100              0         0           0
AP Non-beacon-Frames:0
AP Tarpit Fake Channel:0
Raw Stats
---------
tx-pkt   tx-byte    rx-pkt  rx-byte  tx-retry-pkt
------   -------    ------  -------  ------------
2662202  830665629  31438   440132   0

rx-retry-pkt  tx-frag-pkt  rx-frag-pkt  short-hdr-pkt  long-hdr-pkt
------------  -----------  -----------  -------------  ------------
0             0            0            2662202        0

Frame Type Stats
----------------
type  mgmt-pkt  mgmt-byte  ctrl-pkt  ctrl-byte  data-pkt  data-byte
----  --------  ---------  --------  ---------  --------  ---------
tx    2662202   830665629  0         0          0         0
rx    0         0          31438     440132     0         0
Dest Addr Type Stats
--------------------
bcast-pkt  bcast-byte  mcast-pkt  mcast-byte  ucast-pkt  ucast-byte
---------  ----------  ---------  ----------  ---------  ----------
0          0           0          0           0          0
Frame Size Packet Stats
-----------------------
```

```
type  0-63  64-127  128-255  256-511  512-1023  1024+
----  ----  ------  -------  -------  --------  -----
tx    0     0       0        0        0         0
rx    0     0       0        0        0         0
Frame Rate Stats
----------------
type  pkt-6m  byte-6m  pkt-9m  byte-9m
----  ------  -------  ------  -------
tx    0       0        0       0
rx    0       0        0       0

pkt-12m  byte-12m  pkt-18m  byte-18m
-------  --------  -------  --------
0        0         0        0
0        0         0        0

byte-24m  pkt-36m  byte-36m  pkt-48m  byte-48m  pkt-54m  byte-54m
--------  -------  --------  -------  --------  -------  --------
0         0        0         0        0         0        0
0         0        0         0        0         0        0

HT RX Rate Stats
----------------
Rate  Pkts  Bytes
----  ----  -----
HT TX Rate Stats
-----------------
Rate  Pkts  Bytes
----  ----  -----
Detailed RSSI
-------------
10s  2m   3m   4m   5m   6m   7m   8m   9m   10m  11m  12m  13m  14m  15m
-        ---  --   --   --   --   --   --   --   --   ---  ---  ---  ---  ---  ---
average  40   40   40   40   40   40   40   40   40   40   40   40   40   40   40
high     40   40   40   40   40   40   40   40   40   40   40   40   40   40   40
low      40   40   40   40   40   40   40   40   40   40   40   40   40   40   40
count    110  638  638  638  638  638  649  649  638  638  429  649  638  528  649
Monitored Time:233496
Last Packet Time:233528
Uptime:233529
DoS State
----------
tx  old-tx  rx  old-rx  last-dos-time  ap-ev-time
--  ------  --  ------  -------------  ----------
0   0       0   0       0              0

sta-ev-time  last-enhanced-cm-time  enhanced-cm-ev-time
-----------  ---------------------  -------------------
 0            0                      0
```

show ap monitor status

The following example shows the output of **show ap monitor status** command.

```
AP Info
-------
key           value
---           -----
Uptime        233059
AP Name       d8:c7:c8:cb:d4:20
LMS IP        0.0.0.0
Master IP     0.0.0.0
AP Type       135
Country Code  21
```

```
Wired Interface
----------------
mac                ip            gw-ip         gw-mac
---                --            -----         ------
d8:c7:c8:cb:d4:20  10.17.88.188  10.17.88.129  00:0b:86:40:1c:a0

status  pkts  macs  gw-macs  dot1q-pkts  vlans
------  ----  ----  -------  ----------  -----
enable  2660  4     1        0           0

WLAN Interface
---------------
bssid              scan    monitor  probe-type  phy-type        task   channel  pkts
-----              ----    -------  ----------  --------        ----   -------  ----
d8:c7:c8:3d:42:10  enable  enable   m-portal    80211a-HT-40    tuned  149+     17332616
d8:c7:c8:3d:42:00  enable  enable   sap         80211b/g-HT-20  tuned  1        56090990
WLAN packet counters
---------------------
Interface                 Packets Read  Bytes Read  Interrupts  Buffer Overflows
---------                 ------------  ----------  ----------  ----------------
d8:c7:c8:3d:42:10(wifi0)  17332616      401055780   12288142    703
d8:c7:c8:3d:42:00(wifi1)  56090990      3565742575  50110266    13315

Max PPS  Cur PPS  Max PPI  Cur PPI  Invalid OTA msg
-------  -------  -------  -------  ---------------
1445     216      20       3        0
1024     275      20       1        0

Data Structures
----------------
ap   sta  pap  psta  ch  msg-hash  ap-l
--   ---  ---  ----  --  --------  ----
256  288  45   136   26  2         256
Other Parameters
-----------------
key                   value
---                   -----
Classification        enable
Wireless Containment  disable
Wired Containment     disable
Rogue Containment     disable
System OUI Table
-----------------
oui
---
RTLS Configuration and State
-----------------------------
Type       Server IP  Port  Freq  Active  Rpt-Tags
----       ---------  ----  ----  ------  --------
MMS        N/A        N/A   30            disable
Aeroscout  N/A        N/A   N/A           disable
RTLS       N/A        N/A   30            disable

Tag-Mcast-Addr     Tags-Sent  Rpt-Sta  Incl-Unassoc-Sta  Sta-Sent  Cmpd-Msgs-Sent
--------------     ---------  -------  ----------------  --------  --------------
01:0c:cc:00:00:00  N/A        disable  N/A               N/A       N/A
00:00:00:00:00:00  N/A        disable  N/A               N/A       N/A
01:18:8e:00:00:00  N/A        disable  N/A               N/A       N/A
```

The outputs of the AP monitor command displays the following:

- Active laser beam sources for the OAW-IAP.

- List of OAW-IAPs monitored by the OAW-IAP.
- ARP cache details for the OAW-IAP.
- List of clients monitored by the OAW-IAP.
- Containment details for the OAW-IAP.
- List of potential OAW-IAPs for the OAW-IAP.
- List of potential clients for the OAW-IAP.
- Information about the potential wireless devices.
- Scanned information for the OAW-IAP.
- Configuration and status of monitor information of the OAW-IAP.

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap mpskcache

```
show ap mpskcache
```

Description

This command displays the multiple PSK local cache table for clients associated with the OAW-IAP.

Example

The following example shows the output of **show ap mpskcache** command.

```
MPSK Cache Table
----------------
Client MAC         Key               Expiry  Role              VLAN  ESSID
----------         ---               ------  ----              ----  -----
74:23:44:2d:33:84  1AF366D5AB1D...   4m:41s  00000-mpsk-test   1     00000-mpsk-test
```

Column	Description
`Client MAC`	Indicates the MAC address of the client from which multiple PSK is derived.
`Key`	Displays the cached key for the client.
`Expiry`	Displays the multiple PSK cache expiration details in HH:MM:SS format.
`Role`	Indicates the user role assigned to the client.
`VLAN`	Indicates the VLAN to which the client is assigned.
`ESSID`	Displays the ESSID details to which the client is connected.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap pmkcache

```
show ap pmkcache
```

Description

This command displays the PMK cache table for clients associated with the OAW-IAP.

Example

The following example shows the output of **show ap pmkcache** command.

```
PMK Cache Table
---------------
Client MAC        Key            OKC/11r  Expiry      Name      Role        VLAN   ESSID
----------        ---            -------  ------      ----      ----        ----   -----
00:90:7a:0d:a0:62 1F4C17D8A70C...okc     6h:52m:18s  polycom1  okc-internal  1    okc-internal
00:90:7a:0d:b2:ce F20E35DB311F...okc     7h:31m:15s  polycom2  okc-internal  1    okc-internal
```

Column	Description
`Client MAC`	Indicates the MAC address of the client from the which PMK is derived.
`Key`	Displays the cached key for the client.
`OKC/11r`	Indicates if OKC or 802.11r roaming is enabled.
`Expiry`	Displays the PMK cache expiration details in HH:MM:SS format.
`Name`	Indicates the name of client.
`Role`	Indicates the user role assigned to the client.
`VLAN`	Indicates the VLAN to which the client is assigned.
`ESSID`	Displays the ESSID details to which the client is connected.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap port

```
show ap port [<name>]
```

Description

Displays the operational status of the ethernet ports of the AP.

Parameter	Description	Range	Default
`<name>`	Denotes the ethernet port number of the AP.	eth0, eth1, eth2, eth4, eth4	—

Usage Guidelines

Use this command to view the status of the ethernet ports on the AP.

Example

The following example shows the output of **show ap port** command:

```
(Instant AP)# show ap port
Port Slave APs Status
-----------
Port Name     :eth0
Oper State    :NON-BLOCK
-----------
Port Name     :eth1
Oper State    :NON-BLOCK
-----------
Port Name     :eth2
Oper State    :NON-BLOCK
```

The following example shows the output of **show ap port <name>** command:

```
(Instant AP)# show ap port eth2
Port Slave AP Status
-----------
Port Name     :eth2
Oper State    :NON-BLOCK
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant <Please provide the release in which this command was introduced.>	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ap spectrum ap-list

```
show ap spectrum ap-list
```

Description

This command shows spectrum data seen by an access point that has been converted to a spectrum monitor. The Spectrum Analysis feature provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify 802.11 devices on the network. Issue this command to display and sort APs seen by a specific spectrum monitor.

Examples

The following example is the output of **show ap spectrum ap-list** command. The output in the example below has been divided into two tables to better fit this document. In the AOS-W Instant CLI, the output appears as a single, long table.

```
(Instant AP)# show ap spectrum ap-list
Spectrum AP Table
-----------------
bssid              essid                             spectrum-id  chan  phy-type
-----              -----                             -----------  ----  --------
18:64:72:e3:e9:30  SZL-fast-recovery                 371          132   80211a-VHT-80
18:64:72:e3:e9:20  Specter-fast-recovery             133          1     80211b/g-HT-20
18:64:72:e3:e9:31  LITT-83-NF                        372          132   80211a-VHT-80
18:64:72:e3:e9:21  Zane-83-NF                        134          1     80211b/g-HT-20
18:64:72:e3:e9:32  Wheeler-83-icp                    373          132   80211a-VHT-80
18:64:72:e3:e9:22  Williams-83-icp                   135          1     80211b/g-HT-20
94:b4:0f:02:22:40  Corp-fast-recovery                141          1     80211b/g-HT-20
94:b4:0f:02:22:42  Corp-83-icp                       143          1     80211b/g-HT-20
94:b4:0f:02:22:41  corp-83-NF                        189          1     80211b/g-HT-20
ac:a3:1e:c9:41:30  booth-guest-205                   2376         132   80211a-VHT-80
00:24:6c:0e:c9:21  Test                              446          1     80211b/g-HT-20
84:d4:7e:d2:30:30  c7f8b58fc691071e5c27ac21fbdda79   3143         144*  80211a-VHT-20
84:d4:7e:d2:30:32  Corporate_BYOD                    3164         144*  80211a-VHT-20
84:d4:7e:d2:30:34  Corporate_Office                  3229         144*  80211a-VHT-20
9c:1c:12:fe:71:b0  a                                 3270         132   80211a-VHT-80
18:64:72:ee:b8:f0  test001                           3280         132   80211a-VHT-80
f0:5c:19:22:81:29  fd1_suiteb                        516          1     80211b/g-HT-20

signal(dBm)  ibss  add-time             last-seen
-----------  ----  --------             ---------
0.0          no    2019-05-21 05:38:59  2019-05-24 09:25:05
0.0          no    2019-05-21 05:38:59  2019-05-24 09:25:05
0.0          no    2019-05-21 05:38:59  2019-05-24 09:25:05
0.0          no    2019-05-21 05:38:59  2019-05-24 09:25:05
0.0          no    2019-05-21 05:38:59  2019-05-24 09:25:05
0.0          no    2019-05-21 05:39:00  2019-05-24 09:25:05
-43          no    2019-05-21 06:44:15  2019-05-24 09:24:39
-44          no    2019-05-21 06:44:41  2019-05-24 09:24:40
-44          no    2019-05-21 14:05:35  2019-05-24 09:24:40
-38          no    2019-05-23 00:16:19  2019-05-24 09:16:51
-56          no    2019-05-23 12:54:24  2019-05-24 09:25:05
-48          no    2019-05-23 17:04:19  2019-05-24 09:25:05
-46          no    2019-05-23 17:36:02  2019-05-24 09:25:05
-49          no    2019-05-23 18:41:48  2019-05-24 09:25:05
-42          no    2019-05-23 20:18:16  2019-05-24 09:21:00
-43          no    2019-05-23 20:36:56  2019-05-24 09:25:05
-41          no    2019-05-24 01:13:52  2019-05-24 09:23:56

Spectrum AP Table
```

```
-----------------
bssid              essid                  spectrum-id  chan  phy-type
-----              -----                  -----------  ----  --------
70:3a:0e:91:44:e4  zone6                  573          11    80211b/g-HT-20
f0:5c:19:1c:4e:52  gran-downlink-b        3753         44*   80211a-VHT-80
18:64:72:e3:ed:db  Jia_DL2                3754         36    80211a-VHT-80
9c:1c:12:fe:25:b0  acl-test-456           3765         36    80211a-VHT-80
9c:1c:12:fe:25:b1  vpn-test-205           3767         36    80211a-VHT-80
6c:f3:7f:ef:10:42  0_dcyao_test_2         575          11    80211b/g-HT-20
6c:f3:7f:ef:10:44  0_dcyao_1x             576          11    80211b/g-HT-20
38:17:c3:c7:47:f0  EEE                    3771         36    80211a-VHT-80
f0:5c:19:22:09:77  0_dcyao_4              3774         36    80211a-VHT-80
f0:5c:19:22:09:73  0_dcyao_open           3781         36    80211a-VHT-80
18:64:72:7f:60:11  aaa4                   3792         36    80211a-VHT-80
18:64:72:7f:60:12  0000ppsk-tkip          3793         36    80211a-VHT-80
18:64:72:7f:60:13  aaa1                   3794         36    80211a-VHT-80
18:64:72:7f:60:14  aaa5                   3795         36    80211a-VHT-80
18:64:72:e3:ed:d1  Jia's ssid             3802         36    80211a-VHT-80
18:64:72:e3:ed:d6  Jia_CL2                3804         36    80211a-VHT-80
18:64:72:e3:ed:d7  1111                   3805         36    80211a-VHT-80
18:64:72:e3:ed:d8  abcedd                 3806         36    80211a-VHT-80

signal(dBm)  ibss  add-time             last-seen
-----------  ----  --------             ---------
-47          no    2019-05-24 08:00:11  2019-05-24 09:43:11
-73          no    2019-05-24 08:13:21  2019-05-24 09:43:12
-62          no    2019-05-24 08:14:56  2019-05-24 09:43:12
-56          no    2019-05-24 08:41:49  2019-05-24 09:43:12
-56          no    2019-05-24 08:44:09  2019-05-24 09:43:12
-35          no    2019-05-24 08:44:33  2019-05-24 09:43:12
-42          no    2019-05-24 08:44:33  2019-05-24 09:43:11
-54          no    2019-05-24 08:45:30  2019-05-24 09:42:45
-30          no    2019-05-24 08:50:56  2019-05-24 09:43:12
-30          no    2019-05-24 08:59:59  2019-05-24 09:43:12
-58          no    2019-05-24 09:27:09  2019-05-24 09:43:12
-57          no    2019-05-24 09:27:09  2019-05-24 09:43:12
-57          no    2019-05-24 09:27:44  2019-05-24 09:43:12
-57          no    2019-05-24 09:27:44  2019-05-24 09:43:12
-63          no    2019-05-24 09:29:07  2019-05-24 09:43:12
-59          no    2019-05-24 09:29:07  2019-05-24 09:43:12
-62          no    2019-05-24 09:29:07  2019-05-24 09:43:12
-60          no    2019-05-24 09:29:07  2019-05-24 09:43:12

Start:0
Length:35
Total:35
Current Time:2019-05-24 09:43:12
Channel followed by "*" indicates AP is present on the secondary channel of this AP.
```

The output of this command includes the following information:

Column	Description
`bssid`	Basic Service Set Identifier for an AP. This is usually the MAC address of the AP.
`essid`	Extended service set identifier that names a wireless network.
`spectrum-id`	Identifier assigned to the device by the spectrum monitor.

Column	Description
`chan`	Radio channel used by the BSSID.
`phy-type`	Radio phy type. Possible types include: ■ 802.11a ■ 802.11a-HT-40 ■ 802.11b/g ■ 802.11b/g-HT-20
`signal (dBm)`	Strength of the signal received by the device, in dBm.
`ibss`	Shows if ad hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad hoc BSS (an ibss bit in an 802.11 frame).
`add-time`	Time when the AP was first detected by the spectrum monitor.
`last-seen`	Time when the AP was last seen by the spectrum monitor.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum channel-details

```
show ap spectrum channel-details
```

Description

Show a channel summary table and channel information for Wi-Fi and non-Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio. Issue this command to view detailed information about currently active Wi-Fi and non-Wi-Fi devices seen by the spectrum monitor AP.

Examples

The following example shows the output of **show ap spectrum channel-details** command. The output in the example below has been divided into three tables to better fit this document. In the AOS-W Instant CLI, the output appears as a single, long table.

```
18:64:72:c6:3e:92# show ap spectrum channel-details
Channel Summary Table
---------------------
Channel  Quality(%)  Utilization(%)  WiFi(%)  Bluetooth(%)  Microwave(%)  Cordless Phone(%)
-------  ----------  --------------  -------  ------------  ------------  -----------------
149E     96          45              41       0             0             0
6        62          82              44       0             0             0

Total nonwifi(%)  KnownAPs  UnknownAPs  Noise Floor(dBm)  MaxAPSignal(dBm)
----------------  --------  ----------  ----------------  ----------------
4                 3         64          -92               -21
38                3         1           -89               -35

Max AP SSID  Max AP BSSID       MaxInterference(dBm)  SNIR(dB)
-----------  ------------       --------------------  --------
0_dcyao_4    6c:f3:7f:ef:10:57  -                     71
test         70:3a:0e:4e:e1:4a  -                     54
```

The output of this command includes the following information:

Column	Description
`Channel`	An 802.11a or 802.11g radio channel.
`Quality(%)`	Current relative quality of selected channels in the 802.11a or 802.11g radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
`Utilization (%)`	Percentage of the channel currently in use.
`WiFi (%)`	The percentage of the channel currently being used by Wi-Fi devices.
`Bluetooth (%)`	The computed percentage of time where the channel is occupied by a Bluetooth signal as interference.
`Microwave (%)`	The computed percentage of time where the channel is occupied by a Microwave signal as interference.
`Cordless phone (%)`	The computed percentage of time where the channel is occupied by a Cordless phone signal as interference.
`Total nonwifi (%)`	Strength of the signal sent from the device, in dBm.

Column	Description
`Known APs`	Number of valid APs identified on the radio channel.
`Unknown APs`	Number of invalid or rogue APs identified on the radio channel.
`Noise Floor (dBm)`	Current noise floor recorded on the channel.
`Max AP Signal (dBm)`	Signal strength of the AP that has the maximum signal strength on a channel.
`Max AP SSID`	SSID of the AP on the channel with the highest signal power.
`Max AP BSSID`	BSSID of the AP on the channel with the highest signal power.
`Max Interference (dBm)`	Signal strength of the non-Wi-Fi device that has the highest signal strength.
`SNIR (dB)`	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum channel-metrics

```
show ap spectrum channel-metrics
```

Description

This command shows channel quality, availability, and utilization metrics as seen by a spectrum monitor. This chart displays channel utilization data, showing the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 adjacent channel interference (ACI).

> ACI refers to the interference on a channel created by a transmitter operating in an adjacent channel. A transmitter on a nonadjacent or partially overlapping channel may also cause interference, depending on the transmit power of the interfering transmitter and/or the distance between the devices. In general, ACI may be caused by a Wi-Fi transmitter or a non-Wi-Fi interferer. However, whenever the term ACI appears in Spectrum Analysis graphs, it refers to the ACI caused by Wi-Fi transmitters. The channel utilization option in the Channel Metrics Chart shows the percentage of the channel utilization due to both ACI and non-Wi-Fi interfering devices. Unlike the ACI shown in the show ap spectrum interference-power output, the ACI shown in this graph indicates the percentage of channel time that is occupied by ACI or unavailable for Wi-Fi communication due to ACI.

The Channel Metrics table can also show channel availability, the percentage of each channel that is available for use, or display the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. In the spectrum analysis feature, channel quality is a relative measure that indicates the ability of the channel to support reliable Wi-Fi communication. Channel quality, which is represented as a percentage in this chart, is a weighted metric derived from key parameters that can affect the communication quality of a wireless channel, including noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of retries. Note that channel quality is not directly related to Wi-Fi channel utilization, as a higher quality channel may or may not be highly utilized.

> A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The following example shows the output of **show ap spectrum channel-metrics** command:

```
(Instant AP)# show ap spectrum channel-metrics
Channel Metrics Table
---------------------
Channel  Quality(%)  Noise Floor(dBm)  Availability(%)  Utilization(%)  WiFi Util(%)
-------  ----------  ----------------  ---------------  --------------  ------------
149E     95          -92               52               48              43
6        100         -90               84               16              16

Interference Util(%)
--------------------
5
0

Interference Util: Utilization by Non-WiFi Interference + WiFi ACI (Adjacent Channel
Interference)
```

The output of this command includes the following information:

Column	Description
`Channel`	An 802.11a or 82.11g radio channel.
`Quality(%)`	Current relative quality of selected channels in the 802.11a or 802.11g radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
`Noise Floor (dBm)`	Current noise floor recorded on the channel.
`Availability(%)`	The percentage of the channel currently available for use.
`Utilization(%)`	The percentage of the channel being used.
`WiFi Util(%)`	The percentage of the channel currently being used by Wi-Fi devices.
`Interference Util(%)`	The percentage of the channel currently being used by non-Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum channel-summary

```
show ap spectrum channel-summary
```

Description

This command displays a summary of the 802.11a or 802.11g channels seen by a spectrum monitor. This table can display data aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR).

SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The following example shows the output of **show ap spectrum channel-summary** command:

```
(Instant AP)# show ap spectrum channel-summary
Channel Summary Table
---------------------
Channel  ValidAPs  NotValidAPs  Util(%)  Noise Floor(dBm)  MaxAPSignal(dBm)
-------  --------  -----------  -------  ----------------  ----------------
52E      3         25           24       -92               -42
11       6         16           41       -90               -35

MaxInterference(dBm)  SNIR(dB)
--------------------  --------
-                     50
-                     55
SNIR:Signal to Noise + Interference Ratio
```

The output of this command includes the following information:

Column	Description
`Channel`	An 802.11a or 802.11g radio channel.
`Valid APs`	Number of valid APs identified on the radio channel.
`Not Valid APs`	Number of invalid or rogue APs identified on the radio channel.
`Util (%)`	Percentage of the channel currently in use.
`Noise Floor (dBm)`	Current noise floor recorded on the channel.
`Max AP Signal (dBm)`	Signal strength of the AP that has the maximum signal strength on a channel.
`Max Interference(dBm)`	Signal strength of the non-Wi-Fi device that has the highest signal strength.
`SNIR (dB)`	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platform	Command Mode
All platforms	Privileged EXEC Mode.

show ap spectrum client-list

```
show ap spectrum client-list
```

Description

This command shows details for clients seen by a specified spectrum monitor. Use the output of this command to view channel and signal information for wireless clients seen by the spectrum monitor.

Examples

The following example shows the output of **show ap spectrum client-list** command. The output in the example below has been divided into two tables to better fit this document. In the AOS-W Instant CLI, the output appears as a single, long table.

```
(Instant AP)# show ap spectrum client-list

Spectrum Client Table
---------------------
mac                bssid              essid                            spectrum-id  channel
---                -----              -----                            -----------  -------
f0:5c:19:1c:5d:b0  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  799          116
b4:5d:50:62:eb:71  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  3623         116
38:17:c3:00:02:91  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  3432         116
9c:1c:12:8a:03:30  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  1447         116
70:3a:0e:4e:e2:b1  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  3430         116
a8:bd:27:fa:9f:31  a8:bd:27:fa:46:50  89a7805d5ea1ab6cfe517c8e6d42e87  3232         100
48:4a:e9:4a:1f:51  b4:5d:50:62:e7:35  yhan                             3862         64
c8:b5:ad:ba:fa:10  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  3715         116
a8:bd:27:22:9f:00  6c:f3:7f:77:b6:d0  640eaa67e90dca08a9ae75d2206a9b2  1448         116

phy-type       signal(dBm)  add-time             last-seen
--------       -----------  --------             ---------
80211a-HT-40   -78          2019-05-21 14:38:21  2019-05-24 10:37:33
80211a-HT-40   -83          2019-05-24 05:06:18  2019-05-24 10:56:24
80211a-HT-40   -40          2019-05-23 22:56:03  2019-05-24 10:27:32
80211a-HT-40   -76          2019-05-22 04:32:52  2019-05-24 10:56:29
80211a-HT-40   -43          2019-05-23 22:56:02  2019-05-24 10:30:59
80211a-VHT-80  -49          2019-05-23 18:44:00  2019-05-24 10:54:54
80211a-VHT-80  -71          2019-05-24 10:46:12  2019-05-24 10:54:49
80211a-HT-40   -40          2019-05-24 07:30:04  2019-05-24 10:56:29
80211a-HT-40   -87          2019-05-22 04:33:00  2019-05-24 10:56:24

Start:0
Length:9
Total:9
Current Time:2019-05-24 10:56:29
```

The output of this command includes the following information:

Column	Description
`mac`	MAC address of the client.
`bssid`	Basic Service Set Identifier for a client. This is usually the device’s MAC address.
`essid`	Extended service set identifier that names a wireless network.

Column	Description
`spectrum-id`	Identifier assigned to the client by the spectrum monitor.
`channel`	Radio channel used by the BSSID.
`phy-type`	Radio phy type. Possible types include: ■ 802.11a ■ 802.11a-HT-40 ■ 802.11b/g ■ 802.11b/g-HT-20
`signal(dBm)`	Client signal strength, in dBm.
`add-time`	Time when the client was first detected by the spectrum monitor.
`last-seen`	Time when the spectrum monitor last detected that the client was active.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum device-duty-cycle

```
show ap spectrum device-duty-cycle
```

Description

This command shows the current duty cycle for devices on all channels being monitored by the spectrum monitor or hybrid AP radio. The FFT Duty Cycle table in the output of this command shows the duty cycle for each radio channel. The duty cycle is the percentage of time each device type operates or transmits on that channel. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.

Examples

The following is an example of the **show ap spectrum device-duty-cycle** command. The output of this command shows that Wi-Fi devices sent a signal on channels 132E and 11 during 21% and 2% respectively of the last sample interval.

```
(Instant AP)# show ap spectrum device-duty-cycle
Device Duty Cycle (in %) vs Channel
-----------------------------------
Device Type          132E
-----------          ----
Generic Interferer   0
WIFI                 21
Microwave            0
Bluetooth            0
Generic Fixed Freq   0
Cordless Phone FF    0
Video                0
Audio                0
Generic Freq Hopper  0
Cordless Network FH  0
Xbox                 0
Microwave Inverter   0
Cordless Base FH     0

Device Duty Cycle (in %) vs Channel
-----------------------------------
Device Type          11
-----------          --
Generic Interferer   0
WIFI                 2
Microwave            0
Bluetooth            0
Generic Fixed Freq   0
Cordless Phone FF    0
Video                0
Audio                0
Generic Freq Hopper  0
Cordless Network FH  0
Xbox                 0
Microwave Inverter   0
Cordless Base FH     0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC Mode.

show ap spectrum device-history

```
show ap spectrum device-history
```

Description

This command shows the history of the last 256 non-Wi-Fi devices. Use the output of this command to view channel, signal, and duty-cycle information as well as addor delete times for the last 256 devices seen by a spectrum monitor or hybrid AP.

Non-Wi-Fi Interferers

The following table describes each type of of non-Wi-Fi interferer detected by a spectrum monitor or hybrid AP. Note also that a hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Non-Wi-Fi Interferer Type	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio).*
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones).*
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video*). These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other*). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base*).
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network*). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox*).
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles and cordless or hands-free devices that do not use one of the known cordless phone protocols.

Non-Wi-Fi Interferer Type	Description
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Example

The following example shows the out of **show ap spectrum device-history** command:

```
(Instant AP)# show ap spectrum device-history

Non-WiFi Device History Table: 2GHz
-----------------------------------
Type                ID  CFreq(KHz)  Bandwidth(KHz)  Channels-affected  Signal(dBm)
----                --  ----------  --------------  -----------------  -----------
Microwave Inverter  1   2437000     2000            6                  -60
Microwave Inverter  2   2437000     3000            6                  -67
Microwave Inverter  3   2437000     3000            6                  -62
Microwave Inverter  4   2437000     3000            6                  -61
Microwave Inverter  5   2437000     3000            6                  -69
Microwave Inverter  6   2437000     3000            6                  -62
Microwave Inverter  7   2437000     3000            6                  -67
Microwave Inverter  8   2437000     2000            6                  -72
Microwave Inverter  9   2437000     20000           6                  -72
Microwave Inverter  10  2437000     3000            6                  -65
Microwave Inverter  11  2437000     3000            6                  -62
Microwave Inverter  12  2437000     2000            6                  -61
Microwave Inverter  13  2437000     3000                               -0
Microwave Inverter  14  2437000     20000           6                  -62
Microwave Inverter  15  2437000     20000           6                  -65
Microwave Inverter  16  2437000     20000           6                  -68
Microwave Inverter  17  2437000     20000           6                  -65
Microwave Inverter  18  2437000     4000            6                  -67
Microwave Inverter  19  2437000     20000           6                  -62
Microwave Inverter  20  2437000     20000           6                  -65
Microwave Inverter  21  2437000     20000           6                  -68
Microwave Inverter  22  2462000     2000            11                 -69

Duty-cycle  Add-time             Delete-time
----------  --------             -----------
55          2019-05-28 06:05:24  2019-05-28 06:05:39
55          2019-05-28 06:05:43  2019-05-28 06:05:58
69          2019-05-28 06:06:10  2019-05-28 06:06:25
75          2019-05-28 06:06:36  2019-05-28 06:06:51
```

```
55          2019-05-28 06:07:10  2019-05-28 06:07:25
75          2019-05-28 06:08:09  2019-05-28 06:08:25
55          2019-05-28 06:09:27  2019-05-28 06:09:42
55          2019-05-28 06:28:09  2019-05-28 06:28:24
75          2019-05-28 06:30:11  2019-05-28 06:30:26
75          2019-05-28 06:32:18  2019-05-28 06:32:33
55          2019-05-28 06:33:16  2019-05-28 06:33:32
75          2019-05-28 06:33:52  2019-05-28 06:34:08
0           2019-05-28 06:34:52  2019-05-28 06:35:08
55          2019-05-28 06:44:02  2019-05-28 06:44:21
55          2019-05-28 06:45:00  2019-05-28 06:45:31
62          2019-05-28 06:48:14  2019-05-28 06:48:36
55          2019-05-28 08:07:59  2019-05-28 08:08:21
62          2019-05-28 08:08:47  2019-05-28 08:09:03
75          2019-05-28 08:09:03  2019-05-28 08:09:22
55          2019-05-28 08:12:06  2019-05-28 08:12:22
62          2019-05-28 08:24:04  2019-05-28 08:24:32
75          2019-05-28 08:31:32  2019-05-28 08:31:48

Total:22
Current Time:2019-05-28 08:52:36
```

The output of this command includes the following information:

Column	Description
`Type`	Device type. This parameter can be any of the following: ■ audio FF (fixed frequency) ■ bluetooth ■ cordless base FH (frequency hopper) ■ cordless phone FF (fixed frequency ■ cordless network FH (frequency hopper) ■ generic FF (fixed frequency ■ generic FH (frequency hopper) ■ generic interferer ■ microwave ■ microwave inverter ■ video ■ xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.
`ID`	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
`Cfreq`	Center frequency of the signal sent from the device.
`Bandwidth`	Channel bandwidth used by the device, in KHz.
`Channels-affected`	Radio channels affected by the wireless device, in KHz.
`Signal (dBm)`	Strength of the signal sent from the device, in dBm.
`Duty-cycle`	Device duty cycle. This value represents the percent of time the device broadcasts on the specified channel or frequency.
`Add-time`	Time at which the device was first detected.
`Delete-time`	Time at which the device was aged out.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum device-list

```
show ap spectrum device-list
```

Description

Show a device summary table and channel information for non-Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio. Issue this command to view detailed information about currently active non-Wi-Fi devices on the network. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.

NOTE

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The following example shows the output of **show ap spectrum device-list** command:

```
(Instant AP)#  show ap spectrum device-list
Non-WiFi Device List: 5GHz
--------------------------
Type  ID  CFreq(KHz)  Bandwidth(KHz)  Channels-affected  Signal(dBm)
----  --  ----------  --------------  -----------------  -----------
Video 1   5760000     2000            153                -32

Duty-cycle  Add-time             Update-time
----------  --------             -----------
65          2019-05-24 03:09:12  2019-05-24 03:20:43

Non-WiFi Device List: 2GHz
--------------------------
Type                ID  CFreq(KHz)  Bandwidth(KHz)  Channels-affected  Signal(dBm)
----                --  ----------  --------------  -----------------  -----------
Cordless Base FH    70  2444000     80000           6                  -71

Duty-cycle  Add-time             Update-time
----------  --------             -----------
5           2019-05-29 04:37:51  2019-05-29 07:26:31

Total:0
Current Time:2019-05-28 09:34:43
```

The output of this command includes the following information:

Column	Description
`Type`	Device type. This parameter can be any of the following: ■ audio FF (fixed frequency) ■ bluetooth ■ cordless base FH (frequency hopper) ■ cordless phone FF (fixed frequency ■ cordless network FH (frequency hopper) ■ generic FF (fixed frequency ■ generic FH (frequency hopper) ■ generic interferer ■ microwave ■ microwave inverter ■ video ■ xbox

Column	Description
	NOTE: For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.
`ID`	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
`Cfreq (KHz)`	Center frequency of the signal sent from the device.
`Bandwidth (KHz)`	Channel bandwidth used by the device.
`Channels-affected`	Radio channels affected by the wireless device.
`Signal (dBm)`	Strength of the signal sent from the device, in dBm.
`Duty-cycle`	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
`Add-time`	Time at which the device was first detected.
`Update-time`	Time at which the status of the device was updated.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum device-log

```
show ap spectrum device-log
```

Description

This command shows a time log of add and delete events for non-Wi-Fi devices. Use this table to show a time log of when non-Wi-Fi devices were added to and deleted from the Wi-Fi Device log table. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The output of this example shows that the spectrum monitor logged data for eight microwave inverter devices seen by its 802.11g radio. Note that the output below is divided into two sections to better fit on the page of this document. In the AOS-W Instant CLI, this information is displayed in a single long table.

```
(Instant AP)# show ap spectrum device-log

Non-WiFi Device Log Table: 2GHz
-------------------------------
Type                ID  CFreq(KHz)  Bandwidth(KHz)  Channels Affected
----                --  ----------  --------------  -----------------
Microwave Inverter  1   2437000     2000            6
Microwave Inverter  1   2437000     2000            6
Microwave Inverter  2   2437000     3000            6
Microwave Inverter  2   2437000     3000            6
Microwave Inverter  3   2437000     3000            6
Microwave Inverter  3   2437000     3000            6
Microwave Inverter  4   2437000     3000            6
Microwave Inverter  4   2437000     3000            6
Microwave Inverter  5   2437000     3000            6
Microwave Inverter  5   2437000     3000            6
Microwave Inverter  6   2437000     3000            6
Microwave Inverter  6   2437000     3000            6
Microwave Inverter  7   2437000     3000            6
Microwave Inverter  7   2437000     3000            6
Microwave Inverter  8   2437000     2000            6
Microwave Inverter  8   2437000     2000            6

Signal(dBm)  Duty Cycle  Event    Time
-----------  ----------  -----    ----
-60          55          Added    2019-05-28 06:05:24
-60          55          Deleted  2019-05-28 06:05:39
-67          55          Added    2019-05-28 06:05:43
-62          69          Added    2019-05-28 06:06:10
-62          69          Deleted  2019-05-28 06:06:25
-61          75          Added    2019-05-28 06:06:36
-61          75          Deleted  2019-05-28 06:06:51
-69          55          Added    2019-05-28 06:07:10
-69          55          Deleted  2019-05-28 06:07:25
-62          75          Added    2019-05-28 06:08:09
-62          75          Deleted  2019-05-28 06:08:25
-67          55          Added    2019-05-28 06:09:27
-67          55          Deleted  2019-05-28 06:09:42
-72          55          Added    2019-05-28 06:28:09
-72          55          Deleted  2019-05-28 06:28:24
```

```
Total:16
Current Time:2019-05-28 11:23:17
```

The output of this command includes the following information:

Column	Description
`Type`	Type of non-Wi-Fi device detected by the spectrum monitor or hybrid AP
`ID`	The spectrum ID number assigned to that device. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
`CFreq(KHz)`	Center frequency of the signal sent by the device.
`Bandwidth`	Amount of signal bandwidth used by the device, in kilohertz.
`Channels affected`	Radio channels affected by the device signal.
`Signal(dBm)`	Strength of the signal sent by the device.
`Duty Cycle`	Device duty cycle. This value represents the percent of time a signal is broadcast on a specific channel or frequency.
`Event`	Denotes whether the device was added to the log or deleted from the log table.
`Time`	The time when the event occured.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum device-summary

```
show ap spectrum device-summary
```

Description

This command shows the numbers of Wi-Fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor or hybrid AP. Use this command to show the types of devices that the spectrum device can detect on each channel it monitors. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 585.

Examples

The following example shows the output of **show ap spectrum device-summary** command. The output of this example shows that the spectrum monitor is able to detect 27 Wi-Fi devices on channel 132E and 15 Wi-Fi devices on channel 1:

```
(Instant AP)# show ap spectrum device-summary

Number of Devices vs Channel
----------------------------
Device Type          132E
-----------          ----
Generic Interferer   0
WIFI                 27
Microwave            0
Bluetooth            0
Generic Fixed Freq   0
Cordless Phone FF    0
Video                0
Audio                0
Generic Freq Hopper  0
Cordless Network FH  0
Xbox                 0
Microwave Inverter   0
Cordless Base FH     0

Number of Devices vs Channel
----------------------------
Device Type          1
-----------          -
Generic Interferer   0
WIFI                 15
Microwave            0
Bluetooth            0
Generic Fixed Freq   0
Cordless Phone FF    0
Video                0
Audio                0
Generic Freq Hopper  0
Cordless Network FH  0
Xbox                 0
Microwave Inverter   0
Cordless Base FH     0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum interference-power

```
show ap spectrum interference-power
```

Description

This command shows the interference power detected by a 802.11a or 802.11g radio on a spectrum monitor or hybrid AP. This table displays information about AP power levels, channel noise, and adjacent channel interference seen on each channel by a spectrum monitor or hybrid AP radio.

The output of this command displays the noise floor of each selected channel in dBm. The noise floor of a channel depends on the noise figure of the RF components used in the radio, temperature, presence of certain types of interferers or noise, and the width of the channel. For example, in a clean environment, the noise floor of a 20 MHz channel will be around -95 dBm and that of a 40 MHz channel will be around -92 dBm. Certain types of fixed frequency continuous transmitters such as video bridges, fixed frequency phones, and wireless cameras typically elevate the noise floor as seen by the Wi-Fi radio. Other interferers such as the frequency hopping phones, Bluetooth, and Xbox devices may not affect the noise floor of the radio. A Wi-Fi radio can only reliably decode Wi-Fi signals that are a certain dB above the noise floor and therefore estimating and understanding the actual noise floor of the radio is critical to understanding the reliability of the RF environment.

The ACI column displayed in the Interference Power Chart displays adjacent-channel interference (ACI) power levels based on the signal strength(s) of the Wi-Fi APs on adjacent channels. A higher ACI value in Interference Power Chart does not necessarily mean higher interference since the AP that is contributing to the maximum ACI may or may not be very actively transmitting data to other clients at all times. The ACI power levels are derived from the signal strength of the beacons.

Examples

The output of this example shows interference power levels for each channel seen by the spectrum monitor **ap123**.

(Instant AP) #show ap spectrum interference-power

```
Interference Power Table
------------------------
Channel  Noise Floor(dBm)  Max AP Signal(dBm)  Max AP SSID
-------  ----------------  ------------------  -----------
149      -91               -40                 ethersphere-wpa2
153      -63               -42                 guest
157      -92               -48                 alpha
161      -94               -39                 00:24:6C:C0:15:EB
165      -93               -26                 sw-jfb-attack
149+     -60               -40                 ethersphere-wpa2
157+     -89               -39                 00:24:6C:C0:15:EB

Max AP BSSID       WiFi ACI(dBm)  Max Interference(dBm)
------------       --------       ---------------------
00:24:6c:80:7b:c9  -77            -71
00:1a:1e:87:c1:90  -63            -58
00:1a:1e:50:01:30  -74            -60
00:24:6c:81:57:c8  -61            -70
00:1a:1e:9b:1d:c8  -74            -69
00:24:6c:80:7b:c9  -0             -58
00:24:6c:81:57:c8  -0             -60
```

The output of this command includes the following information:

Column	Description
`Channel`	An 802.11a or 802.11g radio channel.
`Noise Floor (dBm)`	Current noise floor recorded on the channel.
`Max AP Signal (dBm)`	Power level of the AP on the channel with the highest signal power.
`Max AP SSID`	SSID of the AP on the channel with the highest signal power.
`Max AP BSSID`	BSSID of the AP on the channel with the highest signal power.
`WiFi ACI (dBm)`	Adjacent channel interference level detected by the spectrum device.
`Max Interference (dBm)`	Signal strength of the non-Wi-Fi device that has the highest signal strength.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap spectrum status

```
show ap spectrum status
```

Description

This command shows spectrum status of this AP. Use the output of this command to check spectrum band, spectrum packet counters, spectrum packet validation, spectrum per channel stats and spectrum ASAP stats.

NOTE

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The following example shows the output of **show ap spectrum status** command:

```
(Instant AP)# show ap spectrum status
Spectrum Band
-------------
Interface  Band  Mode          Channel  Streaming to UI  No FFT/WiFi  Status  No FFT Ticks
---------  ----  ----          -------  ---------------  -----------  ------  ------------
wifi0      5GHz  Access Point  100E     No               9194         enable  0
wifi1      2GHz  Access Point  11       No               13617        enable  0

Spectrum packet counters
-------------------------
Interface  Packets Read  Bytes Read  Interrupts  Buffer Overflows  Max PPS  Cur PPS
---------  ------------  ----------  ----------  ----------------  -------  -------
wifi0      2857574       3026170866  173687      2074              369      175
wifi1      439243        128049601   142542      0                 281      15

Max PPI  Cur PPI  Cur IPS  NB FFTs  WIFI FFTs  WIFI Bursts  Processed Pkts  Rejected Pkts
-------  -------  -------  -------  ---------  -----------  --------------  -------------
20       9        11       0        313910     10974        2857069         505
20       1        8        0        548        355          360382          78861

Spectrum packet validation
---------------------------
Interface  Large RSSI  MaxIndex0  IncorrectMaxIndex  Inv FFT Len  Inv Phy Type
---------  ----------  ---------  -----------------  -----------  ------------
wifi0      0(0%)       0(0%)      0(0%)              0(0%)        0
wifi1      0(0%)       0(0%)      0(0%)              0(0%)        0

Spectrum Per Channel stats
---------------------------
Channel       PPS  WIFI  RSSI-max  RSSI-ps  Noise-ps  Dwell-time  FFT-rate(%)
-------       ---  ----  --------  -------  --------  ----------  -----------
channel 100E  175  123   69        32       92        18          97
channel 11    15   3     50        39       90        18          8

Spectrum ASAP stats for wifi0
------------------------------
bp=d7f40000 lp=d7f80000 wp=d7f4a050 rtp=d7f47a58 rhp=d7f4a050 rx_ctr=2859648 ovfl=2074 sp_
av=101520 sp_nd=1084 zero_fft=0

Spectrum ASAP stats for wifi1
------------------------------
bp=daa40000 lp=daa80000 wp=daa72e20 rtp=daa72ce8 rhp=daa72e20 rx_ctr=439243 ovfl=0 sp_
av=257088 sp_nd=316 zero_fft=0
```

The output of this command includes the following information:

Column	Description
`Max PPS`	Maximum number of packets per second received.
`Cur PPS`	Number of packets per second received on last cycle.
`Max PPI`	Maximum number of packets received per interrupt.
`Cur PPI`	Number of packets received on last interrupt.
`Cur IPS`	Number of interrupts per second.
`NB FFTs`	Currently not in use.
`WIFI FFTs`	Number of packets processed and classified as wifi.
`Wi-Fi Bursts`	Number of WIFI bursts detected .
`Processed Pkts`	Number of FFT packets processed by the classifier.
`Rejected Pkts`	Number of FFT packets rejected by the classifier.
`Interface`	Interface to which the rest of the columns in the same row will refer to. It can be wifi0 or wifi1..
`Large RSSI`	FFT Packets detected with larger RSSI than the noise floor.
`MaxIndex0`	FFT Packets detected with max index set to 0.
`IncorrectMaxIndex`	FFT Packets detected with max index incorrect.
`Inv FFT len`	FFT Packets with incorrect number of FFT bins.
`Inv PHY Type`	FFT Packet identified as to have an invalid phy type.
`Channel`	Channel number to which the rest of the columns in the same row will refer to.
`PPS`	Number of FFT packets per second received..
`WIFI`	Number of FFT packets ID as WiFi received.
`RSSI-max`	Maximum RSSI value detected in last cycle.
`RSSI-ps`	Average RSSI value detected in last cycle.
`Noise-ps`	Average Noise Floor value detected in last cycle.
`Dwell-time`	Amount of time spent on a given channel.
`FFT-rate (%)`	Calculated rate given the PPS and the dwell time.
`Spectrum ASAP stats`	Debug pointers reserved for debug and support.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show ap virtual-beacon-report

```
show ap virtual-beacon-report [client-mac <mac>]
```

Description

This command displays a report with the MAC address details and RSSI information of an OAW-IAP. Use the output of this command to view virtual beacon table of an OAW-IAP. The virtual beacon table with the details of clients associated an OAW-IAP is broadcast by each table.

Example

The following example shows the output of **show ap virtual-beacon-report** command.

```
Virtual Beacon Table
--------------------
Station            CM State  Triggered  Succeeded  Owner
-------            --------  ---------  ---------  -----
00:db:df:0a:57:4e  Adopted   1          1          Yes
                   Normal                          No
                                                   No
                                                   No
                                                   No
                                                   No
a0:88:b4:41:64:18  Normal    1          0          No
                   Normal                          No
                                                   No
                                                   No
                                                   No
                                                   Yes

 AP                            RSSI  Received
 --                            ----  --------
 00:24:6c:07:44:c8 (Local 0)   47    59s
 00:24:6c:07:44:c0 (Local 1)   49    2m:2s
 6c:f3:7f:ef:12:c0             44    18s
 6c:f3:7f:ee:f7:80             44    11s
 6c:f3:7f:ee:f7:90             36    13s
 6c:f3:7f:ef:12:d0             43    13s
 00:24:6c:07:44:c8 (Local 0)   34    20s
 00:24:6c:07:44:c0 (Local 1)   40    18s
 6c:f3:7f:ef:12:c0             43    18s
 6c:f3:7f:ee:f7:80             48    11s
 6c:f3:7f:ee:f7:90             35    13s
 6c:f3:7f:ef:12:d0             36    13s

Normal     Working well
Home       Current AP found a better AP for the client
Deny       Current AP is not the better AP
Target     Current AP is the better AP
Voice      Ready to move, but client is doing voice
Refused    Too many clients try to move to me
Done       Current AP just deauth the client
Adopted    Client has moved to me successfully
Total 2 VBRs
00:24:6c:c8:74:4c# show ap debug client-match 0
Client Match Status:: RUNNING  BALANCING
Associated:1, Threshold:1
Leaving:0, Coming:0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show app-monitoring

```
show app-monitoring [list]
```

Description

This command displays the list of applications supported on an OAW-IAP.

Example

The following example shows the output of the **show app-monitoring list** command:

```
telemetry sendcnt:0
Pre-defined Application Monitoring list
---------------------------------------
App Name              DPI AppID  Inner AppID
--------              ---------  -----------
zoom                  2928       0x0
slack                 2889       0x1
skype                 183        0x2
|_lync-online         1454       0x2
|_alg-skype4b-audio   3769       0x2
|_alg-skype4b-video   3770       0x2
webex                 890        0x4
gotomeeting           889        0x5
office365             1448       0x6
|_excel-online        2748       0x6
|_onedrive            2820       0x6
|_outlook             1478       0x6
|_ms-planner          2712       0x6
|_powerpoint-online   3036       0x6
|_sharepoint-online   1453       0x6
|_ms-sway             2711       0x6
|_word-online         3035       0x6
|_yammer              519        0x6
dropbox               779        0x7
amazon-aws            1183       0x8
github                2559       0x9
ms-teams              3374       0x11
custom1               20000      0x14
custom2               20001      0x15
custom3               20002      0x16
custom4               20003      0x17
custom5               20004      0x18
alg-wifi-calling      3781       0x19
```

The output of this command provides the following information:

Column	Description
`App Name`	Indicates the list of application services available on an OAW-IAP.
`DPI APPID`	Displays the DPI ID of the application
`Inner AppID`	

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show app-services

```
show app-services
```

Description

This command displays the list of application services available on an OAW-IAP.

Example

The following example shows the output of the **show app-services** command:

```
Application Service
-------------------
Name         IP Protocol  Start Port  End Port
----         -----------  ----------  --------
any          0            0           65535
adp          17           8200        8200
bootp        17           67          69
cfgm-tcp     6            8211        8211
cups         6            515         515
dhcp         17           67          68
dns          17           53          53
esp          50           0           65535
ftp          6            21          21
gre          47           0           65535
h323-tcp     6            1720        1720
h323-udp     17           1718        1719
http-proxy2  6            8080        8080
http-proxy3  6            8888        8888
http         6            80          80
https        6            443         443
icmp         1            0           65535
ike          17           500         500
kerberos     17           88          88
l2tp         17           1701        1701
lpd-tcp      6            631         631
lpd-udp      17           631         631
msrpc-tcp    6            135         139
msrpc-udp    17           135         139
natt         17           4500        4500
netbios-dgm  17           138         138
netbios-ns   17           137         137
noe          17           32512       32512
noe-oxo      17           5000        5000
netbios-ssn  6            139         139
nterm        6            1026        1028
ntp          17           123         123
papi         17           8211        8211
pop3         6            110         110
pptp         6            1723        1723
rtsp         6            554         554
sccp         6            2000        2000
sips         6            5061        5061
sip-tcp      6            5060        5060
sip-udp      17           5060        5060
smb-tcp      6            445         445
smb-udp      17           445         445
smtp         6            25          25
snmp         17           161         161
snmp-trap    17           162         162
ssh          6            22          22
```

```
svp           119           0            65535
syslog        17            514          514
telnet        6             23           23
tftp          17            69           69
vocera        17            5002         5002
```

The output of this command provides the following information:

Column	Description
`Name`	Indicates the list of application services available on an OAW-IAP.
`IP Protocol`	Displays the IP protocol numbers for each application service.
`Start Port and End Port`	Indicates the range of port numbers on which the application services are enabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show audit-trail

```
show audit-trail <count>
```

Description

This command lists information of all configuration actions applied to the OAW-IAP. Use the output of this command to display the time, the interface from which the configuration was applied, configuration details and the status of the configuration. This command lists all configurations actions applied on the OAW-IAP since the last factory reset of the AP. To view a specific number of configuration actions, specify the count using the **show audit-trail <count>** syntax.

Example

The following example shows the output of the **show audit-trail** command :

```
time                   From
-------------------  ------------
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli
2017-03-21 02:22:01  from Cli

Command
---------------------------------------------------------------------
<f0:5c:19:c9:f9:6c (SSID Profile "liying-TP2-1") # no explicit-ageout-client> --
successfully.
<f0:5c:19:c9:f9:6c (config) # exit> -- successfully.
<f0:5c:19:c9:f9:6c (Access Rule "liying-TP2-1") # wlan access-rule liying-TP2-1> --
successfully.
<f0:5c:19:c9:f9:6c (Access Rule "liying-TP2-1") # no rule> -- successfully.
<f0:5c:19:c9:f9:6c (Access Rule "liying-TP2-1") # bandwidth-limit peruser downstream 1500> --
successfully.
<f0:5c:19:c9:f9:6c (Access Rule "liying-TP2-1") # rule any any match any any any permit> --
successfully.
<f0:5c:19:c9:f9:6c (config) # exit> -- successfully.
```

Column	Description
`Time`	Displays the time when the configuration command was executed.
`From`	Displays the source from which the configuration command was executed (CLI, WebUI, or other servers).
`Command`	Displays the configuration details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-IAP 300 Series OAW-IAP 310 Series OAW-IAP 320 Series OAW-IAP 330 Series OAW-IAP 360 Series	Privileged EXEC mode

show arm-channels

```
show arm-channels
```

Description

This command displays the ARM channel details configured on an OAW-IAP.

Example

The following example shows the output of **show arm-channels** command:

```
2.4 GHz
-------
Channel  Status
-------  ------
1        disable
2        disable
3        disable
4        disable
5        disable
6        disable
7        disable
8        disable
9        disable
10       disable
11       enable
12       disable
13       disable
1+       enable
2+       disable
3+       disable
4+       disable
5+       disable
6+       disable
7+       enable
5.0 GHz
-------
Channel  Status
-------  ------
36       disable
40       disable
44       disable
48       disable
52       disable
56       enable
60       enable
64       enable
149      enable
153      enable
157      enable
161      enable
165      enable
36+      enable
44+      enable
52+      disable
60+      disable
149+     enable
157+     enable
```

The output of this command provides the following information:

Column	Description
`Channel`	Displays the list of channels available in the 2.4 GHz and 5 GHz bands.
`Status`	Indicates if the channels in the 2.4 GHz and 5 GHz bands are enabled or disabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

```
show arm config
```

Description

This command displays the ARM configuration details for an OAW-IAP.

Example

The following example shows the output of **show arm config** command:

```
Minimum Transmit Power            :18
Maximum Transmit Power            :127
Band Steering Mode       :prefer-5ghz
Client Aware             :enable
Scanning                 :enable
Wide Channel Bands       :5ghz
Air Time Fairness Mode   :fair-access
Spectrum Load Balancing  :disable
SLB NB Matching Percent  :75
SLB Calculating Interval :30
CM Min SNR for HE Steer  :40
SLB Threshold            :2
Custom Channels          :No
2.4 GHz Channels
----------------
Channel  Status
-------  ------
1        enable
2        disable
3        disable
4        disable
5        disable
6        enable
7        disable
8        disable
9        disable
10       disable
11       enable
12       disable
13       disable
1+       enable
2+       disable
3+       disable
4+       disable
5+       disable
6+       disable
7+       enable
5.0 GHz Channels
----------------
Channel  Status
-------  ------
36       enable
40       enable
44       enable
48       enable
52       enable
56       enable
60       enable
64       enable
149      enable
```

```
153      enable
157      enable
161      enable
165      enable
36+      enable
44+      enable
52+      disable
60+      disable
149+     enable
157+     enable
```

The output of this command provides the following information:

Column	Description
`Minimum Transmit Power`	Displays the minimum transmission power configured for the ARM channels.
`Maximum Transmit Power`	Displays the maximum transmission power configured for the ARM channels.
`Band Steering Mode`	Displays the band steering mode configuration parameters.
`client aware`	Indicates the activation status of the Client aware feature.
`Scanning`	Indicates if scanning for available channels is enabled.
`Wide Channel Bands`	Indicates if 40MHz channel are enabled on 2.4 GHz or 5 GHz band.
`Air Time Fairness Mode`	Displays configuration details for the Airtime Fairness Mode feature.
`Spectrum Load Balancing`	Indicates if the Spectrum load balancing feature is enabled or disabled.
`CM Min SNR for HE Steer`	Displays the minimum SNR value configured for HE (802.11ax) steer.
`SLB NB Matching Percent`	Indicates the percentage for comparing client density of OAW-IAP neighbors for spectrum load balancing.
`SLB Calculating Interval`	Indicates the frequency at which the client density on OAW-IAP is calculated for spectrum load balancing.
`Custom Channels`	Displays custom channels if any.
`Channel`	Displays the list of channels available in the 2.4 GHz and 5 GHz bands.
`Status`	Indicates if the channels in the 2.4 GHz and 5 GHz bands are enabled or disabled.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of this command includes the **CM Min SNR for HE Steer** value.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show arp

```
show arp
```

Description

This command displays the ARP entries for the virtual switch. Use the output of this command to view the ARM messages sent or received by the virtual switch.

Example

The following example shows the output of **show arp** command

```
IP address        HW type      Flags        HW address           Mask      Device
192.168.10.2      0x1          0x6          D8:C7:C8:C4:42:98    *         br0
10.17.88.2        0x1          0x2          00:0B:86:40:1C:A0    *         br0
```

The output of this command includes the following information:

Column	Description
`IP address`	Displays the IP address of the device.
`HW Type`	Displays the type of the device.
`Flags`	Displays any flags for this OAW-IAP.
`HW address`	Displays the MAC address of the device.
`Mask`	Displays the network mask or the IP address range.
`Device`	Displays the device used to send ARP requests and replies.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show attack

```
show attack {config| stats}
```

Description

This command displays information about firewall settings configured on an OAW-IAP to protect the network against wired attacks such as ARP attacks or malformed DHCP packets.

Parameter	Description	Range	Default
`config`	Displays firewall configuration details to protect the network from wired attacks.	—	—
`stats`	Displays attack counters.	—	—

Example

The following example shows the output of **show attack config** command:

```
Current Attack
--------------
Attack        Status
------        ------
drop-bad-arp  Disabled
fix-dhcp      Disabled
poison-check  Enabled
```

The output of this command indicates if the firewall settings to block invalid ARP packets and fix malformed DHCP packets are enabled. You can also view the status of the Poison-check parameter, which triggers an alert to notify the user about the ARP poisoning when enabled.

The following example output for the **show attack stats** command shows the attack counters:

```
attack counters
--------------------------------------
Counter                                Value
-------                                -------
arp packet counter                     0
drop bad arp packet counter            0
dhcp response packet counter           0
fixed bad dhcp packet counter          0
send arp attack alert counter          0
send dhcp attack alert counter         0
arp poison check counter               0
garp send check counter                1628
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show auth-survivability

```
show auth-survivability {cached-info| debug-log [<count>]| time-out}
```

Description

This command displays the authentication survivability information for an OAW-IAP. Use this command to view the information cache expiry duration, cached information, and log details to debug when the authentication survivability feature is enabled. The authentication survivability feature supports a survivable authentication framework against the remote link failure when working with the external authentication servers. When enabled, this feature allows the OAW-IAPs to authenticate the previously connected clients against the cached credentials if the connection to the authentication server is temporarily lost.

Parameter	Description	Range	Default
`cached-info`	Displays authentication credentials cached by the OAW-IAP.	—	—
`debug-log [<count>]`	Displays the log details for troubleshooting. The **count** attribute allows you to specify the number of logs to display.	—	—
`time-out`	Displays the duration configured for the cache expiry.	—	—

Examples

The following example shows the output of the **auth-survivability cached-info** command:

```
user-cache-info
---------------
UserName  Remaining-Cache-Time  Aruba-Vlan  Aruba-Named-Vlan
--------  --------------------  ----------  ----------------
pjin      23h:59m:34s           1           vlan

Aruba-No-DHCP-Fingerprint  Aruba-Role  MS-Tunnel-Type
-------------------------  ----------  --------------
True                       role        13

MS-Tunnel-Medium-Type  MS-Tunnel-Private-Group-ID  PW-User-Name
---------------------  --------------------------  ------------
1                      groupid                     guo
PW-Session-Timeout
------------------
12800
Total number of cached username:1
```

The following example shows the output of the **show auth-survivability time-out** command:

```
Auth Survivability time out :24
```

The output of the **auth-survivability cached-info** and **show auth-survivability time-out** commands provide the following information:

Column	Description
`UserName`	Indicates the username of the client whose credentials are cached.

Column	Description
`Remaining Cache-Time`	Displays the remaining duration for cache expiry.
`Auth Survivability time out`	Indicates the configured duration for cache expiry.

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show backup-config

```
show backup-config
```

Description

This command displays the backup configuration information on an OAW-IAP. Use the output of this command to view the current configuration information stored in the OAW-IAP flash memory.

Example

The following text provides an example for the **show backup-config** command output:

```
version 6.4.0.0-4.1.0
virtual-controller-country IN
virtual-controller-key 0cb5770401cdeb6e4363c25fdfde17d907c4b095a9be5e4258
name instant-C4:42:98
terminal-access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap d8:c7:c8:c4:42:98
arm
wide-bands 5ghz
80mhz-support
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
client-match
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin 82c496d47485380deb0a01d41345d3f1
wlan access-rule default_wired_port_profile
index 1
rule any any match any any any permit
wlan access-rule wired-instant
index 2
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule test
index 3
rule any any match any any any deny
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
https
blacklist-time 3600
auth-failure-blacklist-time 3600
ids classification
```

```
ids
wireless-containment none
airgroup
disable
airgroupservice airplay
disable
description AirPlay
airgroupservice airprint
disable
description AirPrint
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show banner

```
show banner
```

Description

This command displays the current login banner of an OAW-IAP. Use the output of this command to review the banner message that appears when you first log in to the CLI of the OAW-IAP.

Example

The following output is displayed for the **show banner** command:

```
######welcome to login instant###########
####please start to input admin and password#########
###Don't leak the password###
```

Command History

OAW-IAP Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show blacklist-client

```
show blacklist-client [config]
```

Description

This command shows the configuration details for blacklisting clients and lists the clients blacklisted by n OAW-IAP.

Parameter	Description	Range	Default
`config`	Displays the parameters and values configured for manual or dynamic blacklisting of clients.	—	—

Example

The following output is displayed for the **show blacklist-client** command:

```
Blacklisted Clients
-------------------
MAC                Reason        Timestamp  Remaining time(sec)  AP name
---                ------        ---------  -------------------  -------
00:24:6c:ca:41:51  user-defined  14:46:18   Permanent            -
```

The output of this command provides information on the MAC address of client that is blacklisted, the reason for blacklisting, timestamp, the associated OAW-IAP name, and the duration until which the client is blacklisted.

The following output is displayed for the **show blacklist-client config** command:

```
Blacklist Time              :3600
Auth Failure Blacklist Time  :3600
Manually Blacklisted Clients
----------------------------
MAC                Time
---                ----
00:24:6c:ca:41:51  14:46:18
Dynamically Blacklisted Clients
-------------------------------
MAC  Reason  Timestamp  Remaining time(sec)  AP name
---  ------  ---------  -------------------  -------
Dyn Blacklist Count  :0
```

The output of this command provides the following information:

Column	Description
`Blacklist Time`	Indicates the duration in seconds since the blacklisting has been triggered due to an ACL rule.
`auth-survivability cache-time-out`	Indicates the duration in seconds after which the clients that exceed the maximum authentication failure threshold are blacklisted.
`Manually Blacklisted clients`	Displays the details of clients that are blacklisted manually.
`Dynamically Blacklisted Clients`	Displays the list of clients that dynamically blacklisted due to multiple authentication rules or an ACL rule trigger.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ble-config

```
show ble-config
```

Description

This command displays the BLE configuration details.

Parameter	Description	Range	Default
`ble-config`	Displays the BLE configuration details.	—	—

Examples

The following example shows the output of the **show ble-config** command:

```
(host)# show ble-config
BLE Configuration
-----------------
Item                            Value
----                            -----
Master IP                       127.0.0.1
Authorization Token             Not Configured
Endpoint URL                    Not Configured
BLE Ready                       No
Update Intvl (in sec)           300
BLE debug log                   Enabled
Operational Mode                Dynamic Console (APB: Dynamic Console)
Uplink Status                   Up (APB: Up)
APB Connection Status           0
Last BLE Device Update Attempt  00:00:00:00:00:00
Last Update Sent Time           No Update Sent
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms except AP-155, OAW-AP203H, OAW-AP207, OAW-AP215, OAW-AP225	Privileged EXEC mode

show ble-console

```
show ble-console
```

Description

This command displays any specific issues or errors detected in the swarm, OmniVista 3600 Air Manager, or VPN connectivity. This command is available only when the dynamic console mode is enabled on the Instant AP.

Parameter	Description	Range	Default
`ble-console`	Displays the connectivity status of the BLE console.	—	—

Examples

The following example shows the output of the **show ble-console** command:

```
(host)# show ble-console
Dynamic BLE Console Debug
-------------------------
Item     state  reason
----     -----  ------
Swarm    ok     n/a
Airwave  error  tcp connect error
Central  n/a    n/a
VPN      n/a    n/a
Last Open Time: 2018-08-09 16:20:14
Last Close Time: 2018-08-09 16:14:12
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms except AP-155, OAW-AP203H, OAW-AP207, OAW-AP215, OAW-AP225	Privileged Exec mode

show-ca-bundle

```
show ca-bundle
   upgrade status
   version
```

Description

This command displays information on the CA certificate bundle installed on the AP.

Parameter	Description
`upgrade status`	Displays the status of the CA certificate bundle update.
`version`	Displays the version details of the CA certificate bundle installed on the AP.

Example

The following example shows the output of **show ca-bundle upgrade status** command:

```
(Instant AP)# show ca-bundle upgrade status
CA-bundle upgrade status :failure
```

The following example shows the output of **show ca-bundle version** command:

```
(Instant AP)# show ca-bundle version
Default CA-bundle    :V2
New CA-bundle        :NONE
Active CA-bundle     :V2
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show calea

```
show calea {config | statistics}
```

Description

This command displays the details configured for CALEA server integration and the tunnel encapsulation statistics on an OAW-IAP. Use the output of this command to view CALEA configuration details and GRE encapsulation statistics for the OAW-IAPs with CALEA server integration feature enabled.

Examples

The following example shows the output of the **show calea config** command:

```
calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150
```

The following example shows the output of the **show calea statistics** command:

```
Rt resolve fail : 0
Dst resolve fail: 0
Alloc failure   : 0
Fragged packets : 0
Jumbo   packets : 263
Total Tx fail   : 0
Total Tx ok     : 263
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show captive-portal

```
show captive-portal [auto-white-list]
```

Description

This command shows the external and internal captive portal parameters configured for a network profile. Use the output of this command to view information about the contents displayed on the internal and external captive portal pages for guest users.

Example

The following output is displayed for the **show captive-portal** command:

```
:Captive Portal Configuration
Background Color:13421772
Banner Color       :16750848
Decoded Texts      :
Banner Text        :Welcome to Guest Network
Use Policy         :Please read terms and conditions before using Guest Network
Terms of Use       :This network is not secure, and use is at your own risk
Internal Captive Portal Redirect URL:
Captive Portal Mode:Acknowledged
:External Captive Portal Configuration
Server:localhost
Port               :80
URL                :/
Authentication Text:Authenticated
External Captive Portal Redirect URL:
Server Fail Through:No
```

The output of this command provides the following information:

Column	Description
`Background Color`	Displays the color code configured for the internal captive portal splash page.
`Banner Color`	Displays the color code configured for the banner on the internal captive portal splash page.
`Banner Text`	Displays the banner text for the internal captive portal splash page.
`decoded-texts`	Displays decoded texts.
`Terms of use`	Displays the terms and conditions that the internal captive portal user must be aware of.
`Use Policy`	Displays usage policy text for the internal captive portal splash page.
`Captive Portal Mode`	Indicates if the authentication is successful and acknowledged.

`Internal Captive Portal Redirect URL`
`External Captive Portal Redirect URL`
	Displays the URL that the users are redirected to, after a successful authentication.

`Server`	Displays the external Captive port server.

Column	Description
`URL`	Displays the URL of the external captive portal splash page server.
`Authentication Text`	Indicates if the external captive portal user authentication is successful.
`Port`	Displays the port used for communicating with the external captive portal splash page server.
`Server Fail Through`	Indicates if the guest clients are allowed to access the Internet when the external captive portal server is not available.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show captive-portal-domains

```
show captive-portal-domains
```

Description

This command displays the internal and external captive portal server domains. Use this command to view information about the internal and external captive portal domains.

Example

The following output is displayed for the **show captive-portal-domains** command:

```
Internal Captive Portal Domain:
securelogin.arubanetworks.com
External Captive Portal Domains:
localhost
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cellular

```
show cellular {config | status}
```

Description

These commands display the status and cellular configuration of the OAW-IAP.

Parameter	Description	Range	Default
`show cellular config`	Displays the cellular configuration details available for the OAW-IAP.	—	—
`show cellular status`	Displays the status of the cellular configuration for the OAW-IAP.	—	—

Example

The following example shows the partial output of the **show cellular config** command:

```
No Comm USB Plugged in
Cellular configuration
----------------------
Type             Value
----             -----
4g-usb-type
usb-type
usb-dev
usb-tty
usb-init
usb-auth-type
usb-user
usb-passwd
usb-dial
usb-modeswitch
modem-isp
modem-country
Supported Modem Types
---------------------
Modem Type       Driver Used
----------       -----------
option           option
acm              acm
airprime         airprime
hso              hso
sierra-evdo      sierra-evdo
sierra-gsm       sierra-gsm
pantech-uml290   pantech-3g
novatal-mc551    ether-3g
sierra-net       sierra-net
franklin-u770    rndis-u770
rndis-l800       rndis-l800
huawei-cdc       huawei-cdc
novatel-u620     novatel-u620
pantech-uml295   rndis-uml295
sierra-gobi      sierra-gobi
Supported Country list
----------------------
Country list
------------
France
```

```
NZ
Israel
HK
Sweden
Spain
China
UK
norway
Germany
Croatia
Saudi-Arabia
US
Japan
Aus
Canada
India
```

The output of this command includes the following parameters:

Column	Description
`Cellular configuration`	Displays the types of cellular configuration and the values associated with the cellular configuration parameters. For example, 3G or 4G modems.
`Supported Modem Types`	Displays the list of supported modems and corresponding drivers.
`Supported Country list`	Lists the countries that support cellular deployment.

The following output is displayed for **show cellular status** command:

```
(Instant AP)(config)# show cellular status
Cellular Status
---------------
card       detect      link        SIM PIN
----       ------      ----        -------
Present    detect-ok   Linkup      N/A

USB Modem Information
---------------------
Parameter                       Value
---------                       ------
Manufacturer                    Linux
Product                         OHCI Host Controller
Serial Number                   0000:00:04.0
Driver                          hub
Vendor ID                       1d6b
Product ID                      0001
Manufacturer
Product                         USB2.0 Hub
Serial Number
Driver                          hub
Vendor ID                       05e3
Product ID                      0608
Manufacturer                    ZTE, Incorporated
Product                         ZTE Wireless Ethernet Adapter
Serial Number                   MF8310ZTED000000
Driver                          option
Vendor ID                       19d2
Product ID                      1405
Model                           MF831
Supported Network Services      LTE WCDMA GSM
Firmware Version                BD_MF831HDV1.0.0B02
```

```
ESN Number                      862828022611876

Cellular Link Status
--------------------
Parameter                       Value
---------                       ------
USB Modem State                 Active
USB Uplink RSSI (in dBm)        -69
Current Network Service         4G-LTE
plugin counter  :               0
plugout counter :               0
```

The output of this command includes the following parameters:

Parameters	Description
`card`	Indicates if the cellular cards are currently configured on the OAW-IAP.
`detect`	Indicates if cellular modems are detected on the OAW-IAP.
`link`	Indicates the current status of cellular link.
`SIM PIN`	Displays the SIM PIN of the model.
`USB Modem Information`	Displays detailed information about the USB modem.
`Cellular Link Status`	Displays cellular link status such as USB modem state, USB uplink RSSI, current network service, plugin, and plugout counters.

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cert all

```
show cert all
```

Description

This command displays the details about the certificates uploaded on an OAW-IAP.

Example

The following example shows the output of **show cert all** command:

```
Default Server Certificate:
Version        :3
Serial Number :01:DA:52
Issuer         :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA
Subject        :0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com,
OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated -
QuickSSL(R) Premium, CN=securelogin.arubanetworks.com
Issued On      :2011-05-11 01:22:10
Expires On     :2017-08-11 04:40:59
Signed Using   :SHA1
RSA Key size   :2048 bits

Default CP Server Certificate:
Version        :3
Serial Number :01:DA:52
Issuer         :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA
Subject        :0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com,
OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated -
QuickSSL(R) Premium, CN=securelogin.arubanetworks.com
Issued On      :2011-05-11 01:22:10
Expires On     :2017-08-11 04:40:59
Signed Using   :SHA1
RSA Key size   :2048 bits
```

The output of this command displays details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the certificates uploaded to the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cert assignment

```
show cert assignment
```

Description

This command displays the certificate assignment details of the OAW-IAP.

Example

```
(Instant AP)# show cert assignment
cert assignment
---------------
Application                Cert type                  Cert name
------------------------   -------------------------  -----------------------
UI                         ServerCert                 UI Certificate
Radsec                     TrustedCA                  Branch Main Cert
```

Table Column	Description
Application	Application using the certificate.
Cert type	The certificate type used.
Cert name	The name of the certificate.

Related Commands

Command	Description
wlan cert-assignment-profile	Configures installed certificates for specific applications.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Instant AP Platform	Command Mode
All platforms	Privileged EXEC mode.

show cert-from-server

```
show cert-from-server <activate|airwave|cloud>
```

Description

This command displays the certificate chain received from the server during SSL handshake. The output of this command is included as a part of the **show tech-support** command.

Parameter	Description
`activate`	Displays certificate chains received from Activate.
`airwave`	Displays certificate chains received from OmniVista 3600 Air Manager.

Example

The following example shows certificates received from Activate server:

```
(Instant AP)# show cert-from-server activate
Received Time :2020-03-27 07:18:48
Version :2
Serial Number :497A3CD8014ED1D5D2B6B93C09D7B7D9
Issuer :/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3
Subject :/C=US/ST=California/L=Santa Clara/O=Aruba Networks, Inc./CN=device.arubanetworks.com
Issued On :Sep 19 00:00:00 2019 GMT
Expires On :Sep 15 23:59:59 2021 GMT
RSA Key size :2048 bits
Signed Using :RSA-SHA256
Extensions :
X509v3 Subject Key Identifier:
47:BB:36:EB:83:61:04:C1:54:21:15:03:E8:EF:40:EB:1A:59:88:9D
X509v3 Subject Alternative Name:
DNS:device.arubanetworks.com
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints:
CA:FALSE
X509v3 Certificate Policies:
Policy: 2.23.140.1.2.2
CPS: https://www.geotrust.com/resources/repository/legal
User Notice:
Explicit Text: https://www.geotrust.com/resources/repository/legal
X509v3 CRL Distribution Points:
Full Name:
URI:http://gn.symcb.com/gn.crl
Authority Information Access:
OCSP - URI:http://gn.symcd.com
CA Issuers - URI:http://gn.symcb.com/gn.crt
X509v3 Authority Key Identifier:
keyid:D2:6F:F7:96:F4:85:3F:72:3C:30:7D:23:DA:85:78:9B:A3:7C:5A:7C
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show clarity

```
show clarity
   config
   history {auth|dhcp|dns|sta|sta-dns}
```

Description

This command displays the status and history of the clarity configuration parameters on the OAW-IAP.

Parameter	Description	Range	Default
`config`	Displays the inline monitoring statistics of the clarity configuration parameters.	—	—
`history`	Displays the history of the clarity configuration parameters.	—	—
`auth`	Displays the history of the authentication statistics generated by inline monitoring.	—	—
`dhcp`	Displays the history of the DHCP related statistics generated by inline monitoring.	—	—
`dns`	Displays the history of the DNS statistics generated by inline monitoring.	—	—
`sta`	Displays the history of the passive STA statistics generated by inline monitoring.	—	—
`sta-dns`	Displays the history of the STA DNS statistics generated by inline monitoring.	—	—

Examples

The following example shows the output of **show clarity config** command:

```
Clarity config
--------------
Parameter          Value
---------          -----
inline Sta stats   enabled
inline Auth stats  enabled
inline DHCP stats  enabled
inline DNS stats   enabled
```

The output of this command provides the following information:

Column	Description
`inline Sta stats`	Indicates the status of the station passive monitor statistics.
`inline Auth stats`	Indicates the status of the authentication statistics.
`inline DHCP stats`	Indicates the status of the DHCP statistics.
`inline DNS stats`	Indicates the status of the DNS statistics.

The following example shows the output of **show clarity history auth** command:

```
Clarity Auth Trace Buffer
```

```
-------------------------
Jan  1 15:47:33  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:31  192.168.0.118  3  4
AUTHSERVER_TIMEOUT
Jan  1 15:47:59  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:31  192.168.0.118  3  6
AUTHSERVER_TIMEOUT
Jan  1 16:05:03  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:31  192.168.0.118  3  6
AUTHSERVER_TIMEOUT
Jun 21 09:25:27  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:21  192.168.0.118  3  13
AUTHSERVER_TIMEOUT
Jun 21 09:25:48  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:31  192.168.0.118  3  4
AUTHSERVER_TIMEOUT
Jun 21 09:26:49  DOT1X_EVENT    00:db:df:0a:41:6e  ac:a3:1e:c9:32:31  192.168.0.118  3  5
AUTHSERVER_TIMEOUT
```

The following example shows the output of **show clarity history dns** command:

```
DNS Server Stats Table ---- In Transaction
------------------------------------------
Server Ip   Max Delay  Min Delay  Avg Delay
---------   ---------  ---------  ---------
10.65.6.33  7758       7758       7758

RCODE0  RCODE1  RCODE2  RCODE3  RCODE4  RCODE5
------  ------  ------  ------  ------  ------
1       0       0       0       0       0

Last Query  Last Resp  Samples  Anomaly Cnt  Anomaly Ip    RCODE History
----------  ---------  -------  -----------  ----------    -------------
107870      4799346    1        1            10.65.66.110  1  0  0  0  0  0

Total dns servers in transaction: 1
DNS Server Stats Table ---- In Pending Send
-------------------------------------------
Server Ip  Max Delay  Min Delay  Avg Delay
---------  ---------  ---------  ---------

RCODE0  RCODE1  RCODE2  RCODE3  RCODE4  RCODE5
------  ------  ------  ------  ------  ------

Last Query  Last Resp  Samples  Anomaly Cnt  Anomaly Ip  RCODE History
----------  ---------  -------  -----------  ----------  -------------

Total pending send: 0
```

The following example shows the output of **show clarity history dhcp** command:

```
DHCP Server Stats Table ---- In Transaction
-------------------------------------------
Client Mac         Sequence  Timestamp  Time Diff1
----------         --------  ---------  ----------
88:32:9b:a5:59:0c  1         552762     0

Time Diff2  Time Diff3  Time Diff4  Server Ip
----------  ----------  ----------  ---------
0           0           0           0.0.0.0

Total dhcp clients in transaction: 1
DHCP Server Stats Table ---- In Pending Send
--------------------------------------------
Client Mac  Sequence  Timestamp  Time Diff1
----------  --------  ---------  ----------

Time Diff2  Time Diff3  Time Diff4  Server Ip
----------  ----------  ----------  ---------
```

```
Total pending send: 0
```

The following example shows the output of **show clarity history sta**command:

```
Passive Sta Table
------------------------
sta-mac            ap-mac             ap-ssid            repeat-count  assoc_rx_time  assoc_
resp_duration  deauth_reason_code  deauth_aruba_code  sta_rx_deauth_code  ft_auth_status  ft_
resp_duration  encryption_method  phyc_d11_supt  deauth_resaon_flag  deauth_time  auth_rx_
time
-------            ------             -------            ------------  -------------  -------
------------  ------------------  -----------------  ------------------  --------------  ----
------------  -----------------  -------------  ------------------  -----------  ------------
f8:38:80:89:ca:8a  70:3a:0e:c1:13:5c  70:3a:0e:91:35:d0  0             0              0
             0                   17                 0                   0               0
            0                  0              18                  0            2019-05-23
07:39:12
f8:38:80:89:ca:8a  70:3a:0e:c1:13:5c  70:3a:0e:91:35:d0  0             0              0
             0                   17                 0                   0               0
            0                  0              18                  0            2019-05-23
07:39:14
f8:38:80:89:ca:8a  70:3a:0e:c1:13:5c  70:3a:0e:91:35:d0  0             0              0
             0                   17                 0                   0               0
            0                  0              18                  0            2019-05-23
07:39:19
```

Command History

Release	Modification
AOS-W Instant 8.6.0.0	The following sub-parameters are added to the show clarity history command: ■ **sta** ■ **sta-dns**
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show clearpassca

```
show clearpassca
```

Description

This command displays the details of the customized ClearPass Policy Manager certificate uploaded on an OAW-IAP.

Example

The following example displays the output of the **show clearpassca** command:

```
Default clearpass CA Certificate:
Version       :3
Serial Number :03
Issuer        :/C=US/ST=California/L=Sunnyvale/O=Aruba Networks/CN=Pengfei-CPPM-6 Server Cert
Root CA/emailAddress=certs@aruba.local
Subject       :/C=US/ST=California/L=Sunnyvale/O=Aruba Networks/CN=Pengfei-CPPM-6 Server Cert
Root CA/emailAddress=certs@aruba.local
Issued On     :Sep 14 02:08:58 2018 GMT
Expires On    :Sep 14 02:38:58 2028 GMT
RSA Key size  :2048 bits
Signed Using  :SHA512-RSA
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show client ip-user

```
show client ip-user <mac>
```

Description

This command displays the IP addresses of the clients connected to the OAW-IAP.

Example

The following example shows the output of **show client ip-user <mac>** command:

```
IP User Table
-------------
IP              MAC                      Timestamp
--              ---                      ---------
10.17.162.2     90:4c:81:cf:77:34
Number of IP address   :1
Info timestamp      :278931
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show clients

```
show clients [<diff>| accounting <mac>| checksum <mac>| debug| roaming| status <mac>| wired
[debug]]
```

Description

This command displays details about the OAW-IAP clients. Use this command to view information about the OAW-IAP clients. The OAW-IAP client table provides basic information about the clients. For detailed information of each client, use the required parameter and specify the MAC address of the client.

Parameter	Description	Range	Default
`<diff>`	Displays difference summary of the client table since the specified interval.	—	—
`accounting <mac>`	Displays accounting information for a specific client MAC address.	—	—
`checksum <mac>`	Filters checksum errors for a specific client MAC address.	—	—
`debug`	Displays the OAW-IAP client configuration details, which can be used for debugging purpose.	—	—
`roaming`	Displays information about roaming clients.	—	—
`status <mac>`	Displays the current status for a client based on the specified MAC address.	—	—
`wired [debug]`	Displays the list of clients connected to wired or Ethernet interface. You can also use the optional debug parameter to view the end-to-end information of the wired clients for debugging purpose.	—	—

Example

show clients and show clients wired

The following output is displayed for the **show clients** command:

```
Client List
-----------
Name                    IP Address     MAC Address        OS  ESSID     Access Point
----                    ----------     -----------        --  -----     ------------
132-15-Auto-PC-Change  10.17.133.241  08:ed:b9:e1:51:7b      rev_ipv6  ac:a3:1e:cd:46:94

Channel Type  Role      IPv6 Address                          Signal   Speed (mbps)
------- ----  ----      ------------                          ------   ------------
36+     AN    rev_ipv6  2001:470:36:5c3:ffff:ffff:ffff:64  0(poor)  0(poor)
`
Number of Clients    :1
Info timestamp       :605085
```

A similar output is displayed for the **show clients wired** command.

The client list in the command output for both wireless and wired clients provides the following information:

Column	Description
`Name`	Displays the name of the client.
`IP address`	Displays the IP address of the client.
`MAC address`	Displays the MAC address of the client.
`OS`	Indicates the OS running on the client system.
`Network`	Indicates the SSID and network to which the client is connected.
`Access Point`	Indicates the IP address of the access point to which the client is connected.
`Channel`	Indicates the channel assigned to the client.
`Type`	Indicates the type of the Wi-Fi client device.
`Role`	Indicates the role assigned to the client.
`Signal`	Indicates the current signal strength of the client, as detected by the OAW-IAP.
`Speed(Mbps)`	Indicates the current speed at which data is transmitted. When the client is associated with an OAW-IAP, it constantly negotiates the speed of data transfer. A value of 0 means that the OAW-IAP has not received any packets from the client for some time.

show clients <diff>

The **show clients <diff>** command displays the change in the clients table data that occurred during the specified interval. For example, if the value specified for <diff> parameter is 10 seconds, the client table displays the changes such as signal strength or speed that occurred since the last 10 seconds.

show accounting <mac>

The **show accounting <mac>** command displays the accounting information such as status and session ID for a specific client MAC address.

show checksum <mac>

The following output is displayed for the **show checksum <mac>** command:

```
Mac Address:08:ed:b9:e1:51:7d
Basic info
----------
mac
---
08 ed b9 e1 51 7d
bssid
d8 c7 c8 3d 3d 52
ap_ip
0a 11 58 ba
name
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        00 00
00 00 00 00
essid
73 72 6f 79 2d 73 6f 6d 65 74 68 69 6e 67 00 00 00 00 00 00 00 00 00 00 00 00 00        00 00
00 00 00 00
auth_failure_count
00
acl
00 8a
acct_session
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
user_role
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
swarm_basic_client_t
08 ed b9 e1 51 7d d8 c7 c8 3d 3d 52 0a 11 58 ba 73 72 6f 79 2d 73 6f 6d 65 74 68 69 6e 67 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8a a9 fe 5a 9a 03 e8 00 00
checksum
02 ec ba ec
```

The **show checksum <mac>** command displays the checksum errors associated with the OAW-IAP clients.

show clients debug and show clients wired debug

The **show clients debug** command displays detailed information about the clients MAC and IP addresses, client role, authentication aging time, and accounting intervals, ESSID and BSSID details, VLAN and multicast groups to which the client is associated, and DHCP roles and options associated with the client. The **show clients wired debug** command displays a similar output.

The following example shows the **show clients debug** command output:

```
Client List
-----------
Name                   IP Address     MAC Address        OS  ESSID     Access Point
----                   ----------     -----------        --  -----     ------------
132-15-Auto-PC-Change  10.17.133.241  08:ed:b9:e1:51:7b      rev_ipv6  ac:a3:1e:cd:46:94

Channel Type  Role      IPv6 Address                       Signal   Speed (mbps)  Reauth Age
------- ----  ----      ------------                       ------   ------------  -----------
36+     AN    rev_ipv6  2001:470:36:5c3:ffff:ffff:ffff:64  0(poor)  0(poor)       0


Reauth Interval   Reauth ESSID  Auth Type   Authenticated  DEL  Age  Vlan      ESSID
----------------  -------------  ---------  -------------- ---  ---  ----      ------
0                                N/A        no              no   9    1(SSID)  ()

Private role info  Accouting Session Name  BSSID              Idle Timeout  csum  mcast
groups
-----------------  ----------------------  -----              ------------  ----  -----------
-
0(0-0)             132-15-Auto-PC-Change  ac:a3:1e:54:69:50   1000          0000  (0)


Acct Interval  Class Attribute  Dhcp-Opt Vlan  Dhcp-Opt role  Intercept  Offline  FB Token
-------------  ---------------  -------------  -------------  ---------  -------  --------
0              null             0,(null)       ,0,0-0         no         no       null

FB RxBytes  FB TxBytes  SLAAC IP Address                    Link Local IP Address
----------  ----------  ----------------                    ---------------------
null         null       2001:470:36:5c3:406b:7c14:9d1d:142d fe80::9198:30aa:5217:d22a

DHCP Status  DHCP v6 Status
-----------  --------------
Completed    Soliciting
```

show clients status

The **show clients status <mac>** command displays the status of an OAW-IAP client.

show clients roaming

The **show clients roaming** command displays the MAC address and IP address details of OAW-IAP from which the client has roamed and IP address of the OAW-IAP to which the client is roamed.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show clock

```
show clock [summer-time| timezone [all]]
```

Description

This command displays the system clock, current timezone, and the DST configured on an OAW-IAP. Use this command to display the system clock. Include the optional summer-time parameter to display configured daylight savings time settings. The timezone parameter shows the current timezone, with its time offset from GMT.

Parameter	Description	Range	Default
`summer-time`	Displays the summer (daylight saving) time settings.	—	—
`timezone [all]`	Displays the configured timezone for a specific OAW-IAP or for all OAW-IAPs.	—	—

Example

show clock timezone all

The following example shows the partial output of **show clock timezone all** command:

```
Support Timezones
-----------------
Country                       Timezone   DST Name   DST Recurring
-------                       --------   --------   -------------
International-Date-Line-West  UTC-11
Coordinated-Universal-Time-11 UTC-11
Hawaii                        UTC-10
Alaska                        UTC-09     AKDT       second sunday march 02:00 first sunday
november 02:00
Baja-California               UTC-08     MDT        first sunday april 02:00 last sunday
october 02:00
Pacific-Time                  UTC-08     PDT        second sunday march 02:00 first sunday
november 02:00
Arizona                       UTC-07
Chihuahua                     UTC-07     MDT        first sunday april 02:00 last sunday
october 02:00
La-Paz                        UTC-07     MDT        first sunday april 02:00 last sunday
october 02:00
Mazatlan                      UTC-07     MDT        first sunday april 02:00 last sunday
october 02:00
Mountain-Time                 UTC-07     MDT        second sunday march 02:00 first sunday
november 02:00
Central-America               UTC-06
Central-Time                  UTC-06     CDT        second sunday march 02:00 first sunday
november 02:00
Guadalajara                   UTC-06     CDT        first sunday april 02:00 last sunday
october 02:00
Mexico-City                   UTC-06     CDT        first sunday april 02:00 last sunday
october 02:00
Monterrey                     UTC-06     CDT        first sunday april 02:00 last sunday
october 02:00
Saskatchewan                  UTC-06
Bogota                        UTC-05
Lima                          UTC-05
Quito                         UTC-05
```

```
Eastern-Time                    UTC-05     EDT       second sunday march 02:00 first sunday
november 02:00
Indiana(East)                   UTC-05     EDT       second sunday march 02:00 first sunday
november 02:00
```

The output of this command includes the following information:

Column	Description
`Country`	Displays the country name.
`Timezone`	Displays the name of the timezone.
`DST Name`	Displays the name of the DST.
`DST Recurring`	Displays the name of the Daylight Saving recurring time.

show clock summer-time

The following example shows the partial output of **show clock summer-time** command:

```
Summer Time
-----------
DST Name  Start Week  Start Day  Start Month  Start Hour  End Week  End Day  End  Month  End
Hour

-------- ---------- --------- ----------- ---------- -------- ------- -------- ---------- --------- ----------- ---------- --------------- ---------- --------- -------
---- ----------
PST         recurring   2 Sun          Mar         2:00        first     Sun         Nov
3:00 -8
```

The output of this command includes the following information:

Column	Description
`DST Name`	Name of the DST.
`Start Week`	Enter the week number when the time change begins.
`Start Day`	Enter the weekday when the time change begins.
`Start Month`	Enter the month when the time change begins.
`Start Hour`	Enter the hour when the time change begins.
`End Week`	Enter the week number when the time change ends.
`End Day`	Enter the weekday when the time change ends.
`End  Month`	Enter the month when the time change ends.
`End  Hour`	Enter the hour when the time change ends.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cluster-security

```
show cluster-security [connections][peers][stats]
```

Description

This command displays cluster security configuration details for all the OAW-IAPs in the cluster.

Parameter	Description	Range	Default
`cluster-security`	Displays the status of the DTLS configuration and DTLS state, whether enabled or disabled.	—	—
`connections`	Displays the total number of connections monitored in the swarm by cluster security DTLS.	—	—
`peers`	Displays the details and status of the peers monitored by cluster security DTLS.	—	—
`stats`	Displays the cluster security DTLS monitoring stats for the cluster.	—	—

Example

The following output is displayed for the **show cluster-security** command:

```
Cluster Security Profile
------------------------
Parameter               Value
---------               -----
DTLS config             Disabled
DTLS state              Disabled
Low assurance devices   Disallow
Reboot required         No
```

The following output is displayed for the **show cluster-security connections** command:

```
---------------------------------
IDX         :Connection Index
Flags       :I-Initiator, R-Responsder
Inactivity  :Time remaining till inactivity timeout
Re-Neg      :Time remaining till Re-negotiation
---------------------------------
Cluster Security DTLS Connections
---------------------------------
Local IDX   Remote IDX   State      Flags  Local Address
---------   ----------   -----      -----  -------------
19bb00b0    7df90024     connected  R      10.17.142.77[4434]
19bb00b1    4db20024     connected  R      10.17.142.77[4434]
19bb00b2    1f6e0024     connected  R      10.17.142.77[4434]
19bb00b3    7d6f0024     connected  I      10.17.142.77[4434]
19bb00b4    57fd0024     connected  R      10.17.142.77[4434]

   Peer Address        Rx bytes  Tx bytes  Age           Inactivity  Re-Neg
   ------------        --------  --------  ---           ----------  ------
   10.17.142.74[4434]    673511    138016  05h:04m:32s    01m:55s     01h:54m:37s
   10.17.142.73[4434]    394516     80788  02h:58m:17s    01m:53s     04h:21m:06s
   10.17.142.76[4434]    354332     74632  02h:44m:18s    01m:57s     03h:55m:52s
   10.17.142.71[4434]    269882     57304  02h:09m:39s    01m:57s     04h:33m:12s
   10.17.142.75[4434]     90933     18544  40m:59s        01m:52s     05h:56m:43s
```

```
Total connections count:5
```

The following output is displayed for the **show cluster-security peers** command:

```
---------------------------
IDX        :Connection Index
---------------------------
Cluster Security DTLS Peers
---------------------------
Peer Address        State   Local IDX
------------        -----   ---------
10.17.142.76[4434]  active  19bb00b2
10.17.142.73[4434]  active  19bb00b1
10.17.142.75[4434]  active  19bb00b4
10.17.142.74[4434]  active  19bb00b0
10.17.142.71[4434]  active  19bb00b3
Total peers count:5
```

The following output is displayed for the **show cluster-security stats** command:

```
Cluster Security Statistics
---------------------------
Statistic Name                                Counts
--------------                                ------
No resource                                   0
Dropped messages                              0
New connection alloc success/fail/free        180/0/175
New connection establishment success/fail     180/0
Connection lookup fail                        0
Connection init attempts                      83
Connection renegotiations attempts            83
Connection init request fail                  0
Connection response attempts                  97
Connection disallow, low assurance pki cert   0
New peers alloc success/fail/freed            5/0/0
Peer init response fail                       0
Peer connection slots full                    0
Signing module not init/async fail            3/0
Entropy not available                         0
Retrieve date-time fail                       0
Inits retried                                 3
Connection timeouts                           0
Connection timeouts (inactivity)              0
Connection responses timeouts                 0
Handshake fail after retransmit               0
Handshake fail after signing in retries       0
Signing module op attempts/success/fail/busy  180/180/0/1
Socket msgs rx success/fail                   1221386/0
Discovery msg tx success/fail                 0/0
Discovery msg rx (allowed)                    0
Msg rx on old ports (dropped)                 0
Unsecure msg tx success/fail                  0/0
Unsecure msg rx allow/drop                    586369/0
Loopback msg sent to AP's uplink IP           0
```

The following output is displayed for the **show cluster-security connections stats** command:

```
Cluster Security Connections Statistics for: Local Idx = 19bb00b0
------------------------------------------------------------------
Statistic Name                              Counts
--------------                              ------
IO Send success/fail                        1835/0
IO Receive success/fail                     2583/0
IO Receive peek fail                        0
Peer connection mismatch                    1
Handshake success after signing in retries  0
```

```
Signing still in progress (dropped)         0
Negotiate msg rx success/fail               5/0
Peer init request tx/response rx            0/0
Signing module op attempts/success/fail     1/1/0
Signing in module busy                      0
Verify peer mac address fail                0
Disallow low assurance pki cert.............0
Verify peer certificate fail                0
Retransmitted handshakes                    0
SSL msg write fail (out of resources)       0
SSL msg write fail (error)                  0
SSL msg read fail (out of resources)        0
SSL msg read fail (error)                   0
Total DTLS msg tx/rx                        1825/2575
Cluster Security Connections Statistics for: Local Idx = 19bb00b1
------------------------------------------------------------------
Statistic Name                              Counts
--------------                              ------
IO Send success/fail                        1082/0
IO Receive success/fail                     1522/0
IO Receive peek fail                        0
Peer connection mismatch                    0
Handshake success after signing in retries  0
Signing still in progress (dropped)         0
Negotiate msg rx success/fail               5/0
Peer init request tx/response rx            0/0
Signing module op attempts/success/fail     1/1/0
Signing in module busy                      0
Verify peer mac address fail                0
Disallow low assurance pki cert.............0
Verify peer certificate fail                0
Retransmitted handshakes                    0
SSL msg write fail (out of resources)       0
SSL msg write fail (error)                  0
SSL msg read fail (out of resources)        0
SSL msg read fail (error)                   0
Total DTLS msg tx/rx                        1072/1514
Cluster Security Connections Statistics for: Local Idx = 19bb00b2
------------------------------------------------------------------
Statistic Name                              Counts
--------------                              ------
IO Send success/fail                        1001/0
IO Receive success/fail                     1424/0
IO Receive peek fail                        0
Peer connection mismatch                    0
Handshake success after signing in retries  0
Signing still in progress (dropped)         0
Negotiate msg rx success/fail               5/0
Peer init request tx/response rx            0/0
Signing module op attempts/success/fail     1/1/0
Signing in module busy                      0
Verify peer mac address fail                0
Verify peer certificate fail                0
Retransmitted handshakes                    0
SSL msg write fail (out of resources)       0
SSL msg write fail (error)                  0
SSL msg read fail (out of resources)        0
SSL msg read fail (error)                   0
Total DTLS msg tx/rx                        991/1416
Cluster Security Connections Statistics for: Local Idx = 19bb00b3
------------------------------------------------------------------
Statistic Name                              Counts
--------------                              ------
```

```
IO Send success/fail                        772/0
IO Receive success/fail                     1086/0
IO Receive peek fail                        0
Peer connection mismatch                    0
Handshake success after signing in retries  0
Signing still in progress (dropped)         0
Negotiate msg rx success/fail               5/0
Peer init request tx/response rx            1/1
Signing module op attempts/success/fail     1/1/0
Signing in module busy                      0
Verify peer mac address fail                0
Verify peer certificate fail                0
Retransmitted handshakes                    0
SSL msg write fail (out of resources)       0
SSL msg write fail (error)                  0
SSL msg read fail (out of resources)        0
SSL msg read fail (error)                   0
Total DTLS msg tx/rx                        763/1077
Cluster Security Connections Statistics for: Local Idx = 19bb00b4
------------------------------------------------------------------
Statistic Name                              Counts
--------------                              ------
IO Send success/fail                        263/0
IO Receive success/fail                     384/0
IO Receive peek fail                        0
Peer connection mismatch                    0
Handshake success after signing in retries  0
Signing still in progress (dropped)         0
Negotiate msg rx success/fail               6/0
Peer init request tx/response rx            0/0
Signing module op attempts/success/fail     1/1/0
Signing in module busy                      0
Verify peer mac address fail                0
Verify peer certificate fail                0
Retransmitted handshakes                    0
SSL msg write fail (out of resources)       0
SSL msg write fail (error)                  0
SSL msg read fail (out of resources)        0
SSL msg read fail (error)                   0
Total DTLS msg tx/rx                        253/376
18:64:72:cf:ec:9a# show cluster-security peers stats
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.76
----------------------------------------------------------------------
Statistic Name                                                     Counts
--------------                                                     ------
Peer collisions occurred/resolved                                  0/0
Peer connections active/connected/recv data/close notify/shutdown  36/16/0/20/0
Peer connections being renegotiated                                15
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.73
----------------------------------------------------------------------
Statistic Name                                                     Counts
--------------                                                     ------
Peer collisions occurred/resolved                                  0/0
Peer connections active/connected/recv data/close notify/shutdown  36/21/0/15/0
Peer connections being renegotiated                                20
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.75
----------------------------------------------------------------------
Statistic Name                                                     Counts
--------------                                                     ------
Peer collisions occurred/resolved                                  0/0
Peer connections active/connected/recv data/close notify/shutdown  36/17/0/19/0
Peer connections being renegotiated                                16
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.74
```

```
---------------------------------------------------------------------
Statistic Name                                                   Counts
--------------                                                   ------
Peer collisions occurred/resolved                                0/0
Peer connections active/connected/recv data/close notify/shutdown  36/18/0/18/0
Peer connections being renegotiated                              17
Cluster Security Peers' Statistics for: Remote Address = 10.17.142.71
---------------------------------------------------------------------
Statistic Name                                                   Counts
--------------                                                   ------
Peer collisions occurred/resolved                                0/0
Peer connections active/connected/recv data/close notify/shutdown  36/16/0/20/0
Peer connections being renegotiated
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show configuration

```
show configuration
```

Description

This command displays the configuration saved on the OAW-IAP. Use this command to view the entire configuration saved on the OAW-IAP, including all wireless and wired profiles, uplink configuration, ARM settings, radio profiles, ACLs, and interface settings.

Example

The following example displays the **show configuration** command output:

```
version 6.2.1.0-3.3.0.0
virtual-controller-country IN
virtual-controller-key e10e371601fae77a3ba78e44585d06c407f0a3e9a83835c1c4
name Instant-CB:D4:20
terminal-access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap d8:c7:c8:cb:d4:20
allowed-ap d8:c7:c8:cb:d3:98
allowed-ap d8:c7:c8:cb:d3:b4
routing-profile
route  192.0.2.0  255.0.0.0  192.0.2.1
arm
wide-bands 5ghz
a-channels 56,60,64,149,153,157,161,165,36+,44+,149+,157+
g-channels 11,1+,7+
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
syslog-level debug ap-debug
syslog-level debug network
syslog-level debug security
syslog-level debug system
syslog-level debug user
syslog-level debug user-debug
syslog-level debug wireless
mgmt-user admin 16e8d1cbd13f13a18cd1adb8b0d23022
wlan access-rule default_wired_port_profile
rule any any match any any any permit
wlan access-rule wired-instant
rule 192.0.2.1 255.255.255.255 match tcp 80 80 permit
rule 192.0.2.2 255.255.255.255 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule rule-1
rule any any match any any any permit
wlan access-rule rule-local-nw
rule any any match any any any permit
hotspot anqp-nai-realm-profile "test"
enable
nai-realm-name ""
nai-realm-eap-method eap-ttls
nai-realm-auth-id-1 non-eap-inner-auth
```

```
nai-realm-auth-value-1 mschapv2
nai-realm-auth-id-2 credential
nai-realm-auth-value-2 uname-passward
nai-realm-encoding utf8
no nai-home-realm
hotspot anqp-nwk-auth-profile "test"
enable
nwk-auth-type http-redirect
url "http:///"
hotspot anqp-3gpp-profile "test"
enable
3gpp-plmn1 ""
3gpp-plmn2 ""
3gpp-plmn3 ""
3gpp-plmn4 ""
3gpp-plmn5 ""
3gpp-plmn6 ""
hotspot anqp-ip-addr-avail-profile "test"
enable
ipv4-addr-avail
no ipv6-addr-avail
hotspot h2qp-wan-metrics-profile "test"
enable
wan-metrics-link-status (null)
no symm-link
no at-capacity
uplink-speed 0
downlink-speed 0
uplink-load 0
downlink-load 0
load-duration 0
hotspot hs-profile "test"
enable
no comeback-mode
no asra
no internet
no pame-bi
no group-frame-block
no p2p-dev-mgmt
no p2p-cross-connect
query-response-length-limit 5
access-network-type private
venue-group business
venue-type research-and-dev-facility
roam-cons-len-1 0
roam-cons-oi-1 ""
roam-cons-len-2 0
roam-cons-oi-2 ""
roam-cons-len-3 0
roam-cons-oi-3 ""
wlan ssid-profile profile-1
enable
index 0
type employee
essid profile-1
wpa-passphrase c52acfeb3e59ef254a6d14fe2ad565382e46f7eecde33af3
opmode wpa2-psk-aes
max-authentication-failures 0
vlan 333
rf-band all
captive-portal disable
dtim-period 1
inactivity-timeout 1000
```

```
broadcast-filter none
external-server
bandwidth-limit 65535
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
wlan ssid-profile profile-local-nw
enable
index 1
type employee
essid profile-local-nw
wpa-passphrase dd4da86c25c31bf83417024a338982ed4f01e1751e7a4502
opmode wpa2-psk-aes
max-authentication-failures 0
vlan 2
auth-server InternalServer
rf-band all
captive-portal disable
dtim-period 1
inactivity-timeout 1000
broadcast-filter none
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
auth-survivability cache-time-out 24
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
blacklist-time 3600
auth-failure-blacklist-time 3600
ids classification
ids
wireless-containment none
ip dhcp something-vlan10
server-type Centralized,L2
server-vlan 333
ip dhcp local-vw-vlan2
server-type Local
server-vlan 2
subnet 192.0.2.5
subnet-mask 255.255.255.0
wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
```

```
duplex full
no poe
type employee
captive-portal disable
no dot1x
enet0-port-profile default_wired_port_profile
uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180
airgroup
enable
airgroupservice airplay
disable
description AirPlay
airgroupservice airprint
disable
description AirPrint
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show config-status

```
show config-status
```

Description

This command displays the details about the configuration status of an OAW-IAP. Use this command to view the current configuration status of the OAW-IAP in flash memory.

Example

The following example shows the output of the **show config-status** command:

```
Config Status
-------------
Config Name  Compressed
-----------  ----------
Primary      No
Backup       No
```

The backup configuration is used when the primary configuration is lost. And the **Compressed** option indicates that the configuration file has been compressed if the file size is large.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show console-settings

```
show console-settings
```

Description

This command displays the details about the console settings of an OAW-IAP. Use this command to view if the access to OAW-IAP console is enabled or disabled.

Example

The following example shows the output of the **show console-settings** command:

```
(Instant AP)# show console-settings
Console Setting
---------------
Status
------
enabled
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show country-codes

```
show country-codes
```

Description

This command shows the list of supported country codes for the OAW-IAP.

Example

The following example shows a partial output of the **show country-codes** command:

```
CA:Canada
DE:Germany
NL:Netherlands
IT:Italy
PT:Portugal
LU:Luxembourg
NO:Norway
SE:Sweden
FI:Finland
DK:Denmark
CH:Switzerland
CZ:Czech Republic
BE:Belgium
ES:Spain
GB:United Kingdom
KR:Republic of Korea (South Korea)
CN:China
FR:France
HK:Hong Kong
SG:Singapore
TW:Taiwan
MY:Malaysia
BR:Brazil
SA:Saudi Arabia
LB:Lebanon
AE:United Arab Emirates
ZA:South Africa
AR:Argentina
AU:Australia
AT:Austria
BO:Bolivia
CL:Chile
GR:Greece
HU:Hungary
IS:Iceland
IN:India
IE:Ireland
KW:Kuwait
LV:Latvia
LI:Liechtenstein
LT:Lithuania
MX:Mexico
MA:Morocco
NZ:New Zealand
PL:Poland
SK:Slovak Republic
SI:Slovenia
TH:Thailand
UY:Uruguay
PA:Panama
```

```
RU:Russia
EG:Egypt
TT:Trinidad and Tobago
TR:Turkey
CR:Costa Rica
EC:Ecuador
HN:Honduras
KE:Kenya
UA:Ukraine
VN:Vietnam
BG:Bulgaria
CY:Cyprus
EE:Estonia
MT:Malta
MU:Mauritius
RO:Romania
CS:Serbia and Montenegro
ID:Indonesia
PE:Peru
VE:Venezuela
JM:Jamaica
BH:Bahrain
OM:Oman
JO:Jordan
BM:Bermuda
CO:Colombia
DO:Dominican Republic
GT:Guatemala
PH:Philippines
LK:Sri Lanka
SV:El Salvador
TN:Tunisia
MO:Macau
PK:Islamic Republic of Pakistan
QA:Qatar
DZ:Algeria
NG:Nigeria
HR:Croatia
GH:Ghana
BA:Bosnia and Herzegovina
MK:Macedonia
MI:Maritime Offshore
MB:Maritime Forward Operating Base
KZ:Kazakhstan
TD:Chad
ML:Mali
```

The following output of the **show country-codes** command displays the country codes of the US and its territories:

```
US:United States
PR:Puerto Rico
GU:Guam
MH:Marshall Islands
FM:Federated States of Micronesia
MP:Northern Mariana Islands
VI:US Virgin Islands
AS:American Samoa
```

Command History

Release	Modification
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cpcert

```
show cpcert
```

Description

This command displays the details of the captive portal server certificate used by the OAW-IAP for guest authentication.

Example

The following example shows the default certificate details of the captive portal server in the output of the **show cpcert** command:

```
Default Server Certificate:
Version       :3
Serial Number :01:DA:52
Issuer        :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SSL CA
Subject       :0x05=lLUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com,
OU=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated -
QuickSSL(R) Premium, CN=securelogin.arubanetworks.com
Issued On     :2011-05-11 01:22:10
Expires On    :2017-08-11 04:40:59
Signed Using  :SHA1
RSA Key size  :2048 bits
```

The output of this command describes details such as the version, serial number, subject, issue date, expiry date, type of encryption, and RSA key information for the captive portal certificates uploaded to the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show cpu

```
show cpu [details]
```

Description

This command displays the CPU details. Use this command to view CPU load for application and system processes.

Parameter	Description	Range	Default
`details`	Include this optional parameter at the request of Alcatel-Lucent technical support to display additional CPU troubleshooting statistics.	—	—

Example

The following example shows the output of **show cpu** command:

```
user   0% nice   8% system   1% idle  89% io   0% irq   0% softirq   2%
```

The following example shows the output of **show cpu details** command:

```
Mem: 66488K used, 59668K free, 0K shrd, 0K buff, 22540K cached
Load average: 0.12 0.09 0.09  (Status: S=sleeping R=running, W=waiting)
PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
1434 root     R N     5540  1377  8.3  4.3 sapd
13137 root     R <      356 12694   2.3  0.2 top
1430 root     R <     7256  1377  0.0  5.7 cli
12694 root     S <     2880 12685   0.0  2.2 cli
1429 root     S       2508     1  0.0  1.9 cli
1682 root     S <     2392  1377  0.0  1.8 radiusd-term
1699 root     S <     2384  1377  0.0  1.8 radiusd
1442 root     S <     2092  1377  0.0  1.6 snmpd
1436 root     S <     1804  1377  0.0  1.4 stm
1449 root     S <     1472  1377  0.0  1.1 meshd
1413 root     R N     1408  1377  0.0  1.1 awc
1448 root     S <     1332  1377  0.0  1.0 lldpd
1445 root     S <     1164  1377  0.0  0.9 mdns
1259 root     S        948     1  0.0  0.7 tinyproxy
1377 root     S <      844     1  0.0  0.6 nanny
1450 root     S <      796  1377  0.0  0.6 hostapd
1281 root     S <      748     1  0.0  0.5 mini_httpd
1284 root     S <      740     1  0.0  0.5 mini_httpd
1278 root     S <      728     1  0.0  0.5 mini_httpd
1382 root     S <      688  1377  0.0  0.5 msgHandler
1451 root     S <      624  1377  0.0  0.4 wpa_supplicant
```

The output of this command shows the percentage of CPU utilization.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show datapath

```
show datapath {acl <ID>|acl-all|acl-allocation|acl-rule <rule>|acl-rule-
detail<acl>|bridge|bwm-table|counters|device <statistics>|https-blocked-ip-cache|ipv6
{session|user}|dmo-session|dmo-station <mac>
|dns-id-map|mcast|nat-pool <ID>|route|sbr|session[ucc|dpi <verbose>]|statistics|subnet
|user|vlan|vlan-mcast[vlan-ID]|vlan-port-mapping|dns-ip-learning}
```

Description

This command shows the system statistics for your OAW-IAP. Use this command to display various datapath statistics for debugging purposes.

Parameter	Description	Range	Default
`acl <ID>`	Displays datapath statistics associated with a specified ACL.	—	—
`acl-all`	Displays datapath statistics associated with all ACLs.	—	—
`acl-allocation`	Displays ACL table allocation details.	—	—
`acl-rule <rule>`	Displays the name of the ACL.	—	—
`acl-rule-detail <acl>`	Displays the ACL rule details.	—	—
`bridge`	Shows bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for anOAW-IAP.	—	—
`bwm-table`	Displays the configured bandwidth contracts and the allocated bandwidth contracts.	—	—
`counters`	Displays various counters maintained in the datapath. This parameter is useful in debugging any datapath issue.	—	—
`device <statistics>`	Displays various datapath counters for packets that are received from and sent to the devices.	—	—
`https-blocked-ip-cache`	Displays cached entries for the HTTPS error page ACL in datapath.	—	—
`ipv6 session`	Displays datapath for IPv6 session table.	—	—
`ipv6 user`	Displays datapath statistics for IPv6 users.	—	—
`dmo-session`	Displays details of a DMO session.	—	—
`dmo-station <mac>`	Displays details of a DMO station.	—	—

Parameter	Description	Range	Default
`dns-id-map`	Displays IP address of the domain name configured in a domain-based ACL.	—	—
`dns-ip-learning`	Displays the list of IP addresses learned by the Wi-Fi client during the DNS learning phase.	—	—
`mcast`	Displays multicast table statistics for the OAW-IAP.	—	—
`nat-pool <ID>`	Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, SITP start, SIP end and DIP.	—	—
`route`	Displays datapath route table statistics.	—	—
`sbr`	Displays the destination servers that are reachable through a particular IP address.	—	—
`session {ucc|dpi<verbose>]`	Displays datapath session statistics.	—	—
`statistics`	Displays datapath station association table statistics.	—	—
`subnet`	Displays the datapath subnet table.	—	—
`user`	Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.	—	—
`vlan`	Displays VLAN table information such as VLAN memberships inside the datapath including L2 tunnels which tunnel L2 traffic.	—	—
`vlan-mcast`	Displays the multicast table statistics for the OAW-IAP.	—	—
`vlan-port-mapping`	Displays the user VLAN details for the OAW-IAP.	—	—

Examples

show datapath acl

The following example shows the output of **show datapath acl** command.

```
Datapath ACL 3 Entries
-----------------------
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
I - Invert SA, i - Invert DA, H - high prio, O - set prio,
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
```

```
----------------------------------------------------------------
```

show datapath acl-all

The following example shows the output of **show datapath acl-all** command.

```
ACL Name {magic-vlan} Number {106}
1:  any  any  17 0-65535 8209-8211  P4
2:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  any  P4
3:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  any  P4
4:  192.168.10.0 255.255.254.0  any  any  PS4
5:  any  any  any  P4  hits 2127
----------------------------------------------------------------
ACL Name {internal-cp-magic} Number {107}
1:  any  192.168.10.1 255.255.255.255  6 0-65535 80-80  PSD4
2:  any  192.168.10.1 255.255.255.255  6 0-65535 443-443  PSD4
3:  any  any  6 0-65535 80-80  PSD4
4:  any  any  6 0-65535 443-443  PSD4
5:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  17 0-65535 67-68  P4
6:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  17 0-65535 67-68  P4
7:  192.168.10.0 255.255.254.0  any  17 0-65535 67-68  PS4
8:  any  any  17 0-65535 67-68  P4
9:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  17 0-65535 53-53  P4
10:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  17 0-65535 53-53  P4
11:  192.168.10.0 255.255.254.0  any  17 0-65535 53-53  PS4
12:  any  any  17 0-65535 53-53  P4
13:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  6 0-65535 8081-8081  P4
14:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  6 0-65535 8081-8081  P4
15:  192.168.10.0 255.255.254.0  any  6 0-65535 8081-8081  PS4
16:  any  any  6 0-65535 8081-8081  P4
17:  any  any  any  4
----------------------------------------------------------------
ACL Name {external-cp-magic} Number {108}
1:  any  192.168.10.1 255.255.255.255  6 0-65535 80-80  PSD4
2:  any  192.168.10.1 255.255.255.255  6 0-65535 443-443  PSD4
3:  any  any  6 0-65535 80-80  PSD4
4:  any  any  6 0-65535 443-443  PSD4
5:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  17 0-65535 67-68  P4
6:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  17 0-65535 67-68  P4
7:  192.168.10.0 255.255.254.0  any  17 0-65535 67-68  PS4
8:  any  any  17 0-65535 67-68  P4
9:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  17 0-65535 53-53  P4
10:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  17 0-65535 53-53  P4
11:  192.168.10.0 255.255.254.0  any  17 0-65535 53-53  PS4
12:  any  any  17 0-65535 53-53  P4
13:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  6 0-65535 8081-8081  P4
14:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  6 0-65535 8081-8081  P4
15:  192.168.10.0 255.255.254.0  any  6 0-65535 8081-8081  PS4
16:  any  any  6 0-65535 8081-8081  P4
17:  any  any  any  4
----------------------------------------------------------------
```

show datapath acl-allocation

The following example shows the output of **show datapath acl-allocation** command.

```
ACL    ACE Start     ACE Block Size
----   ----------    ---------------
105    3200            32
103    3234            16
107    3250            32
104    3282            16
108    3298            32
100    3330             2
101    3332             4
```

```
102    3336            4
134    3340            4
135    3344            8
136    3352            4
143    3360            8
145    3372            8
130    3380           16
131    3412           16
132    3444           16
133    3476           16
137    3508            8
139    3520            8
141    3532            8
146    3540            4
147    3544            8
148    3552            4
149    3556            8
150    3564            4
151    3568            4
152    3572            4
153    3576            4
138    3580            8
140    3588            8
142    3596            8
144    3604            8
106    3612            8
```

show datapath acl-rule

The following example shows the output of **show datapath acl-rule** command.

```
Datapath SSID: test ACL Entries
----------------------------------------------------------------
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter
S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror
I - Invert SA, i - Invert DA, H - high prio, O - set prio,
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
----------------------------------------------------------------
ACL Name {test 0} Number {142}
1:  any  any  17 0-65535 8209-8211  P4
2:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  any  P4
3:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  any  P4
4:  192.168.10.0 255.255.254.0  any  any  PS4
5:  any  any  any  P4
----------------------------------------------------------------
ACL Name {test 1} Number {143}
1:  any  any  17 0-65535 8209-8211  P4
2:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  any  P4
3:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  any  P4
4:  192.168.10.0 255.255.254.0  any  any  PS4
5:  any  any  any  P4
----------------------------------------------------------------
ACL Name {test 2} Number {144}
1:  any  any  17 0-65535 8209-8211  P4
2:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  any  PT4
3:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  any  PT4
4:  192.168.10.0 255.255.254.0  any  any  PST4
5:  any  any  any  PT4
----------------------------------------------------------------
ACL Name {test 3} Number {145}
1:  any  any  17 0-65535 8209-8211  P4
2:  192.168.10.0 255.255.254.0  192.168.10.0 255.255.254.0  any  PT4
3:  192.168.10.0 255.255.254.0  224.0.0.0 224.0.0.0  any  PT4
4:  192.168.10.0 255.255.254.0  any  any  PST4
```

```
5:  any  any  any  PT4
----------------------------------------------------------------
```

show datapath bridge

The following example shows the output of **show datapath bridge** command.

```
Datapath Bridge Devices
-----------------------------
Flags: F - source-filter, T - trusted, Q - tagged, I - IP
S - split-tunnel, B - bridge, M - mesh, P - PPPoE
C - content-filter, O - corp-access, h - to HAP, f - to FAP
h - dhcp-redirect b - blocked by STP
Dev Name VLANs PVID ACLs MTU FramesRx FramesTx Flags
--- ----------------- ----- ---- ----------- ---- -------- -------- --------
3 eth1 1 3333 134/0 0 1700 0 0 FB
5 bond0 3 1 0/0 106 3500 359364 69733 FTQB
12 br0 0 1 105/0 0 1300 45731 0 IB
16 aruba000 1 111 130/0 0 1500 0 0 B
17 aruba100 1 111 130/0 0 1500 0 0 B
18 aruba001 1 1 136/0 0 1500 23443 1142 B
19 aruba101 1 1 136/0 0 1500 0 0 B
…
Datapath Bridge Table Entries
-----------------------------
Flags: P - Permanent, D - Deny, R - Route, M - Mobile, X - Xsec, A - Auth
AP Flags: X - Awaiting 1X reply, B - Block all non-1X traffic, F - Force bridge role
MAC          VLAN  Assigned VLAN  Destination  Flags  AP Flags  Bridge Role ACL
-----------------  ----  -------------  -----------  -----  --------  ---------------
00:1A:1E:0D:7E:D3  1     1              dev3                                        0
D8:C7:C8:C4:42:98  1     1              local        P                              0
D8:C7:C8:C4:42:98  3333  3333           local        P                              0
00:0B:86:40:1C:A0  1     1              dev3                                        0
6C:F3:7F:C3:5C:12  64    64             dev3                                        0
```

show datapath bwm-table

The following example shows the output of **show datapath bwm-table** command.

```
Received BWM Config:
--------------------
ACL  DIR   Contract-ID  PerUser  UseCount  Rate
---  ---   -----------  -------  --------  ----
135  up    2            1        1         1000000
135  down  1            1        1         1000000
139  up    4            0        2         5000000
139  down  3            0        2         5000000
143  up    6            1        1         4555000
143  down  5            1        1         4555000
173  up    8            0        1         1111000
173  down  7            0        1         1111000
175  up    10           0        1         1111000
175  down  9            0        1         1111000
177  up    12           0        1         1111000
177  down  11           0        1         1111000
179  up    14           0        1         1111000
179  down  13           0        1         1111000
181  up    16           0        1         1111000
181  down  15           0        1         1111000
183  up    18           0        1         1111000
183  down  17           0        1         1111000
185  up    20           0        1         1111000
185  down  19           0        1         1111000
187  up    22           0        1         1111000
187  down  21           0        1         1111000
```

```
189  up    24           0        1         1111000
189  down  23           0        1         1111000
Allocated Contracts:
--------------------
Contract-ID  Rate     UseCount  ACL  Available-Bytes  Max-Bytes
-----------  ----     --------  ---  ---------------  ---------
1            1000000  1         0/0  3907             3907
2            1000000  1         0/0  3907             3907
3            5000000  2         0/0  19532            19532
4            5000000  2         0/0  19532            19532
5            4555000  1         0/0  17793            17793
6            4555000  1         0/0  17793            17793
7            1111000  1         0/0  4340             4340
8            1111000  1         0/0  4340             4340
9            1111000  1         0/0  4340             4340
10           1111000  1         0/0  4340             4340
11           1111000  1         0/0  4340             4340
12           1111000  1         0/0  4340             4340
13           1111000  1         0/0  4340             4340
14           1111000  1         0/0  4340             4340
15           1111000  1         0/0  4340             4340
16           1111000  1         0/0  4340             4340
17           1111000  1         0/0  4340             4340
18           1111000  1         0/0  4340             4340
19           1111000  1         0/0  4340             4340
20           1111000  1         0/0  4340             4340
21           1111000  1         0/0  4340             4340
22           1111000  1         0/0  4340             4340
23           1111000  1         0/0  4340             4340
24           1111000  1         0/0  4340             4340

Policed-Bytes  Queued-Bytes  Queued-Pkts  Dropped-pkts
-------------  ------------  -----------  ------------
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0
0              0             0            0

Bandwidth Contracts for cpu type 0 has 25 contracts
BWM divisor for type:0 : 32(32)
1(cpu:0): flags 0, 1000192 bps, policed 0,  dropped 0 queued 0/0, avail 3907, pktq 0/0 0/0
r:1000000 t:0
```

```
2(cpu:0): flags 0, 1000192 bps, policed 0,  dropped 0 queued 0/0, avail 3907, pktq 0/0 0/0
r:1000000 t:0
3(cpu:0): flags 0, 5000192 bps, policed 0,  dropped 0 queued 0/0, avail 19532, pktq 0/0 0/0
r:5000000 t:6203
4(cpu:0): flags 0, 5000192 bps, policed 0,  dropped 0 queued 0/0, avail 19532, pktq 0/0 0/0
r:5000000 t:5177
5(cpu:0): flags 0, 4555008 bps, policed 0,  dropped 0 queued 0/0, avail 17793, pktq 0/0 0/0
r:4555000 t:0
6(cpu:0): flags 0, 4555008 bps, policed 0,  dropped 0 queued 0/0, avail 17793, pktq 0/0 0/0
r:4555000 t:0
7(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
8(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
9(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
10(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
11(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
12(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
13(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
14(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
15(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
16(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
17(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
18(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
19(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
20(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
21(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
22(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
23(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
24(cpu:0): flags 0, 1111040 bps, policed 0,  dropped 0 queued 0/0, avail 4340, pktq 0/0 0/0
r:1111000 t:0
Bandwidth Contracts for cpu type 0 has 0 cp contracts total queued in CPU 0 total queing fail
0
Queued pkts in cpus:
```

show datapath counters

The following example shows the output of **show datapath counters** command.

```
IAP Datapath Counter Stats
--------------------------
Firewall Queue scheduled 5919 Firewall Queue scheduled 345724
Firewall Rx Queue: length 0, dropped 0
Firewall Tx Queue: length 0, dropped 0
DMO queue: size:512, dropped:0, rescheduled:0, length:0, high-water:0
CPU 0: Tlet Calls=0 Rx=0/0 SJRx=0/0 Tx=0 yields=0/0 EthIn=0
CPU 1: Tlet Calls=0 Rx=0/329806 SJRx=0/0 Tx=21835 yields=0/2 EthIn=329806
GMAC 0 Statistics:
RX Frames:        bf5690c0   TX Frames:        00000000
RX Failures:      00055d99   TX Failures:      00000000
Dot1dDiscards:    000000c7   Policed Frames:    00000000
```

```
v4 FW Denied:     00000008   v6 FW Denied:       00000000
GMAC 1 Statistics:
RX Frames:        bf569310   TX Frames:        00000000
GMAC 2 Statistics:
RX Frames:        bf569560   TX Frames:        00000000
Dot1dDiscards:    0000081d   Policed Frames:    00000000
Maintenance Statistics:
Application Statistics:
RX ICMP Errors:   0000081d   RX ICMP Denied:   00000003
Bridge Statistics:
Cur Entries:      00000007   High Entries:     00000009
Max Entries:      00004000   Total Entries:    0000191e
IP Reassembly Statistics:
cpu| cur   | high |  max | tot   | full |ageidx|
IP Reverse Fragment Statistics:
cpu| cur   | high |  max | tot   | full | ctx_w_buf | aged |
IPv6 Reassembly Statistics:
cpu| cur   | high |  max | tot   | full |ageidx|
IPv6 Reverse Fragment Statistics:
cpu| cur   | high |  max | tot   | full | ctx_w_buf | aged |
WiFi Reassembly Statistics:
cpu| cur   | high |  max | tot   | full |ageidx|
0| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |
1| 0000 | 0000 | 0000 | 0000 | 0000 | 0000 |
Route Cache Statistics:
Cur Entries(v4/v6):      00000003/00000000   High Entries:     00000007
Max Entries:      00001000   Total Entries:    00000003
Overflows:        00000000   Stale Entries: 0000000d/00000000
session_fib 0  session_fib_routed 0 session_fib_stale 0 session_fib_rt_fallback 0 session_
fib_race 0
Route Table Statistics:
Cur Entries(v4/v6):      00000003/00000000   High Entries:     00000003
Max Entries:      00000080   Total Entries:    00000009
Patricia: Cur 00000003 Full 00000000 Dup 00000000 Ignore 00000000
Null: Cur 00000000 Full 00000000 ECMP Full 00000000
Session Statistics:
Cur Entries:      00000003/00000000   High Entries:     0000005b/00000003
Max Entries:      00008000            Total Entries:    000021fc/0000003a
Aged Entries:     000021ed/0000003a
Stale Entries:    00000001/00000000
Max link length :
Cur Entries:      00000001            High Entries:     00000003
User Statistics:
Uke Cur Entries:      00000003/00000001/00000002/00000000   High Entries:     00000008
Max Entries:      00000fff   Total Entries:    00000026
Full:        00000000   Denied:           00000000/00000000
Uae Cur Entries:      00000002   High Entries:     00000006
Station list Statistics:
Cur Entries:      00000002   High Entries:     00000000
Max Entries:      000007ff   Total Entries:    00000002
```

show datapath device statistics

The following example shows the output of **show datapath device statistics** command.

```
dev            InPkts   FAST     IP    UDP   DHCP     TCP    ARP  MCAST
------------   ------   ----     --    ---   ----     ---    ---  -----
eth1                0      0      0      0      0      0      0      0
bond0             638      0    225     37     36    178      1    448
br0               167      0    167     11      0    156      0      0
------------   ------   ----     --    ---   ----     ---    ---  -----

UCAST  OutPkts   FAST     IP    UDP   DHCP     TCP    ARP  MCAST  UCAST
-----  -------   ----     --    ---   ----     ---    ---  -----  -----
```

```
 0      448       0       36     36     36      0      0    448      0
190      168      0       167    11     0     156      1      0    168
167      601      0       189    1      0     178      0    412    189
-----  -------   ----     --    ---   ----    ---    ---  -----  -----
```

show datapath ipv6 session

The following example shows the output of the **show datapath ipv6 session** command:

```
Datapath Session Table Entries (v6)
-----------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based
Source IP                               Destination  IP  Prot SPort Dport
--------------------------------------  ------------- --- ---- ----- -----
fe80::aea3:1eff:fecd:4708               ff02::16      58   5782  36608
fe80::6273:5cff:fe65:ee19               ff02::16      58   53973 36608
fe80::9198:30aa:5217:d22a               ff02::16      58   47682 36608
fe80::6273:5cff:fe65:ee19               ff02::d       103  0     0
fe80::6273:5cff:fe65:ee19               ff02::1       58   43684 33280
fe80::f25c:19ff:fecb:34d0               ff02::16      58   64552 36608
fe80::9198:30aa:5217:d22a               ff02::16      58   30486 36608
fe80::3e97:eff:fe48:9e45                ff02::16      58   59459 36608
fe80::aea3:1eff:fecd:4694               ff02::16      58   5968  36608
fe80::aea3:1eff:fecd:471a               ff02::16      58   1289  36608
Cntr Prio ToS Age Destination TAge  Flags
---- ---- --- --- ----------- ---- -----
0    0    0   1   dev8        6e   C
0    0    0   1   dev8        63   C
0    0    0   1   dev8        60   C
0    0    0   0   dev8        8    C
0    0    0   1   dev8        88   C
0    0    0   1   dev8        82   C
0    0    0   1   dev8        6c   C
0    0    0   1   dev8        59   C
0    0    0   1   dev8        62   C
0    0    0   1   local       76   C
```

show datapath ipv6 user

The following example shows the output of the **show datapath ipv6 user** command:

```
Datapath User Table Entries (v6)
--------------------------------
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP                                  MAC                ACLs    Contract   Location  Age
----------------------------------  -----------------  ------  ---------  --------  -----
2001:470:36:5c3:ffff:ffff:ffff:5b   AC:A3:1E:CD:47:1A  105/0      0/0     0         0
fe80::aea3:1eff:fecd:471a           AC:A3:1E:CD:47:1A  105/0      0/0     0         0

Sessions   Flags     Vlan  FM
---------  -----     ----  --
0/65535              1   N
0/65535              1   N
```

show datapath dmo-session

The following example shows the output of **show datapath dmo-session** command.

```
MCAST Groups:
--------------
Source  Group           Vlan    Age[s]  BSSs    Received        Multicast

Converted       Unicast Dropped         _Stas   _l2grp  _l3grp

DMO queue: size:256, dropped:0, rescheduled:0, length:0, high-water:0
DMO Sessions:
-------------
```

show datapath dmo-station

The following example shows the output of **show datapath dmo-station** command.

```
Group             Ref_count         Position
```

show datapath dns-id-map

The following example shows the output of **show datapath dns-id-map** command:

```
entry:0 id:1 www.google.com
93.46.8.89          173.252.71.184
entry:1 id:2 facebook.com
93.46.8.89          173.252.120.6
entry:2 id:3 twitter.com
104.244.42.129      104.244.42.1        74.117.182.194
```

show datapath dns-ip-learning

The following example shows the output of show datapath dns-ip-leanring command:

```
DNS IP            Carrier
--------------    -----------
208.54.85.64      T-Mobile
208.54.65.100     T-Mobile
```

show datapath https-blocked-ip-cache

The following example shows the output of **show datapath https-blocked-ip-cache** command:

```
IP                    Network                         LifeTime
------------------- ------------------------------ -------------
106.38.179.32         4                               95
106.39.178.1          4                               59
54.239.25.192         4                               7
54.239.26.128         3,4                             0
119.188.142.1         3                               26
61.135.144.254        4                               16
```

show datapath mcast

The following example shows the output of **show datapath mcast** command:

```
Dev       Vlans
--------  ----------------------
dev3      1
dev11     1
dev12     1
dev13     1
dev14     1
```

show datapath nat-pool

The following example shows the output of **show datapath nat-pool** command.

```
Datapath NAT Pool Entries
```

```
-------------------------
ID  Begin Source IP  End Source IP  Destination IP  Flags
--  ---------------  -------------  --------------  -----
```

show datapath route

The following example shows the output of **show datapath route** command.

```
Route Table Entries
-------------------
Flags: L - Local, P - Permanent,  T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop
IP                Mask            Gateway          Cost  VLAN  Flags
---------------  ---------------  ---------------  ----  ----  -----
0.0.0.0          0.0.0.0          10.17.88.2          0     0
192.168.10.0     255.255.254.0    192.168.10.1        0  3333  D
0.0.0.0          255.255.255.192  10.17.88.59         0     1  L
Route Cache Entries
-------------------
Flags: L - local, P - Permanent,  T - Tunnel, I - IPsec, M - Mobile, A - ARP, D - Drop
IP                MAC                VLAN        Flags
---------------  -----------------  -----------  -----
10.17.88.2       00:0B:86:40:1C:A0            1  A
10.17.88.59      D8:C7:C8:C4:42:98            1  LP
192.168.10.1     D8:C7:C8:C4:42:98         3333  LP
```

show datapath sbr

The following example shows the partial output of **show datapath sbr** command.

```
Source Based Routing Datapath Table
-----------------------------------
Source   SBR Index  Mask           Gateway    VLAN  Used
------   ---------  ----           -------    ----  ----
1.1.1.2  1          255.255.255.0  1.1.1.254  4     1
```

show datapath session

The following example shows the partial output of **show datapath session** command.

```
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based

Source IP    Destination IP Prot SPort Dport TAge Flags
------------- -------------- ---- ----- -----
10.17.141.42  10.17.141.44   17   4434  4434
10.17.141.44  10.17.141.42   17   4434  4434

Cntr Prio ToS Age Destination Packets Bytes Dpi InnerAppID PktsAppMoni  TAge  Flags
---- ---- --- --- ----------- ------- ----- ---- --------- -----------  ----- -----
0     0  0   0   local       106     c016   5      c           13      4e9c  F
0     0  0   0   local       670     13cd50 5      c           f       4e9c  FC
```

The following example shows the partial output of **show datapath session ucc** command.

```
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
```

```
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based

Source IP       Destination IP  Prot SPort Dport
------------    --------------  ---- ----- -----
10.17.138.91    10.17.138.90    17   50023 50022
10.17.138.90    10.17.138.91    17   50022 50023
10.17.138.91    10.17.138.90    17   50012 50014
10.17.138.90    10.17.138.91    17   50014 50012

Cntr Prio ToS   Destination Flags Codec
---- ---- ---   ----------- ----- --------
0    0    40    dev18       FHTCVL X_H264UC
0    0    40    dev18       FHTVL  X_H264UC
0    0    48    dev18       FHTCVL SILK
0    0    48    dev18       FHTVL  SILK
```

The following example shows the output of **show datapath session dpi** command.

```
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based
DPI Flags: a - app extraction done, b - URL extraction done
c - copied to dpimgr, d - dropped reverse session on bca cache miss
w - waiting for classification, e - enforcement done
f - app classification done, g - webcc classification done
DPI WebRep: 1 - High Risk Sites, 2 - Suspicious Sites
3 - Moderate Risk Sites, 4 - Low Risk Sites
5 - Trustworthy Sites
Source IP         Destination IP  Prot SPort Dport App
----------------  --------------  ---- ----- ----- --------------------------
10.20.120.252     173.223.235.19  6    63421 80    linkedin            [305 ]
10.20.120.228     10.13.5.200     17   50338 53    incomplete          [6   ]
10.22.152.66      10.20.120.252   6    443   63460 https               [68  ]
10.20.120.240     132.245.73.194  6    54365 443   office365           [1448]
74.125.68.188     10.20.120.228   6    5228  5844  gtalk               [1441]
10.1.10.10        10.20.120.252   6    139   63391 incomplete          [6   ]
15.50.26.221      10.20.120.144   6    5222  50783 App-Not-Class       [0   ]
10.20.120.187     216.58.197.69   17   57576 443   incomplete          [6   ]
10.20.120.173     10.22.35.50     6    50162 22    ssh                 [198 ]
10.20.120.147     40.113.14.159   6    51324 443   office365           [1448]
computer-and-intern [5  ] 5
10.20.120.187     10.20.50.10     6    55956 135   epm                 [37  ]
10.20.120.198     172.217.26.78   6    56432 443   google              [54  ]
news-and-media      [63 ] 5
10.20.120.147     10.44.96.64     6    62236 44591 App-Not-Class       [0   ]
132.245.244.146   10.20.120.198   6    443   54673 office365           [1448]
10.20.120.198     10.1.10.10      6    56463 445   incomplete          [6   ]
```

```
10.20.120.251     59.161.166.108  6    37685 8080  incomplete          [6   ]
132.245.242.114   10.20.120.173   6    443   50119 office365           [1448]
10.1.8.53         10.20.120.153   6    80    49543 soap                [191 ]
10.29.83.170      10.20.120.173   6    22    63997 ssh                 [198 ]
24:77:03:CE:B3:1C               0806            App-Not-Class          [0   ]
216.58.197.78     10.20.120.228   6    443   8590  google-play         [1122]
10.20.120.228     10.53.12.175    6    5017  22    ssh                 [198 ]
10.20.120.198     172.217.26.78   6    56433 443   google              [54  ]
10.20.120.252     10.1.8.53       6    63454 80    soap                [191 ]
10.22.152.66      10.20.120.252   6    443   63269 https               [68  ]
10.22.152.66      10.20.120.252   6    443   63461 https               [68  ]
10.20.120.240     10.20.120.255   17   137   137   nbns                [128 ]
10.20.120.173     10.13.5.200     17   60658 53    incomplete          [6   ]
10.1.10.10        10.20.120.252   6    139   63390 incomplete          [6   ]
10.44.96.200      10.20.120.252   6    41050 62338 msrpc               [742 ]


 Webcat                    WebRep Packets Bytes PktsDpi Flags  DPIFlags
------------------------- ------ ------- ----- ------- ----- ---------
content-delivery-ne [65 ] 5      0       0     1       C      abcdefg
Web-Not-Class       [0  ] 0      1       55    1       FCIA   ac
Web-Not-Class       [0  ] 0      0       0     3              acef
computer-and-intern [5  ] 5      0       0     1       CGs    abcefg
category-unknown    [84 ] 7      0       0     0              acef
category-unknown    [84 ] 7      0       0     3       F      ace
Web-Not-Class       [0  ] 0      0       0     0       YA
Web-Not-Class       [0  ] 0      5       220   5       FC     ace
category-unknown    [84 ] 7      0       0     1       C      acef
business-and-econom [4  ] 5      0       0     1       CGs    abcefg
computer-and-intern [5  ] 5
category-unknown    [84 ] 7      0       0     1       FC     acef
shopping            [7  ] 5      1       29    1       CGs    abcefg
news-and-media      [63 ] 5
Web-Not-Class       [0  ] 0      0       0     0       C
computer-and-intern [5  ] 5      0       0     0              abcefg
category-unknown    [84 ] 7      3       108   6       FC     ace
category-unknown    [84 ] 7      0       0     3       C      ace
computer-and-intern [5  ] 5      0       0     0              abcefg
private-ip-addresse [77 ] 4      7       354   0       F      abcefg
category-unknown    [84 ] 7      1       28    0              acef
Web-Not-Class       [0  ] 0      0       0     0       F
shareware-and-freew [30 ] 5      1       34    0              abcefg
category-unknown    [84 ] 7      0       0     0       C      acef
search-engines      [50 ] 5      1       29    1       CGs    abcefg
private-ip-addresse [77 ] 4      0       0     2       FC     abcefg
Web-Not-Class       [0  ] 0      0       0     3              acef
Web-Not-Class       [0  ] 0      0       0     3              acef
Web-Not-Class       [0  ] 0      5       186   1       FC     acef
Web-Not-Class       [0  ] 0      0       0     1       FCIA   ac
category-unknown    [84 ] 7      0       0     5       F      ace
category-unknown    [84 ] 7      1       34    0              acef
```

show datapath statistics

The following example shows the partial output of **show datapath statistics** command.

```
Datapath Counters
---------------------
Counter                                                          Value
-------                                                         ------
Tagged frames dropped on untagged interface                          0
Frames dropped for being too short                                   0
Frames received on port not in VLAN                                  0
Non-dot1x frames dropped during L2 blocking                          0
```

```
Frames dropped for ingress change on permanent bridge entry          0
Frames received on port not in VLAN                                  0
Unicast frames filtered                                             86
Frames dropped due to FP firewall                                    6
Frames that failed FP spoofing check                                 0
Frames dropped with logging                                          0
Frames dropped due to unknown FP opcode                              0
Frames freed by FP                                                   3
Frames that failed SP spoofing check                                 0
Frames dropped due to excessive user misses                          0
Frames dropped due to no buffers                                     0
Frames dropped due to no 'br0' device                                0
Frames dropped due to no stack IP address                            0
Frames dropped while user miss pending                               0
Frames dropped when user entry creation failed                       0
Frames dropped due to unknown FP opcode                              0
Frames dropped due to initial IP route lookup failure                0
Frames dropped due to final IP route lookup failure                  0
Frames dropped due to ARP processing failure                         0
Frames dropped due to illegal device index                           0
Frames dropped due to interface being down                           0
Unicast frames not bridged due to split-tunnel destination           0
Unicast frames from bridge role user dropped                         0
Unicast frames that could not be bridged to split tunnel             0
Frames dropped due to missing PPP device                             0
Frames dropped due to pullup failure                                 0
Frames dropped due to misalignment                                   0
Frames received by firewall                                     715679
DHCP frames on DHCP local VLAN                                   96041
PPPOE frames to session processing                                   0
Frames needing bridging                                         716075
Mesh frames forwarded                                                0
Thin AP frames forwarded                                             0
Frames to session processing                                    718714
Frames to SP                                                     21792
Frames bridged by SP                                               396
Frames routed by SP                                                  0
Frames for SP session processing                                 17454
Frames for FP application processing                              3942
Frames bridged by FP                                                 0
Frames for FP session processing                                  2725
Frames routed by FP                                              18577
FP user misses                                                      73
Frames not tunneled from bridge role user                            0
SP user misses                                                      73
Frames to DHCP                                                      18
Frames to DNS                                                        0
Frames held                                                          0
Frames needed routing                                           715572
Frames needed forwarding                                        634373
Frames redirected to CSS tunnel                                      0
Frames sent by firewall                                          94681
Frames delivered to stack                                        82061
Frames delivered to CP                                               0
Frames to be flooded                                            538842
Frames potentially needing flooding                             637659
```

show datapath subnet

The following example shows the output of **show datapath subnet** table command.

```
Subnet Datapath Table
---------------------------
Flags: L - local, G - Gateway, D - DNS, S - Static
```

```
VLAN    IP              MASK            MAC                     IP Age  MAC Age Flags
-----   ------------    ------          -----------------       ------- ------- ---
1       10.17.162.1     255.255.255.0   D8:C7:C8:C4:42:98       13      13      G
3333    172.38.92.1     255.255.254.0   20:4c:03:24:89:18       0       0       LG
```

show datapath user

The following example shows the partial output of **show datapath user** command.

```
Datapath User Table Entries
---------------------------
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
R - ProxyARP to User, N - VPN, L - local
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP                MAC                ACLs    Contract   Location
---------------  -----------------  -------  ---------  --------
10.17.88.59      D8:C7:C8:C4:42:98   105/0      0/0      0
0.0.0.0          D8:C7:C8:C4:42:98   105/0      0/0      0
192.168.10.1     D8:C7:C8:C4:42:98   105/0      0/0      0

 Age    Sessions   Flags     Vlan  FM
 -----  ---------  -----     ----  --
 0        1/65535              1   N
 0        0/65535  P           1   N
 11115    0/65535  P        3333   B
```

show datapath vlan

The following example shows the partial output of **show datapath vlan** command.

```
Datapath VLAN Table Entries
---------------------------
Flags: N - Nat Inside, M - Route Multicast, R - Routing
S - Snoop MLD, G - Snoop IGMP, P - Proxy IGMP
VLAN  Flags   Ports
----  ------  -----
1     R        dev3
1     R        dev11
1     R        dev12
1     R        dev13
1     R        dev14
```

show datapath vlan-mcast

The following example shows the output of the **show datapath vlan-mcast** command.

```
Datapath VLAN Multicast Entries
---------------------------
VLAN  Destinations
----  ------------
1     dev8
121   dev8, dev18, dev19, dev20, dev21
3333  dev3, dev8, dev22, dev23
```

show datapath vlan-port-mapping

The following example shows the partial output of the **show datapath vlan-port-mapping** command.

```
Datapath VLAN-Port-Mapping Table Entries
---------------------------
VLAN  Port  Users
----  ----  -----
```

The outputs of the **show datapath** command indicates the following:

- ACL table allocation details for the OAW-IAP.

- OAW-IAP Datapath ACL Tables.
- List of ACL rules configured for the SSID and Ethernet port profiles.
- Bridge table entry statistics including MAC address, VLAN, assigned VLAN, destination and flag information for the OAW-IAP.
- Details of a DMO session.
- Multicast table statistics for the OAW-IAP.
- Route table statistics for the OAW-IAP.
- Datapath session table statistics for the OAW-IAP
- Hardware packet statistics for the OAW-IAP.
- Datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length for the OAW-IAP.
- VLAN table information such as VLAN memberships inside the datapath including L2 tunnels for the OAW-IAP.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The output of the **show datapath session** command was modified to include the following columns: ■ InnerAppID ■ PktsAppMoni
Alcatel-Lucent AOS-W Instant 8.5.0.0	The **subnet** parameter was added.
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **dns-ip-learning** parameter was added.
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ddns

```
show ddns [clients]
```

Description

This command displays the DDNS status of the OAW-IAP and the list of DDNS clients.

Example

The following output is displayed for the **show ddns** command:

```
DDNS Enabled      :Enabled
DDNS Server       :10.17.132.85
DDNS Key          :hmac-sha1:ddns-key:asdafsdfasdfsgdsgs=
DDNS Interval     :900
```

The following output is displayed for the **show ddns clients** command:

```
DDNS Client List
----------------
Host Name       Domain Name  IP Address      DHCP profile name  Success Count  Failure Count
---------       -----------  ----------      -----------------  -------------  -------------
iap1-ddns-home  test.ddns    192.192.192.17  None               16             22
132-13-Auto-PC  test.ddns    192.168.99.18   DistL3             9              3
132-14-Auto-PC  test.ddns    192.168.99.4    DistL3             2              0

Last updated    Last update status
------------    ------------------
7 seconds ago   Success
7 seconds ago   Success
7 seconds ago   Success
```

NOTE

DHCP profile name is None for the Master OAW-IAP update sent.

The output of this command provides the following information:

Column	Description
Host Name	Displays the host name of the DDNS client
Domain Name	Displays the domain name mapped to the DDNS client.
IP Address	Denotes the IP address of the DDNS client.
DHCP profile name	Denotes the profile name of the DHCP server.
Success Count	Indicates the number of times the update sent to the DNS server succeeded.
Failure Count	Indicates the number of times the update sent to the DNS server got failed.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show debug ap log

```
show debug ap log
   <ip>
```

Description

This command shows the debug log of the OAW-IAP. Use this command to view the debug log of the OAW-IAPs. To view the debug log, enable debug logging for the OAW-IAP using the **debug ap log enable** command. To view the debug log of an individual AP from the master OAW-IAP, specify the IP address of the AP using the following format: **show debug ap log <ip>**.

Parameter	Description
`show debug ap log`	Displays the debug log of the AP.
`<ip>`	Specify the IP address of the AP for which you want to view the debug log.

Example

The following example shows the output of **show debug ap log** command:

```
AP debug log :enabled
AP-10.65.65.14
--------------
Index  Time                Context
-----  ----                -------
0      Mar 20 10:02:39  recv_heartbeat_local 6877 heartbeat, cfg_id:0, current:0 top:0.
checksum error.
1      Mar 20 10:02:39  send_config_init 12339 delta_cfg_id:0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show debug pkt status

```
show debug pkt status
```

Description

This command shows the configuration of the **debug pkt** command.

Example

The following example shows the output of **show debug pkt status** command:

```
Enter 'debug pkt dump' to dump packets on console
OR 'debug pkt mirror <ip>' to mirror them
If source, destination or target IP is 10.20.102.208
AND packet is of type ICMP
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show delta-config

```
show delta-config [<cfgid>]
```

Description

This command displays the difference between the current configuration in the current CLI session and the configuration that is saved on the OAW-IAP. Use this command to view the difference between the current configuration information stored in the OAW-IAP flash memory and the configuration information saved in the OAW-IAP memory.

Example

The following example shows the output of the **show delta-config** command:

```
103-Master# show delta-config
IAP delta configuration current_config_id:7
IAP delta configuration top_config_id:7
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show derivation-rules

```
show derivation-rules
```

Description

This command displays the list of role and VLAN derivation rules configured for the WLAN SSIDs and wired profiles in an OAW-IAP. Use this command to view the derivation rules configured for a network profile.

Example

The following example shows the output of the **show derivation-rules** command:

```
SSID:Example1
Role Derivation Rules
---------------------
Attribute   Operation  Operand  Role Name  Index  Hits
--------   ---------  -------  ---------  -----  ----
Filter-Id  contains   123456   Example1   8      0
AP-Name    contains   instant  instant    9      0
Vlan Derivation Rules
---------------------
Attribute   Operation  Operand  Vlan Id  Hits
--------   ---------  -------  -------  ----
AP-Group   contains   instant  200      0
Filter-Id  contains   123456   200      0
```

The output of the command provides a list of role and VLAN derivation rules configured for each SSID and wired profile.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dhcp

```
show dhcp
  opt82 xml-config
  subnets
```

Description

This command displays the subnet details and the gateway IP for Distributed L2 and Distributed L3 networks and also displays the status of option 82 configuration.

Example

The following example shows the output of the **show dhcp subnets** command:

```
DHCP Subnet Table
-----------------
VLAN Type  Subnet         Mask             Gateway      Mode                Rolemap
----  ----  ------         ----             -------      ----                -------
532   l2    192.168.132.0 255.255.255.0    0.0.0.0      remote,full-tunnel  VLAN532
539   nat   192.168.1.0    255.255.255.0    192.168.1.1  local,split-tunnel  VLAN532
538   l3    192.168.2.0    255.255.255.0    192.168.2.1  local,split-tunnel  VLAN532
534   l2    0.0.0.0        255.255.255.255  0.0.0.0      remote,full-tunnel  VLAN532
```

The output of this command displays the following information:

Column	Description
`VLAN`	Displays the VLAN details.
`Type`	Displays the type of DHCP assignment mode.
`Subnet`	Displays the subnet details.
`Mask`	Displays the subnet mask details.
`DNS Server`	Displays the DNS server IP address.
`Gateway`	Displays the gateway IP address.
`Mode`	Displays details of the tunnel mode.
`Rolemap`	Displays the role assigned to the clients.

The following example shows the output of the **show dhcp opt82 xml-config** command. This is in a scenario where the XML file is not uploaded in flash and the DHCP option 82 parameters are not configured.

```
DHCP Option82 XML
----------------------------
XML File Downloaded in Flash       : No
XML based DHCP Option82 Configured : No
```

The following example shows the output of the **show dhcp opt82 xml-config** command. This is in a scenario where the XML file is successfully uploaded in flash and the DHCP option 82 parameters are configured.

```
DHCP Option82 XML
----------------------------
XML File Downloaded in Flash                : /tmp/mydhcpoption82.xml
XML File Load Command                       :http://10.20.52.131/dhcp.xml
XML File Load Status                        : Success
XML based DHCP Option82 Configured          : Yes
DHCP Option82 Circuit_ID
-----------------------------------
->:Circuit_ID is added first in DHCP Opt82
->:SubOption APMAC to be added in ASCII format separated with <-> in lower-case at position 1
in Circuit_ID of DHCP option82
DHCP Option82 Remote_ID
--------------------------------------
->:Remote_IDis added second in DHCP Opt82
->:SubOption UEMAC to be added in ASCII format separated with <-> in lower-case at position 1
in Remote_ID of DHCP option82
```

The following example shows the output of the **show dhcp opt82 xml-config** command. This is in a scenario where a user tries to download a file with a different extension:

```
DHCP Option82 XML
-----------------
XML File Downloaded in Flash        :No
XML File Load Command               :http://10.20.52.131/dhcp.c
XML File Load Status                :Failed
XML File Loading Error              :Specified file does not have .xml extension
XML based DHCP Option82 Configured  :No
```

The output of this command displays the following information:

Column	Description
`XML File Downloaded in Flash`	Displays the XML file in flash. It is set to No if the file is not in Flash.
`XML File Load Command`	Displays the downloaded URL that is utilized.
`XML File Load Status`	Displays the status of the XML file download. If the XML file is uploaded in flash, then the file upload status is successful. When the file upload status is unsuccessful, a new parameter is added to display the error occurred.
`XML File Load Error`	This is visible only when the file upload is unsuccessful. This displays the error occurred.
`XML based DHCP Option82 Configured`	Indicates whether the DHCP Option 82 parameters are configured using the **dhcp option82-xml <mydhcpoption82.xml>** command.
`DHCP Option82 Circuit_ID`	Displays information regarding the order of circuit ID in option 82, and the sub-options configured.
`DHCP Option82 Remote_ID`	Displays information regarding the order of remote ID in option 82, and the sub-options configured.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **opt82 xml-config** parameter was introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dhcp-allocation

```
show dhcp-allocation
```

Description

This command displays information about the DHCP address allocation. Use this command to view DHCP address allocation for network address translated clients to allow mobility of the clients across OAW-IAPs.

Example

The following example shows the output of **show dhcp-allocation** command:

```
(Instant AP)# show dhcp-allocation
---------------------/etc/dnsmasq.conf--------------------
listen-address=127.0.0.1
addn-hosts=/etc/ld_eth_hosts
addn-hosts=/etc/ld_ppp_hosts
dhcp-src=192.168.10.1
dhcp-leasefile=/tmp/dnsmasq.leases
dhcp-authoritative
filterwin2k
#magic-vlan
{
vlan-id=3333
dhcp-range=192.168.10.3,192.168.11.254,255.255.254.0,12h
dhcp-option=1,255.255.254.0
dhcp-option=3,192.168.10.1
dhcp-option=6,10.1.1.50
dhcp-option=54,192.168.10.1
}
---------------------/tmp/dnsmasq.leases------------------
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dhcpc-opts

```
show dhcpc-opts
```

Description

This command displays the DHCP options configured on an OAW-IAP. Use this command to view the current status of the vendor-specific DHCP options configured on anOAW-IAP. The DHCP options are configured and enabled for assignment and distribution to DHCP clients based on the type of DHCP server, scope, and clients.

Example

The following output is displayed for the **show dhcpc-opts** command:

```
-------------------DHCP option43 --------------------
Not available
```

The output of this command displays the vendor-specific DHCP option configured for a DHCP scope and the current status of the DHCP option.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dhcps config

```
show dhcps config
```

Description

This command provides information about the DHCP scopes configured for an OAW-IAP. Use this command to view configuration details associated with the DHCP scopes enabled on an OAW-IAP.

Example

The following example shows the output of the **show dhcps config** command:

```
Distributed DHCP Scopes
-----------------------
Name        Type            VLAN  Netmask  Default Router  DNS Server  Domain Name
----        ----            ----  -------  --------------  ----------  -----------
Instnt-DL2  Distributed,L2  100   0.0.0.0  0.0.0.0         0.0.0.0

Lease Time  IP Address Range  Client Count  DHCP Option  Reserve First  Reserve Last
----------  ----------------  ------------  -----------  -------------  ------------
43200                         10                         0              0

Branch ID  Branch Netmask  Branch Router  DHCP Host  DHCP DDNS  DDNS Key
---------  --------------  -------------  ---------  ---------  --------
0.0.0.0    0.0.0.0         0.0.0.0                   Disabled


Centralized DHCP Scopes
-----------------------
Name          Type            VLAN   DHCP Relay  DHCP Relay Servers  DHCP Option 82  VLAN IP
VLAN Mask  Split Tunnel
----          ----            ----   ----------  ------------------  --------------  -------
---------  ------------
CL2           Centralized,L2  400    OFF         0.0.0.0             None
           enable
cl-vlan34-50  Centralized,L2  20-50  OFF         0.0.0.0             None
           disable
cl3-123       Centralized,L3  123    ON          123.123.123.3

DHCP Option 82  VLAN IP        VLAN Mask      Split Tunnel
--------------  -------        ---------      ------------
None                                          enable
None                                          enable
None            123.123.123.1  255.255.255.0  enable

Local DHCP Scopes
-----------------
Name       Type      VLAN  Network        Netmask        Exclude Address   Mask
----       ----      ----  -------        -------        ---------------  --------------
local-112  Local,L2  112   112.112.112.0  255.255.255.0                    1.2.3.4

Default Router  DNS Server  Domain Name  Lease Time  DHCP Option  DHCP Host
----------      -----------  ----------  ----------- ---------    ---------
0.0.0.0          43200                    0          Disabled

DNS Cache  Available Address Range   VLAN IP  VLAN
-----------------------           -------  ---------
112.112.112.0 - 112.112.112.255     0.0.0.0  0.0.0.0
```

The output of this command displays the following information:

Column	Description
`Name`	Displays the name of the DHCP scope.
`type`	Displays the DHCP assignment modes. The current release of AOS-W Instant supports the following DHCP assignment modes. ■ **Distributed, L2** ■ **Distributed, L3** ■ **Local** ■ **Local, L3** ■ **Centralized, L2**
`VLAN`	Indicates the VLAN ID assigned to DHCP scope.
`Netmask`	Displays the subnet mask.
`DNS Server`	Displays the DNS server IP address.
`Domain Name`	Displays the domain name configured for the DHCP scope.
`Default router`	Displays the IP address of the default router.
`lease-time`	Displays the lease-time configured for the DHCP clients.
`IP Address Range`	Displays the range of IP addresses configured for the distributed DHCP scopes.
`client-count <number>`	Displays the number of clients allowed per DHCP branch.
`DHCP Option`	Displays the DHCP option if configured.
`Reserve First and Reserve Last`	Displays the first few and the last few IP addresses reserved in the subnet.
`Branch ID`	Displays the DHCP branch ID.
`Branch Netmask`	Displays the branch subnet mask.
`Branch Router`	Displays the IP address if the branch router.
`Exclude IP address`	Displays the excluded IP address. The value displayed in this determines the exclusion range of the subnet. Based on the size of the subnet, the IP addresses that come before or after the IP address value specified in this field are excluded.
`DHCP Relay`	Displays the DHCP relay information that enables the OAW-IAPs to intercept the broadcast packets and relay DHCP requests directly to corporate network.
`DHCP Relay Server`	Displays the IP address of the corporate DHCP server for the DHCP request relay.
`Split Tunnel`	Indicates if the split-tunnel function is enabled or disabled.
`DHCP Host`	Indicates the DHCP host name if configured.
`DNS cache`	Indicates if DNS caching is enabled or disabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Output of the command modified.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show distributed-dhcp-branch-counts

```
show distributed-dhcp-branch-counts <type> <sip> <eip>
```

Description

This command displays the branch count for the distributed DHCP scopes configured on an OAW-IAP.

Parameter	Description
`type`	Displays the branch details for the distributed DHCPs based on the type of the DHCP scope specified. The current release of AOS-W Instant supports the following distributed DHCP assignment modes. ■ **Distributed, L2** ■ **Distributed, L3**
`<sip> <eip>`	Filters the branch count information based on an IP address range specified for the starting IP address <sip> and ending IP address parameters. You can specify up to four different ranges of IP addresses to filter the command output.

Example

The following example shows the output of the **show distributed-dhcp-branch-counts** command:

```
Branch Count Table
-------------------
Client Count Upto  Branch Count
-----------------  ------------
1                  10
2                  4
3                  3
7                  1
```

The output of this command displays the following information:

Column	Description
`Client Count Upto`	Displays the number of clients allowed for each DHCP branch.
`Branch Count`	Displays the number of branches allowed for the specified range of IP addresses.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show domain-names

```
show domain-names
```

Description

This command displays the list of enterprise-domains configured on an OAW-IAP. Use this command to view enterprise-domains list. The enterprise domains list displays the DNS domain names that are valid on the enterprise network.

This list is used to determine how client DNS requests should be routed. When Content Filtering is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the configured DNS server.

Example

The following example shows the output of the **show domain-names** command:

```
example1.com
example.com
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dpi

```
show dpi {app <name_all>|appcategory <name_all>|debug {<statistics>|<status>|ssid-
table}|qsessions [detail][<session_id>]|webcategory <name_all>|webcategory-lookup
<url>|webcc-url-prefix-table [referenced|unreferenced]}
```

Description

This command displays the DPI configuration information.

Parameter	Description	Range	Default
`app <name_all>`	Displays a list of all applications (with the **all** keyword) and details such as application name, ID, application category, and default ports when a specific application name is provided.	—	—
`appcategory <name_all>`	Displays the list of all application categories (with the **all** keyword) and details of the applications that belong to a specific application category when an application category is specified.	—	—
`debug {statistics|status}`	Displays DPI statistics or status that can be used for debugging. The **ssid-table** parameter shows the mapping of WLAN index and BSSID in DPI process.	—	—
`qsessions [detail [<session_id>]`	Displays advanced debug statistics for troubleshooting the DPI issues.	—	—
`webcategory <name_all>`	Displays the list of web categories.	—	—
`webcategory-lookup <URL>`	Displays the details for a given URL and the reputation score based on security rating. Run this command twice to fetch information from the cloud server.	—	—
`webcc-url-prefix-table [referenced|unreferenced]`	Displays all the current webcc url prefix entries stored in the dpimgr webcc hash table. ■ **referenced**—Displays all the current webcc url prefix entries referenced in the current 15-minute cycle present in the dpimgr webcc hash table. ■ **unreferenced**—Displays all the existing webcc url prefix entries stored in the dpimgr hash table which	—	—

Parameter	Description	Range	Default
	have not been referenced in the current 15-minute cycle.		

Example

show dpi app

The following example shows the output of the **show dpi app <name_all>** command:

```
(Instant AP)# show dpi app wikipedia

Pre-defined Application
-----------------------
Name       App ID  App Category  Default Ports
----       ------  ------------  -------------
wikipedia  222     web           tcp 80
```

The output of this command displays details such as the name of the application, application category, default ports configured for DPI.

show dpi appcategory

The following example shows the output of the **show dpi appcategory all** command:

```
(Instant AP)# show dpi appcategory all
Pre-defined Application Categories
----------------------------------
Name                    App Category ID
----                    ---------------
antivirus               1
authentication          2
behavioral              3
cloud-file-storage      4
collaboration           5
encrypted               6
enterprise-apps         7
gaming                  8
im-file-transfer        9
instant-messaging       10
mail-protocols          11
mobile-app-store        12
network-service         13
peer-to-peer            14
social-networking       15
standard                16
streaming               17
thin-client             18
tunneling               19
unified-communications  20
web                     21
webmail                 22
mobile                  23
Total application categories = 23
```

The output of this command displays all application categories.

show dpi debug statistics

The following example shows the output of the **show dpi debug statistics** command.

```
DPI Engine Version          :4.20.0-34 (build date Aug 21 2016)
API Version                 :1.190.0
Protocol Bundle Version     :1.230.0-20 (build date Aug 21 2016)
Dpimgr Debug Statistics
```

```
------------------------
Key                                          Value
---                                          -----
dpimgr total pkt handled                     2043(1961)
dpimgr total classified                      581(556)
dpimgr qsession total alloc                  1026(981)
dpimgr qsession total uapp alloc             800(765)
dpimgr qsession total uapp alloc free        799(764)
dpimgr qsession total session age            1024(979)
dpimgr qsession classified skipped           73(73)
dpimgr qsession event param error            16(16)
dpimgr qsession total classified             562(537)
dpimgr qsession total request received       1691(1624)
dpimgr bca total cloud lookup                23(17)
dpimgr bca total cached lookup               226(225)
dpimgr bca total request received            258(242)
dpimgr bca total classified                  19(19)
Dpimgr cloud internal stats
----------------------------
dns/name server configured           :yes
url cloud lookup server reachable    :yes
number of cache hits                 :227
number of cloud hits                 :22
number of cloud lookups              :22
Max time taken for cloud lookups     :0.230000
number of local database hits        :0
number of uncategorized responses    :1
number of cache entries              :16
maximum queue depth reached          :1
trusted user rep average             :91
guest user rep average               :0
total number of lookup errors        :0 (net: 0 + http: 0 + proto: 0)
current major version                :0
current minor version                :0
DPI datapath stats
-------------------
number of pkts send to dpimgr                    :1691
number of msg prepare failure                    :0
number of visibility stats cpy to dpimgr failure :0
number of cloud dpi session mismatch             :0
number of cloud dpi session unclassified         :0
number of bytes in tx socket buffer              :0
number of bytes in rx socket buffer              :0
total number of incomplete session               :0
number of dpi session mismatch                   :0
IAP average cpu usage in 10 secs                 :20
allowed unclassified session in 10 secs (max=0)  :0
unclassified dpi session in 10 secs              :8
total number of unclassified session             :406
DPI debug pkt stats
```

show dpi debug status

The following example shows the output of the **show dpi debug status** command:

```
Dpimgr Running                     :TRUE
Dpimgr Hello count                 :1
Dpimgr Agent                       :All set - App, Webcc & URL
Dpimgr Status value                :0x3b
Dpimgr Platform Status             :App + WebCC + URL
Dpimgr Visibility Status           :App + WebCC
Dpimgr Enforcement Status          :None
Dpimgr External Visibility Status :None
Dpimgr BCA Proxy Connection        :Established
Dpimgr BCA Server SSL Established :True
Dpimgr BCA Server Reachable       :Unknown
```

The output of this command includes the following parameters:

Column	Description
`Dpimgr Running`	Displays the current state of the DPIMGR process.
`Dpimgr Hello count`	Denotes the number of times the DPIMGR process has restarted and completed initialization.
`Dpimgr Agent`	Displays the DPIMGR components that are currently running.
`Dpimgr Status value`	Denotes the DPIMGR configuration flags set.
`Dpimgr Platform Status`	Denotes the DPIMGR configuration that the current platform can support
`Dpimgr Visibility Status`	Displays the DPIMGR components that are configured for visibility.
`Dpimgr Enforcement Status`	Denotes if the DPIMGR statistics are reported to ALE, and AMP.
`Dpimgr External Visibility Status`	Denotes the DPIMGR components that are configured for enforcement.
`Dpimgr BCA Proxy Connection`	Indicates if a connection is established between the OAW-IAP and the proxy server. This parameter has 4 states: ■ **Configured**—Denotes that the proxy configuration is present ■ **Not Configured**—Denotes that the proxy configuration is not present ■ **Established**—Denotes that a TCP connection has been established between the OAW-IAP and the BCA proxy server ■ **Failure**—Denotes a failure in establishing a TCP connection between the OAW-IAP and the BCA proxy server
`Dpimgr BCA Server SSL Established`	Indicates if an SSL connection has been established with the Bright Cloud server or not.
`Dpimgr BCA Server Reachable`	Indicates if the Bright Cloud server is reachable or not. This parameter has 3 states: ■ **Unknown**—Indicates the state when the DPI manager does not know if the BCA server is reachable or not. ■ **Reachable**—Indicates the state when the BCA server is reachable during a web category lookup. ■ **Not Reachable**—Indicates the state when the BCA server is unreachable during a web category lookup.

show dpi debug ssid-table

The following example shows the output of the **show dpi debug ssid-table** command:

```
network id  bssid offset  essid
----------  ------------  -----
0           -             8.4-advanced-zone-test0
1           -             8.4-advanced-zone-test1
2           2             8.4-advanced-zone-test2
3           -             8.4-advanced-zone-test3
4           -             8.4-advanced-zone-test4
5           -             8.4-advanced-zone-test5
6           -             8.4-advanced-zone-test6
7           -             8.4-advanced-zone-test7
```

```
8           -             8.4-advanced-zone-test8
9           -             8.4-advanced-zone-test9
10          3             8.4-advanced-zone-test10
11          -             8.4-advanced-zone-test11
12          -             8.4-advanced-zone-test12
13          -             8.4-advanced-zone-test13
14          -             8.4-advanced-zone-test14
15          4             8.4-advanced-zone-test15
16          -             8.4-advanced-zone-test16
17          5             8.4-advanced-zone-test17
18          6             8.4-advanced-zone-test18
19          7             8.4-advanced-zone-test19
20          8             8.4-advanced-zone-test20
21          9             8.4-advanced-zone-test21
22          10            8.4-advanced-zone-test22
23          11            8.4-advanced-zone-test23
24          12            8.4-advanced-zone-test24
25          13            8.4-advanced-zone-test25
26          14            8.4-advanced-zone-test26
27          15            8.4-advanced-zone-test27
28          -             8.4-advanced-zone-test28
29          -             8.4-advanced-zone-test29
30          -             8.4-advanced-zone-test30
255         -
```

show dpi webcategory

The following example shows the output of the **show dpi webcategory all** command:

```
(Instant AP)# show dpi  webcategory all
Pre-defined BrightCloud Web Categories
--------------------------------------
Name                                 Web Category ID
----                                 ---------------
real-estate                          1
computer-and-internet-security       2
financial-services                   3
business-and-economy                 4
computer-and-internet-info           5
auctions                             6
shopping                             7
cult-and-occult                      8
travel                               9
abused-drugs                         10
adult-and-pornography                11
home-and-garden                      12
military                             13
social-networking-web                14
dead-sites                           15
individual-stock-advice-and-tools    16
training-and-tools                   17
dating                               18
sex-education                        19
religion                             20
entertainment-and-arts               21
personal-sites-and-blogs             22
legal                                23
local-information                    24
streaming-media                      25
job-search                           26
gambling                             27
translation                          28
reference-and-research               29
shareware-and-freeware               30
```

```
peer-to-peer-web                  31
marijuana                         32
hacking                           33
games                             34
philosophy-and-political-advocacy  35
weapons                           36
pay-to-surf                       37
hunting-and-fishing               38
society                           39
educational-institutions          40
online-greeting-cards             41
sports                            42
swimsuits-and-intimate-apparel    43
questionable                      44
kids                              45
hate-and-racism                   46
personal-storage                  47
violence                          48
keyloggers-and-monitoring         49
search-engines                    50
internet-portals                  51
web-advertisements                52
cheating                          53
gross                             54
web-based-email                   55
malware-sites                     56
phishing-and-other-frauds         57
proxy-avoidance-and-anonymizers   58
spyware-and-adware                59
music                             60
government                        61
nudity                            62
news-and-media                    63
illegal                           64
content-delivery-networks         65
internet-communications           66
bot-nets                          67
abortion                          68
health-and-medicine               69
spam-urls                         71
dynamically-generated-content     74
parked-domains                    75
alcohol-and-tobacco               76
private-ip-addresses              77
image-and-video-search            78
fashion-and-beauty                79
recreation-and-hobbies            80
motor-vehicles                    81
web-hosting                       82
category-incomplete               83
category-unknown                  84
Total web categories = 81
```

The output of this command displays the list of web categories and the IDs associated with these categories.

show dpi webcategory-lookup

The following example shows the output of the **show dpi webcategory-lookup <url>** command:

```
(Instant AP)# show dpi webcategory-lookup www.yahoo.com
Input URL: www.yahoo.com
Request sent for CLOUD LOOKUP, please try again.
```

On running command again, the following information is retrieved from the cloud server and displayed as the output:

```
Input URL: www.yahoo.com
Found CACHED RESULT:
URL: yahoo.com REP: 81 A1: 0, Serial = 0x200001
Index: 0 Category: internet-portals(51) Confidence level: 98
```

show dpi webcc-url-prefix-table

The following example shows the output of the **show dpi webcc-url-prefix-table** command:

```
(Instant AP)# show dpi webcc-url-prefix-table
Client DPI Webcc Url Prefix Table
---------------------------------------------
DstIP URL Referenced
----- --- - -------------
151.101.158.2 jimdo.com 1
23.212.50.39 ctv.com 0
219.238.238.52 39.net 0
52.77.199.193 hostgator.com 1
162.13.248.104 indeed.co.in 1
66.29.212.110 w3schools.com 0
200.221.2.45 uol.com.br 1
50.23.192.82 dreamstime.com 1
Num of Entries:8
Current Webcc URL Prefix count: 85
Last Phase out Timestamp: Mon Jan 21 14:21:34 2019
Last Central Statistics Send Timestamp: Mon Jan 21 19:06:27 2019
```

show dpi webcc-url-prefix-table referenced

The following example shows the output of the **show dpi webcc-url-prefix-table referenced** command:

```
(Instant AP)# show dpi webcc-url-prefix-table referenced
Client DPI Webcc Url Prefix Table
---------------------------------------------
DstIP            URL                    Referenced
-----            --- -                  -------------
151.101.158.2    jimdo.com              1
52.77.199.193    hostgator.com          1
162.13.248.104   indeed.co.in           1
200.221.2.45     uol.com.br             1
50.23.192.82     dreamstime.com         1
Num of Entries:5
Current Webcc URL Prefix count: 8
Last Phase out Timestamp: Mon Jan 21 14:21:34 2019
Last Central Statistics Send Timestamp: Mon Jan 21 19:06:27 2019
```

show dpi webcc-url-prefix-table unreferenced

The following example shows the output of the **show dpi webcc-url-prefix-table unreferenced** command:

```
(Instant AP)# show dpi webcc-url-prefix-table unreferenced
Client DPI Webcc Url Prefix Table
---------------------------------------------
DstIP URL Referenced
----- --- - -------------
23.212.50.39 ctv.com 0
219.238.238.52 39.net 0
66.29.212.110 w3schools.com 0
Num of Entries:3
Current Webcc URL Prefix count: 8
Last Phase out Timestamp: Mon Jan 21 14:21:34 2019
Last Central Statistics Send Timestamp: Mon Jan 21 19:06:27 2019
```

Command History

Release	Modification
AOS-W Instant 8.5.0.0	The **show dpi webcc-url-prefix-table** command is added.
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **debug ssid-table** parameter was introduced.
Alcatel-LucentAOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dpi-error-page-urls

```
show dpi-error-page-urls
```

Description

This command displays the list of custom error page URLs that are displayed when web access is blocked by the AppRF policies configured on the OAW-IAP. The custom error page URLs are configured using **dpi-error-page-urls** command.

Example

The following example shows the output of the **show dpi-error-page-url** command:

```
Global DPI error page URLs Config
---------------------------------
ID  URL
--  ---
0   https://www.yahoo.com
1   https://www.test.com
```

The output of this command displays IDs and URLs that are blocked.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show dpi-stats

```
show dpi-stats
   app [id <app> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name] full |
   deny [full] | full]
   appcategory [id <appcat> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name]
   full | deny [full] | full]
   session [full]
   webcategory [id <web> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name]
   full | deny [full] | full]
   webreputation  [id <rep> [deny] [full] |user ip <ipaddr> [deny] [full] | [ssid <ssid-name]
   full | deny [full] | full]
```

Description

This command displays the DPI statistics.

Parameter	Description
`app`	Displays application statistics.
`appcategory`	Displays the DPI statistics for application category.
`session`	Displays datapath session details for DPI.
`webcategory`	Displays the DPI statistics for web category.
`webreputation`	Displays the DPI statistics for web reputation score.
`ssid`	Displays the DPI statistics for the last 15 minutes from each OAW-IAP connected to the SSID in the network.
`ssid name`	Displays DPI statistics for the last 15 minutes for the specified SSID.
`id`	Displays DPI statistics for the specified application, application category, web category or web reputation ID.
`user ip <ip-addr>`	Displays DPI statistics for specified user IP address.
`full`	Displays the complete DPI statistics for the application, application category, session, web category, and web reputation stored on the OAW-IAP since the last 15 minutes.
`deny`	Displays the blocked URLs and web content related traffic.

Example

show dpi-stats app

The following example shows the output of the **show dpi-stats app full** command:

```
Last snapshot timestamp 17:10:47
Dpi Top Application list
------------------------
App              AppId  Total bytes
---              -----  -----------
apple            306    10172
apns             1118   278
Not-Classified   0      160
---------------------------
Total bytes                   :10610
```

```
Classication percentage      :98
```

show dpi-stats appcategory

The following example shows the output of the **show dpi-stats appcategory full** command:

```
Last snapshot timestamp 17:10:47
Dpi Top Application category list
---------------------------------
App Category      App Category Id  Total bytes
------------      ---------------  -----------
web               20               10172
mobile-app-store  11               278
Not-Classified    0                160
---------------------------
Total bytes                  :10610
Classication percentage      :98
```

show dpi-stats session

The following example shows the output of the **show dpi-stats session full** command:

```
Datapath DPI CDR Session Table Entries
--------------------------------------
Source IP       App                Webcat                         Webrep
                                                TX Bytes  Rx Bytes
---------       ---                ------                         ------
                                                --------  --------
172.31.98.103   google-plus(1125)  social-networking-web(14)      trustworthy-sites(5)
8635      3697
172.31.98.103   krb5(97)           Not-Classified(0)              Not-Classified
                                      (0)       8237      5998
172.31.98.189   smb(185)           Not-Classified(0)              Not-Classified
                                      (0)       886       0
172.31.98.103   http(67)           Not-Classified(0)              Not-Classified
                                      (0)       507       4074
172.31.98.103   https(68)          computer-and-internet-info(5)  trustworthy-sites(5)
449597    644401
172.31.98.103   yahoo(1294)        web-based-email(55)            trustworthy-si
                                      tes(5)    6044      10818
172.31.98.103   gtalk(1441)        Not-Classified(0)              Not-Classified
                                      (0)       3375      5904
172.16.100.174  ssdp(197)          Not-Classified(0)              Not-Classified
                                      (0)       4339      0
Datapath DPI CDR Session Table Entries
--------------------------------------
Source IP       App                Webcat                         Webrep
                                              TX Bytes  Rx Bytes
---------       ---                ------                         ------
                                              --------  --------
10.17.139.167   ssdp(197)          Not-Classified(0)              Not-Classified
                                      (0)     6923      0
10.17.139.183   ssdp(197)          Not-Classified(0)              Not-Classified
                                      (0)     5458      0
172.16.100.174  udp(216)           Not-Classified(0)              Not-Classified
                                      (0)     152       0
10.17.139.167   windowslive(298)   internet-portals(51)           trustworthy-sites(5)  893
    5907
172.31.98.103   http(67)           computer-and-internet-info(5)  trustworthy-sites(5)  439
    1783
10.17.139.183   http(67)           computer-and-internet-info(5)  trustworthy-sites(5)  643
    620
Num of Entries:47
```

show dpi-stats webcategory

The following example shows the output of the **show dpi-stats webcategory full** command:

```
Last snapshot timestamp 17:25:43
Dpi Top Web Category list
-------------------------
Web Category                Web Category Id  Total bytes
------------                ---------------  -----------
computer-and-internet-info  5                740
---------------------------
Total bytes                  :740
```

show dpi-stats webreputation

The following example shows the output of the **show dpi-stats webreputation full** command:

```
Last snapshot timestamp 15:39:32
Dpi Top Web Reputation list
---------------------------
Web Reputation        Web Reputation Id  Total bytes
--------------        -----------------  -----------
trustworthy-sites     5                  1211900
moderate-risk-sites   3                  2998
---------------------------
Total bytes                  :1214898
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show drt state

```
show drt state
```

Description

This command displays the status of DRT upgrade in an OAW-IAP cluster.

Example

The following output is displayed for the **show drt state** command:

```
swarm drt upgrade status
------------------------
Mac                IP Address       AP Class   Status
---                ----------       --------   ------
70:3a:0e:cc:ed:5a  192.168.100.244  Lupus      drt-ok
84:d4:7e:c5:23:ae  192.168.100.251  Hercules   drt-ok
a8:bd:27:c7:a5:3e  192.168.100.237  Ursa       drt-ok
a8:bd:27:c7:a4:0e  192.168.100.174  Ursa       drt-ok
f0:5c:19:cb:3f:b4  192.168.100.245  Hercules   drt-ok
f0:5c:19:cb:3e:94  192.168.100.177  Hercules   drt-ok
40:e3:d6:cf:f7:46  192.168.100.236  Ursa       drt-ok
f0:5c:19:c9:c7:be  192.168.100.240  Vela       drt-ok
ac:a3:1e:c5:c5:58  192.168.100.238  Centaurus  drt-ok
20:4c:03:0e:c4:74  192.168.100.248  Vela       drt-ok
94:b4:0f:c1:bc:84  192.168.100.249  Centaurus  drt-ok
00:0b:86:8f:54:12  192.168.100.254  Aries      drt-ok
94:b4:0f:ca:ba:e4  192.168.100.241  Centaurus  drt-ok
40:e3:d6:cf:f4:de  192.168.100.252  Ursa       drt-ok
94:b4:0f:ca:d7:38  192.168.100.243  Centaurus  drt-ok
20:4c:03:17:d7:84  192.168.100.135  Ursa       drt-ok
c8:b5:ad:c3:ad:0a  192.168.100.250  Draco      drt-ok
a8:bd:27:cf:ec:4c  192.168.100.253  Hercules   drt-ok
a8:bd:27:ca:2b:5c  192.168.100.242  Vela       drt-ok
DRT version           :1.0_63044
DRT build time        :Jan 2,2018
Default from Image    :Yes
Upgrade in process    :No
Upgrade status        :drt ok
DRT sync in process   :No
Reset in process      :No
```

Column	Description
`DRT version`	Shows the DRT version of the OAW-IAP.
`DRT build time`	Shows the date the DRT build has passed.
`Default from Image`	Shows whether the OAW-IAP is using the default DRT from the image.
`Upgrade in process`	Shows whether the DRT upgrade of the AOS-W Instant cluster is in progress.
`Upgrade status`	Shows the status of DRT upgrade.
`DRT sync in process`	Shows if there is a slave OAW-IAP synchronizing the DRT file from the master OAW-IAP.
`Reset in process`	Shows if the new DRT file is being reset to the default DRT of the image.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show election

```
show election {statistics}
```

Description

This command shows the election statistics of the master OAW-IAP selected as Virtual Controller.

Parameter	Description	Range	Default
`statistics`	Shows master election statistics.	—	—

Example

The following example shows the output of **show election statistics** command:

```
State          : Master
master_beacon    : sent=657538 rcvd=0
hierarchy_beacon: sent=618829 rcvd=0
hierarchy_ack    : sent=0 rcvd=0
beacon_req       : sent=0 rcvd=0
beacon_resp      : sent=0 rcvd=0
election wait    : 0
timer slow       : 0
master high cpu : 0
ap cpu usage     : 7
Slave->Pot-Master : 0 time
Pot-master->Master: 0 time
Pot-master->Slave : 0 time
last spoof arp rcvd: 0
last spoof mac: 00:00:00:00:00:00
last beacon received ticks: 0
uplink flap count          : 0
max beacon miss ticks      : 0
hierarchy mode             : 0
last hierarchy beacon received ticks: 0
provisioned master denied : 0
```

The output of this command includes the following information:

Parameter	Description
`State`	Indicates if the OAW-IAP is provisioned as master.
`master_beacon`	Displays the number of beacons transmitted and received by the master OAW-IAP.
`hierarchy_beacon`	Displays the number of hierarchy beacons transmitted and received.
`hierarchy_ack`	Displays the number of hierarchy messages transmitted and received.
`beacon_req`	Displays the number of beacons required.
`beacon_resp`	Displays a response from the master OAW-IAP to the beacon request of the slave OAW-IAP.

Parameter	Description
`election wait`	Displays the shortest waiting time of an OAW-IAP between one Virtual Controller going down and the new Virtual Controller becoming active.
`timer slow`	Indicates that the OAW-IAP has waited longer than expected, and that the timer slow is caused by a CPU overload.
`master high cpu`	Indicates the CPU usage of the master OAW-IAP. The allowed limit is 85.
`ap cpu usage`	Indicates the CPU usage of the existing OAW-IAP.
`Slave->Pot-Master`	Displays a count of transitions from slave to pot-master state.
`Pot-master->Master`	Displays a count of transitions from pot master to master state.
`Pot-master->Slave`	Displays a count of transitions from pot master to slave state.
`last spoof arp rcvd`	Displays the last detected ARP spoof attack.
`last spoof mac`	Displays the MAC address of the last spoof detected.
`last beacon received ticks`	Displays the last tick time of the received beacon.
`uplink flap count`	Displays the count of the uplink flap.
`max beacon miss ticks`	Displays the maximum time between the current beacon and last beacon.
`hierarchy mode`	Indicates that the OAW-IAP is in hierarchy mode.
`last hierarchy beacon received ticks`	Displays the time between the current hierarchy beacon and last hierarchy beacon.
`provisioned master denied`	Indicates that the preferred OAW-IAP has been denied as a master.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode	
All platforms	Privileged EXEC mode	

show esl-radio

```
show esl-radio [status [<name>]]
```

Description

This command displays the status of Electronic Shelf Label Radio (USB dongle) traffic.

Example

The following example shows the output of **show esl-radio status** command:

```
SES ESL-Radio Status
--------------------
NAME                   MAC                 ESL-Radio Status    ESL-Radio Device ID
----                   ---                 ----------------     ------------------
325-test           f0:5c:19:c9:fa:ea        Plugged                0x10c4ea60
b4:5d:50:c5:46:80  b4:5d:50:c5:46:80        Plugged                0x10c4ea60
b4:5d:50:c5:46:46  b4:5d:50:c5:46:46        Not Plugged
```

The output of this command provides the following information:

Column	Description
NAME	Displays the OAW-IAP device name.
MAC	Displays the OAW-IAP's MAC address.
ESL-Radio Status	Shows if the USB dongle is plugged to the OAW-IAP.
ESL-Radio Device ID	Shows the USB dongle's device ID.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP303H, OAW-IAP304, OAW-IAP305, OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-IAP334, OAW-IAP335, OAW-AP-344, OAW-AP-345, OAW-AP514, and OAW-AP515	Privileged EXEC mode

show esl

```
show esl {status}
```

Description

This command displays the status of SES-imagotag's Electronic Shelf Label configuration for an OAW-IAP.

Example

The following example shows the output of **show esl status** command:

```
ESL Status
----------
Item           Value
----           -----
ESL Server     10.65.39.210
ESL Channel    8
CONFIG State   CONFIG-UPDATE-END
```

The output of this command provides the following information:

Column	Description
`ESL Server`	Displays the IP address of the ESL server.
`ESL Channel`	Displays the ESL radio channel.
`CONFIG State`	Displays the configuration status of the specified ESL profile.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
OAW-AP303H, OAW-IAP304, OAW-IAP305, OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-IAP334, OAW-IAP335, OAW-AP-344, OAW-AP-345, OAW-AP514, and OAW-AP515	Privileged EXEC mode

show est status

```
show est status
```

Description

Displays the information of the activated EST profiles along with the current status of the EST information on the device.

Example

The output of this command shows the current EST status of a single OAW-IAP:

```
(Instant AP)# show est status
EST STATUS
----------
Profile Name        : ssetty26_new
Server Host         : 10.20.21.26
Server Port         : 8443
Enrollment status   : Re-enrolled
Arbitrary label enrollment : /ca:7
Arbitrary label reenrollment : /ca:7
Expiry status       : EXPIRING SOON
Valid from          : 2020-03-01 06:02:30
Valid till          : 2020-03-02 06:02:30
Re-enrollment due   : 2020-03-02 00:02:30
```

Related Commands

Platforms	Licensing
est profile	This command configures an EST profile on the OAW-IAP.
est-activate	This command is used to activate an existing EST profile on the OAW-IAP.

Command History

Version	Description
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Enable mode on Mobility Master.

show external-captive-portal

```
show external-captive-portal [<name>]
```

Description

This command displays the external captive portal configuration details.

Parameter	Description	Range	Default
`name`	Filters the output based on an existing external captive portal profile.	—	—

Example

The following output is displayed for the **show external-captive-portal** command:

```
External Captive Portal
-----------------------
Name     Server     Port  Url  Auth Text      Redirect Url  Server Fail Through
----     ------     ----  ---  ---------      ------------  -------------------
default  localhost  80    /    Authenticated                Disable
Samuel   localhost  80    /    Authenticated                Disable
test     localhost  80    /    Authenticated                Disable

Disable Auto Whitelist  Use HTTPs  Server Offload
----------------------  ---------  --------------
Enable                  Yes        No
Disable                 No         No
Disable                 No         No

Prevent Frame Overlay  In Use  Redirect Mode
---------------------  ------  -------------
Disable                No      Yes
Disable                No      No
Disable                No      No
```

The output of this command displays details such as the external captive portal profile name, server name, server port, redirection URL, and automatic whitelisting status.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show facebook

```
show facebook
```

Description

This command displays the Facebook configuration details when an OAW-IAP successfully registers with Facebook.

Example

The following example shows the output of **show facebook** command:

```
Facebook Id     :461857943969928
Config Url      :https://www.facebook.com/wifiauth/config?gw_id=461857943969928
```

The output of this command displays the Facebook ID and the configuration URL if the OAW-IAP registration with Facebook is successful.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show fault

```
show fault [history]
```

Description

This command displays the list of active faults that occur in the event of a system fault and the faults that were cleared from the system.

Parameter	Description
`history`	Displays the list of faults that were cleared.

Example

The following example shows the output for the **show fault** command:

```
Active Faults
-------------
Time  Number  Description
----  ------  -----------
Total number of entries in the queue    :0
```

The following example shows the output for the **show fault history** command:

```
Cleared Faults
--------------
Time  Number  Cleared By  Description
----  ------  ----------  -----------
Total number of entries in the queue    :0
```

The output of these commands provide the following information:

Parameter	Description
`Timestamp`	Displays the system time at which an event occurs.
`Number`	Indicates the sequence
`Cleared By`	Displays the module which cleared this fault.
`Description`	Provides a short description of the event details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show firewall

```
show firewall
```

Description

This command displays the firewall configuration details of an OAW-IAP.

Example

The following example shows the output of **show firewall** command:

```
Firewall
--------
Type                 Value
----                 -----
Auto topology rules  disable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show flow-offload status

```
show flow-offload status
```

Description

This command displays the current status of flow offload configuration of the OAW-IAP.

Example

The following example displays the flow offload status of the OAW-IAP:

```
(Instant AP)#show flow-offload
Flow offload is enabled
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP535 and OAW-AP555 access points	Privileged EXEC mode

show g-max-clients

```
show g-max-clients [<ssid_profile>]
```

Description

This command displays the maximum number of clients allowed for an SSID profile on a 2.4 GHz radio channel.

Parameter	Description	Range	Default
`<ssid_profile>`	Denotes the SSID profile for which the maximum clients limit is set.	—	—

Example

The following **show g-max-clients** command output displays the maximum number of clients allowed to connect to the each SSID:

```
(Instant AP)# show g-max-clients
test1 : 77
test2 : 200
test3 : 64
```

The following **show g-max-clients <ssid_profile>** command output displays the maximum number of clients allowed to connect to the **test1** SSID:

```
(Instant AP)# show g-max-clients test1
g-max-clients: 77
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All Platforms	Privileged EXEC mode

show ids

```
show ids {ap <mac>| aps| client <mac>|clients| phy-types| rap-types| rogue-ap <mac>}
```

Description

This command displays the list of unknown APs and clients detected by the OAW-IAP with the Intrusion Detection System (IDS) feature enabled.

Parameter	Description	Range	Default
`ap <mac>`	Displays the signal details for the OAW-IAP.	—	—
`aps`	Displays the unknown Access Points detected by the OAW-IAP.	—	—
`client <mac>`	Displays a details of the OAW-IAP to which the client is connected.	—	—
`clients`	Displays a list of unknown clients detected by the OAW-IAP.	—	—
`phy-types`	Displays the PHY details of the OAW-IAP.	—	—
`rap-types`	Displays a list of Remote APs (OAW-RAPs) detected by the OAW-IAP.	—	—
`rogue-ap <mac>`	Displays the list of rogue OAW-IAPs detected by the master OAW-IAP in the OAW-IAP cluster.	—	—

Examples

The following output is displayed for the **show ids aps** command:

```
Unknown Access Points Detected
------------------------------
MAC Address Network Classification Chan. Type Last Seen
----------- ------- -------------- ----- ---- ---------
6c:f3:7f:56:6d:01 NTT-SPOT Interfering 1 G 17:32:19
6c:f3:7f:56:67:41 NTT-SPOT Interfering 1 G 17:37:49
00:24:6c:2a:78:d2 edward-suiteb-178 Interfering 11 GN 20MZ 17:37:19
6c:f3:7f:94:63:30 avyas_vap1 Interfering 6 G 17:40:20
6c:f3:7f:94:63:02 avyas_vap2 Interfering 6 G 17:40:20
00:24:6c:2a:7d:0b edward-suiteb Interfering 149 AN 40MZ 17:39:19
6c:f3:7f:a5:df:34 sw-san-rapng-nat Interfering 153 AN 20MZ 17:38:49
6c:f3:7f:56:7d:00 7SPOT Interfering 1 GN 20MZ 17:32:19
00:24:6c:80:8e:82 instant Interfering 11 GN 20MZ 17:29:48
00:1a:1e:40:06:00 test123 Interfering 11 G 17:37:49
00:24:6c:2a:78:d3 ssid_edward_psk_178 Interfering 11 GN 20MZ 17:37:49
6c:f3:7f:94:63:31 avyas_vap2 Interfering 6 G 17:40:20
6c:f3:7f:b5:bd:22 iClarice2 Interfering 6 GN 20MZ 17:39:19
6c:f3:7f:94:63:03 avyas_vap1 Interfering 6 G 17:40:20
00:24:6c:2a:7d:0c edward_tls2k Interfering 149 AN 40MZ 17:39:19
6c:f3:7f:a5:df:35 sw-san-native Interfering 153 AN 20MZ 17:38:49
00:24:6c:80:4f:88 ethersphere-wpa2 Interfering 52 AN 40MZ 17:40:20
```

The **show ids aps** command output provides information on the MAC address of interfering OAW-IAPs, the network to which the unknown OAW-IAPs are connected, the interference classification, channels on which the unknown APs are detected, the radio configuration type and recent timestamp of the interference.

The following output is displayed for the **show ids clients** command:

```
Unknown Clients Detected
------------------------
MAC Address        Network           Classification  Chan.  Type     Last Seen
```

```
-----------        -------          --------------  -----  ----     ---------
00:26:c6:4d:2b:74  ethersphere-wpa2  Interfering     1      GN 20MZ  17:26:48
00:24:d7:40:a8:64  akvoice1          Interfering     6      G        17:38:49
00:24:d7:40:ca:88  akvoice1          Interfering     6      G        17:39:50
74:e5:43:4b:3b:ff  manju34-vap1      Interfering     44     AN 40MZ  17:39:50
```

The **show ids clients** command output provides information on the MAC address of interfering clients, the network to which the unknown clients are connected, the interference classification, channels on which the unknown clients are detected, the radio configuration type and recent timestamp of the interference.

The following output is displayed for the **show ids phy-types** command:

```
Physical Types
--------------
Keyword  Value
-------  -----
b        0
a        1
g        2
ag       3
```

The following output is displayed for the **show ids rap-types** command:

```
RAP Types
---------
Keyword            Value
-------            -----
valid              0
interfering        1
rogue              2
dos-attack         3
unknown            4
known-interfering  5
suspect-rogue      6
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ids-detection config

```
show ids-detection config
```

Description

This command displays the list of intrusion detection policies configured on an OAW-IAP.

Example

The following output is displayed for the **show ids-detection** command:

```
infrastructure detection level        :off
---------------------------------------------------
Policies                           Status   Low      Medium   High
--------                           ------   ---      ------   ----
detect-ap-spoofing                 disable  enable   enable   enable
detect-windows-bridge              disable  enable   enable   enable
signature-deauth-broadcast         disable  enable   enable   enable
signature-deassociation-broadcast  disable  enable   enable   enable
detect-adhoc-using-valid-ssid      enable   disable  enable   enable
detect-malformed-large-duration    enable   disable  enable   enable
detect-ap-impersonation            enable   disable  disable  enable
detect-adhoc-network               enable   disable  disable  enable
detect-valid-ssid-misuse           enable   disable  disable  enable
detect-wireless-bridge             disable  disable  disable  enable
detect-ht-40mhz-intolerance        disable  disable  disable  enable
detect-ht-greenfield               disable  disable  disable  enable
detect-ap-flood                    disable  disable  disable  enable
detect-client-flood                disable  disable  disable  enable
detect-bad-wep                     disable  disable  disable  enable
detect-cts-rate-anomaly            disable  disable  disable  enable
detect-rts-rate-anomaly            disable  disable  disable  enable
detect-invalid-addresscombination  disable  disable  disable  enable
detect-malformed-htie              disable  disable  disable  enable
detect-malformed-assoc-req         disable  disable  disable  enable
detect-malformed-frame-auth        disable  disable  disable  enable
detect-overflow-ie                 disable  disable  disable  enable
detect-overflow-eapol-key          disable  disable  disable  enable
detect-beacon-wrong-channel        disable  disable  disable  enable
detect-invalid-mac-oui             disable  disable  disable  enable
client detection level        :off
---------------------------------------------------
Policies                           Status   Low      Medium   High
--------                           ------   ---      ------   ----
detect-valid-clientmisassociation  disable  enable   enable   enable
detect-disconnect-sta              disable  disable  enable   enable
detect-omerta-attack               disable  disable  enable   enable
detect-fatajack                    disable  disable  enable   enable
detect-block-ack-attack            disable  disable  enable   enable
detect-hotspotter-attack           disable  disable  enable   enable
detect-unencrypted-valid           disable  disable  enable   enable
detect-power-save-dos-attack       disable  disable  enable   enable
detect-eap-rate-anomaly            disable  disable  disable  enable
detect-rate-anomalies              disable  disable  disable  enable
detect-chopchop-attack             disable  disable  disable  enable
detect-tkip-replay-attack          disable  disable  disable  enable
signature-airjack                  disable  disable  disable  enable
signature-asleap                   disable  disable  disable  enable
```

The output for this command provides the following information:

Parameter	Description	Range	Default
`Infrastructure detection level`	Indicates if the detection level for the policies is set to off, low, medium, or high.	—	—
`Policies`	Displays the list of intrusion detection policies.	—	—
`Status`	Indicates if a policy is enabled or disabled.	—	—
`Low`	Indicates if the detection level for a policy is set to low.	—	—
`Medium`	Indicates if the detection level for a policy is set to medium.	—	—
`High`	Indicates if the detection level for a policy is set to high.	—	—

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ids-protection config

```
show ids-protection config
```

Description

This command displays the list of infrastructure protection policies for an OAW-IAP.

Examples

The following output is displayed for the **show ids-protection config** command:

```
Wireless Containment                       :none
Wired Containment                          :off
infrastructure protection level            :off
---------------------------------------------------
Policies                  Status   Low      High
--------                  ------   ---      ----
protect-ssid              disable  enable   enable
rogue-containment         disable  enable   enable
protect-adhoc-network     disable  disable  enable
protect-ap-impersonation  disable  disable  enable
client protection level                    :off
---------------------------------------------------
Policies                Status   Low      High
--------                ------   ---      ----
protect-valid-sta       disable  enable   enable
protect-windows-bridge  disable  disable  enable
```

Parameter	Description
`Infrastructure protection level`	Indicates if the protection level for the policies is set to off, low, medium, or high.
`Policies`	Displays the list of wired and wireless network infrastructure protection policies.
`Status`	Indicates if a policy is enabled or disabled.
`Low`	Indicates if the protection level for a policy is set to low.
`Medium`	Indicates if the protection level for a policy is set to medium.
`High`	Indicates if the protection level for a policy is set to high.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show gre config

```
show gre config
```

Description

This command displays the the GRE configuration information for an OAW-IAP.

Example

The following example shows the output of **show gre-config** command:

```
GRE Primary Server           :pgre.arubanetworks.com
GRE Primary IP               :2000:172:16:168::1
GRE Backup Server            :sgre.arubanetworks.com
GRE Backup IP                :2000:172:16:168::2
GRE Type                     :25944 (0x6558)
GRE Per AP Tunnel            :disable
GRE Preemption               :enable
GRE Holdon Time              :60 (secs)
GRE Failover type            :ping
GRE Ping Interval            :10 (secs)
GRE Allowed Inactive Time    :10 (secs)
GRE Ping Retry Count         :3
GRE Reconnect User On Failover :enable
GRE Reconnect Time On Failover :60 (secs)
```

The output of this command provides the following information:

Parameter	Description
`GRE Primary Server`	Displays the primary GRE Server information.
`GRE Primary IP`	Displays the primary GRE IP address.
`GRE Backup Server`	Displays the backup GRE Server information.
`GRE Backup IP`	Displays the backup GRE IP address.
`GRE Type`	Displays the GRE type.
`GRE Per AP Tunnel`	Denotes if the per-ap tunnel is enabled or disabled.
`GRE Preemption`	Denotes if the preemption is enabled or disabled.
`GRE Holdon Time`	Denotes the hold down time (in seconds) before which the GRE tunnel recovers from the backup to the primary tunnel.
`GRE Failover type`	Displays the GRE failover type.
`GRE Ping Interval`	Displays the ping interval configured.
`GRE Allowed Inactive Time`	Displays the time for tunnel inactivity check.
`GRE Ping Retry Count`	Displays the ping count for bringing the tunnel DOWN.
`GRE Reconnect User On Failover`	Displays the time (in seconds) after which the user will try to reconnect.
`GRE Reconnect Time On Failover`	Denotes if the reconnect user on tunnel failover is enabled or disabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show gre status

```
show gre status
```

Description

This command displays the various parameters indicating the status of GRE.

Example

The following example shows the output of **show gre status** command:

```
GRE Tunnel Status
-----------------
Active Tunnel            : Primary (2000:172:16:168::1) created at 2018-11-08 12:39:21
Uptime of the Tunnel     :34 days 4 hours 48 minutes 53 seconds
GRE Tunnel status        :Up
Next inactivity check    :0 (sec)
Total Ping sent          :0
Total Ping missed        :0
Next Ping packet after   :8 (secs)
Expired Hold on Time     :0 (sec)
```

The output of this command provides the following information:

Parameter	Description
`Active Tunnel`	Displays the current tunnel with its creation date and time.
`Uptime of the Tunnel`	Displays the uptime of the current tunnel.
`GRE Tunnel status`	Denotes if the tunnel is up or down.
`Next inactivity check`	Displays the counter for tunnel inactivity check, which indicates when to start another counter for next ping to send. If there is no reply, its value is 0; if there is reply, its value is 10. This starts from 10 and decreases to 0. When the value is 0, the counter **Next Ping packet after** starts to decrease from 10 to 0.
`Total Ping sent`	Denotes the ping packets sent.
`Total Ping missed`	Denotes the number of ping packets missed out of ping packets sent.
`Next Ping packet after`	Displays the counter for the next ping packet. By default the value is set to 10, and will start decreasing when **Next inactivity check** is equal to 0. When the value for the **Next Ping packet after** is 0, the value of Total Ping sent is incremented.
`Expired Hold on Time`	Displays the counter for hold on time check. This is 0 if current endpoint is primary. If endpoint is backup, the value starts increasing. When it reaches its upper limit, the ping to primary is done and accordingly the tunnel endpoint is changed.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show image

```
show image version
```

Description

This command displays the AOS-W Instant software version running on an OAW-IAP.

Example

The following example shows the output of **show image version** command:

```
Primary Partition                 :0
Primary Partition Build Time      :2018-07-15 14:28:33 PDT
Primary Partition Build Version   :8.4.0.0_65801 (Digitally Signed - Production       Build)
Backup Partition                  :1
Backup Partition Build Time       :2018-07-9 05:24:22 PDT
Backup Partition Build Version    :8.4.0.0_65715 (Digitally Signed - Production       Build)
AP Images Classes
-----------------
Class
-----
Aries
Centaurus
Ursa
Vela
Lupus
Hercules
```

Parameter	Description
`Primary Partition Build Time`	Shows the OAW-IAP image build time.
`Primary Partition Build Version`	Shows the OAW-IAP build version.
`AP Image Class`	Indicates the OAW-IAP class. The following examples describe the image class for different OAW-IAP models: ■ For OAW-RAP155/155P—AlcatelInstant_Aries_<build-version> ■ For all other OAW-IAPs—AlcatelInstant_Orion_<build-version>

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show inbound-firewall-rules

```
show inbound-firewall-rules
```

Description

This command displays the details of inbound firewall rules configured on an OAW-IAP.

Example

The following output is displayed for the **show inbound-firewall-rules** command:

```
Access Rules
------------
Src IP  Src Mask  Dest IP    Dest Mask      Dest Match  Protocol (id:sport:eport)
Application  Action  Log  TOS  802.1P  Blacklist  App Throttle (Up:Down)  Mirror  DisScan
ClassifyMedia
------  --------  -------    ---------      ----------  -------------------------  ----------
-  ------  ---  ---  ------  ---------  ----------------------  ------  --------  ------------
-
any     any       any        any            match       h323-tcp
  permit
any     any       192.0.2.0  255.255.255.0  match       h323-udp
  permit
```

The output of this command displays information about the inbound firewall access rule configuration parameters, which indicate whether a particular type of traffic is to allowed to a particular destination from the source subnet, and the service and protocol in use. It also indicates if other options such as logging and prioritizing traffic are enabled when the rule is triggered.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show interface counters

```
show interface counters
```

Description

This command shows the Ethernet interface packet counters for the OAW-IAP.

Example

The following example shows the partial output of **show interface counters** command:

```
bond0 is up, line protocol is up
Hardware is Gigabit Ethernet, address is d8:c7:c8:c4:42:98
Speed 1000Mb/s, duplex full
Received packets                  9441
Received bytes                    1134064
Receive dropped                   0
Receive errors                    0
Receive missed errors             0
Receive overrun errors            0
Receive frame errors              0
Receive CRC errors                0
Receive length errors             0
Transmitted packets               16435
Transmitted bytes                 841278
Transmitted dropped               0
Transmission errors               0
Lost carrier                      0
```

Parameter	Description
`Speed`	Shows speed of the Ethernet interface.
`Received packets`	Shows total number of received packets.
`Received bytes`	Shows the total number of received bytes.
`Receive dropped`	Shows total number of packets dropped.
`Receive errors`	Shows total number of errors during packet receive.
`Receive missed errors`	Shows total number of errors missed during packet receive.
`Receive overrun errors`	Shows total number of received overrun errors.
`Receive frame errors`	Shows total number of frame errors during packet receive.
`Receive CRC errors`	Shows total number of CRC errors during packet receive.
`Receive length errors`	Shows total length of the error.
`Transmitted packets`	Shows total number of transmitted packets.
`Transmitted bytes`	Shows total number of transmitted bytes.
`Transmitted dropped`	Shows total number of packets dropped.
`Transmission errors`	Shows total number of errors during packet transmit.
`Lost carrier`	Shows total number of lost carriers.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show iot radio-profile

```
show iot radio-profile [<profile-name>]
```

Description

This command displays the IoT radio profile status information.

Example

The following example shows the output of **show iot radio-profile** command:

```
IoT Radio Profile List
----------------------
Name  References  Instance  Mode
----  ----------  --------  ----
test  0           internal  none
------------
Total:1
```

The following example shows the output of **show iot radio-profile <profile_name>** command:

```
(Instant AP)#  show iot radio-profile test3
IoT Radio Profile List
----------------------
Name  References  Instance  Mode
----  ----------  --------  ----
test  0           internal  none
------------
Total:1
90:4c:81:c3:28:1e# show iot radio-profile test
Name                :test
References          :0
Instance            :internal
Mode                :none
BLE Opmode          :scanning beaconing
BLE Console         :
BLE TxPower (dBm)   :0
Zigbee Mode         :coordinator
Zigbee Channel(s)   :auto
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show iot transportProfile

```
show iot transportProfile [<profile-name>]
```

Description

This command displays the IoT profile status information.

Example

The following example shows the output of **show iot transportProfile** command:

```
Default Meridian Profile for BLE
---------------------
Endpoints                                References
----                                     ----------
Beacon-Management                        0
Asset-Tracking-WSS                       0
Asset-Tracking-HTTPS                     0
=========================================
IoT Data Profile List
---------------------
Name                                     References           EndpointType
----                                     ----------           ------------
test10                                   1                    Meridian-Asset-Tracking
test3                                    1                    ZF
test2                                    1                    Meridian-Beacon-Management
Total:3
xg_test# show iot transportProfile test3
IoT Data Profile "test3"
---------------------
Parameter                  Value
---------                  ------
Name                       :test
EndpointURL                :https://app.detagtive.com
EndpointType               :Meridian-Beacon-Management
PayloadContent             :aruba-sensors
TransportInterval          :600
EndpointToken              :N/A
EndpointID                 :N/A
Username                   :samuelrichard@gmail.com
Password                   :It2GbjTXFAYEpHg43VOK2_2KrWePwmVPKwSHBTEj-jM
UUIDFilter                 :N/A
CellSizeFilter             :N/A
MovementFilter             :N/A
AgeFilter                  :N/A
AuthenticationURL          :N/A
UIDNamespaceFilter         :N/A
URLFilter                  :N/A
VendorFilter               :N/A
RSSIReporting              :average
EnvironmentType            :office
CustomFadingFactor         :20
AccessID                   :N/A
ProxyServer                :10.65.18.29:8087
ProxyPort                  :N/A
ProxyUsername              :N/A
ProxyPassword              :a2328td
VLAN                       :none
rtlsDestMAC                :a3:3d:cc:44:5e:78
deviceCountOnly            :TRUE
ZSDFilter                  :N/A
```

```
DataFilter                  :N/A
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The following parameters were included in the output: ■ **ZSDFilter** ■ **DataFilter** The following payload content were included in the output: ■ **wiliot** ■ **exposure-notification**
OAW-IAP 8.6.0..0	The **Proxy Server**, **Vendor Filter** configuration information was included in the output.
AOS-W Instant 8.5.0.0	The **aruba-sensors** sub-parameter is introduced under the **payloadContent** parameter.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ip dhcp database

```
show ip dhcp database
```

Description

This command displays the DHCP server settings. The DHCP server is a built-in server, used for networks in which clients are assigned IP addresses by the Virtual Controller.

Example

The following output is displayed for the **show ip dhcp database** command:

```
DHCP Subnet          :192.0.2.0
DHCP Netmask         :255.255.255.0
DHCP Domain Name     :example.com
DHCP DNS Server      :192.0.2.1
DHCP DNS Cache       :Disabled
```

The output of this command provides the following information:

Column	Description
`DHCP subnet`	Indicates the network range for the client IP addresses.
`DHCP Netmask`	Indicates the subnet mask specified for the IP address range for the DHCP subnet.
`DHCP Lease Time(m)`	Indicates the duration of DHCP lease. The lease time refers to the duration of lease that a DHCP-enabled client has obtained for an IP address from a DHCP server.
`DHCP Domain Name`	Indicates the domain-name of the DHCP client.
`DHCP DNS Server`	Indicates the IP address of the DNS server.
`DHCP DNS Cache`	Indicates if the DNS cache is enabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ip igmp

```
show ip igmp group [maddr <multicast-addr>]
```

Description

This command displays information about the IGMP group table for an OAW-IAP.

Parameter	Description
`maddr <multicast-addr>`	Filters group table information based on the multicast IP address.

Example

The following output is displayed for the **show ip igmp group** command:

```
IGMP Group Table
----------------
Group            Members        vlan
239.255.255.250  1               333
224.0.0.251      1               333
224.0.0.252      1               333
```

The following output is displayed for the **show ip igmp group maddr <multicast-addr>** command:

```
IGMP Group 224.0.0.251 Table
--------------------------------
Member           Mac               Vlan    Destination       Age
------           ---               ----    -----------       ---
10.17.88.226     08:ed:b9:e1:51:7d 333     aruba002          15
```

The output of this command includes the following parameters:

Parameter	Description
`IGMP Group Table`	Displays details for the IGMP multicast group.
`Group`	Indicates the IP addresses for the multicast group.
`Members`	Indicates the number of members assigned to the multicast group.
`VLAN`	Indicates the VLAN ID associated with the multicast group.
`IGMP Group <multicast-address> Table`	Displays the IGMP details specific to a multicast address.
`Member`	Indicates the IP address of the member associated with the specified multicast group address.
`MAC`	Indicates the MAC address of member associated with the specified multicast group address.
`VLAN`	Indicates the VLAN ID associated with the multicast groups or a specific multicast group address.
`Destination`	Indicates the destination to which the multicast packets are routed.
`Age`	Indicates the aging time of the forwarding table entries.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ip interface

```
show ip interface
   brief
   detail
```

Description

This command displays a summary of IP related information for all interfaces configured on an OAW-IAP.

Usage Guidelines

Use this command to view a brief summary of IP related information for the OAW-IAP interfaces.

Example

The following output is displayed for the **show ip interface brief** command:

```
Interface                    IP Address / IP Netmask          Admin    Protocol
br0                          10.17.88.188 / 255.255.255.192   up       up
```

The output of the **show ip interface brief** command provides the following information:

Column	Description
`Interface`	Lists the interface and interface identification, where applicable.
`IP Address /IP Netmask`	Lists the IP address and subnet mask for the interface.
`Admin`	Displays the administrative status of the interface. ■ Enabled—up ■ Disabled—down
`Protocol`	Displays the status of the IP on the interface. ■ Enabled—up ■ Disabled—down

The following output is displayed for the **show ip interface detail** command:

```
ifname : br0
--------------------
ifindex         : 10
vlan-id         : 1
vlan-type       : mgmt
primary IP type : dhcp
IP              : 10.17.196.130/32 dev br0
IP              : 10.17.196.141/28 dev br0
ifname : br0.3333
--------------------
ifindex         : 16
vlan-id         : 3333
vlan-type       : magic
primary IP type : static
IP              : 172.31.98.1/23 dev br0.3333
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **detail** parameter introduced.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ip route

```
show ip route
```

Description

This command displays the OAW-IAP routing table.

Examples

The following output shows the ip address of routers and the VLANs to which they are connected.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS  Window   irtt Iface
172.16.10.1     0.0.0.0         255.255.255.255 UH        0  0           0 tun0
10.17.88.128    0.0.0.0         255.255.255.192 U         0  0           0 br0
2.2.2.0         0.0.0.0         255.255.255.0   U         0  0           0 br0
192.168.10.0    0.0.0.0         255.255.254.0   U         0  0           0 br0
0.0.0.0         10.17.88.129    0.0.0.0         UG        0  0           0 br0
```

The output of this command provides the following information:

Column	Description
`Destination`	Displays the destination IP address for the IP routes.
`Gateway`	Displays the gateway IP address for the IP routes.
`Genmask`	Displays the subnet mask details for the IP routes.
`Flags`	Indicates if the route is up, targeted to the host , or if it uses Gateway.
`MSS`	Indicates the default MSS for TCP connections over this route.
`Window`	Indicates the default window size for TCP connections over this route.
`irrt`	Indicates the initial RTT. The kernel uses this to determine the best TCP protocol parameters instead of relying on slow responses.
`Iface`	Indicates the Interface to which packets are routed.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ipv6 interface

```
show ipv6 interface {brief|details}
```

Description

Shows IPv6-related information for all interfaces on the OAW-IAP.

Parameter	Description
`brief`	Displays a brief summary of the IPv6-related information on all interfaces of an OAW-IAP.
`details`	Displays detailed information on the interfaces that support IPv6.

Example

The following example shows the output of the **show ipv6 interface brief** command:

```
IPv6 is enable, link-local address is fe80::aea3:1eff:fecd:471a/64
br0 is up, line protocol is up
Global unicast address(es):
2001:470:36:5c3:aea3:1eff:fecd:471a/64, subnet is 2001:470:36:5c3::/64
2001:470:36:5c3:ffff:ffff:ffff:1001/128, subnet is 2001:470:36:5c3:ffff:ffff:ffff:1001/128
2001:470:36:5c3:ffff:ffff:ffff:5b/64, subnet is 2001:470:36:5c3::/64
```

The following example shows the output of the **show ipv6 interface details** command:

```
1: lo: <LOOPBACK,UP,10000> mtu 16436
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
15: br0: <BROADCAST,MULTICAST,UP,10200> mtu 1300 qlen 1000
inet6 2001:470:36:5c3:ffff:ffff:ffff:5b/64 scope global
valid_lft forever preferred_lft forever
inet6 2001:470:36:5c3:aea3:1eff:fecd:471a/64 scope global dynamic
valid_lft 2963sec preferred_lft 1963sec
inet6 2001:470:36:5c3:ffff:ffff:ffff:1001/128 scope global
valid_lft forever preferred_lft forever
inet6 fe80::aea3:1eff:fecd:471a/64 scope link
valid_lft forever preferred_lft forever
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platform	Command Mode
OAW-IAP214/215, OAW-IAP224/225, OAW-IAP274/275, OAW-IAP314/315, OAW-APAP-324/325, OAW-IAP334/335	Privileged EXEC mode

show ipv6 route

```
show ipv6 route
```

Description

This command displays the IPv6 routing table.

Usage Guidelines

Use this command to view the static IPv6 routes configured on the OAW-IAP.

Examples

The following example shows the output of the **show ipv6 route** command:

Kernel IPv6 routing table

```
Destination                                 Next Hop                     Flags Metric
-----------                                 --------                     ----- ------
2001:470:36:5c3:ffff:ffff:ffff:1001/128     ::                           U     256
2001:470:36:5c3::/64                        ::                           UA    256
fe80::/64                                   ::                           U     256
::/0                                        fe80::6273:5cff:fe65:ee19    UGDA  1024
::1/128                                     ::                           U     0
2001:470:36:5c3:aea3:1eff:fecd:471a/128     ::                           U     0
2001:470:36:5c3:ffff:ffff:ffff:5b/128       ::                           U     0
2001:470:36:5c3:ffff:ffff:ffff:1001/128     ::                           U     0
fe80::aea3:1eff:fecd:471a/128               ::                           U     0
ff02::d/128                                 ff02::d                      UC    0
ff02::1:2/128                               ff02::1:2                    UC    0
ff00::/8                                    ::                           U     256
Ref    Use Iface
---    ---------
0        0 br0
0        0 br0
0        0 br0
0        0 br0
0        1 lo
0        1 lo
2800     1 lo
6        1 lo
6602     1 lo
12194    0 br0
2        0 br0
0        0 br0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.5.0.0-4.3.0.0	Command introduced.

Command Information

Platform	Command Mode
OAW-IAP214/215, OAW-IAP224/225, OAW-IAP274/275, OAW-IAP314/315, OAW-APAP-324/325, OAW-IAP334/335	Privileged EXEC mode

show lacp status

```
show lacp status
```

Description

This command displays the LACP configuration status on an OAW-IAP.

Use this command to view the LACP status on OAW-IAP224 or OAW-IAP225 devices. LACP provides a standardized means for exchanging information with partner systems to form a dynamic LAG. The LACP feature is automatically enabled during OAW-IAP boots and it dynamically detects the OAW-IAP if connected to a partner system with LACP capability, by checking if there is any LACP PDU received on either ethernet 0 or ethernet 1 port.

Example

The following example shows the output of the **show lacp status** command:

```
AP LACP Status
--------------
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----------  ---------  ---------  ---------  -----------  -----------
Up           slow       2          17         1            70:81:05:11:3e:80
Slave Interface Status
----------------------
Slave I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link Fail Count
--------------  ------------------  -----------  -------------  ---------------
eth0            6c:f3:7f:c6:76:6e   Up           Yes            0
eth1            6c:f3:7f:c6:76:6f   Up           Yes            0
Traffic Sent on Enet Ports
--------------------------
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count
---------  ---------------  ---------------
0          0                0
1          0                0
non-wifi   2                17
```

The output of this command displays details such as the link status, number of ports, OAW-IAP partner MAC address, and the interface status.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP 220 Series access points	Privileged EXEC mode

show l3-mobility

```
show l3-mobility {config| datapath| events [<count> <mac>]| status}
```

Description

This command displays details about the L3 events, mobility configuration, and roaming status of the OAW-IAP clients.

Parameter	Description
`config`	Displays the L3 mobility configuration details for an OAW-IAP.
`datapath`	Displays the datapath statistics associated with L3 mobility.
`events [<count> <mac>]`	Displays L3 mobility events for all OAW-IAP clients or individual clients filtered based on MAC address.
`status`	Displays the L3 mobility status for an OAW-IAP.

Examples

show l3-mobility config

The following example shows the output of the **show l3-mobility config** command:

```
Flags
-----
Type                         Value
----                         -----
Home Agent Load Balancing  enable
Virtual Controller Table
------------------------
Virtual Controller IP
---------------------
192.0.1.0
Subnet Table
------------
Subnet     Netmask          VLAN  Virtual Controller
------     -------          ----  ------------------
192.0.2.0  255.255.255.255  2     192.0.1.0
```

The output of this command provides the following information:

Column	Description
`Flags`	Indicates if any L3 mobility features are enabled.
`Type`	Indicates the type of the flag.
`Value`	Indicates if a flag is enabled.
`Virtual Controller IP`	Displays the Virtual Controller IP address. The Virtual Controller IP configuration for each OAW-IAP allows the clients to roam seamlessly among all the OAW-IAPs.
`Subnet`	Indicates the IP address for the mobility domain.
`Netmask`	Displays the subnet mask configuration details.

Column	Description
`VLAN`	Displays the VLAN ID configured for the mobility domain.
`Virtual Controller`	Displays the Virtual Controller configuration associated with the mobility domain.

show l3-mobility datapath

The following example shows the output of **show l3-mobility datapath** command:

```
L3 Mobility Datapath Home Table
-------------------------------
Client Index  Client MAC  Home Vlan  Destinaton Device Index
------------  ----------  ---------  -----------------------
L3 Mobility Datapath Foreign Table
----------------------------------
Client Index  Client MAC  Home Vlan  VAP Vlan  Destinaton Device Index  HAP IP  Virtual
Controller IP  Packets Forwarded
--------------  -----------------
L3 Mobility Datapath Tunnel Table
---------------------------------
Tunnel Device  Remote Protocol  Dest IP  Clients  Idle Time  Rx Packets  Tx Packets  Rx
Mcasts  Tx Mcasts  ARP Proxy Pkts  Tx Jumbo  MTU  Rx HB  Tx HB  MTU Reqs  MTU Resps  HB
Mismatch  IP Mismatch  Type  Vlan Translations
-------------  ---------------  -------  -------  ---------  ----------  ----------  --------
-  ---------  --------------  --------  ---  -----  -----  --------  ---------  -----------
-----------  ----  -----------------
```

The output of this command provides the following information:

Parameter	Description
`L3 Mobility Datapath Home Table`	Displays details such as client index, client MAC address, VLAN, destination device associated with the L3 mobility home subnet.
`L3 Mobility Datapath Foreign Table`	Displays details such as client index, client MAC address, VLAN, Destination device, home OAW-IAP IP address, Virtual Controller IP address and packet details associated with the L3 mobility foreign subnet.
`L3 Mobility Datapath Tunnel table`	Displays the following details about L3 mobility tunnel: ■ Tunnel - Indicates the tunnel interface. ■ Device - Displays the device ID. ■ Remote Protocol - Indicates the remote protocol used by the roaming clients. ■ Dest IP - Indicates the destination IP address to which the packets are routed. ■ Clients - Displays the list of clients ■ Idle Time - Displays the idle time ■ Rx Packets - Displays information about packets received. ■ Tx Packets - Displays information about packets transmitted. ■ Rx Mcasts - Displays information about multicast packets received. ■ Tx Mcasts - Displays information about multicast packets transmitted. ■ ARP Proxy Pkts - Displays information packets resolved to destination IP address by the proxy ARP. ■ Tx Jumbo MTU - Displays information about the MTU in

Parameter	Description
	jumbo frames. ■ Rx HB ■ Tx HB ■ MTU Reqs - Indicates the number of MTU requests sent. ■ MTU Resps - Indicates the number of MTU responses received. ■ HB Mismatch ■ IP Mismatch - Indicates IP address mismatch if any ■ Type ■ Vlan Translations - Displays details about VLAN translation.

show l3-mobility events

The following example shows the output of the **show l3-mobility events** command:

```
L3 Mobility Events
------------------
Time             Client MAC         Event                   IP            Dir

----             ----------         -----                   --            ----       May  9
23:26:29  08:ed:b9:e1:51:87  Station Offline         10.17.88.59   <-
May  9 23:26:29  08:ed:b9:e1:51:87  Potential Foreign Client10.17.88.59   <-

May  9 23:09:05  08:ed:b9:e1:51:87  This Client is Normal   10.17.88.59   ->

Peer IP  Home Vlan  VAP Vlan  Tunnel ID  Old AP IP  FAP IP  HAP IP  VC IP Additional Info
----     ----------  --------  -------  ---------  -------- -----    ----  ---------
self     -             1        -         -          -          -      -       -
self     -             -        -         -          -          -      -       -
self     -             1        -         -       10.17.88.59   -          l2-timed-
out,test
```

The output of this command provides the following information:

Parameter	Description
`Time`	Indicates the timestamp of the L3 mobility event.
`Client MAC`	Indicates the MAC address of the roaming clients.
`Event`	Provides a description of the mobility event.
`IP`	Indicates the IP address of the roaming client.
`Dir`	Indicates if the client has roamed in or out of the mobility subnet.
`Peer IP`	Displays the peer IP address, if any peer clients are configured.
`Home Vlan`	Displays the VLAN ID associated with the home subnet.
`VAP Vlan`	Displays the VLAN ID associated with the Virtual OAW-IAP.
`Tunnel ID`	Indicates the tunnel interface used for routing packets.
`Old AP IP`	Indicates the IP address of the OAW-IAP from which the client has roamed.
`FAP IP`	Indicates the IP address of the OAW-IAP in the foreign subnet.

Parameter	Description
`HAP IP`	Indicates the IP address of the OAW-IAP in the home subnet, to which the client is currently connected.
`VC IP`	Indicates the IP address of the Virtual Controller.
`Additional Info`	Displays additional information if any.

show l3-mobility status

The following example shows the output of the **show l3-mobility status** command:

```
Roaming Client Table
--------------------
Client MAC  Home Vlan  VAP Vlan  Tunnel ID  Status  Virtual Controller IP  Peer IP  Old AP IP
 Device Name
----------  ---------  --------  ---------  ------  ---------------------  -------  ---------
 -----------
Tunnel Table
------------
Peer IP  Local Tunnel ID  Remote Tunnel ID  Use Count  Type
-------  ---------------  ----------------  ---------  ----
Virtual Controller Table
------------------------
Virtual Controller IP  Type  HAP IP  Local Tunnel ID  Remote Tunnel ID
---------------------  ----  ------  ---------------  ----------------
192.0.1.0              C     -       -                -
```

The output of this command provides the following information:

Parameter	Description
`Roaming Client Table`	Displays details such as client MAC address, Home OAW-IAP and Virtual OAW-IAP VLAN, Tunnel ID, roaming status, Virtual Controller IP address, peer IP address, old IP address, and the name of the device.
`Tunnel Table`	Displays details such as peer IP address, local tunnel ID. remote tunnel ID, tunnel count, and the type of tunnel used for routing packets.
`Virtual Controller Table`	Displays details such as Virtual Controller IP address, type, Home OAW-IAP IP address, local tunnel ID, and remote tunnel ID.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ldap-servers

```
show radius-servers
```

Description

This command displays the LDAP servers configured for user authentication on the Virtual Controller.

Example

The following example shows the output of **show ldap-servers** command:

```
LDAP Servers
------------
Name     IP Address  Port  Timeout Retry Count Admin-DN          Admin Password
----     ----------  ----  ------- ----------- --------          --------------
Server1  192.0.2.5    389   5         3        admin-dn cn=admin  password123

Base-DN               Filter          Key-Attribute   In Use   Deadtime
-----                 ------          -------------   ------    ------
dc=example, dc=com  (objectclass=*)  sAMAccountName  No
```

The output of this command provides the following information:

Parameter	Description
`Name`	Displays the name of the LDAP authentication server.
`IP Address`	Displays the IP address of the LDAP server.
`Port`	Displays the authorization port number of the LDAP server.
`Timeout`	Displays a timeout value for the LDAP requests from the clients.
`Retry Count`	Displays number of times that the clients can attempt to connect to the server.
`Admin-DN`	Displays DN for the administrator.
`Admin Password`	Displays the password for LDAP administrator.
`Base-DN`	Displays a DN for the node which contains the entire user database.
`Filter`	Shows the filter to apply when searching for a user in the LDAP database.
`Key-Attribute`	Displays the attribute to use as a key when searching for the LDAP server. For Active Directory, the value is **sAMAccountName**
`In Use`	Indicates if the server is in use.
`Deadtime`	

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log ap-debug

```
show log ap-debug{count}
```

Description

This command shows the debug logs of an OAW-IAP. Logs related to servers in the output are tagged with the server label.

Example

The following example shows the output of **show log ap-debug** command:

```
(Instant AP)# show log ap-debug
Mar 30 13:51:58 awc[6211]: [activate] receive isc request
Mar 30 13:51:58 awc[6211]: [activate] tcp_connect: begin resolve 'device.arubanetworks.com'
Mar 30 13:51:58 awc[6211]: [activate] tcp_connect: 241: recv timeout set to 5
Mar 30 13:51:58 awc[6211]: [activate] tcp_connect: 248: send timeout set to 5
Mar 30 13:51:58 awc[6211]: [activate] awc_init_connection: 2901: connected to
device.arubanetworks.com:443
Mar 30 13:51:58 awc[6211]: [activate] awc_init_connection: 2991: Loading local CA
certificates
Mar 30 13:51:59 awc[6211]: [activate] verify_callback: 2800: preverify_ok:1, chain count:3.
Mar 30 13:51:59 awc[6211]: [activate] verify_peer_domain_name: 1518: Verifying peer domain
name device.arubanetworks.com
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Server labels were added to logs related to server for enhanced debugging.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log apifmgr

```
show log apifmgr <count>
```

Description

This command shows the log information for OAW-IAP interface manager.

Parameter	Description
`count`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log convert

```
show log convert
```

Description

This command shows image conversion details for the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log debug

```
show log debug{count}
```

Description

This command shows the OAW-IAP full log.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log papi-handler

```
show log papi-handler {count}
```

Description

This command shows the cluster security debugging logs.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log driver

```
show log driver <count>
```

Description

This command displays the status of drivers configured on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log kernel

```
show log kernel
```

Description

This command shows AP's kernel logs.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log l3-mobility

```
show log l3-mobility [<count>]
```

Description

This command displays the logs for Layer-3 mobility domains configured on an OAW-IAP.

Parameter	Description
<count>	Filters the log output based on the number specified.

Example

The following output is displayed for the **show log l3-mobility** command:

```
May  9 21:23:07: Potential Foreign Client Information: mac c4:85:08:de:06:d4 rcvd from self
vlan 0, 1 tid 255 oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info l2-timed-
out,test
May  9 01:43:22: Station Offline: mac 08:ed:b9:e1:51:87 rcvd from self vlan 0, 0 tid 255
oldapip 0.0.0.0 fapip 0.0.0.0 hapip 0.0.0.0 vcip 0.0.0.0 info
May  9 01:25:53: This Client is Normal: mac 08:ed:b9:e1:51:87 sent to self vlan 0, 1 tid 255
oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info
May  9 01:25:53: Too many retries: mac 08:ed:b9:e1:51:87 rcvd from self vlan 0, 1 tid 255
oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info
May  9 01:25:52: Potential Foreign Client Information: mac 08:ed:b9:e1:51:87 rcvd from self
vlan 0, 1 tid 255 oldapip 0.0.0.0 fapip 10.17.88.59 hapip 0.0.0.0 vcip 0.0.0.0 info l2-timed-
out,test
```

The output of this command provides the following information:

Content	Description
Timestamp	Indicates the timestamp of the L3 mobility event.
Client MAC	Indicates the MAC address of the roaming clients.
Event	Provides a description of the mobility event.
Home Vlan	Displays the VLAN ID associated with the home subnet.
VAP Vlan	Displays the VLAN ID associated with the Virtual OAW-IAP.
tid	Indicates the tunnel interface used for routing packets.
Old AP IP	Indicates the IP address of the OAW-IAP from which the client has roamed.
FAP IP	Indicates the IP address of the OAW-IAP in the foreign subnet.
HAP IP	Indicates the IP address of the OAW-IAP in the home subnet, to which the client is currently connected.
VC IP	Indicates the IP address of the Virtual Controller.
Additional Info	Displays additional information if any.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log network

```
show log network <count>
```

Description

This command shows network logs for the OAW-IAP.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log pppd

```
show log pppd <count>
```

Description

Shows the PPPd network connection details.

Parameter	Description
`<count>`	PPPd network count.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log provision

```
show log provision
```

Description

Displays logs related to provision update with Activate.

Parameter	Description	Range	Default
`provision`	Displays logs related to provision update with Activate.	—	—

Example

The following example displays the output of the **show log provision** command:

```
Time                      State        Type         Log Message
----                      -----        ----         -----------
Mon Aug 20 05:40:21 2018  UAP ADP      Warning      ADP info: Not CAP-only sku
Mon Aug 20 05:40:25 2018  DHCP Option  In progress  Performing DHCP discovery
Mon Aug 20 05:40:26 2018  DHCP Option  In progress  DHCP lease of 10.65.17.190 obtained,
lease time 43200 seconds
Mon Aug 20 05:41:25 2018  UAP ADP      Warning      ADP info: No rule in flash.
Mon Aug 20 05:41:26 2018  UAP ADP      Warning      ADP info: Reset the provision status for
new master.
Mon Aug 20 05:41:26 2018  Activate     In progress  Attempting provisioning via Activate
server: device.arubanetworks.com
Mon Aug 20 05:41:26 2018  UAP ADP      Warning      ADP info: First provision at first
beginning.
Mon Aug 20 05:41:26 2018  UAP ADP      Warning      ADP info: Send one first provision
request.
Mon Aug 20 05:41:28 2018  Activate     Debug        Sent challenge response to Activate
Server: device.arubanetworks.com
Mon Aug 20 05:41:38 2018  UAP ADP      Warning      ADP info: Activate Conversion of IAP to
CAP started
Mon Aug 20 05:41:38 2018  UAP ADP      Warning      ADP info: Explicit type of rule is
configured for the AP.
Mon Aug 20 05:41:38 2018  UAP ADP      Warning      ADP info: Provision rule from activate is
changed.
Mon Aug 20 05:41:38 2018  UAP ADP      Warning      ADP info: Retrieve the valid provision
rule.
Mon Aug 20 05:41:38 2018  UAP ADP      Warning      ADP info: handle_post_auth_provision:
7100: applying controller='10.65.17.230'
                                                    mode='CAP' keep_cap_controller='Yes'
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log rapper

```
show log rapper
```

Description

This command shows the details of VPN connection logs in detail.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log rapper-brief

```
show log rapper-brief
```

Description

This command provides brief information about IKE message transactions with the message and timestamp details.

Example

The following example shows the output of **show log rapper-brief** command.

```
2017-05-03 03:00:16 SEND: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 03:00:16 RECV: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 03:00:16 ESP: spi[868dd900] 10:17:140:252 << 10:17:140:226 udp-encap
2017-05-03 03:00:16 ESP: spi[497d2f00] 10:17:140:226 << 10:17:140:252 udp-encap
2017-05-03 04:41:09 SEND: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 04:41:09 RECV: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 04:41:09 ESP: spi[7dead700] 10:17:140:252 << 10:17:140:226 udp-encap
2017-05-03 04:41:09 ESP: spi[84fee200] 10:17:140:226 << 10:17:140:252 udp-encap
2017-05-03 06:22:02 SEND: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 06:22:02 RECV: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 06:22:02 ESP: spi[56b60c00] 10:17:140:252 << 10:17:140:226 udp-encap
2017-05-03 06:22:02 ESP: spi[e2920a00] 10:17:140:226 << 10:17:140:252 udp-encap
2017-05-03 08:02:55 SEND: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
2017-05-03 08:02:55 RECV: 70947477257fa7e3 : eaca9e0d1af43efb , np=46, EXHG: CREATE_CHILD_SA
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show log rapper-counter

```
show log rapper-counter
```

Description

This command displays information about the IKE message exchange, cookie, SPI, and error status for the IPsec SA creation, with timestamp details.

Example

The following example shows the output of **show log rapper-counter** command.

```
AP Mac: 18:64:72:c8:20:00
TIME PEER IP COOKIES SPI EXCH ERR
---- ------- ------- --- ---- ---
2017-05-02 06:49:38 | 10.17.140.252 | {6904164c4f81ce9d : e37903823fa5ca58} | {0x7a379000 :
0x4c966100} | IKE_AUTH |
SUCCESS
2017-05-02 08:30:31 | 10.17.140.252 | {6904164c4f81ce9d : e37903823fa5ca58} | {0xbbb7bb00 :
0xeeb51a00} | CREATE_CHILD_SA |
SUCCESS
2017-05-02 10:11:25 | 10.17.140.252 | {6904164c4f81ce9d : e37903823fa5ca58} | {0xcfeb3300 :
0xfb1f1400} | CREATE_CHILD_SA |
SUCCESS
2017-05-02 11:52:18 | 10.17.140.252 | {6904164c4f81ce9d : e37903823fa5ca58} | {0xb2dd5100 :
0x1dad7500} | CREATE_CHILD_SA |
SUCCESS
2017-05-02 13:33:11 | 10.17.140.252 | {8048813ca5b1eef9 : af50609e79ce0102} | {0x2e3d9b00 :
0x76928b00} | CREATE_CHILD_SA |
SUCCESS
2017-05-02 15:14:04 | 10.17.140.252 | {8048813ca5b1eef9 : af50609e79ce0102} | {0x6b0f4400 :
0x61f8bf00} | CREATE_CHILD_SA |
SUCCESS
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

show log sapd

```
show log sapd <count>
```

Description

This command shows the SAPd details.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log scd

```
show log scd [count]
```

Description

This command displays the status of the Serial Communication Daemon process.

Parameter	Description
`count`	Displays a count of the SCD requests.

Example

The following example displays the output of the **show log scd** command:

```
[5998]2018-05-24 07:21:21 ReplyBatch: packetLength= 1833, data.length= 1837, templateLength =
114, requestCount = 16!
[5998]2018-05-24 07:21:22 Received slot request = 353, replyStatus = 0!
[5998]2018-05-24 07:21:22 Received slot request = 354, replyStatus = 0!
[5998]2018-05-24 07:21:22 Got Alive-Ping message header.
[5998]2018-05-24 07:21:22 PacketMaxLength = 1160!
[5998]2018-05-24 07:21:22 Handling SYNC packet read
[5998]2018-05-24 07:21:22 Accepting SYNC packet
[5998]2018-05-24 07:21:22 Adding SYNC with slotId = 368!
[5998]2018-05-24 07:21:22 Adding SYNC with slotId = 369!
[5998]2018-05-24 07:21:22 Adding SYNC with slotId = 370!
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP303H, OAW-IAP304, OAW-IAP305, OAW-IAP314, OAW-IAP315, OAW-IAP324, OAW-IAP325, OAW-IAP334, OAW-IAP335, OAW-AP-344, OAW-AP-345, OAW-AP514, and OAW-AP515	Privileged EXEC mode

show log security

```
show log security <count>
```

Description

This command shows security logs of the OAW-IAP.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log system

```
show log system <count>
```

Description

This command shows system logs of OAW-IAP.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log ucm

```
show log ucm
```

Description

This command displays the log of UCM processes on the OAW-IAP.

Example

The following example displays the log of UCM processes on the AP:

```
(Instant AP) #show log ucm
[7965] Fri May 15 10:23:30 2020.145681 DBUG vm_sip_midcall_request_2xx_success:3359 Audio
VOIP_START 10.15.41.250 10.15.41.243 52042 53384 1 sd 2 dd 2
[7965] Fri May 15 10:23:30 2020.232966 DBUG vm_sip_midcall_request_2xx_success:3359 Audio
VOIP_START 10.15.41.243 10.15.41.250 53384 55042 1 sd 2 dd 2
[7965] Fri May 15 10:24:48 2020.194041 DBUG vm_sip_connected_bye_req:2533 Audio VOIP_STOP
10.15.41.243 10.15.41.250 53384 52042 1
[7965] Fri May 15 10:24:48 2020.194041 DBUG vm_sip_connected_bye_req:2533 Audio VOIP_STOP
10.15.41.250 10.15.41.243 52042 53384 1
```

Related Commands

Command	Description
ucm-logging	Toggles the logging of UCM processes on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log upgrade

```
show log upgrade
```

Description

This command shows image download from URL and upgrade details for both local image file and URL for the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log user

```
show log user [count]
```

Description

This command shows the OAW-IAP user logs.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log user-debug

```
show log user-debug [count]
```

Description

This command shows the OAW-IAP user debug logs.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show log vpn-tunnel

```
show log vpn-tunnel [count]
```

Description

This command shows VPN tunnel status for the OAW-IAP. Use this command without the optional <count> parameter to view a complete table of VPN tunnel status. Include the <count> parameter to display status for the specified count of VPN tunnels.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Example

The following example shows the output of **show log vpn-tunnel** command:

```
2017-05-02 06:49:16 tunnel_profile_init(2644): init tunnel profile <default>.
2017-05-02 06:49:18 tunnel_uplink_change(3552): uplink changed, the new uplink device br0
2017-05-02 06:49:18 tunnel_stop_check_primary_timer(995): current using tunnel=unselected
tunnel
2017-05-02 06:49:36 addroute(529):Dst 0 mask 0 gw a118cee
2017-05-02 06:49:36 addroute(529):Dst a118cfc mask 0 gw a118cee
2017-05-02 06:49:36 tunnel_start_status_monitor_timer(1101): start tunnel status monitor
timer.
2017-05-02 06:49:36 tunnel_sysctl_set_hbt_booster: enable heartbeat tunnel
2017-05-02 06:49:53 tunnel_preempt_config(2985): send message to config preemption option to
none-preempt
2017-05-02 06:49:53 tunnel_preempt_config(3006): config preemption option to none-preempt
2017-05-02 06:49:53 tunnel_preempt_config(3031): Warning!!! preempt have same configure,
return.
2017-05-02 06:49:53 cli_vpn_factory(2303): monitor frequency configure here.
2017-05-02 06:49:53 tunnel_send_pkt_freq_config(3255): config send icmp packet freq 5 for
monitor tunnel device.
2017-05-02 06:49:53 tunnel_psk_config(3124): config cert
2017-05-02 06:49:53 Manual GRE primary endpoint 0.0.0.0
2017-05-02 06:49:55 tunnel_sysctl_set_lmsip: Set LMSIP=172.16.0.254
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platform	Command Mode
All platforms	Privileged EXEC mode

show log vpn-tunnel-primary

```
show log vpn-tunnel-primary
```

Description

This command shows the primary VPN tunnel status for the OAW-IAP.

Parameter	Description
`primary tunnel`	Displays the log output from the primary VPN tunnel.

Example

The following example shows the output of **show log vpn-tunnel-primary** command:

```
2017-04-19 10:07:49 [primary tunnel] cli_proc_rapper_msg(852): Receive rapper msg from 8423
port.
2017-04-19 10:07:49 [primary tunnel] Error!!!: Received RC_OPCODE_ERROR lms 10.17.132.51
tunnel 0.0.0.0 RC_ERROR_IKEP2_PKT1 debug-error:-8949
2017-04-19 10:07:49 [primary tunnel] tunnel_err_msg_recv(1588): Error!!! Received RC_OPCODE_
ERROR peer public ip 10.17.132.51 tunnel ip 0.0.0.0, controller ip 0.0.0.0, RC_ERROR_IKEP2_
PKT1 debug-error:-8949 (ERR_IKE_TIMEOUT)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode

show log vpn-tunnel-backup

```
show log vpn-tunnel-primary
```

Description

This command shows the backup VPN tunnel status for the OAW-IAP.

Parameter	Description
`backup tunnel`	Displays the log output from the backup VPN tunnel.

Example

The following example shows the output of **show log vpn-tunnel-backup** command:

```
2017-05-02 06:49:53 [backup tunnel] tunnel_config_remove(2896): configure remove, tunnel
backup
tunnel, type ipsec tunnel
2017-05-02 06:49:53 [backup tunnel] SM Handler not needed for state TUNNEL_STATE_INIT event
TUNNEL_EVENT_TUNNEL_DISCONNECT
2017-05-02 06:49:53 [backup tunnel] tunnel_unregister_action(2372): unregister ipsec action.
2017-05-02 06:49:53 [backup tunnel] tunnel_unregister_action(2388): ipsec client space
already
free.
E_TIMEOUT)
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode

show log wireless

```
show log wireless [<count>]
```

Description

This command shows wireless logs of the OAW-IAP.

Parameter	Description
`<count>`	Starts displaying the log output from the specified number of lines from the end of the log.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show memory

```
show memory
```

Description

Displays the information about memory utilization for an OAW-IAP.

Example

The following example shows the output of the **show memory** command:

```
MemTotal:          248048 kB
MemFree:           169204 kB
Buffers:                0 kB
Cached:             18164 kB
SwapCached:             0 kB
Active:             21472 kB
Inactive:           12640 kB
Active(anon):       15948 kB
Inactive(anon):         0 kB
Active(file):        5524 kB
Inactive(file):     12640 kB
Unevictable:            0 kB
Mlocked:                0 kB
SwapTotal:              0 kB
SwapFree:               0 kB
Dirty:                  0 kB
Writeback:              0 kB
AnonPages:          15972 kB
Mapped:              7728 kB
Shmem:                  0 kB
Slab:               32252 kB
SReclaimable:         884 kB
SUnreclaim:         31368 kB
KernelStack:          816 kB
PageTables:           512 kB
NFS_Unstable:           0 kB
Bounce:                 0 kB
WritebackTmp:           0 kB
CommitLimit:       124024 kB
Committed_AS:       33616 kB
VmallocTotal:      516096 kB
VmallocUsed:        39452 kB
VmallocChunk:      449532 kB
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show mgmt-user

```
show mgmt-user
```

Description

This command displays the credentials for management users for the OAW-IAP management interface. Use this command to view the admin user credentials required for accessing the OAW-IAP and external server configuration details for the management users.

Examples

The following output is displayed for the **show mgmt-user** command:

```
Server Load Balancing :Disabled
Local User DB Backup  :Disabled
Hash Management Password  :Enabled
Authentication Servers
----------------------
Name  Type  IP Address  Port  Key  Timeout  Retry Count  NAS IP Address  NAS Identifier
RFC3576
----  ----  ----------  ----  ---  -------  -----------  --------------  --------------  ----
---
Management User Table
---------------------
Name   Password                                                                      Type
----   --------                                                                      ----
admin  0603e7ee02ede87d7fb6081270dd548a69df219e8ef4a457f99e190f66cd4298bb97f7afab   Admin
                                                                                    Local
                                                                                    Read-Only
                                                                                    Guest-
Mgmt
```

The output of this command provides the following information:

Column	Description
`Server Load Balancing`	Indicates if load balancing is enabled when two authentication servers are used.
`Local User DB Backup`	Indicates if the backing up of the local user database is enabled.
`Hash Management Password`	Indicates if hashing of management user password is enabled or disabled.
`Name (Authentication Servers Table)`	Indicates the name of the RADIUS server.
`Type`	Indicates the type of the RADIUS server.
`IP address`	Indicates the IP address of the RADIUS server.
`Port`	Indicates the authorization port number of the RADIUS server.
`Key`	Indicates the key for communicating with the RADIUS server.
`Timeout`	Indicates timeout value in seconds for one RADIUS request.

Column	Description
`Retry count`	Indicates the maximum number of authentication requests sent to the RADIUS server.
`NAS IP address`	Displays the IP address of the NAS if NAS is configured.
`NAS Identifier`	Indicates the NAS identifier to be sent with the RADIUS requests if NAS is configured.
`In Use`	Indicates if the server is in use.
`RFC3576`	Indicates if the OAW-IAPs are configured to process RFC 3576-compliant CoA.
`NAS IP address`	Displays the IP address of the NAS if NAS is configured.
`Name (Management User Table)`	Indicates the username of the management user
`Password`	Indicates the password of the admin user.
`Type`	Indicates if the type of the user (admin, read-only, or guest management user).

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show network

```
show network <name>
```

Description

This command shows network configuration details for an OAW-IAP. Use this command without the optional <name> parameter to view a complete configuration details of a network profile on the OAW-IAP. Include the <name> parameter to display settings for a single network SSID only.

Parameter	Description
`<name>`	Displays the name of a network profile.

Example

The following example shows the partial output of **show network <name>** command:

```
Name                   :test
ESSID                  :test
Status                 :Enabled
Mode                   :wpa2-aes
Band                   :all
Type                   :employee
Termination            :Disabled
Passphrase             :
WEP Key                :
WEP Key Index          :1
VLAN                   :
Server Load Balancing  :Disabled
MAC Authentication     :Disabled
L2 Auth Failthrough    :Disabled
Captive Portal         :disable
Exclude Uplink       :none
Hide SSID              :Disabled
Content Filtering      :Disabled
Auth Survivability     :Disabled
Auth Survivability time-out     :24
RADIUS Accounting           :Disabled
Interim Accounting Interval :0
Radius Reauth Interval      :0
Download Roles from CPPM    :Enabled
DTIM Interval               :1
Inactivity Timeout          :1000
Legacy Mode Bands           :all
G Minimum Transmit Rate     :1
G Maximum Transmit Rate     :54
A Minimum Transmit Rate     :6
A Maximum Transmit Rate     :54
Multicast Rate Optimization :Disabled
LEAP Use Session Key        :Disabled
mPSK                        :Enabled
Broadcast-filter       :none
Max Authentication Failures :0
Blacklisting                :Disabled
WISPr                       :Disabled
Accounting mode             :Authentication
Work without usable uplink  :Disabled
Percentage of Airtime: :Unlimited
Overall Limit:         :Unlimited
```

```
Per-user Limit:         :Unlimited
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The output of this command now includes the following: ■ status of the **Download roles for CPPM** configuration is now shown as part of the output. ■ Status of the **mPSK** passphrase.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show network-summary

```
show network-summary
```

Description

This command displays the status of the available network configurations on the OAW-IAP.

Examples

The following output is displayed for the **show network-summary** command:

```
Internet reachable             :Detection disabled
Active uplink                  :eth0
Primary VPN                    :Not configured
Secondary VPN                  :Not configured
AirWave                        :Not configured
```

The output of this command provides the following information:

Column	Description
`Internet Reachable`	Indicates the status of the WLAN network.
`Active uplink`	Indicates the uplink that is currently active on the OAW-IAP.
`Primary VPN`	Indicates the status of the Primary VPN configuration.
`Secondary VPN`	Indicates the status of the Secondary VPN connection.
`Airwave`	Indicates the status of the OmniVista 3600 Air Manager configuration.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ntp debug

```
show ntp debug
```

Description

This command shows NTP logs of the OAW-IAP.

Example

The following example shows the output of **show ntp debug** command:

```
17 Apr 16:07:06 ntpdate[6049]: ntpdate 4.2.8p9@1.3265 Thu Mar  1 07:22:25 UTC 2018 (1)
Looking for host pool.ntp.org and service ntp
193.175.73.151 reversed to char-ntp-pool.charite.de
host found : char-ntp-pool.charite.de
transmit(193.175.73.151)
transmit(107.155.79.108)
receive(193.175.73.151)
transmit(176.96.138.245)
receive(107.155.79.108)
transmit(196.192.32.7)
receive(176.96.138.245)
receive(196.192.32.7)
transmit(193.175.73.151)
transmit(107.155.79.108)
receive(193.175.73.151)
transmit(176.96.138.245)
receive(107.155.79.108)
receive(176.96.138.245)
transmit(196.192.32.7)
receive(196.192.32.7)
transmit(193.175.73.151)
transmit(107.155.79.108)
receive(193.175.73.151)
transmit(176.96.138.245)
receive(107.155.79.108)
receive(176.96.138.245)
transmit(196.192.32.7)
receive(196.192.32.7)
transmit(193.175.73.151)
transmit(107.155.79.108)
receive(193.175.73.151)
transmit(176.96.138.245)
receive(107.155.79.108)
receive(176.96.138.245)
transmit(196.192.32.7)
receive(196.192.32.7)
server 193.175.73.151, port 123
stratum 1, precision -20, leap 00, trust 000
refid [SHM], delay 0.33315, dispersion 0.00175
transmitted 4, in filter 4
reference time:    e0615d2c.2b8716d9  Wed, Apr 17 2019 16:07:08.170
originate timestamp: e0615d33.390a63e8  Wed, Apr 17 2019 16:07:15.222
transmit timestamp:  e0615d33.13911ea1  Wed, Apr 17 2019 16:07:15.076
filter delay:  0.33888  0.33315  0.33887  0.33620
0.00000  0.00000  0.00000  0.00000
filter offset: -0.00995 -0.00745 -0.01030 -0.00895
0.000000 0.000000 0.000000 0.000000
delay 0.33315, dispersion 0.00175
offset -0.007457
server 107.155.79.108, port 123
```

```
stratum 2, precision -24, leap 00, trust 000
refid [107.155.79.108], delay 0.22690, dispersion 0.00002
transmitted 4, in filter 4
reference time:    e0615d14.6b1f8397  Wed, Apr 17 2019 16:06:44.418
originate timestamp: e0615d33.5d36de8b  Wed, Apr 17 2019 16:07:15.364
transmit timestamp:  e0615d33.46c40655  Wed, Apr 17 2019 16:07:15.276
filter delay:  0.22742  0.22691  0.22690  0.22690
0.00000  0.00000  0.00000  0.00000
filter offset: -0.01285 -0.01291 -0.01293 -0.01296
0.000000 0.000000 0.000000 0.000000
delay 0.22690, dispersion 0.00002
offset -0.012936
server 176.96.138.245, port 123
stratum 2, precision -24, leap 00, trust 000
refid [176.96.138.245], delay 0.26892, dispersion 0.00003
transmitted 4, in filter 4
reference time:    e0615d1e.6749d40d  Wed, Apr 17 2019 16:06:54.403
originate timestamp: e0615d33.a14dc6a9  Wed, Apr 17 2019 16:07:15.630
transmit timestamp:  e0615d33.79f6f2bb  Wed, Apr 17 2019 16:07:15.476
filter delay:  0.26941  0.26892  0.26898  0.26900
0.00000  0.00000  0.00000  0.00000
filter offset: 0.032115 0.031937 0.031911 0.031946
0.000000 0.000000 0.000000 0.000000
delay 0.26892, dispersion 0.00003
offset 0.031937
server 196.192.32.7, port 123
stratum 3, precision -24, leap 00, trust 000
refid [196.192.32.7], delay 0.56461, dispersion 0.00012
transmitted 4, in filter 4
reference time:    e0615a14.dcdc289c  Wed, Apr 17 2019 15:53:56.862
originate timestamp: e0615d34.8fb2dfd8  Wed, Apr 17 2019 16:07:16.561
transmit timestamp:  e0615d34.46c3f3e0  Wed, Apr 17 2019 16:07:16.276
filter delay:  0.56711  0.56461  0.56482  0.56476
0.00000  0.00000  0.00000  0.00000
filter offset: 0.016337 0.015284 0.015292 0.015304
0.000000 0.000000 0.000000 0.000000
delay 0.56461, dispersion 0.00012
offset 0.015284
17 Apr 16:07:16 ntpdate[6049]: adjust time server 193.175.73.151 offset -0.007457 sec
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms except IAP-155	Privileged EXEC mode

show ntp status

```
show ntp status
```

Description

This command shows information about the NTP peerings of the OAW-IAP. You can troubleshoot and view connection information of the OAW-IAP with its NTP peer.

Example

The following example shows the output of **show ntp status** command:

```
(Instant AP)# show ntp status
address         refid           st      when    poll    delay   offset      disp
5.103.139.163   GPS             1       1620    1800    0.19952 0.008499    0.00603
5.79.108.34     5.79.108.34     2       1620    1800    0.17981 0.011906    0.00018
193.228.143.13  193.228.143.13  2       1620    1800    0.30267 0.054445    24.00096
193.228.143.22  193.228.143.22  2       1620    1800    0.30556 0.043135    8.00839
```

The output of this command includes the following information:

Column	Description
address	IP address of peer.
refid	Address of reference clock of peer.
st	Stratum of peer.
when	Time since last NTP packet from peer in seconds.
poll	Polling interval in seconds.
delay	Round-trip delay to peer in milliseconds.
offset	Relative time of peer clock to local clock in milliseconds.
disp	The maximum error inherent in measurement in seconds.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show out-of-service

```
show out-of-service
```

Description

This command displays the details of the out of service operations triggered on the OAW-IAP. Use this command to view the out-of-service operations and the SSID availability based on the out-of-service states detected on the OAW-IAP.

Example

The following example shows the output of the **show out-of-service** command:

```
Out of service trigger Status
-----------------------------
uplink-down  primary-uplink-down  internet-down  vpn-down
-----------  -------------------  -------------  --------
No           No                    -             Yes

The following out-of-service events got triggered in last out-of-service-hold-on-time(45) sec
: None
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show port status

```
show port status [details]
```

Description

Displays the activity statistics on each of the port on the switch.

Example

The following example shows the output of the **show port status** command:

```
Port Status
-----------
Port  Type  Admin-State  Oper-State  STP-State  Dot3az
----  ----  -----------  ----------  ---------  ------
eth0  GE    up           up          Off        Disable
eth1  GE    up           up          Off        Disable
eth2  GE    up           down        Off        Disable

Loop-Protect  Storm-Control  Loop-Detection-TX  Loop-Detection-RX
------------  -------------  -----------------  -----------------
OFF           OFF            0                  1
ON            ON             39153              4
ON            ON             306                4
```

The output of this command provides the following information:

Parameter	Description
`Port`	Displays the port number on the switch.
`Type`	Displays the port type.
`Admin-State`	Displays if the port is enabled or disabled.
`Oper-State`	Displays if the port is currently up and running.
`STP-State`	Displays if the spanning tree of this port is on or off.
`Dot3az`	Displays if the Dot3az of this port is enabled or disabled.
`Loop-Protect`	Shows the status of the loop protection feature.
`Storm-Control`	Shows the status of the storm control feature.
`Loop-Detection-TX`	Shows the number of loop packets transmitted on the interface.
`Loop-Detection-RX`	Shows the number of loop packets received on the interface.

The following example shows the output of the **show port status details** command:

```
Swarm Port Stats
----------------
Mac Address        AP                 IF Index  Frames  [in]  Frames [out]
-----------        --                 --------  ------------  ------------
20:4c:03:0e:c6:cf  20:4c:03:0e:c6:cf  0         10732         88696
```

```
20:4c:03:0e:c6:d0  20:4c:03:0e:c6:cf  1         310513        213194
20:4c:03:0e:c6:d1  20:4c:03:0e:c6:cf  2         271365        1682

Bytes   [in]  Bytes  [out]  Speed  Duplex  Link
------------  ------------  -----  ------  ----
1413854       3584848       100    full    up
14283598      14585336      100    full    up
12482790      120570        0      full    down
```

The output of this command provides the following information:

Parameter	Description
`Mac Address`	Shows the MAC address of the OAW-IAP.
`AP`	Shows the name of the OAW-IAP.
`IF Index`	Shows the index of the OAW-IAP interface.
`Frames [in]`	Shows the number of packets received on the interface.
`Frames [out]`	Shows the number of packets transmitted on the interface.
`Bytes [in]`	Shows the number of bytes received on the interface.
`Bytes [out]`	Shows the number of bytes transmitted on the interface.
`Speed`	Shows the speed of the Ethernet interface.
`Duplex`	Shows the full or half duplex value of the Ethernet interface.
`Link`	Shows the Up or Down state of the Ethernet interface.

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **Details** parameter was introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platforms	Command Mode
All platforms	Privileged Exec mode

show port transceiver

```
show port transceiver
```

Description

Displays the SFB optical module transceiver information in the AP. The optical module information can be obtained only from the APs that have a fiber optic port. The following APs support a fiber optic port:

- OAW-AP-374
- OAW-AP-375
- OAW-AP-377
- OAW-AP-318

Example

The following example shows the output of the **show port transceiver** command on an AP that supports fiber port:

<please provide an output example for the show port transceiver command>

The output of this command provides the following information:

Parameter	Description
`Manufacturer`	Denotes the Vendor name.
`Part Number`	Part number provided by the SFP vendor
`S/N`	Serial number provided by the SFP vendor
`Date Code`	Denotes the vendor's manufacturing date code. It consists of 6 numbers each, two of them represent year, month and day of month respectfully. It also includes a vendor specific lot code which may be blank.
`Optional Signals`	Indicates which optional enhanced features are implemented in the transceiver. This information only indicates a capability and not the actual features.
`Supported Modes`	Denotes the transceiver type and the description value.
`Wavelength`	Displays the wavelength in nm.

The following example shows the output of the **show port status transceiver** command on APs that do not support a fiber port:

```
(Instant AP)# show port transceiver
AP does not support fiber port
```

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command introduced

Command Information

OAW-IAP Platforms	Command Mode
OAW-AP-318 OAW-370 Series	Privileged Exec mode

show pppoe

```
show pppoe {config|debug logs|debug status}
```

Description

This command shows PPPoE debug logs and uplink status.

Parameter	Description
`config`	Displays PPPoE configuration details.
`debug logs`	Displays PPPoE debug logs.
`debug status`	Displays the uplink status.

Example

The following example shows the configuration of the PPPoE **show pppoe config** command.

```
PPPoE Configuration
-------------------
Type                     Value
----                     -----
User                     user
Password                 d226ccefac5a95cd6bb04ca74f20473eae9085fb16892b66
Service name             ServiceA
CHAP secret              8acc867926ad85681fd0b0c1a15bb818
Unnumbered dhcp profile  dhcpProfile1
```

The following example shows the configuration of the PPPoE **show pppoe debug logs** command.

```
pppd log not available
```

The following example shows the configuration of the PPPoE **show pppoe debug status** command.

```
pppoe uplink state                  :Suppressed.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show process

```
show process
```

Description

This command displays a list of processes running on an OAW-IAP. You can use it for debugging.

Example

The following example shows the partial output for the **show process** command:

```
PID Uid    VmSize Stat Command
1 root        332 S   init
2 root            SWN [ksoftirqd/0]
3 root            SW< [events/0]
4 root            SW< [khelper]
5 root            SW< [kthread]
6 root            SW< [kblockd/0]
7 root            SW  [pdflush]
8 root            SW  [pdflush]
10 root            SW< [aio/0]
9 root            SW  [kswapd0]
992 root        348 S   /sbin/udhcpc -i br0 -b
1343 root        744 S   /aruba/bin/tinyproxy
1344 root        476 S   /aruba/bin/tinyproxy
1345 root        476 S   /aruba/bin/tinyproxy
1348 root        476 S   /aruba/bin/tinyproxy
1349 root        476 S   /aruba/bin/tinyproxy
1350 root        476 S   /aruba/bin/tinyproxy
1351 root        476 S   /aruba/bin/tinyproxy
1362 root        716 S   /usr/sbin/mini_httpd -c *.cgi -d /etc/httpd -u root
1365 root        732 S   /usr/sbin/mini_httpd -c *.cgi -d /etc/httpd -u root -
1368 root        732 S   /usr/sbin/mini_httpd -c *.cgi -d /etc/httpd -u root -
```

The output of this command provides information on the process ID, user ID of the user running the process, virtual memory consumed by the process, statistics and the command associated with the processes running on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show proxy config

```
show proxy config
```

Description

This command displays the HTTP proxy configuration settings on an OAW-IAP.

Example

The following example shows the output of **show proxy config** command:

```
Proxy server   :10.15.107.210
Proxy port     :1337
Proxy username :user1
Proxy password :*******
Exceptions
----------
No  Exception
--  ---------
1   10.15.107.214
```

The output of this command provides the following information:

Parameter	Description
`Proxy server`	Displays the IP address of the HTTP proxy.
`Proxy port`	Displays the port number configured for the HTTP proxy.
`Exceptions`	Displays the IP address of the hosts for which HTTP proxy configuration is not applied.
`Proxy username`	Displays the user name set to authenticate the proxy server.
`Proxy password`	Displays the password set to authenticate the proxy server in the encrypted format.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	**Proxy username** and **Proxy password** parameters added to the output.
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radio config

```
show radio config
```

Description

This command displays the 2.4 GHz and 5 GHz radio configuration details for an OAW-IAP.

Example

The following example shows the output of **show radio config** command:

```
(Instant AP)# show radio config
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:0
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Cell Size Reduction:0

5.0 GHz:
Legacy Mode:enable
Beacon Interval:100
802.11d/802.11h:enable
Interference Immunity Level:2
Channel Switch Announcement Count:2
MAX Distance:600
Channel Reuse Type:disable
Channel Reuse Threshold:0
Background Spectrum Monitor:disable
Standalone Spectrum Band:5ghz-upper
Cell Size Reduction:0
```

The output of this command provides the following information:

Parameter	Description
`Legacy Mode`	Indicates if the legacy mode is enabled on the OAW-IAPs to run the radio in the non-802.11n mode.
`Beacon Interval`	Displays beacon interval for the OAW-IAP in milliseconds. When beacon interval is configured, the 802.11 beacon management frames are transmitted by the access point at the specified interval.
`802.11d/802.11h`	Displays if the OAW-IAP is allowed advertise its 802.11d (country information) and 802.11h capabilities.
`Interference Immunity Level`	Displays the immunity level configured for an OAW-IAP radio profile to improve performance in high-interference environments. For more information on configuring immunity levels, see rf dot11a-radio-profile and rf dot11g-radio-profile.
`Channel Switch Announcement Count`	Displays the number of channel switching announcements that are sent before switching to a new channel.
`MAX distance`	Indicates the maximum distance in meters between a client and an OAW-IAP or between a mesh point and a mesh portal.

Parameter	Description
`Channel Reuse Type`	Indicates if channel reuse type is enabled.
`Channel Reuse Threshold`	Displays the channel reuse threshold configured for channel reuse type.
`Background Spectrum Monitor`	Indicates background spectrum monitoring is enabled. When enabled, the OAW-IAPs in access mode continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring OAW-IAPs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.
`Standalone Spectrum`	Indicates the portion of the channel (upper, middle, or lower) that is being monitored on the 5 GHz band.
`Cell Size Reduction`	Indicates the Rx sensitivity values configured on the 2.4 GHz and 5.0 GHz radio profiles.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radio profile

```
show radio profile [<profile_name>]
```

Description

This command displays the 2.4 GHz and 5 GHz radio profile details for an OAW-IAP.

Example

The following example shows the output of **show radio profile** command:

```
(Instant AP)# show radio profile

2.4G Radio profile
------------------
Name     Legacy Mode  Single Chain Legacy  Beacon Interval  802.11d/802.11h  Interference
Immunity Level  CSA Count  MAX Distance  Channel Reuse Type  Channel Reuse Threshold
Spectrum Monitor  Max Tx Power  Min Tx Power  Cell Size Reduction  Smart Antenna  zone   WIDS
Override  Active  40M intolerance  Honor 40 intolerance
----     -----------  -------------------  ---------------  ---------------  ----------------
-----------  ---------  ------------  ------------------  -----------------------  ----------
------  ------------  ------------  -------------------  -------------  ----   -------------
------  ---------------  --------------------
default  disable      disable              100              disable          2
            0          600           disable             0                        disable
      0             0             0                    disable                dynamic
Yes     disable          enable
test1    disable      disable              100              disable          2
            0          600           disable             0                        disable
      0             0             0                    disable        test1  dynamic
No      disable          enable

5.0G Radio profile
------------------
Name     Legacy Mode  Single Chain Legacy  Beacon Interval  802.11d/802.11h  Interference
Immunity Level  CSA Count  MAX Distance  Channel Reuse Type  Channel Reuse Threshold
Spectrum Monitor  Standalone Spectrum Band  Max Tx Power  Min Tx Power  Cell Size Reduction
Smart Antenna  VHT     zone   WIDS Override  Active  40M intolerance  Honor 40 intolerance
----     -----------  -------------------  ---------------  ---------------  ----------------
-----------  ---------  ------------  ------------------  -----------------------  ----------
------  ------------------------  ------------  ------------  -------------------  ----------
---  ---     ----   -------------  ------  ---------------  --------------------
default  disable      disable              100              disable          2
            0          600           disable             0                        disable
      5ghz-upper                0             0             0                     disable
  enable         dynamic         Yes     disable          enable
aaa      disable      disable              100              disable          2
            0          600           disable             0                        disable
      5ghz-upper                0             0             0                     disable
  enable         dynamic         No      disable          enable
test1    disable      disable              100              disable          2
            0          600           disable             0                        disable
      5ghz-upper                0             0             0                     disable
  enable  test1  dynamic         No      disable          enable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radius-redirect-url

```
show radius-redirect-url
```

Description

This command displays the RADIUS redirection url received from a CPPM or any authentication server.

Example

The following example shows the output of **show radius-redirect-url** command:

```
c8:b5:ad:c3:af:16# sh radius-redirect-url
Radius VSA Redirect URL
-----------------------
MAC  URL
---  ---
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Release	Modification
All platforms	Privileged EXEC mode

show radius-servers support

```
show radius-servers support
```

Description

This command displays the RADIUS server configuration details for an OAW-IAP.

Example

The following example shows the output of **show radius-servers support** command:

```
RADIUS Servers
--------------
Name            IP Address     Port  Acctport  Key
----            ----------     ----  --------  ---
 InternalServer  127.0.0.1      1616  1813      596ff8d50a0662b542e96567bb87db331

208cc412bfb4aade8033ca9b46e5f09f933f89bb374bdd80b9acadcc981fdf5ea5ea13e33e43378f
                                                                56913cd3e76dc7a


test            test@abc.com   1812  1813
testServer      test@test.com  1812  1813

 Timeout  Retry Count  NAS IP Address  NAS Identifier  In Use  RFC3576
-------  -----------  --------------  --------------  ------  -------
 5        3                                            Yes

 5        3                                            No

Airgroup RFC3576-ONLY  Airgroup RFC3576 port  Deadtime DRP IP   DRP IP Mask
------  -------------  ---------------------- -------  ------   ------------
                Y               5999            5
                                                5
DRP VLAN  DRP Gateway  Radsec    Radsec port
--------- -----------  --------  -----------
                        Disabled  Disabled
                         Enabled      2083
```

The output of this command provides the following information:

Parameter	Description
`Name`	Indicates the name of the RADIUS server.
`IP address`	Indicates the IP address of the RADIUS server.
`Port`	Indicates the authorization port number of the RADIUS server.
`AcctPort`	Indicates the authorization port number of the RADIUS server.
`Key`	Indicates the key for communicating with the RADIUS server.
`Timeout`	Indicates timeout value in seconds for one RADIUS request.
`Retry count`	Indicates the maximum number of authentication requests sent to the RADIUS server.
`NAS IP address`	Displays the IP address of the NAS if NAS is configured.

Parameter	Description
`NAS Identifier`	Indicates the NAS identifier to be sent with the RADIUS requests.
`In Use`	Indicates if the server is in use.
`RFC3576`	Indicates if the OAW-IAPs are configured to process RFC 3576-compliant CoA.
`Airgroup RFC3576-ONLY`	Indicates if OAW-IAPs are configured to be RFC 3576 compliant only.
`Airgroup RFC3576 port`	Indicates the port number used for sending AirGroup CoA.
`Deadtime`	Indicates the RADIUS server dead-time.

`DRP IP`
`DRP Mask`
`DRP VLAN`
	Indicates the IP address, net mask, and DRP VLAN configuredfor DRP.

`RadSec`
`RadSec Port`
	Indicates if RadSec protocol for the RADIUS communiation over TLS is enabled. If RadSec is enabled, the RadSec port number is displayed.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radius status

```
show radius status
```

Description

This command displays the status of TLS tunnel between the OAW-IAP and RadSec proxy. Use this command to view the status of TLS tunnel when RADIUS communication over TLS is enabled on an OAW-IAP.

Example

The following example shows the output of **show radius status** command:

```
Radius server status
--------------------
Name            Server IP  Source IP      Server Name     Protocol    Port  Connected sockets
----            ---------  ---------      -----------     --------    ----  -----------------
InternalServer  127.0.0.1  10.17.129.253  Not configured  RADIUS/UDP  1616  Not Applicable
test            10.0.0.1   10.17.129.253  Not configured  RADIUS/UDP  1812  Not Applicable
t_test          127.0.0.1  10.17.129.253  Not configured  RADIUS/UDP  2630  Not Applicable
Radius1         10.0.0.2   10.17.129.253  Not configured  RADIUS/UDP  1812  Not Applicable
t_Radius1       127.0.0.1  10.17.129.253  Not configured  RADIUS/UDP  2632  Not Applicable

Status          Last connection tried at    Next connection at
------          ------------------------    ------------------
Not Applicable  Not Applicable              Not Applicable
Not Applicable  2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable  2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable  2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
Not Applicable  2015-07-07 00:00:00.000000  2015-07-07 00:00:05.5000000
```

The output of this command provides the following information:

Parameter	Description
`Name`	Indicates the name of the RADIUS server.
`Server IP`	Indicates the IP address of the RADIUS server.
`Source IP`	Indicates the source IP address.
`Server Name`	Indicates the name of the server.
`Protocol`	Indicates the type of protocol used for RADIUS communication with the OAW-IAP clients.
`Port`	Indicates the authorization port number of the RADIUS server.
`Connected Sockets`	Indicates connected sockets if any.
`Status`	Indicates status of the server connection.
`Last connection tried at`	Indicates the time stamp during which the last connection between the server and client was attempted.
`Next connection at`	Indicates the time at which the next attempt will be made to establish the connection with the RADIUS server.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show radseccert

```
show radseccert
```

Description

This command displays details of the RadSec client and CA certificates uploaded on the OAW-IAP. Use this command to view the RadSec certificate details on the OAW-IAP.

Example

The following example shows the output of the **show radseccert** command:

```
Current radsec CA Certificate:
Version       :3
Serial Number :DE:DF:11:F6:AC:C0:91:00
Issuer        :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Subject       :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Issued On     :Mar 24 15:14:41 2011 GMT
Expires On    :Mar 21 15:14:41 2021 GMT
Signed Using  :SHA1-RSA
RSA Key size  :1024 bits
Current radsec Certificate:
Version       :3
Serial Number :DE:DF:11:F6:AC:C0:91:03
Issuer        :/C=GB/ST=Berkshire/O=My Company
Ltd/OU=Leon/CN=Leon/emailAddress=lzheng@arubanetworks.com
Subject       :/C=GB/ST=Berkshire/L=Newbury/O=My Company
Ltd/CN=ClientCert/emailAddress=lzheng@arubanetworks.com
Issued On     :Mar 24 15:25:24 2011 GMT
Expires On    :Mar 21 15:25:24 2021 GMT
Signed Using  :SHA1-RSA
RSA Key size  :1024 bits
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show rtls-logs

```
show rtls-logs
```

Description

This command displays the debugging logs generated for the RTLS tags by the OAW-IAP.

Example

The following example shows the output of the **show rtls-logs** command:

```
2018-04-13 07:49:33 ----------AS (aeroscout) Config------
2018-04-13 07:49:33 AP - f0:5c:19:c9:c5:18, IP - 10.65.65.221, Port - 15407
2018-04-13 07:49:33 TOUT 0, TAG ADDR 00:00:00:00:00:00
2018-04-13 07:49:33 DFactor 0 DTimeout 0
2018-04-13 07:49:33 Report Tag - 0, Report MU - 0
2018-04-13 07:49:33 Tag Sent - 0, MU Sent - 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show rtls-tags

```
show rtls-tags
```

Description

This command displays list of RTLS tags associated with the OAW-IAP.Use this command to view the RTLS tags list.

Example

The following example shows the output of the **show rtls-tags** command:

```
RTLS Device Table [Tags]
-------------------------
MAC                RSSI  BSSID            Batt(%)  Data Rate  TX Power  Channel  Vendor ID
Last Update
---                ----  ---  -----       -------  --------- --------  -------  ---------  ---
--------
00:0c:cc:55:73:8e  -10   a8:bd:27:18:49:c0  0        10        0         6        0
10s
00:0c:cc:02:b4:eb  -30   a8:bd:27:18:49:c0  0        10        0         6        0
107s
00:0c:cc:55:73:7c  -41   a8:bd:27:18:49:c0  0        10        0         6        0
213s

Total devices:3
-------------------------------
Report Tag                           : Off
Report Interval                      : 60
Debug Logs                           : On
Last Send Time                       : 2018-04-13 15:32:21
Tags Chirps                          : 8223
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show running-config

```
show running-config
```

Description

This command displays the current configuration running on an OAW-IAP, including the current changes that are yet to be saved. Use this command to view the current configuration information stored in the OAW-IAP flash memory.

Example

The following example shows the partial output of the **show running-config** command output:

```
version 6.4.0.0-4.1.0
virtual-controller-country IN
virtual-controller-key 0cb5770401cdeb6e4363c25fdfde17d907c4b095a9be5e
name instant-C4:42:98
terminal-access
clock timezone none 00 00
rf-band all
allow-new-aps
allowed-ap d8:c7:c8:c4:42:98
arm
wide-bands 5ghz
80mhz-support
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
client-match
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin aba950f14f5764975371fcb66a72d10f
wlan access-rule default_wired_port_profile
index 1
rule any any match any any any permit
wlan access-rule wired-instant
index 2
rule masterip 0.0.0.0 match tcp 80 80 permit
rule masterip 0.0.0.0 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule test
index 3
rule any any match any any any deny
wlan ssid-profile test
enable
index 1
type employee
essid instant
opmode opensystem
max-authentication-failures 0
rf-band all
```

```
captive-portal disable
dtim-period 1
inactivity-timeout 1000
broadcast-filter none
dmo-channel-utilization-threshold 90
local-probe-req-thresh 0
max-clients-threshold 64
dot11k
dot11v
auth-survivability cache-time-out 24
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
auto-whitelist-disable
https
blacklist-time 3600
auth-failure-blacklist-time 3600
ids
wireless-containment none
wired-port-profile wired-instant
switchport-mode access
allowed-vlan all
native-vlan guest
no shutdown
access-rule-name wired-instant
speed auto
duplex auto
no poe
type guest
captive-portal disable
no dot1x
wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
enet0-port-profile default_wired_port_profile
uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180
airgroup
disable
airgroupservice airplay
disable
description AirPlay
airgroupservice airprint
disable
description AirPrint
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show snmp-configuration

```
show snmp-configuration
```

Description

This command displays the SNMP configuration details for a Virtual switch. Use this command to view the SNMP information configured on a Virtual switch.

Example

The following example shows the output of **show snmp-configuration** command:

```
Engine ID:D8C7C8CBD420
Community Strings
-----------------
Name
----
Test
SNMPv3 Users
------------
Name   Authentication Type  Encryption Type
----   -------------------  ---------------
hallo  SHA                  NONE
DES    SHA                  DES
SNMP Trap Hosts
---------------
IP Address       Version  Name  Port  Inform
----------       -------  ----  ----  ------
192.0.2.1  v3       miro  162   Yes
```

The output of this command includes the following parameters:

Parameter	Description
Engine ID	Displays the SNMP engine ID.
Community Strings	Displays the SNMP community strings..
SNMPv3 Users	Displays details about the SNMPv3 users.
Name	Indicates the name of the SNMP user.
Authentication Type	Indicates the authentication protocol configured for the SNMP users.
Encryption Type	Indicates the encryption type, for example, CBC-DES Symmetric Encryption Protocol configured for SNMP users.
SNMP Trap Hosts	Displays the traps generated by the host system.
IP Address	Indicates the host IP address generating the SNM trap.
Version	Displays the SNMP version for which the trap is generated.
Name	Indicates the name of system generating the SNMP traps.
Port	Indicates the port number to which notification messages are sent.
Inform	Displays the SNMP inform messages to send to the configured host.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show snmp trap-queue

```
show snmp trap-queue
```

Description

This command displays the list of SNMP traps in queue.

Example

The following example shows the partial output of **show snmp trap-queue** command:

```
2013-05-12 14:05:27 An AP (NAME d8:c7:c8:cb:d4:20 and MAC d8:c7:c8:cb:d4:20 on RADIO 2)
detected an interfering access point (BSSID 00:24:6c:80:7d:11 and SSID NTT-SPOT on CHANNEL
1).
2013-05-12 14:09:53 An AP (NAME d8:c7:c8:cb:d4:20 and MAC d8:c7:c8:cb:d4:20 on RADIO 2)
detected an interfering access point (BSSID 6c:f3:7f:45:5d:20 and SSID 7SPOT on CHANNEL 1).
2013-05-12 14:10:36 An AP (NAME d8:c7:c8:cb:d4:20 and MAC d8:c7:c8:cb:d4:20 RADIO 2) changed
its channel from channel 1 (secchan offset 1) to channel 7 (secchan offset 1) due to reason
12.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show spectrum-alert

```
show spectrum-alert
```

Description

This command displays the list of spectrum alerts for an OAW-IAP.

When a new non-Wi-Fi device is found, an alert is reported to the Virtual Controller. The spectrum alert messages provide information about the device ID, device type, IP address of the spectrum monitor or hybrid OAW-IAP, and the timestamp. The Virtual Controller reports the detailed device information to OmniVista 3600 Air Manager Management server.

Parameter	Description
`<count>`	Filters the alerts based on the specified number.

Example

The following example shows the output for the **show spectrum-alert** command when no alerts are generated.

```
Spectrum Alerts
---------------
Timestamp  Type  ID  Access Point
---------  ----  --  ------------
```

The output of this command provides the following information:

Parameter	Description
`Timestamp`	Displays the time at which alert was recorded.
`Type`	Displays the type of the device that generated the alert.
`ID`	Displays the device ID for which the alert is generated.
`Access Point`	Displays the IP address of the OAW-IAP.

Command History

Release	Description
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show speed-test

```
show speed-test
```

Description

This command displays the details obtained from the Virtual Controller speed-test client.

Examples

The following output is displayed for the **show speed-test** command:

Speed Test Data for traffic : From Client to Server

```
Time of Execution :Mon, 02 Nov 2015 09:18:07 GMT
Server IP :10.17.138.2
Local IP :10.17.138.188
Local Port :51308
Remote Port :5201
Protocol :UDP
Duration :20
Bytes Txferred :249271000
Bandwitdh(bps) :99706100
Jitter(millisec) :0
Datagrams sent :249270
```

Speed Test Data for traffic : From Server to Client

```
Time of Execution :Mon, 02 Nov 2015 09:18:28 GMT
Server IP :10.17.138.2
Local IP :10.17.138.188
Local Port :56423
Remote Port :5201
Protocol :UDP
Duration :20
Bytes Txferred :234013000
Bandwitdh(bps) :93603500
Jitter(millisec) :0
Datagrams sent :234009
```

The output of this command provides the following information:

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ssh

```
show ssh
```

Description

This command displays the SSH cipher configuration details.

Example

The following example shows the output of **show ssh** command:

```
SSH Ciphers Settings:
Ciphers       :aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
```

The following example shows the output of **show ssh** command if the OAW-IAP runs on a Dropbear platform:

```
SSH Ciphers Settings:
Ciphers       :aes256-ctr,aes128-ctr,aes256-cbc,aes128-cbc
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show stats

```
show stats {ap <IP-address>| client <MAC-address> | global | network <network-name>} [count]
```

Description

This command displays the aggregate statistics for OAW-IAPs, OAW-IAP clients, OAW-IAP cluster, and network profiles configured on an OAW-IAP.

Parameter	Description
`ap <IP-address>`	Displays information on OAW-IAP utilization, RF trends, and client details for a specific OAW-IAP.
`client <MAC-address>`	Displays information on a client and its mobility records, the cluster to which the client has joined, and the details of the OAW-IAP to which it is currently connected.
`global`	Displays global statistics for the OAW-IAP cluster, and the OAW-IAPs and clients connected to the OAW-IAP cluster.
`network <network-name>`	Displays aggregate information about a network profile configured on anOAW-IAP.
`[count]`	Allows you to filter the command output for the OAW-IAP, client, global, and network profile statistics based on the specified number.

This command shows the following information:

- Utilization trend—Displays information about the OAW-IAP utilization, the number of clients associated with an OAW-IAP, Virtual Controller, or the OAW-IAP network over the last 15 minutes.
- RF trends—Displays information the utilization, noise, or error threshold for an OAW-IAP. It also shows the current speed or signal strength for the clients in the network and the RF information for the OAW-IAPs to which the clients are connected.
- Mobility Trail—Shows duration of the client is association with an OAW-IAP and the name of the OAW-IAP to which it is currently connected.

Examples

show stats ap

The following example shows the output for the **show stats ap <IP-address>** command:

```
Util Level:good
Noise Level:good
Error Level:good
2.4 GHz Channel:7
5.0 GHz Channel:149+
Usage
-----
Timestamp  CPU Utilization (%)  Memory Free (MB)  Neighboring APs [Valid]  Neighboring APs
[Interfering]  Neighboring APs [Rogue]  Neighboring Clients [Valid]  Neighboring Clients
[Interfering]  Clients  Throughput [Out] (bps)  Throughput [In] (bps)
---------  -------------------  ----------------  -----------------------  ------------------
-----------  -----------------------  ---------------------------  --------------------------
-------  -------  ----------------------  ---------------------
00:34:46   8                    164               4                        239
            0                        1                            8
       1        93                      99
```

```
00:34:17   8                    164              4                        239
            0                        1                            8
       1        186                     199
                          0                        1                            9

RF Trends
---------
Timestamp  Utilization [2.4 GHz] (%)  Utilization [5.0 GHz] (%)  Noise Floor [2.4 GHz]
 (dBm)  Noise Floor [5.0 GHz] (dBm)  2.4 GHz Frames [Errors] (fps)  5.0 GHz Frames [Errors]
(fps)  2.4 GHz Frames [Out] (fps)  5.0 GHz Frames [Out] (fps)  2.4 GHz Frames [In] (fps)  5.0
GHz Frames [In] (fps)  2.4 GHz Frames [Drops] (fps)  5.0 GHz Frames [Drops] (fps)  2.4 GHz
Mgmt Frames [In] (fps)  5.0 GHz Mgmt Frames [In] (fps)  2.4 GHz Mgmt Frames [Out] (fps)  5.0
GHz Mgmt Frames [Out] (fps)
-----  ---------------------------  -----------------------------  --------------------------
---  --------------------------  --------------------------  -------------------------  -----
--------------------  ----------------------------  ----------------------------  -----------
-------------------  ------------------------------  -------------------------------  -------
------------------------
00:34:46   59                          4                          -91
-93                          41                            0                              0
                         0                           68                          18
             1                             1                             403
           265                             1                              0
00:34:17   61                          5                          -92
-93                          45                            0                              0
                         1                           78                          21
             1                             1                             408
           287                             1                              1
Client Heatmap
--------------
Clients  Signal  Speed  IP Address
-------  ------  -----  ----------
AP List
-------
Name                IP Address    Mode    Spectrum  Clients  Type  CPU Utilization %:  Memory
Free (MB):  Serial Number:  Need Antenna Config  From Port
----                ----------    ----    --------  -------  ----  ------------------  -------
----------  --------------  -------------------  ---------
d8:c7:c8:cb:d4:20  10.17.88.188  access  disable   1        135   8                   164
           AX0059921       No                    none
```

show stats client

The following example shows the output for the **show stats client <mac>** command:

```
Name::
IP Address::169.254.90.154
MAC Address::08:ed:b9:e1:51:7d
Access Point::d8:c7:c8:cb:d4:20
Channel::149+
Network::Network1
Connection Time::4h:50m:48s
Type::AN
OS::
Swarm Client Stats
------------------
Timestamp  Signal (dB)  Frames [In] (fps)  Frames [Out] (fps)  Throughput [In] (bps)
Throughput [Out] (bps)  Frames [Retries In] (fps)  Frames [Retries Out] (fps)  Speed (mbps)
---------  -----------  -----------------  ------------------  ---------------------  -------
---------------  -------------------------  --------------------------  -----------
00:32:46   47           0                  0                   0                      170
                0                  0                            6
00:32:16   47           0                  0                   0                      170
                0                  0                            6
00:31:46   47           0                  1                   0                      5946
                0                  0                            6
```

```
00:31:16   49           0                  0                   0                      316
                0                          0                           6

Mobility Trail
--------------
Association Time  Access Point
----------------  ------------
11:04:56          d8:c7:c8:cb:d4:20
Client Heatmap
--------------
Client          Signal  Speed  IP Address
------          ------  -----  ----------
169.254.90.154  good    good   169.254.90.154
Access Point Heatmap
--------------------
Access Point       Utilization  Noise  Errors
------------       -----------  -----  ------
d8:c7:c8:cb:d4:20  good         good   good
Client List
-----------
Name  IP Address      MAC Address        OS  Network         Access Point       Channel  Type
 Role
----  ----------      -----------        --  -------         ------------       -------  ----
 ----
169.254.90.154  08:ed:b9:e1:51:7d      Network1  d8:c7:c8:cb:d4:20  149+     AN    Network1
Info timestamp      :48662
```

show stats global

The following example shows the output for the **show stats global** command:

```
Swarm Global Stats
------------------
Timestamp  Clients  Frames [Out] (fps)  Frames [In] (fps)  Throughput [Out] (bps)  Throughput
[In] (bps)
---------  -------  ------------------  -----------------  ----------------------  ----------
-----------
00:38:05   1        0                   0                  294                     380
00:37:35   1        0                   0                  98                      101
00:37:04   1        0                   0                  0                       0
00:36:33   1        0                   0                  0                       0
00:36:03   1        0                   0                  0                       0
00:35:32   1        0                   0                  46                      49
00:35:01   1        0                   0                  93                      99
00:34:31   1        0                   0                  186                     199
00:34:00   1        0                   0                  0                       0
00:33:29   1        0                   0                  0                       0
00:32:59   1        0                   0                  0                       170
00:32:28   1        0                   0                  0                       170
00:31:58   1        0                   1                  2961                    5946
00:31:27   1        0                   0                  196                     316
00:30:56   1        0                   0                  196                     202
Access Point Heatmap
--------------------
Access Points  Utilization  Noise  Errors
-------------  -----------  -----  ------
Client Heatmap
--------------
Clients  Signal  Speed  IP Address
-------  ------  -----  ----------
```

show stats network

The following example shows the output for the **show stats network <network-name>** command:

```
Swarm Network Stats
```

```
-------------------
Timestamp  Clients  Frames [Out] (fps)  Frames [In] (fps)  Throughput [Out] (bps)  Throughput
[In] (bps)
---------  -------  ------------------  -----------------  ----------------------  ----------
-----------
16:39:25   0        0                   0                  0                       0
16:38:55   0        0                   0                  0                       0
16:38:25   0        0                   0                  0                       0
16:37:54   0        0                   0                  0                       0
16:37:24   0        0                   0                  0                       0
16:36:54   0        0                   0                  0                       0
16:36:24   0        0                   0                  0                       0
16:35:54   0        0                   0                  0                       0
16:35:23   0        0                   0                  0                       0
16:34:53   0        0                   0                  0                       0
16:34:23   0        0                   0                  0                       0
Access Point Heatmap
--------------------
Access Points      Utilization  Noise  Errors
-------------      -----------  -----  ------
d8:c7:c8:c4:42:98  poor         good   good
Client Heatmap
--------------
Clients  Signal  Speed  IP Address
-------  ------  -----  ----------
Name                   :test123
ESSID                  :test123
Status                 :Enabled
Mode                   :wpa2-aes
Band                   :all
Type                   :employee
Termination            :Disabled
Passphrase             :
WEP Key                :
WEP Key Index          :1
VLAN                   :
Server Load Balancing  :Disabled
MAC Authentication     :Disabled
L2 Auth Failthrough    :Disabled
Captive Portal         :disable
Exclude Uplink       :none
Hide SSID              :Disabled
Content Filtering      :Disabled
Auth Survivability     :Disabled
Auth Survivability time-out     :24
RADIUS Accounting           :Disabled
Interim Accounting Interval :0
Radius Reauth Interval      :0
DTIM Interval               :1
Inactivity Timeout          :1000
Legacy Mode Bands           :all
G Minimum Transmit Rate     :1
G Maximum Transmit Rate     :54
A Minimum Transmit Rate     :6
A Maximum Transmit Rate     :54
Multicast Rate Optimization :Disabled
LEAP Use Session Key        :Disabled
Broadcast-filter       :none
Max Authentication Failures :0
Blacklisting                :Disabled
WISPr                       :Disabled
Accounting mode             :Authentication
Work without usable uplink  :Disabled
```

```
Percentage of Airtime: :Unlimited
Overall Limit:         :Unlimited
Per-user Limit:        :Unlimited
Access Control Type:   :Role
Machine-only Role:     :test1
User-only Role:        :test1
Dynamic Multicast Optimization      :Disabled
DMO Channel Utilization Threshold   :90
Local Probe Request Threshold       :0
Max Clients Threshold       :64
Background WMM Share       :0
Best Effort WMM Share      :0
Video WMM Share            :0
Voice WMM Share            :0
Certificate Installed: :No
Internal Radius Users:  :0
Internal Guest Users:  :0
Role Derivation Rules
---------------------
Attribue  Operation  Operand  Role Name  Index
--------  ---------  -------  ---------  -----
Vlan Derivation Rules
---------------------
Attribue  Operation  Operand  Vlan Id
--------  ---------  -------  -------
RADIUS Servers
--------------
Name     IP Address  Port  Key      Timeout  Retry Count  NAS IP Address  NAS Identifier
RFC3576
----     ----------  ----  ---      -------  -----------  --------------  --------------  ---
----
test     10.0.0.1    1812  test123  5        3
test123  10.0.0.0    1812  test123  5        3
LDAP Servers
------------
Name  IP Address  Port  Timeout  Retry Count  Admin-DN  Admin Password  Base-DN
----  ----------  ----  -------  -----------  --------  --------------  -------
test  0.0.0.0     0     5        3
Access Rules
------------
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport)  Action  Log  TOS  802.1P
Blacklist  Mirror  DisScan  ClassifyMedia
-------  ---------  ----------  -------------------------  ------  ---  ---  ------  --------
-  ------  -------  -------------
any      any        match       any                        permit
Vlan Id           :0
ACL Captive Portal:disable
:Captive Portal Configuration
Background Color:13421772
Banner Color       :16750848
Decoded Texts      :
Banner Text        :Welcome to Guest Network
Use Policy         :Please read terms and conditions before using Guest Network
Terms of Use       :This network is not secure, and use is at your own risk
Internal Captive Portal Redirect URL:
Captive Portal Mode:Acknowledged
:External Captive Portal Configuration
Server:localhost
Port               :80
URL                :/
Authentication Text:Authenticated
External Captive Portal Redirect URL:
Server Fail Through:No
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show subscription-aps

```
show subscription-aps
```

Description

This command displays the subscription status of an OAW-IAP.

Example

```
(Instant AP) (config) # show subscription-aps

IAP controlled by Cloud-Server:disable
subscription enabled by manually :disable
Subscription Ap List
--------------------
MAC Address Status
----------- ------
d8:c7:c8:c4:56:de ACTIVE
d8:c7:c8:c4:57:06 ACTIVE
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show summary

```
show summary {<difference> | support}
```

Description

This command shows the current configuration details.

Parameter	Description
`<difference>`	Shows the difference in configuration.
`support`	Shows the summary support containing the configuration details used by support.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show swarm

```
show swarm {state|mode|image-sync}
```

Description

This command displays the various entities associated with the swarm.

Parameter	Description
`state`	Displays the current status of the OAW-IAP cluster.
`mode`	Displays the functioning mode of the OAW-IAP cluster.
`image-sync`	Displays the image-sync OAW-IAP list.

Example

The following example shows the output of **show swarm state** command:

```
AP Swarm State           :swarm_config_sync_complete
mesh auto eth0 bridging  :no
Config in flash       :yes
factory SSID in flash :no
extended-ssid configured :yes
extended-ssid active     :yes
advanced-zone            :yes
Factory default stat     :no
Source of system time    :Image file
Config load cnt       :1
VC Channel index      :1
IDS Client Gateway Detect :yes
Config Init success cnt for heartbeat   :0
Config Init success cnt for register    :0
Config Init skipping cnt for heartbeat  :0
Config Init skipping cnt for register   :0
Config Init last success reason    :N/A
Config Init last success time      :N/A
```

The output of this command describes synchronization status of the OAW-IAP cluster.

The following text shows an example output for the **show swarm mode** command:

```
Swarm Mode       :Cluster
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	The **advanced-zone** parameter was added.
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were added: ■ image-sync ■ Source of system time
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show supported-cert-formats

```
show supported-cert-formats
```

Description

This command displays the supported server and CA certificate formats.

Examples

The following example shows the output of **show supported-cert-formats** command:

```
Server Certificate Formats
--------------------------
Name
----
PEM
CA Certificate Formats
----------------------
Name
----
PEM
DER
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command modified.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show syslog-level

```
show syslog-level
```

Description

This command displays the Syslog logging levels configured for an OAW-IAP.

Example

The following example shows to output of the **show syslog-level** command:

```
Logging Level
-------------
Facility    Level
--------    -----
ap-debug    debug
network     debug
security    debug
system      debug
user        debug
user-debug  debug
wireless    debug
```

The output of this command provides the following information:

Parameter	Description
`Facility`	Displays the list of logging facilities configured on the OAW-IAP.
`ap-debug`	Generates a log for the OAW-IAP device for debugging purposes.
`network`	Generates a log when there is a change in the network, for example, when a new OAW-IAP is added to a network.
`security`	Generates a log for network security, for example, when a client connects using wrong password.
`system`	Generates a log about the system configuration and status.
`user`	Generates a log for the OAW-IAP clients.
`user-debug`	Generates a detailed log about the clients for debugging purposes.
`wireless`	Generates a log about radio configuration.
`syslog-level <level>`	Displays any of the following Syslog logging level configured for the Syslog facility. ■ Emergency—Panic conditions that occur when the system becomes unusable. ■ Alert—Any condition requiring immediate attention and correction. ■ Critical—Any critical conditions, for example, hard drive error. ■ Errors—Error conditions. ■ Warning—Warning messages. ■ Notice—Significant events of a non-critical and normal nature. The default value for all Syslog facilities. ■ Informational—Messages of general interest to system users. ■ Debug—Messages containing information useful for debugging.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show tacacs-servers

```
show tacacs-servers
```

Description

This command displays all the tacacs servers configured on an OAW-IAP.

Example

The following example shows the output of the **show tacacs-servers** command:

```
TACACS Servers
--------------
Name IP Address Port Key Timeout Retry Count In Use
---- ---------- ---- --- ------- ----- ----- ------
tacacs1 10.64.16.240 49 pass123 20 1 Yes
tacacs2 192.168.0.100 49 pass456 10 2 No
```

The output of this command provides the following information:

Parameter	Description
`Name`	Indicates the list of tacacs server available on an OAW-IAP.
`IP Address`	Displays the IP address for each tacacs server.
`Port`	Indicates the TCP Port in use for the tacacs server.
`key`	Indicates the shared secret key used to authenticate and access tacacs server.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show tech-support

```
show tech-support
```

Description

This command displays the complete OAW-IAP information and the associated configuration details, which can be used by the technical support representatives for debugging.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show time-profile

```
show time-profile
```

Description

This command displays all the time range profiles, the respective SSIDs and access rules on which they are applied, and the status (enabled or disabled).

Example

The following example shows the output of the **show time-profile** command:

```
Time Range SSID Profile
-----------------------
Time Profile Name  SSID profile Name  Enable/Disable
-----------------  -----------------  --------------
Lunch Break         Test123             Enable

Time Range ACL Profile
----------------------
Time Profile Name       Access Role Name        Rule
-----------------       ----------------        ----------------
Evening_5_7             sandeepy                 any any match any any any permit
                                                 time-range hello_world
```

The output of this command provides the following information:

Parameter	Description
`Time Profile Name`	Name of the time profile.
`SSID Profile Name`	The WLAN SSID profiles for which the time profile is applied.
`Access Role Name`	The access role name for which the time profile is applied.
`Enable/Disable`	Status of the time range profile on the SSID.
`Rule`	Displays the access rule configuration.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **Access Role Name** and **Rule** parameters were introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show time-range

```
show time-range
```

Description

This command displays a list of the time range profiles configured on the OAW-IAP.

Example

The following example shows the output of the **show time-range** command:

```
Time Range Summary
------------------
Profile Name  Type      Start Day   Start Time  End Day     End Time  Valid
------------  ----      ---------   ----------  -------     --------  -----
test          Periodic  daily       13:00       -           14:00     No
test1         Absolute  11/17/2015  10:00       11/24/2015  17:00     No
Lunchbreak    Periodic  weekday     12:00       -           13:00     No
Lunchbreak1   Periodic  daily       12:00       -           13:00     No
```

The output of this command provides the following information:

Parameter	Description
`Profile Name`	Indicates the name of Time Profiles created on the OAW-IAP.
`Type`	Indicates the type of time profile created.
`Start Day`	Indicates the date on which the time profile is enabled on the SSID.
`Start Time`	Indicates the time at which the time profile is made active on the SSID.
`End Day`	Indicates the date on which the time profile is disabled on the SSID.
`End Time`	Indicates the time at which the time profile is disabled on the SSID.
`Valid`	Indicates if the profile is valid for current time. For example, if a profile is run only during a specific time of the day and is not active when the command is run, the **Valid** column displays the status as **No**.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show tspec-calls

```
show tspec-calls
```

Description

This command displays the TSPEC statistics when voice traffic is prioritized and TSPEC function is enabled on an SSID.

Example

The following example shows the output of the **show tspec-calls** command:

```
TSPEC Stats
-----------
SSID      Total ADDTS  Accepted calls  Refused calls  DELTS Received  DELTS Sent
----      -----------  --------------  -------------  --------------  ----------
Aruba-ap  0            0               0              0               0
Aruba-ap  0            0               0              0               0
TSPEC SSIDs
------------
SSID      Radio  Max Bandwidth  Available Bandwidth
----      -----  -------------  -------------------
Aruba-ap  1      0.00           0.00
TSPEC Calls
-----------
Client  Client MAC  Allocated Bandwidth  Active flows
------  ----------  -------------------  ------------
TSPEC SSIDs
------------
SSID      Radio  Max Bandwidth  Available Bandwidth
----      -----  -------------  -------------------
Aruba-ap  0      0.00           0.00
TSPEC Calls
-----------
Client  Client MAC  Allocated Bandwidth  Active flows
------  ----------  -------------------  ------------
```

The output of this command displays information about the voice calls, the SSIDs on which TSPEC is enabled, and the OAW-IAP clients connected to the SSIDs with TSPEC enabled.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show ucm cdrs

```
show ucm cdrs
```

Description

This command displays the UCM call data records stored on the OAW-IAP.

Example

The following example displays the UCM call data records on the AP:

```
(Instant AP) #show ucm cdrs
UCC Call ID                                              src-ip          src-port   dst-ip
      dst-port        APP
[A] 6d339bfa456b2a11058f79df7d47affd@10.15.80.80:5060    10.15.41.250    52656
10.15.41.243    53932           SIP
[A] 102651NDU0ZDk1ZTYyYjc5MTYwNDRjYjg1OGFlM2UyYzQzNWQ    10.15.41.243    53932
10.15.41.250    52656           SIP
```

The output of this command includes the following information:

Column	Description
UCC Call ID	Call ID of the video or voice session.
src-ip	Source IP of session packets.
src-port	Source port of the session packets.
dst-ip	Destination IP of the session packets.
dst-port	Destination port of the session packets.
APP	Application used for the video or voice session.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show uncommitted-config

```
show uncommitted-config
```

Description

This command displays the current configuration details that are yet to be committed and saved on the OAW-IAP.

Use the **commit apply** command to commit the configuration changes.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show upgrade info

```
show upgrade info
```

Description

This command displays the image upgrade details for an OAW-IAP.

Example

The following example shows the output of **show upgrade info** command:

```
Image Upgrade Progress
----------------------
Mac                IP Address    AP Class    Status    Image Info  Error Detail
---                ----------    --------    ------    ----------  ------------
d8:c7:c8:cb:d4:20  10.17.88.188  Cassiopeia  image-ok  image file  none
Auto reboot           :enable
Use external URL      :disable
```

The output of this command provides the following information:

Parameter	Description
`Mac`	Shows the MAC address of the OAW-IAP.
`IP Address`	Shows the IP address of the OAW-IAP.
`AP Image Class`	Indicates the OAW-IAP class. The following examples describe the image class for different OAW-IAP models: ■ For OAW-RAP155/155P—AlcatelAOS-W Instant_Aries_<build-version> ■ For OAW-IAP224/225 and OAW-IAP274/275—AlcatelAOS-W Instant_Centaurus_<build-version> ■ For OAW-APAP-324/325—AlcatelAOS-W Instant Hercules_8.7.0.X.0_xxxx ■ For all other OAW-IAPs—AlcatelAOS-W Instant_Orion_<build-version>
`Status`	Indicate the current status of the image upgrade.
`Image Info`	Indicates the source of image.
`Error Detail`	Displays errors generated when an upgrade fails.
`Auto Reboot`	Indicates if automatic rebooting of OAW-IAP is enabled on a successful upgrade.
`Use External URL`	Indicates if an external URL can be used for loading an image file.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show uplink

```
show uplink {config|stats}
```

Description

This command displays uplink configuration details and status of for an OAW-IAP.

Parameter	Description
`show uplink config`	Displays the uplink interface configuration details for an OAW-IAP.
`show uplink stats`	Displays the aggregate uplink statistics for an OAW-IAP.

Example

The following output is displayed for the **show uplink config** command:

```
Uplink preemption            :enable
Uplink enforce               :none
Ethernet uplink eth0         :DHCP
Internet failover            :disable
Max allowed test packet loss:10
Secs between test packets    :30
VPN failover timeout (secs)  :180
```

The output of this command provides the following information:

Column	Description
`Uplink preemption`	Indicates if the uplink preemption is enabled.
`Uplink enforce`	Indicates if any uplinks are enforced.
`Ethernet uplink eth0`	Indicates if Ethernet uplink is configured.
`Max allowed test packet loss`	Indicates an allowed number of test packets that can be lost verifying the Internet availability.
`Secs between test packets`	Indicates the frequency at which the test packets are sent to verify the Internet availability.
`VPN failover timeout (secs)`	Indicates the number of seconds to wait, before trying a different uplink when a VPN tunnel is down.

The following output is displayed for the **show uplink status** command:

```
Uplink preemption            :enable
Uplink enforce               :none
Ethernet uplink eth0         :DHCP
Uplink Table
------------
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     0         Yes
Wifi-sta  INIT   6         No
3G/4G     INIT   7         No

Internet failover            :disable
Max allowed test packet loss:10
Secs between test packets    :30
```

```
VPN failover timeout (secs) :180
ICMP pkt sent          :0
ICMP pkt lost          :0
Continuous pkt lost    :0
VPN down time          :0
```

The output of this command provides the following information:

Column	Description
`Uplink preemption`	Indicates if the uplink preemption is enabled.
`Uplink enforce`	Indicates if any uplinks are enforced.
`Ethernet uplink eth0`	Indicates if Ethernet uplink is configured.
`Type`	Indicates the type of the uplink.
`State`	Indicates the uplink status.
`Priority`	Indicates if any priority levels are assigned to the uplink.
`In Use`	Indicates if the uplink is in use.
`Max allowed test packet loss`	Indicates an allowed number of test packets that can be lost verifying the Internet availability.
`Secs between test packets`	Indicates the frequency at which the test packets are sent to verify the Internet availability.
`VPN failover timeout (secs)`	Indicates the number of seconds to wait, before trying a different uplink when a VPN tunnel is down.
`ICMP pkt sent`	Indicates the number of ICMP packets sent to verify the Internet availability for uplink switchover.
`ICMP pkt lost`	Indicates the number of ICMP packets lost.
`Continuous pkt lost`	Indicates if the packets are lost continuously.
`VPN down time`	Indicates the time since the VPN connection is unavailable.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show uplink-vlan

```
show uplink-vlan
```

Description

This command displays the uplink VLAN configuration details for the management traffic.

The uplink management VLAN configuration allows you to tag management traffic and connect multiple OAW-IAP clusters to the same port on an upstream switch (for example, OmniVista 3600 Air Manager server).

Example

The following output is displayed for the **show uplink-vlan** command:

```
Uplink Vlan Current      :0
Uplink Vlan Provisioned  :
```

The output of this command provides the following information:

Column	Description
`Uplink Vlan Current`	Indicates if the VLAN ID.
`Uplink Vlan Provisioned`	Indicates if the uplink VLAN is provisioned.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show url-visibility

```
show url-visibility [verbose]
```

Description

This command displays the url visibility status of the outstanding user sessions.

Example

The following output is displayed for the **show url-visibility** command:

```
Client URL List
----------------
SrcIP          DstIP          MAC                URL                      URL Length
-----          -----          ---                ---                      ----------
10.17.139.214  104.244.42.5   c4:d9:87:04:6c:c6  t.co                     4
10.17.139.214  216.58.203.131 c4:d9:87:04:6c:c6  google.com.hk            13
10.17.139.214  151.101.1.67   c4:d9:87:04:6c:c6  edition.cnn.com          15
10.17.139.214  216.58.203.131 c4:d9:87:04:6c:c6  google.pl                9
10.17.139.214  172.217.26.201 c4:d9:87:04:6c:c6  blogspot.in              11
10.17.139.214  212.58.246.78  c4:d9:87:04:6c:c6  bbc.co.uk                9
10.17.139.214  216.58.203.131 c4:d9:87:04:6c:c6  google.com.au            13

HTTP Method  Last hit timestamp  HitCount
-----------  ------------------  --------
GET          05:29:23            1
GET          05:28:44            1
GET          05:29:30            1
GET          05:29:36            1
GET          05:29:35            1
GET          05:29:23            1
GET          05:29:36            1

Num of Entries:12
Last URL flash timestamp: 00:00:00
Last flash URL session count: 0
Max URL table size: 2097152 bytes
Current URL count: 7
Current URL size: 426 bytes
```

The output of this command provides the following information:

Column	Description
`SrcIP`	Indicates the source IP.
`DstIP`	Indicates the destination IP.
`MAC`	Indicates the client MAC address.
`URL`	Lists the URL of the session.
`URL Length`	Indicates the length of the URL.
`HTTP Method`	Indicates one of the following methods: ■ Get ■ POST ■ HEAD ■ PUT

Column	Description
	■ Non-HTTP
`Last hit timestamp`	Indicates the last hit timestamp of the URL .
`HitCount`	Indicates the number of hits on the URL.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **MAC**, **HTTP Method**, and **Last hit timestamp** parameters were added.
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show usb

```
show usb
   acl-profile [<profile_name>]
   devices
   profile [<profile_name>]
   status
   supported {vendor-product}
```

Description

This command displays the detailed USB device information on an OAW-IAP.

Parameter	Description
acl-profile [<profile_name>]	Lists the AP USB ACL profiles configured on the OAW-IAP. Specify the profile name to view the **USB rule name** and **USB rule action** configuration on the ACL profile.
devices	Displays the device info of the USB device.
profile [<name>]	Displays the AP USB profile information, such as profile name, ACL profile, and profile binding. Include the profile name when executing this command, to view the details of a single USB profile.
`status`	Displays the status of the cellular devices.
supported {vendor-product}	Displays the list of third party USB devices that are supported by the AP.

Examples

The following sample shows the output of the **show usb acl-profile** command:

```
(Instant AP)# show usb acl-profile
AP USB ACL Profile
------------------
Profile Name
------------
sample-acl-profile-1
sample-acl-profile-2
```

The following sample shows the output of the **show usb acl-profile <profile_name>** command:

```
(Instant AP)# show usb acl-profile sample-acl-profile-1
AP USB ACL Profile
------------------
USB rule name  USB rule action
-------------  ---------------
Hanshow         permit
```

The following sample shows the output of the **show usb profile** command:

```
(Instant AP)# show usb profile
AP USB Profile
--------------
Profile Name            ACL Profile             Binding
------------            -----------             -------
sample-profile-1        sample-acl-profile-1    Yes
sample-profile-2        sample-acl-profile-2    No
```

The following example shows the output of the **show usb status** command:

```
(Instant AP)(config)# show usb status
```

```
Cellular Status
---------------
card      detect     link       SIM PIN
----      ------     ----       -------
Present   detect-ok  Linkup     N/A

USB Modem Information
---------------------
Parameter                       Value
---------                       ------
Manufacturer                    Linux
Product                         OHCI Host Controller
Serial Number                   0000:00:04.0
Driver                          hub
Vendor ID                       1d6b
Product ID                      0001
Manufacturer
Product                         USB2.0 Hub
Serial Number
Driver                          hub
Vendor ID                       05e3
Product ID                      0608
Manufacturer                    ZTE, Incorporated
Product                         ZTE Wireless Ethernet Adapter
Serial Number                   MF8310ZTED000000
Driver                          option
Vendor ID                       19d2
Product ID                      1405
Model                           MF831
Supported Network Services      LTE WCDMA GSM
Firmware Version                BD_MF831HDV1.0.0B02
ESN Number                      862828022611876

Cellular Link Status
--------------------
Parameter                       Value
---------                       ------
USB Modem State                 Active
USB Uplink RSSI (in dBm)        -69
Current Network Service         4G-LTE
plugin counter  :               0
plugout counter :               0
```

The following example shows the output of the **show usb supported vendor-products** command:

```
(Instant AP)# show usb supported vendor-products
Supported USB Device
--------------------
Vendor-Product
--------------
All
Solu-M-SLG-DM101
HanShow
SES-Imagotag-021
Sierra-881U
Sierra-Compass-885
Globetrotter-ICON-322
Huawei-E170-E272-E220
Sierra-305-308
Sierra-330U
Sierra-250U
Pantech-UM150
Pantech-UM175
```

```
Pantech-UM190
Utstarcom-UM100C
ZTE-AC3781
Icon-452
Sierra-Compass-597
Huawei-E1762
Huawei-E1820e
Sierra-598
Novatel-Ovation-U727
Franklin-U300
Franklin-U301
Franklin-U600
Novatel-U760-Sprint
Novatel-U760-Virgin
Novatel-U727
Novatel-U720
Novatel-MiFi-2200
UGM1831
UMG181
ZTE-MF110
ZTE-Fivespot
Huawei-E367
Huawei-K4505
Huawei-E160
ZTE-MF637-MF656
ZTE-MF190-Egypt
ZTE-MF190-Thailand
ZTE-MF633-MF636
ZTE-MF190-India
Longcheer-WM72
Sierra-Tstick-C597
Huawei-E220
Sierra-885
Sierra-306-308-503-312U
Sierra-320U
Huawei-E176-E176G-E1553
Huawei-E180-E1692-E1762
Huawei-E3765
Huawei-E1552
Huawei-E1750
Huawei-E3765
Huawei-E352s-5
Huawei-E173
Huawei-e398
Huawei-E180
Huawei-EC150
Huawei-E1731-177DT06
Huawei-E169-E180-E220-E272
Huawei-D41HW
Huawei-E353
Huawei-KDDI-DATA07
Huawei-EC167
Globetrotter-ICON-225
ZTE-MF820D
C-motech-CNU-680
Novatel-MC545
Qualcomm-SXC-1080
ZTE-AC2726
ZTE-AC2736
EpiValley-SEC-8089
ZTE-K4505-z
ZTE-MF668
NTT-DoCoMo-L-08C
```

```
NTT-DoCoMo-L-02C
NTT-DoCoMo-L-05A
NTT-DoCoMo-L-02A
ZTE-MF820
ZTE-3565
ZTE-MF180-HSDPA
ZTE-MF683-HSDPA
ZTE-MF591
SIMTech
Fujisoft
Huawei-E392
Huawei-K3772
Huawei-K3770
Huawei-E157
Huawei-E261
Huawei-E353-E1750-E367
Huawei-K4605
Huawei-E3272s-153
Huawei-E3131
Huawei-K4510
Huawei-K4605
Pantech-UML290
Pantech-UML295
Novatel-MC551L
Novatel-U620L
Fraklin-u770-u772
Netgear-340u
Netgear-341u
Alcatel-L800
Sierra-313u
Huawei-HWD12-LTE
Huawei-3276s-150
Huawei-E3372
Huawei-K5150
Huawei-K5160
Huawei-E8372
ZTE-MF832U
ZTE-MF832U-Zero
ZTE-MF832S
ZTE-MF825C
ZTE-MF831
ZTE-MF79S
ZTE-MF823
Huawei-E3276s-500
Huawei-E3276
Pantech-UML295-cold
Huawei-E3372h-153-modem
Huawei-E3372h-153-hilink
Amberbox-detector
Amberbox-gateway
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode

show usb status

```
show usb status
```

Description

This command displays the status of the cellular modem link on the OAW-IAP, the USB devices connected to an OAW-IAP, and the USB and ACL profiles configured on the OAW-IAP.

Example

The following example shows the output of the **show usb status** command:

```
(Instant AP)(config)# show usb status
Cellular Status
---------------
card       detect     link       SIM PIN
----       ------     ----       -------
Present    detect-ok  Linkup     N/A

USB Modem Information
---------------------
Parameter                       Value
---------                       ------
Manufacturer                    Linux
Product                         OHCI Host Controller
Serial Number                   0000:00:04.0
Driver                          hub
Vendor ID                       1d6b
Product ID                      0001
Manufacturer
Product                         USB2.0 Hub
Serial Number
Driver                          hub
Vendor ID                       05e3
Product ID                      0608
Manufacturer                    ZTE, Incorporated
Product                         ZTE Wireless Ethernet Adapter
Serial Number                   MF8310ZTED000000
Driver                          option
Vendor ID                       19d2
Product ID                      1405
Model                           MF831
Supported Network Services      LTE WCDMA GSM
Firmware Version                BD_MF831HDV1.0.0B02
ESN Number                      862828022611876

Cellular Link Status
--------------------
Parameter                       Value
---------                       ------
USB Modem State                 Active
USB Uplink RSSI (in dBm)        -69
Current Network Service         4G-LTE
plugin counter  :               0
plugout counter :               0
```

The output of this command includes the following parameters:

Parameters	Description
`card`	Indicates if the cellular cards are currently configured on the OAW-IAP.
`detect`	Indicates if cellular modems are detected on the OAW-IAP.
`link`	Indicates the current status of cellular link.
`SIM PIN`	Displays the SIM PIN of the model.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were added: ■ **plugin counter** ■ **plugout counter**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show users

```
show user [portal| Radius]
```

Description

This command displays users configured for an OAW-IAP.

Parameter	Description
`portal`	Displays the OAW-IAP user credentials.
`radius`	Displays the user credentials for the RADIUS server authentication

Examples

The following output is displayed for the **show user** command:

```
show user
User Table
----------
Name  Password  Attribute
----  --------  ---------
d8:c7:c8:cb:d4:20# show user portal
Portal User Table
-----------------
Name  Password
----  --------
d8:c7:c8:cb:d4:20# show user radius
Radius User Table
-----------------
Name  Password
----  --------
```

The output of this command provides the following information:

Column	Description
`Name`	Indicates the username of the OAW-IAP, portal, and the RADIUS users.
`Password`	Indicates the password details of the users.
`Attribute`	Indicates the attributes

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show valid-channels

```
show valid-channels
```

Description

This command displays the list of channels that are valid for an OAW-IAP serving a specific regulatory domain.

Example

The following example shows the output of **show valid-channels** command:

```
2.4 GHz
1
2
3
4
5
6
7
8
9
10
11
12
13
1+
2+
3+
4+
5+
6+
7+
5.0 GHz
36
40
44
48
52
56
60
64
149
153
157
161
165
36+
44+
52+
60+
149+
157+
```

The output of this command provides the following information:

Parameter	Description
`2.4 GHz`	Displays the list of channels valid for an OAW-IAP in the 2.4 GHz band.
`5.0 GHz`	Displays the list of channels valid for an OAW-IAP in the 5 GHz band.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show valid-channels dual-5ghz-mode

```
show valid-channels dual-5ghz-mode
```

Description

This command displays the list of channels that are valid for an OAW-IAP that has dual 5 GHz mode enabled.

Example

The following example shows the output of **show valid-channels dual-5ghz-mode** command:

```
c8:b5:ad:c3:ab:dc# show valid-channels dual-5ghz-mode
Radio 0
100
104
108
112
116
120
124
128
132
136
140
144
149
153
157
161
165
100+
108+
116+
124+
132+
140+
149+
157+
100E
116E
132E
149E
100S
Radio 1
36
40
44
48
52
56
60
64
36+
44+
52+
60+
36E
52E
36S
c8:b5:ad:c3:ab:dc#
```

The output of this command provides the following information:

Parameter	Description
`Radio 0`	Displays the list of upper channel valid for an OAW-IAP in dual 5 GHz mode.
`Radio 1`	Displays the list of lower channels valid for an OAW-IAP in dual 5 GHz mode.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-AP-344/OAW-AP-345	Privileged EXEC mode

show version

```
show version
```

Description

This command displays the AOS-W Instant software version running on an OAW-IAP.

Example

The following example shows the output of the **show version** command:

```
Alcatel-Lucent Operating System-Wireless.
AOS-W (MODEL: OAW-AP105), Version 6.4.3.1-4.2.0.0
Website: http://enterprise.alcatel-lucent.com/
All Rights Reserved (c) 2005-2015, Alcatel-Lucent.
Compiled on 2015-08-05 at 02:11:11 PDT (build 51112) by p4build
FIPS Mode :disabled
AP uptime is 18 hours 55 minutes 44 seconds
Reboot Time and Cause: AP rebooted Thu Jan 1 12:54:27 UTC 2015; Image Upgrade Successful
```

The output of this command provides the following information:

Parameter	Description
`Version`	Indicates the version of OAW-IAP software.
`Reboot Time and Cause`	Indicates the reason for which the OAW-IAP was last rebooted and the reboot time.
`Model`	Indicates the OAW-IAP model.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show vlan

```
show vlan [mapping]
```

Description

This command displays the mapping of a VLAN name and its corresponding VLAN ID in an SSID profile.

Example

The following example shows the output of **show vlan mapping** command:

```
Vlan Mapping Table
------------------
VLAN Name  VLAN ID
---------  -------
myvlan     30
```

The output of this command provides the following information:

Parameter	Description
`VLAN Name`	Displays the configured VLAN name for an SSID profile.
`VLAN ID`	Displays the configured VLAN ID for an SSID profile.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show vpn

```
show vpn {config|status|tunnels}
```

Description

This command displays the status and configuration details for VPN-enabled OAW-IAPs.

Syntax

Parameter	Description
config	Displays configuration details for the VPN-enabled OAW-IAPs.
status	Displays the status of the VPN connections enabled on an OAW-IAP.
tunnels	Displays the IAP-VPN retry counter statistics.

Example

The following example shows the output displayed for **show vpn config** command:

```
Concentrator
------------
Type                        Value
----                        -----
VPN Primary Server
VPN Backup Server
VPN Preemption              disable
VPN Fast Failover           disable
VPN Hold Time               600
VPN Monitor Pkt Send Freq   5
VPN Monitor Pkt Lost Cnt    2
VPN Ikepsk
VPN Username
VPN Password                95a5624fbf08dfb3e794ac2c6686e330
GRE outside vpn             disable
GRE Server
GRE IP Address              0.0.0.0
GRE Type                    1
GRE Per AP Tunnel           disable
Reconnect User On Failover  disable
Reconnect Time On Failover  60
Routing Table
-------------
Destination  Netmask  Gateway  Type
-----------  -------  -------  ----
```

The output displayed for this command provides information on the parameters configured for the VPN concentrator.

For more information on the VPN configuration parameters, see the following commands:

- vpn primary
- vpn backup
- vpn preemption
- vpn fast-failover
- vpn gre-outside
- vpn hold-time

- vpn monitor-pkt-lost-cnt
- vpn monitor-pkt-send-freq
- vpn ikepsk
- gre

The following example shows the output displayed for **show vpn status** command:

```
profile name:default
--------------------------------------------------
current using tunnel                            :unselected tunnel
ipsec is preempt status                         :disable
ipsec is fast failover status                   :disable
ipsec hold on period                            :600
ipsec tunnel monitor frequency (seconds/packet) :5
ipsec tunnel monitor timeout by lost packet cnt :2
ipsec     primary tunnel crypto type            :Cert
ipsec     primary tunnel peer address           :N/A
ipsec     primary tunnel peer tunnel ip         :N/A
ipsec     primary tunnel ap tunnel ip           :N/A
ipsec     primary tunnel current sm status      :Init
ipsec     primary tunnel tunnel status          :Down
ipsec     primary tunnel tunnel retry times     :0
ipsec     primary tunnel tunnel uptime          :0
ipsec      backup tunnel crypto type            :Cert
ipsec      backup tunnel peer address           :N/A
ipsec      backup tunnel peer tunnel ip         :N/A
ipsec      backup tunnel ap tunnel ip           :N/A
ipsec      backup tunnel current sm status      :Init
ipsec      backup tunnel tunnel status          :Down
ipsec      backup tunnel tunnel retry times     :0
ipsec      backup tunnel tunnel uptime          :0
```

The **show vpn status** command displays the current status of VPN connection, IP address configured for VPN or IPsec connections, and the tunnel details.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.4.0.2-4.1.0.0	The **tunnels** keyword added.
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	Command output modified.
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show vpn tunnels

```
show vpn tunnels
```

Description

This command shows VPN tunnel information for the OAW-IAP.

Parameter	Description
`Source IP`	Displays the source IP address of the VPN tunnel.
`Destination IP`	Displays the destination IP address of the VPN tunnel.
`End IP`	Displays the end IP address of the VPN tunnel.
`Default GW`	Displays the default gateway address of the VPN tunnel.
`Use count`	Displays the use count value.
`Ifindex`	Displays the VPN index value
`Ifname`	Displays the VPN tunnel name
`Flags`	Displays the VPN flag type.
`Retry count for Register Request`	Displays the retry count for the registration request.
`GRE Encap/Decap`	Displays the encapsulation or decapsulation counters of GRE tunnel.
`Retry count for Vlan Add Request`	Displays the VLAN addition request count.
`Old Subnet Status`	Displays the previous subnet status.
`Existing Subnet Status`	Displays the current subnet status.

Example

The following example shows the output of **show vpn-tunnels** command:

```
Tunnel Flags: M = Master IAP; S = Slave IAP; Primary = Primary Tunnel
B = Backup Tunnel; R = Registered; H = Heartbeat Enable
Tunnel Info for peer address  172.16.0.254
-------------------------------------------
Type                               Value
----                               -----
Source IP                          3.6.9.2
Destination IP                     172.16.0.254
End IP                             10.17.140.252
Default GW                         10.17.140.238
Use count                          0
Ifindex                            15
Ifname                             tun0
Flags                              MPR
Retry count for Register Request   0
GRE Encap/Decap                    0/0
For DHCP Profile                   aaa-dhcp
Retry count for Vlan Add Request  0
Old Subnet Status                 Normal
Existing Subnet Status            Normal
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	**GRE Encap/Decap** parameter was introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platforms	Command Mode
All platforms	Privileged EXEC mode

show walled-garden

```
show walled-garden
```

Description

This command displays the domain names and websites that are blacklisted or whitelisted by an OAW-IAP.

A walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the “allowed” websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. This works for client devices with or without HTTP proxy settings.

When a user attempts to navigate to other websites, which are not in the whitelist of the walled garden profile, the user is redirected to the login page. In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Example

The following example shows the output of **show walled-garden** command:

```
White List
----------
Domain Name
-----------
example.com
Black List
----------
Domain Name
-----------
example2.com
```

The output of this command provides the following information:

Parameter	Description
`Domain Name`	Displays the blacklisted or whitelisted domain names and URLs.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show wifi-uplink

```
show wifi-uplink { auth | config | status | config no-encrypt | debug | stats | neighbors |
candidates | blacklist | connection-history | connection-trace }
```

Description

This command displays the configuration details, status, connection information, and logs for Wi-Fi uplink configured on an OAW-IAP.

Parameter	Description
`auth`	Displays the authentication log.
`blacklist`	Displays the details of failed uplink associations.
`candidates`	Displays the list of candidate APs that match the ESSID configured in the wlan station profile.
`config`	Displays the Wi-Fi uplink configuration parameters enabled on an OAW-IAP.
`config no-encrypt`	Displays the Wi-Fi uplink configuration parameters enabled on an OAW-IAP with the passphrase unmasked.
`connection-history`	Displays the connection history of Wi-Fi uplink.
`connection-trace`	Displays the connection log between the Instant Access Point and the wireless network for Wi-Fi uplink.
`debug`	Displays debugging information for the Wi-Fi uplink.
`mat-table`	Displays the MAC address translation table of connected clients.
`neighbors`	Displays the information of nearby scanned wireless networks.
`stats`	Displays the statistics information of the Wi-Fi uplink.
`status`	Displays the status of the Wi-Fi uplink connection.

Example

show wifi-uplink auth

The following output is displayed for the **show wifi-uplink auth** command:

```
----------------------------------------------------------------------
wifi uplink auth log:
----------------------------------------------------------------------
[1536]2013-05-08 23:42:06.647: Global control interface '/tmp/supp_gbl'
```

show wifi-uplink config no-encrypt

The following output is displayed for the **show wifi-uplink config** command:

```
ESSID           :Wifi
Cipher Suite    :wpa-tkip-psk
Passphrase      :test1234
Band            :dot11a
```

The output for this command displays the following information:

Parameter	Description
`ESSID`	Displays the name of the network for which the Wi-Fi uplink is configured.
`Cipher Suite`	Displays the encryption settings configured for the Wi-Fi uplink. For example, wpa-tkip-psk or wpa2-ccmp-psk.
`Passphrase`	Displays the WPA passphrase configured for the Wi-Fi uplink.
`uplink-band <band>`	Displays the band configured for the Wi-Fi uplink connection. For example, dot11a and dot11g.

show wifi-uplink status

The following output is displayed for the **show wifi-uplink status** command:

```
# show wifi-uplink status
Configured                      :YES
Enabled                         :YES
State                           :UP
Interfaces                      :aruba000
Now                             :2019-12-24 20:07:11
SSID                            :test-5G
BSSID                           :88:bf:e4:6b:69:03
Unicast/Multicast Encryption    :wpa2-aes-psk wpa2-aes-psk
Link Health                     :100
AID                             :8
IP Address                      :192.168.8.151
Subnet Mask                     :255.255.255.0
Gateway                         :192.168.8.1
Associated Time                 :49s
Associated AP Beacon Time       :1d:0h:27m:8s
Channel                         :36E
RSSI                            :15
Noise Floor                     :98
Phy                             :5GHz-VHT-80sgi-1ss
Maximum Speed (mbps)            :433
Overall/Tx/Rx Goodput (mbps)    :0 0 0
Last Tx Timestamp               :2019-12-24 20:07:11
Last Rx Timestamp               :2019-12-24 20:07:11
Last Tx Rate (mbps)             :390
Last Rx Rate (mbps)             :263
Last ACK RSSI                   :18
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The **IP address**, **Subnet mask**, and **Gateway** information of the layer 3 network were added to the output of **show wifi-uplink status** command.
AOS-W Instant 8.5.0.0	The following parameters were added: ■ **config no-encrypt** ■ **debug** ■ **stats** ■ **neighbors** ■ **candidates** ■ **blacklist** ■ **connection-history**

Release	Modification
	- **connection-trace** The **auth log** parameter is replaced by **auth**.
AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show wired-port

```
show wired-port <profile-name>
```

Description

This command displays the configuration details associated with a wired profile configured on an OAW-IAP.

Parameter	Description
<profile-name>	Displays the current configuration details for a specific wired profile.

Example

The following example shows the output of the **show wired-port <profile-name>** command:

```
Name                   :default_wired_port_profile
VLAN Mode              :Trunk
Allowed VLANs          :all
Native VLAN            :1
Admin Status           :Down
Role                   :default_wired_port_profile
Speed                  :auto
Duplex                 :full
POE                    :No
Type                   :employee
Content Filtering      :Disabled
Server Load Balancing  :Disabled
MAC Authentication     :Disabled
8021.x                 :Disabled
L2 Auth Fallthrough    :Disabled
Captive Portal         :disable
Exclude Uplink       :none
Access Control Type    :Network
Uplink enable          :Disabled
Certificate Installed: :No
Internal Radius Users:  :0
Internal Guest Users:  :0
Role Derivation Rules
---------------------
Attribue  Operation  Operand  Role Name  Index
--------  ---------  -------  ---------  -----
Vlan Derivation Rules
---------------------
Attribue  Operation  Operand  Vlan Id
--------  ---------  -------  -------
RADIUS Servers
--------------
Name  IP Address  Port  Key  Timeout  Retry Count  NAS IP Address  NAS Identifier  RFC3576
----  ----------  ----  ---  -------  -----------  --------------  --------------  -------
LDAP Servers
------------
Name  IP Address  Port  Timeout  Retry Count  Admin-DN  Admin Password  Base-DN
----  ----------  ----  -------  -----------  --------  --------------  -------
Access Rules
------------
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport)  Action  Log  TOS  802.1P
Blacklist  Mirror  DisScan
-------  ---------  ----------  -------------------------  ------  ---  ---  ------  --------
-  ------  -------
any      any        match       any                        permit
```

```
Vlan Id            :0
ACL Captive Portal:disable
:Captive Portal Configuration
Background Color:13421772
Banner Color        :16750848
Decoded Texts       :
Banner Text         :Welcome to Guest Network
Use Policy          :Please read terms and conditions before using Guest Network
Terms of Use        :This network is not secure, and use is at your own risk
Internal Captive Portal Redirect URL:
Captive Portal Mode:Acknowledged
Custom Logo
:External Captive Portal Configuration
Server:localhost
Port                :80
URL                 :/
Authentication Text:Authenticated
External Captive Portal Redirect URL:
Server Fail Through:No
```

The output of this command shows the configuration parameters associated with the selected wired profile and the value assigned for each of these parameters:

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show wired-port-settings

```
show wired-port-settings
```

Description

This command displays the list of wired profiles configured on an OAW-IAP.

Example

The following example shows the output of **show wired-port-settings** command:

```
Wired Port Profiles
-------------------
Name          VLAN Mode Allowed VLANs Native VLAN  Admin Status  Role           Speed
----          --------- ------------- -----------  ------------  ----           ----
wiredProf1    Access     all          guest        Up            wired-instant  auto
WiredProf2    Trunk      all            1          Down          WiredProf2     auto

Duplex  POE  In Use  Authentication Method Trusted
-----  -----   ----  ---------------------------     -------
auto    Yes  Yes     None Yes
full    No   Yes     None No

Port Profile Assignments
------------------------
Port  Profile Name
----  ------------
0     default_wired_port_profile
1     example1-crash
2     wired-instant
3     wired-instant
4     wired-instant
```

The output of this command provides the following information:

Column	Description
`Name`	Indicates the name of the wired port profile.
`VLAN Mode`	Indicates the name of switchport mode for the wired profiles. The VLAN modes can be **Access** or **Trunk**.
`Allowed VLAN`	Indicates the list of allowed VLANs. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
`Native VLAN`	Indicates the values assigned for Native VLAN. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN.
`Admin Status`	Indicates the status of admin port.
`Role`	Indicates the role assigned to the wired profile users.
`Speed`	Indicates the speed of wired client traffic.
`duplex`	Indicates if the client traffic duplexing full, half, or automatically assigned based on the capabilities of the client, the OAW-IAP, and the cable.
`poe`	Indicates if PoE is enabled.

Column	Description
`In Use`	Indicates if the wired profile is in use.
`Authentication Method`	Indicates the authentication method configured for the wired profile.
`Trusted`	Indicates if a trusted port is supported in an OAW-IAP.
`Port`	Indicates the port number to which a wired profile is assigned.
`Profile`	Indicates the name of wired profile assigned to a wired port.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **Trusted** parameter was introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show wispr config

```
show wispr config
```

Description

This command displays the WISPr authentication parameters configured on an OAW-IAP.

Example

The following example shows the output of **show wispr config** command:

```
WISPr ISO Country Code   :91
WISPr E.164 Country Code :IN
WISPr E.164 Area Code    :80
WISPr SSID               :Network1
WISPr Operator Name      :XYZ
WISPr Location Name      :airport
```

The output of this command provides the following information:

Parameter	Description
`WISPr ISO Country Code`	Indicates the ISO country code configured for WISPr authentication.
`WISPr E.164 Country Code`	Indicates the E.164 Country Code for the WISPr Location ID.
`WISPr E.164 Area Code`	Indicates the E.164 Area Code for the WISPr Location ID.
`WISPr SSID`	Indicates the SSID for which the WISPr authentication profile is configured.
`WISPr Operator Name`	Indicates the hotspot operator profile associated with the WISPr authentication profile.
`WISPr Location Name`	Indicates Hotspot location associated with the WISPr profile.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show xml-api-server

```
show xml-api-server config
```

Description

This command displays the XML API server configuration details.

Example

The following example shows the output of the **show xml-api-server** command:

```
ip :192.0.2.5
key :user1234
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

show zigbee service-profile

```
show zigbee service-profile [<service-profile>]
```

Description

This command shows the ZigBee service profile.

Parameter	Description
`<service-profile>`	Name of the ZigBee service profile.

Example

The following example shows the output for the **show zigbee service-profile** command:

```
(Instant AP)# show zigbee service-profile

ZigBee Service Profile List
---------------------------
Name                         References  Profile Status
----                         ----------  --------------
sample_zb_service_profile    0

Total:1
```

The following example shows the output for the **show zigbee service-profile <service_profile>** command:

```
(Instant AP)# show zigbee service-profile sample_zb_service_profile
```

```
ZigBee Service Profile "sample_zb_service_profile"
--------------------------------
Parameter              Value
---------              -----
Radio Instance         all
Zigbee Security        enable
Zigbee Permit Joining  on
PANID                  auto
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

show zigbee socket-device-profile

```
show zigbee socket-device-profile [profile_name]
```

Description

This command shows the ZigBee socket device profile(s).

Parameter	Description
`[profile_name]`	Name of the ZigBee socket device profile.

Example

The following example shows the output for the **show zigbee socket-device-profile** command:

```
Zigbee Socket Device Profile List
---------------------------------
Name References Inbound Sockets Outbound Sockets
---- ---------- --------------- ----------------
zsd  2          1               3
zsd2 1          1               0
------------
Total:2
```

The following example shows the output for the **show zigbee socket-device-profile <profile_name>** command:

```
80:8d:b7:c0:08:3d# show zigbee socket-device-profile zsd
Name :zsd
References :2
------------
Zigbee Socket List
------------------
Direction Source Endpoint Destination Endpoint Destination Profile Destination Cluster APS
Ack
--------- --------------- -------------------- ------------------- ------------------- ------
-
inbound         1               1                       1234        5678            n/a
outbound        1               1                       7abc        fc00            yes
outbound        1               1                       7fff        00ff            no
outbound        2               2                       0002        0002            yes
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

snmp-server

```
snmp-server
   community <address>
   engine-id <engineID>
   host <ipaddr> version {1 <name> udp-port <port>}|{2c|3 <name> [inform] [udp-port <port>]}
   user <name> <auth-prot> <password> <priv-prot> <password>
```

Description

This command configures SNMP parameters.

Parameter	Description	Range	Default
`community`	Sets the read-only community string.	—	—
`engine-id`	Sets the SNMP server engine ID as a hexadecimal number.	24 characters maximum	—
`host <ipaddr>`	Configures the IP address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the switch.	—	—
`version`	Configures the SNMP version and security string for notification messages.	1,2c,3	—
`inform`	Sends SNMP inform messages to the configured host.	—	—
`udp-port`	Indicates the port number to which notification messages are sent.	—	162
`user`	Configures an SNMPv3 user profile for the specified username.	—	—
`auth-prot`	Indicates the authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol or HMAC-SHA-98 Digest Authentication Protocol, and the password to use with the designated protocol.	MD5/SHA	SHA
`priv-prot`	Indicates the privacy protocol for the user and the password to use with the designated protocol. CBC-DES Symmetric Encryption Protocol is the default option.	DES	DES

Example

The following example configures an SNMP host and community string:

```
(Instant AP)(config)# snmp-server community user123
(Instant AP)(config)# snmp-server host 10.0.0.1 version 2c  udp-port 162 inform
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

speed test

```
speed-test
   bandwidth <bandwidth>
   include-reverse
   omit
   on-boot
   parallel
   protocol [<tcp>|<udp>]
   sec-to-measure <secs>
   server-ip <server>
   server-port <port>
   time-interval <interval>
   window
   no...
```

Description

This command enables the user to configure an Iperf3 client on the Virtual Controller to run each time the OAW-IAP boots up and additionally configure time intervals at which it is executed periodically.

Parameter	Description	Range	Default
`speed test`	Enables **speed-test** configuration sub-mode for speed-test profile configuration.	—	—
`bandwidth <bandwidth>`	Configures the bandwidth length in Mbps.	—	—
`include-reverse`	The direction of traffic is reversed and sent from the server to the client. This option enables Iperf to run the speed test for an extended duration.	—	—
`omit`	Enter the number of initial seconds to omit.	1–5	–
`on-boot`	Configures the OAW-IAP to run the speed test during boot up.	—	—
`parallel`	Enter the number of parallel client streams.	1–30	—
`protocol [<tcp>|<udp>]`	Configures the speed test profile to be executed using the UDP or TCP protocol.	—	tcp
`sec-to-measure <secs>`	Configures the duration of the speed test.	0–20 seconds	10 seconds
`server-ip <server>`	Denotes the IP address of the Iperf server which is used to run the speed test.	—	—

Parameter	Description	Range	Default
`server-port <port>`	Denotes the server port that the client needs to connect to execute the speed test.	—	5201
`time-interval <internal>`	Configures a time interval (in seconds) to run the speed test on a regular basis. The minimum time interval is 60 seconds.	—	—
`window`	Indicates the TCP window size or socket buffer size sent to the server while running speed test.	64000–16384000	—
`no`	Removes the speed-test profile configuration.	—	—

Examples

The following example configures the speed test profile:

```
(Instant AP)(config)# speed-test
(Instant AP)(speed-test)# server-ip 10.17.138.2
(Instant AP)(speed-test)# server-port 5201
(Instant AP)(speed-test)# sec-to-measure 20
(Instant AP)(speed-test)# include-reverse
(Instant AP)(speed-test)# omit 5
(Instant AP)(speed-test)# parallel 10
(Instant AP)(speed-test)# protocol udp
(Instant AP)(speed-test)# bandwidth 100
(Instant AP)(speed-test)# time-interval 600
(Instant AP)(speed-test)# window 1
(Instant AP)(speed-test)# end
(Instant AP)(speed-test)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **omit** , **parallel**, and **window** parameters were introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and speed test configuration sub-mode.

speed test <server>

```
speed-test {<server> <protocol> [<bandwidth> | <include-reverse> | <omit> | <parallel> |
<sec-to-measure> | <server-port> | <window>]}
```

Description

This command enables the user to run a speed test on the Iperf server at any point in time. The speed test configuration is not saved and can be executed only once.

Parameter	Description	Range	Default
`server`	Enter the IP address of the Iperf server on which the speed test needs to be run.	—	—
`protocol [<tcp>|<udp>]`	Enter the protocol type used for executing the speed test.	—	tcp
`bandwidth <bandwidth>`	Enter the bandwidth length in Mbps.	—	—
`include-reverse`	The direction of traffic is reversed and sent from the server to the client. This option enables Iperf to run the speed test for an extended duration.	—	—
`omit`	Enter the number of initial seconds to omit.	1–5	—
`parallel`	Enter the number of parallel client streams.	1–30	—
`sec-to-measure <secs>`	Specify a duration (in secs) for the speed test.	0-20 secs	10 secs
`server-port <port>`	Enter the server port that the client needs to connect to execute the speed test.	—	5201
`window`	Indicates the TCP window size or socket buffer size sent to the server while running speed test.	64000–16384000	—

Examples

The following example runs a speed test on the Iperf server:

```
(Instant AP)# speed-test 10.17.138.2 udp bandwidth 100 sec-to-measure 20 server-port 5201
parallel 12 omit 2 window 1
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **omit** , **parallel**, and **window** parameters were introduced.
Alcatel-Lucent AOS-W Instant 8.3.0.0	This command is introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

split-5ghz-mode

```
split-5ghz-mode <enabled | disabled>
no...
```

Description

This command configures split 5Ghz mode on the OAW-IAP. Use this command to split the 8x8 5Ghz radio into two 4x4 5Ghz radios operating on the upper and lower bands of the 5Ghz radio antenna.

Parameter	Description
`enabled`	Enables split 5Ghz radio on the OAW-IAP.
`disabled`	Disables split 5Ghz radio on the OAW-IAP.
`no...`	Removes the configuration.

Example

The following example enables split 5 Ghz radio on the OAW-IAP:

```
(Instant AP)#config
(Instant AP)(config)#split-5ghz-mode enabled
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-550 Series access points	Configuration mode

ssh

```
ssh
   disable-ciphers {aes-cbc | aes-ctr}
   no...
```

Description

This command configures ciphers for SSH connection to an OAW-IAP.

The SSH server supports AES-CBC and AEC-CTR ciphers. Use this command if you want to disable one of the ciphers. This configuration is applicable only to non-FIPS builds.

Parameter	Description	Range	Default
`disable-ciphers`	Disables cipher authentication for SSH. Specify the cipher to be disabled.	—	—
`aes-cbc`	Disables AES-CBC authentication for SSH. This parameter enables the AES-CTR encryption.	—	—
`aes-ctr`	Disables AES-CTR authentication for SSH. This parameter enables the AES-CBC encryption.	—	—
`no`	Enables the disabled cipher encryptions on the SSH server:	—	—

Examples

The following command enables AES-CBC and disables AES-CTR on the SSH server:

```
(Instant AP)(config) #ssh disable-ciphers aes-ctr
```

The following command enables the disabled cipher encryptions on the SSH server:

```
(Instant AP)(config) #no ssh disable-ciphers
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

subscription-ap

```
subscription-ap <MAC-address> status <status>
no…
```

Description

This command configures the subscription status for an OAW-IAP.

Parameter	Description	Range	Default
`<MAC-address>`	Enter the MAC address of the OAW-IAP.	—	—
`<status>`	Enter the subscription status for the OAW-IAP.	—	—
`no…`	Removes the configuration.	—	—

Example

```
(Instant AP)(config) # subscription-ap a1:b2:c3:d4:42:98 status
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

subscription-ap-enable

```
subscription-ap-enable
no…
```

Description

This command enables the subscription of an OAW-IAP.

Parameter	Description	Range	Default
`subscription-ap-enable`	Enables the subscription for an OAW-IAP.	—	—
`no`	Removes the configuration.	—	—

Example

```
(Instant AP)(config) # subscription-ap-enable
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

swarm-mode

```
swarm-mode <mode>
```

Description

This command allows you to provision an OAW-IAP in the standalone or cluster mode.

When an OAW-IAP is converted to the standalone mode, it cannot join a cluster of OAW-IAPs even if the OAW-IAP is in the same VLAN. If the OAW-IAP is in the cluster mode, it can form a cluster with other Virtual Controller OAW-IAPs in the same VLAN.

Parameter	Description	Range	Default
`<mode>`	Provisions the OAW-IAP in the standalone or cluster mode. The **swarm-mode standalone** command converts the OAW-IAP to the standalone mode, whereas the **swarm-mode cluster** command converts it to the cluster mode.	Standalone or Cluster	—

Example

The following command allows you to convert an OAW-IAP to a standalone OAW-IAP:

```
(Instant AP)# swarm-mode standalone
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

syslocation

```
syslocation <syslocation>
no…
```

Description

This command allows you to define the physical location for the OAW-IAP.

Parameter	Description	Range	Default
`<syslocation>`	Allows you to specify a physical location.	—	—
`no`	Removes the configuration.	—	—

Example

The following example sets the physical location of the OAW-IAP to Sunnyvale:

```
(Instant AP)(config) # syslocation <Sunnyvale>
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

syslog-level

```
syslog-level <level> {ap-debug|network|security|system|user|user-debug|wireless}
no...
```

Description

This command configures syslog facility levels. Syslog Facility is an information field associated with a syslog message.

Parameter	Description	Range	Default
`syslog-level <level>`	Configures the Syslog facility level. You can configure any of the following logging levels: ■ Emergency—Panic conditions that occur when the system becomes unusable. ■ Alert—Any condition requiring immediate attention and correction. ■ Critical—Any critical conditions such as a hard drive error. ■ Errors—Error conditions. ■ Warning—Warning messages. ■ Notice—Significant events of a non-critical and normal nature. The default value for all Syslog facilities. ■ Informational—Messages of general interest to system users. ■ Debug—Messages containing information useful for debugging.	Emergency, Alert, Critical, Errors, Warning, Notice, Informational, Debug	Notice
`ap-debug`	Generates a log for the OAW-IAP device for debugging purposes.	—	—
`network`	Generates a log when there is a change in the network, for example, when a new OAW-IAP is added to a network.	—	—
`security`	Generates a log for network security, for example, when a client connects using wrong password.	—	—
`system`	Generates a log about the system configuration and status.	—	—
`user`	Generates a log for the OAW-IAP clients.	—	—
`user-debug`	Generates a detailed log about the clients for debugging purposes.	—	—
`wireless`	Generates a log about radio configuration.	—	—
no...	Removes the configuration.	—	—

Example

The following example configures syslog facility levels for ap-debug and user-debug:

```
(Instant AP)(config)# syslog-level error ap-debug
(Instant AP)(config)# end
```

```
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

syslog-server

```
syslog-server <ip-address> <ip address 2> <ip-address 3>
no…
```

Description

This command configures Syslog servers for an OAW-IAP to which the AP will periodically send system logs. Up to 3 syslog servers can be configured for an AP and each servers should be separated using a space.

Parameter	Description	Range	Default
`syslog-server <ip-address> <ip address 2> <ip-address 3>`	Specifies the IP address to configure the syslog server.	—	—
`no…`	Removes the configuration.	—	—

Example

The following command configures the IP address of the syslog server for an OAW-IAP.

```
(Instant AP)(config)# syslog-server 192.0.2.9 199.5.5.11
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Support for configuration of up to 3 syslog servers was added.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

telnet

```
telnet <host> [telnet-port <port>]
```

Description

This command initiates a telnet session with external servers from the AOS-W Instant CLI.

Syntax

Command/Parameter	Description	Range	Default
`host`	The IP address of the destination server.	—	—
`<telnet-port>`	The physical port number of the server to which a connection needs to be established through Telnet.	—	—

Example

The following example initiates a telnet session with external servers:

```
(Instant AP) telnet 10.0.0.1 23
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

telnet-server

```
telnet-server
no…
```

Description

This command enables Telnet access to AOS-W Instant CLI.

Parameter	Description	Range	Default
`telnet-server`	Enables Telnet access to the AOS-W Instant CLI.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables Telnet access to the OAW-IAP:

```
(Instant AP)(config)# telnet-server
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

terminal-access

```
terminal-access
no…
```

Description

This command enables SSH access to AOS-W Instant CLI.

Syntax

Parameter	Description	Range	Default
`terminal-access`	Enables terminal access to the AOS-W Instant CLI.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables terminal access to the OAW-IAP:

```
(Instant AP)(config)# terminal-access
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

tftp-dump-server

```
tftp-dump-server <IP-address>
no…
```

Description

This command configures TFTP dump server for an OAW-IAP. Use this command to configure TFTP dump server for storing core dump files.

Parameter	Description	Range	Default
`tftp-dump-server <IP-address>`	Configures TFTP dump server IP address.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a TFTP dump server:

```
(Instant AP)(config)# tftp-dump-server <IP-address>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

time-range

```
time-range <name> {absolute start | periodic { daily | weekday |weekend} <starttime> to
<endtime>} <startday <starttime> to <endday> <endtime>}
no time-range <name>
```

Description

This command allows you to create time range profiles on an OAW-IAP to enable or disable access to an SSID during a specific period of time. Use this command to create a time range profile using the AOS-W Instant CLI. You can create an absolute time profile to execute once during a specific date and time configured in the profile or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration. These time based profiles can be applied to existing SSIDs in the OAW-IAP.

Parameter	Description	Range	Default
`name`	Enter the profile name for the time range profile.	—	—
`absolute start {<startdate> <starttime>} end {<enddate> <endtime>}`	The SSID is made available only during the specified date and time range. Configure the following time range parameters: ■ startday—Enter the start date in the mm/dd/yyyy format. ■ starttime—Enter the start time in the hh:mm format. ■ endday—Enter the end date in the mm/dd/yyyy format. ■ endtime—Enter the end time in the hh:mm format.	—	—
`periodic {<startday> <starttime>} to {<endday> <endtime>}`	The availability of the SSID will be periodically changed based on the time range set in the profile. Configure the following time range parameters: ■ startday—Specify any day of the week from Monday to Sunday ■ starttime—Enter the start time in the hh:mm format. ■ endday—Enter the end day for the time range profile. ■ endtime—Enter the end time in the hh:mm format.	—	—
`periodic <daily> [<starttime> to <endtime>]`	■ daily—The time range profile is applied on the SSID on a daily basis. ■ starttime—Enter the start time in the hh:mm format. ■ endtime—Enter the end time in the hh:mm format.	—	—
`periodic <weekday> [<starttime> to <endtime>]`	■ weekday—The time range profile is applied only during the weekday ■ starttime—Enter the start time in the hh:mm format. ■ endtime—Enter the end time in	—	—

Parameter	Description	Range	Default
	the hh:mm format.		
`periodic <weekend> [<starttime> to <endtime>]`	■ weekend—The time range profile is applied only during the weekend. ■ starttime—Enter the start time in the hh:mm format. ■ endtime—Enter the end time in the hh:mm format.	—	—
`no time-range <name>`	Removes the time range configuration.	—	—

Example

The following example creates an absolute time range profile :

```
(Instant AP) (config) # time-range test1234 absolute start 10/20/2013 10:40 end 10/20/2015
10:50
```

The following example creates a periodic time range profile that executes on the specified day of the week:

```
(Instant AP) (config) # time-range test1234 periodic monday 10:40 to tuesday 10:50
```

The following example creates a periodic time range profile that executes daily:

```
(Instant AP) (config) # time-range testhshs12 periodic daily 10:20 to 10:35
```

The following example creates a periodic time range profile that executes during the weekday:

```
(Instant AP) (config) # time-range test123 periodic weekday 10:20 to 10:35
```

The following example creates a periodic time range profile that executes during the weekend:

```
(Instant AP) (config) # time-range test12 periodic weekend 10:20 to 10:30
```

The following example removes the time range configuration:

```
(Instant AP) (config) # no time-range testhshs12
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

traceroute

```
traceroute <ipaddr>
```

Description

This command traces the route to the specified IP address. Use this command to identify points of failure in your network.

Parameter	Description	Range	Default
`<ipaddr>`	Displays the destination IP address.	—	—

Example

The following example shows the output of the **traceroute** command:

```
<Instant Access Point>  #traceroute 10.1.2.3
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

ucm-logging

```
ucm-logging
no ucm-logging
```

Description

This command enables logging of UCM processes on the OAW-IAP.

Parameter	Description
`ucm-logging`	Enables UCM logging on the AP.
`no ucm-logging`	Disables UCM logging on the AP.

Example

The following example enables UCM logging on the AP:

```
(Instant AP) #ucm-logging
```

The following example disables UCM logging on the AP:

```
(Instant AP) #no ucm-logging
```

Related Commands

Command	Description
show log ucm	Displays the log of UCM processes on the OAW-IAP.
show ucm cdrs	Displays the UCM call data records stored on the OAW-IAP.

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

upgrade-drt

```
upgrade-drt <url>
```

Description

Use this command to upgrade anOAW-IAP by using a DRT file uploaded from the FTP or the TFTP server, or by using an HTTP URL. Before uploading the DRT file, ensure that you have the latest DRT file for your OAW-IAP.

Parameter	Description	Range	Default
`upgrade-drt`	Upgrades the OAW-IAP to use a new DRT version.	—	—
`<url>`	Allows you to specify the FTP, TFTP, or HTTP URL.	—	—

Examples

The following example shows how to upgrade an OAW-IAP by using a DRT file from the FTP server:

```
(Instant AP)# upgrade-drt ftp://192.0.2.7/reg-data-1.0_62178.dat
```

The following example shows how to upgrade an OAW-IAP by using a DRT file from the TFTP server:

```
(Instant AP)# upgrade-drt tftp://192.168.0.1/reg-data-1.0_62178.dat
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

upgrade-image

```
upgrade-image
upgrade-image2
upgrade-image2-no-reboot
upgrade-image2-no-switch-partition-reboot
   {<url> [ /ftp | /tftp | /http]}
```

Description

These commands allow you to upgrade an OAW-IAP to use a new image file from the FTP or TFTP server, or by using an HTTP URL. Before uploading an image file, ensure that you have the appropriate image file for your OAW-IAP. The following examples describe the image class for different OAW-IAP models:

- For OAW-RAP155/155P—AlcatelInstant_Aries_<build-version>
- For OAW-IAP224/225, OAW-IAP228, OAW-IAP274/275, and OAW-IAP277—AlcatelInstant_Centaurus_<build-version>
- For OAW-APAP-324/325—AlcatelInstant Hercules_8.7.0.X_xxxx
- For all other OAW-IAPs—AlcatelInstant_Orion_<build-version>

Parameter	Description	Range	Default
`upgrade-image`	Upgrades the OAW-IAP to use a new image.	—	—
`upgrade-image2`	Uploads an additional image file and upgrades the OAW-IAP to use this image file when required. You can also use this command to upgrade images for multi-class OAW-IAP cluster.	—	—
`upgrade-image2-no-reboot`	Uploads an image file and upgrades the OAW-IAP to use the new image without rebooting the OAW-IAPs.	—	—
`upgrade-image2-no-switch-partition-reboot`	Uploads an additional image file into the backup partition.	—	—
`<url>`	Allows you to specify the FTP, TFTP, or HTTP URL.	—	—

Example

The following examples upgrade an OAW-IAP by using an image file from the FTP server:

```
(Instant AP)# upgrade-image ftp://192.0.2.7/AlcatelInstant_Hercules_6.5.1.0-4.3.1.0_xxxx
(Instant AP)# upgrade-image ftp://Alcatel:123456@192.0.2.7/AlcatelInstant_Hercules_6.5.1.0-
4.3.1.0_xxxx
(Instant AP)# upgrade-image2-no-reboot ftp://192.0.2.7/AlcatelInstant_Hercules_6.5.1.0-
4.3.1.0_xxxx
```

```
(Instant AP)# upgrade-image2-no-reboot ftp://Alcatel:123456@192.0.2.7/AlcatelInstant_
Hercules_6.5.1.0-4.3.1.0_xxxx
```

To upgrade images for a multi-class OAW-IAP cluster:

```
(Instant AP)# upgrade-image2 Pegasus@tftp://192.168.0.1/ArubaInstant_Pegasus_6.5.2.0_
xxxxx;Ursa@tftp://192.168.0.1/ArubaInstant_Ursa_6.5.2.0_xxxxx
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

uplink

```
uplink
   enforce {ethernet| cellular |wifi | none}
   failover-internet
   failover-internet-ip <ip>
   failover-internet-ip-for-cellular-uplink <ip>
   failover-internet-check-timeout
   failover-internet-pkt-lost-cnt <count>
   failover-internet-pkt-send-freq <frequency>
   failover-vpn-timeout <seconds>
   no...
   preemption [interval <interval>]
   uplink-priority {cellular <priority> | {ethernet <priority>| [port <Interface-number>
   <priority>}|wifi <priority>}
no uplink
```

Description

This command configures uplink connections. Use this command to set preferences for enforcing uplinks or enabling preemption and to configure uplink switchover.

Parameter	Description	Range	Default
`uplink`	Enables the uplink configuration sub-mode.	—	—
`enforce {ethernet|cellular|wifi|none}`	Enforces the specified uplink connection. You can specify the following types of uplink: ■ ethernet ■ cellular ■ wifi ■ none	ethernet, cellular, wifi, none	None
`failover-internet`	Enables uplink switchover based on the availability of the Internet.	—	Disabled

Parameter	Description	Range	Default
	When enabled, the OAW-IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the OAW-IAP switches to a different connection.		
`failover-internet-ip`	Allows you to configure the IP address to which the ICMP packets are sent in the event of Internet failure.	Any IP address	8.8.8.8

Parameter	Description	Range	Default
	If the out-of-service feature is enabled for the Internet down event in the SSID and the Internet is down, the ICMP packets are sent to the configured IP address to verify if the Intenet is reachable from current uplink. By default, the master OAW-IAPs send the ICMP packets to 8.8.8.8 IP address to verify if the Internet is reachable.		
`failover-internet-ip-for-cellular-uplink <ip>`	Configures the Internet failover IP address for a cellular 3G/4G uplink.	Any IP address	—
`failover-internet-check-timeout`	Configures the number of seconds after which the Internet based uplink verification times out.	0–3600	10
`failover-internet-pkt-lost-cnt <count>`	Configures the number of packets that are to be lost when verifying the uplink availability using the Internet.	1–1000	10

Parameter	Description	Range	Default
`failover-internet-pkt-send-freq <frequency>`	Configures the frequency in seconds, at which the ICMP packets are sent to verify the uplink availability using the Internet.	1–3600	30
`failover-vpn-timeout <seconds>`	Configures a duration to wait for an uplink switch based on VPN status.	—	180 seconds
`preemption`	Enables pre-emption when no uplinks are enforced. When enabled, if the current uplink is active, the OAW-IAP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.	—	Disabled

`uplink-priority {cellular <priority>|{ethernet <priority>|`
`port <Interface-number> <priority>}|wifi <priority>}`
	Sets an uplink priority.
	You can specify the type of uplink to configure and assign a priority. If Ethernet uplink needs to be prioritized, specify the interface port number.
		Integer	Ethernet 0

Parameter	Description	Range	Default
`no…`	Disables the parameters configured under the **uplink** command.	—	—
`no uplink`	Removes the uplink configuration.	—	—

Enforcing uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the OAW-IAP uses the specified uplink as the primary uplink regardless of uplink preemption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the OAW-IAP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and preemption is not enabled, and if the current uplink fails, the OAW-IAP tries to find an available uplink based on the priority configured. The uplink with the highest priority is used as the primary uplink. For example, if WiFi-sta has the highest priority, it is used as the primary uplink.
- When no uplink is enforced and preemption is enabled, and if the current uplink fails, the OAW-IAP tries to find an available uplink based on the priority configured. If current uplink is active, the OAW-IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

Uplink Preemption

When no uplink is enforced and preemption is enabled, and if the current uplink fails, the OAW-IAP tries to find an available uplink based on in the priority configured. If current uplink is active, the OAW-IAP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

Uplink Priority

When uplink priority is configured, the OAW-IAP tries to get a higher priority link every ten minutes even if the current uplink is up. This does not affect the current uplink connection. If the higher uplink is usable, the OAW-IAP switches over to that uplink. Preemption is enabled by default.

Uplink Switchover

The default priority for uplink switchover is Ethernet and then 3G or 4G. The OAW-IAP has the ability to switch to the lower priority uplink if the current uplink is down.

Uplink Switching based on VPN Status

AOS-W Instant supports switching uplinks based on the VPN status when deploying mixed uplinks (Ethernet 0, 3G or 4G,Wi-Fi). When VPN is used with multiple backhaul options, the OAW-IAP switches to an uplink connection based on the VPN connection status instead of only using Ethernet 0, the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Ethernet 0 and the VPN connection is down, the OAW-IAP will retry to connect to VPN. This retry time depends on the configuration of primary/backup and fast-failover for VPN. If all the possibilities fail, then the OAW-IAP waits for a vpn-failover-timeout and then a different u plink (3G,Wi-Fi) is selected.

- If the current uplink is 3G or Wi-Fi, and Ethernet 0 has a physical link, the OAW-IAP periodically suspends user traffic to try and connect to the VPN on the Ethernet 0. If the OAW-IAP succeeds, then the OAW-IAP switches to Ethernet 0. If the OAW-IAP does not succeed, then the OAW-IAP restores the VPN connection to the current uplink.

Switching Uplinks Based on Internet Availability

When the uplink switchover based on Internet availability is enabled, the OAW-IAP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the public Internet is not reachable from the current uplink, the OAW-IAP switches to a different connection.

Example

The following example configures uplink priority:

```
(Instant AP)(uplink)# uplink-priority ethernet port 0 1
(Instant AP)(uplink)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **failover-internet-ip-for-cellular-uplink <ip>** parameter was added.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and uplink configuration sub-mode.

uplink-vlan

```
uplink-vlan <vlan-ID>
```

Description

This command configures uplink VLAN for management traffic on an OAW-IAP. When configured, the uplink management VLAN allows you to tag management traffic and connect multiple OAW-IAP clusters to the same port on an upstream switch (for example, OmniVista 3600 Air Manager server).

Parameter	Description	Range	Default
`<vlan-ID>`	Assigns a VLAN ID for the uplink management traffic.	0–4093	0

Example

The following example configures uplink management VLAN:

```
(Instant AP)# uplink-vlan 0
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

url-visibility

```
url-visibility
no…
```

Description

This command enables url visibility on the OAW-IAP and extracts the full URL information of the http and https sessions along with the session-ip and periodically logs them on the ALE server. To verify if the configuration has been applied correctly, use the **show dpi debug status** command.

Parameter	Description	Range	Default
`url-visibility`	Enables URL visibility on the OAW-IAP.	—	—
`no...`	Disables URL visibility.	—	—

Example

The following example enables url visibility:

```
(Instant AP)(config)# url-visibility
(Instant AP)(config)# end
(Instant AP)# commit apply
```

The following example shows the output of the show dpi debug status command:

```
Dpimgr Running :TRUE
Dpimgr Hello count :1
Dpimgr Agent :App
Dpimgr Status value :0x17d
Dpimgr Visibility Status :URL + App
Dpimgr Enforcement Status :App
Dpimgr External Visibility Status :AMP
Dpimgr BCA Proxy Connection        :Established
Dpimgr BCA Server SSL Established :True
Dpimgr BCA Server Reachable        :Unknown
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

usb acl-profile

```
usb acl-profile <profile_name> | no | rule <name> {deny|permit}}
```

Description

This command is used to create a AP USB ACL profile.

Parameter	Description
`<profile-name>`	Name of the AP USB ACL profile.
`no`	Negate any configured parameter.

Parameter	Description
rule	USB access rule.
<vendor_name>	Name of USB vendor. Available options are: ■ Alcatel-L800 ■ Amberbox-detector ■ Amberbox-gateway ■ C-motech-CNU-680 ■ EpiValley-SEC-8089 ■ Fraklin-u770-u772 ■ Franklin-U300 ■ Franklin-U301 ■ Franklin-U600 ■ Fujisoft ■ Globetrotter-ICON-225 ■ Globetrotter-ICON-322 ■ HanShow ■ Huawei-3276s-150 ■ Huawei-D41HW ■ Huawei-E1552 ■ Huawei-E157 ■ Huawei-E160 ■ Huawei-E169-E180-E220 ■ Huawei-E170-E272-E220 ■ Huawei-E173 ■ Huawei-E1731-177DT06 ■ Huawei-E1750 ■ Huawei-E176-E176G-E1553 ■ Huawei-E1762 ■ Huawei-E180 ■ Huawei-E180-E1692-E1762 ■ Huawei-E1820e ■ Huawei-E220 ■ Huawei-E261 ■ Huawei-E3131 ■ Huawei-E3272s-153 ■ Huawei-E3276 ■ Huawei-E3276s-500 ■ Huawei-E3372 ■ Huawei-E3372h-153-hil ■ Huawei-E3372h-153-modem ■ Huawei-E352s-5 ■ Huawei-E353 ■ Huawei-E353-E1750-E367 ■ Huawei-E367 ■ Huawei-E3765 ■ Huawei-E392 ■ Huawei-e398 ■ Huawei-E8372 ■ Huawei-EC150 ■ Huawei-EC167 ■ Huawei-HWD12-LTE ■ Huawei-K3770 ■ Huawei-K3772 ■ Huawei-K4505 ■ Huawei-K4510 ■ Huawei-K4605 ■ Huawei-K5150 ■ Huawei-K5160 ■ Huawei-KDDI-DATA07

Parameter	Description
	■ Icon-452 ■ Longcheer-WM72 ■ Netgear-340u ■ Netgear-341u ■ Novatel-MC545 ■ Novatel-MC551L ■ Novatel-MiFi-2200 ■ Novatel-Ovation-U727 ■ Novatel-U620L ■ Novatel-U720 ■ Novatel-U727 ■ Novatel-U760-Sprint ■ Novatel-U760-Virgin ■ NTT-DoCoMo-L-02A ■ NTT-DoCoMo-L-02C ■ NTT-DoCoMo-L-05A ■ NTT-DoCoMo-L-08C ■ Pantech-UM150 ■ Pantech-UM175 ■ Pantech-UM190 ■ Pantech-UML290 ■ Pantech-UML295 ■ Pantech-UML295-cold ■ Qualcomm-SXC-1080 ■ SES-Imagotag-021 ■ Sierra-250U ■ Sierra-305-308 ■ Sierra-306-308-503-312U ■ Sierra-313u ■ Sierra-320U ■ Sierra-330U ■ Sierra-598 ■ Sierra-881U ■ Sierra-885 ■ Sierra-Compass-597 ■ Sierra-Compass-885 ■ Sierra-Tstick-C597 ■ SIMTech ■ Solu-M-SLG-DM101 ■ UGM1831 ■ UMG181 ■ Utstarcom-UM100C ■ ZTE-3565 ■ ZTE-AC2726 ■ ZTE-AC2736 ■ ZTE-AC3781 ■ ZTE-Fivespot ■ ZTE-K4505-z ■ ZTE-MF110 ■ ZTE-MF180-HSDPA ■ ZTE-MF190-Egypt ■ ZTE-MF190-India ■ ZTE-MF190-Thailand ■ ZTE-MF591 ■ ZTE-MF633-MF636 ■ ZTE-MF637-MF656 ■ ZTE-MF668 ■ ZTE-MF683-HSDPA ■ ZTE-MF79S

Parameter	Description
	- ZTE-MF820 - ZTE-MF820D - ZTE-MF823 - ZTE-MF825C - ZTE-MF831 - ZTE-MF832S - ZTE-MF832U - ZTE-MF832U-Zero
deny permit	- deny - Access to USB device is denied - permit - Access to USB device is granted

Example

The following command creates a USB ACL profile named sample-usb-acl-profile with rule to permit USB devices from HanShow:

```
(Instant AP)(config)# usb acl-profile sample-usb-acl-profile
(Instant AP)(AP USB ACL Profile "sample-usb-acl-profile")# rule HanShow permit
```

Command History

Release	Modification
AOS-W 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Enable Mode.

usb-port-disable

```
usb-port-disable
no…
```

Description

This command disables the USB port on the OAW-IAP. To re-enable the port, run the **no usb-port-disable** command. Reboot the OAW-IAP after changing the USB port status.

Example

The following example shows how to disable the USB port on the OAW-IAP:

```
(Instant AP)# usb-port-disable
Remind: Command takes effect after AP reboot.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

usb profile

```
usb profile <profile-name> { no | usb-acl-profile}
```

Description

This command is used to create a AP USB profile.

Parameter	Description
`<profile-name>`	Name of the AP USB profile.
`no`	Negate any configured parameter.
`usb-acl <name>`	Apply USB ACL profile to AP USB profile.

Example

The following command creates an AP USB profile named sample-ap-usb-profile and applies a USB ACL profile named sample-usb-acl-profile to it:

```
(Instant AP)(config)# ap usb-profile sample-ap-usb-profile
(Instant AP)(AP USB profile "sample-ap-usb-profile")# usb-acl-profile sample-usb-acl-profile
```

Command History

Release	Modification
AOS-W 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Enable Mode.

usb-profile-binding

```
usb-profile-binding <profile_name>
```

Description

This command is used to bind the AP USB profile with the supported vendor product.

Parameter	Description
`<profile-name>`	Name of the AP USB profile.

Example

The following command binds a USB ACL profile named sample-usb-acl-profile:

```
(Instant AP)(config)# usb-profile-binding sample-usb-profile
```

Command History

Release	Modification
AOS-W 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Privileged EXEC mode.

user

```
user <username> [<password>][portal| radius]
no…
```

Description

This command creates users for an OAW-IAP. The AOS-W Instant user database consists of a list of guest and employee users. Addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Instant system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.

An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

The user database is also used when an OAW-IAP is configured as an internal RADIUS server. The local user database of OAW-IAPs can support up to 512 user entries except OAW-IAP-9x supports only 256 user entries. If there are already 512 users, OAW-IAP-9x will not be able to join the cluster.

Parameter	Description	Range	Default
`user <username>`	Creates a username for the OAW-IAP user.	—	—
`<password>`	Assigns a password for the OAW-IAP user.	—	—
`portal`	Configures a guest user.	—	—
`radius`	Configures an employee user.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures an employee user for an OAW-IAP:

```
(Instant AP)(config)# user user1 password123 radius
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

version

```
version <version-number>
```

Description

This command configures a version number for the OAW-IAP.

Parameter	Description
version <version-number>	Assigns a version number for the OAW-IAP.

Example

The following example configures a version number for the OAW-IAP.

```
(Instant AP)(config)# version 2
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

virtual-controller

```
virtual-controller
   country <country-code>
   dnsip <addr>
   ip <IP-address>
   ipv6 <IPv6 address>
   key <name>
   vlan <virtual-controller-vlan> <virtual-controller-mask> <virtual-controller-gateway>
   no…
```

Description

This command configures the virtual switch settings such as country code and VC key, and network parameters such as IPv4 or IPv6 addresses, VLAN, and DNS IP address.

Parameter	Description	Range	Default
`country <country-code>`	Defines the country of operation of an OAW-IAP. Slave OAW-IAPs obtain country code configuration settings from the master OAW-IAP.	—	—
`dnsip <addr>`	Configures the DNS IP address for the virtual switch.	—	—
`ip <IP-address>`	Assigns an IP address for the virtual switch.	—	—
`ipv6 <IPv6 address>`	Assigns an IPv6 address for the virtual switch.	—	—
`key <name>`	Defines a unique name for the virtual switch.	1–64	—
`vlan <virtual-controller-vlan>`	Associates a VLAN ID with the virtual switch.	—	—
`<virtual-controller-mask>`	Configures a subnet mask for the virtual switch.	—	—
`<virtual-controller-gateway>`	Configures a gateway for the virtual switch.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a country code for an OAW-IAP:

```
(Instant AP)(config)# virtual-controller-country US
(Instant AP)(config)# end
(Instant AP)# commit apply
```

The following example configures a DNS IP address for the virtual switch:

```
(Instant AP)(config)# virtual-controller-dnsip 192.0.2.2
(Instant AP)(config)# virtual-controller-ip 192.0.2.2
(Instant AP)(config)# virtual-controller-ipv6 10.17.154.132
(Instant AP)(config)# virtual-controller-key
541a271a01f722ac28c1f8cfcbc4529021bcfb130d4e59ac93
(Instant AP)(config)# virtual-controller-vlan 1961 255.255.255.240 10.17.196.17
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vlan

```
vlan {<vlan_name> [<vlan id>]}
no…
```

Description

This command configures a VLAN mapping for an SSID profile.

Parameter	Description	Range	Default
`<vlan_name>`	Configures the OAW-IAP's VLAN name.	1–32	—
`<vlan id>`	Configures the OAW-IAP's VLAN ID.	—	—
`no…`	Removes the configuration.	—	—

Usage Guidelines

Use this command to define the mapping of the VLAN name and VLAN ID. VLAN names are not case sensitive.

Example

The following example configures VLAN ID mapping to a specific VLAN name.

```
(Instant AP)(config)# vlan myvlan 30
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vlan-name

```
vlan-name <name>
no…
```

Description

This command configures the named VLAN in a WLAN SSID profile.

Syntax

Parameter	Description	Range	Default
`<name>`	Configures the VLAN name for an SSID profile.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a VLAN name:

```
(Instant AP)(config)# vlan-name <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

voip_qos_trusted

```
voip_qos_trusted
```

Description

This command prioritizes the RTP traffic based on the DSCP value set by the end user device instead of overriding the DSCP values based on the SSID configuration.

Example

The following CLI command passes the RTP tracffic without changing the DSCP value:

```
(Instant AP)(config)# voip_qos_trusted
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn backup

```
vpn backup <name>
no…
```

Description

This command configures a secondary or backup VPN server for VPN connections. When both primary and secondary VPN servers are configured, the OAW-IAP can switch to the available VPN connection when a the primary VPN server is not available.

Parameter	Description	Range	Default
`vpn backup <name>`	Configures an FQDN for the secondary VPN or IPsec endpoint.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a backup server for VPN connections:

```
(Instant AP)(config)# vpn backup <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.2.1.0-3.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn fast-failover

```
vpn fast-failover
no…
```

Description

This command configures fast failover feature for VPN connections. Enabling the fast failover feature allows the OAW-IAP to create a backup VPN tunnel to the switch along with the primary tunnel, and maintain both the primary and backup tunnels separately. If the primary tunnel fails, the OAW-IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

Parameter	Description	Range	Default
`vpn fast-failover`	Enables fast failover feature for VPN connections.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures the VPN fast failover feature:

```
(Instant AP)(config)# fast-failover
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn gre-outside

```
vpn gre-outside
no…
```

Description

This command enables automatic configuration of the GRE tunnel between the OAW-IAP and the switch.Use this command to enable automatic configuration of the GRE tunnel between the OAW-IAP and the switch to provide L2 connectivity.

Example

The following example configures an automatic GRE tunnel:

```
(Instant AP)(config)# vpn gre-outside
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn hold-time

```
vpn hold-time <seconds>
no...
```

Description

This command configures the time interval after which the OAW-IAP can switch over to the primary host when preemption is enabled. Use this command to configure a period to hold on switching to the primary server when pre-emption is enabled.

Parameter	Description	Range	Default
`vpn hold-time <seconds>`	Configures a time period in seconds after which the OAW-IAPs can switch to primary VPN server.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a hold-time to switch to the primary host server:

```
(Instant AP)(config)# hold-time <seconds>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn ikepsk

```
vpn ikepsk <ikepsk> username <username> password <password>
no…
```

Description

This command configures user credentials for the VPN connection.

Parameter	Description	Range	Default
`vpn ikepsk <ikepsk>`	Specifies an IKE authentication for VPN connection using PSKs.	—	—
`username <username>`	Defines a username that enables access to VPN.	—	—
`password <password>`	Defines a password that enables access to VPN.	—	—
`no…`	Removes the configuration.	—	—

Example

The following commands enable user access to VPN connection.

```
(Instant AP)(config)# vpn ikepsk secretKey username User1 password password123
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn monitor-pkt-lost-cnt

```
vpn monitor-pkt-lost-cnt <count>
no...
```

Description

This command configures the number of lost packets after which the OAW-IAP can determine that the VPN connection is not available. Use this command to configure a count for the lost packets, so that the OAW-IAPs can determine if the VPN connection is unavailable.

Parameter	Description	Range	Default
`vpn monitor-pkt-lost-cnt <count>`	Defines the number of lost packets for VPN connection test or monitoring by the OAW-IAP.	—	2
`no…`	Removes the configuration.	—	—

Example

The following example configures a count for the lost packets:

```
(Instant AP)(config)# vpn monitor-pkt-lost-cnt <count>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn monitor-pkt-send-freq

```
vpn monitor-pkt-send-freq <frequency>
no...
```

Description

This command configures the frequency at which the OAW-IAP can verify if the active VPN connection is available. Use this command to monitor VPN connections and verify its availability at regular intervals.

Parameter	Description	Range	Default
`vpn monitor-pkt-send-freq <frequency>`	Configures a frequency interval in seconds at which the test packets are sent.	—	5
`no…`	Removes the VPN monitoring frequency configuration.	—	—

Example

The following example configures the VPN monitoring frequency:

```
(Instant AP)(config)# vpn monitor-pkt-send-freq 10
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn preemption

```
vpn preemption
no…
```

Description

This command enables pre-emption to allow the VPN tunnel to switch back to the primary host after a failover. Use this command to enable pre-emption when both primary and secondary servers are configured and fast failover feature is enabled.

Parameter	Description	Range	Default
`vpn preemption`	Enables pre-emption to allow the VPN tunnel to switch to the primary VPN server when it becomes available after a failover.	—	—
`no…`	Removes the VPN pre-emption configuration.	—	—

Example

The following example enables VPN pre-emption.

```
(Instant AP)(config)# vpn preemption
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn primary

```
vpn primary <name>
no...
```

Description

This command configures a primary VPN server for VPN connections. When a secondary VPN server is configured along with the primary server, you can enable the fast failover feature that allows the OAW-IAP to create a backup VPN tunnel to the switch along with the primary tunnel, and maintain both the primary and backup tunnels separately.

Parameter	Description	Range	Default
`vpn primary <name>`	Configures a FQDN for the main VPN or IPsec endpoint.	—	—
`no…`	Removes the VPN server configuration.	—	—

Example

The following example configures a primary VPN server:

```
(Instant AP)(config)# vpn primary <name>
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn reconnect-duration

```
vpn reconnect-duration <1-3600>
```

Description

This command configures the time period after which the OAW-IAP fails over to the backup switch in IAP-VPN connections. Use this command to configure the time period for which the OAW-IAP will try attempting to connect to the primary switch before failing over to the backup switch.

Parameter	Description	Range	Default
`vpn reconnect-duration <1-3600>`	Configures the time period after which the OAW-IAPfails over to the backup switch.	1-3600	30

Example

The following example configures a backup internal authentication server:

```
(Instant AP)(config)# vpn reconnect-duration 60
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn reconnect-time-on-failover

```
vpn reconnect-time-on-failover <down-time>
no…
```

Description

This command defines a period after which the VPN connection can be reestablished when the primary VPN tunnel fails. When configured , the OAW-IAP reconnects the user session when the interval specified for this command expires.

Parameter	Description	Range	Default
`vpn reconnect-time-on-failover <down-time>`	Configures a time period in minutes after which the VPN is reconnected when the primary VPN tunnel fails.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a VPN reconnection duration:

```
(Instant AP)(config)# vpn reconnect-time-on-failover 20
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn reconnect-user-on-failover

```
vpn reconnect-user-on-failover
no…
```

Description

This command enables the users to reconnect to the VPN when the primary VPN tunnel fails. When enabled , the OAW-IAP reconnects the user during a VPN failover.

Parameter	Description	Range	Default
`vpn reconnect-user-on-failover`	Enables users to reconnect to the VPN during a VPN failover.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example enables users to reconnect to VPN after a failover:

```
(Instant AP)(config)# vpn reconnect-user-on-failover
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

vpn tunnel-profile

```
vpn tunnel-profile <name>
   primary <IP address or domain name>
   backup <name>
   fast-failover
   gre-ouitside
   hold-time <hold_time>
   monitor-pkt-lost-cnt <monitor_pkt_lost_cnt>
   monitor-pkt-send-freq <monitor_pkt_send_freq>
   per-ap-tunnel
   preemption
   primary <name>
   use custom-cert
no..
```

Description

This command is used to configure a VPN tunnel profile. The profile created can be associated to an SSID profile.

Parameter	Description	Range	Default
`vpn tunnel-profile <name>`	Creates a VPN tunnel profile.	—	—
`backup <name>`	Configures an FQDN for the secondary VPN or IPsec endpoint.	—	—
`fast-failover`	Enables fast failover feature for VPN connections.	—	—
`hold-time <hold_time>`	Configures a time period in seconds after which the Instant APs can switch to primary VPN server.	—	—
`monitor-pkt-lost-cnt <monitor_pkt_lost_cnt>`	Defines the number of lost packets for VPN connection test or monitoring by the OAW-IAP.	—	2
`monitor-pkt-send-freq <monitor_pkt_send_freq>`	Configures a frequency interval in seconds at which the test packets are sent.	—	5
`no...`	Removes the parameters configured under the **vpn tunnel-profile** command.	—	—

Parameter	Description	Range	Default
`preemption`	Enables pre-emption to allow the VPN tunnel to switch to the primary VPN server when it becomes available after a failover.	—	—
`primary <name>`	Configures a FQDN for the main VPN or IPsec endpoint.	—	—
`gre-ouitside`	This command enables automatic configuration of the GRE tunnel between the OAW-IAP and the switch.	—	—
`per-ap-tunnel`	This command configures a per ap GRE tunnel.	—	—
`use custom-cert`	Configures an IPsec tunnel to use a customized certificate.	—	—

Example

The following example configures a non-default VPN tunnel profile:

```
(Instant AP)(config)# vpn tunnel-profile <profile_name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# primary <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# backup <IP address or domain name>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# fast-failover
(Instant AP)(VPN Tunnel Profile "<profile_name>")# hold-time <seconds>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# preemption
(Instant AP)(VPN Tunnel Profile "<profile_name>")# monitor-pkt-send-freq <frequency>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# monitor-pkt-lost-cnt <count>
(Instant AP)(VPN Tunnel Profile "<profile_name>")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

web-server

```
web-server
  ciphers <security_level> {high|medium|low}
  ssl-protocol {all|tlsv1|tlsv1.1|tlsv1.2}
  no…
```

Description

This command allows you to configure web server and enable or disable the TLS protocol. Use this command to enable secure communication with the web server through the TLS protocol.

Parameter	Description	Range	Default
`ciphers`	Configures the strength of the cipher suite: ■ **high**: encryption keys larger than 128 bits ■ **low**: 56 or 64 bit encryption keys ■ **medium**: 128 bit encryption keys	high, medium, low	high
`ssl-protocol`	Enables SSL protocol for secure communication with the web server.	—	all
`all`	Enables all versions of TLS protocol for secure communication with the web server.	—	—
`tlsv1`	Enables TLS v1 protocol.	—	—
`tlsv1.1`	Enables TLS v1.1 protocol.	—	—
`tlsv1.2`	Enables TLS v1.2 protocol.	—	—
`no…`	Removes the configuration.	—	—

Example

The following example shows how to enable TLS v1.0:

```
(Instant AP)(config)# web-server
(Instant AP)(web-server)# ssl-protocol tlsv1
(Instant AP)(web-server)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

wifi0-mode

```
wifi0-mode <mode>
```

Description

This command configures the Wi-Fi 0 interface of the OAW-IAP. Use this command to configure a Wi-Fi0 interface of an OAW-IAP to function in the access, monitor, or spectrum monitor mode.

Parameter	Description	Range	Default
`<mode>`	Configures the OAW-IAP to function in any of the following modes: ■ **Access**— In Access mode, the OAW-IAP serves clients, while also monitoring for rogue OAW-IAPs in the background. ■ **Monitor**—In Monitor mode, the OAW-IAP acts as a dedicated monitor, scanning all channels for rogue OAW-IAPs and clients. ■ **Spectrum Monitor**— In Spectrum Monitor mode, the OAW-IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring OAW-IAPs or from non-WiFi devices such as microwaves and cordless phones. **NOTE:** In Monitor and Spectrum Monitor modes, the OAW-IAP does not provide access services to clients.	access, monitor, spectrum-monitor	access

Example

The following example configures the wifi0 interface to use the access mode:

```
(Instant AP)# wifi0-mode access
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

wifi1-mode

```
wifi1-mode <mode>
```

Description

This command configures the Wi-Fi1 interface of an OAW-IAP. Use this command to configure the Wi-Fi1 interface of an OAW-IAP to function in the access, monitor, or spectrum monitor mode.

Parameter	Description	Range	Default
`<mode>`	Configures the OAW-IAP to function in any of the following modes: ■ **Access**— In Access mode, the OAW-IAP serves clients, while also monitoring for rogue OAW-IAPs in the background. ■ **Monitor**—In Monitor mode, the OAW-IAP acts as a dedicated monitor, scanning all channels for rogue OAW-IAPs and clients. ■ **Spectrum Monitor**— In Spectrum Monitor mode, the OAW-IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring OAW-IAPs or from non-WiFi devices such as microwaves and cordless phones. **NOTE:** In Monitor and Spectrum Monitor modes, the OAW-IAP does not provide access services to clients.	access, monitor, spectrum-monitor	access

Example

The following example configures the wifi0 interface to use the access mode:

```
(Instant AP)# wifi1-mode access
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

wifi2-mode

```
wifi2-mode <mode>
```

Description

This command configures the Wi-Fi2 interface of an OAW-IAP. Use this command to configure the Wi-Fi2 interface, the secondary 5GHz radio, of an OAW-IAP to function in the access, monitor, or spectrum monitor mode. The Wi-Fi2 mode can only be configured when **split-5ghz-radio** is enabled on the access point.

Parameter	Description	Range	Default
`<mode>`	Configures the OAW-IAP to function in any of the following modes: ■ **Access**— In Access mode, the OAW-IAP serves clients, while also monitoring for rogue OAW-IAPs in the background. ■ **Monitor**—In Monitor mode, the OAW-IAP acts as a dedicated monitor, scanning all channels for rogue OAW-IAPs and clients. ■ **Spectrum Monitor**— In Spectrum Monitor mode, the OAW-IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring OAW-IAPs or from non-WiFi devices such as microwaves and cordless phones. **NOTE:** In Monitor and Spectrum Monitor modes, the OAW-IAP does not provide access services to clients.	access, monitor, spectrum-monitor	access

Example

The following example configures the Wi-Fi2 interface to function in the access mode:

```
(Instant AP)# wifi2-mode access
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.6.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
OAW-550 Series access points	Privileged EXEC mode.

wificall-dns-pattern

```
wificall-dns-pattern <dns_pattern>
no…
```

Description

This command configures a DNS pattern for Wi-Fi calling clients. Wi-Fi Calling is enabled by default. The DSCP value for the voice session is 48 (without ACP) and 46 (with ACP).

Parameter	Description	Range	Default
`<dns_pattern>`	Configure the DNS pattern for the carrier. A maximum of 10 DNS patterns can be configured. DNS patterns for known carriers are configured by default. Default built-in patterns are: ■ 3 HK - wlan.three.com.hk ■ ATT - epdg.epc.att.net ■ Rogers-epdg.epc.mnc720.mcc302.pub.3gppnetwork.org ■ SmarTone-epdg.epc.mnc006.mcc454.pub.3gppnetwork.org ■ Sprint - primgw.vowifi2.spcsdns.net ■ T-Mobile - ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org ■ Verizon - wo.vzwwo.com ■ If the ePDG FQDN of the carrier does not match with the default patterns, use this option to configure the DNS pattern for the carrier. **NOTE:** The DNS IP address that OAW-IAP learns for Wi-Fi calling age out automatically, if there was no DNS query or response matching that IP for more than seven days.	priority voice: 0-62	priority voice: 46
`no…`	Remove the configuration	—	—

Example

The following example configures the DNS pattern for a Wi-Fi calling client:

```
(Instant AP)(config)# wificall-dns-pattern xo.xyz.com
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

wired-port-profile

```
wired-port-profile <port>
   access-rule-name <name>
   allowed-vlan [<vlan>]
   auth-server <name>
   auto-recovery
   auto-recovery-interval <interval>
   called-station-id
   captive-portal {<type> [exclude-uplink <types>] | external [Profile <name>] [exclude-
   uplink <types>]}
   content-filtering
   dot1x
   dot1x-timer-idrequest-period
   dot3bz
   duplex <duplex>
   deny-intra-vlan-traffic
   inactivity-timeout <interval>
   l2-auth-failthrough
   loop-detection-interval <interval>
   loop-protect
   mac-authentication
   native-vlan <vlan>
   no...
   poe
   radius-accounting
   radius-accounting-mode {user-association|user-authentication}
   radius-interim-accounting-interval <minutes>
   radius-reauth-interval <minutes>
   server-load-balancing
   set-role <attribute>{{equals|not-equal|starts-with|ends-with|contains}<operator>
   <role>|value-of}
   set-role-mac-auth <mac-only>
   set-role-machine-auth <machine-only> <user-only>
   set-role-pre-auth <role>
   set-role-unrestricted
   set-vlan <attribute>{equals|not-equals|starts-with|ends-with|contains} <operator> <VLAN-
   ID>|value-of}
   shutdown
   spanning-tree
   speed <speed>
   storm-control-broadcast
   storm-control-threshold <threshold>
   switchport-mode <mode>
   trusted
   type <type>
   uplink-enable
   use-ip-for-calling-station
no wired-port-profile <port>
```

Description

This command configures a wired port profile for wired OAW-IAP clients. Use this command to create a wired profile for employee and guest users. The Ethernet ports allow third-party devices such as VoIP phones or printers (which support only wired connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

Parameter	Description	Range	Default
`wired-port-profile <port>`	Creates a wired profile.	—	—
`access-rule-name <name>`	Maps the already configured access rules with the wired profile.	—	—
`allowed-vlan [<vlan>]`	Configures a list of allowed VLANs. The Allowed VLAN refers to the VLANs carried by the port in Access mode. You can configure the list of comma separated digits or ranges 1,2,5 or 1-4, or all.	—	—
`auth-server <name>`	Configures the authentication server for the wired profile.	—	—
`auto-recovery`	Enables automatic recovery of the port in the OAW-IAP that is shut down because of loop protection. After the automatic recovery, if the loop re-occurs, then the port is shutdown again.	—	Disabled

Parameter	Description	Range	Default
`auto-recovery-interval <interval>`	Specify the time, in seconds, to automatically recover the port in the OAW-IAP that is shut down because of loop protection.	30–43200 seconds	300 seconds

`called-station-id {type{ap-group|apname|`
`ipaddr|macaddr|vlan-id}`
	Configures the following called-station-id types:
	■ **ap-group** — The Virtual Controller name is used as the called-station-id.
	■ **ap-name** — The OAW-IAP hostname is used as the called-station-id.
	■ **vlan-id** — The VLAN ID of the client is used as the called-station-id.
	■ **ipaddr** — The IP address of the OAW-IAP is used as the called-station-id.
		—	called-station-id {type <macaddr>}

Parameter	Description	Range	Default
	- **macaddr** — The MAC address of the OAW-IAP is used as the calling-station-id. - **vlan-id** — The VLAN ID of the client is used as the called-station-id.		
`captive-portal{<type>[exclude-uplink <types>]|external [exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}`	Enables internal or external captive portal authentication for the wired profile users. You can also disable redirection to the captive portal based on the type of current uplink. If the external captive profiles are created, you can specify the profile name by using the **external** and **profile** keywords and associated parameters.	—	—
`content-filtering`	Enables content filtering.	—	—

Parameter	Description	Range	Default
`deny-intra-vlan-traffic`	Disables client-to-client communication in a network. When intra vlan traffic is disabled, the IAP only fowards client traffic to gateway and configured wired servers. All other traffic from the client is dropped.	—	Disabled
`dot1x`	Enables 802.11X authentication for the Wired profile users.	—	Disabled
`dot1x-timer-idrequest-period`	Interval in seconds, 802.1X identity request retries.	—	—
`dot3bz`	Enables 802.3bz authentication for the wired profile users.		Disabled
`duplex <duplex>`	Assigns a value for duplexing client traffic based on the capabilities of the client, the OAW-IAP, and the cable. You can specify **full**, **half**, or **auto**.	full, half, auto	auto

Parameter	Description	Range	Default
`inactivity-timeout <interval>`	Configures a timeout value for the inactive client sessions. When a client session is inactive for the specified duration, the session expires and the clients are required to log in again.	60-86400 seconds	1000 seconds
`l2-auth-failthrough`	Allows the clients to use 802.1X authentication when MAC authentication fails.	—	Disabled
`loop-detection-interval <interval>`	Specify the time, in seconds, to send loop detection packets on the ports of an OAW-IAP.	1–10 seconds	2 seconds
`loop-protect`	Enables loop protection on the ports of an OAW-IAP.	—	Disabled
`mac-authentication`	Enables MAC authentication.	—	Disabled
`native-vlan <vlan>`	Configures a value for Native VLAN. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN.	1-4093	—
`poe`	Enables PoE.	—	Enabled

Parameter	Description	Range	Default
`radius-accounting`	Enables accounting for the RADIUS server authentication. When enabled, the OAW-IAPs post accounting information to the Radius server at the specified accounting interval.	—	—
`radius-accounting-mode {user-association|user-authentication}`	Configures an accounting mode for the captive portal users. You can configure any of the following modes for accounting: ■ **user-authentication**— when configured, the accounting starts only after client authentication is successful and stops when the client logs out of the network. ■ **user-association**— When configured, the accounting starts when the	—	User-authentication

Parameter	Description	Range	Default
	client associates to the network successfully and stops when the client is disconnected.		
`radius-interim-accounting-interval <minutes>`	Configures an interval for posting accounting information as RADIUS INTERIM accounting records to the RADIUS server. When configured, the OAW-IAP sends interim-update messages with current user statistics to the RADIUS server at regular intervals.	0–60	—
`radius-reauth-interval <minutes>`	Configures a reauthentication interval at which all associated and authenticated clients must be reauthenticated.	0–32768	—
`server-load-balancing`	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	—	Enabled

Parameter	Description	Range	Default

`set-role <attribute> {{equals| not-equal|starts-with|ends-with`
`| contains}operator> <role>| value-of}`
	Assigns a user role to the clients. The first rule that matches the configured condition is applied.
	You can specify any of the following conditions:
	■ contains—The rule is applied only if the attribute value contains the specified string.
	■ ends-with—The rule is applied only if the attribute value ends with the specified string.
	■ equals—The rule is applied only if the attribute value is equal to the specified string.
	■ not-equals—The rule is applied only if the attribute value is not equal to the specified string.
	■ starts-with—
		—	—

Parameter	Description	Range	Default
	The rule is applied only if the attribute value begins with the specified string. ■ value-of - This rule sets the user role to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the OAW-IAP.		
`set-role-machine-auth <machine-only><user-only>`	Configures a machine authentication rule. You can assign different rights to clients based on whether their hardware device supports machine authentication.	—	—

Parameter	Description	Range	Default
	Machine authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.		
`set-role-mac-auth <mac-only>`	Configures a MAC authentication based user role.	—	—
`set-role-pre-auth <role>`	Configures a pre-authentication role to allow some access to the guest users before the client authentication.	—	—
`set-role-unrestricted`	Configures unrestricted access control.	—	—

`set-vlan <attribute> {equals|not-equals| starts-with|`
`ends-with| contains} <operator> <VLAN-ID>| value-of}`
	Assigns a VLAN name to the clients. The first rule that matches the configured condition is applied. You can specify any of the following conditions:
	■ contains—The rule is applied only if the attribute value
		—	—

Parameter	Description	Range	Default
	contains the specified string. ■ ends-with—The rule is applied only if the attribute value ends with the specified string. ■ equals—The rule is applied only if the attribute value is equal to the specified string. ■ not-equals—The rule is applied only if the attribute value is not equal to the specified string. ■ starts-with—The rule is applied only if the attribute value begins with the specified string. ■ value-of - This rule sets the VLAN to the value of the attribute returned. To set a user role, the value of the		

Parameter	Description	Range	Default
	attribute must already be configured on the OAW-IAP.		
`shutdown`	Shuts down the admin status port.	up, down	up
`spanning-tree`	Enables STP on the wired profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP will not operate on the uplink port and is supported only on OAW-IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.	—	—
`speed <speed>`	Assigns a value for indicating speed of client traffic based on the capabilities of the client, the OAW-IAP, and the cable.	10,100, 200, auto	auto

Parameter	Description	Range	Default
`storm-control-broadcast`	Enables the broadcast storm control. When this parameter is enabled, if the OAW-IAP detects a loop on one of its Ethernet port, it shuts down the Ethernet port. This prevents the OAW-IAP from receiving or sending any frames.	—	Disabled
`storm-control-threshold <threshold>`	Specify the broadcast packets per second on each Ethernet port of an OAW-IAP before the Ethernet port is shut down.	100-1000000 packets per second	2000 packets per second
`switchport-mode <mode>`	Defines the switchport mode for the wired profile. You can specify any of the following modes: ■ **Access**—Use this mode to allow the port to carry a single VLAN specified as the native VLAN. ■ **Trunk**—	access, trunk	trunk

Parameter	Description	Range	Default
	Use this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.		
`trusted`	Supports trusted ports to enable wired users in an L3 mode to connect to a switch or a router that is connected to the downlink port of an OAW-IAP. In this mode, `mac-authentication`, `dot1x`, and `captive-portal` parameters will not take any effect.	—	No
`type <type>`	Defines the primary usage of the wired profile.	employee, guest	employee
`uplink-enable`	Enables uplink for the wired profile.	—	—
`use-ip-for-calling-station`	The IP address of the client will be used as the calling-station-id.	—	—

Parameter	Description	Range	Default
`no…`	Removes the parameters configured under the **wired-port-profile** command.	—	—
`no wired-port-profile <port>`	Removes the wired port profile configuration.	—	—

Example

The following example configures a wired profile for an employee network:

```
(Instant AP)(config)# wired-port-profile employeeWired1
(Instant AP)(wired ap profile"employeeWired1")# type employee
(Instant AP)(wired ap profile"employeeWired1")# speed auto
(Instant AP)(wired ap profile"guestWired1")# dot3bz
(Instant AP)(wired ap profile"employeeWired1")# duplex auto
(Instant AP)(wired ap profile"employeeWired1")# no shutdown
(Instant AP)(wired ap profile"employeeWired1")# poe
(Instant AP)(wired ap profile"employeeWired1")# uplink-enable
(Instant AP)(wired ap profile"employeeWired1")# called-station-id type 10.64.1.23
(Instant AP)(wired ap profile"employeeWired1")# content-filtering
(Instant AP)(wired ap profile"employeeWired1")# switchport-mode trunk
(Instant AP)(wired ap profile"employeeWired1")# allowed-vlan 2,3,5
(Instant AP)(wired ap profile"employeeWired1")# native-vlan 1
(Instant AP)(wired ap profile"employeeWired1")# mac-authentication
(Instant AP)(wired ap profile"employeeWired1")# dot1x
(Instant AP)(wired ap profile"employeeWired1")# use-ip-for-calling-station
(Instant AP)(wired ap profile"employeeWired1")# l2-auth-failthrough
(Instant AP)(wired ap profile"employeeWired1")# auth-server server1
(Instant AP)(wired ap profile"employeeWired1")# server-load-balancing
(Instant AP)(wired ap profile"employeeWired1")# radius-reauth-interval 20
(Instant AP)(wired ap profile"employeeWired1")# access-rule-name wiredACL
(Instant AP)(wired ap profile"employeeWired1")# set-role Group-Name contains wired wired-
instant
(Instant AP)(wired ap profile"employeeWired1")# set-vlan ap-name equals test 400
(Instant AP)(wired ap profile"employeeWired1")# trusted
(Instant AP)(wired ap profile"employeeWired1")# end
(Instant AP)# commit apply
```

The following example configures a guest wired profile:

```
(Instant AP)(config)# wired-port-profile guestWired1
(Instant AP)(wired ap profile"guestWired1")# type guest
(Instant AP)(wired ap profile"guestWired1")# speed auto
(Instant AP)(wired ap profile"guestWired1")# dot3bz
(Instant AP)(wired ap profile"guestWired1")# duplex auto
(Instant AP)(wired ap profile"guestWired1")# no shutdown
(Instant AP)(wired ap profile"guestWired1")# poe
(Instant AP)(wired ap profile"guestWired1")# uplink-enable
(Instant AP)(wired ap profile"guestWired1")# content-filtering
(Instant AP)(wired ap profile"guestWired1")# switchport-mode trunk
(Instant AP)(wired ap profile"guestWired1")# allowed-vlan 200,201,400
(Instant AP)(wired ap profile"guestWired1")# native-vlan 1
(Instant AP)(wired ap profile"guestWired1")# captive-portal external exclude-uplink Ethernet
(Instant AP)(wired ap profile"guestWired1")# mac-authentication
```

```
(Instant AP)(wired ap profile"guestWired1")# auth-server server1
(Instant AP)(wired ap profile"guestWired1")# server-load-balancing
(Instant AP)(wired ap profile"guestWired1")# access-rule-name wiredACL
(Instant AP)(wired ap profile"guestWired1")# set-role Group-Name contains wired wired-instant
(Instant AP)(wired ap profile"guestWired1")# set-vlan ap-name equals test 200
(Instant AP)(wired ap profile"guestWired1")# trusted
(Instant AP)(wired ap profile"guestWired1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	The **deny-intra-vlan-traffic** parameter was added.
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were introduced: ■ **auto-recovery** ■ **auto-recovery-interval <interval>** ■ **loop-detection-interval <interval>** ■ **loop-protect** ■ **storm-control-broadcast** ■ **storm-control-threshold <threshold>**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and Wired port profile configuration sub-mode.

wlan access-list eth

```
wlan access-list eth <name>
   no
   rule {any | <eth-type>} {permit | deny}
```

Description

This command configures an ethertype access control list for non IP packets. Use this command to configure an ethertype ACL to create firewall policies based on the ethertype for non-IP packets. Ethertype ACL allows upto 256 access control entries in a single ACL.

Parameter	Description	Range	Default
`wlan access-list eth <name>`	Specifies the profile name of the access list configured.	—	—
`no`	Removes the definition of parameters under **wlan access-list eth** command.	—	—
`rule`	Creates an access list rule. You can create up to 256 ACEs in an ACL for a user role. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
`any`	Match any ethertype.	—	—
`<eth-type>`	Specify the ethertype in decimal or hexadecimal.	(0-65535)	—
`permit`	Creates a rule to allow the specified packets.	—	—
`deny`	Creates a rule to reject the specific packets.	—	—

Example

The following example configures an ethertype ACL for the network:

```
(Instant AP)(config)# wlan access-list eth eth-acl
(Instant AP)(Eth-ACL "eth-acl")#rule 0x888e permit
(Instant AP)(Eth-ACL "eth-acl")#rule 0x0806 permit
(Instant AP)(Eth-ACL "eth-acl")#rule any deny
(Instant AP)(Eth-ACL "eth-acl")#end
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command Introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

wlan access-list session

```
wlan access-list session <name>
   no
   rule <src> <smask> <dest> <mask> <match> {<protocol> <start-port> <end-port>
   {permit|deny|src-nat [vlan <vlan id>|tunnel <tunnel ip>]|dst-nat{<IP-address> <port>|
   <port>}| markapp <custom1....custom5> | app <app> {permit| deny}| appcategory <appgrp>|
   webcategory <webgrp> {permit| deny}| webreputation <webrep>}[{ log | blacklist | disable-
   scanning | tos <0-63> | dot1p-priority <0-7> | throttle-upstream <bandwidth in Kbps>
   throttle-downstream <bandwidth in Kbps> }]
```

Description

This command configures a session access control list for a WLAN SSID or wired profile. Use this command to configure an session ACL to create firewall policies based on the source and destination IP address, port number or IP protocol. Session ACL allows upto 256 access control entries in a single ACL.

Parameter	Description	Range	Default
`wlan access-list session <name>`	Specifies the profile name of the access list configured.	—	—
`no`	Removes the definition of parameters under **wlan access-list session** command.	—	—
`rule`	Creates an access list rule. You can create up to 256 ACEs in an ACL for a user role. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
`<src>`	Allows you to specify the source IP address.	—	—
`<smask>`	Specifies the subnet mask for the source IP address.	—	—
`<dest>`	Allows you to specify the destination IP address.	—	—
`<mask>`	Specifies the subnet mask for the destination IP address.	—	—
`<match>`	- **match**—Indicates if the	match invert	—

Parameter	Description	Range	Default
	rule specific to the destination IP address and subnet mask matches the value specified for protocol. ■ **invert**—Indicates if the rule allows or denies traffic with an exception to the specified destination IP address and subnet mask.		
`<protocol>`	Configures any of the following: ■ Protocol number between 0-255 ■ any: any protocol ■ tcp: Transmission Control Protocol ■ udp: User Datagram Protocol	1–255	—
`<sport>`	Specifies the starting port number from which the rule applies.	1–65534	—
`<eport>`	Specifies the ending port number until which the rule applies.	1–65534	—
`dst-nat`	Allows the OAW-IAP to perform destination NAT on packets.	—	—
`src-nat [vlan <vlan id>|tunnel]`	Allows the OAW-IAP to perform source-NAT on packets. When configured, the source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). ■ **vlan** - All client based traffic will be directed to the specified uplink	—	—

Parameter	Description	Range	Default
	VLAN using the IP address of the interface that OAW-IAP has on that VLAN; if the interface is not found, this option has no effect. ■ **tunnel** - The traffic from the Network Assigned clients is directed to the VPN tunnel.		
`<dst-nat-IP-address>`	Specifies the destination-NAT IP address for the specified packets when dst-nat action is configured.	—	—
`<dst-nat-port>`	Specifies the destination-NAT port for the specified packets when dst-nat action is configured.	—	—
`markapp <custom1....custom5>`	Allows you to configure a custom application ID.	custom1 to custom5	—
`app <app>`	Specifies a rule to allow or deny access to a specific type of application.	To view the list of applications, run the **show dpi app all** command.	—
`appcategory <appgrp>`	Specifies a rule to allow or deny access to a specific category of application.	To view the list of application categories, run the **show dpi appcategory all** command.	—
`webcategory <webgrp>`	Specifies a rule to allow or deny access to websites based on website category.	To view the list of website categories, run the **show dpi webcategory all** command.	–
`webreputation <webrep>`	Specifies a rule to allow or deny access to websites based on security rating.	■ trustworthy-sites ■ low-risk-sites ■ moderate-risk-sites ■ suspicious-sites	—

Parameter	Description	Range	Default
		- high-risk-sites	
`permit`	Creates a rule to allow the specified packets.	—	—
`deny`	Creates a rule to reject the specified packets.	—	—
`<opt0…opt11>`	Allows you to configure any of the following options:	—	—
`log`	Creates a log entry when this rule is triggered.	—	—
`blacklist`	Blacklists the client when this rule is triggered.	—	—
`disable-scanning`	Disables ARM scanning when this rule is triggered.	—	—
`tos <tos value>`	Specifies a DSCP value to prioritize traffic when this rule is triggered.	0-63	—
`dot1p-priority <priority>`	Sets an 802.1p priority.	0-7	—

`throttle-upstream <bandwidth in kbps>`
`throttle-downstream <bandwidth in kbps>`
	Sets a bandwidth limit based on application, application category, web category or website reputation, you can configure application throttling by using the **throttle-downstream** and **throttle-up** options. For example, you can limit the bandwidth rate for video streaming applications such as Youtube or Netflix, or set a low bandwidth for suspicious websites.	1-65535	—

Example

The following example configures a session ACL for the network:

```
(Instant AP)(config)# wlan access-list session ses-acl
(Instant AP)(Session-ACL "ses-acl")# rule 10.1.1.1 255.255.255.255 20.1.1.1 255.255.255.255
match any any any permit
```

```
(Instant AP)(Session-ACL "ses-acl")#rule 10.1.1.1 255.255.255.255 30.1.1.1 255.255.255.255
match any any any src-nat
(Instant AP)(Session-ACL "ses-acl")#end
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The **rule markapp <custom1....custom5>** parameter was added.
Alcatel-Lucent AOS-W Instant 8.5.0.0	Command Introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

wlan access-rule

```
wlan access-rule <name>
   access-list session <acl-name>
   access-list eth <acl-name>
   bandwidth-limit {downstream <kbps>| upstream <kbps>| peruser { downstream <kbps>| upstream
   <kbps>}}
   calea
   captive-portal {external [profile <name>]|internal}
   dpi-error-page-url <idx>
   index <index>
   no
   rule <dest> <mask> <match> {<protocol> <start-port> <end-port> {permit|deny|src-nat [vlan
   <vlan id>|tunnel <tunnel ip>]|dst-nat{<IP-address> <port>| <port>} | markapp
   <custom1....custom5> | app <app> {permit| deny}| appcategory <appgrp>| webcategory
   <webgrp> {permit| deny}| webreputation <webrep>}[{ log | blacklist | disable-scanning |
   tos <0-63> | dot1p-priority <0-7> | desc <description>  throttle-upstream <bandwidth in
   Kbps> throttle-downstream <bandwidth in Kbps> }]
   redirect-blocked-https-traffic
   vlan <vlan>
   no…
no wlan access-rule <name>
```

Description

This command configures access rules for WLAN SSID or wired profile. Use this command to configure access rules for user roles, create a captive-portal role, and to assign VLANs for the clients.

NOTE

If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.

Syntax

Parameter	Description	Range	Defaul t
`wlan access-rule <name>`	Specifies the profile name for which the access rule is configured.	—	—
`access-list session <acl-name>`	Specifies the session type access list to be added to the access rule.	—	—
`access-list eth <acl-name>`	Specifies the ethertype access list to be added to the access rule.	—	—

`bandwidth-limit {downstream <kbps>|`
`upstream <kbps>| peruser {downstream <kbps>|`
	Assign bandwidth contracts to user roles.	1–65535 Kbps	—

Parameter	Description	Range	Defaul t
`upstream <kbps>}}`	The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the OAW-IAP) or downstream (OAW-IAP to clients) traffic for a user role. If you want to assign a bandwidth contract specific for each user, you can run the command with **peruser** parameter. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. **NOTE:** In the earlier releases, bandwidth contract could be assigned per SSID. In the current release, the bandwidth contract can also be assigned per SSID user. If the bandwidth contract is assigned for an SSID in Instant 6.2.1.0-3.4.0.0 image and when the OAW-IAP is upgraded to 6.3.1.1-4.0.0.0 release version, the bandwidth configuration per SSID will be		

Parameter	Description	Range	Default
	treated as per-user downstream bandwidth contract for that SSID.		
`calea`	Creates an access rule for CALEA integration.	—	—
`captive-portal {external [profile <name>]|internal}`	Configures a captive-portal role, to assign to the users role after a successful authentication.	—	—
`dpi-error-page-url <idx>`	Creates an access rule to display a specific error page when clients access the HTTP websites blocked by AppRF policies.	—	—
`<index>`	Creates an index entry for access rules.	—	—
`rule`	Creates an access rule. You can create up to 128 ACEs in an ACL for a user role. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	—	—
`<dest>`	Allows you to specify the destination IP address.	—	—

Parameter	Description	Range	Defaul t
`<mask>`	Specifies the subnet mask for the destination IP address.	—	—
`<match>`	- **match**—Indicates if the rule specific to the destination IP address and subnet mask matches the value specified for protocol. - **invert**—Indicates if the rule allows or denies traffic with an exception to the specified destination IP address and subnet mask.	match invert	—
`<protocol>`	Configures any of the following: - Protocol number between 0-255 - any: any protocol - tcp: Transmission Control Protocol - udp: User Datagram Protocol	1–255	—
`<sport>`	Specifies the starting port number from which the rule applies.	1–65534	—
`<eport>`	Specifies the ending port number until which the rule applies.	1–65534	—

Parameter	Description	Range	Default
`dst-nat`	Allows the OAW-IAP to perform destination NAT on packets.	—	—
`src-nat [vlan <vlan id>|tunnel]`	Allows the OAW-IAP to perform source-NAT on packets. When configured, the source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). ■ **vlan** - All client based traffic will be directed to the specified uplink VLAN using the IP address of the interface that OAW-IAP has on that VLAN; if the interface is not found, this option has no effect. ■ **tunnel** - The traffic from the Network Assigned clients is directed to the VPN tunnel.	—	—

Parameter	Description	Range	Default
`<dst-nat-IP-address>`	Specifies the destination-NAT IP address for the specified packets when dst-nat action is configured.	—	—
`<dst-nat-port>`	Specifies the destination-NAT port for the specified packets when dst-nat action is configured.	—	—
`markapp <custom1....custom5>`	Allows you to configure a custom application ID.	custom1 to custom5	—
`app <app>`	Specifies a rule to allow or deny access to a specific type of application.	To view the list of applications, run the **show dpi app all** command.	—
`appcategory <appgrp>`	Specifies a rule to allow or deny access to a specific category of application.	To view the list of application categories, run the **show dpi appcategory all** command.	—
`webcategory <webgrp>`	Specifies a rule to allow or deny access to websites based on website category.	To view the list of website categories, run the **show dpi webcategory all** command.	–
`webreputation <webrep>`	Specifies a rule to allow or deny access to websites based on security rating.	■ trustworthy-sites ■ low-risk-sites ■ moderate-risk-sites ■ suspicious-sites ■ high-risk-sites	—

Parameter	Description	Range	Default
`permit`	Creates a rule to allow the specified packets.	—	—
`deny`	Creates a rule to reject the specified packets.	—	—
`<opt0…opt11>`	Allows you to configure any of the following options:	—	—
`log`	Creates a log entry when this rule is triggered.	—	—
`blacklist`	Blacklists the client when this rule is triggered.	—	—
`disable-scanning`	Disables ARM scanning when this rule is triggered.	—	—
`tos <tos value>`	Specifies a DSCP value to prioritize traffic when this rule is triggered.	0-63	—
`dot1p-priority <priority>`	Sets an 802.1p priority.	0-7	—
`desc <description>`	A comment entered by the user to easily identify the purpose of the access rule.	—	—

Parameter	Description	Range	Default

`throttle-upstream <bandwidth in kbps>`
`throttle-downstream <bandwidth in kbps>`
	Sets a bandwidth limit based on application, application category, web category or website reputation, you can configure application throttling by using the **throttle-downstream** and **throttle-up** options. For example, you can limit the bandwidth rate for video streaming applications such as Youtube or Netflix, or set a low bandwidth for suspicious websites.	1-65535	—

`redirect-blocked-https-traffic`	Configures an access rule to redirect users to a custom error page URL when accessing blocked HTTPS websites for the WLAN SSID or Wired profile.	—	—
`vlan <vlan>`	Configures a VLAN name or a VLAN ID in a derivation rule.	1–4093	—
`no...`	Removes the definition of parameters under **wlan access-rule** command.	—	—
`no wlan access-rule`	Removes the WLAN access rule configuration.	—	—

Example

The following example configures access rules for the wireless network:

```
(Instant AP)(config)# wlan access-rule WirelessRule
(Instant AP)(Access Rule "WirelessRule")# access-list session ses-acl
(Instant AP)(Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.0 192.0.2.7
255.255.255.0 match tcp 21 21 deny
(Instant AP)(Access Rule "WirelessRule")# rule 192.0.2.2  255.255.255.0 192.0.2.7
255.255.255.0 match udp 21 21 deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match app youtube permit throttle-
downstream 256 throttle-up 256
(Instant AP)(Access Rule "WirelessRule")# rule any any match appcategory webmail permit
throttle-downstream 256 throttle-up 256
(Instant AP)(Access Rule "WirelessRule")# rule 192.0.2.2 255.255.255.255 match 17 0-65535 0-
65535 permit markapp custom1
(Instant AP)(Access Rule "WirelessRule")#  rule any any match webcategory gambling  deny
(Instant AP)(Access Rule "WirelessRule")# rule any any match webcategory training-and-tools
permit
(Instant AP)(Access Rule "WirelessRule")# rule any any match webreputation high-risk-sites
deny
(Instant AP)(Access Rule "WirelessRule")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	The following parameters were added: ■ **rule desc <description>** ■ **rule markapp <custom1........custom5>**
Alcatel-Lucent AOS-W Instant 8.5.0.0	The following parameters were added: ■ **access-list session <acl-name>** ■ **access-list eth <acl-name>**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and access rule configuration sub-mode.

wlan auth-server

```
wlan auth-server <auth_profile_name>
  acct-modifier
  acctport <accounting-port>
  auth-modifier
  cppm [username <username> password <password>]
  cppm-rfc3576-only
  cppm-rfc3576-port <rfc3576-port>
  deadtime <time>
  drp-ip <IP> <mask> vlan <vlan> gateway <gateway>
  ip <host>
  key <key>
  nas-id <ID>
  nas-ip <IP-address>
  port <port>
  radsec [port <port>]
  retry-count <count>
  rfc3576
  rfc5997 {auth-only|acct-only}
  service-type-framed-user {1x|cp|mac}
  timeout <value>
  no...
```

Description

This command configures an external RADIUS server for user authentication and ClearPass Policy Manager server as a RADIUS server for AirGroup CoA requests.

Parameter	Description	Range	Default
`wlan auth-server <auth_profile_name>`	Configures the external RADIUS server authentication profile.	—	—
`acct-modifier`	Attributes modifier for accounting request.	—	—
`acctport <accounting-port>`	Configures the accounting port number used for sending accounting records to the RADIUS server.	—	1813
`auth-modifier`	Attributes modifier for access request.	—	—
`cppm [username <username> password <password>]`	Configures a **username** and **password** for the ClearPass Policy Manager server .	—	—

Parameter	Description	Range	Default
`cppm-rfc3576-only`	Configures a ClearPass Policy Manager server used for AirGroup CoA with RFC3576 only. The ClearPass Policy Manager server acts as a RADIUS server and asynchronously provides the Air Group parameters for the client device, including shared user, shared role and shared location.	—	—
`cppm-rfc3576-port <rfc3576-port>`	Configures the port number for sending AirGroup CoA, instead of the standard CoA port.	—	5999
`deadtime <time>`	Configures a dead time interval for the authentication server. When two or more authentication servers are configured on the OAW-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.	1–1440 minutes	5 minutes
`drp-ip <IP-address> <mask> vlan <vlan> gateway <gateway-IP-address>`	Configures the IP address, net mask and VLAN, which will be used as source address and VLAN for RADIUS packets. Before configuring DRP IP address, ensure that dynamic-radius-proxy is enabled, and a static virtual switch IP is configured.	—	—

Parameter	Description	Range	Default
`ip <host>`	Configures the IP address or the host name of the RADIUS server.	—	—
`key <key>`	Configures a shared key communicating with the external RADIUS server.	—	—
`nas-id <ID>`	Configures NAS identifier strings for RADIUS attribute 32, which is sent with RADIUS requests to the RADIUS server.	—	—
`nas-ip <IP>`	Configures the Virtual Controller IP address as the NAS address which is sent in data packets.	—	—
`port <port>`	Configures the authorization port number of the external RADIUS server.	—	1812
`radsec [port <port>]`	The **RadSec** command enables secure communication between the RADIUS server and OAW-IAP clients by creating a TLS tunnel between the OAW-IAP and the server. When RadSec is enabled, the **port** command can be used for specifying the communication port number for RadSec TLS connection. By default, the port number is set to 2083.	1–65534	2083

Parameter	Description	Range	Default
`retry-count <count>`	Configures the maximum number of authentication requests that can be sent to the server group.	1–5	3
`rfc3576`	Allows the OAW-IAPs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server. Disconnect messages cause a user session to be terminated immediately, whereas the CoA messages modify session authorization attributes such as data filters.	—	Disabled
`rfc5997 {auth-only|acct-only}`	When enabled, this parameter allows the OAW-IAP to send a status-server request to determine the actual status of the authentication or accounting server. This proves useful when there is a authentication or request time **rfc5997**—RFC5997 support enabled for both authentication and accounting on the authentication server. **auth-only**—RFC5997 support enabled for authentication only. acct-only—RFC5997 support enabled for accounting only **no rfc5997**—Disables RFC5997 support for the authentication server.	—	Disabled

Parameter	Description	Range	Default
`service-type-framed-user {1x|cp|mac}`	Changes the service type to frame for the following RADIUS authentication methods: ■ 1x—Changes Service-Type to Framed for 802.1X authentication. ■ cp—Changes Service-Type to Framed for Captive Portal authentication. ■ mac—Changes Service-Type to Framed for MAC authentication.	1x,cp,mac	—
`timeout <value>`	Configures a timeout value in second to determine when a RADIUS request must expire. The OAW-IAP retries to send the request several times (as configured in the Retry count), before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds.	1 to 30 seconds	5 seconds
`no…`	Removes the parameter configuration.	—	—

Example

The following example configures the external RADIUS server parameters:

```
(Instant AP)(config)# wlan auth-server RADIUS1
(Instant AP)(Auth Server <RADIUS1>)# ip 192.0.0.5
(Instant AP)(Auth Server <RADIUS1>)# key SecretKey
(Instant AP)(Auth Server <RADIUS1>)# port 1812
(Instant AP)(Auth Server <RADIUS1>)# acctport 1813
(Instant AP)(Auth Server <RADIUS1>)# cppm username admin password eTIPS123
(Instant AP)(Auth Server <RADIUS1>)# rfc3576
(Instant AP)(Auth Server <RADIUS1>)# rfc5997 auth-only
(Instant AP)(Auth Server <RADIUS1>)# no nas-id
```

```
(Instant AP)(Auth Server <RADIUS1>)# no nas-ip
(Instant AP)(Auth Server <RADIUS1>)# drp-ip 192.0.2.11 255.255.255.255 vlan 200 gateway
192.0.2.15
(Instant AP)(Auth Server <RADIUS1>)# timeout 10
(Instant AP)(Auth Server <RADIUS1>)# retry-count 3
(Instant AP)(Auth Server <RADIUS1>)# service-type-framed-user cp
(Instant AP)(Auth Server <RADIUS1>)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	The **cppm [username <username> password <password>]** parameter was added.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and authentication server profile sub-mode.

wlan captive-portal

```
wlan captive-portal
   authenticated
   background-color <background-color>
   banner-color <banner-color>
   banner-text <banner-text>
   custom-logo <name>
   decoded-texts <decoded-text>
   redirect-url <url>
   no...
   terms-of-use <terms-of-use-text>
   use-policy <policy-text>
no wlan captive-portal
```

Description

This command customizes the appearance of the internal captive portal splash page of the guest users.

Parameter	Description	Range	Default
`wlan captive-portal`	Displays the sub-mode for configuring internal captive portal splash page.	—	—
`authenticated`	Configures the authentication text. The **authenticated** text is used for indicating that the authentication mode is enabled for the internal captive portal users. When the authentication mode is enabled, the OAW-IAP displays a splash page that requires the guest users to enter their credentials. The users allowed to access the Internet only if they complete the authentication successfully.	—	—
`background-color <background-color>`	Configures the color code for the internal captive portal splash page.	Web color codes	134217772
`banner-color <banner-color>`	Configures the color code for the banner on the splash page.	Web color codes	16750848
`banner-text <banner-text>`	Configures the text displayed on splash page banner.	Text string not exceeding 127 characters	Welcome to Guest Network.
`custom-logo`	Allows you to save the customized logo to the internal captive portal server.	—	—
`decoded-texts <decoded-text>`	Displays decoded texts.	—	—

Parameter	Description	Range	Default
`redirect-url <url>`	Configures a URL to redirect the users after a successful authentication. **NOTE:** By default, after entering the requested info at the splash page, the users are redirected to the URL that was originally requested. When a URL is configured for redirection, it overrides the user's original request and redirects them to URL configured for redirection.	—	—
`terms-of-use <terms-of-use-text>`	Defines the terms and conditions that the user must be aware of.	Text string	This network is not secure, and use is at your own risk.
`use-policy <policy-text>`	Configures usage policy text for splash page.	Text string	Please read terms and conditions before using Guest Network.
`no…`	Removes the definition of the **authenticated**, **decoded text**, and **redirect-url** parameters configured under the **wlan captive-portal** command.	—	—
`no wlan captive-portal`	Removes the captive portal configuration.	—	—

Example

The following example configures the contents of the internal captive portal splash page:

```
(Instant AP)(config)# wlan captive-portal
(Instant AP)(Captive Portal)# authenticated
(Instant AP)(Captive Portal)# background-color 13421772
(Instant AP)(Captive Portal)# banner-color 16750848
(Instant AP)(Captive Portal)# banner-text "Welcome to Guest Network"
(Instant AP)(Captive Portal)# no decoded-texts
(Instant AP)(Captive Portal)# redirect-url example1.com
(Instant AP)(Captive Portal)# terms-of-use "This network is not secure, and use is at your
own risk"
(Instant AP)(Captive Portal)# use-policy "Please read terms and conditions before using Guest
Network"
(Instant AP)(Captive Portal)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 6.3.1.1-4.0.0.0	This command was modified.
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and captive portal sub-mode.

wlan external-captive-portal

```
wlan external-captive-portal [profile-name]
   auth-text <text>
   auto-whitelist-disable
   https
   port <port>
   prevent-frame-overlay
   redirect-url <redirection-url>
   out-of-service-page <url>
   server <server-name>
   server-fail-through
   switch-ip
   server-offload
   url <url>
   no…
no wlan external-captive-portal
```

Description

This command configures profiles for external captive portal. Use this command to configure external captive portal profiles for guest users. When the captive portal profile is applied to an SSID or a wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. You can create up to 8 external captive portal profiles.

Parameter	Description	Range	Default
`wlan external-captive-portal [profile-name]`	Creates an external captive portal profile. You can create multiple external captive portal profiles and apply to an SSID or a wired profile.	—	—
`auth-text <text>`	Configures the authentication text to be returned by the external server. The authentication text command configuration is required only for the External - Authentication Text splash mode.	—	—
`auto-whitelist-disable`	Disables automatic whitelisting of URLs.	—	—
`https`	Enables HTTPS for client connections.	—	—
`Port <port>`	Configures the port to use for communication with the external captive portal server.	—	80

Parameter	Description	Range	Default
`prevent-frame-overlay`	Prevents overlay of frames. when configured, a frame displays a page only if it is in the same domain as the main page.	—	—
`redirect-url <redirection-url>`	Configures a URL to redirect the users after a successful authentication. **NOTE:** By default, after entering the requested info at the splash page, the users are redirected to the URL that was originally requested. When a URL is configured for redirection, it overrides the user's original request and redirects them to URL configured for redirection.	—	—
`out-of-service-page <url>`	Configures a URL to redirect the users when the internet uplink is down.	—	—
`server <server-name>`	Configures the external captive portal server.	—	—
`server-fail-through`	Allows the guest clients to access the Internet when the external captive portal server is not available.	—	Disabled
`switch-ip`	Sends the IP address of the Virtual Controller in the redirection URL when external captive portal servers are used.	—	Disabled

Parameter	Description	Range	Default
`server-offload`	Enables the server-offload feature to reduce the load on the external captive portal server by allowing the OAW-IAP to use a Meta tag to redirect HTTP and HTTPS requests from the client. When enabled, this feature prevents the non-browser client applications from following unnecessary 302-redirects generated by their background HTTP or HTTPS requests.	—	—
`url <url>`	Configures the URL of the external captive portal server.	—	—
`no…`	Removes the definition of the following parameters configured under the **wlan external-captive-portal** command. ■ **auto-whitelist-disable** ■ **https** ■ **out-of-service-page** ■ **prevent-frame-overlay** ■ **server-fail-through** ■ **server-offload** ■ **switch-ip**	—	—
`no wlan external-captive-portal`	Removes the external captive portal configuration.	—	—

Example

The following example configures external captive portal splash page:

```
(Instant AP)(config)# wlan external-captive-portal AuthText1
(Instant AP)(External Captive Portal "AuthText1")# auth-text authenticated
(Instant AP)(External Captive Portal "AuthText1")# port 80
(Instant AP)(External Captive Portal "AuthText1")# redirect-url http://www.example1.com
(Instant AP)(External Captive Portal "AuthText1")# out-of-service-page
http://www.example2.com
(Instant AP)(External Captive Portal "AuthText1")# server CPServer1
(Instant AP)(External Captive Portal "AuthText1")# url "/example.php"
(Instant AP)(External Captive Portal "AuthText1")# server-fail-through
(Instant AP)(External Captive Portal "AuthText1")# switch-ip
```

```
(Instant AP)(External Captive Portal "AuthText1")# no auto-whitelist-disable
(Instant AP)(External Captive Portal "AuthText1")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and external captive portal sub-mode.

wlan ldap-server

```
wlan ldap-server <server-name>
   admin-dn <domain-name>
   admin-password <password>
   base-dn <base_domain-name>
   deadtime <time>
   filter <filter>
   key-attribute <key-attribute>
   ip <IP-address>
   port <port-name>
   timeout <seconds>
   retry-count <count>
   no...
no wlan ldap-server <server-name>
```

Description

This command configures a LDAP server for user authentication on the virtual switch. Use this command to configure an LDAP server as an external authentication server. The LDAP service is based on a client-server model. The OAW-IAP client requests for an LDAP session after connecting to the LDAP server and server sends its responses.

Parameter	Description	Range	Default
`wlan ldap-server <server-name>`	Configures an LDAP authentication server.	—	—
`admin-dn <domain-name>`	Configures a DN for the administrator with read and search privileges across all the entries in the LDAP database. The user need not have write privileges, but the user must be able to search the database, and read attributes of other users in the database.	—	—
`admin-password <password>`	Configures a password for administrator.	—	—
`base-dn <base-domain-name>`	Configures a DN for the node which contains the entire user database.	—	—
`deadtime <time>`	Configures a dead time interval for the authentication server. When two or more authentication servers are configured on the OAW-IAP and a server is unavailable, the dead time configuration determines the duration for which the authentication server would be available if the server is marked as unavailable.	1–1440 minutes	5 minutes

Parameter	Description	Range	Default
`filter <filter>`	Configures the filter to apply when searching for a user in the LDAP database.	strings	(objectclass=*)
`key-attribute <key-attribute>`	Configures the attribute to use as a key when searching for the LDAP server. For Active Directory, the value is **sAMAccountName**.	—	—
`ip <IP-address>`	Configures the IP address of the LDAP server.	—	—
`port <port>`	Configures the authorization port number of the LDAP server.	—	389
`timeout <seconds>`	Configures a timeout value for LDAP requests from the clients.	1–30 seconds	5 seconds
`retry-count <count>`	Defines the number of times that the clients can attempt to connect to the server.	1–5	3
`no…`	Removes the definition of the following parameters configured under the **wlan ldap-server** command. ■ **deadtime** ■ **retry-count** ■ **timeout**	—	—
`no wlan ldap-server <server-name>`	Removes the LDAP authentication server configuration.	—	—

Example

The following example configures an LDAP server:

```
(Instant AP)(config)# wlan ldap-server Server1
(Instant AP)(LDAP Server <name>)# ip 192.0.1.5
(Instant AP)(LDAP Server <name>)# port 389
(Instant AP)(LDAP Server <name>)# admin-dn cn=admin
(Instant AP)(LDAP Server <name>)# admin-password password123
(Instant AP)(LDAP Server <name>)# base-dn dc=example, dc=com
(Instant AP)(LDAP Server <name>)# filter (objectclass=*)
(Instant AP)(LDAP Server <name>)# key-attribute sAMAccountName
(Instant AP)(LDAP Server <name>)# timeout 5
(Instant AP)(LDAP Server <name>)# retry-count 3
(Instant AP)(LDAP Server <name>)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and LDAP server sub-mode.

wlan mesh-profile

```
wlan mesh-profile
   a-tx-rates
   children
   heartbeat-threshold
   hop-count
   link-threshold
   max-retries
   mesh-private-vlan
   metric-algorithm
   prefer-uplink-radio
   reselection-mode
   no
```

Description

This command configures the mesh profile for the OAW-IAP. Use this command to configure the mesh link settings for the OAW-IAP.

Parameter	Description	Range	Default
`a-tx-rates`	Configures the transmission rate at which the AP can transmit data to clients connected on the 5 GHz band. The value is defined in Mbps.	6,9,12,18,24,36,48,54	—
`children`	Configures the maximum number of mesh children APs that can be connected to the AP.	1-64	8
`heartbeat-threshold`	Configures the heartbeat threshold for mesh neighbor APs. The AP will drop connection with the neighboring AP when the missed heartbeat count exceeds the defined threshold.	1-255	12
`hop-count`	Configures the maximum number of hop counts allowed between the AP and the mesh portal. The parent mesh AP will be dynamically selected on the number of number of hop counts allowed.	1-32	2
`link-threshold`	Configures the threshold RSSI value below which mesh links incur a metric penalty.	10-90	12

Parameter	Description	Range	Default
`max-retries`	Configures the maximum number of retries the OAW-IAP attempts when the client is not responding to the 802.11 frames.	1-15	8
`mesh-private-vlan`	Configures the mesh private VLAN ID for control traffic between a remote mesh portal and mesh node.	0-4094	0
`metric-algorithm`	Configures the metric algorithm used for path selection to the mesh portal AP. The options available are: **best-link-rssi**—Combine link-RSSI with a node cost based on hop-count alone. **distributed-tree-rssi**—Combine link-RSSI with a node cost based on number of children.	distributed-tree-rssi, best-link-rssi	distributed-tree-rssi
`prefer-uplink-radio`	Configures the preferred 5 GHz radio for mesh links. Mesh link neighbors identified in this radio band will be prioritized over other neighbors identified in the other radio band. This parameter will only take effect when dual 5 GHz or split 5 GHz radio is enabled on the AP and **mesh-split5g-radio-band** is set to full.	none, 5g-lower, 5g-upper	none
`reselection-mode`	Configures the reselection mode of operation.	never, subthreshold, startup-subthreshold, anytime	startup-subthres hold
`no…`	Removes the configuration and enables communication between the AP and Activate.	—	—

Example

The following command configures the mesh profile for the OAW-IAP:

```
(Instant AP)(config) #wlan mesh-profile
(Instant AP)(Mesh Profile) # a-tx-rates 12,18,24,36,48,54
(Instant AP)(Mesh Profile) # children 10
(Instant AP)(Mesh Profile) # heartbeat-threshold 20
(Instant AP)(Mesh Profile) # hop-count 4
(Instant AP)(Mesh Profile) # link-threshold 12
(Instant AP)(Mesh Profile) # max-retries 8
```

```
(Instant AP)(Mesh Profile) # mesh-private-vlan 2
(Instant AP)(Mesh Profile) # metric-algorithm best-link-rssi
(Instant AP)(Mesh Profile) # prefer-uplink-radio 5g-lower
(Instant AP)(Mesh Profile) # reselection-mode anytime
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

wlan mpsk-local

```
wlan mpsk-local <profile_name>
   mpsk-local-passphrase <key_name> <key>
no..
```

Description

This command configures a local MPSK profile on the OAW-IAP.

Parameter	Description
`wlan mpsk-local <profile_name>`	Denotes the name of the local MPSK profile.
`   mpsk-local-passphrase <key_name> <key>`	Denotes the WPA2-PSK passphrase to be entered for a WLAN employee network.
`no..`	Removes the configuration.

Example

The following CLI commands configure a local MPSK profile:

```
(Instant AP)(config)# wlan-mpsk-local example_profile
(Instant AP)(MPSK Local "example_profile")# mpsk-local-passphrase pass 1234
(Instant AP)(MPSK Local "example_profile")# mpsk-local-passphrase test 3637
(Instant AP)(MPSK Local "example_profile")# mpsk-local-passphrase exam 6354
(Instant AP)(MPSK Local "example_profile")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and **wlan mpsk-local**configuration sub-mode.

wlan cert-assignment-profile

```
wlan cert-assignment-profile
  pki-cert-assign application <radius|captive-portal|radsec|ui|datatunnel|clearpass|webcc>
  cert-type { PublicCert| ServerCert| TrustedCA| ClientCert} certname <certname>
  no pki-cert-assign application <radius|captive-
  portal|radsec|ui|datatunnel|clearpass|webcc> cert-type { PublicCert| ServerCert|
  TrustedCA| ClientCert}
```

Description

This command configures the certificate assignments on the OAW-IAP. Certificates must be installed before they can be assigned to an application. Use this command to configure certificates that should be used for an application. The following is the list of application and the certificates types supported:

Application	Certificate Type Supported
radius	ServerCert, CA Cert
captive-portal	ServerCert
ui	
radsec	TrustedCA, ClientCert
datatunnel	
clearpass	TrustedCA
webcc	

Parameter	Description	Range
`application {radius|captive-portal|radsec|ui|datatunnel|clearpass|webcc}`	Specify the application for which you want to configure a certificate.	radius, captive-portal, radsec, ui, datatunnel, clearpass, webcc

Parameter	Description	Range
`cert-type { PublicCert| ServerCert| TrustedCA| ClientCert}`	Specify the certificate type.	PublicCert, ServerCert, TrustedCA, ClientCert
`certname <certname>`	Specify the name of the certificate. This name will be used to assign the certificate to an application.	—
`no`	Removes certificate for the specified application.	—

Example

The following commands configures a server certificate for AOS-W Instant WebUI:

```
(Instant AP)(config) # wlan cert-assignment-profile
(Instant AP) (cert assignment) # pki-cert-assign application ui cert-type ServerCert certname
UICertificate
```

The following commands removes the server certificate for AOS-W Instant WebUI:

```
(Instant AP)(config) # wlan cert-assignment-profile
(Instant AP) (cert assignment) # no pki-cert-assign application ui cert-type ServerCert
```

Related Commands

Command	Description
crypto pki-import	Imports and installs certificates on the AP.
crypto pki-remove	Removes certificates installed on the AP.
show ap checksum	Displays the number of certificates installed on the AP.
show cert assignment	Displays the list of certificates assigned to applications on the AP.

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Instant AP Platform	Command Mode
All platforms	Configuration mode.

wlan ssid-profile

```
wlan ssid-profile <ssid_profile>
   a-basic-rates <rate>
   a-max-tx-rate <rate>
   a-min-tx-rate <rate>
   a-tx-rates <rate>
   accounting-server <name>
   advertise-ap-name
   air-time-limit <limit>
   allowed-5ghz-radio <first-dot11a-radio-only | second-dot11a-radio-only | all>
   auth-pkt-mac-format {delimiter|upper-case}
   auth-req-thresh <threshold>
   auth-server <name>
   auth-survivability
   bandwidth-limit <limit>
   blacklist
   broadcast-filter {All|ARP|Unicast-ARP-Only|Disabled}
   called-station-id {type{ap-group|ap-name|ipaddr|macaddr|clan-id} |include-ssid
   [delimiter]}
   captive-portal {<type> [exclude-uplink <types>] | external [Profile <name>] [exclude-
   uplink <types>]}
   captive-portal-proxy-server <ip> <port>
   cdc-enable
   content-filtering
   deny-inter-user-bridging
   deny-intra-vlan-traffic
   deny-local-routing
   disable
   dmo-channel-utilization-threshold <threshold>
   dot11k
   dot11k-profile <profile name>
   dot11r
   dot11v
   download-role
   dot1x-timer-idrequest-period
   dot1x-wpa-key-period
   dot1x-wpa-key-retries
   dtim-period <value>
   dynamic-multicast-optimization
   enable
   enforce-dhcp
   essid <essid>
   explicit-ageout-client
   external-server
   g-basic-rates
   g-min-tx-rate <rate>
   g-max-tx-rate <rate>
   g-tx-rates
   hide-ssid
   high-efficiency-enable
   high-efficiency-disable
   high-throughput-enable
   high-throughput-disable
   no high-throughput-enable
   hotspot-profile <name>
   inactivity-timeout <interval>
   index <idx>
   key-duration <duration>
   l2-auth-failthrough
   leap-use-session-key
```

```
local-probe-req-thresh <threshold>
mac-authentication
mac-authentication-delimiter <delim>
mac-authentication-upper-case
max-authentication-failures <limit>
max-clients-threshold <Max_clients>
max-retries
max-ipv4-users <threshold>
mbo-enable
mdid <Mobility domain ID>
mfp-capable
mfp-required
multicast-rate <rate>
multicast-rate-optimization
mpdu-agg-disable
no
okc
openflow-enable
opmode <opmode>
opmode-transition
opmode-transition-disable
out-of-service <def> <name>
per-user-bandwidth-limit <limit>
priority-use-local-cache-auth
radius-accounting
radius-accounting-mode {user-association|user-authentication}
radius-interim-accounting-interval <minutes> {<seconds>}
radius-reauth-interval <minutes>
rf-band <band>
rrm-quiet-ie
rts-threshold
rx-ampdu-agg-disable
server-load-balancing
set-role <attribute> {{contains|ends-with|equals|matches-regular-expression|not-
equals|starts-with} <operand> <role>|value-of}
set-role-by-ssid
set-role-mac-auth <mac_only>
set-role-machine-auth {<machine_only>|<user_only>}
set-role-pre-auth <role>
set-role-unrestricted
set-vlan <attribute> {{contains|ends-with|equals|matches-regular-expression|not-
equals|starts-with} <operand> <vlan>|value-of}
short-preamble-disable
strict-svp
supported-mcs-set
temporal-diversity
termination
time-range <name> {enable| disable}
tspec
tspec-bandwidth
type {employee|voice|guest}
use-ip-for-calling-station
utf8
vlan
very-high-throughput-disable
vht-supported-mcs-map
vht-mu-txbf-disable
vht-txbf-explicit-enable
vlan <vlan>
wep-key <wep-key>
wispr
wmm-background-dscp <dscp>
wmm-background-share <share>
```

```
   wmm-best-effort-dscp <dscp>
   wmm-best-effort-share <share>
   wmm-uapsd-disable
   wmm-video-dscp <dscp>
   wmm-video-share <share>
   wmm-voice-dscp <dscp>
   wmm-voice-share <share>
   work-without-uplink
   wpa-passphrase <wpa-passphrase>
   zone <zone>
no wlan ssid-profile <ssid_profile>
```

Description

This command configures a WLAN SSID profile. Use this command to configure a WLAN SSID profile to set up an employee, voice, or guest network.

The following commands related to the WMM Traffic Management feature are not supported on OAW-AP203H, OAW-AP203R, OAW-AP203RP, OAW-AP207, OAW-AP228, OAW-AP277, OAW-AP200 Series, OAW-AP210 Series, OAW-AP 220 Series, OAW-340 Series, OAW-500 Series, and OAW-510 Series access points:

- **wmm-background-dscp <dscp>**
- **wmm-background-share <share>**
- **wmm-best-effort-dscp <dscp>**
- **wmm-best-effort-share <share>**
- **wmm-uapsd-disable**
- **wmm-video-dscp <dscp>**
- **wmm-video-share <share>**
- **wmm-voice-dscp <dscp>**
- **wmm-voice-share <share>**

Parameter	Description	Range	Defau lt
`wlan ssid-profile <ssid_profile>`	Creates a WLAN SSID profile.	—	—
`a-basic-rates`	Allows you to define a set of modulation rates to use for the clients on the 5 GHz radio band.	6,9,12,18,24,36, 48,54 in Mbps	6, 12, 24
`a-max-tx-rate <rate>`	Configures the specify the maximum transmission rate for the 5 GHz band.	6,9,12,18,24,36, 48,54 in Mbps	54
`a-min-tx-rate <rate>`	Configures the specify the minimum transmission rate for the 5 GHz band.	6,9,12,18,24,36, 48,54 in Mbps	6

Parameter	Description	Range	Default
`a-tx-rate <rate>`	Allows you to configure specific transmission rate at which OAW-IAP can transmit data to the clients connected on 5 GHz band.	6,9,12,18,24,36, 48,54 in Mbps	All
`accounting-server <name>`	This command configures a server for accounting purpose.	—	—
`allowed-5ghz-radio <first-dot11a-radio-only | second-dot11a-radio-only | all >`	This command configures the 5GHz radio to which the SSID should be assigned. The no allowed-5ghz-radio command removes the configuration.	—	all
`adverstise-ap-name`	When enabled, the OAW-IAP will broadcast the AP Name information in the beacons frames and probe responses.	–	–
`air-time-limit <limit>`	Configures an aggregate amount of airtime that all clients using this SSID can use for sending and receiving data.	—	—
`auth-pkt-mac-format {delimiter|upper-case}`	Configures a delimiter and upper-case characters in a MAC Address string of authentication packet or the username and password of the client. The **delimiter** and **upper-case** parameters in this command are available for all authentication methods. And without the mac-authentication-delimiter and mac-authentication-upper-case configuration, it works on the username and password for MAC Authentication.	—	—
`auth-req-thresh`	Allows you to set a threshold for authentication requests for the SSID profile.	—	—

Parameter	Description	Range	Default
`auth-server <name>`	Configures an authentication server for the SSID users.	—	—
`auth-survivability`	Enables the authentication survivability feature. The default value of the cache timeout period is 24 hours. **NOTE:** The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is applicable only when external servers such as RADIUS are configured for the SSID. When enabled, AOS-W Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.	—	Disabled
`bandwidth-limit <limit>`	Configures an aggregate amount of bandwidth that each radio is allowed to provide for the connected clients.	1–65535	—
`blacklist`	Enables dynamic blacklisting of clients.	—	—
`broadcast-filter {All|ARP|Unicast-ARP-Only|Disabled}`	Configures broadcast filtering parameters: You can configure any of the following filtering parameters: ■ **All** — When set to All, the OAW-IAP drops all broadcast and multicast frames except DHCP, ARP, igmp-group queries, and IPv6 neighbor discovery protocol.	All, ARP, Unicast-ARP-Only, Disabled	ARP

Parameter	Description	Range	Default
	■ **ARP** — When set to ARP, the OAW-IAP drops all broadcast and multicast frames except ARP, DHCP, igmp-group queries, IPv6 neighbor discovery protocol, and additionally converts ARP frames to unicast. ■ **Unicast-ARP-Only** — When set to Unicast-ARP-Only, the OAW-IAP allows all broadcast and multicast frames as it is, however the ARP requests are converted to unicast frames and sends them to the associated clients. ■ **Disabled** — When set to Disabled, the OAW-IAP routes all the broadcast and multicast frames to the wireless interfaces.		
`called-station-id {type {ap-group|ap-name|ipaddr|macaddr|vlan-id} |include-ssid [delimiter]}`	Configures the following called-station-id types: ■ **ap-group** — The Virtual Controller name is used as the called-station-id. ■ **ap-name** — The OAW-IAP hostname isused as the called-station-id. ■ **vlan-id** — The VLAN ID of the client is used as the called-station-id. ■ **ipaddr** — The IP address of the OAW-IAP is used as the called-station-id. ■ **macaddr** — The MAC address of the OAW-IAP is used as the calling-station-id. ■ **include-ssid {delimiter <delimiter>}** — The SSID is appeneded to the original called-station-id. You can optionally set a delimiter at the end.	—	called-station-id {type <macaddr>}

Parameter	Description	Range	Default
`captive-portal {<type>[exclude-uplink <types>] |external[exclude-uplink <types>| profile <name>[exclude-uplink <types>]]}`	Configures captive portal authentication for the SSID. If the external captive profiles are created, you can specify the profile name by using the **external** and **profile** keywords and associated parameters.	—	—
	You can also exclude an uplink type for the captive portal based SSID profiles. When an uplink type is selected for the **exclude-uplink** option, redirection to the captive portal based on the type of specified uplink is disabled.	3G, 4G, wifi, ethernet	—
`captive-portal-proxy-server <ip> <port>`	Allows you to specify an IP address and port number that match the proxy configuration of your browser.	—	—
`cdc-enable`	Advertizes the Cellular Data Capability (CDC) attribute of an MBO. **NOTE:** NOTE: CDC can only be enabled when MBO is enabled.	—	—
`content-filtering`	Routes all DNS requests for the non-corporate domains to the configured DNS on this network.	—	Disabled
`deny-inter-user-bridging`	Disables the bridging traffic between two clients connected to the same SSID on the same VLAN. When inter-user bridging is disabled, the clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision.	—	—

Parameter	Description	Range	Default
`deny-intra-vlan-traffic`	Disables client-to-client communication in a network. When intra vlan traffic is disabled, the IAP only fowards client traffic to gateway and configured wired servers. All other traffic from the client is dropped.	—	Disabled
`deny-local-routing`	Disables the routing traffic between two clients connected to the same SSID on different VLANs. When local routing is disabled, the clients can connect to the Internet, but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision.	—	—
`disable`	Disables the SSID. By default all SSIDs are enabled.	—	—
`dmo-channel-utilization-threshold <threshold>`	Sets a threshold for DMO channel utilization. OAW-IAP sends multicast traffic over the wireless link.	1–100 percentage value	90
`dot11k`	Enables 802.11k roaming on the SSID profile. The 802.11k protocol enables OAW-IAPs and clients to dynamically measure the available radio resources. When 802.11k is enabled, OAW-IAPs and clients send neighbor reports, beacon reports, and link measurement reports to each other.	—	—
`dot11k-profile <profile name>`	Configures a dot11k-profile to the WLAN SSID	—	—
`dot11r`	Enables 802.11r on the SSID profile.	—	—

Parameter	Description	Range	Defau lt
	802.11r or fast BSS FT is an IEEE standard that permits continuous connectivity across wireless devices during client mobility. Fast BSS Transition mechanism minimizes the delay in roaming when a client transitions from one BSS to another within the same cluster. Fast BSS Transition is operational only if the wireless client supports 802.11r standard. If the client does support 802.11r standard, it falls back to normal WPA-2 authentication method.		
`dot11v`	Enables 802.11v based BSS transition.	—	—
`download-role`	Enables user role download from ClearPass Policy Manager to the OAW-IAP	—	—
`dot1x-timer-idrequest-period`	Sets timer options for 802.1X authentication at intervals, in seconds, between identity request retries.	—	—
`dot1x-wpa-key-period`	Interval, in milliseconds, between each WPA key exchange.	—	—
`dot1x-wpa-key-retries`	Set the number of times WPA key messages are retried.	—	—
`dtim-period <value>`	Configures the DTIM interval for the SSID profile. The DTIM interval determines how often the OAW-IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersaving mode.	1–10 beacons	1

Parameter	Description	Range	Defau lt
	When configured, the client checks for buffered data on the OAW-IAP at the specified number of beacons. You can also configure a higher value for DTIM interval for power saving.		
`dynamic-multicast-optimization`	Allows the OAW-IAP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. **NOTE:** When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.	—	Disabl ed
`enable`	Re-enables the deactivated SSIDs.	—	Enable d
`enforce-dhcp`	Blocks OAW-IAP traffic to the clients that do obtain IP address from DHCP.	—	Disabl ed
`essid <essid>`	Defines a variable for each OAW-IAP that identifies a WLAN network. The OAW-IAP takes this parameter from its **per-AP-ssid** specific configuration.	—	—
`external-server`	Configures an external RADIUS server for authentication.	—	—
`explicit-ageout-client`	Allows the OAW-IAP to send a deauthentication frame to the client and clear client entry.	—	Disabl ed
`g-basic-rates`	Allows you to define a set of modulation rates to use for the clients on the 2.4 GHz radio band.	1,2,5,6,9,11,12,1 8,24,36,48,54 in Mbps	1, 2

Parameter	Description	Range	Default
`g-min-tx-rate <rate>`	Configures the specify the minimum transmission rate for the 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54 in Mbps	1
`g-max-tx-rate <rate>`	Configures the specify the maximum transmission rate for the 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54 in Mbps	54
`g-tx-rates`	Allows you to configure specific transmission rate at which the OAW-IAP can transmit data to the clients connected on 2.4 GHz band.	1,2,5,6,9,11,12,18,24,36,48,54	All
`hide-ssid`	Hides the SSID. When enabled, the SSID will not be visible for the users.	—	Disabled
`high-efficiecny-enable`	Enables the high effiency feature on 802.11ax devices	—	Enabled
`high-efficiency-disable`	Disables the high effiency feature on 802.11ax devices	—	—
`high-throughput-enable`	Enables the 802.11n high throughput functionality.	—	Enabled
`high-throughput-disable`	Disables the 802.11n high throughput functionality.	—	—
`no high-throughput-disable`	Enables the 802.11n high throughput functionality. This is an OmniVista 3600 Air Manager specific command.	—	—
`hotspot-profile <name>`	Associates a hotspot profile with the WLAN SSID profile.	—	—
`inactivity-timeout <interval>`	Configures a timeout value for the inactive client sessions. When a client session is inactive for the specified duration, the session expires and the clients are required to log in again.	60–86400 seconds	1000

Parameter	Description	Range	Default
`index <idx>`	Assigns an index value for the SSID.	—	—
`key-duration <duration>`	The r1 key timeout value in seconds for decrypt-tunnel or bridge mode.	—	—
`l2-auth-failthrough`	Allows the clients to use 802.1X authentication when MAC authentication fails.	—	Disabled
`leap-use-session-key`	Allows the users to derive session keys for LEAP authentication. Configure this command for old printers that use dynamic WEP and if you do not want use a session key from the RADIUS Server to derive pair wise unicast keys.	—	Disabled
`local-probe-req-thresh <threshold>`	Configures a RSSI threshold value to limit the number of incoming probe requests. When enabled, this command controls the system response to the broadcast probe requests sent by clients to search for the available SSIDs and ignores the probe request if required,	0–100 dB	—
`mac-authentication`	Enables MAC authentication for clients that use this SSID profile.	—	Disabled
`mac-authentication-delimiter <delim>`	Allows you to set a delimiter that can be used in the MAC address string for MAC authentication. You can specify colon or dash for delimiter. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. If you specify colon for the delimiter, the MAC addresses in the xx:xx:xx:xx:xx:xx format are used.	colon or dash	—

Parameter	Description	Range	Defau lt
`mac-authentication-upper-case`	Enables the OAW-IAP to use uppercase letters in MAC address string for MAC authentication.	—	—
`max-authentication-failures <limit>`	Configures the maximum number of authentication failures to dynamically blacklist the users. The users who exceed the number of authentication failures configured through this command are dynamically blacklisted.	—	—
`max-retries`	Denotes the maximum number of retries the OAW-IAP attempts when the client is not responding to the 802.11 frames.	1–128	8
`max-ipv4-users <threshold>`	Configures the maximum number of wired IPv4 users that can connect to the wireless client bridge.	1-32	2
`mbo-enable`	Enables the Agile Multiband Operations (MBO). Enables the mfp-capable, 802.11k and 802.11u-interworking implicitly on the AP.	—	—
`mdid`	Denotes the mobility domain identifier. An OAW-IAP uses this parameter to announce that it is a part of the OAW-IAP group that constitutes a mobility domain.	1–65535	Disabl ed
`mfp-capable`	When enabled, the SSID supports Management Frame Protection capable clients and non-MFP clients.	—	Disabl ed
`mfp-required`	When enabled, the SSID supports only the clients that exhibit the MFP functionality.	—	Disabl ed

Parameter	Description	Range	Default

`multicast-rate <rate>`	Increases the video transmission rate of the OAW-IAP. The OAW-IAPs can select the rate for video multicast frames. Ensure that you tag the multicast traffic with video priority.
	You can configure MCS rates as well. MCS is an important setting because it provides a greater throughput.
	The following information displays the MCS rate of the OAW-IAP:
	`MCS  Streams  20 MHz  20 MHz SGI`
	`---  -------  ------  ----------`
	`0    1        6.5     7.2`
	`1    1        13.0    14.4`
	`2    1        19.5    21.7`
	`3    1        26.0    28.9`
	`4    1        39.0    43.3`
	`5    1        52.0    57.8`
	`6    1        58.5    65.0`
	`7    1        65.0    72.2`
	`8    2        13.0    14.4`
	`9    2        26.0    28.9`
	`10   2        39.0    43.3`
	`11   2        52.0    57.8`
	`12   2        78.0    86.7`
	`13   2        104.0   115.6`
	`14   2        117.0   130.0`
	`15   2        130.0   144.4`
		default, 6, 9, 12, 18, 24, 36, 48, 54 Mbps
		mcs0-mcs15
			default

Parameter	Description	Range	Default
	The MCS rates for video multicast are supported in all the 802.11n-capable OAW-IAPs, and in the OAW-AP200 Series access points which are 802.11ac-capable. **NOTE:** This parameter is not supported on OAW-300 Series access points.		
`multicast-rate-optimization`	Allows the OAW-IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When enabled, the multicast traffic can be sent at the rate of 1-24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and 5 GHz is 6 Mbps.	—	Disabled
`mpdu-agg-disable`	Disables MPDU aggregation.	—	—
`no...`	Removes the parameters configured under the **wlan ssid-profile** command.	—	—
`okc`	Enables OKC. In the OKC based roaming, the OAW-IAP stores one PMK per client, which is derived from last 802.1X authentication completed by the client in the network. The cached PMK is used when a client roams to a new OAW-IAP to allow faster roaming of clients. **NOTE:** If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever it	—	Disabled

Parameter	Description	Range	Default
	roams to a new OAW-IAP. OKC is supported on WPA-2-AES Enterprise network only.		
`openflow-enable`	Configures OpenFlow to an OAW-IAP.	—	—
`opmode <opmode>`	Configures the layer-2 authentication and encryption for this SSID to protect access and ensure the privacy of the data transmitted to and from the network. You can configure any of the following types of encryption: ■ opensystem—No authentication and encryption. ■ wpa2-aes—WPA-2 with AES encryption and dynamic keys using 802.1X. ■ wpa2-psk-aes—WPA-2 with AES encryption using a preshared key. ■ wpa-tkip—WPA with TKIP encryption and dynamic keys using 802.1X. ■ wpa-psk-tkip—WPA with TKIP encryption using a PSK. ■ wpa-tkip, wpa2-aes—WPA with TKIP and WPA-2 with AES encryption. ■ wpa-psk-tkip,wpa2-psk-aes - WPS with TKIP and WPA-2 with AES encryption using a PSK. ■ static-wep—WEP with static keys. ■ dynamic-wep—WEP with dynamic keys. ■ mpsk-aes—Multiple PSK for SSID with AES encryption. ■ enhanced-open—Improved data encryption in open Wi-Fi networks and	opensystem|wpa2-aes|wpa2-psk-aes|wpa-tkip|wpa-psk-tkip|wpa-tkip,wpa2-aes|wpa-psk-tkip,wpa2-psk-aes|static-wep|dynamic-wep|mpsk-aes|enhanced-open|wpa3-sae-aes|wpa3-aes-ccm-128|wpa3-cnsa|wpa3-aes-gcm-256	opensystem

Parameter	Description	Range	Default
	protects data from sniffing. Enhanced open replaces open system as the default opmode. ■ wpa3-sae-aes—WPA3 with AES encryption using Simultaneous Authentication of Equals. ■ wpa3-aes-ccm-128—WPA3 with AES CCM-128 encryption and dynamic keys using 802.1X. ■ wpa3-cnsa—WPA3 with AES GCM-256 encryption using CNSA (192 bit). ■ wpa3-aes-gcm-256—WPA3 with AES GCM-256 encryption.		
`opmode-transition`	Enables backward compatibility for enhanced-open and wpa3-sae-aes opmodes	—	Enabled
`opmode-transition-disable`	Disables opmode transition for enhanced-open or wpa3-sae-aes opmodes	—	—
`out-of-service <def> <name>`	Enables or disables the SSID based on any of the out of service states of the OAW-IAP: ■ VPN down ■ Uplink down ■ Internet down ■ Primary uplink down The network will be out of service when selected event occurs and the SSID is enabled or disabled as per the configuration settings applied. For example, if you select the VPN down option from the dropdown and set the status to enabled, the SSID is enabled when the VPN connection is down and is disabled when the VPN connection is restored.	For out-of-service states,any of the following valies is allowed: vpn-down uplink-down internet-down primary-uplink-down For SSID status, select enable or disable.	—

Parameter	Description	Range	Default
`per-user-bandwidth-limit <limit>`	Configures a bandwidth limit in Kbps for the SSID users. **NOTE:** The bandwidth contracts can also be applied per SSID user.	1–65535 Kbps	—
`priority-use-local-cache-auth`	Authenticates clients using the local cache maintained for authentication survivability before sending out an authentication request to the RADIUS server. This feature is only supported for clients authenticated using MAC and 802.1X authentication. **NOTE:** This feature is available only when authentication survivability feature is enabled.	—	Disabled
`radius-accounting`	Enables accounting for the RADIUS server authentication. When enabled, the OAW-IAPs post accounting information to the Radius server at the specified accounting interval.	—	—
`radius-accounting-mode {user-association|user-authentication}`	Configures an accounting mode for the captive portal users. You can configure any of the following modes for accounting: ■ **user-authentication**—when configured, the accounting starts only after client authentication is successful and stops when the client logs out of the network. ■ **user-association**—When configured, the accounting starts when the client associates to the	—	user-authentication

Parameter	Description	Range	Default
	network successfully and stops when the client is disconnected.		
`radius-interim-accounting-interval <minutes> {<seconds>}`	Configures an interval for posting accounting information as RADIUS INTERIM accounting records to the RADIUS server. The **<seconds>** definition is optional. When configured, the OAW-IAP sends interim-update messages with current user statistics to the RADIUS server at regular intervals.	0–60	—
`radius-reauth-interval <minutes>`	Allows you to configure an interval after which the OAW-IAPs can redo the RADIUS transaction to reauthenticate clients. If the reauthentication interval is configured: ■ On an SSID performing L2 authentication (MAC or 802.1X authentication): When reauthentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful reauthentication. If reauthentication fails, the client retains the pre-authentication role. ■ On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When reauthentication	Any integer value in minutes	—

Parameter	Description	Range	Default
	succeeds, the client retains the role that is already assigned. If reauthentication fails, a pre-authentication role is assigned to the client. ■ On an SSID performing only L3 authentication (captive portal authentication): When reauthentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access.		
`rf-band <band>`	Configures the radio frequency band on which this SSID will be broadcast. You can select either 2.4 GHz, 5 GHz, or all to specify both bands.	2.4 GHz, 5 GHz, all	—
`rrm-quiet-ie`	Configures a radio resource management IE profile to define the information elements advertised by an OAW-IAP.	—	—
`rts-threshold <threshold>`	Configures a threshold to trigger the RTS or CTS handshake.	0–2347	2333

Parameter	Description	Range	Defau lt
	The RTS or CTS mechanism allows devices to reserve the RF medium and minimizes frame collisions introduced by the hidden stations. When RTS is enabled, a higher number of retransmissions occurring on the WLAN trigger the RTS or CTS handshake and the transmitter station sends an RTS frame to the receiver station. The receiver station responds with a CTS frame. Typically, the RTS or CTS frames are not sent, unless the packet size exceeds the RTS threshold. By default, the RTS threshold is set to 2333 octets. When the size of the packets sent by the transmitter exceeds the configured threshold, RTS frames are sent.		
`rx-ampdu-agg-disable`	When this parameter is disabled, OAW-IAPs reject A-MPDU based aggregations in the Add Block Acknowledgement response frames. This parameter can be configured on OAW-300 Series OAW-IAPs.	—	Enable d
`server-load-balancing`	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	—	Enable d
`set-role{{contains|ends-with|equals|matches-regular-expression|not-equals|starts-with} <operand> <role>|value-of}`	Assigns a user role to the clients. The first rule that matches the configured condition is applied. You can set any of the following conditions: ■ contains—The rule is applied only if the attribute value contains the specified string.	—	—

Parameter	Description	Range	Defau lt
	- ends-with—The rule is applied only if the attribute value ends with the specified string. - equals—The rule is applied only if the attribute value is equal to the specified string. - not-equals—The rule is applied only if the attribute value is not equal to the specified string. - starts-with—The rule is applied only if the attribute value begins with the specified string. - value-of - This rule sets the user role to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the OAW-IAP. - matches-regular-expression—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down.		
`set-role-by-ssid`	Configures a user role based on the type of SSID configured.	—	—
`set-role-mac-auth <mac-only>`	Configures a MAC authentication based user role.	—	—
`set-role-machine-auth <machine_only> <user_only>`	Configures a machine authentication rule. You can assign different rights to clients based on whether their hardware device supports machine authentication.	—	—

Parameter	Description	Range	Default
	Machine authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.		
`set-role-pre-auth <role>`	Configures a pre-authentication role to allow some access to the guest users before the client authentication.	—	—
`set-role-unrestricted`	Configures unrestricted access control.	—	—
`set-vlan <attribute>{{contains|ends-with|equals|matches-regular-expression|not-equals|starts-with} <operand> <vlan>|value-of}`	Assigns a VLAN to the clients. The first rule that matches the configured condition is applied. You can specify any of the following conditions: ■ contains—The rule is applied only if the attribute value contains the specified string. ■ ends-with—The rule is applied only if the attribute value ends with the specified string. ■ equals—The rule is applied only if the attribute value is equal to the specified string. ■ not-equals—The rule is applied only if the attribute value is not equal to the specified string. ■ starts-with—The rule is applied only if the attribute value begins with the specified string. ■ value-of - This rule sets the VLAN to the value of the attribute returned. To set a user role, the value of the attribute must already be configured on the OAW-IAP. ■ matches-regular-	—	—

Parameter	Description	Range	Default
	expression—The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** drop-down.		
`short-preamble-disable`	Disables the transmission and reception of short preamble frames for the clients connected to an SSID. By default, short preamble is enabled.	—	—
`strict-svp`	Enables Strict SVP and prioritizes voice traffic for SVP handsets.	—	—
`supported-mcs-set`	Allows you to define a set of MCS rates for HT channels.	0–23	0–23
`temporal-diversity`	Shows if the temporal diversity feature has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the OAW-IAP attempts two hardware retries. If the hardware retries are not successful, it attempts software retries. When this feature is disabled, the OAW-IAP attempts only hardware retries.	enable, disable	disable
`tspec`	Allows the OAW-IAPs to prioritize time-sensitive traffic such as voice traffic initiated by the client.	—	—
`tspec-bandwidth`	Reserves the configured bandwidth for prioritizing voice traffic when TSPEC is enabled.	200–600000 Kbps	2000 Kbps

Parameter	Description	Range	Default
`termination`	Configures the EAP portion of 802.1X authentication on the OAW-IAP, instead of the RADIUS server. When enabled, this command reduces network traffic to the external RADIUS server by terminating the authorization protocol on the OAW-IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the OAW-IAP acts as a relay for this exchange. The OAW-IAP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server.	—	Disabled
`time-range <name> {enable | disable}`	Specify the time range profile name to apply. ■ When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day. ■ If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.	—	—

Parameter	Description	Range	Default
`type {employee|voice|guest}`	Configures the type of network such as employee, voice, guest network.	—	—
`use-ip-for-calling-station`	The IP address of the client will be used as the calling-station-id.	—	—
`utf8`	Encodes the SSID. When enabled, the SSID name is displayed in the UTF-8 format. SSIDs are not encoded by default.	—	—
`vlan`	Configures a VLAN name or VLAN ID in the SSID profile.	—	—
`very-high-throughput-disable`	Disables VHT for clients connecting the WLAN SSID profile.	—	—
`vht-mu-txbf-disable`	Disables MU-MIMO. The MU-MIMO feature allows the 802.11ac Wave 2 OAW-IAPs to send multiple frames to multiple clients simultaneously over the same frequency spectrum. With MU-MIMO, APs can support simultaneous directional RF links and up to four simultaneous full-rate Wi-Fi connections (For example, smart phone, tablet, laptop, multimedia player or other client device). The MU-MIMO feature is enabled by default on WLAN SSIDs.	—	—
`vht-supported-mcs-map`	Allows you to define a combination of VHT MCS and spatial streams as a VHT MCS rate set.	-, 7, 8, 9	9 for each spatial stream
`vht-txbf-explicit-disable`	Disables VHT TX beamforming on the OAW-AP200 Series Series access points. This feature is available only on the OAW-AP200 Series access points.	—	—

Parameter	Description	Range	Defau lt
`vlan <vlan>`	Allows you to assign a unique VLAN ID or a VLAN name to a specified SSID user. The OAW-IAP takes this parameter from its **per AP vlan** specific configuration.	1–4095	—
`wep-key <wep-key>`	Static WEP key associated with the key index. The WEP key values can be 10 or 26 hexadecimal characters in length.	—	—
`wispr`	Enables WISPr authentication for the SSID profile.	—	—
`wmm-background-dscp <dscp>`	Allows you to specify the DSCP mapping value for the background traffic.	0–63	—
`wmm-background-share <share>`	Allocates bandwidth for background traffic such as file downloads or print jobs.	—	—
`wmm-best-effort-dscp <dscp>`	Allows you to specify the DSCP mapping value for the best effort traffic.	0–63	—
`wmm-best-effort-share <share>`	Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS.	—	—
`wmm-uapsd-disable`	Disables UAPSD on all WMM ACs. By default, UAPSD or WMM power save is enabled.	—	—
`wmm-video-dscp <dscp>`	Allows you to specify the DSCP mapping value for the video traffic.	0–63	—
`wmm-video-share <share>`	Allocates bandwidth for video traffic generated from video streaming.	—	—
`wmm-voice-dscp <dscp>`	Allows you to specify the DSCP mapping value for the voice traffic.	0–63	—

Parameter	Description	Range	Defau lt
`wmm-voice-share <share>`	Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication.	—	—
`work-without-uplink`	Allows the SSID to be used without an uplink connection. **NOTE:** In AOS-W Instant 6.4.4.4-4.2.3.0 release, the work-without-uplink is not operational. To configure SSID availability based on the uplink connection status, use the out-of-service parameter.	—	—
`wpa-passphrase <passphrase>`	Defines a WPA passphrase with which you can generate a PSK.	—	—
`zone <zone>`	Specify the zone names for the SSID profile. When the zone is defined in SSID profile and if the same zone is defined on anOAW-IAP, the SSID is created on that OAW-IAP. Enter multiple zone name as comma-separated values.	—	—
`no wlan ssid-profile <ssid_profile>`	Removes the WLAN SSID profile configuration.	—	—

Example

The following example configures an employee WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile employee1
(Instant AP)(SSID Profile "employee1")# type employee
(Instant AP)(SSID Profile "employee1")# essid employee1
(Instant AP)(SSID Profile "employee1")# enable
(Instant AP)(SSID Profile "employee1")# vlan 1
(Instant AP)(SSID Profile "employee1")# wpa-passphrase user@123
(Instant AP)(SSID Profile "employee1")# opmode wpa2-psk-aes
(Instant AP)(SSID Profile "employee1")# max-authentication-failures 0
(Instant AP)(SSID Profile "employee1")# mac-authentication
(Instant AP)(SSID Profile "employee1")# l2-auth-failthrough
(Instant AP)(SSID Profile "employee1")# termination
(Instant AP)(SSID Profile "employee1")# blacklist
(Instant AP)(SSID Profile "employee1")# cdc-enable
(Instant AP)(SSID Profile "employee1")# mbo-enable
(Instant AP)(SSID Profile "employee1")# mac-authentication
```

```
(Instant AP)(SSID Profile "employee1")# auth-server InternalServer
(Instant AP)(SSID Profile "employee1")# rf-band all
(Instant AP)(SSID Profile "employee1")# dtim-period 1
(Instant AP)(SSID Profile "employee1")# inactivity-timeout 1000
(Instant AP)(SSID Profile "employee1")# broadcast-filter none
(Instant AP)(SSID Profile "employee1")# use-ip-for-calling-station
(Instant AP)(SSID Profile "employee1")# dmo-channel-utilization-threshold 90
(Instant AP)(SSID Profile "employee1")# local-probe-req-thresh 0
(Instant AP)(SSID Profile "employee1")# max-clients-threshold 64
(Instant AP)(SSID Profile "employee1")# set-role Group-Name contains wireless employee
(Instant AP)(SSID Profile "employee1")# set-vlan mac-address-and-dhcp-options matches-
regular-expression ..link 200
(Instant AP)(SSID Profile "employee1")# no wmm-background-dscp
(Instant AP)(SSID Profile "employee1")# wmm-best-effort-dscp 21
(Instant AP)(SSID Profile "employee1")# no wmm-video-dscp
(Instant AP)(SSID Profile "employee1")# wmm-voice-dscp 46,44,42,41
(Instant AP)(SSID Profile "employee1")# zone Zone1
(Instant AP)(SSID Profile "employee1")# end
(Instant AP)# commit apply
```

The following example configures a guest WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile guestNetwork
(Instant AP)(SSID Profile "guestNetwork")# type guest
(Instant AP)(SSID Profile "guestNetwork")# essid guestNetwork
(Instant AP)(SSID Profile "guestNetwork")# enable
(Instant AP)(SSID Profile "guestNetwork")# opmode opensystem
(Instant AP)(SSID Profile "guestNetwork")# rf-band all
(Instant AP)(SSID Profile "guestNetwork")# dtim-period 1
(Instant AP)(SSID Profile "guestNetwork")# g-min-tx-rate 1
(Instant AP)(SSID Profile "guestNetwork")# g-max-tx-rate 54
(Instant AP)(SSID Profile "guestNetwork")# a-min-tx-rate 6
(Instant AP)(SSID Profile "guestNetwork")# a-max-tx-rate 54
(Instant AP)(SSID Profile "guestNetwork")# inactivity-timeout 1000
(Instant AP)(SSID Profile "guestNetwork")# vlan 1
(Instant AP)(SSID Profile "guestNetwork")# dmo-channel-utilization-threshold 90
(Instant AP)(SSID Profile "guestNetwork")# max-clients-threshold 64
(Instant AP)(SSID Profile "guestNetwork")# local-probe-req-thresh 0
(Instant AP)(SSID Profile "guestNetwork")# blacklist
(Instant AP)(SSID Profile "guestNetwork")# max-authentication-failures 3
(Instant AP)(SSID Profile "guestNetwork")# radius-interim-accounting-interval 10
(Instant AP)(SSID Profile "guestNetwork")# radius-reauth-interval 30
(Instant AP)(SSID Profile "guestNetwork")# captive-portal external
(Instant AP)(SSID Profile "guestNetwork")# mac-authentication
(Instant AP)(SSID Profile "guestNetwork")# auth-server server1
(Instant AP)(SSID Profile "guestNetwork")# set-role-by-ssid
(Instant AP)(SSID Profile "guestNetwork")# set-role-pre-auth test1
(Instant AP)(SSID Profile "guestNetwork")# end
(Instant AP)# commit apply
```

The following example configures multiple zones in a WLAN SSID profile:

```
(Instant AP)(config)# wlan ssid-profile default
(Instant AP)(SSID Profile "default") # zone zone1,zone2,zone3
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	■ The functionality of **advertise-ap-name** parameter was modified to advertise the ap-name in probe

Release	Modification
	responses. - The **radius-interim-accounting-interval <minutes>** parameters was modified to include an additional **{<seconds>}** definition.
Alcatel-Lucent AOS-W Instant 8.6.0.0	The following parameters were added: - **allowed-5ghz-radio** - **cdc-enable** - **max-ipv4-users <threshold>** - **mbo-enable** - **opmode <wpa3-aes-gcm-256>** - **priority-use-local-cache-auth**
Alcatel-Lucent AOS-W Instant 8.5.0.0	The following parameters were added: - **deny-intra-vlan-traffic** - **high-throughput-enable** - **high-throughput-disable** - **no high-throughput-disable**
Alcatel-Lucent AOS-W Instant 8.4.0.0	The following parameters were added: - **download-role** - **advertise-ap-name** - **opmode <mpsk-aes>** - **opmode <wpa3-aes-ccm-128>** - **opmode <wpa-sae-aes>** - **opmode <wpa3-cnsa>** - **opmode-transition** - **opmode-transition-disable** - **enhanced-open** - **high-efficiency-enable** - **high-efficiency-disable**
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Configuration mode and WLAN SSID profile configuration sub-mode.

wlan sta-profile

```
wlan sta-profile
   cipher-suite <clear | wpa-tkip-psk | wpa2-ccmp-psk | wpa-tkip | wpa2-ccmp>
   disable-on-mesh-point
   essid <ESSID>
   no
   uplink-band <band>
   wifi1x {peap <username> <password> | tls <tpm> <user>}
   wifi1x-eap-server <validate-server>
   wpa-passphrase <WPA-key>
   no wpa-passphrase
```

Description

This command enables Wi-Fi uplink on an OAW-IAP. Use this command to configure Wi-Fi uplink for a client station connected to an OAW-IAP.

Parameter	Description	Range	Default
`wlan sta-profile`	Configures a Wi-Fi uplink profile for an OAW-IAP.	—	—
`essid <ESSID>`	Defines a unique name for the network on which the Wi-Fi uplink will be enabled.	—	—
`cipher-suite <clear | wpa-tkip-psk | wpa2-ccmp-psk | wpa-tkip | wpa2-ccmp>`	Configures encryption settings. You can specify the following types of encryption: ■ clear—To clear a cipher suite ■ wpa-tkip-psk—To use WPA with TKIP encryption	—	—

Parameter	Description	Range	Default
	along with PSK. - wpa2-ccmp-psk—To use WPA-2 with Counter Cipher Mode with Block CCMP, an AES-based encryption mode with strong security.		
`disable-on-mesh-point`	In Mesh deployments, the configurations are synced to all peer APs, irrespective of their mesh roles. Use this command to disable the configuration of wifi uplink on mesh points. When this is configured the only the master AP uses wi-fi uplink to connect to the Internet.	—	—

Parameter	Description	Range	Default
`wpa-passphrase <WPA-key>`	Defines a WPA passphrase with which a PSK can be generated. The passphrase must be between 8 and 64 characters.	—	—
`wifi1x {peap <username> <password> | tls <tpm> <user>}`	Defines the 802.1X authentication method used. this mode is available when wpa-tkip and wpa2-ccmp modes are used.	—	—
`wifi1x-eap-server <validate-server>`	Validates the server certificate when tls method is used for 802.1X authentication.	—	—
`no wpa-passphrase`	Removes the configuration of the **wpa-passphrase** parameter.	—	—
`uplink-band <band>`	Configures the band for uplink connection. The valid options are 802.11a and 802.11g.	dot11a / dot11g	dot11g
`no wlan sta-profile`	Removes the WLAN sta-profile configuration.	—	—

Example

The following commands configure the Wi-Fi uplink profile:

```
(Instant AP)(config) # wlan sta-profile corpnet
(Instant AP)(sta uplink)# uplink-band dot11a
(Instant AP)(sta uplink)# cipher-suite wpa-tkip-psk
(Instant AP)(sta uplink)# wpa-passphrase user@123
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and Wi-Fi uplink sub-mode.

wlan tacacs-server

```
wlan tacacs-server <profile-name>
   deadtime <minutes>
   ip <IP-address>
   key <key>
   no
   port <port>
   retry-count <number>
   session-authorization
   timeout <seconds>
   no…
no tacacs-server <profile-name>
```

Description

This command is used to configure a TACACS server for management users. Use this command to configure a TACACS server as an external authentication server. This configuration applies only for management users in AOS-W Instant and not for the other SSID or wired profile users.

Parameter	Description	Range	Default
`wlan tacacs-server`	Configures the TACACS server profile.	—	—
`deadtime <minutes>`	Configures an interval.	—	—
`ip <IP-address>`	Configures the IP address of the TACACS server.	—	—
`port <port>`	Configures the TCP port for the server.	—	49
`key`	Configures a shared secret key to authenticate communication between the TACACS+ client and server.	—	—
`timeout <seconds>`	Configures a timeout value for TACACS+ requests from the management users.	—	20
`retry-count <number>`	Configures the maximum number of authentication requests that are sent to the server.	—	3
`session-authorization`	Enables session authorization for the admin users. By default, session authorization is disabled.	—	—
`no…`	Removes the definition of the following parameters configured under the **wlan tacacs-server** command. ■ **deadtime** ■ **key** ■ **port** ■ **retry-count** ■ **session-authorization** ■ **timeout**	—	—
`no tacacs-server <profile-name>`	Removes the TACACS server configuration.	—	—

Example

The following example configures the TACACS protocols:

```
(Instant AP)(config)# wlan tacacs-server Server1
(Instant AP)(TACACS Server < Server1>) # ip <10.17.121.54>
(Instant AP)(TACACS Server <Server1>) # port <49>
(Instant AP)(TACACS Server <Server1>) # key <pass123>
(Instant AP)(TACACS Server <Server1>) # timeout <30>
(Instant AP)(TACACS Server <Server1>) # retry-count <4>
(Instant AP)(TACACS Server <Server1>) # deadtime <30>
(Instant AP TACACS Server <Server1>) # end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command Introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and TACACS server profile sub-mode.

wlan walled-garden

```
wlan walled-garden
   white-list <domain>
   black-list <domain>
   no…
no wlan walled-garden
```

Description

This command configures a walled garden profile to control user access to the web content and services. A walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents. The users who do not sign up for the Internet service can view the “allowed” websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. This works for client devices with or without HTTP proxy settings. When a user attempts to navigate to other websites not in the whitelist of the walled garden profile, the user is redirected to the login page. Similarly, a blacklisted walled garden profile blocks the users from accessing some websites.

Parameter	Description	Range	Default
`wlan walled-garden`	Creates a Walled Garden profile for the OAW-IAP.	—	—
`white-list <domain>`	Configures a whitelist of URLs to allow the authenticated users to access to a specific domain. You can specify the URLs which the users can access. To allow access to various sites in the same domain, you can specify a POSIX regular expression (regex(7)). For example, **yahoo.com/*** to provide access to various domains such as **news.yahoo.com, travel.yahoo.com** and **finance.yahoo.com**. Similarly, the www.apple.com/library/test is only allow a subset of www.apple.com site corresponding to path /library/test/*.	URLs, URLs with POSIX regular expression (regex(7))	—
`black-list <domain>`	Configures a blacklist to prevent the users from accessing the websites in a specific domain. You can specify the URLs for which the user access is denied. When a URL specified in blacklist is accessed by an unauthenticated user, OAW-IAP sends an HTTP 403 response to the client with a simple error message.	URLs	—
`no…`	Removes the configuration settings of the **white-list** and **black-list** parameters.	—	—
`no wlan walled-garden`	Deletes the walled garden configuration.	—	—

Example

The following example configures a walled garden profile:

```
(Instant AP)(config)# wlan walled-garden
(Instant AP)(Walled Garden)# white-list <domain>
(Instant AP)(Walled Garden)# black-list <domain>
(Instant AP)(Walled Garden)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

wlan wispr-profile

```
wlan wispr-profile
   wispr-location-id-ac <ac>
   wispr-location-id-cc <cc>
   wispr-location-id-isocc <issoc>
   wispr-location-id-network <network>
   wispr-location-name-location <location-name>
   wispr-location-name-operator-name <operator-name>
   no...
no wlan wispr-profile
```

Description

This command configures a WISPr authentication profile for an OAW-IAP. WISPr authentication allows a smart client to authenticate on the network when they roam between WISPrs, even if the wireless hotspot uses an ISP with whom the client may not have an account. Use this command to configure a WISPr authentication profile for the captive portal users. AOS-W Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass GIS redirect, authentication, and logoff messages within HTML messages that are sent to the OAW-IAP.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine the parameter values for WISPr profile configuration. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and http://www.itu.int).

Parameter	Description
`wlan wispr-profile`	Creates a WISPr authentication profile
`wispr-location-id-ac <ac>`	Configures an E.164 Area Code for the WISPr Location ID.
`wispr-location-id-cc <cc>`	Configures an E.164 Country Code for the WISPr Location ID.
`wispr-location-id-isocc <issoc>`	Configures an ISO Country Code for the WISPr Location ID.
`wispr-location-id-network <network>`	Configures an SSID associated with the WISPr Location ID.
`wispr-location-name-location <location-name>`	Associates the Hotspot location to the WISPr profile.
`wispr-location-name-operator-name <operator-name>`	Associates the hotspot operator profile to the WISPr authentication profile.
no...	Removes the parameters configured under the **wlan wispr-profile** command.
no wlan wispr-profile	Removes the **wlan wispr-profile** command.

Example

The following commands configure a WISPr authentication profile:

```
(Instant AP)(config)# wlan wispr-profile
(Instant AP)(WISPr)# wispr-location-id-ac 408
(Instant AP)(WISPr)# wispr-location-id-cc 1
(Instant AP)(WISPr)# wispr-location-id-isocc US
(Instant AP)(WISPr)# wispr-location-id-network wispr
(Instant AP)(WISPr)# wispr-location-name-location airport
(Instant AP)(WISPr)# wispr-location-name-operator-name KNP
(Instant AP)(WISPr)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode and WISPr profile sub-mode.

write

```
write {erase <all> <reboot>|memory}
```

Description

This command saves the running configuration to memory or displays the running configuration on the screen. This command can also be used to erase the running configuration and return to factory default setting. Configuration changes made using the CLI affect only the current session. You must save your changes for them to be retained across system reboots. Changes are lost if the system reboots before saving the changes.

The following command assumes you have already saved your configuration. Reboot the OAW-IAP:

The OAW-IAP returns the following messages:

```
Do you really want to reset the system(y/n): y
System will now restart!
...
Restarting system.
```

Parameter	Description
`erase <all> <reboot>`	Erases the running system configuration file. Rebooting the OAW-IAP resets it to the factory default configuration. If you specify all, the configuration and all data in the OAW-IAP databases are erased.
`memory`	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.

Example

The following command saves your changes so they are retained after a reboot:

```
write memory

Save configuration.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode

xml-api-server

```
xml-api-server [<xml_api_server_profile>]
   ip <addr> [mask <mask>]
   key <key>
   no…
no xml-api-server [<xml_api_server_profile>]
```

Description

This command integrates an XML API interface to the OAW-IAP.

Parameter	Description	Range	Default
`xml-api-server`	Displays the sub-mode for configuring the XML API interface parameters.	—	—
`<xml_api_server_profile>`	Creates an XML API server profile.	—	—
`ip <subnet> mask [<mask]`	Configures the subnet of the XML API server. You can optionally configure the subnet mask for the XML API server.	—	—
`key <shared-key>`	Configures the key required for accessing the XML API interface.	—	—
`no…`	Removes the parameter definitions configured under the **xml-api-server** command.	—	—
`no xml-api-server[<xml_api_server_profile>]`	Removes the XML API configuration.	—	—

Example

The following command configures the XML API Server details on an OAW-IAP:

```
(Instant AP)(config)# xml-api-server test-xml
(Instant AP)(xml-api-server "test-xml")# ip 12.0.132.61
(Instant AP)(xml-api-server "test-xml")# key123
(Instant AP)(xml-api-server "test-xml")# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode

zeroize-tpm-keys

```
zeroize-tpm-keys
no…
```

Description

This command enables zeroization of FIPS-based OAW-IAPs under circumstances that present a threat to their integrity such as unauthorized removal of FIPS-based OAW-IAPs, evidence of tampering, and so on.

Parameter	Description	Range	Default
`zeroize-tpm-keys`	Zeroizes TPM keys in the OAW-IAP.	—	—
`no…`	Erases the stored keys from the OAW-IAP.	—	—

Example

The following example configures a zone name on an OAW-IAP:

```
(Instant AP)# zeroize-tpm-keys

WARNING: The effect of the action you are about to execute is not reversible.
Do you really want to zeroise the TPM keys(y/n): y
This action will void the warranty on the IAP and nullify the RMA. Are you still sure you
want to do this?(y/n)y
You are about to wipe the contents of the TPM and render the IAP permanently inoperable. Are
you ready to go ahead?(y/n):y
Running Clear Command.....
Completed Executing Clear Command.
Running tcsd -c command
Completed executing tcsd -c  Command.
TPM Keys Cleared Successfully.
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.4.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

zigbee service-profile

```
zigbee service-profile <profile_name>
   no
   panid <panid>
   permit-joining {off|on}
   radio-instance {all|external|internal}
   security {disable|enable}
```

Description

This command configures or modifies a ZigBee service profile.

Parameter	Description	Range	Default
`no`	Removes any existing configuration.	—	—
`panid`	ZigBee hexadecimal Pan identity.	auto, 0000-FFF0	—
`permit-joining`	Allow or disallow joining.	off, on	—
`radio-instance`	The IoT ZigBee radio instance.	all, external, internal	—
`security`	Enable or disable ZigBee security.	disable, enable	—

Example

The following example configures a ZigBee service profile:

```
(Instant AP)(config) #zigbee service-profile sample_zb_service_profile
(Instant AP)(ZigBee Service Profile "sample_zb_service_profile") #panid auto
(Instant AP)(ZigBee Service Profile "sample_zb_service_profile") #permit-joining on
(Instant AP)(ZigBee Service Profile "sample_zb_service_profile") #radio-instance all
(Instant AP)(ZigBee Service Profile "sample_zb_service_profile") #security enable
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Configuration mode.

zigbee socket-device-profile

```
zigbee socket-device-profile <profile-name>
   inbound {<source_endpoint>|<endpoint>|<profile>|<cluster>}
   no
   outbound {<source_endpoint>|<endpoint>|<profile>|<cluster> [aps-ack]}
```

Description

This command configures or modifies a ZigBee socket device profile.

Parameter	Description	Range	Default
`inbound`	Inbound socket from ZigBee inbound socket profile.	—	—
`<source_endpoint>`	Denotes the source endpoint value.	1-254	—
`<endpoint>`	Denotes the destination endpoint value	—	—
`<profile>`	Denotes the profile identity.	0x0000 to 0x7FFF and 0xC000 to 0xFFF	—
`<cluster>`	Denotes the destination cluster ID.	0x0000 to 0x7FFF and 0xC000 to 0xFFF	—
`no`	Removes any existing configuration.	—	—
`outbound`	Outbound socket from ZigBee outbound socket profile.	—	—
`<source_endpoint>`	Denotes the source endpoint value.	1-254	—
`<endpoint>`	Denotes the destination endpoint value	—	—
`<profile>`	Denotes the profile identity.	0x0000 to 0x7FFF and 0xC000 to 0xFFF	—
`<cluster>`	Denotes the destination cluster ID.	0x0000 to 0x7FFF and 0xC000 to 0xFFF	—
`aps-ack`	Denotes whetther APS acknowledgment is enabled.	—	—

Example

The following example configures a ZigBee socket device profile:

```
(host) [mynode] (config) #zigbee socket-device-profile sample_zb_socket_device_profile
(host) [mynode] (Zigbee Socket Device Profile "sample_zb_socket_device_profile") #inbound 1 1
1234 5678
```

```
(host) [mynode] (Zigbee Socket Device Profile "sample_zb_socket_device_profile") #outbound 1
1 7abc fc00 yes
```

Command History

Release	Modification
AOS-W Instant 8.7.0.0	Command introduced.

Command Information

Platforms	Command Mode
All platforms	Configuration mode.

zigbee use-service-profile

```
zigbee use-service-profile <profile_name>
```

Description

This command sets a zigbee service profile on an AOS-W Instant network.

Syntax

Parameter	Description	Range	Default
`<profile_name>`	Name of the Zigbee service profile.	—	—

Example

The following example sets a zigbee service profile:

```
(Instant AP)(config)# zigbee use-service-profile sample
(Instant AP)(config)# end
(Instant AP)# commit apply
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.7.0.0	Command introduced.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Configuration mode.

zonename

```
zonename <name>
no…
```

Description

This command configures a zone name for the OAW-IAP. You can configure zone settings on an OAW-IAP and the SSID profile, to assign an SSID to a specific OAW-IAP. To assign an SSID to a specific OAW-IAP, the OAW-IAP zone name must be configured on the WLAN SSID profile.

The following constraints apply to the OAW-IAP zone configuration:

- An OAW-IAP can belong to six zones and only six zones can be configured on an SSID.
- If an SSID belongs to a zone, all OAW-IAPs in this zone can broadcast this SSID. If no OAW-IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all OAW-IAPs can broadcast this SSID.

Parameter	Description	Range	Default
`zonename <name>`	Configures zone on an OAW-IAP. You can configure up to six SSID zones per AP, and up to 32 SSID zones per ssid-profile. Use comma separators when listing multiple zones.	32 –192	—
`no…`	Removes the configuration.	—	—

Example

The following example configures a zone name on an OAW-IAP:

```
(Instant AP)# zonename zoneA
```

Command History

Release	Modification
Alcatel-Lucent AOS-W Instant 8.3.0.0	The range of **zonename** parameter was updated due to support for multiple zone configuration.

Command Information

OAW-IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

Appendix A

Glossary of Terms

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the “common name”, which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account’s session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deplyed at branch office sites and are connected to the central network on a WAN link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documentss.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnp is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.