


# **Aruba Instant 6.3.1.1-4.0 Command-Line Interface**



Reference Guide

## Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFPProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.



This document describes the Aruba 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 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.

## Intended Audience

This guide is intended for customers who configure and use Aruba Instant.

## Related Documents

In addition to this document, the Aruba Instant product documentation includes the following:

- *Aruba Instant Installation Guides*
- *Aruba Instant 6.3.1.1-4.0 Quick Start Guide*
- *Aruba Instant 6.3.1.1-4.0 User Guide*
- *Aruba Instant 6.3.1.1-4.0 MIB Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Syslog Messages Reference Guide*
- *Aruba Instant 6.3.1.1-4.0 Release Notes*

## Conventions

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

**Table 1:** *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used for emphasizing important terms and to mark the titles of books.
<b>Boldface</b>	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.

Type Style	Description
<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:




---

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

---




---

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

---




---

Indicates a risk of personal injury or death.

---

## Contacting Support

### What is New in Aruba Instant 6.3.1.1-4.0

This section lists the new and modified commands in the Aruba Instant 6.3.1.1-4.0 release.

#### New Commands

The following commands are added in the Aruba Instant 6.3.1.1-4.0 release:

**Table 2:** *New Commands in 6.3.1.1-4.0*

Command	Description
ale-server	Configures Analytics and Location Engine (ALE) server details to enable IAP integration with ALE.
ale-report-interval	Configures the interval at which an IAP sends data to the Analytics and Location Engine (ALE)

**Table 2: New Commands in 6.3.1.1-4.0**

Command	Description
	server.
firewall-external-enforcement	Configures external firewall such as Palo Alto Networks (PAN) firewall to enable integration with the IAP
iap-master	Provisions an IAP as a master IAP.
proxy	Configures a HTTP proxy on an IAP for cloud image download.
restrict-corp-access	Configures restricted access to the corporate network.
restricted-mgmt-access	Configures management subnets to enable restricted access to the corporate network.
show airgroupservice-id	Displays the AirGroup service IDs configured on an IAP for its AirGroup clients.
show ale	Displays the ALE configuration details.
show ap client-match-history	Displays a historical record of the client match events and actions for the clients associated with an IAP.
show ap client-match-live	Displays the current client match events and actions for clients associated with an IAP.
show ap client-match-refused	Displays the list of clients for which the channel allocation is refused as per the client match configuration parameters.
show ap client-probe-report	Displays the client probe report for an IAP.
show ap client-view	Displays information about the clients in the AP neighborhood.
show ap debug client-match	Displays the information about the client match configuration status on an AP radio interface.
show ap debug spanning-tree	Displays the Spanning Tree Protocol (STP) information for a W-IAP if configured.
show ap pmkcache	Displays the pairwise master key (PMK) cache table for clients associated with an IAP.
show ap virtual-beacon-report	Displays a report with the MAC address details and RSSI information of an IAP.
show captive-portal-domains	Displays the internal and external Captive portal server domains.
show external-captive-portal	Displays the external Captive portal configuration details.
show lacp status	Displays the Link Aggregation Control Protocol (LACP) configuration status on an IAP.

**Table 2: New Commands in 6.3.1.1-4.0**

Command	Description
show proxy config	Displays the HTTP proxy configuration details.
telnet-server	Allows Telnet access to the Instant CLI.
vpn-gre-outside	Configures an automatic GRE tunnel for Aruba controller.

## Modified Commands

The following commands are modified in the Aruba Instant 6.3.1.1-4.0 release:

**Table 3: Modified Commands in 6.3.1.1-4.0**

Command	Description
airgroupservice	The <b>airgroupservice</b> allows you configure AirGroup services such as iTunes, Sharing, Chat, and so on. You can configure all services at once.
ams-backup-ip	The <b>ams-backup-ip</b> command is enhanced to support a backup domain name along with the backup IP address.
ams-ip	The <b>ams-ip</b> command is enhanced to support domain name along with the IP address.
arm	The <b>arm</b> command is enhanced to support client match configuration.
commit	The commit command is enhanced to provide an option ( <b>commit apply no-save</b> command) for applying the configuration changes to the cluster without saving the configuration.
copy	The <b>copy tftp</b> command is enhanced to upload customized logo images to the IAP database.
download-cert	The <b>download-cert</b> command is enhanced to allow the downloading of Captive portal server certificates from an FTP or TFTP server, or by using an HTTP URL.
ip dhcp	The <b>ip dhcp</b> command is modified to include centralized L3.
mgmt-user	The <b>mgmt-user</b> command now allows you to configure read-only users and users for the guest management interface.
show airgroup	The <b>show airgroup</b> command is enhanced to include <b>blocked-queries</b> , <b>blocked-service-id</b> , <b>internal-state statistics</b> , and <b>swarm-info</b> commands.
show airgroupservice	The <b>show airgroupservice</b> command output is enhanced to display the configuration status of all AirGroup services.
wired-port-profile	The <b>wired-port-profile</b> is modified to include the spanning-tree command parameter to allow the administrators to enable Spanning Tree Protocol (STP) for the wired profile users.
wlan access-rule	The <b>wlan access-rule</b> command is enhanced to include the <b>bandwidth-limit</b> command to allow the administrators to allocate bandwidth limit to the SSID users.
wlan auth-server	The <b>wlan auth-server</b> command is enhanced to include the dynamic RADIUS proxy configuration parameters.
wlan external-captive-	The <b>wlan external-captive-portal</b> command is enhanced to allow the administrators to

**Table 3: Modified Commands in 6.3.1.1-4.0**

Command	Description
<code>portal</code>	create multiple profiles and assign the required profiles to a WLAN SSID or wired profile.
<code>wlan ssid-profile</code>	<p>The <b>wlan ssid-profile</b> command is modified to include the following parameters:</p> <ul style="list-style-type: none"><li>● <b>okc-disable</b> – For Opportunistic Key Caching (OKC) roaming support</li><li>● <b>dot11r</b> – For 802.11r roaming support</li><li>● <b>mac-authentication-delimiter</b> – To allow the use of delimiters such as colon and dash in MAC address string.</li><li>● <b>mac-authentication-upper-case</b> – To allow the use of uppercase letters in MAC address string.</li></ul>





Instant supports the use of Command Line Interface (CLI) for scripting purposes. You can access the Instant CLI through a Secure Shell (SSH).

To enable the SSH access to the Instant CLI:

1. From the Instant UI, 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 Access Point)
User: admin
Password: *****
```

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

```
(Instant Access Point)#
```

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 Access Point)# configure terminal
```

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

```
(Instant Access Point)(config)#
```

The 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.



---

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 IAPs in a cluster. When you make configuration changes on a master IAP in the CLI, all associated 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, 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 Access Point)# commit apply
```

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

```
(Instant Access Point)# commit apply no-save
```

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

```
(Instant Access Point)# show uncommitted-config
```

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

```
(Instant Access Point)# commit revert
```

### Example:

```
(Instant Access Point) (config)# rf dot11a-radio-profile
(Instant Access Point) (RF dot11a Radio Profile)# beacon-interval 200
(Instant Access Point) (RF dot11a Radio Profile)# no legacy-mode
(Instant Access Point) (RF dot11a Radio Profile)# dot11h
(Instant Access Point) (RF dot11a Radio Profile)# interference-immunity 3
(Instant Access Point) (RF dot11a Radio Profile)# csa-count 2
(Instant Access Point) (RF dot11a Radio Profile)# spectrum-monitor
(Instant Access Point) (RF dot11a Radio Profile)# end
```

```
(Instant Access Point)# show uncommitted-config
  rf dot11a-radio-profile
  no legacy-mode
  beacon-interval 200
  no dot11h
  interference-immunity 3
  csa-count 1
  no spectrum-monitor
```

```
Instant Access Point# commit apply
```

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

## Using Sequence Sensitive Commands

The Instant CLI does not support positioning or precedence of sequence-sensitive commands. Therefore, 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
<code>opendns &lt;username &lt;password&gt;</code>	<code>no opendns</code>
<code>rule &lt;dest&gt; &lt;mask&gt; &lt;match&gt; &lt;protocol&gt; &lt;start-port&gt; &lt;end-port&gt; {permit  deny   src-nat   dst-nat {&lt;IP-address&gt; &lt;port&gt;  &lt;port&gt;}}[&lt;option1...option9&gt;]</code>	<code>no rule &lt;dest&gt; &lt;:mask&gt; &lt;match&gt; &lt;protocol&gt; &lt;start-port&gt; &lt;end-port&gt; {permit   deny   src-nat   dst-nat}</code>
<code>mgmt-auth-server &lt;auth-profile-name&gt;</code>	<code>no mgmt-auth-server &lt;auth-profile-name&gt;</code>
<code>set-role &lt;attribute&gt;{{equals  not-equals  starts-with  ends-with  contains} &lt;operator&gt; &lt;role&gt;  value-of}</code>	<code>no set-role &lt;attribute&gt;{{equals  not-equals  starts-with  ends-with  contains} &lt;operator&gt;  value-of}</code> <code>no set-role</code>
<code>set-vlan &lt;attribute&gt;{{equals  not-equals  starts-with  ends-with  contains} &lt;operator&gt; &lt;VLAN-ID&gt;  value-of}</code>	<code>no set-vlan &lt;attribute&gt;{{equals  not-equals  starts-with  ends-with  contains} &lt;operator&gt;  value-of}</code> <code>no set-vlan</code>
<code>auth-server &lt;name&gt;</code>	<code>no auth-server &lt;name&gt;</code>

## Saving Configuration Changes

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

```
(Instant Access Point) # 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 Access Point)# write memory
```

## Commands that Reset the IAP

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

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

Address/Identifier	Description
Netmask address	For subnet addresses, specify a subnet mask in dotted decimal notation (for example, 255.255.255.0).
Media Access Control (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).
Service Set Identifier (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).
Basic Service Set Identifier (BSSID)	This entry is the unique hard-wireless MAC address of the AP. 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.
Extended Service Set Identifier (ESSID)	Typically the unique logical name of a wireless network. If the ESSID includes spaces, enclose the name in quotation marks.

## aaa test-server

```
aaa test-server <servername> <username>
```

### Description

This command tests a configured authentication server.

### Syntax

Parameter	Description
<servername>	Allows you to specify the authentication server for which the authentication test is run.
<username>	Allows you to specify the user name for which the authentication test is run.

### Usage Guidelines

Use this command to view the CPU load for application and system processes. This command allows you to verify a configured RADIUS authentication server or the internal database. You can use this command to check for an “out of service” RADIUS server.

### Example

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

```
Authentication is successful
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## a-channel

a-channel <channel> <tx-power>

### Description

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

### Syntax

Parameter	Description	Range
<channel>	Configures the specified 5 GHz channel.	The valid channels for a band are determined by the AP regulatory domain.
<tx-power>	Configures the specified transmission power values.	0-127 dBm

### Usage Guidelines

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

### Example

The following example configures the 5 GHz radio channel:

```
(Instant Access Point)# a-channel 44 18
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

### Syntax

Parameter	Description	Range
<gain>	Configures the antenna gain. You can configure a gain value in dBi for the following types of antenna: <ul style="list-style-type: none"><li>• Dipole/Omni</li><li>• Panel</li><li>• Sector</li></ul>	Diploe/Omni - 6 Panel -14 Sector - 14

### Usage Guidelines

If your IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's Equivalent Isotropically Radiated Power (EIRP) is in compliance with the limit specified by the regulatory authority of the country in which the 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 AP device supports external antenna connectors, see the *Install Guide* that is shipped along with the AP 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):

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$

The following table describes this formula:

**Table 7:** Formula Variable Definitions

Formula Element	Description
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 [www.arubanetworks.com](http://www.arubanetworks.com).

### Example

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

```
(Instant Access Point)# a-external-antenna 14
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## aeroscout-rtls

```
aeroscout-rtls <IP-address> <Port> [include-unassoc-sta]
no...
```

### Description

This command configures the Aeroscout Real-Time Asset Location Server (RTLS) settings for Instant and sends the Radio-frequency identification (RFID) tag information to an Aeroscout RTLS server.

### Syntax

Command/Parameter	Description	Default
<IP-address>	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 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 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 IAP are sent to the AeroScout RTLS. You can also send the RFID tag information for the stations that are not associated with any IAP.

### Example

The following example configures the Aeroscout RTLS server:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	Command was introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# airgroup

```
airgroup
  cppm enforce-registration
  cppm-query-interval <interval>
  cppm-server <server-name>
  disable
  enable
  enable-guest-multicast
  multi-swarm
  no...
```

## Description

This command configures the AirGroup settings for Instant.

## Syntax

Parameter	Description	Range	Default
cppm enforce-registration	Enforces the discovery of the CPPM registered devices. When enabled, only devices registered with CPPM will be discovered by Bonjour® devices, based on the CPPM policy configured.	–	Enabled
cppm-query-interval <interval>	Configures a time interval at which 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	Enables the AirGroup feature.	–	–
enable-guest-multicast	Allows the users to use the Bonjour services enabled in a guest VLAN. When enabled, the Bonjour devices will be visible only in the guest VLAN and AirGroup will not discover or enforce policies in guest VLAN.	–	–
multi-swarm	Enables inter cluster or intra cluster mobility. <ul style="list-style-type: none"><li>• In the Intra Cluster model, the IAP does not share the Multicast DNS (mDNS) database information with the other clusters.</li><li>• In the Inter Cluster model, the IAP shares the mDNS database information with the other clusters. The mDNS records in the Virtual Controller can be shared with the all the Virtual Controllers specified for L3 Mobility.</li></ul>	–	Disabled
no...	Removes the specified configuration parameter.	–	–

## Usage Guidelines

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

## Example

The following example configures an AirGroup profile:

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

## airgroupservice

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

### Description

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

### Syntax

Parameter	Description	Default
<AirGroup-service>	<p>Specifies the AirGroup service to configure.</p> <p>The following services are available for IAP clients:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• AirPrint™– Apple® AirPrint™ allows you to print from an iPad®, iPhone®, or iPod® Touch directly to any AirPrint™ compatible printers.</li><li>• iTunes– iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple® devices.</li><li>• RemoteMgmt– Use this service for remote login, remote management, and FTP utilities on Apple® devices.</li><li>• 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.</li><li>• Chat– The iChat® (Instant Messenger) application on Apple® devices uses this service.</li></ul> <p>You can allow all services or add custom services. Up to 10 services can be configured on an IAP.</p>	–
<description>	Adds a description to the AirGroup Service profile.	–
disallow-role <role>	Restricts the user roles specified for role from accessing the AirGroup service.	Disabled
disallow-vlan <VLAN-ID>	Restricts the users assigned to these VLANs from accessing the AirGroup service.	Disabled
enable	Enables the AirGroup service for the profile.	–
disable	Disables AirGroup services for the profile.	–
id <AirGroupservice-ID>	<p>Indicates the AirGroup service ID, which is the name of a Bonjour service offered by a Bonjour-enabled device or application.</p> <p><b>NOTE:</b> The service IDs cannot be added for the pre-configured services.</p>	–
no...	Removes the AirGroup service configuration.	–

## Usage Guidelines

Use this command to enforce AirGroup service policies and define the availability of a Bonjour services such as Apple® AirPrint and AirPlay for an AirGroup profile. When configuring Bonjour 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 Access Point) (config) # airgroupservice AirPlay
(Instant Access Point) (airgroup-service) # id 23
(Instant Access Point) (airgroup-service) # description AirPlay Service
(Instant Access Point) (airgroup-service) # disallow-role guest
(Instant Access Point) (airgroup-service) # disallow-vlan 200
(Instant Access Point) (airgroup-service) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

## airwave-rtls

```
airwave-rtls <IP-address> <Port> <key> <frequency> [include-unassoc-sta]
no...
```

### Description

This command integrates AirWave Real-Time Asset Location Server (RTLS) settings for Instant and sends the Radio-frequency identification (RFID) tag information to an AirWave RTLS server with the RTLS feed to accurately locate the wireless clients.

### Syntax

Command/Parameter	Description	Default
<IP-address>	Configures the IP address of the AirWave RTLS server.	–
<Port>	Configures the port for the AirWave 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 AirWave RTLS server for the client stations that are not associated to any IAP (unassociated stations).	Disabled
no...	Removes the specified configuration parameter.	–

### Usage Guidelines

Use this command to send the RFID tag information to AirWave RTLS. Specify the IP address and port number of the AirWave 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 AirWave RTLS:

```
(Instant Access Point) (config) # airwave-rtls ams-ip 192.0.2.3 3030 pass@1234 5 include-unasso
c-sta
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP sends data to the Analytics and Location Engine (ALE) server.

### Syntax

Command/Parameter	Description	Range	Default
ale-report-interval <seconds>	Configures an interval at which the Virtual Controller can report the 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 IAP and ALE server communication.

### Example

The following example configures the ALE server details:

```
(Instant Access Point) (config) # ale-report-interval 60
```

### Command History

Version	Description
Aruba Instant6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## ale-server

```
ale-server <server>  
no...
```

### Description

This command configures Analytics and Location Engine (ALE) server details for IAP integration with ALE.

### Syntax

Command/Parameter	Description
ale-server <server>	Allows you to specify the Fully Qualified Domain Name (FQDN) or IP address of the ALE server.
no...	Removes the specified configuration parameter.

### Usage Guidelines

Use this command to enable an IAP for ALE support.

### Example

The following example configures the ALE server details:

```
(Instant Access Point) (config) # ale-server AleServer1
```

### Command History

Version	Description
Aruba Instant6.3.1.1-4.0	This command is introduced.

### Command Information

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 Application Layer Gateway (ALG) protocols enabled on an IAP. An application-level gateway consists of a security component that augments a firewall or NAT used in a network.

## Syntax

Command/Parameter	Description	Default
sccp-disable	Disables the Skinny Call Control Protocol (SCCP).	Enabled
sip-disable	Disables the Session Initiation Protocol (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 Access Point) (config) # alg
(Instant Access Point) (ALG) # sccp-disable
(Instant Access Point) (ALG) # no sip-disable
(Instant Access Point) (ALG) # no ua-disable
(Instant Access Point) (ALG) # no vocera-disable
(Instant Access Point) (ALG) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP cluster.

## Syntax

Command/Parameter	Description
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 IAP cluster.

## Example

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

```
(Instant Access Point) (config) # allow-new-aps
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## allowed-ap

```
allowed-ap <MAC-address>  
no...
```

### Description

This command allows an AP to join the IAP cluster.

### Syntax

Command/Parameter	Description
allowed-ap <MAC-address>	Specifies the MAC address of the IAP that is allowed to join the cluster.
no...	Removes the specified configuration parameter.

### Usage Guidelines

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

### Example

The following command configures an allowed IAP:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration 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 AirWave Management server.

### Syntax

Parameter	Description
<IP-address or domain name>	Configures the IP address or domain name of the secondary AirWave Management Server.
no...	Removes the specified configuration parameter.

### Usage Guidelines

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

### Example

The following command configures an AirWave backup server.

```
(Instant Access Point) (config) # ams-backup-ip 192.0.2.1
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# ams-identity

ams-identity <Name>

## Description

This command uniquely identifies the group of IAPs managed or monitored by the AirWave Management console. The name can be a location, vendor, department, or any other identifier.

## Syntax

Parameter	Description
ams-identity <Name>	Configures a name that uniquely identifies the IAP on the AirWave Management server. The name defined for this command will be displayed under the <b>Groups</b> tab in the AirWave user interface.

## Usage Guidelines

Use this command to assign an identity for the IAPs monitored or managed by the AirWave Management Server.

## Example

The following command configures an AirWave identifier:

```
(Instant Access Point)(config)# ams-identity aruba
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 AirWave Management console for an IAP.

### Syntax

Parameter	Description
<IP-address or domain name>	Configures the IP address or domain name of an AirWave Management server for an IAP.

### Usage Guidelines

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

### Example

The following command configures the AirWaveManagement Server.

```
(Instant Access Point) (config)# ams-ip 192.0.1.2
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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
<key>	Authorizes the first Virtual Controller to communicate with the AirWave 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 AP in the IAP network.

### Example

The following command configures the shared key for the AirWave management server.

```
(Instant Access Point) (config) # ams-key key@789
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## arm

arm

```
80mhz-support
a-channels <a-channel>
air-time-fairness-mode {<default-access>| <fair-access>| <preferred-access>}
band-steering-mode {balance-bands|prefer-5ghz| force-5ghz| disable}
client-aware
client-match [calc-interval <seconds>| calc-threshold <threshold> | debug <level>| holdtime
<number> | max-adoption <count>| max-request <count> |nb-matching <percentage> | slb-mode
<mode>
g-channels
max-tx-power
min-tx-power
scanning
wide-bands {<none>| <all>| <2.4>| <5>}
no...
```

### Description

This command assigns an Adaptive Radio Management (ARM) profile for an IAP and configures ARM features such as band steering, spectrum load balancing, airtime fairness mode, and access control features.

### Syntax

Command/Parameter	Description	Range	Default
80mhz-support	Enables the use of 80 MHz channels on APs with 5GHz radios, which support a very high throughput. <b>NOTE:</b> Only the APs 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: <ul style="list-style-type: none"><li>• default-access – To provide access based on client requests. When this mode is configured, the per user and per SSID bandwidth limits are not enforced.</li><li>• fair-access – To allocate Airtime evenly across all the clients.</li><li>• preferred-access – To set a preference where 11n clients are assigned more airtime than 11a/11g. The 11a/11g clients get more airtime than 11b. The ratio is 16:4:1.</li></ul>	default-access, fair-access, preferred-access	default-access
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	balance-bands, prefer-5ghz, force-5ghz,	balance-bands

Command/Parameter	Description	Range	Default
	<p>GHz band than on the 2.4 GHz band. You can configure any of the following band-steering modes:</p> <ul style="list-style-type: none"> <li>prefer-5ghz – To allow the IAP to steer the client to 5 GHz band (if the client is 5 GHz capable). However, the IAP allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association.</li> <li>force-5ghz – To enforce 5 GHz band steering mode on the IAPs, so that the 5 GHz capable clients are allowed to use only the 5GHz channels.</li> <li>balance-bands – To allow the IAPs to balance the clients across the two 2.4 GHz and 5 GHz radio and to utilize the available bandwidth.</li> <li>disable – To allow the clients to select the bands.</li> </ul>	disable	
client-aware	Enables the client aware feature. When enabled, the 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 APs. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients.If spectrum load balancing is triggered and a client's Received Signal Strength Indication (RSSI) is or less than 20 dB , clients are moved from one AP to another for better performance and client experience. In the current release, the client match feature is supported only within an IAP cluster.		
calc-interval<seconds>	Configures an interval at which client match is calculated.	10-600	30 seconds
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 AP reaches or exceeds the threshold in comparison, client match is enabled on that AP.	1-20	2
debug <level>	Displays information requires for debugging client match issues.	0-4 0–none, 1–error, 2–	0

Command/Parameter	Description	Range	Default
		information, 3–debug, 4–dump	
holdtime <number>	Configures a hold time for client match.	1–1800	900
max-adoption <count>	Configure a maximum number for adopting clients.	0-100	5
max-request <count>	Configures the maximum number of requests for client match.	0-100	5
nb-matching <percentage>	Configures a percentage value to be considered in the same virtual RF neighborhood of Client match.	20-100%	75%
slb-mode <mode>	Configures a balancing strategy for client match.	1–3 1–Channel-based 2–Radio-based 3–Channel and Radio based	1
g-channels <g-channel>	Configures 2.4 GHz channels.	–	–
min-tx-power <power>	Sets the minimum transmission power. This indicates the minimum Effective Isotropic Radiated Power (EIRP). If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting.	0-127 dBm	18
max-tx-power <power>	Sets the highest transmit power levels for the AP. If the maximum transmission EIRP configured on an AP is not supported by the AP model, the value is reduced to the highest supported power setting.  <b>NOTE:</b> Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	0-127 dBm	127
scanning	Allows the IAPs to scan other channels for RF Management and Wireless Intrusion Protection System enforcement.	–	Disabled
wide-bands {<none>  <all>  <2.4>  <5>}	Allows administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded	none, all, 2.4, and 5	5

Command/Parameter	Description	Range	Default
	together. The 40 MHz channels double the frequency bandwidth available for data transmission. For high performance, enter 5GHz. If the AP density is low, enter 2.4GHz.		
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 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 Access Point) (config) # arm
(Instant Access Point) (ARM) # 80mhz-support
(Instant Access Point) (ARM) # a-channels 44
(Instant Access Point) (ARM) # min-tx-power 18
(Instant Access Point) (ARM) # max-tx-power 127
(Instant Access Point) (ARM) # band-steering-mode prefer-5ghz
(Instant Access Point) (ARM) # air-time-fairness-mode fair-access
(Instant Access Point) (ARM) # scanning
(Instant Access Point) (ARM) # client-aware
(Instant Access Point) (ARM) # client-match
(Instant Access Point) (ARM) # wide-bands 5
(Instant Access Point) (ARM) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

Command/Parameter	Description
drop-bad-arp-enable	Enables the IAP to block the bad ARP request.
fix-dhcp-enable	Enables the IAP to fix the malformed DHCP packets.
poison-check-enable	Enables the IAP to trigger an alert notifying the user about the ARP poisoning that may have been caused by the rogue APs.
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 Access Point) (config) # attack
(Instant Access Point) (ATTACK) # drop-bad-arp-enable
(Instant Access Point) (ATTACK) # fix-dhcp-enable
(Instant Access Point) (ATTACK) # poison-check-enable
(Instant Access Point) (ATTACK) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAPs to dynamically blacklist the clients when they exceed the authentication failure threshold.

### Syntax

Parameter	Description	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 Access Point) (config) # auth-failure-blacklist-time 60
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 Access Point) (config)# auth-survivability cache-time-out 60
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	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.

### Syntax

Parameter	Description
<code>blacklist-client &lt;MAC-address&gt;</code>	Adds the MAC address of the client to the blacklist.
<code>no...</code>	Removes the specified configuration parameter.

### Usage Guidelines

Use this command to blacklist the MAC addresses of clients.

### Example

The following command blacklists an IAP client:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

### Syntax

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

### Usage Guidelines

Use this command to configure the duration in seconds for which the clients can be blacklisted when the blacklisting rule is triggered.

### Examples

The following command configures the duration for blacklisting clients:

```
(Instant Access Point) (config) # blacklist-time 30
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## calea

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

### Description

This command creates a Communications Assistance for Law Enforcement Act (CALEA) profile to enable IAPs for Lawful Intercept (LI) compliance and CALEA integration.

### Syntax

Command/Parameter	Description	Range	Default
calea	Enables <b>calea</b> configuration sub-mode for CALEA profile configuration.	–	–
encapsulation-type <gre>	Specifies the encapsulation type for Generic Routing Encapsulation (GRE) packets.	GRE	GRE
ip <IP-address>	Configures the IP address of the CALEA server on a IAP.	–	–
ip mtu <size>	Configures the Maximum Transmission Unit size to use.	68–1500	1500
gre-type	Specifies GRE type.	–	25944
no...	Removes the configuration	–	–

### Usage Guidelines

Use this command to configure a IAP to support Lawful Intercept (LI). LI allows the Law Enforcement Agencies (LEA) to conduct an authorized electronic surveillance. Depending on the country of operation, the service providers (SPs) 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 IAPs for CALEA integration, see *Aruba Instant User Guide*.

### Example

The following example configures a CALEA profile:

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

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-isp <modem_isp>
  modem-country <modem-country>
  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>
  modem-isp <modem_isp>
  modem-country <modem-country>
  no...
```

### Description

This command provisions the cellular (3G/4G) uplink profiles on an IAP. Contact your IT administrator or the manufacturer of your modem to obtain the parameter details for command execution.

### Syntax

Parameter	Description	Range	Default
cellular-uplink-profile <profile>	Configures a 3G or 4G cellular profile for an IAP.	–	–
4g-usb-type <4G-usb-type>	Configures the driver type for the 4G modem.	ether-lte, pantech-lte, none	–
modem-isp <modem_isp>	Specifies the name of the ISP to connect.	–	–
modem-country <modem-country>	Specifies the country for the deployment.	–	–
usb-auth-type <usb_authentication_type>	Specifies the authentication type for USB.	PAP, CHAP	PAP
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.	–	–

Parameter	Description	Range	Default
usb-modeswitch <usb-modeswitch>	Specifies the parameter used to switch modem from storage mode to modem mode.	–	–
usb-type <usb-type>	Configures the driver type for the 3G modem.	acm, airprime, hso, option, pantech-3g, sierra-evdo, sierra-gsm,none	–
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 specified configuration parameter.	–	–

## Usage Guidelines

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



The 3G and 4G LTE USB modems can be provisioned on RAP-3WN/3WNP and RAP-155/155P.

## Types of Modems

Instant supports the following three types of 3G modems:

- **True Auto Detect**– Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country**– Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect**– Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Instant when the appropriate parameters are configured.

The following table lists the types of supported 3G modems:

**Table 8:** List of Supported 3G Modems

Modem Type	Supported 3G Modems
True Auto Detect	<ul style="list-style-type: none"> <li>• USBConnect 881 (Sierra 881U)</li> <li>• Quicksilver (Globetrotter ICON 322)</li> <li>• UM100C (UTstarcom)</li> <li>• Icon 452</li> <li>• Aircard 250U (Sierra)</li> </ul>

**Table 8:** List of Supported 3G Modems

Modem Type	Supported 3G Modems
	<ul style="list-style-type: none"> <li>● USB 598 (Sierra)</li> <li>● U300 (Franklin wireless)</li> <li>● U301 (Franklin wireless)</li> <li>● USB U760 for Virgin (Novatel)</li> <li>● USB U720 (Novatel/Qualcomm)</li> <li>● UM175 (Pantech)</li> <li>● UM150 (Pantech)</li> <li>● UMW190(Pantech)</li> <li>● SXC-1080 (Qualcomm)</li> <li>● Globetrotter ICON 225</li> <li>● UMG181</li> <li>● NTT DoCoMo L-05A (LG FOMA L05A)</li> <li>● NTT DoCoMo L-02A</li> <li>● ZTE WCDMA Technologies MSM (MF668?)</li> <li>● Fivespot (ZTE)</li> <li>● c-motech CNU-600</li> <li>● ZTE AC2736</li> <li>● SEC-8089 (EpiValley)</li> <li>● Nokia CS-10</li> <li>● NTT DoCoMo L-08C (LG)</li> <li>● NTT DoCoMo L-02C (LG)</li> <li>● Novatel MC545</li> <li>● Huawei E220 for Movistar in Spain</li> <li>● Huawei E180 for Movistar in Spain</li> <li>● ZTE-MF820</li> <li>● Huawei E173s-1</li> <li>● Sierra 320</li> <li>● Longcheer WM72</li> <li>● U600 (3G mode)</li> </ul>
<p><b>Auto-detect + ISP/country</b></p>	<ul style="list-style-type: none"> <li>● Sierra USB-306 (HK CLS/1010 (HK))</li> <li>● Sierra 306/308 (Telstra (Aus))</li> <li>● Sierra 503 PCle (Telstra (Aus))</li> <li>● Sierra 312 (Telstra (Aus))</li> <li>● Aircard USB 308 (AT&amp;T's Shockwave)</li> <li>● Compass 597(Sierra) (Sprint)</li> <li>● U597 (Sierra) (Verizon)</li> <li>● Tstick C597(Sierra) (Telecom(NZ))</li> <li>● Ovation U727 (Novatel) (Sprint)</li> <li>● USB U727 (Novatel) (Verizon)</li> <li>● USB U760 (Novatel) (Sprint)</li> <li>● USB U760 (Novatel) (Verizon)</li> <li>● Novatel MiFi 2200 (Verizon Mifi 2200)</li> <li>● Huawei E272, E170, E220 (ATT)</li> <li>● Huawei E169, E180,E220,E272 (Vodafone/SmarTone (HK))</li> <li>● Huawei E160 (O2(UK))</li> <li>● Huawei E160 (SFR (France))</li> <li>● Huawei E220 (NZ and JP)</li> <li>● Huawei E176G (Telstra (Aus))</li> <li>● Huawei E1553, E176 (3/HUTCH (Aus))</li> <li>● Huawei K4505 (Vodafone/SmarTone (HK))</li> <li>● Huawei K4505 (Vodafone (UK))</li> <li>● ZTE MF656 (Netcom (norway))</li> <li>● ZTE MF636 (HK CSL/1010)</li> <li>● ZTE MF633/MF636 (Telstra (Aus))</li> </ul>

**Table 8: List of Supported 3G Modems**

Modem Type	Supported 3G Modems
	<ul style="list-style-type: none"> <li>• ZTE MF637 (Orange in Israel)</li> <li>• Huawei E180, E1692,E1762 (Optus (Aus))</li> <li>• Huawei E1731 (Airtel-3G (India))</li> <li>• Huawei E3765 (Vodafone (Aus))</li> <li>• Huawei E3765 (T-Mobile (Germany))</li> <li>• Huawei E1552 (SingTel)</li> <li>• Huawei E1750 (T-Mobile (Germany))</li> <li>• UGM 1831 (TMobile)</li> <li>• Huawei D33HW (EMOBILE(Japan))</li> <li>• Huawei GD01 (EMOBILE(Japan))</li> <li>• Huawei EC150 (Reliance NetConnect+ (India))</li> <li>• KDDI DATA07(Huawei) (KDDI (Japan))</li> <li>• Huawei E353 (China Unicom)</li> <li>• Huawei EC167 (China Telecom)</li> <li>• Huawei E367 (Vodafone (UK))</li> <li>• Huawei E352s-5 (T-Mobile (Germany))</li> </ul>
No auto-detect	<ul style="list-style-type: none"> <li>• Huawei D41HW</li> <li>• ZTE AC2726</li> </ul>

**Table 9: 4G Supported Modem**

Modem Type	Supported 4G Modem
True Auto Detect	<ul style="list-style-type: none"> <li>• Pantech UML290</li> <li>• Ether-lte</li> </ul>



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

The following example configures a cellular uplink profile:

```
(Instant Access Point) (config) # cellular-uplink-profile
(Instant Access Point) (cellular-uplink-profile) # 4g-usb-type pantech-lte
(Instant Access Point) (cellular-uplink-profile) # modem-country India
(Instant Access Point) (cellular-uplink-profile) # modem-isp example
(Instant Access Point) (cellular-uplink-profile) # usb-auth-type PAP
(Instant Access Point) (cellular-uplink-profile) # usb-user user1
(Instant Access Point) (cellular-uplink-profile) # usb-passwd user123
(Instant Access Point) (cellular-uplink-profile) # modem-country India
(Instant Access Point) (cellular-uplink-profile) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.



## Command Information

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

## clear

```
clear
  ap <ip-address>
  arp <ip-address>
  client <mac>
  datapath {session-all| statistics}
```

### Description

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

### Syntax

Parameter	Description
ap <ip-address>	Clears all IAP related information.
arp <ip-address>	Clears all ARP table information for an IAP.
client <mac>	Clears all information pertaining to an 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 IAP.

### Example

The following command clears all information related to an IAP:

```
(Instant Access Point)# clear ap 192.0.2.3
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC 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 IAP database.

### Example

The following command clears AirGroup statistics:

```
(Instant Access Point)(config)# clear airgroup state statistics
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## clear-cert

```
clear-cert {ca| server}
```

### Description

This command clears client and server certificates from the IAP database.

### Syntax

Parameter	Description
ca	Clears all certificates uploaded for the client system.
server	Clears all Server certificates.

### Usage Guidelines

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

### Example

The following command shows an example for clearing server certificates:

```
(Instant Access Point)# clear-cert server
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## clock set

clock set <year> <month> <day> <time>

### Description

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

### Syntax

Parameter	Description	Range
<year>	Sets the year. Requires all 4 digits.	Numeric
<month>	Sets the month.	1-12
<day>	Sets the day.	1-31
<time>	Sets the time. Specify hours, minutes, and seconds separated by spaces.	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 Access Point)# clock set 2013 5 21 1 3 52
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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> <week> <eday> <emonth> <ehour>  
no...
```

### Description

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

### Syntax

Parameter	Description	Range
clock summer-time <timezone>	Configures Daylight Saving time.	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
<week>	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 daylight saving time ensures that the IAPs reflect the seasonal time changes in the region they serve.

### Example

The following example configures daylight saving for a timezone:

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description	Range
clock timezone <name>	Configures the required timezone.	All supported timezones
<hour-offset>	Specifies the hours offset from the Universal Time Clock (UTC).	–
<minute-offset>	Specifies the hours offset from the Universal Time Clock (UTC).	–
no...	Removes the timezone configuration.	–

### Usage Guidelines

Use this command to set the timezone on an IAP.

### Example

The following example configures the PST timezone:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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
apply	Applies and saves the IAP configuration changes.
no-save	Applies the configuration changes to the cluster, but does not save the configuration. To save the configuration, run the <b>write memory</b> or <b>commit apply</b> command.
revert	Reverts the changes committed to the current configuration of an IAP.

### Usage Guidelines

Each command processed by the Virtual Controller is applied on all the slave 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, Aruba 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 Access Point) # commit apply
```

The following command reverts the already committed changes.

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 Access Point) (config) #
```

To return to EXEC mode, enter Ctrl-Z, end or exit.

## Example

The following command allows you to enter configuration commands:

```
(Instant Access Point) # configure terminal
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC 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 OpenDNS.

## Syntax

Command/Parameter	Description
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 open DNS server.

## Example

The following example enables content filtering:

```
(Instant Access Point)# content-filtering  
(Instant Access Point)# end  
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## convert-aos-ap

```
convert-aos-ap <mode> <controller-IP>
```

### Description

This command allows you to provision an IAP as a Campus AP or Remote AP in a controller-based network, or as a standalone AP.

### Syntax

Parameter	Description	Range
<mode>	Provisions the IAP as remote AP or campus AP in a controller-based network or as a standalone AP.	RAP, CAP, StandaloneAP
<controller-IP>	Allows you to specify the IP address of the Controller to which the Remote AP or Campus AP will be connected.	–

### Usage Guidelines

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

### Example

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

```
(Instant Access Point)# convert-aos-ap RAP 192.0.2.5
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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> {cpserver cert <password> format {p12|pem} | portal
logo | system {1xca [format {der|pem}]]|1xcert <password>[format {p12|pem}]}|config|flash}}
```

### Description

This command copies files to and from the IAP.

### Syntax

Parameter	Description
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 IAP database from a TFTP server.
<ip-address>	Copies files to the specified TFTP server IP address.
<file-name>	Indicates the name of the file to be copied.
cpserver cert <password>	Copies internal Captive portal server certificate.
portal logo	Copies customized logo for the internal Captive portal server.
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.
<password>	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 IAP database.

### Example

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

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

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command was modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP on different VLANs. Routing traffic between the clients will be sent to the upstream device to make the forwarding decision.

## Syntax

Parameter	Description
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 Access Point) (config) # deny-local-routing  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode



## device-id

device-id <device>

### Description

This command assigns an ID for the AP device.

### Syntax

Parameter	Description
device-id <device>	Configures an ID for the IAP device.

### Usage Guidelines

Use this command to configure a device identification.

### Example

The following example configures a device ID:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# disconnect-user

disconnect-user

## Description

This command disconnects the clients from an IAP.

## Example

The following example shows the output of **disconnect-user** command:

```
(Instant Access Point)# disconnect-user
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## download-cert

```
download-cert {ca|cp|server} <URL>
```

### Description

This command allows you to download the client, authentication server, and Captive portal server certificates from an FTP or TFTP server, or by using an HTTP URL.

### Syntax

Parameter	Description
ca	Downloads client certificates.
cp	Downloads Captive portal server certificates.
server	Downloads Server certificates.
<url>	Allows you to specify the FTP, TFTP, or HTTP URL.

### Usage Guidelines

Use this command to download certificates.

### Example

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

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

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	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 IAP.

## Syntax

Parameter	Description
auto	Configures the IAP to automatically enable or disable CPU management feature during run-time. When configured, the 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 <b>auto</b> option is the default and recommended setting.
disable	Disables CPU management on all APs, 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.

## Usage Guidelines

Use this command to enable or disable resource management across different functions performed by an IAP.

## Example

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

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

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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.

## Syntax

Command/Parameter	Description
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.

## Usage Guidelines

Ensure that you set the Virtual Controller IP address as a NAS client in the RADIUS server when Dynamic RADIUS proxy is enabled.

## Example

The following example enables the dynamic RADIUS proxy feature:

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## enet-vlan

```
enet-vlan <vlan-ID>  
no...
```

### Description

This command configures a VLAN for Ethernet connections.

### Syntax

Parameter	Description	Range
enet-vlan <vlan-ID>	Configures VLAN for Ethernet ports and wired profiles	0-4093
no...	Removes the configuration	–

### Usage Guidelines

Use this command to configure VLAN for the Ethernet connections.

### Example

The following example configures VLAN for the Ethernet ports:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# enet0-bridging

enet0-bridging

## Description

This command allows you to use all ports on the APs as downlink ports.

## Usage Guidelines

Use this command for IAP models that have only one Ethernet port enabled. When Eth0 bridging is configured, ensure that the uplink for each IAP is mesh link, Wi-Fi, or 3G/4G.

## Example

The following command enables Eth0 bridging:

```
(Instant Access Point)# enet0-bridging
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 Ethernet 0 port on an IAP.

## Syntax

Parameter	Description
enet0-port-profile <profile>	Assigns a wired profile to the Ethernet 0 interface port.

## Usage Guidelines

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

## Example

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

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode



# enet1-port-profile

enet1-port-profile <profile>

## Description

This command assigns a wired profile to the Ethernet 1 port on an IAP.

## Syntax

Parameter	Description
enet1-port-profile <profile>	Assigns a wired profile to the Ethernet 1 interface port.

## Usage Guidelines

Use this command to assign a wired profile to the Ethernet 1 port to activate the wired profile.

## Example

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

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## enet2-port-profile

enet2-port-profile <profile>

### Description

This command assigns a wired profile to the Ethernet 2 port on an IAP.

### Syntax

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

### Usage Guidelines

Use this command to assign a wired profile to the Ethernet 2 port to activate the wired profile.

### Example

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

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## enet3-port-profile

enet3-port-profile <profile>

### Description

This command assigns a wired profile to the Ethernet 3 port on an IAP.

### Syntax

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

### Usage Guidelines

Use this command to assign a wired profile to the Ethernet 3 port to activate the wired profile.

### Example

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

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# enet4-port-profile

enet4-port-profile <profile>

## Description

This command assigns a wired profile to the Ethernet 4 port on an IAP.

## Syntax

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

## Usage Guidelines

Use this command to assign a wired profile to the Ethernet 4 port to activate the wired profile.

## Example

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

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## extended-ssid

extended-ssid  
no...

### Description

This command enables the configuration of additional WLAN SSIDs.

### Syntax

Command/Parameter	Description
extended-ssid	Enables the users to configure additional SSIDs.
no...	Removes the configuration.

### Usage Guidelines

Use this command to create additional SSIDs. By default, you can create up to six WLAN SSIDs. With the Extended SSID option enabled, you can create up to 16 WLANs. The following IAPs support 16 WLANs:

- RAP-3WNP
- IAP-93
- IAP-134
- IAP-135

The number of SSIDs that become active on each IAP depends on the IAP platform.

### Example

The following example enables the configuration of extended SSIDs:

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

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# factory-ssid-enable

factory-ssid-enable

## Description

This command resets the IAP to use the factory configuration.

## Syntax

Parameter	Description
factory-ssid-enable	Enables factory SSID configuration.

## Usage Guidelines

Use this command to reset an IAP to use the factory default SSID.

## Example

The following example enables factory default configuration:

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## firewall-external-enforcement

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

### Description

This command configures external firewall details such as Palo Alto Networks (PAN) firewall to enable integration with the IAP.

### Syntax

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 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 IAP.	–	–
no...	Removes the specified configuration parameter.	–	–

### Usage Guidelines

Use this command to enable external firewall integration with an IAP. In Instant 6.3.1.1-4.0 release, IAPs can be integrated with external firewall such as PAN firewall. The PAN firewall is based on user ID, which provides many methods for connecting to sources of identity information and associating them with firewall policy rules. The functionality provided by the PAN firewall based on user ID requires the collection of information from the network. IAP maintains the network (such as mapping IP address) and user information for those clients in the network and provides the required information for the user ID feature on PAN firewall.

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

### Example

The following example configures PAN firewall information on an IAP:

```
(Instant Access Point) (config)# firewall-external-enforcement pan
(Instant Access Point) (firewall-external-enforcement pan)# enable
(Instant Access Point) (firewall-external-enforcement pan)# ip 192.0.2.11
(Instant Access Point) (firewall-external-enforcement pan)# port 443
```

```
(Instant Access Point) (firewall-external-enforcement pan)# user admin1 admin1
(Instant Access Point) (firewall-external-enforcement pan)# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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



## g-channel

g-channel <channel> <tx-power>

### Description

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

### Syntax

Parameter	Description	Range
<channel>	Configures the specified 2.4 GHz channel.	The valid channels for a band are determined by the AP regulatory domain.
<tx-power>	Configures the specified transmission power values.	0-127 dBm

### Usage Guidelines

Use this command to configure radio channels for the 2.4 GHz band for a specific IAP.

### Example

The following example configures the 2.4 GHz radio channel:

```
(Instant Access Point)# g-channel 11 18
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Syntax

Parameter	Description	Range	Default
<gain>	Configures the antenna gain. You can configure gain value in dBi for the following types of antenna: <ul style="list-style-type: none"><li>• Dipole/Omni</li><li>• Panel</li><li>• Sector</li></ul>	Dipole/Omni - 6 Panel -12 Sector - 12	–

## Usage Guidelines

If your IAP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's Equivalent Isotropically Radiated Power (EIRP) is in compliance with the limit specified by the regulatory authority of the country in which the 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 AP device supports external antenna connectors, see the *Install Guide* that is shipped along with the AP 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):

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$

The following table describes this formula:

**Table 10:** Formula Variable Definitions

Formula Element	Description
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 [www.arubanetworks.com](http://www.arubanetworks.com).

## Example

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

```
(Instant Access Point)# g-external-antenna 12
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

## gre per-ap-tunnel

```
gre per-ap-tunnel  
no...
```

### Description

This command configures a generic routing encapsulation (GRE) tunnel from each IAP to the VPN/GRE Endpoint rather than the tunnels created just from the Virtual Controller.

### Syntax

Parameter	Description
gre per-ap-tunnel	Creates a GRE tunnel from the IAP to the VPN/GRE endpoint.
no...	Removes the configuration.

### Usage Guidelines

Use this command to allow the traffic to be sent to the corporate network through a Layer-2 GRE tunnel from the IAP itself. When a GRE tunnel per IAP is created, the traffic need not be forwarded through the Virtual Controller.

### Example

The following example creates a GRE tunnel for the IAP:

```
(Instant Access Point) (config) # gre per-ap-tunnel  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## gre primary

```
gre primary <name>  
no...
```

### Description

This command configures a host for the primary VPN/GRE endpoint.

### Syntax

Parameter	Description
gre primary <name>	Specifies the fully qualified domain name (FQDN) of the primary host.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure the primary VPN/GRE host.

### Example

The following example configures a GRE primary host:

```
(Instant Access Point) (config)# gre primary <name>  
(Instant Access Point) (config)# end  
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## gre type

gre type <type>

### Description

This command configures a GRE protocol number as GRE type.

### Syntax

Parameter	Description	Range	Default
gre type <type>	Configures the protocol number or IP address for GRE type	16-bit protocol number	0

### Usage Guidelines

Use this command to specify GRE type. The 16-bit protocol number uniquely identifies a Layer-2 tunnel. The IAPs or controllers at both endpoints of the tunnel must be configured with the same protocol number.

### Example

The following example configures the GRE type:

```
(Instant Access Point) (config)# gre type 0
(Instant Access Point) (config)# end
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# help

help

## Description

This command displays help for the CLI.

## Usage Guidelines

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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# hostname

hostname <name>

## Description

This command changes the hostname of the Virtual Controller.

## Syntax

Parameter	Description
<name>	Configures a hostname for the Virtual Controller.

## Usage Guidelines

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.

## Example

The following example configures host name for an IAP.

```
(Instant Access Point)# hostname IAP1
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 3rd Generation Partnership Project (3GPP) Cellular Network for hotspots that have roaming relationships with cellular operators.

### Syntax

Parameter	Description
hotspot anqp-3gpp-profile <profile-name>	Creates a 3GPP profile.
3gpp-plmn1...3gpp-plmn6 <PLMN-ID>	Configures the Public Land Mobile Networks (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 Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
enable	Activates the configuration profile.
no...	Removes the configuration

### Usage Guidelines

Use this command to configure a 3GPP Cellular Network hotspot profile that defines the ANQP information element (IE) for 3G Cellular Network for hotspots. The IE defined in this profile will be sent in a Generic Advertisement Service (GAS) query response from an IAP in a cellular network hotspot. The 3GPP Mobile Country Code (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.

### Example

The following command configures a 3GPP profile:

```
(Instant Access Point)(config)# hotspot anqp-3gpp-profile cellcorp1
(Instant Access Point)(3gpp "cellcorp1")# 3gpp-plmn1 310026
(Instant Access Point)(3gpp "cellcorp1")# 3gpp_plmn2 208000
(Instant Access Point)(3gpp "cellcorp1")# 3gpp_plmn3 208001
(Instant Access Point)(3gpp "cellcorp1")# enable
(Instant Access Point)(3gpp "cellcorp1")# end
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

### Syntax

Parameter	Description
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

### Usage Guidelines

Use this command to configure a domain name in the ANQP Domain Name profile. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an IAP, the 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.

### Example

The following command defines a domain name for the ANQP domain name profile:

```
(Instant Access Point) (config)# hotspot anqp-domain-name-profile domain1
(Instant Access Point) (domain-name "domain1")# domain-name example.com
(Instant Access Point) (domain-name "domain1")# enable
(Instant Access Point) (domain-name "domain1")# end
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All 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  
  ipv6-addr-avail  
  no...
```

### Description

This command defines the available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

### Syntax

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	Indicates the availability of an IPv4 network.
ipv6-addr-avail	Indicates the availability of an IPv6 network.
no...	Removes the existing configuration.

### Usage Guidelines

Use this command to configure the IP Address availability information and IP address types which could be allocated to the clients after they associate to the hotspot IAP.

### Example

The following command configures an AP using this profile to advertise a public IPv4 network.

```
(Instant Access Point) (config) # hotspot anqp-ip-addr-avail-profile default  
(Instant Access Point) (IP-addr-avail "default") # ipv4-addr-avail  
(Instant Access Point) (IP-addr-avail "default") # ipv6-addr-avail  
(Instant Access Point) (IP-addr-avail "default") # enable  
(Instant Access Point) (IP-addr-avail "default") # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All 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 Network Access Identifier (NAI) realm information that can be sent as an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

### Syntax

Parameter	Description	Range
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 <b>nai-realm-auth-id-1</b> command to send the one of the following authentication methods for the primary NAI realm ID. Use the <b>nai-realm-auth-id-2</b> 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: <ul style="list-style-type: none"><li>● <b>credential</b>— Uses credential authentication.</li><li>● <b>eap-inner-auth</b>—Uses EAP inner authentication type.</li><li>● <b>exp-inner-eap</b>— Uses the expanded inner EAP authentication method.</li><li>● <b>expanded-eap</b>—Uses the expanded EAP authentication method.</li><li>● <b>non-eap-inner-auth</b>—Uses non-EAP inner authentication type.</li><li>● <b>reserved</b>—Uses the reserved authentication method.</li></ul>	credential eap-inner-auth exp-inner-auth expanded-eap non-eap-inner-auth reserved
nai-realm-auth-value-1 nai-realm-auth-value-2	Configures a value for NAI realm authentication. Use the <b>nai-realm-auth-value-1</b> command to select an authentication value for the authentication method specified by <b>nai-realm-auth-id-1</b> . Use the <b>nai-realm-auth-value-2</b> command to select the authentication value for the authentication method specified by <b>nai-realm-auth-id-2</b> .	–

Parameter	Description	Range
<auth-value>	<p>Configures any of following types of authentication values for the specified &lt;auth-id&gt;:</p> <ul style="list-style-type: none"> <li>For <b>credential</b> &lt;auth-ID&gt;, specify the following values: <ul style="list-style-type: none"> <li>sim</li> <li>usim</li> <li>nfc-secure</li> <li>hw-token</li> <li>softoken</li> <li>certificate</li> <li>uname-password</li> <li>none</li> <li>reserved</li> <li>vendor-specific</li> </ul> </li> <li>For <b>eap-inner-auth</b> &lt;aut-ID&gt;, specify the following values: <ul style="list-style-type: none"> <li>reserved</li> <li>pap</li> <li>chap</li> <li>mschap</li> <li>mschapv2</li> </ul> </li> <li>For <b>exp-inner-eap</b> &lt;auth-ID&gt;, specify <b>exp-inner-eap</b> as the authentication value.</li> <li>For <b>expanded-eap</b>&lt;auth-ID&gt;, specify <b>expanded-eap</b> as the authentication value</li> <li>For <b>non-eap-inner-auth</b>&lt;auth-ID&gt; specify any of the following values: <ul style="list-style-type: none"> <li>reserved</li> <li>pap</li> <li>chap</li> <li>mschap</li> <li>mschapv2</li> </ul> </li> </ul>	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
nai-realm-eap-method	Configures an EAP method for NAI realm.	
<eap-method>	<p>Configures any of the following EAP methods:</p> <ul style="list-style-type: none"> <li><b>crypto-card</b>— Crypto card authentication</li> <li><b>eap-aka</b>—EAP for UMTS Authentication and Key Agreement</li> <li><b>eap-sim</b>—EAP for GSM Subscriber Identity Modules</li> <li><b>eap-tls</b>—EAP-Transport Layer Security</li> <li><b>eap-ttls</b>—EAP-Tunneled Transport Layer Security</li> <li><b>generic-token-card</b>—EAP Generic Token Card (EAP-GTC)</li> <li><b>identity</b>— EAP Identity type</li> <li><b>notification</b>—The hotspot realm uses EAP Notification messages for authentication.</li> <li><b>one-time-password</b>—Authentication with a single-use password</li> <li><b>peap</b>—Protected Extensible Authentication Protocol</li> <li><b>peapmschapv2</b>— Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2</li> </ul>	crypto-card, eap-aka, eap-sim, eap-tls, eap-ttls, generic-token-card, identity notification, one-time-password, peap, peapmschapv2
nai-realm-encoding <encoding>	Configures a UTF-8 or rfc4282 formatted character string for NAI realm encoding.	rfc4282, utf8

Parameter	Description	Range
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.	–

## Usage Guidelines

Use this command to configure an NAI Realm profile that identifies and describes a NAI realm accessible to the IAP, and the method used for NAI realm authentication. The settings configured in this profile determine the NAI realm elements that are included as part of a GAS Response frame.

## Example

The following example creates an NAI realm profile:

```
(Instant Access Point) (config) # hotspot anqp-nai-realm-profile home
(Instant Access Point) (nai-realm "home") # nai-realm-name home-hotspot.com
(Instant Access Point) (nai-realm "home") # nai-realm-encoding utf8
(Instant Access Point) (nai-realm "home") # nai-realm-eap-method eap-sim
(Instant Access Point) (nai-realm "home") # nai-realm-auth-id-1 non-eap-inner-auth
(Instant Access Point) (nai-realm "home") # nai-realm-auth-value-1 mschapv2
(Instant Access Point) (nai-realm "home") # nai-home-realm
(Instant Access Point) (nai-realm "home") # enable
(Instant Access Point) (nai-realm "home") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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.

### Syntax

Parameter	Description	Range
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: <ul style="list-style-type: none"><li>● <b>accept-term-and-cond</b>—When configured, the network requires the user to accept terms and conditions. <b>NOTE:</b> This option requires you to specify a redirection URL string as an IP address, FQDN or URL.</li><li>● <b>online-enrollment</b>—When configured, the network supports the online enrollment.</li><li>● <b>http-redirect</b>—When configured, additional information on the network is provided through HTTP/HTTPS redirection.</li><li>● <b>dns-redirect</b>—When configured, additional information on the network is provided through DNS redirection. <b>NOTE:</b> This option requires you to specify a redirection URL string as an IP address, FQDN or URL.</li></ul>	accept-term-and-cond, online-enrollment, http-redirect, dns-redirect
url	Configures URL, IP address, or FQDN used by the hotspot network for the <b>accept-term-and-cond</b> or <b>dns-redirect</b> network authentication types.	—
no...	Removes any existing configuration.	—

### Usage Guidelines

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.

### Example

The following command configures a network authentication profile for DNS redirection.

```
(Instant Access Point) (config)# hotspot anqp-nwk-auth-profile default
```

```
(Instant Access Point) (network-auth "default") # nwk-auth-type dns-redirectio
n
(Instant Access Point) (network-auth "default") # url http://www.example.com
(Instant Access Point) (network-auth "default") # enable
(Instant Access Point) (network-auth "default") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Organization Identifier (OI) information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

### Syntax

Parameter	Description	Range
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 <b>roam-cons-oi-len</b> parameter must equal upon the number of octets of the <b>roam-cons-oi</b> field. <ul style="list-style-type: none"><li>● <b>0</b>: 0 Octets in the OI (Null)</li><li>● <b>3</b>: OI length is 24-bit (3 Octets)</li><li>● <b>5</b>: OI length is 36-bit (5 Octets)</li></ul>	—
no...	Removes any existing configuration.	—

### Usage Guidelines

Use this command to configure the roaming consortium OIs assigned to service providers when they register with the IEEE registration authority. The Roaming Consortium Information Elements (IEs) contain information about the network and service provider, whose security credentials can be used to authenticate with the IAP transmitting this IE.

### Example

The following command defines the roaming consortium OI and OI length in the ANQP roaming consortium profile:

```
(Instant Access Point) (config) # hotspot anqp-roam-cons-profile profile1
(Instant Access Point) (roaming-consortium "profile1") # roam-cons-oi 506F9A
(Instant Access Point) (roaming-consortium "profile1") # roam-cons-oi-len 3
(Instant Access Point) (roaming-consortium "profile1") # enable
(Instant Access Point) (roaming-consortium "profile1") # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

### Syntax

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 APs associated with this hotspot profile. <ul style="list-style-type: none"><li>● assembly</li><li>● business</li><li>● educational</li><li>● factory-and-industrial</li><li>● institutional</li><li>● mercantile</li><li>● outdoor</li><li>● residential</li><li>● storage</li><li>● utility-and-misc</li><li>● vehicular</li></ul> <b>NOTE:</b> This parameter only defines the venue group advertised in the IEs from hotspot APs. To define the venue group to be included in ANQP responses, use <b>anqp-venue-name-profile &lt;profile-name&gt;</b> command.	assembly, business, educational, factory-and-industrial, institutional, mercantile, outdoor, residential, storage, unspecified, utility-and-misc, vehicular	unspecified
venue-lang-code <language>	Configures an ISO 639 language code that identifies the language used in the Venue Name field.	–	–

Parameter	Description	Range	Default
<code>venue-name &lt;name&gt;</code>	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".	–	–
<code>venue-type &lt;type&gt;</code>	Specifies the venue type to be advertised in the IEs.	The complete list of supported venue types is described in <a href="#">hotspot anqp-venue-name-profile on page 101</a> .	unspecified
<code>no...</code>	Removes any existing configuration.	–	–

## Usage Guidelines

Use this command to configure the venue group and venue type in an ANQP Venue Name profile. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an Access Point, the IAP will return ANQP Information Elements with the values configured in this profile.

## Venue Types

The following list describes the different venue types for each venue group:

Venue Group	Associated Venue Type Value
<code>assembly</code>	<ul style="list-style-type: none"> <li>● arena</li> <li>● stadium</li> <li>● passenger-terminal</li> <li>● amphitheater</li> <li>● amusement-park</li> <li>● place-of-worship</li> <li>● convention-center</li> <li>● library</li> <li>● museum</li> <li>● restaurant</li> <li>● theater</li> <li>● bar</li> <li>● coffee-shop</li> <li>● zoo-or-aquarium</li> <li>● emergency-cord-center</li> <li>● unspecified</li> </ul>
<code>business</code>	<ul style="list-style-type: none"> <li>● doctor</li> <li>● bank</li> <li>● fire-station</li> <li>● police-station</li> <li>● post-office</li> <li>● professional-office</li> <li>● research-and-dev-facility</li> <li>● attorney-office</li> <li>● unspecified</li> </ul>

Venue Group	Associated Venue Type Value
educational	<ul style="list-style-type: none"> <li>● school-primary</li> <li>● school-secondary</li> <li>● univ-or-college</li> <li>● unspecified</li> </ul>
factory-and-industrial	<ul style="list-style-type: none"> <li>● factory</li> <li>● unspecified</li> </ul>
institutional	<ul style="list-style-type: none"> <li>● hospital</li> <li>● long-term-care</li> <li>● alc-drug-rehab</li> <li>● group-home</li> <li>● prison-or-jail</li> <li>● unspecified</li> </ul>
mercantile	<ul style="list-style-type: none"> <li>● retail-store</li> <li>● grocery-market</li> <li>● auto-service-station</li> <li>● shopping-mall</li> <li>● gas-station</li> <li>● unspecified</li> </ul>
outdoor	<ul style="list-style-type: none"> <li>● muni-mesh-network</li> <li>● city-park</li> <li>● rest-area</li> <li>● traffic-control</li> <li>● bus-stop</li> <li>● kisok</li> <li>● unspecified</li> </ul>
residential	<ul style="list-style-type: none"> <li>● private-residence</li> <li>● hotel</li> <li>● dormitory</li> <li>● boarding-house</li> <li>● unspecified</li> </ul>
storage	unspecified
utility-and-misc	unspecified
vehicular	<ul style="list-style-type: none"> <li>● unspecified</li> <li>● automobile-or-truck</li> <li>● airplane</li> <li>● bus</li> <li>● ferry</li> <li>● ship</li> <li>● train</li> <li>● motor-bike</li> </ul>

## Example

The following command defines an ANQP Venue Name profile for a shopping mall:

```
(Instant Access Point) (config) # hotspot anqp-venue-name-profile Mall1
(Instant Access Point) (venue-name "Mall1") # venue-name ShoppingCenter1
(Instant Access Point) (venue-name "Mall1") # venue-group mercantile
(Instant Access Point) (venue-name "Mall1") # venue-type shopping-mall
(Instant Access Point) (venue-name "Mall1") # venue-lang-code EN
(Instant Access Point) (venue-name "Mall1") # enable
```

```
(Instant Access Point) (venue-name "Mall1")# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Hotspot 2.0 Query Protocol (H2QP) profile that advertises hotspot protocol and port capabilities.

### Syntax

Parameter	Description
hotspot h2qp-conn-cap-profile<profile-name>	Creates a connection capability profile.
enable	Enables the connection capability H2QP profile.
esp-port	Enables the Encapsulating Security Payload (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)
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.

## Usage Guidelines

Use this command to configure the values to be sent in an ANQP IE to provide information about the IP protocols and associated port numbers that are available and open for communication.

## Example

The following example allows the H2QP connection capability profile to advertise the availability of ICMP and HTTP ports.

```
(Instant Access Point)(config) # hotspot h2qp-conn-cap-profile Wan1
(Instant Access Point)(connection-capabilities "Wan1")# icmp
(Instant Access Point)(connection-capabilities "Wan1")# tcp-http
(Instant Access Point)(connection-capabilities "Wan1")# enable
(Instant Access Point)(connection-capabilities "Wan1")# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Hotspot 2.0 Query Protocol (H2QP) operator-friendly name profile.

## Syntax

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 <b>op-fr-name</b> command.	–	–
no...	Removes any existing configuration.	–	–

## Usage Guidelines

Use this command to configure an operator-friendly name that can identify the operator and also provides information about the location.

## Example

The following example configures an operator friendly profile:

```
(Instant Access Point) (config) # hotspot h2qp-oper-name-profile Profile1
(Instant Access Point) (operator-friendly-name "Profile1") # op-fr-name hotspot1
(Instant Access Point) (operator-friendly-name "Profile1") # op-lang-code EN
(Instant Access Point) (operator-friendly-name "Profile1") # enable
(Instant Access Point) (operator-friendly-name "Profile1") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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 Hotspot 2.0 Query Protocol (H2QP) profile that defines the Operating Class to be sent in the H2QP IE.

### Syntax

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.	–	–

### Usage Guidelines

Use this command to configure values for the H2QP Operating Class profile that lists the channels on which the hotspot is capable of operating.

### Example

The following example configures and enables a profile with the default operating class value.

```
(Instant Access Point)(config) # hotspot h2qp-oper-class-profile Profile1
(Instant Access Point)(operator-class"Profile1")# op-class 1
(Instant Access Point)(operator-class"Profile1")# enable
(Instant Access Point)(operator-class"Profile1")# end
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and the H2QP operating class 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
  uplink-load <load>
  uplink-speed <speed>
  wan-metrics-link-status <status>
  no...
```

### Description

This command configures a Hotspot 2.0 Query Protocol (H2QP) profile that specifies the hotspot WAN status and link metrics.

### Syntax

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 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)
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 <b>uplink &lt;speed&gt;</b> 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: <ul style="list-style-type: none"> <li>• <b>link-up</b>– Indicates if WAN link is up.</li> <li>• <b>link-down</b>– Indicates if WAN link is down</li> <li>• <b>link-under-test</b>–Indicates if WAN link is currently in a test state.</li> </ul>	link-down, link-under-test, link-up	unspecified

## Usage Guidelines

Use this command to configure the values be sent in an H2QP IE to provide information about access network characteristics such as link status and the capacity and speed of the WAN link to the Internet.

## Examples

The following example configures a WAN metric profile:

```
(Instant Access Point) (config) # hotspot h2qp-wan-metrics-profile Wan1
(Instant Access Point) (WAN-metrics "Wan1") # at-capacity
(Instant Access Point) (WAN-metrics "Wan1") # downlink-load 5
(Instant Access Point) (WAN-metrics "Wan1") # downlink-speed 147
(Instant Access Point) (WAN-metrics "Wan1") # load-duration 60
(Instant Access Point) (WAN-metrics "Wan1") # symm-link
(Instant Access Point) (WAN-metrics "Wan1") # uplink-load 10
(Instant Access Point) (WAN-metrics "Wan1") # uplink-speed 147
(Instant Access Point) (WAN-metrics "Wan1") # wan-metrics-link-status link_up
(Instant Access Point) (WAN-metrics "Wan1") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All 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|anqp-domain-name|anqp-ip-addr-avail|anqp-nai-realm| anqp-n
wk-auth|anqp-roam-cons|anqp-venue-name|h2qp-conn-cap|h2qp-oper-class|h2qp-oper-name|h2qp-wa
n-metrics} <profile-name>
  advertisement-protocol <protocol>
  asra
  comeback-mode
  enable
  gas-comeback-delay <delay>
  group-frame-block
  hessid <id>
  internet
  no
  p2p-cross-connect
  p2p-dev-mgmt
  pame-bi
  query-response-length-limit <len>
  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>
```

### Description

This command configures a hotspot profile for an 802.11u public access service provider.

### Syntax

Parameter	Description	Range	Default
<code>access-network-type &lt;type&gt;</code>	<p>Configures any of the following access network (802.11u network type) type:</p> <ul style="list-style-type: none"><li>● <b>private</b> – 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.</li><li>● <b>private-with-guest</b> – 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.</li><li>● <b>chargeable-public</b> – This network provides access to the</li></ul>	private, private-with-guest, chargeable-public, free-public, personal-device, emergency-services, test, wildcard	chargeable-public



Parameter	Description	Range	Default
	<p>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.</p> <ul style="list-style-type: none"> <li>● <b>free-public</b> –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.</li> <li>● <b>personal-device</b> – 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.</li> <li>● <b>emergency-services</b> –This network is limited to accessing emergency services only. The corresponding integer value for this network type is 5.</li> <li>● <b>test</b> – This network is used for test purposes only. The corresponding integer value for this network type is 14.</li> <li>● <b>wildcard</b> –This network indicates a wildcard network. The corresponding integer value for this network type is 15.</li> </ul>		
<pre>addtl-roam-cons-ois &lt;addtl-roam-cons-ois&gt;</pre>	<p>Configures the number of additional roaming consortium Organization Identifiers (OIs) advertised by the AP. 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.</p>	–	–
<pre>advertisement-profile {anqp-3gpp  anqp-domain-name  anqp-ip-addr-avail  anqp-nai-realm  anqp-nwk-auth  anqp-roam-cons  anqp-venue-name  h2qp-conn-cap  h2qp-oper-class  h2qp-oper-name </pre>	<p>Associates an advertisement profile with the hotspot profile. You can associate any of the following advertisement profiles:</p> <ul style="list-style-type: none"> <li>● anqp-3gpp</li> <li>● anqp-domain-name</li> <li>● anqp-ip-addr-avail</li> <li>● anqp-nai-realm</li> <li>● anqp-nwk-auth</li> <li>● anqp-roam-cons</li> <li>● anqp-venue-name</li> </ul>	–	–

Parameter	Description	Range	Default
h2qp-wan-metrics}	<ul style="list-style-type: none"> <li>h2qp-conn-cap</li> <li>h2qp-oper-class</li> <li>h2qp-oper-name</li> <li>h2qp-wan-metrics</li> </ul>		
<profile-name>	Allows you to associate a specific advertisement profile to the hotspot profile.	–	–
advertisement-protocol <protocol>	Configures the <b>anqp</b> : Access Network Query Protocol (ANQP) advertisement protocol.	anqp	–
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.	–	–
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	500
group-frame-block	Configures the Downstream Group Addressed Forwarding (DGAF) Disabled Mode. This feature ensures that the IAP does not forward downstream group-addressed frames. It is disabled by default, allowing the IAP to forward downstream group-addressed frames.	–	–
hessid	Configures a homogenous ESS identifier (HESSID)	MAC address in colon-separated hexadecimal format	–
internet	Allows the IAP to send an Information Element (IE) indicating that the network allows the Internet access. By default, a hotspot profile does not advertise network internet access.	–	–

Parameter	Description	Range	Default
no	Removes any existing configuration.	–	–
p2p-cross-connect	Advertises support for P2P Cross Connections.	–	Disabled
p2p-dev-mgmt	Advertises support for P2P device management.	–	Disabled
pame-bi	Enables the Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, which is used by an AP to indicate whether the AP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.	–	–
query-response-length-limit <len>	Configures the maximum length of the Generic Advertisement Service (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 IAP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame.	1-127	127
roam-cons-len-1	Configures the length of the OI. The value of the <b>roam-cons-len-1</b> parameter is based upon the number of octets of the <b>roam-cons-oi-1</b> field.	<b>0:</b> Zero Octets in the OI (Null), <b>3:</b> OI length is 24-bit (3 Octets), <b>5:</b> OI length is 36-bit (5 Octets)	–
roam-cons-len-2	Length of the OI. The value of the <b>roam-cons-len-2</b> parameter is based upon the number of octets of the <b>roam-cons-oi-2</b> field.	<b>0:</b> Zero Octets in the OI (Null), <b>3:</b> OI length is 24-bit (3 Octets), <b>5:</b> OI length is 36-bit (5 Octets)	–
roam-cons-len-3	Length of the OI. The value of the <b>roam-cons-len-3</b> parameter is based upon the number of octets of the <b>roam-cons-oi-3</b> field.	<b>0:</b> Zero Octets in the OI (Null), <b>3:</b> OI length is 24-bit (3 Octets), <b>5:</b> OI length is 36-bit (5 Octets)	–

Parameter	Description	Range	Default
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 <b>addtl-roam-cons-&lt;oisaddtl-roam-cons-ois&gt;</b> parameter is set to 1 or higher. <b>NOTE:</b> The service provider's own roaming consortium OI is configured using the <b>hotspot anqp-roam-cons-profile</b> command.	—	—
venue-group <venue-group>	Configures one of the following venue groups to be advertised in the IEs from APs associated with this hotspot profile. <ul style="list-style-type: none"> <li>• assembly</li> <li>• business</li> <li>• educational</li> <li>• factory-and-industrial</li> <li>• institutional</li> <li>• mercantile</li> <li>• outdoor</li> <li>• residential</li> <li>• storage</li> <li>• unspecified</li> <li>• utility-and-misc</li> <li>• vehicular</li> </ul> <b>NOTE:</b> This parameter only defines the venue group advertised in the IEs from hotspot APs. To define the venue group to be included in ANQP responses, use <b>anqp-venue-name-profile &lt;profile-name&gt;</b> 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 APs associated with this hotspot profile. The complete list of supported venue types is described in <a href="#">Venue Types on page 118</a> <b>NOTE:</b> This parameter only defines the venue type advertised in the IEs from hotspot APs. To define the venue type to be included in ANQP responses, use the <b>hotspot anqp-venue-name-profile &lt;profile-name&gt;</b> command.	—	—

## Usage Guidelines

Use this command to configure a hotspot profile. 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, Generic Advertisement Service (GAS) and Access Network Query Protocol (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 Generic Advertisement Service (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.

### Generic Advertisement Service (GAS) Queries

An Organization Identifier (OI) is a unique identifier assigned to a service provider when it registers with the IEEE registration authority. An 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 IAP using the security credentials corresponding to that service provider.

If the client does *not* recognize the OI, that client can send a Generic Advertisement Service (GAS) query to the AP to request more information more about the network before associating.

### ANQP Information Elements

ANQP Information Elements (IEs) are additional data that can be sent from the AP to the client to identify the AP's network and service provider. If a client requests this information via a GAS query, the hotspot AP 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

Organization Identifiers (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 `adtl-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
<b>unspecified</b> The associated numeric value is <b>0</b> .	–
<b>assembly</b> The associated numeric value is <b>1</b> .	<ul style="list-style-type: none"> <li>• unspecified–The associated numeric value is <b>0</b>.</li> <li>• arena–The associated numeric value is <b>1</b>.</li> <li>• stadium–The associated numeric value is <b>2</b>.</li> <li>• passenger-terminal–The associated numeric value is <b>3</b>.</li> <li>• amphitheater–The associated numeric value is <b>4</b>.</li> <li>• amusement-park–The associated numeric value is <b>5</b>.</li> <li>• place-of-worship–The associated numeric value is <b>6</b>.</li> <li>• convention-center–The associated numeric value is <b>7</b>.</li> <li>• library–The associated numeric value is <b>8</b>.</li> <li>• museum–The associated numeric value is <b>9</b>.</li> <li>• restaurant–The associated numeric value is <b>10</b>.</li> <li>• theater–The associated numeric value is <b>11</b>.</li> <li>• bar –The associated numeric value is <b>12</b>.</li> <li>• coffee-shop –The associated numeric value is <b>13</b>.</li> <li>• zoo-or-aquarium –The associated numeric value is <b>14</b>.</li> <li>• emergency-cord-center–The associated numeric value is <b>15</b>.</li> </ul>
<b>business</b> The associated numeric value is <b>2</b> .	<ul style="list-style-type: none"> <li>• unspecified–The associated numeric value is <b>0</b>.</li> <li>• doctor–The associated numeric value is <b>1</b></li> <li>• bank–The associated numeric value is <b>2</b></li> <li>• fire-station–The associated numeric value is <b>3</b></li> <li>• police-station–The associated numeric value is <b>4</b></li> <li>• post-office–The associated numeric value is <b>6</b></li> <li>• professional-office–The associated numeric value is <b>7</b></li> <li>• research-and-dev-facility–The associated numeric value is <b>8</b></li> <li>• attorney-office–The associated numeric value is <b>9</b></li> </ul>
<b>educational</b> The associated numeric value is <b>3</b> .	<ul style="list-style-type: none"> <li>• unspecified–The associated numeric value is <b>0</b>.</li> <li>• school-primary–The associated numeric value is <b>1</b>.</li> <li>• school-secondary–The associated numeric value is <b>2</b>.</li> <li>• univ-or-college–The associated numeric value is <b>3</b>.</li> </ul>
<b>factory-and-industrial</b> The associated numeric value is <b>4</b> .	<ul style="list-style-type: none"> <li>• unspecified–The associated numeric value is <b>0</b>.</li> <li>• factory–The associated numeric value is <b>1</b>.</li> </ul>
<b>institutional</b> The associated numeric value is <b>5</b> .	<ul style="list-style-type: none"> <li>• unspecified–The associated numeric value is <b>0</b>.</li> <li>• hospital–The associated numeric value is <b>1</b>.</li> <li>• long-term-care–The associated numeric value is <b>2</b>.</li> <li>• alc-drug-rehab–The associated numeric value is <b>3</b>.</li> <li>• group-home–The associated numeric value is <b>4</b>.</li> </ul>

Venue Group	Associated Venue Type Value
	<ul style="list-style-type: none"> <li>prison-or-jail—The associated numeric value is <b>5</b>.</li> </ul>
<b>mercantile</b> The associated numeric value is <b>6</b> .	<ul style="list-style-type: none"> <li>unspecified—The associated numeric value is <b>0</b>.</li> <li>retail-store—The associated numeric value is <b>1</b>.</li> <li>grocery-market—The associated numeric value is <b>2</b>.</li> <li>auto-service-station—The associated numeric value is <b>3</b>.</li> <li>shopping-mall—The associated numeric value is <b>4</b>.</li> <li>gas-station—The associated numeric value is <b>5</b>.</li> </ul>
<b>residential</b> The associated numeric value is <b>7</b> .	<ul style="list-style-type: none"> <li>unspecified—The associated numeric value is <b>0</b>.</li> <li>private-residence—The associated numeric value is <b>1</b>.</li> <li>hotel—The associated numeric value is <b>3</b>.</li> <li>dormitory—The associated numeric value is <b>4</b>.</li> <li>boarding-house—The associated numeric value is <b>5</b>.</li> </ul>
<b>storage</b> The associated numeric value is <b>8</b> .	unspecified—The associated numeric value is <b>0</b> .
<b>utility-misc</b> The associated numeric value is <b>9</b> .	unspecified—The associated numeric value is <b>0</b> .
<b>vehicular</b> The associated numeric value is <b>10</b> .	<ul style="list-style-type: none"> <li>unspecified—The associated numeric value is <b>0</b>.</li> <li>automobile-or-truck—The associated numeric value is <b>1</b>.</li> <li>airplane—The associated numeric value is <b>2</b>.</li> <li>bus—The associated numeric value is <b>3</b>.</li> <li>ferry—The associated numeric value is <b>4</b>.</li> <li>ship —The associated numeric value is <b>5</b>.</li> <li>train —The associated numeric value is <b>6</b>.</li> <li>motor-bike—The associated numeric value is <b>7</b>.</li> </ul>
<b>outdoor</b> The associated numeric value is <b>11</b> .	<ul style="list-style-type: none"> <li>unspecified—The associated numeric value is <b>0</b>.</li> <li>muni-mesh-network—The associated numeric value is <b>1</b>.</li> <li>city-park—The associated numeric value is <b>2</b>.</li> <li>rest-area—The associated numeric value is <b>3</b>.</li> <li>traffic-control—The associated numeric value is <b>4</b>.</li> <li>bus-stop—The associated numeric value is <b>5</b>.</li> <li>kiosk —The associated numeric value is <b>6</b>.</li> </ul>

## Example

The following commands configure a hotspot profile:

```
(Instant Access Point) (config) # hotspot hs-profile hs1
(Instant Access Point) (Hotspot2.0 "hs1") # enable
(Instant Access Point) (Hotspot2.0 "hs1") # comeback-mode
(Instant Access Point) (Hotspot2.0 "hs1") # gas-comeback-delay 10
(Instant Access Point) (Hotspot2.0 "hs1") # no asra
(Instant Access Point) (Hotspot2.0 "hs1") # no internet
(Instant Access Point) (Hotspot2.0 "hs1") # query-response-length-limit 127
(Instant Access Point) (Hotspot2.0 "hs1") # access-network-type chargeable-public
(Instant Access Point) (Hotspot2.0 "hs1") # roam-cons-len-1 3
(Instant Access Point) (Hotspot2.0 "hs1") # roam-cons-oi-1 123456
(Instant Access Point) (Hotspot2.0 "hs1") # roam-cons-len-2 3
(Instant Access Point) (Hotspot2.0 "hs1") # roam-cons-oi-2 223355
(Instant Access Point) (Hotspot2.0 "hs1") # addtl-roam-cons-ois 0
(Instant Access Point) (Hotspot2.0 "hs1") # venue-group business
(Instant Access Point) (Hotspot2.0 "hs1") # venue-type research-and-dev-facility
(Instant Access Point) (Hotspot2.0 "hs1") # pame-bi
(Instant Access Point) (Hotspot2.0 "hs1") # group-frame-block
```

```
(Instant Access Point) (Hotspot2.0 "hs1") # p2p-dev-mgmt
(Instant Access Point) (Hotspot2.0 "hs1") # p2p-cross-connect
(Instant Access Point) (Hotspot2.0 "hs1") # end
(Instant Access Point) # commit apply
```

The following commands associate **anqp-3gpp** advertisement profile with a hotspot profile:

```
(Instant Access Point) (config) # hotspot hs-profile hs1
(Instant Access Point) (Hotspot2.0"hs1") # advertisement-protocol anqp
(Instant Access Point) (Hotspot2.0"hs1") # advertisement-profile anqp-3gpp 3gpp1
(Instant Access Point) (Hotspot2.0"hs1") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and the hotspot profile configuration sub-mode



# iap-master

iap-master  
no...

## Description

This command provisions an IAP as a master IAP.

## Syntax

Command/Parameter	Description
iap-master	Provisions the IAP as a master IAP.
no...	Removes the configuration.

## Usage Guidelines

Use this command to manually provision an IAP as a master IAP.

## Example

The following example provisions a master IAP:

```
(Instant Access Point)# iap-master
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## ids

ids

```
client-detection-level <type>
client-protection-level <type>
detect-adhoc-network
detect-ap-flood
detect-ap-impersonation
detect-ap-spoofing
detect-bad-wep
detect-beacon-wrong-channel
detect-block-ack-attack
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
infrastructure-detection-level <type>
infrastructure-protection-level <type>
protect-adhoc-network
protect-ap-impersonation
protect-ssid
protect-valid-sta
protect-windows-bridge
rogue-containment
signature-airjack
signature-asleep
signature-deassociation-broadcast
signature-deauth-broadcast
wired-containment
wireless-containment <type>
no...
```

### Description

This command configures an IDS policy for an IAP.

## Syntax

Parameter	Description	Range	Default
<code>ids</code>	Creates an IDS policy	–	–
<code>client-detection-level &lt;type&gt;</code>	Sets the client detection level.	off, low, medium, high	off
<code>client-protection-level &lt;type&gt;</code>	Sets the client protection level.	off, low, medium, high	off
<code>detect-adhoc-network</code>	Enables detection of adhoc networks.	–	–
<code>detect-ap-flood</code>	Enables detection of flooding with fake IAP beacons to confuse the legitimate users and to increase the amount of processing needed on client operating systems.	–	–
<code>detect-ap-impersonation</code>	Enables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack.	–	–
<code>detect-ap-spoofing</code>	Enables AP Spoofing detection.	–	–
<code>detect-bad-wep</code>	Enables detection of WEP initialization vectors that are known to be weak and/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.	–	–
<code>detect-beacon-wrong-channel</code>	Enables detection of beacons advertising the incorrect channel.	–	–
<code>detect-block-ack-attack</code>	Enables detection of attempts to reset traffic receive windows using the forged Block ACK Add messages.	–	–
<code>detect-chopchop-attack</code>	Enables detection of ChopChop attack.	–	–
<code>detect-client-flood</code>	Enables detection of client flood attack.	–	–
<code>detect-cts-rate-anomaly</code>	Enables detection of CTS rate	–	–

Parameter	Description	Range	Default
	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 AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association.	–	–
detect-eap-rate-anomaly	Enables Extensible Authentication Protocol (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 APs advertising 40 MHz intolerance will be reported.	–	–
detect-ht-greenfield	Enables detection of high throughput 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 organizationally unique identifier (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
<code>detect-malformed-large-duration</code>	Enables detection of unusually large durations in frames.	–	–
<code>detect-omerta-attack</code>	Enables detection of Omerta attack.	–	–
<code>detect-overflow-eapol-key</code>	Enables detection of overflow EAPOL key requests.	–	–
<code>detect-overflow-ie</code>	Enables detection of overflow Information Elements (IE).	–	–
<code>detect-power-save-dos-attack</code>	Enables detection of Power Save DoS attack.	–	–
<code>detect-rate-anomalies</code>	Enables detection of rate anomalies.	–	–
<code>detect-rts-rate-anomaly</code>	Enables detection of RTS rate anomaly.	–	–
<code>detect-tkip-replay-attack</code>	Enables detection of TKIP replay attack.	–	–
<code>detect-unencrypted-valid</code>	Enables detection of unencrypted valid clients.	–	–
<code>detect-valid-clientmisassociation</code>	Enables detection of misassociation between a valid client and an unsafe AP. This setting can detect the following misassociation types: <ul style="list-style-type: none"> <li>• MisassociationToRogueAP</li> <li>• MisassociationToExternalAPI</li> <li>• MisassociationToHoneypotAP</li> <li>• MisassociationToAdhocAP</li> <li>• MisassociationToHostedAP</li> </ul>	–	–
<code>detect-valid-ssid-misuse</code>	Enables detection of interfering or Neighbor APs using valid or protected SSIDs.	–	–
<code>detect-windows-bridge</code>	Enables detection of Windows station bridging.	–	–
<code>detect-wireless-bridge</code>	Enables detection of wireless bridging.	–	–
<code>infrastructure-detection-level &lt;type&gt;</code>	Sets the infrastructure detection level.	off, low, medium, high	off
<code>infrastructure-protection-level &lt;type&gt;</code>	Sets the infrastructure protection level.	off, low, medium, high	off
<code>protect-adhoc-network</code>	Enables protection from adhoc networks. When adhoc networks are detected, they are disabled using a	–	–

Parameter	Description	Range	Default
	denial of service attack		
protect-ap-impersonation	Enables protection from AP impersonation attacks. When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack.	–	–
protect-ssid	Enables use of SSID by valid IAPs only.	–	–
protect-valid-sta	Enables protection of valid stations. When enabled valid stations are not allowed to connect to an invalid AP.	–	–
protect-windows-bridge	Enables protection of a windows station bridging	–	–
rogue-containment	Controls Rogue APs. When rogue APs are detected, they are not automatically disabled.  This option automatically shuts down rogue APs. When this option is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.	–	–
signature-airjack	Enables signature matching for the AirJack frame type.	–	–
signature-asleep	Enables signature matching for the ASLEAP frame type.	–	–
signature-deassociation-broadcast	Configures signature matching for the deassociation broadcast frame type.	–	–
signature-death-broadcast	Configures signature matching for the death broadcast frame type.	–	–
wired-containment	Controls Wired attacks.	–	–
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 AP that is being contained.  <ul style="list-style-type: none"> <li>• death-only– Enables Containment using deauthentication only .</li> <li>• none– Disables wireless</li> </ul>	death-only, none, tarpit-all-sta, tarpit-non-valid-sta	death-only

Parameter	Description	Range	Default
	containment. <ul style="list-style-type: none"> <li>• <code>tarpit-all-sta</code>—Enables wireless containment by tarpit of all stations.</li> <li>• <code>tarpit-non-valid-sta</code>— Enables wireless containment by tarpit of non-valid clients</li> </ul>		
<code>no...</code>	Removes any existing configuration.	—	—

## Usage Guidelines

Use this command to configure Intrusion Detection System (IDS) detection and protection policies. The IDS feature monitors the network for the presence of unauthorized IAPs and clients and enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. It also logs information about the unauthorized IAPs and clients, and generates reports based on the logged information.

Wireless Intrusion Protection (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 Aruba network, the WIP can be configured on the 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 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

## Example

The following example configures detection and protection policies:

```
(Instant Access Point) (config) # ids
(Instant Access Point) (IDS) # infrastructure-detection-level low
(Instant Access Point) (IDS) # client-detection-level low
(Instant Access Point) (IDS) # infrastructure-protection-level low
(Instant Access Point) (IDS) # client-protection-level low
(Instant Access Point) (IDS) # wireless-containment deauth-only
(Instant Access Point) (IDS) # wired-containment
(Instant Access Point) (IDS) # detect-ap-spoofing
(Instant Access Point) (IDS) # detect-windows-bridge
(Instant Access Point) (IDS) # signature-deauth-broadcast
(Instant Access Point) (IDS) # signature-deassociation-broadcast
(Instant Access Point) (IDS) # detect-adhoc-using-valid-ssid
(Instant Access Point) (IDS) # detect-malformed-large-duration
(Instant Access Point) (IDS) # detect-ap-impersonation
(Instant Access Point) (IDS) # detect-adhoc-network
(Instant Access Point) (IDS) # detect-valid-ssid-misuse
```

```

(Instant Access Point) (IDS) # detect-wireless-bridge
(Instant Access Point) (IDS) # detect-ht-40mhz-intolerance
(Instant Access Point) (IDS) # detect-ht-greenfield
(Instant Access Point) (IDS) # detect-ap-flood
(Instant Access Point) (IDS) # detect-client-flood
(Instant Access Point) (IDS) # detect-bad-wep
(Instant Access Point) (IDS) # detect-cts-rate-anomaly
(Instant Access Point) (IDS) # detect-rts-rate-anomaly
(Instant Access Point) (IDS) # detect-invalid-addresscombination
(Instant Access Point) (IDS) # detect-malformed-htie
(Instant Access Point) (IDS) # detect-malformed-assoc-req
(Instant Access Point) (IDS) # detect-malformed-frame-auth
(Instant Access Point) (IDS) # detect-overflow-ie
(Instant Access Point) (IDS) # detect-overflow-eapol-key
(Instant Access Point) (IDS) # detect-beacon-wrong-channel
(Instant Access Point) (IDS) # detect-invalid-mac-oui
(Instant Access Point) (IDS) # detect-valid-clientmisassociation
(Instant Access Point) (IDS) # detect-disconnect-sta
(Instant Access Point) (IDS) # detect-omerta-attack
(Instant Access Point) (IDS) # detect-fatajack
(Instant Access Point) (IDS) # detect-block-ack-attack
(Instant Access Point) (IDS) # detect-hotspotter-attack
(Instant Access Point) (IDS) # detect-unencrypted-valid
(Instant Access Point) (IDS) # detect-power-save-dos-attack
(Instant Access Point) (IDS) # detect-eap-rate-anomaly
(Instant Access Point) (IDS) # detect-rate-anomalies
(Instant Access Point) (IDS) # detect-chopchop-attack
(Instant Access Point) (IDS) # detect-tkip-replay-attack
(Instant Access Point) (IDS) # signature-airjack
(Instant Access Point) (IDS) # signature-asleap
(Instant Access Point) (IDS) # protect-ssid
(Instant Access Point) (IDS) # rogue-containment
(Instant Access Point) (IDS) # protect-adhoc-network
(Instant Access Point) (IDS) # protect-ap-impersonation
(Instant Access Point) (IDS) # protect-valid-sta
(Instant Access Point) (IDS) # protect-windows-bridge
(Instant Access Point) (IDS) # end
(Instant Access Point) # commit apply

```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and IDS configuration sub-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
<code>inactivity-ap-timeout &lt;seconds&gt;</code>	Configures the inactivity timeout interval in seconds.	1-1000	1000
<code>no...</code>	Removes any existing configuration.	–	–

### Usage Guidelines

Use this command to configure an inactivity timeout interval for an IAP.

### Example

The following example configures the inactivity timeout interval:

```
(Instant Access Point) (config) # inactivity-ap-timeout 180  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## 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 open DNS server.

### Example

The following example configures the internal domains for a network:

```
(Instant Access Point) (config) # internal-domains
(Instant Access Point) (domain) # domain-name www.example.com
(Instant Access Point) (domain) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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

### Syntax.

Parameter	Description
<ip-address>	Assigns an IP address to the IAP.
<subnet-mask>	Specifies the subnet mask.
<nexthop-ip-address>	Specifies the gateway IP address.
<dns-ip-address>	Specifies the DNS server IP address.
<domain-name>	Specifies the domain name.

### Usage Guidelines

Use this command to assign a static IP address to the IAP.

### Example

The following example configures an IP address for the IAP.

```
(Instant Access Point)# ip-address 192.0.2.0 255.255.255.0 192.0.2.3 192.0.2.2 example.com
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## ip dhcp

```
ip dhcp <dhcp_profile>
  bid <branch-ID>
  client-count <number>
  default-router <IP-address>
  dhcp-relay
  dhcp-server <IP-address>
  dns-server <IP-address>
  domain-name <domain-name>
  exclude-address <IP-address>
  ip-range <Start-IP-address> <End-IP-address>
  lease-time <seconds>
  option <type> <value>
  option82 alu
  reserve {first <count> | last <count>}
  server-type <type>
  server-vlan <vlan-index>
  subnet <IP-address-subnet>
  subnet-mask <Subnet-Mask>
  vlan-ip <IP-address> mask <VLAN mask>
no...
```

### Description

This command configures DHCP assignment modes and scopes for Instant network.

### Syntax

Parameter	Description	Range	Default
<code>ip dhcp &lt;profile&gt;</code>	Creates a DHCP profile with a unique name.	—	—
<code>bid &lt;branch-ID&gt;</code>	Defines the branch ID. <b>NOTE:</b> You can allocate multiple branch IDs (BID) per subnet. The IAP generates a subnet name from the DHCP IP configuration, which the controller 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.	—	—
<code>client-count &lt;number&gt;</code>	Defines the number of clients allowed per DHCP branch. <b>NOTE:</b> 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	—	—

Parameter	Description	Range	Default
	allocated to a branch. The 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 <IP-address>	Defines the IP address of the default router for the Distributed, L2 DHCP scope.	–	–
dns-server <IP-address>	Defines the DNS server IP address.	–	–
dhcp-relay	<p>Enables the IAPs to intercept the broadcast packets and relay DHCP requests directly to corporate network.</p> <p>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.</p>	–	–
dhcp-server <DHCP-server-name>	Defines the IP address of the corporate DHCP server for DHCP request relay.	–	–
domain-name <Domain-name>	Defines the domain name.	–	–
exclude-address<IP-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.	–	–
ip-range <Start-IP-address> <End-IP-address>	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	–	–

Parameter	Description	Range	Default
	<p>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</p> <ul style="list-style-type: none"> <li>For <b>Distributed, L2</b> 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.</li> <li>For <b>Distributed, L3</b> mode, you can configure any discontinuous IP ranges. The configured IP range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.</li> </ul>		
<code>lease-time &lt;minutes&gt;</code>	Defines a lease time for the client in minutes.	–	720
<code>option &lt;type&gt; &lt;value&gt;</code>	<p>Defines the type and a value for the DHCP option to use.</p> <p>You can configure up to eight DHCP options supported by the DHCP server and enter the option value in "" not exceeding 255 characters.</p>	–	–
<code>option82 alu</code>	Enables the DHCP Option 82 for the Centralized, I2 DHCP scope to allow clients to send DHCP packets with the Option 82 string.	–	–
<code>reserve {first &lt;count&gt;   last &lt;count&gt;}</code>	Reserves the first few and last few IP addresses in the subnet.	–	–
<code>server-type &lt;type&gt;</code>	<p>Defines any of the following DHCP assignment modes:</p> <ul style="list-style-type: none"> <li><b>Distributed, L2</b></li> <li><b>Distributed, L3</b></li> <li><b>Local</b></li> <li><b>Local, L3</b></li> <li><b>Centralized</b></li> </ul>	distributed, I2, distributed, I3, local, local, I3, centralized, I2	Local

Parameter	Description	Range	Default
server-vlan <VLAN-ID>	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 <IP-address>	Defines the network IP address	–	–
subnet-mask <subnet-mask>	Defines the subnet mask for Local, Local,L3, and distributed,I3 DHCP scopes. The subnet mask and the network determine the size of subnet.	–	–
vlan-id <IP-address> mask <VLAN mask>	Defines the IP address and subnet mask for vlan of the DHCP server.	–	–
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 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, 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 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**–When a centralized DHCP scope is configured, The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the controller over the IPsec tunnel.

## Example

The following example configures a distributed,I2 DHCP scope:

```
(Instant Access Point) (config) # ip dhcp corpNetwork1
(Instant Access Point) (DHCP Profile"corpNetwork1") # ip dhcp server-type distributed,l2
(Instant Access Point) (DHCP Profile"corpNetwork1") # server-vlan 1
```

```
(Instant Access Point) (DHCP Profile"corpNetwork1")# subnet 192.0.1.0
(Instant Access Point) (DHCP Profile"corpNetwork1")# subnet-mask 255.255.255.0
(Instant Access Point) (DHCP Profile"corpNetwork1")# default-router 192.0.1.1
(Instant Access Point) (DHCP Profile"corpNetwork1")# client-count 0
(Instant Access Point) (DHCP Profile"corpNetwork1")# dns-server 192.0.1.2
(Instant Access Point) (DHCP Profile"corpNetwork1")# domain-name www.example.com
(Instant Access Point) (DHCP Profile"corpNetwork1")# lease-time 1200
(Instant Access Point) (DHCP Profile"corpNetwork1")# ip-range 192.0.1.0 192.0.1.17
(Instant Access Point) (DHCP Profile"corpNetwork1")# reserve first 2
(Instant Access Point) (DHCP Profile"corpNetwork1")# option 176 "MCIPADD=10.72.80.34,MCPORT=171
9,TFTPSRV=10.80.0.5,L2Q=1,L2QVLAN=2,L2QAUD=5,L2QSIG=3"
(Instant Access Point) (DHCP Profile"corpNetwork1")# end
(Instant Access Point))# commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and IP DHCP profile configuration sub-mode.



## ip dhcp pool

```
ip dhcp pool
  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-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.	–	720
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 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 IAP answers the request.

### Example

The following command configures a DHCP pool:

```
(Instant Access Point)(config)# ip dhcp pool
(Instant Access Point)(DHCP)# domain-name example.com
(Instant Access Point)(DHCP)# dns-server 192.0.2.1
(Instant Access Point)(DHCP)# lease-time 20
(Instant Access Point)(DHCP)# subnet 192.0.2.0
(Instant Access Point)(DHCP)# subnet-mask 255.255.255.0
(Instant Access Point)(DHCP)# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and IP DHCP configuration sub-mode.

## I2tpv3 session

```
l2tpv3 session <l2tpv3_session_profile>
  cookie len <cookie_length> value <cookie_value>
  l2tpv3 tunnel <l2tpv3_tunnel_name_to_associate>
  tunnel-ip <local_ip_addr_tunnel> mask <tunnel_mask_ip_addr> vlan <vlan_ID>
no...
```

### Description

This command configures an Layer-2 Tunnel Protocol (L2TP) session profile.

### Syntax

Parameter	Description	Range	Default
l2tpv3 session <name>	Configures the session profile name.	–	–
cookie len <length_of_cookie> value <cookie_value>	Configures length and alphanumeric value for the cookie.	Length: 4/8 If cookie length is 4, the cookie value should have exactly 8 hex characters If cookie length is 8, the cookie value should have exactly 16 hex characters	Not set.
l2tpv3 tunnel <l2tpv3_tunnel_profile_name>	Selects the tunnel profile name where the session will be associated.	–	–
tunnel <local_ip_addr_tunnel> mask <tunnel_mask_ip_addr> vlan <vlan_ID>	Configures the local IP address, network mask, and VLAN ID of the tunnel.	VLAN ID: 2-4094	–
no...	Removes the configuration.	–	–

### Usage Guidelines

Use this command to configure the session to carry the L2TP data.

### Example

The following example configures the L2TPv3 session:

```
(Instant Access Point) (config) # l2tpv3 session test_session
(Instant Access Point) (L2TPv3 Session Profile "test_session")# cookie len 4 value 12345678
(Instant Access Point) (L2TPv3 Session Profile "test_session")# l2tpv3 tunnel test_tunnel
(Instant Access Point) (L2TPv3 Session Profile "test_session")# tunnel-ip 1.1.1.1 mask 255.255.255.0 vlan 2
(Instant Access Point) (L2TPv3 Session Profile "test_session")# end
```

```
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

IAP Platform	Command Mode
RAP-108 RAP-109 IAP-135	Configuration mode and L2TPV3 session profile configuration sub-mode.

## I2tpv3 tunnel

```
l2tpv3 tunnel <l2tpv3_tunnel_profile>
  backup peer-address <peer_IP_address_backup_tunnel>
  checksum
  failover-mode <preemptive|non-preemptive>
  failover-retry-count <retry_count>
  failover-retry-interval <interval_in_seconds>
  hello-timeout <interval_in_seconds>
  local-port <local_udp_port_number>
  message-digest-type <digest_algorithm>
  mtu <tunnel_MTU_size>
  peer-port <peer_udp_port_number>
  primary peer-address <peer_IP_address_primary_tunnel>
  secret-key <secret_key>
  no...
```

### Description

This command configures an L2TP tunnel profile.

### Syntax

Parameter	Description	Range	Default
l2tpv3 tunnel <profile-name>	Configures the tunnel profile name and allows you to enter the L2TP tunnel sub-configuration mode.	–	–
backup peer-address <peer_IP_address_ backup_tunnel>	Assigns IP address of the remote end backup tunnel.	–	–
checksum	Enables the generation of UDP checksums in packets sent to L2TP peer IP address.	–	enabled
failover-mode <mode>	Assigns the backup/primary tunnel failover mode.	preemptive, non-preemptive	preemptive
failover-retry-count <count>	Assigns the number of failover attempts.	0-5	0
failover-retry-interval <interval_in_sec>	Assigns the interval between each failover attempt.	60-300 seconds	60
hello-timeout <interval_in_seconds>	Configures the interval (in seconds) at which hello packets are routed in the tunnel.	5-300	60
local-port <local_udp_port>	Assigns the local UDP port number of the client.	1–65535	1701

Parameter	Description	Range	Default
message-digest-type <digest_algo>	Configures the message digest to be used to create the MD AVP.	MD5, SHA1, none	MD5
mtu <MTU-size>	Configures a Maximum Transmission Unit (MTU) value for the tunnel.	1–65535	1460
peer-port <peer_udp_port>	Assigns a UDP server port to the remote end.	1–65535	1701
primary peer-address <peer_IP_address_primary_tunnel>	Assigns IP address of the remote end tunnel.	–	–
secret-key <key>	Configures a shared key to use for message digest.	–	–

## Usage Guidelines

Use this command tunnel data or traffic to L2TP Network Server (LNS).

## Example

The following example configures the L2TPv3 tunnel:

```
(Instant Access Point) (config) # l2tpv3 tunnel test_tunnel
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # primary peer-address 10.0.0.65
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # backup peer-address 10.0.0.63
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # failover-mode non-preemptive
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # failover-retry-count 5
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # failover-retry-interval 80
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # hello-timeout 150
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # mtu 1570
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # peer-port 3000
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # secret-key test123
(Instant Access Point) (L2TPv3 Tunnel Profile "test_tunnel") # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

IAP Platform	Command Mode
RAP-108 RAP-109 IAP-135	Configuration mode and L2TPV3 tunnel configuration sub-mode.

## I3-mobility

```
l3-mobility
  home-agent-load-balancing
  virtual-controller <IP-address>
  subnet <IP-address-subnet> <subnet-mask> <vlan> <virtual-controller-IP-address>
no...
```

### Description

This command configures Layer-3 mobility on an IAP.

### Syntax

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 AP for roamed clients by using a round robin policy. With this policy, the load for the APs acting as Home Agents for roamed clients is uniformly distributed across the IAP cluster.	–	Disabled
virtual-controller <IP-address>	Adds the IP address of a Virtual Controller to the mobility domain.  In the typical deployment scenario, all the APs are configured in one subnet and all the clients in another subnet. You can also deploy APs across different subnets, in which case the APs in each subnet will form a cluster with its own Virtual Controller IP address. To allow clients to roam seamlessly among all the APs, the Virtual Controller IP for each of the foreign subnets must be configured for each IAP cluster.	–	–
<IP-address>	Configures the IP address for the subnets support in an IAP cluster.	–	–
subnet <subnet-mask>	Specifies the subnet mask.	–	–
<vlan>	Assigns the VLAN applicable to the IAP cluster.	1-4093	–
<virtual-controller IP>	Specifies the IP address of the Virtual Controller in an IAP cluster.	–	–
no...	Removes the configuration.	–	–

### Usage Guidelines

Use this command to configure layer-3 mobility domains on an IAP.

### Example

The following example configures L3-mobility:

```
(Instant Access Point) (config) # l3-mobility
(Instant Access Point) (L3-mobility) # home-agent-load-balancing
(Instant Access Point) (L3-mobility) # virtual-controller 192.0.2.1
(Instant Access Point) (L3-mobility) # subnet 192.0.2.2 255.255.255.0 1 192.0.2.1
(Instant Access Point) (L3-mobility) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and L3 mobility configuration sub-mode.



## led-off

led-off  
no...

### Description

This command disables LED display on an IAP.

### Syntax

Command/Parameter	Description
led-off	Disables LED display.
no...	Re-enables LED display.

### Usage Guidelines

Use this command to disable the LED display.

### Example

The following example disables LED display on an IAP:

```
(Instant Access Point)# led-off
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# logout

logout

## Description

This command logs you out of the current CLI session.

## Usage Guidelines

Use this command to log out of the current CLI session and return to the user login prompt.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# mas-integration

mas-integration  
no...

## Description

This command enables Mobility Access Switch integration on an IAP.

## Syntax

Parameter	Description
mas-integration	Enables you to integrate the IAP with a Mobility Access Switch.
no...	Removes the configuration.

## Usage Guidelines

Use this command to integrate Mobility Access Switch with an IAP.

You can integrate an IAP with a Mobility Access Switch by connecting it directly to the switch port. The following Mobility Access Switch integration features can be applied while integrating with an IAP:

- **Rogue AP containment**—When a rogue AP is detected by an IAP, it sends the MAC Address of the rogue AP to the Mobility Access Switch. The Mobility Access Switch blacklists the MAC address of the rogue AP and turns off the PoE on the port.
- **PoE prioritization**— When an IAP is connected directly into the Mobility Access Switch port, the Mobility Access Switch port increases the PoE priority of the port. This is done only if the PoE priority is set by default in the Mobility Access Switch.



The PoE Prioritization and Rogue AP Containment features is available for ArubaOS 7.2 release on Aruba Mobility Access Switches.

- **GVRP Integration**—Configuring GARP VLAN Registration Protocol (GVRP) enables the switch to dynamically register or de-register VLAN information received from a GVRP applicant such as an IAP. GVRP also enables the switch to propagate the registered VLAN information to the neighboring switches in the network.



The associated static VLANs in the wired and wireless profiles are propagated to the upstream Mobility Access Switch using GVRP messages.

When an IAP is integrated with a Mobility Access Switch, the Link Layer Discovery Protocol (LLDP) is enabled. Using this protocol, the IAPs instruct the Mobility Access Switch to turn off the ports where rogue APs are connected, perform actions such as increasing the PoE priority, and configure the VLANs on the ports to which the IAPs are connected.

## Example

The following example enables Mobility Access Switch integration for an IAP:

```
(Instant Access Point) (config) # mas-integration
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# mesh

mesh  
no...

## Description

This command sets up mesh network on an IAP.

## Syntax

Parameter	Description
mesh	Enables mesh network on the IAP.
no...	Removes the configuration.

## Usage Guidelines

Use this command to set up mesh network on an IAP. Mesh network requires at least one valid uplink (wired or 3G) connection. Any provisioned IAP that has a valid uplink (wired or 3G) functions as a mesh portal, and the IAP without an Ethernet link functions as a mesh point. The mesh portal can also act as a Virtual Controller. A Mesh portal (MPP) 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 IAPs configured for mesh.

Mesh IAPs detect the environment when they boot up, locate and associate with their nearest neighbor, to determine the best path to the mesh portal.

Instant mesh functionality is supported only on dual radio IAPs only. On dual-radio 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.



---

Mesh service is automatically enabled on 802.11a band for dual-radio IAP only, and this is not configurable.

---

The mesh network must be provisioned for the first time by plugging into the wired network. After that, mesh works on IAP ROWs like any other regulatory domain.

## Example

The following example enables mesh network on an IAP:

```
(Instant Access Point) (config)# mesh
(Instant Access Point) (config)# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## mgmt-auth-server

```
mgmt-auth-server <server>  
no...
```

### Description

This command configures authentication servers for management user interface of the Virtual Controller.

### Syntax

Parameter	Description
mgmt-auth-server <server>	Configures a server for management user authentication.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure a management authentication server for administrator users of a Virtual Controller.

### Example

The following example configures an authentication server for the management user interface:

```
(Instant Access Point) (config) # mgmt-auth-server server1  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

## Syntax

Parameter	Description
mgmt-auth-server-load-balancing	Enables load balancing between the primary and the backup authentication servers
no...	Removes the configuration.

## Usage Guidelines

Use this command to enable load-balancing when two servers are configured.

## Example

The following example enables load-balancing between two authentication servers.

```
(Instant Access Point) (config) # mgmt-auth-server-load-balancing  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

## Syntax

Parameter	Description
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.

## Usage Guidelines

Use this command to configure a backup authentication server for the Virtual Controller management interface.

## Example

The following example configures a backup internal authentication server:

```
(Instant Access Point) (config) # mgmt-auth-server-local-backup  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## mgmt-user

mgmt-user <username> [<password>] [<type>]

### Description

This command configures user credentials for access to the Virtual Controller Management User Interface.

### Syntax

Parameter	Description
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.

### Usage Guidelines

Use this command to configure administrator credentials to access and configure the IAP.

### Example

The following example configures administrator login credentials for the IAP management interface:

```
(Instant Access Point) (config) # mgmt-user User1 Password123 guest-mgmt
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## name

name <name>

### Description

This command configures a unique name for the IAP.

### Syntax

Parameter	Description
name <name>	Configures a name for the IAP or the Virtual Controller.

### Usage Guidelines

Use this command to configure a name for the IAP:

### Example

The following example configures a name for the IAP:

```
(Instant Access Point)# hostname <system-name>
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## ntp-server

```
ntp-server <Name>  
no...
```

### Description

This command configures NTP server for an IAP.

### Syntax

Parameter	Description	Default
ntp-server <Name>	Configures the IP address or the URL (domain name) of the NTP server.	pool.ntp.org
no	Removes the configuration	—

### Usage Guidelines

The Network Time Protocol (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 Instant network, an IAP reboot may lead to variation in time data.

### Example

The following command configures an NTP server for an IAP:

```
(Instant Access Point) (config) # ntp-server <name>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# opendns

```
opendns <user> <password>  
no...
```

## Description

This command configures OpenDNS credentials for filtering content and to create Internet access policies that allow or deny user access to Websites based on Website categories and security ratings.

## Syntax

Parameter	Description
opendns	Configures user credentials to enable access to OpenDNS to provide enterprise-level content filtering.
<user>	Configures user name to access OpenDNS.
<password>	Configures password to access OpenDNS.
no...	Removes the configuration.

## Usage Guidelines

Use this command to configure OpenDNS credentials to allow Instant to filter content at the enterprise-level.

## Example

The following example configures OpenDNS credentials:

```
(Instant Access Point) (config) # opendns <username <password>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# organization

organization <name>  
no...

## Description

This command configures an organization string for IAPs managed or monitored by the AirWave Management console.

## Syntax

Parameter	Description	Range
organization <name>	Specifies the name of your organization.	You can use any of the following strings: <ul style="list-style-type: none"><li>• AMP Role– "Org Admin" (initially disabled)</li><li>• AMP User– "Org Admin" (assigned to the role "Org Admin")</li><li>• Folder– "Org" (under the Top folder in AMP)</li><li>• Configuration Group– "Org"</li></ul> You can also assign additional strings to create a hierarchy of sub folders under the folder named "Org": For example: <ul style="list-style-type: none"><li>• subfolder1 for a folder under the "Org" folder</li><li>• subfolder2 for a folder under subfolder1</li></ul>
no...	Removes the configuration settings.	–

## Usage Guidelines

Use this command to specify an organization string for integrating the AirWave Management Server with the IAP. The organization is a set of colon-separated strings created by the AirWave administrator to accurately represent the deployment of each IAP. This string is defined by the installation personnel on the site.

## Example

The following command configures an AirWave organization string:

```
(Instant Access Point)(config)# organization aruba
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# ping

ping <host>

## Description

This command sends ICMP echo packets to the specified IP address.

## Syntax

Parameter	Description
<host>	Displays the IP address of the host.

## Usage Guidelines

You can send up to five ICMP echo packets to a specified IP address. The IAP times out after two seconds.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	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.

### Syntax

Parameter	Description
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 Challenge Handshake Authentication Protocol (CHAP) authentication.  You can use a maximum of 34 characters for the CHAP secret key.
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.

### Usage Guidelines

Use this command to configure PPPoE uplink connection for an IAP.

### Example

The following example configures the PPPoE uplink on an IAP:

```
(Instant Access Point) (config) # pppoe-uplink-profile
(Instant Access Point) (pppoe-uplink-profile) # pppoe-username User1
(Instant Access Point) (pppoe-uplink-profile) # pppoe-passwd Password123
(Instant Access Point) (pppoe-uplink-profile) # pppoe-svcname internet03
(Instant Access Point) (pppoe-uplink-profile) # pppoe-chapsecret 8e87644deda9364100719e017f88ebc
e
(Instant Access Point) (pppoe-uplink-profile) # pppoe-unnumbered-local-l3-dhcp-profile dhcpProfile1
(Instant Access Point) (pppoe-uplink-profile) # end
(Instant Access Point) # commit apply
```



## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and PPPoE uplink profile configuration sub-mode.

## proxy

```
proxy {exception <host>| server <host> <port>}
```

### Description

This command configures HTTP proxy settings.

### Syntax

Parameter	Description
exception <hostname>	Sets the IP address or the domain name of the host to be added under the exception list.
server <hostname> <port number>	Sets the HTTP proxy server's IP address or domain name and the port number.

### Usage Guidelines

This command configures the HTTP proxy settings in an IAP to download the image from the cloud server.

### Example

The following example configures an HTTP proxy settings in an IAP:

```
(Instant Access Point) (config) # proxy exception 192.0.2.2
(Instant Access Point) (config) # proxy server 192.0.2.1 8080
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# reload

reload <all>

## Description

This command performs a reboot of the Virtual Controller.

## Syntax

Parameter	Description
<all>	Reloads all IAPs in a cluster.

## Usage Guidelines

Use this command to reboot an IAP after making configuration changes or under the guidance of Aruba Networks customer support. The reload command powers down the IAP, making it unavailable for configuration. After the IAP reboots, you can access it via a local console connected to the serial port, or through an SSH, Telnet, or WebUI session. If you need to troubleshoot the IAP during a reboot, use a local console connection.

After you use the reload command, the IAP prompts you to confirm this action. If you have not saved your configuration, the 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 IAP.

If your configuration has already been saved, the IAP returns the following message:

```
Do you really want to reset the system(y/n):
```

- Enter **y** to reboot the IAP.
- Enter **n** to cancel this action.

The command will timeout if you do not enter **y** or **n**.

## Example

The following command assumes you have already saved your configuration and you must reboot the IAP:

The IAP returns the following messages:

```
Do you really want to reset the system(y/n): y
System will now restart!
...
Restarting system.
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

## Syntax

Parameter	Description
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.

## Usage Guidelines

Use this command to remove the entries for the clients that are dynamically blacklisted.

## Example

The following command deletes the blacklisted IAP client entries:

```
(Instant Access Point) (config) # remove-blacklist-client d7:a:b2:c3:45:67 AP125
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

### Syntax

Parameter	Description
no...	Removes the configuration.

### Usage Guidelines

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 IAP, including clients connected to a slave IAP.

### Example

The following example enables restricted access to the corporate network;

```
(Instant Access Point) (config) # restrict-corp-access  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

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 IAP.

### Syntax

Parameter	Description
subnet	Configures a management subnet address.
mask	Configures the subnet mask for the management subnet address.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure management subnets. This ensures that the 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.

### Example

The following example configures a management subnet;

```
(Instant Access Point) (config) # restricted-mgmt-access 192.0.2.13 255.255.255.255  
(Instant Access Point) (config) # end  
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## rf dot11a-radio-profile

```
rf dot11a-radio-profile
  beacon-interval <interval>
  csa-count <count>
  dot11h
  interference-immunity <immunity-level>
  legacy-mode
  max-distance <count>
  spectrum-band <type>
  spectrum-monitor
  no...
```

### Description

This command configures a 5.0GHz or 802.11a radio profile for an IAP.

### Syntax

Parameter	Description	Range	Default
rf dot11a-radio-profile	Enables the 5.0 GHz RF configuration sub-mode	–	–
beacon-interval <interval>	Enter the Beacon period for the IAP in milliseconds.  When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.	60-500	100
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
dot11h	Allows the IAP to advertise its 802.11d (country information) and 802.11h (transmit power control) capabilities.	–	Disabled
interference-immunity <immunity-level>	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: <ul style="list-style-type: none"><li>• Level 0– no ANI adaptation.</li><li>• 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.</li><li>• 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.</li><li>• 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</li></ul>	0-5	2



Parameter	Description	Range	Default
	<p>sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones.</p> <ul style="list-style-type: none"> <li>Level 4– Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference.</li> <li>Level 5– The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing.</li> </ul> <p><b>NOTE:</b> Increasing the immunity level makes the AP to lose a small amount of range.</p>		
legacy-mode	Enables the IAPs to run the radio in non-802.11n mode.	–	Disabled
max-distance <count>	<p>Configures the maximum distance between a client and an AP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times.</p> <p>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.</p>	600-100000 meters	0
spectrum-band <type>	Allows you to specify the portion of the channel to monitor for 5 GHz configuration.	–	–
spectrum-monitor	Allows the IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	–	–
no...	Removes the configuration.	–	–

## Usage Guidelines

Use this command to create a 5.0 GHz radio profile on an IAP.

## Example

The following example configures the 5 GHz radio profile:

```
(Instant Access Point) (config)# rf dot11a-radio-profile
(Instant Access Point) (RF dot11a Radio Profile)# beacon-interval 100
(Instant Access Point) (RF dot11a Radio Profile)# legacy-mode
(Instant Access Point) (RF dot11a Radio Profile)# dot11h
(Instant Access Point) (RF dot11a Radio Profile)# interference-immunity 3
(Instant Access Point) (RF dot11a Radio Profile)# max-distance 600
(Instant Access Point) (RF dot11a Radio Profile)# csa-count 2
(Instant Access Point) (RF dot11a Radio Profile)# spectrum-monitor
(Instant Access Point) (RF dot11a Radio Profile)# end
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and RF dot11a Radio Profile configuration sub-mode

## rf dot11g-radio-profile

```
rf dot11g-radio-profile
  beacon-interval <interval>
  csa-count <count>
  dot11h
  interference-immunity <immunity-level>
  legacy-mode
  max-distance <count>
  spectrum-monitor
  no...
```

### Description

This command configures a 2.4.GHz or 802.11g radio profile for an IAP.

### Syntax

Parameter	Description	Range	Default
<code>rf dot11g-radio-profile</code>	Enables the 2.4 GHz RF configuration sub-mode	–	–
<code>beacon-interval &lt;interval&gt;</code>	Enter the Beacon period for the IAP in milliseconds.  When enabled, the 802.11 beacon management frames are transmitted by the access point at the specified interval.	60-500	100
<code>csa-count &lt;count&gt;</code>	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
<code>dot11h</code>	Allows the IAP to advertise its 802.11d (country information) and 802.11h (transmit power control) capabilities.	–	Disabled
<code>interference-immunity &lt;immunity-level&gt;</code>	Configures the immunity level to improve performance in high-interference environments. You can specify any of the following immunity levels: <ul style="list-style-type: none"><li>• Level 0– no ANI adaptation.</li><li>• 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.</li><li>• 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</li></ul>	0-5	2

Parameter	Description	Range	Default
	<p>high-level of interference related to 2.4 GHz appliances such as cordless phones.</p> <ul style="list-style-type: none"> <li>Level 4– Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference.</li> <li>Level 5– The AP completely disables PHY error reporting, improving performance by eliminating the time the IAP would spend on PHY processing.</li> </ul> <p><b>NOTE:</b> Increasing the immunity level makes the AP to lose a small amount of range.</p>		
legacy-mode	Enables the IAPs to run the radio in non-802.11n mode.	–	Disabled
max-distance <count>	<p>Configures the maximum distance between a client and an AP or between a mesh point and a mesh portal in meters. This value is used to derive ACK and CTS timeout times.</p> <p>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.</p>	600-100000 meters	0
spectrum-monitor	Allows the IAPs in access mode to continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving clients.	–	Disabled
no...	Removes the configuration.	–	–

## Usage Guidelines

Use this command to create a 2.4 GHz radio profile on an IAP.

## Example

The following example configures the 2.4GHz radio profile:

```
(Instant Access Point) (config) # rf dot11g-radio-profile
(Instant Access Point) (RF dot11g Radio Profile) # beacon-interval 200
(Instant Access Point) (RF dot11g Radio Profile) # no legacy-mode
(Instant Access Point) (RF dot11g Radio Profile) # dot11h
(Instant Access Point) (RF dot11g Radio Profile) # interference-immunity 3
(Instant Access Point) (RF dot11g Radio Profile) # max-distance 600
(Instant Access Point) (RF dot11g Radio Profile) # csa-count 2
(Instant Access Point) (RF dot11g Radio Profile) # spectrum-monitor
(Instant Access Point) (RF dot11g Radio Profile) # end
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and RF dot11g Radio Profile sub-mode

## rf-band

```
rf-band {2.4| 5| all}
```

### Description

This command configures the radio frequency band for an IAP.

### Syntax

Parameter	Description	Range	Default
<code>rf-band {2.4  5  all}</code>	Configures a radio frequency band for an IAP. You can configure any of the following options: <ul style="list-style-type: none"><li>• 2.4 – For 2.4 GHz band or 802.11g configuration</li><li>• 5 – For 5 GHz and 802.11a configuration</li><li>• all - For a mixed configuration of 2.4.GHz and 5 GHz</li></ul>	2.4, 5, all	all

### Usage Guidelines

Use this command to configure RF band for an IAP.

### Example

The following example configures the 5 GHz RF band for an IAP.

```
(Instant Access Point) (config) # rf-band 5
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## routing-profile

```
routing-profile
  route <destination> <mask> <gateway>
  no...
```

### Description

This command configures a routing profile to define the corporate subnets, which must to be tunneled through IPsec.

### Syntax

Parameter	Description
routing-profile <profile>	Creates a routing profile for routing traffic into the VPN tunnel.
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 controller IP address on which the VPN connection is terminated.
no...	Removes the configuration

### Usage Guidelines

Use this command to configure a routing profile for VPN connections.

### Example

The following example configures a routing profile:

```
(Instant Access Point) (config) # routing-profile
(Instant Access Point) (Routing-profile) # route 192.0.1.0 255.255.255.0 192.0.2.0
(Instant Access Point) (Routing-profile) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and routing profile configuration sub-mode.

## show 1xcert

show 1xcert

### Description

This command displays the details about the external server certificate, which is used by the IAP for client authentication.

### Usage Guidelines

Use this command to view information about the server certificates uploaded to an IAP.

### Example

The following example shows the output of **show 1xcert** command:

```
Default Server Certificate:
Version      :3
Serial Number :01:DA:52
Issuer       :C=US, O=GeoTrust Inc., OU=Domain Validated SSL, CN=GeoTrust DV SS
              L CA
Subject      :0x05=1LUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.aruban
              etworks.com, OU=GT28470348, OU=See www.geotrust.com/resources/cps
              (c)11, OU=Doma in Control Validated - QuickSSL(R) Pr
emium, 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 IAP.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# show about

show about

## Description

This command displays information about Instant.

## Usage Guidelines

Use this command to view information such as Instant version, build time and IAP model.

## Example

The **show about** command displays the Build Time, IAP model number, the Instant version, Website address of organization, and Copyright information. The following example shows the **show about** command output:

```
Name           :Aruba Operating System Software
Type           :135
Build Time     :2013-03-31 11:47:06 PDT
Version        :6.2.1.0-3.3.0.0_37845
Website        :http://www.arubanetworks.com
Legal          :Copyright (c) 2002-2013, Aruba Networks, Inc.
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

### Syntax

Parameter	Description
<name>	Displays the access rule configuration details based the name specified for this parameter.

### Usage Guidelines

Use this command to view information an access rule configured for a network profile.

### Example

The following output is displayed for the **show access-rule** command:

```
Dest IP   Dest Mask  Dest Match  Protocol (id:sport:eport)  Action  Log  TOS  802.1P
-----
any       any        match      https                      permit
any       any        match      http-proxy2                permit
any       any        match      h323-tcp                   permit
any       any        match      gre                         permit

Blacklist Mirror DisScan ClassifyMedia
-----
```

The output of this command displays information about the access rule configuration parameters, which indicate whether a particular type of traffic is to allowed to a particular destination, 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show access-rule-all

show access-rule-all

### Description

This command displays details of all access rules configured on the IAP.

### Usage Guidelines

Use this command to view information access rules configured on the IAP.

### Example

The following output is displayed for 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) Action  Log  TOS  802.1P  Blacklist
Mirror  DisScan  ClassifyMedia
-----  -----  -----  -----  -----  ---  ---  ---  -----
any      any      match      any      permit
Vlan Id           :0
ACL Captive Portal:disable
Access Rule Name :wired-instant
In Use           :Yes
Access Rules
-----
Dest IP  Dest Mask  Dest Match  Protocol (id:sport:eport) Action  Log  TOS  802.1P
Blacklist Mirror  DisScan  ClassifyMedia
-----  -----  -----  -----  -----  ---  ---  ---  -----
10.17.88.188 255.255.255.255 match      http      permit
10.17.88.188 255.255.255.255 match      6:4343:4343 permit
any          any      match      dhcp      permit
any          any      match      dns       permit
Vlan Id           :0
ACL Captive Portal:disable
Access Rule Name :Network1
In Use           :Yes
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
Access Rule Name :Rule2
In Use           :Yes
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

The output of this command includes the following parameters:

Parameter	Description
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show airgroup

```
show airgroup {blocked-queries| blocked-service-id | cache {<MAC-address> | entries} | cppm {a
uth server [coa-capable | non-coa-only] | entries | query-interval | server} |cppm-entry <MA
C-address> | debug statistics| internal-state statistics | servers [verbose] | status | swarm-
info| users}
```

### Description

This command displays the AirGroup configuration details for an IAP client.

### Syntax

Parameter	Description
blocked-queries	Displays blocked queries if any.
blocked-service-id	Displays blocked services and service IDs if any.
cache <MAC-address> cache entries	Displays AirGroup cache details for a specific IAP or for the IAP clients in a cluster.
cppm {auth server [coa-capable   non- coa-only]   entries   query-interval   server}	Displays CPPM server details associated with AirGroup configuration.
cppm-entry <MAC- address>	Displays CPPM server details for an AirGroup client.
debug statistics	Displays debug statistics for AirGroup enabled IAPs.
internal-state statistics	Displays statistical details of queries and responses, and RADIUS client messages.
servers [verbose]	Displays AirGroup server details.
status	Indicates the AirGroup feature activation status.
swarm-info	Displays information about the AirGroup cluster.
users	Displays the list of AirGroup users.

### Usage Guidelines

Use the **show airgroup** commands to view the AirGroup configuration details on an IAP.

### 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
-----
```

The output of this command includes the following information:

Column	Description
Name	Indicates the name of IAP.
Type	Indicates the IAP model.
Class	Indicates if the IAP is serving as master or slave.
TTL	Indicates the duration after which the cache entries expire.
Origin	Indicates the origin 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 CPPM server.
IP address	Indicates the IP address of the CPPM server.
Port	Indicates the authorization port number of the CPPM server.
timeout	Indicates timeout value in seconds for one RADIUS request.
rfc3576	Indicates if the IAPs are configured to process RFC 3576-compliant Change of Authorization (CoA).
rfc3576-only	Indicates if 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 IAP.
ap id	Displays the MAC address of the IAP on which AirGroup is configured.
ap ip	Displays the IP address of the IAP on which AirGroup is configured.
update no	Indicates the number of configuration updates if any.

Column	Description
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 AP name
shared location-id AP-FQLN	Indicates the shared location ID associated with the fully qualified domain name of the AP
shared location-id AP-group	Indicates the shared location ID associated with the AP 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 CPPM 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              :0x1f
```

#### AirGroup Debug Statistics

```
-----
Key                          Value
---                          -
network cache init counter    1 (1)
mdns apdb init counter        1 (1)
airgroup restore count        1 (1)
mdns ap to swarm hello tx     6 (6)
mdns total pkt sent to asap tx 6 (6)
swarm vc ip not configured    6 (6)
```

The output of this command provides the following information:

Column	Description
Airgroup slave status	Indicates the AirGroup configuration status on the slave IAP.
Airgroup master status	Indicates the AirGroup configuration status on the slave IAP.
Airgroup multi swarm status	Indicates the status of the inter cluster mobility.
status value	Indicates the status value.
Airgroup Debug Statistics	Displays details of AirGroup counters.

### show airgroup internal-state statistics

The following output is displayed for the **show airgroup internal-state statistics** command:

```
Time: Tue Jan 4 00:25:01 2000
```

```
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 Statistics
-----
Functionality          Hit Count Since Last Read Hit Count Total Average Time in microsec (s
ince 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 Host Name Service VLAN Wired/Wireless Role Username AP-Name Rec-dropped Rec-f
iltered Rec-responded Last-query
-----
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.
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.
Username	Displays the username details.

Column	Description
AP-name	Displays the name of the AP.
Rec-dropped	Indicates the records that were dropped.
Rec-filteres	Indicates the records that were filtered.
Rec-responded	Indicates the records to which responses were received.
Last-query	Displays the last query.
Num servers	Displays the total number of servers.
Max Servers	Displays the maximum number of servers that can be configured.

### show airgroup status

The following output is displayed for the **show airgroup status** command:

```
AirGroup 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   Enabled
itunes     Disabled
remotemgmt Enabled
sharing    Enabled
chat       Enabled
allowall   Disabled
```

The output of this command provides the following information:

Column	Description
Airgroup feature status	Indicates if the AirGroup feature 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 CPPM 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.

Column	Description
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 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show airgroupservice

show airgroupservice [disallow {role| vlan}]

## Description

This command displays the AirGroup service configuration details for an IAP.

## Syntax

Parameter	Description
show airgroupservice	Displays a summary of the configuration details for AirGroup services such as AirPlay and AirPrint.
disallow {role  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 AirPrint or AirPlay.

## Usage Guidelines

Use the **show airgroupservice** command to view the AirGroup services configured on an IAP.

## Examples

The following output is displayed for the **show airgroupservice** command:

```
AirGroupService Details
-----
Service   Description   Disallowed-Role           Disallowed-VLAN   ID
-----   -
airplay   AirPlay      default_wired_port_profile 1                   _airplay._tcp
          port         100                       200                 _raop._tcp
          port         100                       200                 _ptp._tcp
airprint  AirPrint     default_wired_port_profile 1                   _ipp._tcp
          port         100                       100                 _pdl-datastream._tcp
          port         200                       200                 _printer._tcp
          port         200                       200                 _scanner._tcp
          port         200                       200                 _universal._sub._ipp._tcp
          port         200                       200                 _printer._sub._http._tcp
          port         200                       200                 _http._tcp
          port         200                       200                 _http-alt._tcp
          port         200                       200                 _ipp-tls._tcp
          port         200                       200                 _fax-ipp._tcp

Num Services:2
Num Service-ID:13
```

The following example shows the 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 output displayed for the **show airgroupservice disallow vlan** command:

```
airplay
```

```

-----
1
100
200
airprint
-----
1
100
200

```

The output of these commands provides the following information:

Column	Description
Service	Indicates the AirGroup services such as AirPlay and AirPrint services enabled on an IAP.
Description	Displays a brief description of the AirGroup service.
Disallowed-Role	Indicates the user roles that are restricted from accessing the AirGroup service.
Disallowed-VLAN	Indicates the VLANs that are restricted from accessing the AirGroup service.
ID	Displays the ID associated with AirPlay and AirPrint services.
airplay	Displays the list of user roles and VLANs that are not allowed to access the AirPlay service.
airprint	Displays the list of user roles and VLANs that are not allowed to access the AirPrint service.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP for its AirGroup clients.

### Syntax

Parameter	Description
service	Indicates the name of the service and displays the service ID details of specified AirGroup service.

### Usage Guidelines

Use the **show airgroupservice** command to view the IDs of the AirGroup services configured on an IAP.

### Examples

The following output is displayed for the **show airgroupservice-ids** command for the AirPlay service:

```
(Instant Access Point)# show airgroupservice-ids airplay
airplay
-----
Service ids
-----
_airplay._tcp
_raop._tcp
_appletv-v2._tcp
```

The output of this command displays the service ID associated with the AirGroupservice.

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ale

```
show ale {config| status}
```

### Description

This command displays the ALE configuration details.

### Syntax

Parameter	Description
config	Displays the ALE configuration details.
status	Displays the status of ALE server.

### Usage Guidelines

Use this command to view the ALE configuration status.

### Example

The following example shows the output of the **show ale config** command:

```
(Instant Access Point)# 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 status** command:

```
(Instant Access Point)# 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.



## Command Information

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 IAP.

### Syntax

Parameter	Description
<count>	Filters client alerts based on the specified number.

### Usage Guidelines

Use this command to view the client alerts for an IAP. The client alerts occur when clients are connected to the Instant network. Alerts are generated when a client encounters problems while accessing or connecting to the IAP network.

### 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 when no client alerts are generated.

```
Client Alerts
-----
Timestamp  Type  MAC Address  Description  Access Point
-----  ---  -

```

The output of this command provides the following information:

Parameter	Description
Timestamp	Displays the time at which the client alert was recorded.
MAC Address	Displays the MAC address of the client that caused the alert.
Description	Provides a short description of the alert.
Access Point	Displays the IP address of the IAP to which the client is connected.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show alg

show alg

## Description

This command displays the Application Layer Gateway (ALG) protocol information configured on an IAP.

## Usage Guidelines

Use this command to view configuration details for the ALG protocols. 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 Skinny Call Control Protocol (SCCP), Session Initiation Protocol (SIP), Alcatel-Lucent NOE (UA), and VOCERA are enabled.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show allowed-aps

show allowed-aps

## Description

This command displays the list of IAPs that are allowed to join the IAP cluster.

## Usage Guidelines

Use this command to view the IAP whitelist.

## 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:

Parameter	Description
Allow New APs	Indicates if the new IAPs are allowed to join the network.
MAC Address	Displays the MAC address of the IAPs that are allowed to join the network.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show apas status

```
show apas status
```

### Description

This command displays the Aruba Product Activation Services (APAS) status for Instant provisioning.

### Usage Guidelines

Use this command to view the provisioning status of an IAP.

### Example

The following examples show the output displayed for the **show apas status** command:

```
APAS Status           :connection-failed
APAS Status           :protocol-error-XXX
```

The *connection-failed* message indicates that the IAP failed to establish a connection to activate server.

The *protocol-error-XXX* message indicates that the IAP encountered an internal protocol error when negotiating with the Aruba Activate server. Contact the Instant support team to debug this issue.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap-env

show ap-env

### Description

This command displays all provisioned AP parameters such as the type of antenna used by an. The output of this command also indicates if the IAP is provisioned as a master IAP.

### Usage Guidelines

Use this command to view the antenna configuration details for an IAP.

### Example

The following output is displayed for the **show ap-env** command:

```
Antenna Type:Internal  
Iap_master:1
```

The output of this command indicates if the IAP is configured to use an external or integrated antenna and if the IAP is configured as a master IAP.

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show aps

```
show aps [scanning][sync]
```

### Description

This command displays all active IAPs, IAP scanning, and synchronization status.

### Syntax

Parameter	Description
aps	Displays the list of all active IAPs in the cluster.
aps scanning	Displays IAP scanning details.
aps sync	Displays IAP synchronization details.

### Usage Guidelines

Use this command to view the list of active IAPs, IAP scanning and synchronization details.

### Example

The following output is displayed for the **show aps** command:

```
AP List
-----
Name           IP Address           Mode   Spectrum  Clients  Type  Mesh Role  2.4 Channel
-----
d8:c7:c8:cb:d4:20 10.17.88.188 access  disable   1        135    Portal    7

2.4 Power (dB)  2.4 Utilization (%)  2.4 Noise Floor (dBm)  5.0 Channel  5.0 Power (dB)
-----
21              52 (ok)              -91 (good)              44+          22

5.0 Utilization (%)  5.0 Noise Floor (dBm)  Need Antenna Config  From Port  Config Id
-----
3 (good)            -91 (good)              No                    none       1
```

The output of this command includes the following parameters:

Column	Description
Name	Displays the Name of the IAPs.
IP address	Displays the IP address of the IAPs.
Mode	Displays the operating mode. For example, access, monitor, or spectrum monitor modes.
Spectrum	Indicates if spectrum monitoring is enabled or disabled.
Client	Indicates the number of client associated with the IAP.
Type	Displays the IAP model.

Column	Description
Mesh Role	Indicates if the IAP is functioning as Mesh Point or mesh Portal.
2.4 Channel	Indicates the channels used by the IAP in the 2.4 GHz band.
2.4 Power (dB)	Indicates the transmission power allocated for 2.4 Ghz band channels.
2.4 Utilization	Indicates the percentage of utilization of 2.4 GHz channels.
2.4 Noise Floor	Indicates the noise floor of the 2.4 GHz channels.
5.0 Channel	Indicates the channels used by the IAP in the 5 GHz band.
5.0 Power (dB)	Indicates the transmission power allocated for 5 GHz band channels.
5.0 Utilization	Indicates the percentage of utilization of 5 GHz channels.
5.0 Noise Floor	Indicates the 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.

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 IAP.
IP address	Displays the IP address of the IAP.
2.4 Reqs 5.0 Reqs	Displays the counters that indicate channel scanning requirements.
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 video traffic.

The following output is displayed for the **show aps scanning** 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 IAP with which the current IAP is synchronized.
IP address	Displays the IP address of the IAP.
Class	Indicates if the IAP is serving as master or slave.
Current Version	Displays the Instant version currently running on the IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap allowed-channels

show ap allowed-channels <country-code>

## Description

This command displays a list of allowed channels for an IAP.

## Syntax

Parameter	Description
<country-code>	Specify a country code to display allowed channels for that country.

## Usage Guidelines

Specify the country code for your 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:

```
Allowed Channels for 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
```

The output of this command includes the following information:

Parameter	Description
PHY Type	Indicates the PHY types for the following bands: types: <ul style="list-style-type: none"><li>802.11a</li><li>802.11g</li></ul>
Allowed Channels	Displays the list of allowed channels for a specific regulatory domain.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap allowed-max-EIRP

show ap allowed-max-EIRP [<country>]

### Description

This command displays the maximum EIRP settings for the country in which the IAP is currently operational. You can also view the maximum EIRP settings for a specific country.

### Syntax

Parameter	Description
[<country>]	Displays the EIRP settings allowed for a specific country.

### Usage Guidelines

Use this command to view the maximum EIRP settings for a IAP. You can also filter the output to view the EIRP settings for a specific country.

### Example

The following example shows the output of the **show ap allowed-max-EIRP <country>** 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
136 140 149 153
-----
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
22 22 23 23
HT 20 22 22 22 22 22 22 22 22 22 22 * * * 21 21 21 21
22 22 22 23
HT 40 19 19 20 21 22 23 22 22 22 21 21 * * * 20 20 20 20
22 22 22 22
23 23 23 23 22 22 22 22 * * *
22 20 17
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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, IAP neighbors, RF summary, and scanning details for the IAP.

### Syntax

Parameter	Description
bandwidth management	Displays ARM bandwidth details for an 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 an IAP
scan-times	Displays ARM channel scanning details for an IAP.

### Usage Guidelines

Use this command to view information about the Adaptive Radio Management (ARM) bandwidth configuration, historical statistics, IAP neighbors, RF summary, and scanning details on an 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 IAP.
Shaping table	Displays information on the ARM configuration details for the clients associated with the IAP.

Column	Description
Client	Displays the list of IAP clients connected through the Wi-Fi interface.
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 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 :wifil

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 thresh old 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 IAP before the ARM change.
New channel	Displays the channel number used by the IAP after the ARM change.
Old Power	Indicates power values configured on the IAP before the ARM change.
New Power	Indicates power values configured on the 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 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 IAP neighbors.
ssid	Indicates the ESSID of the IAP neighbors.
Channel	Indicates the channels assigned to the IAP neighbors
rssi	Indicates the Received signal strength indication (RSSI) values associated with the ARM channels to which IAP neighbors are connected.
tx power	Indicates the transmission power.
PL	Indicates power loss.
AP Flags	Indicates the status of IAP neighbors.
Last Update	Displays details of last updates if any.
Total updates	Displays a summary if updates.

## show ap arm rf-summary

The **show ap arm rf-summary** command shows the statistics for all channels monitored by an 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        93     3/2/0/0/94  0/0 (0)          97/40//0/0 (137)
40       0      0        0        93     9/2/0/0/92  0/0 (0)          120/82//0/0 (202)
44       0      0        0        93     2/1/0/1/99  0/0 (0)          161/88//0/0 (249)
48       0      0        0        93     9/2/0/0/93  0/0 (0)          157/59//0/0 (216)
52       0      0        0        93     0/0/0/0/93  0/0 (0)          15/52//0/0 (67)
56       0      0        0        93     5/0/0/0/95  0/0 (0)          0/18//0/0 (18)
```



```

60      0      0      0      93      0/0/0/0/94      0/0(0)      29/14//0/0(43)
64      0      0      0      93      6/0/0/0/94      0/0(0)      43/10//0/0(53)
149     0      0      0      93      3/2/0/0/99      0/0(0)      113/41//0/0(154)
153     0      0      2      93      23/23/0/1/100  0/0(0)      124/68//0/0(192)
157     0      0      0      93      2/1/0/1/94      0/0(0)      97/79//0/0(176)
161     0      0      5      93      3/2/0/0/99      9/0(9)      115/66//0/0(181)
165     0      0      0      94      10/10/0/0/100  0/0(0)      99/38//0/0(137)
1       0      0      12     78      60/50/3/0/79    8/0(8)      448/79//0/0(527)
6       0      0      0      78      12/11/0/0/81    0/0(0)      483/227//0/0(710)
11      0      0      8      78      71/54/3/16/86   0/0(0)      703/126//0/0(829)

```

Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality

HT Channel Summary

-----

channel\_pair Pairwise\_intf\_index

-----

149-153 346

36-40 339

157-161 357

44-48 465

Interface Name :wifi0

Current ARM Assignment :161-/27

Covered channels a/g :1/0

Free channels a/g :7/0

ARM Edge State :disable

Last check channel/pwr :2m:36s/4m:24s

Last change channel/pwr :8m:19s/1d:23h:47m:12s

Next Check channel/pwr :2m:36s/2m:15s

Assignment Mode :Single Band

Interface Name :wifil

Current ARM Assignment :1/24

Covered channels a/g :0/1

Free channels a/g :0/2

ARM Edge State :disable

Last check channel/pwr :5m:31s/3m:33s

Last change channel/pwr :15m:50s/1d:23h:47m:13s

Next Check channel/pwr :16s/2m:33s

Assignment Mode :Single Band

The output of this command includes the following information:

Column	Description
channel	Displays the list of channels enabled on an IAP.
retry	Indicates the number of retry attempts.
Phy-err	Indicates the PHY errors on the current channels of an IAP.
Mac-err	Indicates the MAC errors on the current channels of an 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 IAP uses this metric to measure RF coverage. The coverage index is calculated as x+y, where "x" is the IAP's weighted calculation of the Signal-to- Noise Ratio (SNR) on all valid APs on a specified 802.11 channel, and "y" is the weighted calculation of the IAPs SNR detected by

Column	Description
	the neighboring APs on that channel.
intf_idx(Total	Displays channel interference details. The IAP uses this metric to measure co-channel and adjacent channel interference. The Interference Index is calculated as $a/b/c/d$ , where: <ul style="list-style-type: none"> <li>• Metric value “a” is the channel interference the AP sees on its selected channel.</li> <li>• Metric value “b” is the interference the AP sees on the adjacent channel.</li> <li>• Metric value “c” is the channel interference the AP’s neighbors see on the selected channel.</li> <li>• Metric value “d” is the interference the AP’s neighbors see on the adjacent channel.</li> <li>• To calculate the total Interference Index for a channel add “a+b+c+d”.</li> </ul>
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 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 IAPs on the network edge will not function as Air Monitors.
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.

### show ap arm scan-times

The **show ap arm scan-times** command shows the AM channel scan times for an 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 IAP.
assign-time (ms)	Displays the time since IAP is assigned a channel.
scans-attempted	Indicates the number times an IAP has attempted to scan another channel.
scans-rejected	Displays the number of times an 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 an IAP.
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.

Column	Description
current-scan-channel	Indicates the current channel scanned.
last-dos-channel	Indicates the last channel on which Denial of Service (DOS) 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap association

```
show ap association
```

### Description

This command displays the association table for an AP group or for an individual IAP.

### Usage Guidelines

Use this command to view information about the clients associated with an 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 an IAP or the AP group.
bssid	Indicates Basic Service Set Identifier (BSSID) associated with the IAP. The Basic Service Set Identifier (BSSID) is usually the MAC address of the IAP.
mac	Indicates the MAC address of the IAP clients.
auth	Displays the status of client authentication. Indicates <b>y</b> if the IAP is configured for 802.11 authorization frame types. Otherwise, it displays an <b>n</b> .
assoc	Displays the status of user association. Indicates <b>y</b> if the IAP is configured for 802.11 association frame types. Otherwise, it displays an <b>n</b> .
aid	Indicates 802.11 association ID. A client receives a unique 802.11 association ID when it associates to an IAP.
l-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 IAP's Extended Service Set Identifier (ESSID).
vlan-id	Indicates the VLAN ID associated with the IAP.

Column	Description
tunnel-id	Indicates the identification number of the IAP tunnel.
assoc. time	Indicates the amount of time the client has been associated with the IAP, in the hours:minutes:seconds format.
num assoc	Indicates the number of clients associated with the IAP.
flags	Displays flags for this 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 IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap bss-table

show ap bss-table

### Description

This command displays an AP's Basic Service Set (BSS).

### Usage Guidelines

The output of the show ap bss-table command shows the Aruba AP BSS table for all APs. To filter this information and view BSS table data for an individual AP 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:

```
Aruba AP BSS Table

-----
bss          ess          port ip          phy  type  ch/EIRP/max-EIRP  cur-cl a
p name      in-t(s)  tot-t          --          --          --  ---  -----  ----- -
-----
d8:c7:c8:3d:42:12  example1  ?/?  10.17.88.188  a-HT  ap    149+/20/22.5      1      d8:c7:c
8:cb:d4:20  0      18h:13m:58s
d8:c7:c8:3d:42:13  example-local-nw  ?/?  10.17.88.188  a-HT  ap    149+/20/22.5      0
d8:c7:c8:cb:d4:20  0      18h:13m:58s
d8:c7:c8:cb:d4:21  __wired__eth1  ?/?  10.17.88.188  b      ap    0/0/0              0      d
8:c7:c8:cb:d4:20  0      18h:13m:59s
d8:c7:c8:3d:42:02  example1  ?/?  10.17.88.188  g-HT  ap    7/21.5/21.5       0      d8:c7:c
8:cb:d4:20  0      18h:13m:58s
d8:c7:c8:3d:42:03  example-local-nw  ?/?  10.17.88.188  g-HT  ap    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 AP Basic Service Set Identifier (BSSID). This is usually the MAC address of the AP.
ess	Displays the AP Extended Service Set Identifier (ESSID).
port	Displays port used by the IAP.
ip	Displays the IP address of an AP.
phy	Displays an AP radio type. Possible values are: <ul style="list-style-type: none"><li>• a-802.11a</li><li>• a-HT-802.11a high throughput</li><li>• g- 802.11g</li></ul>

Column	Description
	<ul style="list-style-type: none"> <li>g-HT-802.11g high throughput</li> </ul>
type	Shows whether the AP is working as an access point (AP) or air monitor (AM).
ch/EIRP/max-EIRP	Displays the radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.
cur	Displays the current number of clients on the AP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
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.

### Usage Guidelines

Use this command to view the history of clients match actions for the clients associated with an IAP.

### 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view the current clients match actions for the clients associated with an 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
<radio>	Allows you to filter the output based the ID number of the radio (for example, 0 or 1).

### Usage Guidelines

Use this command to view the list of clients for which client match actions are refused. When the client match feature is enabled on an IAP, the IAP measures the RF health of its associated clients. If spectrum load balancing is triggered and a client's Received Signal Strength Indication (RSSI) is or less than 20 dB, clients are moved from one AP to another for better performance and client experience.

### 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
<radio>	Allows you to filter the output based the ID number of the radio (for example, 0 or 1).

### Usage Guidelines

Use this command to view a probe report for the clients associated with an IAP.

### Example

The following example shows the output of the **show ap client-probe-report** command.

```
AP Client Probe Report for Wifi0
-----
MAC                RSSI  In Swarm  Received
-----
12:c6:00:04:00:00  45    No        36s
12:22:00:00:00:63  44    No        4s
12:3c:00:04:00:00  44    No        1s
02:88:00:00:00:02  44    No        1m:3s
12:ce:00:00:40:00  44    No        27s
12:4c:00:04:00:00  40    No        42s
02:10:00:00:00:06  34    No        40s
00:26:c6:bd:50:96  37    No        45s
08:ed:b9:e1:51:8b  47    No        1h:49m:18s
00:eb:2d:a5:a1:17  51    No        11h:59m:22s
00:19:77:71:41:20  28    No        2m:24s
12:13:00:00:11:10  38    No        59s
24:77:03:11:71:bc  19    No        2s
c4:85:08:dd:f1:58  46    No        55s
08:ed:b9:e1:52:19  56    No        9h:9m:30s
84:85:06:a0:62:86  16    No        5s
00:24:d7:ac:42:78  19    No        1m:38s
b4:b6:76:42:33:fd  32    No        46s
24:77:03:cf:f4:64  19    No        7h:15m:33s
1c:ab:a7:3f:d4:36  12    No        10m:28s
b4:b6:76:42:34:07  13    No        21s
e0:b9:ba:de:04:f1  11    No        12m:49s
b4:b6:76:42:54:28  50    No        44s
24:77:03:7a:85:24  11    No        8h:31m:1s
c4:85:08:de:45:0e  40    No        49s
c4:85:08:de:35:5a  32    No        58s
c4:85:08:de:45:22  33    No        58s
b4:b6:76:42:55:ea  40    No        59s
b4:b6:76:42:55:b8  49    No        27s
b4:b6:76:42:36:af  51    No        0s
b4:b6:76:42:36:e1  45    No        19s
b4:b6:76:42:36:b4  46    No        29s
3c:a9:f4:1d:b7:94  13    No        14m:0s
```

00:21:6a:ba:b7:ce	31	No	2s
04:0c:ce:e1:98:78	50	No	8h:3m:27s
00:1e:65:71:18:de	8	No	53m:14s
60:67:20:4d:e8:a8	13	No	2h:8m:22s
b4:b6:76:42:49:56	41	No	14s
b4:b6:76:42:49:1f	34	No	25s
c4:85:08:d4:79:48	33	No	29s
b4:b6:76:42:49:4c	48	No	31s
b4:b6:76:42:49:6a	42	No	33s
c8:f7:33:a3:69:2f	33	No	34s
c8:f7:33:a0:a9:6f	35	No	41s
b4:b6:76:42:49:47	37	No	41s
00:0b:6b:b1:79:f5	33	No	0s
58:94:6b:36:5a:58	41	No	9h:27m:23s
c8:f7:33:a4:9a:39	33	No	2m:29s
c8:f7:33:a4:5a:dd	46	No	3s
c8:f7:33:a4:5a:2e	42	No	2s
c8:f7:33:a4:5a:c9	40	No	12s
b4:b6:76:42:5a:9f	37	No	18s
7c:d1:c3:8a:6b:be	56	No	51m:33s
00:26:c6:52:6b:14	43	No	5h:23m:36s
58:94:6b:36:cb:e8	45	No	10h:3m:19s
c4:85:08:db:db:e8	40	No	20s
b4:b6:76:42:5b:3f	38	No	28s
b4:b6:76:42:5b:44	46	No	47s
ac:81:12:59:5c:12	54	No	3h:58m:3s
00:1e:e5:e4:ec:d0	35	No	1h:58m:59s
3c:a9:f4:1d:ac:a4	40	No	10h:27m:17s
00:03:7f:40:0c:13	19	No	30s
c0:cb:38:44:fd:1d	34	No	1h:40m:9s
00:19:7e:76:8d:84	13	No	8m:23s
00:19:77:79:ad:e0	52	No	43s
b4:b6:76:42:6d:05	40	No	7s
b4:b6:76:42:6d:0a	36	No	28s
84:85:06:b3:6d:28	16	No	1m:25s
b4:b6:76:41:fe:a6	45	No	7s
00:15:00:5c:de:00	14	No	53s
88:53:2e:2c:ee:6c	24	No	10s
10:40:f3:e4:5f:62	56	No	8h:50m:12s
00:19:7e:75:ff:35	26	No	26m:50s
00:26:c6:bd:4f:10	28	No	51s
Total 74 Stations			

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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 the AP neighborhood.

### Usage Guidelines

Use this command to view information about the clients associated with the neighboring IAPs.

### Example

The following example shows the output of **show ap client-view** command:

```
Client Match Neighbor Table
-----
MAC          Channel  RSSI  Clients  Threshold  Channel Util (%)  VC Key  Flags  Recei
ved
-----  -----  ----  -
d8:c7:c8:44:50:c0  6      13   1      -          -                -          8m:27
s
d8:c7:c8:44:50:d0  40     8    2      -          -                -          V      1s
d8:c7:c8:44:51:b0  44     40   10     -          -                -          VR     2m:49
s
d8:c7:c8:44:61:a0  1      36   3      -          -                -          VR     58s
d8:c7:c8:44:61:b0  48     24   3      -          -                -          V      1s
d8:c7:c8:44:51:a0  11     50   4      -          -                -          VR     1s
d8:c7:c8:44:62:a0  6      19   2      -          -                -          V      20s
6c:f3:7f:ef:12:c0  1      28   0      1          0                271d9383  VRIC   4s
6c:f3:7f:ef:12:d0  149E   72   0      1          0                271d9383  VRIC   13s
d8:c7:c8:44:62:b0  149    3    3      -          -                -          -      9m:8s
6c:f3:7f:ef:03:00  6      24   0      0          0                847face0  B      5m:7s
d8:c7:c8:44:63:90  153    9    2      -          -                -          V      19s
6c:f3:7f:ee:f7:80  3      76   0      1          0                271d9383  VRIC   6s
6c:f3:7f:ee:f7:90  52E    62   0      1          0                271d9383  VRIC   4s
d8:c7:c8:44:4a:30  161    7    2      -          -                -          S      12m:4
3s
d8:c7:c8:44:4b:80  6      10   3      -          -                -          VR     1m:24
s
d8:c7:c8:44:4b:90  48     17   2      -          -                -          VR     2m:34
s
6c:f3:7f:ee:dc:20  11     32   2      3          0                847face0  -      3m:6s
d8:c7:c8:44:4c:80  6      24   1      -          -                -          VR     2m:27
s
d8:c7:c8:44:4c:90  36     20   11     -          -                -          VR     2m:34
s
6c:f3:7f:e7:5d:40  1      59   1      3          0                847face0  -      14m:2
4s
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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug airwave

show ap debug airwave

## Description

This command displays the list of AirWave servers configured on an IAP.

## Usage Guidelines

Use this command to view the list of AirWave servers configured for an IAP.

## Example

The following example shows the output of **show ap airwave** command:

```
Airwave Server List
-----
Domain/IP Address  Type  Mode  Status
-----  ----  ----  -----
test.com           Primary -    Not connected
test1.com          Backup  -    Not connected
```

The output of this command includes the following information:

Column	Description
Domain/IP Address	Displays the IP address or domain name of the AirWave server.
Type	Displays the type of the AirWave server. For example, backup or primary server.
Mode	Indicates the mode of AirWave operation. <b>NOTE:</b> AirWave can be configured to operate in the Manage Read/Write or Monitor-only+ Firmware Upgrades modes.
Status	Indicates the AirWave login status.

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	The Domain name is added.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug airwave-config-received

```
show ap debug airwave-config-received
```

## Description

This command indicates if any configuration information is received by the IAP from the AirWave server.

## Usage Guidelines

Use this command to view if any configuration information is received from the AirWave server.

## Example

The following example shows the output of the **show ap debug airwave-config-received** command:

```
show ap debug airwave-config-received
No configuration received from AirWave yet
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 AirWave server and the IAP.

## Usage Guidelines

Use this command to view information about the data sent to the AirWave server.

## 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 AirWave server events.

## Usage Guidelines

Use this command to view the pending AirWave 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 AirWave sign on key used by the used by the administrator to manually authorize the first Virtual Controller for an organization.

## Usage Guidelines

Use this command to view the AirWave sign on key details for debugging purpose.

## 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap debug airwave-state

```
show ap debug airwave-state
```

### Description

This command displays the configuration details and status of AirWave events associated with an IAP.

### Usage Guidelines

Use this command to view the current state of AirWave events associated with the 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>Aruba</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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# show ap debug airwave-stats

show ap debug airwave-stats

## Description

This command displays the configuration statistics associated with an IAP managed or monitored by the AirWave server.

## Usage Guidelines

Use this command to view configuration details of an IAP managed or monitored by the AirWave 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

## Syntax

Parameter	Description
mac	MAC address in the trace buffer.

## Example

The following example shows the output of **show ap debug auth-trace-buf** 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
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug auth-trace-buf

show ap debug auth-trace-buf [<Mac>]

## Description

This command displays the trace buffer for authentication events associated with the IAP.

## Syntax

Parameter	Description
<Mac>	Displays the authentication trace information for a specific MAC address.

## Usage Guidelines

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.

## Example

The following example shows the output of **show ap debug auth-trace-buf** 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 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 an AP radio interface.

## Syntax

Parameter	Description
<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.

## Usage Guidelines

Use this command to view the status of client match configuration for a specific radio interface.

## 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap debug client-stats

```
show ap debug client-stats <mac>
```

### Description

This command displays detailed statistics about an IAP client.

### Syntax

Parameter	Description
<mac>	Displays data based on the client MAC address.

### Usage Guidelines

Use this command to view information about an IAP client.

### Example

The following command output displays statistics for packets received from and transmitted to the specified client:

```
Station Stats
-----
Parameter                Value
-----
-----
General Per-radio Statistics
-----
Transmit specific Statistics
Frames Rcvd For TX       22
Tx Frames Dropped        0
Frames Transmitted       22
Success With Retry       1
Tx Mgmt Frames           2
Tx Probe Responses       0
Tx Data Frames           20
Tx CTS Frames            0
Dropped After Retry      0
Dropped No Buffer         0
Missed ACKs              1
Long Preamble            22
Short Preamble           0
Tx EAPOL Frames          13
Tx 6 Mbps                15
Tx 48 Mbps               5
Tx 54 Mbps               2
Tx WMM [VO]              15
UAPSD OverflowDrop       0
-----
Receive specific Statistics
Last SNR                  31
Last SNR CTL0             28
Last SNR CTL1             25
Last SNR CTL2             22
Last ACK SNR              32
Last ACK SNR CTL0         30
Last ACK SNR CTL1         28
Last ACK SNR CTL2         21
Last ACK SNR EXT0         5
Last ACK SNR EXT1         4
Frames Received           2932
Rx Data Frames            2930
Null Data Frames          2879
```

```

Rx Mgmt Frames      1
PS Poll Frames     0
Rx 6 Mbps          14
Rx 12 Mbps         6
Rx 18 Mbps         5
Rx 24 Mbps         2
Rx 36 Mbps        13
Rx 48 Mbps       1162
Rx 54 Mbps       1730
Rx WMM [BE]       39

```

The output of this command includes the following information:

Parameter	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 clear-to-send (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 AP's buffer was full.
Missed ACKs	Shows the number of missed acknowledgements (ACKs)
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 Extensible Authentication Protocol over LAN (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 Wi-Fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. <b>Tx WMM [BE]</b> : Best Effort <b>Tx WMM [BK]</b> : Background <b>Tx WMM [VO]</b> : VoIP <b>Tx WMM [VI]</b> : Video
UAPSD OverflowDrop	Shows the number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
Last SNR	Indicates the last recorded signal-to-noise ratio.

Parameter	Description
Last SNR CTL0	Indicates the signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 MHz mode.
Last SNR CTL1	Indicates the signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL2	Indicates the signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 MHz mode.
Last ACK SNR	Indicates the signal-to-noise ratio for the last received ACK packet.
Last ACK SNR CTL0	Indicates the signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 MHz mode.
Last ACK SNR CTL1	Indicates the signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 MHz mode.
Last ACK SNR CTL2	Indicates the signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 MHz mode.
Last ACK SNR EXT0	Indicates the signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 MHz mode.
Last ACK SNR EXT1	Indicates the signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs 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 Wi-Fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not be displayed in the output of the command. <b>Tx WMM [BE]:</b> Best Effort <b>Tx WMM [BK]:</b> Background <b>Tx WMM [VO]:</b> VoIP <b>Tx WMM [VI]:</b> Video



## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view a list of IAP clients.

### 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:

Parameter	Description
MAC	Indicates the MAC address of the IAP.
ESSID	Indicates the Extended Service Set identifier (ESSID) used by the client. An ESSID is a user-defined name for a wireless network.
BSSID	Filters the IAP Config table by BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
Assoc_State	Shows whether or not the client is currently authorized and/or associated with the IAP.
HT_State	Shows the client's high-throughput (802.11n) transmission type: <ul style="list-style-type: none"><li>• none: AP is a legacy AP that does not support the 802.11n standard.</li><li>• 20Mhz: A high-throughput APs using a single 20 Mhz channel.</li><li>• 40Mhz: A high-throughput APs using two 20 Mhz channels.</li></ul>
AID	Indicates the 802.11 association ID. A client receives a unique 802.11 association ID when it associates to an IAP.

Parameter	Description
UAPSD	<p>Shows the following values for Unscheduled Automatic Power Save Delivery (UAPSD) in comma-separated format: VO, VI, BK, BE, Max SP, Q Len.</p> <ul style="list-style-type: none"> <li>• VO: If 1, UAPSD is enabled for the VoIP access category. If UAPSD is disabled for this access category, this value is 0.</li> <li>• VI: If 1, UAPSD is enabled for the Video access category. If UAPSD is disabled for this access category, this value is 0.</li> <li>• BK: If 1, UAPSD is enabled for the Background access category. If UAPSD is disabled for this access category, this value is 0.</li> <li>• BE: If 1, UAPSD is enabled for the Best Effort access category. If UAPSD is disabled for this access category, this value is 0.</li> <li>• 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.</li> <li>• Q Len: The number of frames currently queued for the client, from 0 to 16 frames.</li> </ul>
Tx_Pkts	Shows the number of packets transmitted by the client.
Rx_Pkts	Shows the number of packets received by the client.
PS_Qlen	Shows power save queue length, in bytes.
Tx_Retries	Shows the number of packets that the client had to resend due to an initial transmission failure.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP that crashed. The stored crash information is cleared from the flash after the IAP reboots.

## Syntax

No parameters

## Usage Guidelines

Use this command to view the IAP crash information for debugging purpose.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap debug dhcp-packets

```
show ap debug dhcp-packets
```

### Description

This command displays information about the DHCP packets sent or received by an IAP.

### Usage Guidelines

Use this command to view information about the DHCP packets trace information for an IAP.

### 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 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

### Usage Guidelines

Use this command to view information about the 802.11x authentication.

### 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 AP 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.

Parameter	Description
MkeyRot	Displays the multicast key rotation details.
802.1X counters	Displays the 802.1X authentication counters.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug driver-config

show ap debug driver-config

## Description

This command displays IAP driver configuration.

## Usage Guidelines

Use this command to review configuration changes made since the IAP driver was last reset.

## Example

The **show ap debug driver-config** command displays the BSSID, SSID, and radio configuration details associated with the 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

### Syntax

Parameter	Description
<mac>	Displays trace information for an 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 23:09:03 assoc-resp d8:c7:c8:c4:29:82 08:ed:b9:e1:51:87 d8:c7:c8:c4:29:82 15 Success  
May 9 22:02:40 auth      d8:c7:c8:c4:29:8b c4:85:08:de:06:d4 d8:c7:c8:c4:29:8b 15 Success  
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP clients.

### Usage Guidelines

Use this command to view information about the clients that are persistently connected to an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap debug radio-stats

```
show ap debug radio-stats [<radio-ID>]
```

### Description

This command displays the aggregate radio debug statistics of an IAP.

### Syntax

Parameter	Description
<radio-ID>	Allows you to specify the ID number of the radio (for example, 0 or 1) for which you want to view statistics.

### Usage Guidelines

Use this command to view the radio debug statistics for an IAP.

### 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap debug radius-statistics

show ap debug radius-statistics

### Description

This command displays the RADIUS statistics for the authentication servers configured on an IAP.

### Usage Guidelines

Use this command to view the authentication server details.

### Example

The output of this command displays general statistics of the authentication servers configured on an IAP.

```
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

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	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 IAP.

### Usage Guidelines

Use this command to view the shaping information for clients connected to an IAP.

### Example

The following output is displayed for the **show ap debug shaping-table** command:

```
Interface :wifil
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    0
```

The output of this command provides the following information:

Column	Description
in	Shows the number of packets received by the AP.
out	Shows the number of packets sent by the AP.
drop	Shows the number of packets dropped by the AP.
fail	Shows the number of packets failed.
Numcl	Shows the number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
TotCl	Shows the total number of clients associated with the AP
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.

Column	Description
last-t	Shows the number of tokens that were allocated to the station last time token allocation algorithm ran.
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug spanning-tree

show ap debug spanning-tree

## Description

This command displays the Spanning Tree Protocol (STP) information for an IAP.

## Usage Guidelines

Use this command to view STP details on an 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 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: can't get info No such device
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap debug stm-config

show ap debug stm-config

## Description

This command displays the IAP station management configuration information.

## Usage Guidelines

Use this command to view the details of station management configuration.

## 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

## Usage Guidelines

Use this command under the guidance of Aruba technical support to troubleshoot network issues. The output of this command displays the following types of information if any for the selected IAP:

• Bootstrap information	• Per-radio statistics	• Ethernet duplex/speed settings
• Descriptor Usage	• Encryption statistics	• Tunnel heartbeat stats
• Interface counters	• AP 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP configuration stored in flash memory.

### Syntax

No parameters

### Usage Guidelines

Use 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:

Parameter	Description
IP Address	Displays the IP address of the 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 IAP.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ap mesh counters

show ap mesh counter

### Description

This command displays the mesh counters for an IAP.

### Usage Guidelines

Use this command to view a list of mesh counters available for an IAP.

### Example

The following example shows the output of **show ap mesh counter** command.

Mesh Packet Counters

```
-----  
Interface  Echo Sent  Echo Recv  Probe Req  Probe Resp  Assoc Req  Assoc Resp
```

```
-----  
          Assoc Fail  Link up/down  Resel.  Switch  Other Mgmt
```

```
-----  
Parent    0          0          770      770(770 HT)  0          0
```

```
0          0          -          -          0
```

Received Packet Statistics: Total 7013859, Mgmt 7013859 (dropped non-mesh 0), Da

ta 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  Assoc Resp  Assoc Fail  Li
```

```
-----  
Parent    0          0          770      770(770 HT)  0          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 AP or a Child AP. 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show ap mesh link

show ap mesh link

### Description

This command shows the mesh link of the IAP.

### Example

The following example shows the output of **show ap mesh link** command:

```
(Instant Access Point)# show ap mesh link
Neighbor list
```

```
-----
MAC      Portal  Channel Age      Hops    Cost  Relation  Flags  RSSI
Rate Tx/Rx
-----
00:0b:86:e8:09:d1 00:1a:1e:88:01:f0 157 0 1 11.00 C 3h:15m:42s - 65
54/54
00:1a:1e:88:02:91 00:1a:1e:88:01:f0 157 0 1 4.00 C 3h:35m:30s HL 59
300/300
00:0b:86:9b:27:78 Yes 157 0 0 12.00 N 3h:22m:46s - 26 -
00:0b:86:e8:09:d0 00:1a:1e:88:01:f0 157 0 1 11.00 N 3h:15m:36s - 65 -
00:1a:1e:88:02:90 00:1a:1e:88:01:f0 157+ 0 1 2.00 N 3h:35m:6s HL 59 -
A-Req A-Resp A-Fail HT-Details Cluster ID
-----
1 1 0 Unsupported sw-ad-GB32
1 1 0 HT-40MHzsgi-2ss sw-ad-GB322
0 0 0 Unsupported mc1
0 0 0 Unsupported sw-ad-GB32
0 0 0 HT-40MHzsgi-2ss sw-ad-GB32
Total count: 5, Children: 2
```

The output of this command includes the following information:

Parameter	Description
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 AP names, if available. The AP 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 AP.
Age	Number of seconds elapsed since the AP 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 AP to the controller. 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 AP and the AP on the neighbor list

Parameter	Description
	<p>and the amount of time that relationship has existed.</p> <ul style="list-style-type: none"> <li>• P = Parent</li> <li>• C = Child</li> <li>• N = Neighbor</li> <li>• B = Blacklisted-neighbor</li> </ul>
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 Receive Signal Strength Indicator (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 AP or BSSID.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 an AP.

## Example

The following example shows the output of **show ap mesh neighbors** command:

```
Neighbor list
-----
MAC          Portal Channel Age Hops Cost Relation      Flags  RSSI  Rate Tx/Rx
A-Req  A-Resp  A-Fail  HT-Details          Cluster ID
---      -
-----
6c:f3:7f:a5:df:90  Yes    157    23    0    5.00  N 23s          HLK    33    -
0          0      0      HT-20MHzsgi-3ss    78042e34005c8b372de0472df0727ef
6c:f3:7f:a5:df:30  Yes    153    0     0    5.00  N 3d:18h:16m:4s HLK    13    -
0          0      0      HT-20MHzsgi-3ss    b8e356bcb60d4ce984d9a7077a43936
d8:c7:c8:3d:3b:10  Yes    161    15    0    5.00  N 15s          HLK    50    -
0          0      0      HT-20MHzsgi-3ss    78042e34005c8b372de0472df0727ef
Total count: 3, 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; L = Legacy allowed
K = Connected; U = Upgrading; G = Descendant-upgrading; Z = Config pending; Y = Assoc-resp/Aut
h 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:

Parameter	Description
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 AP names, if available. The AP 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 AP.
Age	Number of seconds elapsed since the AP 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 AP 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 AP and the AP on the neighbor list and the amount of time that relationship has existed.

Parameter	Description
	<ul style="list-style-type: none"> <li>• P = Parent</li> <li>• C = Child</li> <li>• N = Neighbor</li> <li>• B = Blacklisted-neighbor</li> </ul>
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 Receive Signal Strength Indicator (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 AP or BSSID.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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| containment-info | e
net-wired-mac <mac> | ids-state <type> | pot-ap-list | pot-sta-list | routers | scan-info | st
a-list | state <mac> | stats <mac> | status}
```

### Description

This command shows information for IAP Air Monitors.

### Syntax

Parameter	Description
active-laser-beams	Shows active laser beam generators. The output of this command shows a list of all APs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which AP is sending out deauthorization frames, although it does not specify which AP is being contained.
ap-list	Shows list of APs being monitored.
ap-wired-mac	Shows the MAC address of the wired IAP.
arp-cache	Shows ARP Cache of learned IP to MAC binding
containment-info	<p>Shows containment events and counters triggered by the wired containment and wireless containment features configured in the <a href="#">ids</a>. 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:</p> <ul style="list-style-type: none"><li>• Last Deauth Timer Tick</li><li>• Deauth frames to AP</li><li>• Deauth frames to Client</li><li>• Last Tarpit Timer Tick</li><li>• Tarpit Frames: Probe Response</li><li>• Tarpit Frames: Association Response</li><li>• Tarpit Frames: Authentication</li><li>• Tarpit Frames: Data from AP</li><li>• Tarpit Frames: Data from Client</li><li>• Last Enhanced Adhoc Containment Timer Tick</li><li>• Enhanced Adhoc Containment: Frames To Data Sender</li><li>• Enhanced Adhoc Containment: Frames To Data Receiver</li><li>• Enhanced Adhoc Containment: Response to Request</li></ul> <p>Enhanced Adhoc Containment: Replay Response Wired Containment Counters:</p> <ul style="list-style-type: none"><li>• Last Wired Containment Timer Tick</li><li>• Last Tagged Wired Containment Timer Tick</li><li>• Spoof frames sent</li><li>• Spoof frames sent on tagged VLAN</li></ul>
enet-wired-mac	Shows Wired MAC Addresses learned.
ids-state <type>	Shows IDS State.
pot-ap-list	<p>Display the Potential AP table. The Potential AP table shows the following data:</p> <ul style="list-style-type: none"><li>• bssid: the AP's Basic Service Set Identifier.</li><li>• channel: The AP's current radio channel</li><li>• phy type: The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b/g, 802.11b/g-HT-20.</li></ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>num-beacons: Number of beacons seen during a 10-second scan</li> <li>tot-beacons: Total number of beacons seen since the last reset.</li> <li>num-frames: Total number of frames seen since the last rest.</li> <li>mt: Monitor time; the number of timer ticks elapsed since the first AP is recognized.</li> <li>at: Active time, in timer ticks.</li> <li>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).</li> <li>rss: The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio.</li> </ul> <p>For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.</p>
pot-sta-list	<p>Shows the Potential client table. The Potential Client table shows the following values:</p> <ul style="list-style-type: none"> <li>last-bssid: the Last BSSID to which the client associated.</li> <li>from-bssid,</li> <li>to-bssid</li> <li>mt: Monitor time; the number of timer ticks elapsed since the first client is recognized.</li> <li>it: Client Idle time, expressed as a number of timer ticks.</li> </ul>
routers	Shows Router MAC Addresses learned. The output of this command includes the router's MAC address, IP address and uptime.
scan-info	Shows scanned information for the IAP.
sta-list	Shows the configuration and status of monitor information of the IAP.
state	Shows the AP monitoring state.
stats	Shows the AP monitoring statistics.
status	Shows the status of the AP 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      phy-type      dos      dt/mt      ut
/it   encr      nstas avg-rssi curr-rssi wmacs  ibss
-----
---
```

d8:c7:c8:3d:3a:93	rahul_wep	149	interfering	80211a-HT-40	disable	3904/36	97
/0	wep	0	20	0	no		
00:24:6c:80:7d:11	NTT-SPOT	1	interfering	80211b/g	disable	3897/3897	9/
8	wep	9	11	0	no		
6c:f3:7f:b6:74:22	syelburgi	1	interfering	80211b/g-HT-20	disable	3817/3817	0/
0	wpa2-psk-aes	42	41	0	no		
00:24:6c:80:7d:12	docomo	1	interfering	80211b/g	disable	3779/3779	1/
0	wep	8	7	0	no		
6c:f3:7f:b6:74:32	syelburgi	40	interfering	80211a-HT-40	disable	3729/612	34
/0	wpa2-psk-aes	59	59	0	no		
00:0b:86:51:02:28	kannan-01	44	interfering	80211a	disable	3613/1212	10
/0	wpa2-psk-aes	36	33	3	no		
00:0b:86:51:02:2b	kannan-03	44	interfering	80211a	disable	3555/1154	10
/0	wpa2-psk-aes	38	35	0	no		
00:0b:86:51:02:29	ssid-2	44	interfering	80211a	disable	3518/1117	10
/0	wpa2-psk-aes	37	33	0	no		
00:0b:86:51:02:2c	kannan-04	44	interfering	80211a	disable	3494/1093	10
/0	open	38	35	0	no		
00:0b:86:51:02:2a	kannan-02	44	interfering	80211a	disable	3459/1058	10
/0	open	38	34	0	no		
00:0b:86:51:02:2d	kannan-05	44	interfering	80211a	disable	3459/1058	10
/0	open	37	34	0	no		
00:0b:86:51:02:2e	kannan-06	44	interfering	80211a	disable	3459/1058	10
/0	open	37	33	0	no		
00:0b:86:51:02:2f	kannan-07	44	interfering	80211a	disable	3459/1058	10
/0	open	37	34	0	no		
00:0b:86:51:02:20	kannan-01	11	interfering	80211b/g	disable	3444/1160	23
/0	wpa2-psk-aes	0	24	0	no		
6c:f3:7f:56:81:00	7SPOT	1	interfering	80211b/g-HT-20	disable	3308/3308	72
/71	open	0	10	0	no		
00:0b:86:51:02:21	ssid-2	11	interfering	80211b/g	disable	3277/764	10
1/0	wpa2-psk-aes	0	28	0	no		
00:0b:86:51:02:22	kannan-02	11	interfering	80211b/g	disable	3271/958	58
/0	open	0	27	0	no		

### 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 vlandid 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 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 vlandid 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
```

### 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 Intrusion Detection System (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  num-frames  mt  it  at  ibss
 rssi
-----
-----
d8:c7:c8:3d:3b:13 161      80211a  0             9             0           3  352  1  disable
 26
d8:c7:c8:3d:3b:03 1         80211b  0             9             0           4  363  1  disable
 43
00:24:6c:81:64:a8 36        80211a  0             9             0           3  185  2  disable
 17
00:24:6c:81:64:a9 36        80211a  0             9             0           1  45   1  disable
 17
00:24:6c:80:7a:a2 6         80211b  0             0             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          to-bssid            mt   it   channel
rssi
---               -
-----
00:24:d7:40:bb:b0  00:1a:1e:17:dc:62  00:00:00:00:00:00  00:00:00:00:00:00  133  50   7
44
60:67:20:5f:e1:94  00:1a:1e:17:d4:a0  00:00:00:00:00:00  00:00:00:00:00:00  6    43   7
0
58:94:6b:a0:47:74  00:1a:1e:17:d4:a1  00:00:00:00:00:00  00:00:00:00:00:00  217  104  7
0
b0:ec:71:98:da:44  00:24:6c:80:55:b0  00:00:00:00:00:00  00:00:00:00:00:00  37   2    7
0
00:27:10:2a:c6:ac  00:1a:1e:17:d4:a1  00:00:00:00:00:00  00:00:00:00:00:00  72   50   7
30
b0:65:bd:dc:51:8a  00:24:6c:80:03:4e  00:00:00:00:00:00  00:00:00:00:00:00  217  10   149
11
74:e1:b6:15:1b:5f  d8:c7:c8:3d:42:13  00:00:00:00:00:00  00:00:00:00:00:00  164  19   149
10
60:67:20:5b:33:28  00:1a:1e:17:d4:a1  00:00:00:00:00:00  00:00:00:00:00:00  6    5    7
0
00:27:10:5c:23:78  00:24:6c:80:fd:72  00:00:00:00:00:00  00:00:00:00:00:00  56   53   7
27
00:24:d6:9d:7c:28  00:24:6c:80:a3:90  00:00:00:00:00:00  00:00:00:00:00:00  97   96   7
28
58:94:6b:b3:14:a8  00:24:6c:80:03:4e  00:00:00:00:00:00  00:1c:b0:eb:d7:00  154  1    7
14
24:77:03:d0:0a:d8  00:1a:1e:17:dc:62  00:00:00:00:00:00  00:00:00:00:00:00  19   14   7
16
24:77:03:7a:7f:40  6c:f3:7f:94:63:80  00:00:00:00:00:00  00:00:00:00:00:00  42   41   7
0
24:77:03:ce:a5:fc  00:24:6c:80:4f:80  00:00:00:00:00:00  00:00:00:00:00:00  143  16   7
0
00:23:14:9d:ba:f0  00:1a:1e:17:d4:a1  00:00:00:00:00:00  00:00:00:00:00:00  158  36   7
0
24:77:03:cf:09:2c  00:24:6c:80:4f:81  00:00:00:00:00:00  00:00:00:00:00:00  117  57   7
22
24:77:03:d1:05:b0  00:1a:1e:17:dc:62  00:00:00:00:00:00  00:00:00:00:00:00  169  33   7
37
24:77:03:7a:89:50  00:24:6c:80:a3:91  00:00:00:00:00:00  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** command.

```

DoS State
-----
tx  old-tx  rx  old-rx  last-dos-time  ap-ev-time  sta-ev-time  last-enhanced-cm-time  enhance
d-cm-ev-time
--  -----  --  -----  -----
0  0        0  0        0              0           0             0                       0

```

### show ap monitor stats

The following example shows the output of **show ap monitor stats** command.

```

(Instant Access Point)# 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  rx-retry-pkt  tx-frag-pkt  rx-frag-pkt  sho
rt-hdr-pkt  long-hdr-pkt
-----
2662202  830665629  31438  440132  0           0           0           0           266
2202      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  pkt-12m  byte-12m  pkt-18m  byte-18m  pkt-24m  byte-24
m  pkt-36m  byte-36m  pkt-48m  byte-48m  pkt-54m  byte-54m
-----
tx    0      0      0      0      0      0      0      0      0      0
    0      0      0      0      0      0
rx    0      0      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    110 638 638 638 638 638 638 649 649 638 638 429 649 638 528 649
Monitored Time:233496
Last Packet Time:233528
Uptime:233529
DoS State
-----
tx  old-tx  rx  old-rx  last-dos-time  ap-ev-time  sta-ev-time  last-enhanced-cm-time  enhance
d-cm-ev-time
--  ----  --  -----  -----  -----  -----  -----
0  0      0  0      0          0          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          status  pkts  macs  gw-macs
dot1q-pkts  vlans
---
-----
d8:c7:c8:cb:d4:20 10.17.88.188 10.17.88.129 00:0b:86:40:1c:a0 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  Max PPS  Cur
PPS  Max PPI  Cur PPI  Invalid OTA msg
-----
-----
d8:c7:c8:3d:42:10 (wifi0) 17332616    401055780  12288142   703              1445     216
20          3          0
d8:c7:c8:3d:42:00 (wifi1) 56090990    3565742575 50110266   13315            1024     275
20          1          0
Data Structures
-----
ap  sta  pap  psta  ch  msg-hash  ap-1
--  ---  ---  ----  --  -
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  Tag-Mcast-Addr  Tags-Sent  Rpt-Sta  Inc
l-Unassoc-Sta Sta-Sent  Cmpd-Msgs-Sent
-----
-----
MMS           N/A       N/A   30    disable  01:0c:cc:00:00:00  N/A          disable  N/A
              N/A       N/A
Aeroscout    N/A       N/A   N/A   disable  00:00:00:00:00:00  N/A          disable  N/A
              N/A       N/A
RTLS         N/A       N/A   30    disable  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 IAP.
- List of APs monitored by the IAP.
- ARP cache details for the IAP.

- List of clients monitored by the IAP.
- Containment details for the IAP.
- List of potential APs for the IAP.
- List of potential clients for the IAP.
- Information about the potential wireless devices.
- Scanned information for the IAP.
- Configuration and status of monitor information of the IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap pmkcache

show ap pmkcache

## Description

This command displays the pairwise master key (PMK) cache table for clients associated with the IAP.

## Usage Guidelines

Use this command to view PMK cache table contents for the clients associated with an 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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ap virtual-beacon-report

show ap virtual-beacon-report

## Description

This command displays a report with the MAC address details and RSSI information of an IAP.

## Usage Guidelines

Use this command to view virtual beacon table of an IAP. The virtual beacon table with the details of clients associated an 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  AP                               RSSI  R
received
-----  -----  -
-----  -
00:db:df:0a:57:4e  Adopted  1          1          Yes   00:24:6c:07:44:c8 (Local 0)  47    5
9s
Normal
No              6c:f3:7f:ef:12:c0          44    18s
No              6c:f3:7f:ee:f7:80          44    11s
No              6c:f3:7f:ee:f7:90          36    13s
No              6c:f3:7f:ef:12:d0          43    13s
a0:88:b4:41:64:18  Normal  1          0          No    00:24:6c:07:44:c8 (Local 0)  34    2
0s
Normal
No              6c:f3:7f:ef:12:c0          43    18s
No              6c:f3:7f:ee:f7:80          48    11s
No              6c:f3:7f:ee:f7:90          35    13s
Yes             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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show arm-channels

show arm-channels

### Description

This command displays the ARM channel details configured on an IAP.

### Usage Guidelines

Use this command to view the channel details configured on an 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:

Parameter	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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show arm config

show arm config

### Description

This command displays the ARM configuration details for an IAP.

### Usage Guidelines

Use this command to view the ARM configuration details for an 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
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:

Parameter	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.
SLB NB Matching Percent	Indicates the percentage for comparing client density of AP neighbors for spectrum load balancing.
SLB Calculating Interval	Indicates the frequency at which the client density on 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show arp

show arp

### Description

This command displays the Address Resolution Protocol (ARP) entries for the Virtual Controller.

### Usage Guidelines

Use this command to view the ARP messages sent or received by the Virtual Controller.

### 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:

Parameter	Description
IP address	Displays the IP address of the device.
HW Type	Displays the type of the device.
Flags	Displays any flags for this AP.
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP to protect the network against wired attacks such as ARP attacks or malformed DHCP packets.

### Syntax

Parameter	Description
config	Displays firewall configuration details to protect the network from wired attacks.
stats	Displays attack counters.

### Usage Guidelines

Use this command to view firewall configuration details or attack counters enabled on an IAP to protect the network from ARP attacks and malformed DHCP packets.

### 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show app-services

show app-services

### Description

This command displays the list of application services configured on an IAP.

### Usage Guidelines

Use this command to view the list of application services available on an 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:

Parameter	Description
Name	Indicates the list of application services available on an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show auth-survivability

```
show auth-survivability {cached-info |time-out}
```

### Description

This command displays the authentication survivability information for an IAP.

### Usage Guidelines

Use this command to view the information cached when the authentication survivability feature is enabled and the time-out value configured for the authentication survivability. The authentication survivability feature supports authorization survivability against remote link failure for Mobility Controllers when working with ClearPass Policy Manager (CPPM). When enabled, this feature allows Instant to authenticate the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily lost.

### Example

The following example shows the output of the **auth-survivability cached-info** command:

```
UserName                Remaining Cache-Time(minutes)
-----                -
admin1                  20
```

The following example shows the output of the **show auth-survivability time-out** command:

```
Auth Survivability time out :24
```

The output of these commands provide the following information:

Parameter	Description
UserName	Indicates the username for which the authentication survivability feature is enabled.
Remaining Cache-Time	Displays the remaining number of minutes for cache expiry.
Auth Survivability time out	Indicates the number of minutes after which the cached information for authentication survivability will expire.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

Parameter	Description
config	Displays the parameters and values configured for manual or dynamic blacklisting of clients.

### Usage Guidelines

Use this command to view information about the clients blacklisted by an IAP.

### 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 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:

Parameter	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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show calea config

```
show calea config
```

### Description

This command displays the details configured for CALEA server integration on a IAP.

### Usage Guidelines

Use this command to CALEA configuration details.

### Example

The following example shows the output of the **show calea config** command:

```
(Instant Access Point)# show calea config
calea-ip :10.0.0.5
encapsulation-type :gre
gre-type :25944
ip mtu : 150
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show calea statistics

```
show calea statistics
```

### Description

This command displays the tunnel encapsulation statistics for a IAP.

### Usage Guidelines

Use this command to view the GRE encapsulation statistics for the IAPs with CALEA server integration feature enabled.

### Example

The following example shows the output of the **show calea statistics** command:

```
(Instant Access Point)# show calea statistics

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

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show captive-portal

```
show captive-portal
```

### Description

This command shows the external and internal Captive portal parameters configured for a network profile.

### Usage Guidelines

Use 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:

Parameter	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	Displays the URL that the users are redirected to, after a

Parameter	Description
External Captive Portal Redirect URL	successful authentication.
Server	Displays the external Captive port server.
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

## Usage Guidelines

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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
show cellular config	Displays the cellular configuration details available for the IAP
show cellular status	Displays the status of the cellular configuration for the IAP

### Usage Guidelines

Use these commands to view the details of the cellular configuration and status.

### Example

The following output is displayed for **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  PAP
usb-user
usb-passwd
usb-dial
usb-modeswitch
modem-isp
modem-country
Supported Country list
-----
Country list
-----
France
NZ
Israel
HK
Sweden
Spain
China
UK
norway
Germany
Croatia
Aus
Saudi-Arabia
Japan
India
```

```

US
Canada
Supported ISP list
-----
ISP list
-----
Cincinnati Bell
Virgin
Telecom
Telenor
Vodafone/SmarTone
O2
SFR
Orange
3/HUTCH
Optus
SingTel
HKCSL/1010
Verizon
ICE
Reliance NetConnect+
Tata Indicom
Airtel-3G
Nokia CS-10
NTT
KDDI
Movistar
China Unicom
China Telecom
Vodafone
Netcom
T-Mobile
Telstra
Mobily
EMOBILE
Sprint
Cricket
Vodafone-3G
Airtel
ATT
Rogers
Bell
modem status summary:No USB modem attached

```

The output of this command includes the following parameters:

Parameters	Description
type	Displays the type of cellular configuration. For example, 3G or 4G modems.
value	Displays the values associated with the cellular configuration parameters.
Supported Country list	Lists the countries that support cellular deployment.
ISP List	Lists the service providers that support cellular connections.

The following output is displayed for **show cellular status** command:

```

cellular status
-----
card          detect      link

```

----            -----        ----  
Not-present   Not-detect   Linkdown

The output of this command includes the following parameters:

Parameters	Description
Card	Indicates if the cellular cards are currently configured on the IAP.
detect	Indicates if cellular modems are detected on the IAP
Link	Indicates the current status of cellular link.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view information about the certificates uploaded to an IAP.

### Example

The following example shows the output of **show cert** 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=1LUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com, O
U=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated - Quick
SSL(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=1LUge2fRPkWcJe7boLSVdsKOFK8wv3MF, C=US, O=securelogin.arubanetworks.com, O
U=GT28470348, OU=See www.geotrust.com/resources/cps (c)11, OU=Domain Control Validated - Quick
SSL(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 IAP.

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show clients

```
show clients [<diff>| accounting <mac>| checksum <mac>| debug| roaming| status <mac>| wired [d  
ebug]]
```

### Description

This command displays details about the IAP clients.

### Syntax

Parameter	Description
<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 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.

### Usage Guidelines

Use this command to view information about the IAP clients. The 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.

### 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   Network      Access Point      Channel
----   -
      10.17.88.226  08:ed:b9:e1:51:7d   Network1      d8:c7:c8:cb:d4:20  44+

Type   Role           Signal           Speed (mbps)
----   -
AN    admin1        51 (good)       300 (good)

Info timestamp      :233732
```

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:







## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command was modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 daylight saving time configured on an IAP.

### Syntax

Parameter	Description
summer-time	Displays the summer (daylight saving) time settings.
timezone all	Displays the configured timezone for the IAP.

### Usage Guidelines

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 Greenwich Mean Time.

### 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 nov
ember 02:00
Baja-California                       UTC-08    MDT       first sunday april 02:00 last sunday octob
er 02:00
Pacific-Time                           UTC-08    PDT       second sunday march 02:00 first sunday nov
ember 02:00
Arizona                                UTC-07
Chihuahua                              UTC-07    MDT       first sunday april 02:00 last sunday octob
er 02:00
La-Paz                                 UTC-07    MDT       first sunday april 02:00 last sunday octob
er 02:00
Mazatlan                               UTC-07    MDT       first sunday april 02:00 last sunday octob
er 02:00
Mountain-Time                          UTC-07    MDT       second sunday march 02:00 first sunday nov
ember 02:00
Central-America                       UTC-06
Central-Time                           UTC-06    CDT       second sunday march 02:00 first sunday nov
ember 02:00
Guadalajara                           UTC-06    CDT       first sunday april 02:00 last sunday octob
er 02:00
Mexico-City                            UTC-06    CDT       first sunday april 02:00 last sunday octob
er 02:00
Monterrey                              UTC-06    CDT       first sunday april 02:00 last sunday octob
er 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 nov
ember 02:00
Indiana (East)       UTC-05   EDT   second sunday march 02:00 first sunday nov
ember 02:00

```

The output of this command includes the following information:

Parameter	Description
Country	Displays the country name.
Timezone	Displays the name of the timezone.
DST Name	Displays the name of the Daylight Saving Time.
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 H
our
-----
-----
PST      recurring  2 Sun      Mar          2:00       first    Sun      Nov      3:00
-8

```

The output of this command includes the following information:

Parameter	Description
DST Name	Name of the Daylight Saving Time.
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.

## Related Commands

Command	Description	Mode
<code>clock timezone</code>	Configures timezones for the IAP.	Config mode
<code>clock summer-time</code>	Configures the summer-time for the daylight savings time settings.	Config mode

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show configuration

show configuration

### Description

This command displays the configuration saved on the IAP.

### Usage Guidelines

Use this command to view the entire configuration saved on the 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-password
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 127
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
ssid profile-1
wpa-passphrase c52acfeb3e59ef254a6d14fe2ad565382e46f7eecd33af3
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
ssid 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show country-codes

show country-codes

### Description

This command shows the country code for the IAP. The country code specifies allowed channels for that country.

### Usage Guidelines

Use this command to view a list of IAP country codes.

### Example

The following example shows the output of **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
PR:Puerto Rico
```

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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show cpu

show cpu [details]

### Description

This command displays the CPU details.

### Syntax

Parameter	Description
[details]	Include this optional parameter at the request of Aruba technical support to display additional CPU troubleshooting statistics.

### Usage Guidelines

Use this command to view CPU load for application and system processes.

### 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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|  
dmo session| dmo station <mac>| dns-id-map| mcast|nat-pool <id>|route|session|statistics|user|  
vlan}
```

### Description

This command displays the system statistics for an IAP.

### Syntax

Parameter	Description
acl <id>	Displays datapath statistics associated with a specified ACL.
acl-all	Displays datapath statistics associated with all ACLs.
acl-allocation	Displays datapath statistics associated with allocated ACLs
acl-rule <rule>	Displays ACL rule to be applied.
acl-rule-detail <acl>	Displays the rule details of a specified ACL.
bridge	Displays bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination and flag information for an AP.
dmo session	Displays details of a DMO sessions.
dmo station <mac>	Displays Mac address of a DMO station.
dns-id-map	Displays mapping details for the DNS ID.
mcast	Displays the mobility multicast-group table that is used to flood the multicast RA traffic to the roamed clients.
nat-pool <id>	Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, S1P start, S1P end and DIP.
route	Displays datapath route table statistics.
session	Displays datapath session statistics.
statistics	Displays all the IP flows of a wireless device or Aruba AP. Statistics include table entries including source IP, destination IP, protocol, SPort, DPort, Cntr, priority, ToS, age, destination, TAge and flags.
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 that carry L2 traffic.

### Usage Guidelines

Use the show **datapath** command to display various datapath statistics for debugging purposes.

## Example

The following example shows the output of the **show datapath acl id** command:

```
Datapath ACL 130 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, C - Classify Media
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6
-----
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
```

The following example shows the 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                                  14
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                             4884
DHCP frames on DHCP local VLAN                          776
PPPOE frames to session processing                     0
Frames needing bridging                                 4890
Mesh frames forwarded                                   0
Thin AP frames forwarded                                 0
Frames to session processing                             4892
Frames to SP                                             87
Frames bridged by SP                                     6
```

Frames routed by SP	0
Frames for SP session processing	45
Frames for FP application processing	36

The output of this command includes the following parameters:

Parameter	Description
Counter	Shows counter statistics of the controller.
Value	Values output from this command represent the water-marks since the last boot of the controller.

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

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

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

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.

### Usage Guidelines

Use this command to view DHCP address allocation for network address translated clients to allow mobility of the clients across IAPs.

### Example

The following example shows the output of **show dhcp-allocation** command:

```
(Instant Access Point)# 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show dhcp config

show dhcp config

### Description

This command provides information about the DHCP scopes configured for an IAP.

### Usage Guidelines

Use this command to view configuration details associated with the DHCP scopes enabled on an IAP.

### Example

The following example shows the output of the **show dhcp config** command:

```
Distributed DHCP Scopes
-----
Name          Type          VLAN  Netmask      Default Router  DNS Server  Domain Name
-----
dhcp-11      Distributed,L2  11    11.11.11.0   255.255.255.0  0.0.0.0

Lease Time   IP Address Range  Client Count  DHCP Option  Reserve First  Reserve Last
-----
          43200                5              None

Branch ID   Branch Netmask  Branch Router
-----

Other DHCP Scopes
-----
Name      Type  VLAN  Network      Netmask      Exclude Address  Default Router
-----
dhcp-12   Local  12    12.12.12.0   255.255.255.0  0.0.0.0          0.0.0.0

DNS Server  Domain Name  Lease Time  DHCP Relay  DHCP Relay Servers
-----
0.0.0.0    0.0.0.0     43200      OFF         0.0.0.0

DHCP Option82  DHCP Option
-----
                None
```

The output of this command displays the following information:

Parameter	Description
Name	Displays the name of the DHCP scope.
type	Displays the DHCP assignment modes. The current release of Instant supports the following DHCP assignment modes. <ul style="list-style-type: none"><li>• <b>Distributed, L2</b></li><li>• <b>Distributed, L3</b></li><li>• <b>Local</b></li><li>• <b>Local, L3</b></li><li>• <b>Centralized, L2</b></li></ul>
VLAN	Indicates the VLAN ID assigned to DHCP scope.

Parameter	Description
Netmask	Displays the subnet mask.
Default Router	Displays the IP address of the default router.
DNS Server	Displays the DNS server IP address.
Domain Name	Displays the domain name configured for the DHCP scope.
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 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.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
type	Displays the branch details for the distributed DHCPs based on the type of the DHCP scope specified. The current release of Instant supports the following distributed DHCP assignment modes. <ul style="list-style-type: none"><li>• <b>Distributed, L2</b></li><li>• <b>Distributed, L3</b></li></ul>
<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.

### Usage Guidelines

Use this command to view branch details for the distributed DHCP scopes.

### 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:

Parameter	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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

## Usage Guidelines

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 open DNS server.

## Example

The following example shows the output of the **show domain-names** command:

```
example1.com  
example.com
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show election

```
show election {statistics}
```

### Description

This command shows master controller election statistics.

### Syntax

Parameter	Description
statistics	Shows master election statistics.

### Usage Guidelines

Use this command to view the statistics of the IAP selected as Virtual Controller.

### Example

The following example shows the output of **show election statistics** command:

```
State           : Master
master_beacon   : sent=8162 rcvd=0
hierarchy_beacon: sent=7685 rcvd=0
hierarchy_ack   : sent=0 rcvd=0
beacon_req      : sent=0 rcvd=0
Slave->Pot-Master : 0 time
Pot-master->Master: 0 time
Pot-master->Slave : 0 time
spoof arp rcvd: 0
last spoof mac: 00:00:00:00:00:00
```

The output of this command includes the following information:

Parameter	Description
State	Displays the controller state.
master_beacon	Displays the number of beacons transmitted and received by the master controller.
hierarchy_beacon	Displays the number of beacons transmitted and received.
hierarchy_ack	Displays the number of beacons transmitted and received.
beacon_req	Displays the number of beacons required.
spoof arp rcvd	Displays the number of ARP spoof attacks detected.
last spoof mac	Displays the MAC address of the last spoof detected.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.



## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show external-captive-portal

show external-captive-portal [<name>]

### Description

This command displays the external Captive portal configuration details.

### Syntax

Parameter	Description
name	Filters the output based on an existing external Captive portal profile.

### Usage Guidelines

Use this command to view information about the external Captive portal server configuration details.

### 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  Disable Auto
----      -
default  localhost  80    /    Authenticated  /             Disable              Enable

Whitelist  Use HTTPs  In Use  Redirect Mode
-----
                No      Yes      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

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
history	Displays the list of faults that were cleared.

### Usage Guidelines

Use this command to view the active faults for an IAP. Active faults are generated due to system faults.

### 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ids

```
show ids {ap <mac>| aps| client <mac>|clients| phy-types| rap-types}
```

### Description

This command displays the list of unknown APs and clients detected by the IAP with the IDS feature enabled.

### Syntax

Parameter	Description
ap <mac>	Displays the signal details for the IAP.
aps	Displays the unknown Access Points detected by the IAP.
client <mac>	Displays the details of the IAP to which the client is connected.
clients	Displays the list of unknown clients detected by the IAP.
phy-types	Displays the PHY details of the IAP.
rap-types	Displays the list of Remote APs (RAPs) detected by the IAP.

### Usage Guidelines

Use this command to view the intrusion detection details.

### 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 IAPs, the network to which the unknown 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view a list of intrusion detection policies enabled for an 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-death-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-tdkip-replay-attack              disable disable disable enable
signature-airjack                       disable disable disable enable
```

signature-asleep

disable disable disable enable

The output for this command provides the following information:

Parameter	Description
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view the status of infrastructure protection policies on an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show image

show image version

### Description

This command displays the Instant software version running on an IAP.

### Example

The following example shows the output of **show image version** command:

```
Primary Partition Build Time      :2013-03-31 11:47:06 PDT
Primary Partition Build Version  :6.2.1.0-3.3.0.0_37845
AP Images Classes
-----
Class
-----
Cassiopeia
```

Parameter	Description
Primary Partition Build Time	Shows the IAP image build time.
Primary Partition Build Version	Shows the IAP build version.
AP Image Class	Indicates the IAP class. The following examples describe the image class for different IAP models: <ul style="list-style-type: none"><li>• For IAP-135/134 –Instant_Cassiopeia_&lt;build-version&gt;</li><li>• For RAP-108/109 –Instant_Pegasus_&lt;build-version&gt;</li><li>• For RAP-155/155P–Instant_Aries_&lt;build-version&gt;</li><li>• For all other IAPs –Instant_Orion_&lt;build-version&gt;</li></ul>

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

### Usage Guidelines

Use this command to view table of L2 interface counters.

### 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.

Parameter	Description
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

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

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.

## Usage Guidelines

Use this command to the DHCP server settings. The DHCP server is a built-in server, used for networks in which clients are assigned IP address 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 Lease Time(m)  :20
DHCP Domain Name    :example.com
DHCP DNS Server      :192.0.2.1
```

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.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 Internet Group Management Protocol (IGMP) group table.

## Syntax

Parameter	Description
maddr <multicast-addr>	Filters group table information based on the multicast IP address.

## Usage Guidelines

Use this command to view the IGMP group table information for an IAP.

## 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

Parameter	Description
	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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# show ip interface brief

show ip interface brief

## Description

This command displays a summary of IP related information for all interfaces configured on an IAP.

## Usage Guidelines

Use this command to view a brief summary of IP related information for the 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 this 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. <ul style="list-style-type: none"><li>• Enabled–up</li><li>• Disabled–down</li></ul>
Protocol	Displays the status of the IP on the interface. <ul style="list-style-type: none"><li>• Enabled–up</li><li>• Disabled–down</li></ul>

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show ip route

show ip route

## Description

This command displays the IAP routing table.

## Usage Guidelines

Use this command to view the IP routes configured for an IAP.

## 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 (U), targeted to the host (UH), or if it uses Gateway (UG).
MSS	Indicates the default maximum segment size for TCP connections over this route.
Window	Indicates the default window size for TCP connections over this route.
irtt	Indicates the initial RTT (Round Trip Time). 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show lacp status

show lacp status

### Description

This command displays the Link Aggregation Control Protocol (LACP) configuration status on an IAP.

### Usage Guidelines

Use this command to view the LACP status on IAP-220 Series devices. LACP provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group. The LACP feature is automatically enabled during IAP boots and it dynamically detects the AP if connected to a partner system with LACP capability, by checking if there is any LACP Protocol Data Unit (PDU) received on either eth0 or eth1 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, AP partner MAC address, and the interface status.

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l2tpv3 config

```
show l2tpv3 config
```

### Description

This command displays the L2TPV3 session and tunnel configuration details.

### Usage Guidelines

Use this command to view the tunnel and session configuration details.

### Example

The following example shows the output of the **show l2tpv3 config** command:

```
(Instant Access Point)# show l2tpv3 config
L2TPV3 Tunnel configuration
-----
Tunnel Profile  Primary Peer  Backup Peer  Peer UDP Port  Local UDP Port  Hello Interval  Ho
st Name          MTU    Message Digest Type  secret Key                    Failover Mode  F
ailover Retry Count  Retry Interval  Checksum
-----
-----
test_tunnel     10.0.0.63      10.0.0.65      3000           1701            150            In
stant-C4:42:98  1570          MD5             625beed39fa4ff3424edb3082ede48fa  non-preemptive
5              80            Disabled
L2TPV3 Session configuration
-----
Session Name  Tunnel Name  Local tunnel IP  Tunnel Mask  Tunnel Vlan  Session Cookie Length
Session Cookie  Session Remote End ID
-----
-----
test_session  0           1.1.1.1         255.255.255.0  5            0
```

The output of this command includes the following information:

Parameter	Description
Tunnel Profile	Displays the tunnel profile name.
Primary Peer	Displays the IP address of the remote end tunnel.
Backup Peer	Displays the IP address of the remote end backup tunnel.
Peer UDP Port	Displays the UDP port number of the remote end backup tunnel.
Local UDP Port	Displays the UDP port number of the remote end tunnel.
Hello Interval	Displays the interval (in seconds) at which hello packets are routed in the tunnel.
Host Name	Displays the name of the IAP.
MTU	Displays the value for the tunnel MTU.
Message Digest Type	Displays the message digest to be used to create the MD AVP.

Parameter	Description
secret Key	Displays the shared key used for message digest.
Failover Mode	Displays the backup/primary tunnel failover mode.
Failover Retry Count	Displays the number of failover attempts.
Retry Interval	Displays the interval between each failover.
Checksum	Displays the end-to-end checksum of packets that pass through the tunnel.
Session Name	Displays the session profile name.
Tunnel Name	Displays the tunnel profile name.
Local tunnel IP	Displays the IP address of the remote end tunnel.
Tunnel Mask	Displays the network mask of the tunnel.
Tunnel Vlan	Displays the VLAN number to be carried in this tunnel session.
Session Cookie Length	Displays the cookie length for the cookie.
Session Cookie	Displays the cookie value.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l2tpv3 global

show l2tpv3 global parameter

### Description

This command displays L2TPv3 global configuration details such as hostname.

### Usage Guidelines

Use this command to view the hostname configured.

### Example

The following example shows the output of the **show l2tpv3 global parameter** command:

```
L2TPV3 Global configuration
-----
Host Name
-----
Instant-C4:42:98
```

The output of this command includes the following information:

Parameter	Description
Host Name	Displays the IAP name.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l2tpv3 session

```
show l2tpv3 session status
```

### Description

This command displays the L2TP session connectivity status.

### Usage Guidelines

Use this command to view the session connectivity status.

### Example

The following example shows the output of the **show l2tpv3 session status** command:

```
Session 1821009927 on tunnel 858508253:-  
type: LAC Incoming Call, state: ESTABLISHED  
created at: Jul 2 04:58:45 2013  
administrative name: 'test_session' (primary)  
created by admin: YES, peer session id: 12382  
session profile name: test_session_primary  
data sequencing required: OFF  
use data sequence numbers: OFF  
Peer configuration data:-  
data sequencing required: OFF  
framing types:  
data rx packets: 16, rx bytes: 1560, rx errors: 0 rx cookie error 0  
data tx packets: 6, tx bytes: 588, tx errors: 0
```

The output of this command shows the session connectivity status, tunnel creation time, configuration data, data frame types and so on.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l2tpv3 tunnel

```
show l2tpv3 tunnel {config | status}
```

### Description

This command displays the L2TP tunnel status and configuration details.

### Usage Guidelines

Use this command to view the tunnel connectivity status and configuration details.

### Example

The following example shows the output of the **show l2tpv3 tunnel config** command:

```
Tunnel profile test_tunnel_primary
l2tp host name: arubal600pop658509.hsb-dev4.aus
local UDP port: 1701
peer IP address: 10.13.11.157
peer UDP port: 1701
hello timeout 60, retry timeout 1, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1460
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
```

```
Tunnel profile test_tunnel_backup
l2tp host name: arubal600pop658509.hsb-dev4.aus
local UDP port: 1701
peer IP address: 10.13.11.157
peer UDP port: 1701
hello timeout 60, retry timeout 1, idle timeout 0
rx window size 10, tx window size 10, max retries 5
use UDP checksums: OFF
do pmtu discovery: OFF, mtu: 1460
framing capability: SYNC ASYNC
bearer capability: DIGITAL ANALOG
use tiebreaker: OFF
peer profile: NOT SET
session profile: NOT SET
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
```

The output of this command shows the tunnel profile name, L2TP hostname, local UDP port number, hello packets interval, and so on.

The following example shows the output of the **show l2tpv3 tunnel status** command:

```
Tunnel 858508253, from 10.13.11.29 to 10.13.11.157:-
state: ESTABLISHED
created at: Jul 2 04:58:25 2013
administrative name: 'test_tunnel' (primary)
created by admin: YES, tunnel mode: LAC, persist: YES
local host name: Instant-C4:42:98
peer tunnel id: 1842732147, host name: arubal600pop636635.hsbtst2.aus
UDP ports: local 1701, peer 3000
session limit: 0, session count: 1
tunnel profile: test_tunnel_primary, peer profile: default
```



```

session profile: default
hello timeout: 150, retry timeout: 80, idle timeout: 0
rx window size: 10, tx window size: 10, max retries: 5
use udp checksums: OFF
do pmtu discovery: OFF, mtu: 1460
trace flags: PROTOCOL FSM API AVPDATA FUNC XPRT DATA SYSTEM CLI
peer vendor name: Katalix Systems Ltd. Linux-2.6.32-358.2.1.el6.x86_64 (x86_64)
peer protocol version: 1.0, firmware 0
peer rx window size: 10
Transport status:-
ns/nr: 98/97, peer 98/96
cwnd: 10, ssthresh: 10, congpkt_acc: 9
Transport statistics:-
out-of-sequence control/data discards: 0/0
ACKs tx/txfail/rx: 0/0/96
retransmits: 0, duplicate pkt discards: 0, data pkt discards: 0
hellos tx/txfail/rx: 94/0/95
control rx packets: 193, rx bytes: 8506
control tx packets: 195, tx bytes: 8625
data rx packets: 0, rx bytes: 0, rx errors: 0
data tx packets: 6, tx bytes: 588, tx errors: 0
establish retries: 0

```

The output of this command shows the tunnel profile name, tunnel creation date, hello packets sent or received, and so on.

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l2tpv3 system

show l2tpv3 system statistics

### Description

This command displays the L2TPV3 system statistics details.

### Usage Guidelines

Use this command to view the tunnel and session statistics.

### Example

The following example shows the output of the **show l2tpv3 system statistics** command:

```
(Instant Access Point)# sh l2tpv3 system statistics
L2TP counters:-
Total messages sent: 99, received: 194, retransmitted: 0
illegal: 0, unsupported: 0, ignored AVPs: 0, vendor AVPs: 0
Setup failures: tunnels: 0, sessions: 0
Resource failures: control frames: 0, peers: 0
tunnels: 0, sessions: 0
Limit exceeded errors: tunnels: 0, sessions: 0
Frame errors: short frames: 0, wrong version frames: 0
unexpected data frames: 0, bad frames: 0
Internal: authentication failures: 0, message encode failures: 0
no matching tunnel discards: 0, mismatched tunnel ids: 0
no matching session_discards: 0, mismatched session ids: 0
total control frame send failures: 0, event queue fulls: 0
Message counters:-
Message          RX Good          RX Bad          TX
ILLEGAL          0                0                0
SCCRQ            0                0                1
SCCRP            1                0                0
SCCCN            0                0                1
STOPCCN          0                0                0
RESERVED1        0                0                0
HELLO            95               0                95
OCRQ              0                0                0
OCRP              0                0                0
OCCN              0                0                0
ICRQ              0                0                1
ICRP              1                0                0
ICCN              0                0                1
RESERVED2        0                0                0
CDN               0                0                0
WEN               0                0                0
SLI               0                0                0
```

The output of this command shows the system statistics such as total number of messages sent or received, type of message, and so on.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show l3-mobility

```
show l3-mobility {config| datapath| events [<count> <mac>]| status}
```

### Description

This command displays details about the Layer-3 (L3) events, mobility configuration, and roaming status of the IAP clients.

### Syntax

Parameter	Description
config	Displays the L3 mobility configuration details for an IAP.
datapath	Displays the datapath statistics associated with L3 mobility.
events [<count> <mac>]	Displays L3 mobility events for all IAP clients or individual clients filtered based on MAC address.
status	Displays the L3 mobility status for an IAP.

### Usage Guidelines

Use this command to view the L3 mobility information for an 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.

Column	Description
Virtual Controller IP	Displays the Virtual Controller IP address. The Virtual Controller IP configuration for each IAP allows the clients to roam seamlessly among all the IAPs.
Subnet	Indicates the IP address for the mobility domain.
Netmask	Displays the subnet mask configuration details.
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 Contro
ller 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 AP 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: <ul style="list-style-type: none"> <li>• Tunnel - Indicates the tunnel interface.</li> <li>• Device - Displays the device ID.</li> <li>• Remote Protocol - Indicates the remote protocol used by the roaming clients.</li> <li>• Dest IP - Indicates the destination IP address to which the packets are routed.</li> <li>• Clients - Displays the list of clients</li> <li>• Idle Time - Displays the idle time</li> <li>• Rx Packets - Displays information about packets received.</li> <li>• Tx Packets - Displays information about packets transmitted.</li> <li>• Rx Mcasts - Displays information about multicast packets received.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• Tx Mcasts - Displays information about multicast packets transmitted.</li> <li>• ARP Proxy Pkts - Displays information packets resolved to destination IP address by the proxy Address Resolution Protocol (ARP)</li> <li>• Tx Jumbo MTU - Displays information about the Maximum Transmission Unit (MTU) in jumbo frames.</li> <li>• Rx HB</li> <li>• Tx HB</li> <li>• MTU Reqs - Indicates the number of MTU requests sent.</li> <li>• MTU Resps - Indicates the number of MTU responses received.</li> <li>• HB Mismatch</li> <li>• IP Mismatch - Indicates IP address mismatch if any</li> <li>• Type</li> <li>• Vlan Translations - Displays details about VLAN translation.</li> </ul>

### 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
-----
----                -
: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 -       12-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 AP.
Tunnel ID	Indicates the tunnel interface used for routing packets.

Parameter	Description
Old AP IP	Indicates the IP address of the IAP from which the client has roamed.
FAP IP	Indicates the IP address of the IAP in the foreign subnet.
HAP IP	Indicates the IP address of the 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 I3-mobility status

The following example shows the output of the **show I3-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 AP and Virtual AP 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 AP IP address, local tunnel ID, and remote tunnel ID.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show ldap-servers

```
show radius-servers
```

### Description

This command displays the Lightweight Directory Access Protocol (LDAP) servers configured for user authentication on the Virtual Controller.

### Usage Guidelines

Use this command to view the LDAP server configuration information available on an IAP.

### 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
-----
dc=example, dc=com (objectclass=*) sAMAccountName No
```

The output of this command provides the following information:

Command/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 distinguished name for the administrator.
Admin Password	Displays the password for LDAP administrator.
Base-DN	Displays a distinguished name 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 <b>sAMAccountName</b>
In Use	Indicates if the server is in use.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.



## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log ap-debug

show log ap-debug <count>

## Description

This command shows the IAP debug logs.

## Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines of the log.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log apifmgr

```
show log apifmgr <count>
```

### Description

This command shows the log information for IAP interface manager.

### Syntax

Parameter	Description
count	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log convert

show log convert

## Description

This command shows image conversion details for the IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log debug

show log debug{count}

## Description

This command shows the IAP full log.

## Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
<count>	Filters the log output based on the number specified.

### Usage Guidelines

Use this command to view the L3-mobility logs for an IAP.

### 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 vl
an 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 12-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 oldap
ip 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 o
ldapip 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 olda
pip 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 vl
an 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 12-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 AP.
tid	Indicates the tunnel interface used for routing packets.
Old AP IP	Indicates the IP address of the IAP from which the client has roamed.
FAP IP	Indicates the IP address of the IAP in the foreign subnet.
HAP IP	Indicates the IP address of the IAP in the home subnet, to which the client is currently connected.



Content	Description
VC IP	Indicates the IP address of the Virtual Controller.
Additional Info	Displays additional information if any.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log network

show log network <count>

## Description

This command shows network logs for the IAP.

## Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log pppd

show log pppd <count>

## Description

Shows the Point-to-Point Protocol daemon (PPPd) network connection details.

## Syntax

Parameter	Description
<count>	PPPd network count.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show log rapper

show log rapper

## Description

This command show details the VPN connection logs in detail.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log sapd

show log sapd <count>

### Description

This command shows the SAPd details.

### Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log security

```
show log security <count>
```

### Description

This command shows security logs of the IAP.

### Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log system

show log system <count>

### Description

This command shows system logs of IAP.

### Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# show log user

show log user [count]

## Description

This command shows the IAP user logs.

## Syntax

Parameter	Description
count	Starts displaying the log output from the specified number of lines from the end of the log.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log user-debug

```
show log user-debug [count]
```

### Description

This command shows the IAP user debug logs.

### Syntax

Parameter	Description
count	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Syntax

Parameter	Description
count	Starts displaying the log output from the specified number of lines from the end of the log.

## Usage Guidelines

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.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show log wireless

```
show log wireless [<count>]
```

### Description

This command shows wireless logs of the IAP.

### Syntax

Parameter	Description
<count>	Starts displaying the log output from the specified number of lines from the end of the log.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show memory

show memory

## Description

Displays the information about memory utilization for an IAP.

## Usage Guidelines

Use this command to view information about memory utilization on an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show mgmt-user

```
show mgmt-user
```

### Description

This command displays the credentials for the admin users for the IAP management interface.

### Usage Guidelines

Use this command to view the admin user credentials required for accessing the 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
RADIUS Servers
-----
Name   IP Address  Port  Key                                     Timeout      Retry Count  ---
-----  -
Server1 192.0.2.2  1616  23567aea01cb66d354d2b1f5d13df7f85d4a  d1d1f181fb4827      5

NAS IP Address  NAS Identifier  In Use  RFC3576
-----  -
                                     Yes

Management User Table
-----
Name   Password  Type
----  -
admin  admin     Admin
```

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.
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.
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 Network Access Server (NAS) if NAS is configured.

Column	Description
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 IAPs are configured to process RFC 3576-compliant Change of Authorization (CoA).
NAS IP address	Displays the IP address of the Network Access Server (NAS) if NAS is configured.
Name (Management User Table)	Indicates the username of the admin 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

Version	Description
Aruba Instant 6.3.1.1-4.0	The output of this command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show network

show network <name>

### Description

This command shows network configuration details for an IAP.

### Syntax

Parameter	Description
<name>	Displays the name of a network profile.

### Usage Guidelines

Use this command without the optional <name> parameter to view a complete configuration details of a network profile on the IAP. Include the <name> parameter to display settings for a single network SSID only.

### 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
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

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show.opendns

show.opendns [support]

## Description

This command displays the open DNS configuration details for an IAP.

## Syntax

Parameter	Description
support	Displays if the OpenDNS credentials if the OpenDNS service is configured on the IAP.

## Usage Guidelines

Use this command to view open DNS configuration details. The OpenDNS credentials are used by Instant to access OpenDNS to provide enterprise-level content filtering.

## Example

The following example shows the output of **show.opendns** command:

```
OpenDNS Account      :admin
OpenDNS Password     :admin123
OpenDNS Status       :Not connected
OpenDNS Error Message:N/A
```

The output of this command includes the following parameters:

Column	Description
OpenDNS Account	Indicates the username for the OpenDNS account.
OpenDNS Password	Indicates the username for the OpenDNS account.
OpenDNS Status	Indicates if the IAP is connected to the OpenDNS server.
OpenDNS Error Message	Displays OpenDNS error message.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show port status

```
show port status
```

### Description

Displays the activity statistics on each of the port on the controller.

### Example

The following example shows the output of **show port status** command:

```
(Instant Access Point)# show port status
Port    Type  Admin-State  Oper-State
----    -
bond0   GE    down         up
```

Parameter	Description
Port	Displays the port number on the controller.
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.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Privileged Exec mode.

## show pppoe

```
show pppoe {config|debug logs|debug status}
```

### Description

This command shows PPPoE debug logs and uplink status.

### Syntax

Parameter	Description
config	Displays PPPoE configuration details.
debug logs	Displays PPPoE debug logs.
debug status	Displays the uplink status.

### Example

#### show pppoe config

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
```

#### show pppoe debug logs

The following example shows the configuration of the PPPoE **show pppoe debug logs** command.

```
pppd log not available
```

#### show pppoe debug status

The following example shows the configuration of the PPPoE **show pppoe debug status** command.

```
pppoe uplink state           :Suppressed.
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command was modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show process

show process

### Description

This command displays a list of processes running on an IAP.

### Usage Guidelines

Use this command to view the processes running on the IAP for debugging purpose.

### 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 IAP.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Example

The following example shows the output of **show proxy config** command:

```
Proxy server    :192.0.2.1
Proxy port     :8080
Exceptions
-----
No Exception
--  -----
1  192.0.2.2
```

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.

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view the 2.4 GHz and 5 GHz radio configuration details for an IAP.

### Example

The following example shows the output of **show radio config** command:

```
(Instant Access Point)# 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
```

```
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
```

The output of this command provides the following information:

Parameter	Description
Legacy Mode	Indicates if the legacy mode is enabled on the IAPs to run the radio in the non-802.11n mode.
Beacon Interval	Displays beacon interval for the 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 IAP is allowed advertise its 802.11d (country information) and 802.11h (transmit power control) capabilities.
Interference Immunity Level	Displays the immunity level configured for an AP radio profile to improve performance in high-interference environments. For more information on configuring immunity levels, see <a href="#">rf dot11a-radio-profile</a> and <a href="#">rf dot11g-radio-profile</a> .
Channel Switch	Displays the number of channel switching announcements that are sent before

Parameter	Description
Announcement Count	switching to a new channel.
MAX distance	Indicates the maximum distance in meters between a client and an AP or between a mesh point and a mesh portal.
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 IAPs in access mode continue with normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs 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.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show radius-servers support

```
show radius-servers support
```

### Description

This command displays the RADIUS server configuration details for an IAP.

### Usage Guidelines

Use this command to view the RADIUS server information for an IAP.

### Example

The following example shows the output of **show radius-servers support** command:

```
RADIUS Servers
-----
Name                IP Address  Port  Acctport  Key
-----
Server1            192.0.2.2  1616  1813      23567aea01cb66d354d2b1f5d13df7f85d4a

Timeout            Retry Count  NAS IP Address  NAS Identifier  In Use  RFC3576
-----
d1d1f181fb4827    5
Airgroup RFC3576-ONLY  Airgroup RFC3576 port  Deadtime
-----
                    5
```

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 Network Access Server (NAS) if NAS is configured.
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 IAPs are configured to process RFC 3576-compliant Change of Authorization (CoA).
Airgroup RFC3576-ONLY	Indicates if IAPs are configured to be RFC 3576 compliant only.

Parameter	Description
Airgroup RFC3576 port	Indicates the port number used for sending AirGroup CoA.
Deadtime	Indicates the RADIUS server dead-time.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP, including the current changes that are yet to be saved.

### Usage Guidelines

Use this command to view the current configuration information stored in the IAP flash memory.

### Example

The following text provides an example for the **show running-config** command output:

```
version 6.2.0.0-3.3.0
virtual-controller-country IN
virtual-controller-key fc6520ad018ee6eb13bdc6b985e0fe6361bd37f7d25212a77e
name Instant-C4:42:98
terminal-access
clock timezone pst -08 00
rf-band 2.4
ams-ip 10.0.0.1
ams-backup-ip 10.0.0.5
ams-key e79afb5cd2ebe3731f879fa8827bc7cee3d06ea608a9bcd8
allow-new-aps
allowed-ap d8:c7:c8:c4:42:98
arm
wide-bands 5ghz
min-tx-power 18
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
client-aware
scanning
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
opendns admin 50bb1fc9e4ccc583762cf452dfb118d0779e5c63c66f35af
inactivity-ap-timeout 1000
mgmt-user admin 49fd2144445e9efe346da004d666bd59
wlan access-rule wired-instant
rule 10.17.88.59 255.255.255.255 match tcp 80 80 permit
rule 10.17.88.59 255.255.255.255 match tcp 4343 4343 permit
rule any any match udp 67 68 permit
rule any any match udp 53 53 permit
wlan access-rule test1
rule any any match any any any permit
wlan access-rule default_wired_port_profile
rule any any match any any any permit
wlan access-rule test
rule any any match any any any permit
wlan access-rule test123
rule any any match any any any permit
wlan access-rule port
rule any any match any any any deny
```

```

wlan ssid-profile test
enable
index 0
type employee
ssid test
opmode wpa2-aes
max-authentication-failures 0
auth-server test
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
wlan ssid-profile test123
enable
index 1
type employee
ssid test123
opmode wpa2-aes
max-authentication-failures 0
auth-server test
auth-server test123
set-role-machine-auth test1 test1
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 ldap-server test
ip 0.0.0.0
port 0
wlan auth-server test
ip 10.0.0.1
port 1812
acctport 1813
key 7164cb0c8736ab1ea7ed9541434bbbb
wlan auth-server test123
ip 10.0.0.0
port 1812
acctport 1813
key f9953c075a6c9615f4fda0a800ee60d9
wlan auth-server server1
ip 10.0.0.7
port 1812
acctport 1813
key 28ba549e9bbcd93e2152034af5d42360860d0f504893334a
rfc3576
cppm-rfc3576-only
cppm-rfc3576-port 5999
wlan external-captive-portal
server localhost
port 80
url "/"
auth-text "Authenticated"
wlan wispr-profile

```

```
wispr-location-name-operator-name XYZ
wispr-location-name-location airport
wispr-location-id-network southern
wispr-location-id-cc IN
wispr-location-id-ac 080
wispr-location-id-isocc 91
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
wired-port-profile port
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name port
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
wired-port-profile test
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name test
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x
enet0-port-profile default_wired_port_profile
enet1-port-profile wired-instant
enet2-port-profile wired-instant
enet3-port-profile wired-instant
```

```

enet4-port-profile wired-instant
wlan sta-profile
ssid test
cipher-suite wpa-tkip-psk
wpa-passphrase 69d4410b5bb95dfd6777317aac3dd6a567b794c3a355be92
uplink-band dot11a
uplink
no preemption
enforce ethernet
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180
pppoe-uplink-profile
pppoe-username user
pppoe-passwd b8086124859da5f9c9a25fd97caa47ef743a67481a684e10
pppoe-svcname ServiceA
pppoe-chapsecret 3195f877acb3937cc0e015ee73bd5ab1
l3-mobility
home-agent-load-balancing
virtual-controller 192.0.1.0
subnet 192.0.2.0 255.255.255.255 2 192.0.1.0
airgroup
enable
multi-swarm
enable-guest-multicast
cppm-server test
cppm-server test123
cppm-server server1
cppm enforce-registration
airgroupservice airplay
enable
description AirPlay
id _airplay._tcp
id _raop._tcp
airgroupservice airprint
enable
description AirPrint
id _ipp._tcp
id _pdl-datastream._tcp
id _printer._tcp
id _scanner._tcp
id _universal._sub._ipp._tcp
id _printer._sub._http._tcp
id _http._tcp
id _http-alt._tcp
id _ipp-tls._tcp
id _fax-ipp._tcp
id _riousbprint._tcp
id _cups._sub._ipp._tcp
id _cups._sub._fax-ipp._tcp
id _ica-networking._tcp
id _ptp._tcp
id _canon-bjnp1._tcp

```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.



## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show snmp-configuration

```
show snmp-configuration
```

### Description

This command displays the Simple Network Management Protocol (SNMP) configuration details for a Virtual Controller.

### Usage Guidelines

Use this command to view the SNMP information configured on a Virtual Controller.

### Example

The following example shows the output of **show snmp-configuration** command:

```
Engine ID:D8C7C8CBD420
Community Strings
-----
Name
----
SNMPv3 Users
-----
Name  Authentication Type  Encryption Type
-----
SNMP Trap Hosts
-----
IP Address  Version  Name  Port  Inform
-----
```

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, Advanced Encryption Standard (AES) or CBC-DES Symmetric Encryption Protocol (DES) 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

### Usage Guidelines

Use this command to view the 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Syntax

Parameter	Description
<count>	Filters the alerts based on the specified number.

## Usage Guidelines

Use this command to view the spectrum alerts for an 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 AP, and the timestamp. The Virtual Controller reports the detailed device information to AirWave Management server.

## 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 IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAPs, IAP clients, IAP cluster, and network profiles configured on an IAP.

### Syntax

Parameter	Description
ap <IP-address>	Displays information on IAP utilization, RF trends, and client details for a specific 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 IAP to which it is currently connected.
global	Displays global statistics for the IAP cluster, and the IAPs and clients connected to the IAP cluster.
network <network-name>	Displays aggregate information about a network profile configured on an IAP.
[count]	Allows you to filter the command output for the IAP, client, global, and network profile statistics based on the specified number.

### Usage Guidelines

Use this command to view the following information about IAPs, the clients connected to the IAPs, and the corresponding IAP cluster:

- Utilization trend – Displays information about the IAP utilization, the number of clients associated with an IAP, Virtual Controller, or the IAP network over the last 15 minutes.
- RF trends – Displays information the utilization, noise, or error threshold for an IAP. It also shows the current speed or signal strength for the clients in the network and the RF information for the IAPs to which the clients are connected.
- Mobility Trail – Shows duration of the client is association with an IAP and the name of the 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 [In
terfering] Neighboring APs [Rogue] Neighboring Clients [Valid] Neighboring Clients [Interfe
ring] 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] (f
ps)  2.4 GHz Frames [Out] (fps)  5.0 GHz Frames [Out] (fps)  2.4 GHz Frames [In] (fps)  5.0 GH
z 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 Mg
mt Frames [Out] (fps)
-----
-----
-----

```

```

-----
-----
-----
00:34:46  59          4          -91
-93          41          0          18          0
           0          68          403
           1          1          0
           265          1
00:34:17  61          5          -92          0
-93          45          0          21          0
           1          78          408
           1          1
           287          1

```

Client Heatmap

Clients Signal Speed IP Address

AP List

Name	IP Address	Mode	Spectrum	Clients	Type	CPU Utilization %:	Memory F
ree (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)  Throughp
ut [Out] (bps)  Frames [Retries In] (fps)  Frames [Retries Out] (fps)  Speed (mbps)

```

```

-----
-----
00:32:46  47      0      0      0      0      170
          0
00:32:16  47      0      0      0      6      170
          0
00:31:46  47      0      1      0      6      5946
          0
00:31:16  49      0      0      0      6      316
          0

```

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
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
-----
Attribute  Operation  Operand  Role Name  Index
-----  -
Vlan Derivation Rules
-----
Attribute  Operation  Operand  Vlan Id
-----  -
RADIUS Servers
-----
Name      IP Address  Port  Key      Timeout  Retry Count  NAS IP Address  NAS Identifier  RFC3
576
----      -
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show summary

```
show summary {<difference> | support}
```

### Description

This command shows the current configuration details.

### Syntax

Parameter	Description
<difference>	Shows the difference in configuration.
support	Shows the summary support containing the configuration details used by support.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command was modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show swarm

```
show swarm {state|mode}
```

### Description

This command displays the current status of the IAP cluster and indicates if IAPs are in a cluster or standalone mode.

### Usage Guidelines

Use this command to view the current status of the IAP cluster and to view information about the functioning mode of the IAP cluster.

### Example

The following example shows the output of **show swarm state** command:

```
AP Swarm State      :swarm_config_sync_complete
mesh ldart State    :suspending
```

The output of this command describes synchronization status of the IAP cluster.

The following text shows an example output for the **show swarm mode** command:

```
Swarm Mode          :Cluster
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

### Usage Guidelines

Use this command to view the list certificate formats supported by the IAP.

### Examples

```
Server Certificate Formats
-----
Name
----
PEM
CA Certificate Formats
-----
Name
----
PEM
DER
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	The output of this command is modified.
Aruba Instant 6.2.1.0-3.4	This command was modified.

### Command Information

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 IAP.

### Usage Guidelines

Use this command to view the Syslog logging facilities and the associated logging level.

### Example

The following example shows the 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 IAP.
ap-debug	Generates a log for the AP device for debugging purposes.
network	Generates a log when there is a change in the network, for example, when a new 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 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. <ul style="list-style-type: none"><li>● Emergency – Panic conditions that occur when the system becomes unusable.</li><li>● Alert – Any condition requiring immediate attention and correction.</li><li>● Critical – Any critical conditions, for example, hard drive error.</li><li>● Errors – Error conditions.</li><li>● Warning – Warning messages.</li><li>● Notice – Significant events of a non-critical and normal nature. The default value for all Syslog facilities.</li><li>● Informational – Messages of general interest to system users.</li><li>● Debug – Messages containing information useful for debugging.</li></ul>

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



# show tech-support

show tech-support

## Description

This command displays the complete IAP information and the associated configuration details, which can be used by the technical support representatives for debugging.

## Usage Guidelines

Use this command to view and analyze IAP configuration details for debugging any AP related issues.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

## Usage Guidelines

Use this command to view the uncommitted configuration details. Use the **commit apply** command to commit the configuration changes.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view the image upgrade details for an 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 IAP.
IP Address	Shows the IP address of the IAP.
AP Image Class	Indicates the IAP class. The following examples describe the image class for different IAP models: <ul style="list-style-type: none"><li>• For IAP -135/134 –Instant_Cassiopeia_&lt;build-version&gt;</li><li>• For RAP-108/109 and IAP-114/115– Instant_Pegasus_&lt;build-version&gt;</li><li>• For RAP-155/155P–Instant_Aries_&lt;build-version&gt;</li><li>• For IAP-224/225–Instant_Centaurus_&lt;build-version&gt;</li><li>• For all other IAPs –Instant_Orion_&lt;build-version&gt;</li></ul>
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 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
show uplink config	Displays the uplink interface configuration details for an IAP.
show uplink stats	Displays the aggregate uplink statistics for an IAP

### Usage Guidelines

Use this command to view the information about uplink status and configuration for an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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.

## Usage Guidelines

Use this command to view the uplink VLAN configuration details for management traffic. The uplink management VLAN configuration allows you to tag management traffic and connect multiple IAP clusters (Virtual Controllers) to the same port on an upstream switch (for example, AirWave 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show users

```
show user [portal| Radius]
```

### Description

This command displays users configured for an IAP.

### Syntax

Parameter	Description
portal	Displays the IAP user credentials.
radius	Displays the user credentials for the RADIUS server authentication

### Usage Guidelines

Use this command to view the IAP user credentials.

### 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 IAP, portal, and the RADIUS users.
Password	Indicates the password details of the users.
Attribute	Indicates the attributes

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP serving a specific regulatory domain.

## Usage Guidelines

Use this command to view the list of valid channels that can be configured on your IAP.

## 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 IAP in the 2.4 GHz band.
5.0 GHz	Displays the list of channels valid for an IAP in the 5.0 GHz band.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show version

show version

### Description

This command displays the Instant software version running on an IAP.

### Example

The following example shows the output of the **show version** command:

```
Aruba Operating System Software.  
ArubaOS (MODEL: 135), Version 6.3.1.1-4.0.0.0  
Website: http://www.arubanetworks.com  
Copyright (c) 2002-2013, Aruba Networks, Inc.  
Compiled on 2013-11-12 at 02:36:43 PST (build 40841) by p4build  
AP uptime is 12 minutes 2 seconds  
Reboot Time and Cause: AP rebooted Wed Nov 13 13:14:58 UTC 2013; User Reboot
```

The output of this command provides the following information:

Parameter	Description
Version	Indicates the version of IAP software.
Reboot Time and Cause	Indicates the reason for which the IAP was last rebooted and the reboot time.
Model	Indicates the IAP model.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## show vpn

```
show vpn {config|status}
```

### Description

This command displays the status and configuration details for VPN-enabled IAPs.

### Syntax

Parameter	Description
config	Displays configuration details for the VPN-enabled IAPs.
status	Displays the status of the VPN connections enabled on an IAP.

### 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                        c5b7860366aab19766b90f7df2b31b66
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 VPN configuration parameters and the values assigned to these parameters. 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 type](#)
- [gre primary](#)
- [gre per-ap-tunnel](#)

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/IPSec connections, and the tunnel details.

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	The command output is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	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 IAP.

## Usage Guidelines

Use this command to view the walled garden configuration details for an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## show wifi-uplink

```
show wifi-uplink {auth log |config | status}
```

### Description

This command displays the configuration details, the status, and authentication log for the Wi-Fi uplinks configured on an IAP.

### Syntax

Parameter	Description
auth log	Displays the authentication configuration details and an authentication log.
config	Displays the Wi-Fi configuration parameters enabled on an IAP.
status	Displays the status of the Wi-Fi uplink.

### Usage Guidelines

Use this command to view the information about status and configuration details for the Wi-Fi uplink enabled on an IAP.

### Example

#### show wifi-uplink auth log

The following output is displayed for the **show wifi-uplink auth log** command:

```
-----  
wifi uplink auth configuration:  
-----  
  
wifi uplink auth log:  
-----  
[1536]2013-05-08 23:42:06.647: Global control interface '/tmp/supp_gbl'
```

#### show wifi-uplink config

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:

```
configured      :YES
enabled         :YES
```

The output of this command indicates if the Wi-Fi uplink is configured and enabled on the IAP.

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Syntax

Parameter	Description
<profile-name>	Displays the current configuration details for a specific wired profile.

### Usage Guidelines

Use this command to view the details of a wired profile configured on an IAP.

### 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
-----
Attribute  Operation  Operand  Role Name  Index
-----
Vlan Derivation Rules
-----
Attribute  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  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
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP.

### Usage Guidelines

Use this command to view the wired profiles configured on an 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
-----  ---  ---  -----
auto    Yes  Yes   None
full    No   Yes   None

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 <b>Access</b> or <b>Trunk</b> .
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

Column	Description
	on the capabilities of the client, the AP, and the cable.
poe	Indicates if Power over Ethernet (PoE) is enabled.
In Use	Indicates if the wired profile is in use.
Authentication Method	Indicates the authentication method configured for the wired profile.
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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

# show wispr config

show wispr config

## Description

This command displays the Wireless Internet Service Provider roaming (WISPr) authentication parameters configured on an IAP.

## Usage Guidelines

Use this command to view the WISPr configuration details for an 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

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## snmp-server

```
snmp-server
  community <string> 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.

### Syntax

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	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 controller.	–	–
version	Configures the SNMP version and security string for notification messages.	–	–
inform	Sends SNMP inform messages to the configured host.	–	disabled
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 (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.	MD5/SHA	SHA
priv-prot	Indicate the privacy protocol for the user, either Advanced Encryption Standard (AES) or CBC-DES Symmetric Encryption Protocol (DES), and the password for use with the designated protocol.	AES/DES	DES

### Usage Guidelines

This command configures SNMP on the IAPs only.

### Example

The following example configures an SNMP host and community string:

```
(Instant Access Point) (config) # snmp-server community user123
(Instant Access Point) (config) # snmp-server host 10.0.0.1 version 2c udp-port 162 inform
```



## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration 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.

### Syntax

Parameter	Description	Range	Default
syslog-level <level>	<p>Configures the Syslog facility level.</p> <p>You can configure any of the following logging levels:</p> <ul style="list-style-type: none"><li>• Emergency – Panic conditions that occur when the system becomes unusable.</li><li>• Alert – Any condition requiring immediate attention and correction.</li><li>• Critical – Any critical conditions such as a hard drive error.</li><li>• Errors –Error conditions.</li><li>• Warning – Warning messages.</li><li>• Notice – Significant events of a non-critical and normal nature. The default value for all Syslog facilities.</li><li>• Informational – Messages of general interest to system users.</li><li>• Debug – Messages containing information useful for debugging.</li></ul>	Emergency, Alert, Critical, Errors, Warning, Notice, Informational, Debug	Notice
ap-debug	Generates a log for the AP device for debugging purposes.	–	–
network	Generates a log when there is a change in the network, for example, when a new 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 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.	–	–

## Usage Guidelines

Use this command to configure syslog facility levels and to generate logs based on various user and IAP parameters.

## Example

The following example configures syslog facility levels for ap-debug and user-debug:

```
(Instant Access Point) (config) # syslog-level error ap-debug
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## syslog-server

```
syslog-server <IP-address>  
no...
```

### Description

This command configures Syslog server for an IAP.

### Syntax

Parameter	Description	Range	Default
syslog-server <IP-address>	Specifies the IP address to configure the syslog server.	–	–
no...	Removes the configuration.	–	–

### Usage Guidelines

Use this command to configure syslog server for an IAP.

### Example

The following command configures the IP address of the syslog server for an IAP.

```
(Instant Access Point) (config) # syslog-server 192.0.2.9  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## telnet-server

```
telnet-server  
no...
```

### Description

This command enables Telnet access to Instant command line interface (CLI).

### Syntax

Command/Parameter	Description
telnet-server	Enables Telnet access to the Instant CLI.
no...	Removes the configuration

### Usage Guidelines

Use this command to enable Telnet access to the Instant CLI.

### Example

The following example enables Telnet access to the IAP:

```
(Instant Access Point) (config) # telnet-server  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## terminal-access

terminal-access  
no...

### Description

This command enables Secure Shell (SSH) access to Instant CLI.

### Syntax

Command/Parameter	Description
terminal-access	Enables terminal access to the Instant CLI.
no...	Removes the configuration.

### Usage Guidelines

Use this command to enable SSH access to the Instant CLI.

### Example

The following example enables terminal access to the IAP:

```
(Instant Access Point) (config) # terminal-access  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

### Syntax

Parameter	Description
tftp-dump-server <IP-address>	Configures TFTP dump server IP address.
no...	Removes the configuration

### Usage Guidelines

Use this command to configure TFTP dump server for storing core dump files.

### Example

The following example configures a TFTP dump server:

```
(Instant Access Point) (config) # tftp-dump-server <IP-address>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# traceroute

traceroute <ipaddr>

## Description

This command traces the route to the specified IP address.

## Syntax

Parameter	Description
<ipaddr>	Displays the destination IP address.

## Usage Guidelines

Use this command to identify points of failure in your network.

## Example

The following example shows the output of **traceroute** command:

```
<Instant Access Point> #traceroute 10.1.2.3
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.



## upgrade-image

```
upgrade-image <url>  
upgrade-image2 <url>  
upgrade-image2-no-reboot
```

### Description

These commands allow you to upgrade an IAP to use a new image file.

### Syntax

Parameter	Description
upgrade-image	Upgrades the IAP to use a new image.
upgrade-image2	Uploads an additional image file and upgrades the IAP to use this image file when required.
upgrade-image2-no-reboot	Uploads an additional image file and upgrades the IAP to use the new image without rebooting the IAPs.
<url>	Allows you to specify the FTP, TFTP, or HTTP URL.

### Usage Guidelines

Use these commands to upgrade n IAP to use an image file uploaded 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 IAP. The following examples describe the image class for different IAP models:

- For IAP-134/135—Instant\_Cassiopeia\_<build-version>
- For RAP-108/109 and IAP-114/115—Instant\_Pegasus\_<build-version>
- For RAP-155/155P—Instant\_Aries\_<build-version>
- For IAP-224/255—Instant\_Centaurus\_<build-version>
- For all other IAPs —Instant\_Orion\_<build-version>

### Example

The following examples upgrade an IAP by using an image file from the FTP server:

```
(Instant Access Point)# upgrade-image ftp://192.0.2.7/_Orion_6.2.1.0-4.0.0.0_xxxx  
(Instant Access Point)# upgrade-image2-no-reboot ftp://192.0.2.7/_Orion_6.2.1.0-4.0.0.0_xxxx
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	These commands are introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

# uplink

```
uplink
  enforce {ethernet| cellular |wifi | none}
  failover-internet
  failover-internet-pkt-lost-cnt <count>
  failover-internet-pkt-send-freq <frequency>
  failover-vpn-timeout <seconds>
  preemption
  uplink-priority {cellular <priority> | ethernet <priority>| [port <Interface-number> <priority>]|wifi <priority>}
  no...
```

## Description

This command configures uplink connections.

## Syntax

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: <ul style="list-style-type: none"><li>• ethernet</li><li>• cellular</li><li>• wifi</li><li>• none</li></ul>	ethernet, cellular, wifi, none	None
failover-internet	Enables uplink switchover based on the availability of the Internet. When enabled, the 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 IAP switches to a different connection.	–	Disabled
failover-internet-pkt-lost-cnt <count>	Configures the number of packets lost when verifying the uplink availability using the Internet.	–	10
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.	–	30
failover-vpn-timeout <seconds>	Configures a duration to wait for an uplink switch based on VPN status.	–	180 seconds

Parameter	Description	Range	Default
preemption	Enables pre-emption when no uplinks are enforced. When enabled, if the current uplink is active, the 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	Eth0
no...	Removes the configuration.	–	–

## Usage Guidelines

Use this command to set preferences for enforcing uplinks or enabling preemption and to configure uplink switchover.

### Enforcing uplinks

The following configuration conditions apply to the uplink enforcement:

- When an uplink is enforced, the IAP uses the specified 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 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 IAP tries to find an available uplink based on the priority configured.

### Uplink Preemption

When no uplink is enforced and preemption is enabled, and if the current uplink fails, the IAP tries to find an available uplink based on in the priority configured. If current uplink is active, the 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 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 IAP switches over to that uplink. Preemption is enabled by default.

### Uplink Switchover

The default priority for uplink switchover is Ethernet and then 3G/4G. The IAP has the ability to switch to the lower priority uplink if the current uplink is down.

### Uplink Switching based on VPN Status

Instant supports switching uplinks based on the VPN status when deploying mixed uplinks (Eth0, 3G/4G,Wi-Fi). When VPN is used with multiple backhaul options, the IAP switches to an uplink connection based on the VPN connection status instead of only using Eth0, the physical backhaul link.

The following configuration conditions apply to uplink switching:

- If the current uplink is Eth0 and the VPN connection is down, the 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 IAP waits for a vpn-failover-timeout and then a different uplink (3G,Wi-Fi) is selected.
- If the current uplink is 3G or Wi-Fi, and Eth0 has a physical link, the IAP periodically suspends user traffic to try and connect to the VPN on the Eth0. If the IAP succeeds, then the IAP switches to Eth0. If the IAP does not succeed, then the 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 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 IAP switches to a different connection.

### Example

The following example configures uplink priority:

```
(Instant Access Point) (uplink) # uplink-priority ethernet port 0 1
(Instant Access Point) (uplink) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP.

## Syntax

Parameter	Description	Range	Default
<vlan-ID>	Assigns a VLAN ID for the uplink management traffic	0-4093	0

## Usage Guidelines

Use this command to configure the uplink VLAN configuration details for management traffic. When configured, the uplink management VLAN allows you to tag management traffic and connect multiple IAP clusters (Virtual Controllers) to the same port on an upstream switch (for example, AirWave server).

## Example

The following example configures uplink management VLAN:

```
(Instant Access Point)# uplink-vlan 0
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode

## user

```
user <username> [<password>] [portal| radius]  
no...
```

### Description

This command creates users for an IAP.

### Syntax

Parameter	Description
user <username>	Creates a username for the IAP user.
<password>	Assigns a password for the IAP user
portal	Configures a guest user.
radius	Configures an employee user
no...	Removes the configuration

### Usage Guidelines

The 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 IAP is configured as an internal RADIUS server. The local user database of APs can support up to 512 user entries except IAP-9x supports only 256 user entries. If there are already 512 users, IAP-9x will not be able to join the cluster.

### Example

The following example configures an employee user for an IAP:

```
(Instant Access Point) (config) # user user1 password123 radius  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## version

version <version-number>

### Description

This command configures a version number for the IAP.

### Syntax

Parameter	Description
version <version-number>	Assigns a version number for the IAP.

### Usage Guidelines

Use this command to configure a version number for the IAP.

### Example

The following example configures a version number for the IAP.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode



## virtual-controller-country

virtual-controller-country <country-code>  
no...

### Description

This command configures the location of the IAP.

### Syntax

Parameter	Description
virtual-controller-country <country-code>	Specifies the country of operation for a IAP.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure the country code for IAPs.

### Example

The following example configures a country code for an IAP:

```
(Instant Access Point) (config) # virtual-controller-country US
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## virtual-controller-ip

virtual-controller-ip <IP-address>

### Description

This command configures an IP address for the Virtual Controller.

### Syntax

Parameter	Description
virtual-controller-ip <IP-address>	Assigns an IP address for the Virtual Controller.

### Usage Guidelines

Use this command to configure an IP address for the Virtual Controller.

### Example

The following example assigns an IP address for the Virtual Controller:

```
(Instant Access Point) (config) # virtual-controller-ip 192.0.2.2
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# virtual-controller-key

virtual-controller-key <name>

## Description

This command configures a unique name for the Virtual Controller.

## Syntax

Parameter	Description
virtual-controller-key <name>	Defines a unique name for the Virtual Controller.

## Usage Guidelines

Use this command to assign a name for the Virtual Controller.

## Example

```
(Instant Access Point) (config) # virtual-controller-key <name>
(Instant Access Point) (config) # virtual-controller-ip <IP-address>
(Instant Access Point) (config) # virtual-controller-vlan <Vlan-ID> <Mask> <Gateway-IP-address>
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## virtual-controller-vlan

```
virtual-controller-vlan <virtual-controller-vlan> <virtual-controller-mask> <virtual-controller-gateway>  
no...
```

### Description

This command configures a VLAN for the Virtual Controller.

### Syntax

Parameter	Description
<code>virtual-controller-vlan &lt;virtual-controller-vlan&gt;</code>	Associates a VLAN ID with the Virtual Controller.
<code>&lt;virtual-controller-mask&gt;</code>	Configures a subnet mask for the Virtual Controller.
<code>&lt;virtual-controller-gateway&gt;</code>	Configures a gateway for the Virtual Controller.
<code>no...</code>	Removes the configuration.

### Usage Guidelines

Use this command to configure VLAN, Netmask, and Gateway for the Virtual Controller.

### Example

The following example configures VLAN for the Virtual Controller:

```
(Instant Access Point) (config) # virtual-controller-vlan <Vlan-ID> <Mask> <Gateway-IP-address>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
vpn backup <name>	Configures a fully qualified domain name for the secondary VPN or IPsec endpoint.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure a backup VPN server. When both primary and secondary VPN servers are configured, the IAP can switch to the available VPN connection when the primary VPN server is not available.

### Example

The following example configures a backup server for VPN connections:

```
(Instant Access Point) (config) # vpn backup <name>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

## Syntax

Parameter	Description
vpn fast-failover	Enables fast failover feature for VPN connections.
no...	Removes the configuration.

## Usage Guidelines

Use this command to configure fast failover feature for VPN connections. Enabling the fast failover feature allows the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately. If the primary tunnel fails, the IAP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.

## Example

The following example configures the VPN fast failover feature:

```
(Instant Access Point) (config) # fast-failover  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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 IAP and the controller.

### Usage Guidelines

Use this command to enable automatic configuration of the GRE tunnel between the controller to provide L2 connectivity.

### Example

The following example configures an automatic GRE tunnel:

```
(Instant Access Point) (config) # vpn gre-outside  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is introduced.

### Command Information

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 IAP can switch over to the primary host when preemption is enabled.

### Syntax

Parameter	Description
vpn hold-time <seconds>	Configures a time period in seconds after which the IAPs can switch to primary VPN server.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure a period to hold on switching to the primary server when pre-emption is enabled.

### Example

The following example configures a hold-time to switch to the primary host server:

```
(Instant Access Point) (config) # hold-time <seconds>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
vpn ikepsk <ikepsk>	Specifies an IKE authentication for VPN connection using pre-shared keys
username <username>	Defines a username that enables access to VPN.
password <password>	Defines a password that enables access to VPN.
no...	Removes the configuration.

### Usage Guidelines

Use this command to configure user credentials to establish VPN connection.

### Example

The following commands enable user access to VPN connection.

```
(Instant Access Point)(config)# vpn ikepsk secretKey username User1 password password123  
(Instant Access Point)(config)# end  
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP can determine that the VPN connection is not available.

Parameter	Description	Range	Default
vpn monitor-pkt-lost-cnt <count>	Defines the number of lost packets for VPN connection test or monitoring by the IAP.	–	2
no...	Removes the configuration.	–	–

### Usage Guidelines

Use this command to configure a count for the lost packets, so that the IAPs can determine if the VPN connection is unavailable.

### Example

The following example configures a count for the lost packets:

```
(Instant Access Point) (config) # vpn monitor-pkt-lost-cnt <count>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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 IAP can verify if the active VPN connection is available.

### Syntax

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.	–	–

### Usage Guidelines

Use this command to monitor VPN connections and verify its availability at regular intervals.

### Example

The following example configures the VPN monitoring frequency:

```
(Instant Access Point) (config)# vpn monitor-pkt-send-freq 10  
(Instant Access Point) (config)# end  
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
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.

### Usage Guidelines

Use this command to enable pre-emption when both primary and secondary servers are configured and fast failover feature is enabled.

### Example

The following example enables VPN pre-emption.

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## vpn primary

```
vpn primary <name>  
no...
```

### Description

This command configures a primary Virtual Private Networks (VPN) server for VPN connections.

### Syntax

Parameter	Description	Range	Default
vpn primary <name>	Configures a fully qualified domain name for the main VPN or IPSec endpoint.	–	–
no...	Removes the VPN server configuration.	–	–

### Usage Guidelines

Use this command to configure a primary VPN server for IAP-VPN connections. When a secondary VPN server is configured along with the primary server, you can enable the fast failover feature that allows the IAP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately.

### Example

The following example configures a primary VPN server:

```
(Instant Access Point) (config) # vpn primary <name>  
(Instant Access Point) (config) # end  
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

## vpn reconnect-time-on-failover

vpn reconnect-time-on-failover <down-time>

### Description

This command defines a period after which the VPN connection can be reestablished when the primary VPN tunnel fails.

### Syntax

Parameter	Description
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.

### Usage Guidelines

Use this command to configure a time period for reestablishing VPN connections. When configured, the IAP reconnects the user session when the interval specified for this command expires.

### Example

The following example configures a VPN reconnection duration:

```
(Instant Access Point) (config) # vpn reconnect-time-on-failover 20
(Instant Access Point) (config) # end
(Instant Access Point) # commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

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.

### Syntax

Parameter	Description
vpn reconnect-user-on-failover	Enables users to reconnect to the VPN during a VPN failover.
no...	Removes the configuration.

### Usage Guidelines

Use this command to allow the users to reconnect to the VPN after a VPN failover. When enabled , the IAP reconnects the user during a VPN failover.

### Example

The following example enables users to reconnect to VPN after a failover:

```
(Instant Access Point) (config)# vpn reconnect-user-on-failover  
(Instant Access Point) (config)# end  
(Instant Access Point)# commit apply
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Configuration mode

# wifi0-mode

wifi0-mode <mode>

## Description

This command configures an IAP to function in the access, monitor, or spectrum monitor mode.

## Syntax

Parameter	Description	Range	Default
<mode>	<p>Configures the IAP to function in any of the following modes:</p> <ul style="list-style-type: none"><li>• <b>Access</b>— In Access mode, the IAP serves clients, while also monitoring for rogue APs in the background.</li><li>• <b>Monitor</b>— In Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients.</li><li>• <b>Spectrum Monitor</b>— In Spectrum Monitor mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non-WiFi devices such as microwaves and cordless phones.</li></ul> <p><b>NOTE:</b> In Monitor and Spectrum Monitor modes, the IAP does not provide access services to clients.</p>	access, monitor, spectrum-monitor	access

## Usage Guidelines

Use this command to configure a Wi-Fi interface of an IAP to function in the access, monitor, or spectrum monitor mode.

## Example

The following example configures the wifi0 interface to use the access mode:

```
(Instant Access Point)# wifi0-mode access
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.



# wifi1-mode

wifi1-mode <mode>

## Description

This command configures an IAP to function in the access, monitor, or spectrum monitor mode.

## Syntax

Parameter	Description	Range	Default
<mode>	<p>Configures the IAP to function in any of the following modes:</p> <ul style="list-style-type: none"><li>• <b>Access</b>— In Access mode, the IAP serves clients, while also monitoring for rogue APs in the background.</li><li>• <b>Monitor</b>—In Monitor mode, the AP acts as a dedicated monitor, scanning all channels for rogue IAPs and clients.</li><li>• <b>Spectrum Monitor</b>— In Spectrum Monitor mode, the IAP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from neighboring APs or from non-WiFi devices such as microwaves and cordless phones.</li></ul> <p><b>NOTE:</b> In Monitor and Spectrum Monitor modes, the IAP does not provide access services to clients.</p>	access, monitor, spectrum-monitor	access

## Usage Guidelines

Use this command to configure a Wi-Fi interface of an IAP to function in the access, monitor, or spectrum monitor mode.

## Example

The following example configures the wifi0 interface to use the access mode:

```
(Instant Access Point)# wifi1-mode access
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode.

## wired-port-profile

```
wired-port-profile <port>
  access-rule-name <name>
  allowed-vlan <vlan>
  auth-server <name>
  captive-portal <type> exclude-uplink <Types>
  content-filtering
  dot1x
  duplex <duplex:/full/half/auto>
  l2-auth-failthrough
  mac-authentication
  native-vlan <vlan>
  poe
  radius-reauth-interval <minutes>
  server-load-balancing
  set-role <attribute>{{equals| not-equal|starts-with| ends-with| contains} <operator> <role>
|value-of}
  set-role-machine-auth <machine-authentication> <user-authentication>
  set-role-mac-auth <MAC-authentication>
  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:10/100/1000/auto>
  switchport-mode <mode>
  type <type>
  uplink-enable
  no...
```

### Description

This command configures a wired port profile for wired IAP clients.

### Syntax

Command/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.	–	–
captive-portal <type>	Enables internal or external Captive portal authentication for the wired profile	–	–

Command/Parameter	Description	Range	Default
<code>exclude-uplink {3G  4G  Wifi  Ethernet}</code>	users. You can also disable redirection to the Captive portal based on the type of current uplink.		
<code>content-filtering</code>	Enables content filtering	–	–
<code>dot1x</code>	Enables 802.11X authentication for the Wired profile users	–	Disabled
<code>duplex &lt;full  half  auto&gt;</code>	Assigns a value for duplexing client traffic based on the capabilities of the client, the AP, and the cable.	full, half, auto	auto
<code>l2-auth-failthrough</code>	Allows the clients to use 802.1X authentication when MAC authentication fails.	–	Disabled
<code>mac-authentication</code>	Enables MAC authentication	–	Disabled
<code>native-vlan &lt;vlan&gt;</code>	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	–
<code>poe</code>	Enables power over Ethernet	–	Enabled
<code>radius-reauth-interval &lt;minutes&gt;</code>	Configures a reauthentication interval at which all associated and authenticated clients must be reauthenticated.	–	–
<code>server-load-balancing</code>	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	–	Enabled
<code>set-role &lt;attribute&gt; {{equals  not-equal starts-with  ends-with  contains}operator} &lt;role&gt;  value-of}</code>	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: <ul style="list-style-type: none"> <li>contains – The rule is applied only if the attribute value contains the specified string.</li> <li>ends-with – The rule is applied only if the attribute value ends with the specified string.</li> <li>equals – The rule is applied only if the attribute value is equal to the specified string.</li> <li>not-equals – The rule is applied only if the attribute value is not equal to the specified string.</li> <li>starts-with – The rule is applied only if the attribute value begins with the</li> </ul>	–	–

Command/Parameter	Description	Range	Default
	<p>specified string.</p> <ul style="list-style-type: none"> <li>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 IAP.</li> </ul>		
<pre>set-role-machine-auth &lt;machine-authentication&gt; &lt;user-authentication&gt;</pre>	<p>Configures a machine authentication rule.</p> <p>You can assign different rights to clients based on whether their hardware device supports machine authentication.</p> <p>Machine authentication is only supported on Windows devices, so this can be used to distinguish between Windows devices and other devices such as iPads.</p>	–	–
<pre>set-role-mac-auth &lt;mac-only&gt;</pre>	Configures a MAC authentication based user role.	–	–
<pre>set-role-pre-auth &lt;role&gt;</pre>	Configures a pre-authentication role to allow some access to the guest users before the client authentication.	–	–
<pre>set-role-unrestricted</pre>	Configures unrestricted access control.	–	–
<pre>set-vlan &lt;attribute&gt; {equals not-equals  starts-with  ends-with  contains} &lt;operator&gt; &lt;VLAN-ID&gt;  value-of}</pre>	<p>Assigns a VLAN to the clients. The first rule that matches the configured condition is applied.</p> <p>You can specify any of the following conditions:</p> <ul style="list-style-type: none"> <li>contains – The rule is applied only if the attribute value contains the specified string.</li> <li>ends-with – The rule is applied only if the attribute value ends with the specified string.</li> <li>equals – The rule is applied only if the attribute value is equal to the specified string.</li> <li>not-equals – The rule is applied only if the attribute value is not equal to the specified string.</li> <li>starts-with – The rule is applied only if the attribute value begins with the specified string.</li> <li>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 IAP.</li> </ul>	–	–
<pre>shutdown</pre>	Shuts down the admin status port	up, down	up
<pre>spanning-tree</pre>	Enables Spanning Tree Protocol on the	–	–

Command/Parameter	Description	Range	Default
	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 IAPs with three or more ports. By default Spanning Tree is disabled on wired profiles.		
speed <10  100  1000  auto>	Assigns a value for indicating speed of client traffic based on the capabilities of the client, the AP, and the cable.	10,100,200, auto	auto
switchport-mode <trunk  access>	Defines the switchport mode for the wired profile.  You can specify any of the following modes: <ul style="list-style-type: none"> <li>● <b>Access</b> – Use this mode to allow the port to carry a single VLAN specified as the native VLAN.</li> <li>● <b>Trunk</b> – Use this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.</li> </ul>	access, trunk	trunk
type <type>	Defines the primary usage of the wired profile.	employee, guest	employee
uplink-enable	Enables uplink for the wired profile	–	–
no...	Removes any existing configuration	–	–

## Usage Guidelines

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 Access Control List (ACL) for additional security on the Ethernet downlink.

## Example

The following example configures a wired profile for an employee network:

```
(Instant Access Point) (config) # wired-port-profile employeeWired1
(Instant Access Point) (wired ap profile"employeeWired1") # type employee
(Instant Access Point) (wired ap profile"employeeWired1") # speed auto
(Instant Access Point) (wired ap profile"employeeWired1") # duplex auto
(Instant Access Point) (wired ap profile"employeeWired1") # no shutdown
(Instant Access Point) (wired ap profile"employeeWired1") # poe
(Instant Access Point) (wired ap profile"employeeWired1") # uplink-enable
(Instant Access Point) (wired ap profile"employeeWired1") # content-filtering
(Instant Access Point) (wired ap profile"employeeWired1") # switchport-mode trunk
(Instant Access Point) (wired ap profile"employeeWired1") # allowed-vlan 2,3,5
(Instant Access Point) (wired ap profile"employeeWired1") # native-vlan 1
(Instant Access Point) (wired ap profile"employeeWired1") # mac-authentication
(Instant Access Point) (wired ap profile"employeeWired1") # dot1x
(Instant Access Point) (wired ap profile"employeeWired1") # l2-auth-failthrough
(Instant Access Point) (wired ap profile"employeeWired1") # auth-server server1
(Instant Access Point) (wired ap profile"employeeWired1") # server-load-balancing
```

```
(Instant Access Point) (wired ap profile"employeeWired1")# radius-reauth-interval 20
(Instant Access Point) (wired ap profile"employeeWired1")# access-rule-name wiredACL
(Instant Access Point) (wired ap profile"employeeWired1")# set-role Group-Name contains wired w
ired-instant
(Instant Access Point) (wired ap profile"employeeWired1")# set-vlan ap-name equals test 400
(Instant Access Point) (wired ap profile"employeeWired1")# end
(Instant Access Point)# commit apply
```

The following example configures a guest wired profile:

```
(Instant Access Point) (config)# wired-port-profile guestWired1
(Instant Access Point) (wired ap profile"guestWired1")# type guest
(Instant Access Point) (wired ap profile"guestWired1")# speed auto
(Instant Access Point) (wired ap profile"guestWired1")# duplex auto
(Instant Access Point) (wired ap profile"guestWired1")# no shutdown
(Instant Access Point) (wired ap profile"guestWired1")# poe
(Instant Access Point) (wired ap profile"guestWired1")# uplink-enable
(Instant Access Point) (wired ap profile"guestWired1")# content-filtering
(Instant Access Point) (wired ap profile"guestWired1")# switchport-mode trunk
(Instant Access Point) (wired ap profile"guestWired1")# allowed-vlan 200,201,400
(Instant Access Point) (wired ap profile"guestWired1")# native-vlan 1
(Instant Access Point) (wired ap profile"guestWired1")# captive-portal external exclude-uplink
Ethernet
(Instant Access Point) (wired ap profile"guestWired1")# mac-authentication
(Instant Access Point) (wired ap profile"guestWired1")# auth-server server1
(Instant Access Point) (wired ap profile"guestWired1")# server-load-balancing
(Instant Access Point) (wired ap profile"guestWired1")# access-rule-name wiredACL
(Instant Access Point) (wired ap profile"guestWired1")# set-role Group-Name contains wired wire
d-instant
(Instant Access Point) (wired ap profile"guestWired1")# set-vlan ap-name equals test 200
(Instant Access Point) (wired ap profile"guestWired1")# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.4	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and Wired port profile configuration sub-mode.

## wlan access-rule

```
wlan access-rule <name>
  bandwidth-limit {downstream <kbps>| upstream <kbps>| peruser { downstream <kbps>| upstream
  <kbps>}}
  calea
  captive-portal {external [profile <name>]|internal}
  index <index>
  rule <dest> <mask> <match> <protocol> <start-port> <end-port>{permit| deny| src-nat|dst-nat
  {<IP-address> <port>| <port>}} [<option1...option9>]
  vlan <vlan-id>
  no...
```

### Description

This command configures access rules for WLAN SSID or wired profile.

### Syntax

Command/Parameter	Description	Range	Default
wlan access-rule <name>	Specifies the profile name for which the access rule is configured.	–	–
bandwidth-limit {downstream <kbps>  upstream <kbps>  peruser {downstream <kbps>  upstream <kbps>}}	<p>Assign bandwidth contracts to user roles.</p> <p>The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the IAP) or downstream (IAP to clients) traffic for a user role.</p> <p>If you want to assign a bandwidth contract specific for each user, you can run the command with <b>peruser</b> parameter.</p> <p>The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations.</p> <p><b>NOTE:</b> 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 IAP is upgraded to 6.3.1.1-4.0 release version, the bandwidth configuration per SSID will be treated as per-user downstream bandwidth contract for that SSID.</p>	1-65535 Kbps	–

Command/Parameter	Description	Range	Default
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.	–	–
<index>	Creates an index entry for access rules.	–	–
rule	Creates an access rule.  You can create up to 64 access rules. However, it is recommended to delete any existing configuration and apply changes at regular intervals.	–	–
<dest>	Specifies destination with any of the following values: <ul style="list-style-type: none"> <li>• Destination address (IPv4 or IPv6) and wildcard</li> <li>• any: any destination</li> <li>• host: a single host IP address</li> </ul>	–	–
<mask>	Specifies the subnet mask for the destination IP address.	–	–
<match>	Indicates if the rule specific to the destination IP address and subnet mask matches the value specified for protocol	–	–
<protocol>	Configures any of the following: <ul style="list-style-type: none"> <li>• Protocol number between 0-255</li> <li>• any: any protocol</li> <li>• tcp: Transmission Control Protocol</li> <li>• udp: User Datagram Protocol</li> </ul>	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	–
permit	Creates a rule to allow the specified packets.	–	–



Command/Parameter	Description	Range	Default
deny	Creates a rule to reject the specified packets	–	–
dst-nat	Allows the IAP to perform destination NAT on packets.	–	–
src-nat	Allows the 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).	–	–
<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.	–	–
<option1...option9>	Allows you to specify any of the following options: <ul style="list-style-type: none"> <li>• Log –Creates a log entry when this rule is triggered.</li> <li>• Blacklist – Blacklists the client when this rule is triggered.</li> <li>• Classify-media – Performs a packet inspection on all non-NAT traffic and marks the critical traffic.</li> <li>• Disable-scanning – Disables ARM scanning when this rule is triggered.</li> <li>• DSCP tag – Specifies a DSCP value to prioritize traffic when this rule is triggered.</li> <li>• 802.1p priority – Sets an 802.1p priority.</li> </ul>	–	–
vlan <vlan-id>	Configures an access rule for VLAN assignment.	1-4093	–
no...	Removes the configuration	–	–

## Usage Guidelines

Use this command to configure access rules for user roles, to create a captive-portal role, and to assign VLANs for the clients.

## Example

The following example configures an access rule:

```
(Instant Access Point) (config) # wlan access-rule WirelessRule
(Instant Access Point) (Access Rule WirelessRule) # rule 10.17.88.59 255.255.255.255 match 6 434
3 4343 log classify-media
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.4	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

## wlan auth-server

```
wlan auth-server <auth_profile_name>
  acctport <accounting-port>
  cppm-rfc3576-only
  cppm-rfc3576-port <rfc3576-port>
  deadtime <minutes>
  drp-ip <IP-address> <mask> vlan <vlan> gateway <gateway-IP-address>
  ip <IP-address>
  key <key>
  nas-id <NAS-ID>
  nas-ip <IP-address>
  port <port-name>
  retry-count <count>
  rfc3576
  timeout <seconds>
  no...
```

### Description

This command configures an external RADIUS and CPPM server for user authentication.

### Syntax

Command/Parameter	Description	Range	Default
wlan auth-server <server-profile>	Configures the external RADIUS server authentication profile	—	—
acctport <accounting-port>	Configures the accounting port number used for sending accounting records to the RADIUS server.	—	1813
cppm-rfc3576-only	Configures a CPPM server used for AirGroup CoA (Change of Authorization) with RFC3576 only.  The CPPM 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 <minutes>	Configures a dead time interval for the authentication server.  When two or more authentication servers are configured on the 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	5
drp-ip <IP-address> <mask> vlan <vlan> gateway <gateway-IP-address>	Configures the IP address, net mask and VLAN, which will be used as	—	—

Command/Parameter	Description	Range	Default
IP-address>	source address and VLAN for RADIUS packets.  <b>NOTE:</b> Before configuring DRP IP address, ensure that <a href="#">dynamic RADIUS proxy</a> is enabled, and a static Virtual Controller IP is configured.		
ip <IP-address>	Configures the IP address of the RADIUS server	–	–
key <key>	Configures a shared key communicating with the external RADIUS server.	–	–
nas-id <NAS-ID>	Configures Network Attached Storage (NAS) identifier strings for RADIUS attribute 32, which is sent with RADIUS requests to the RADIUS server.	–	–
nas-ip <IP-address>	Configures the Virtual Controller IP address as the NAS address which is sent in data packets.	–	–
port <port-name>	Configures the authorization port number of the external RADIUS server.	–	1812
retry-count <count>	Configures the maximum number of authentication requests that can be sent to the server group.	1-5	3
rfc3576	Allows the IAPs to process RFC 3576-compliant Change of Authorization (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
timeout <seconds>	Configures a timeout value in second to determine when a RADIUS request must expire.  The 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
no...	Removes the configuration.	–	–

## Usage Guidelines

Use this command to configure an external RADIUS server and a CPPM server as a RADIUS server for AirGroup Change of Authorization (CoA) requests.

## Example

The following example configures the external RADIUS server parameters:

```
(Instant Access Point) (config) # wlan auth-server RADIUS1
(Instant Access Point) (Auth Server <RADIUS1>) # ip 192.0.0.5
(Instant Access Point) (Auth Server <RADIUS1>) # key SecretKey
(Instant Access Point) (Auth Server <RADIUS1>) # port 1812
(Instant Access Point) (Auth Server <RADIUS1>) # acctport 1813
(Instant Access Point) (Auth Server <RADIUS1>) # no nas-id
(Instant Access Point) (Auth Server <RADIUS1>) # no nas-ip
(Instant Access Point) (Auth Server <RADIUS1>) # drp-ip 192.0.2.11 255.255.255.255 vlan 200 gate
way 192.0.2.15
(Instant Access Point) (Auth Server <RADIUS1>) # timeout 10
(Instant Access Point) (Auth Server <RADIUS1>) # retry-count 3
(Instant Access Point) (Auth Server <RADIUS1>) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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>
  terms-of-use <terms-of-use-text>
  use-policy <policy-text>
  no...
```

### Description

This command customizes the appearance of the internal Captive portal splash page of the guest users.

### Syntax

Command/Parameter	Description	Range	Default
wlan captive-portal	Displays the sub-mode for configuring internal Captive portal splash page.	–	–
authenticated	Configures the authentication text. The <b>authenticated</b> text is used for indicating that the authentication mode is enabled for the internal Captive Portal users. When the authentication mode is enabled, the 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.	–	–
redirect-url <url>	Configures a URL to redirect the users after a successful authentication. <b>NOTE:</b> 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	–	–

Command/Parameter	Description	Range	Default
	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 configuration.	–	–

## Usage Guidelines

Use this command to customize the appearance of internal Captive portal splash page for the guest users.

## Example

The following example configures the contents of the internal Captive portal splash page:

```
(Instant Access Point) (config) # wlan captive-portal
(Instant Access Point) (Captive Portal) # authenticated
(Instant Access Point) (Captive Portal) # background-color 13421772
(Instant Access Point) (Captive Portal) # banner-color 16750848
(Instant Access Point) (Captive Portal) # banner-text "Welcome to Guest Network"
(Instant Access Point) (Captive Portal) # no decoded-texts
(Instant Access Point) (Captive Portal) # redirect-url example1.com
(Instant Access Point) (Captive Portal) # terms-of-use "This network is not secure, and use is a
t your own risk"
(Instant Access Point) (Captive Portal) # use-policy "Please read terms and conditions before us
ing Guest Network"
(Instant Access Point) (Captive Portal) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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>
  redirect-url <redirection-url>
  server <server-name>
  server-fail-through
  url <url>
  no...
```

### Description

This command configures profiles for external Captive portal.

### Syntax

Command/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.	–	Enabled
https	Enables HTTPS for client connections.	–	–
Port <port>	Configures the port to use for communication with the external Captive portal server.	–	80
redirect-url <redirection-url>	Configures a URL to redirect the users after a successful authentication. <b>NOTE:</b> 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.	–	–
server <server-name>	Configures the external Captive portal server.	–	–
url <url>	Configures the URL of the external Captive portal server.	–	–
server-fail-through	Allows the guest clients to access the	–	Disabled



Command/Parameter	Description	Range	Default
	Internet when the external captive portal server is not available.		
no...	Removes the configuration.	–	–

## Usage Guidelines

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.

## Example

The following example configures external Captive portal splash page:

```
(Instant Access Point) (config) # wlan external-captive-portal AuthText1
(Instant Access Point) (External Captive Portal) # auth-text authenticated
(Instant Access Point) (External Captive Portal) # port 80
(Instant Access Point) (External Captive Portal) # redirect-url http://www.example1.com
(Instant Access Point) (External Captive Portal) # server CPServer1
(Instant Access Point) (External Captive Portal) # url "/aruba.php"
(Instant Access Point) (External Captive Portal) # server-fail-through
(Instant Access Point) (External Captive Portal) # no auto-whitelist-disable
(Instant Access Point) (External Captive Portal) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.3.1.1-4.0	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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>
  filter <filter>
  key-attribute <key-attribute>
  ip <IP-address>
  port <port-name>
  timeout <seconds>
  retry-count <count>
  no...
```

### Description

This command configures an Lightweight Directory Access Protocol (LDAP) server for user authentication on the Virtual Controller.

### Syntax

Command/Parameter	Description	Range	Default
wlan ldap-server <server-name>	Configures an LDAP authentication server.	–	–
admin-dn <domain-name>	Configures a distinguished name 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 distinguished name for the node which contains the entire user database.	–	–
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 <b>sAMAccountName</b>	–	–
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	1-30	5

Command/Parameter	Description	Range	Default
	requests from the clients	seconds	
<code>retry-count &lt;count&gt;</code>	Defines the number of times that the clients can attempt to connect to the server.	1-5	3
<code>no...</code>	Removes the configuration.	–	–

## Usage Guidelines

Use this command to configure an LDAP server as an external authentication server. The LDAP service is based on a client-server model. The IAP client requests for an LDAP session after connecting to the LDAP server and server sends its responses.

## Example

The following example configures an LDAP server:

```
(Instant Access Point)(config)# wlan ldap-server Server1
(Instant Access Point)(LDAP Server <name>)# ip 192.0.1.5
(Instant Access Point)(LDAP Server <name>)# port 389
(Instant Access Point)(LDAP Server <name>)# admin-dn cn=admin
(Instant Access Point)(LDAP Server <name>)# admin-password password123
(Instant Access Point)(LDAP Server <name>)# base-dn dc=example, dc=com
(Instant Access Point)(LDAP Server <name>)# filter (objectclass=*)
(Instant Access Point)(LDAP Server <name>)# key-attribute sAMAccountName
(Instant Access Point)(LDAP Server <name>)# timeout 5
(Instant Access Point)(LDAP Server <name>)# retry-count 3
(Instant Access Point)(LDAP Server <name>)# end
(Instant Access Point)# commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and LDAP server sub-mode.

## wlan ssid-profile

```
wlan ssid-profile <profile-name>
  a-max-tx-rate <transmission-rate>
  a-min-tx-rate <transmission-rate>
  air-time-limit <percentage-of-limit>
  auth-server <server-name>
  auth-survivability
  bandwidth-limit <limit>
  blacklist
  broadcast-filter <Filter-type>
  captive-portal <type> exclude-uplink <type>
  content-filtering
  disable
  dmo-channel-utilization-threshold <threshold>
  dot11r
  dtim-period <beacons>
  dynamic-multicast-optimization
  enable
  enforce-dhcp
  essid <SSID-Name>
  external-server
  g-min-tx-rate <transmission-rate>
  g-max-tx-rate <transmission-rate>
  hide-ssid
  hotspot-profile <profile-name>
  inactivity-timeout <seconds>
  index
  l2-auth-failthrough
  leap-use-session-key
  local-probe-req-thresh <threshold>
  mac-authentication
  mac-authentication-delimiter <delimiter>
  mac-authentication-uppercase
  max-authentication-failures <limit>
  max-clients-threshold <threshold>
  multicast-rate-optimization
  okc-disable
  opmode {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}
  per-user-bandwidth-limit <percentage-of-limit>
  radius-accounting
  radius-accounting-mode {user-authentication| user-association}
  radius-interim-accounting-interval <minutes>
  radius-reauth-interval <minutes>
  rf-band {2.4| 5.0| all}
  server-load-balancing
  set-role <attribute>{{equals| not-equal|starts-with| ends-with|contains|matches-regular-exp
ression}<operator><role>| value-of}
  set-role-by-ssid
  set-role-mac-auth
  set-role-machine-auth
  set-role-pre-auth
  set-role-unrestricted
  set-vlan <attribute>{{equals|not-equals| starts-with| ends-with|contains|matches-regular-ex
pression}<operator><VLAN-ID>| value-of}
  termination
  type {employee| voice | guest}
  vlan <VLAN-id>
  wep-key <WEP-key>
  wispr
  wmm-background-share <Percentage-of-traffic-share>
```

```

wmm-best-effort-share <Percentage-of-traffic-share>
wmm-video-share <Percentage-of-traffic-share>
wmm-voice-share <Percentage-of-traffic-share>
work-without-uplink
wpa-passphrase <WPA-key>
no...

```

## Description

This command configures a WLAN SSID profile.

## Syntax

Command/Parameter	Description	Range	Default
wlan ssid-profile <profile-name>	Creates a WLAN SSID profile.	–	–
a-max-tx-rate <transmission-rate>	Configures the specify the maximum transmission rate for the 5 GHz band.	6-54 Mbps	54 Mbps
a-min-tx-rate <transmission-rate>	Configures the specify the minimum transmission rate for the 5 GHz band.	6-54 Mbps	6 Mbps
air-time-limit <percentage-of-limit>	Configures an aggregate amount of airtime that all clients using this SSID can use for sending and receiving data.	–	–
auth-server <server-name>	Configures an authentication server for the SSID users.	–	–
auth-survivability	Enables the authentication survivability feature. <b>NOTE:</b> The authentication survivability feature requires ClearPass Policy Manager 6.0.2 or later, and is applicable only when external servers such as RADIUS or LDAP are configured for the SSID. When enabled, Instant authenticates the previously connected clients using EAP-PEAP authentication even when connectivity to ClearPass Policy Manager is temporarily	–	Disabled

Command/Parameter	Description	Range	Default
	lost. The Authentication survivability feature is not applicable when a RADIUS server is configured as an internal server.		
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.	–	Disabled
broadcast-filter {all  ARP  Disbaled}	Configures broadcast filtering parameters: You can configure any of the following filtering parameters: <ul style="list-style-type: none"> <li>• <b>All</b>—When set to All, the IAP drops all broadcast and multicast frames except DHCP and ARP.</li> <li>• <b>ARP</b>—When set to ARP, the IAP converts ARP requests to unicast and send frames directly to the associated client.</li> <li>• <b>Disabled</b>— When set to Disabled, all broadcast and multicast traffic is forwarded.</li> </ul>	All, ARP, Disabled	Disabled
captive-portal{external  internal} exclude-uplink {3G 4G Wifi Ethernet}	Configures Captive portal authentication.	external, internal	–
	Disables redirection to the Captive portal based on the type of current uplink	3G,4G, wifi,ethernet	–
content-filtering	Routes all DNS requests for the non-corporate domains to OpenDNS on this network.	–	Disabled
disable	Disables the SSID. By default all SSIDs are enabled	–	–

Command/Parameter	Description	Range	Default
dmo-channel-utilization-threshold <threshold>	<p>Sets a threshold for DMO channel utilization.</p> <p>IAP sends multicast traffic over the wireless link.</p>	1-100 percentage value	90
dot11r	<p>Enables 802.11R on the SSID profile.</p> <p>802.11R or fast BSS transition (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 WPA2 authentication method.</p>	–	–
dtim-period <beacons>	<p>Configures the Delivery Traffic Indication Message (DTIM) interval for the SSID profile.</p> <p>The DTIM interval determines how often the IAP should deliver the buffered broadcast and multicast frames to associated clients in the powersaving mode.</p> <p>When configured, the client checks for buffered data on the IAP at the specified number of beacons. You can also configure a higher value for DTIM interval for power saving.</p>	1-10 beacons	1

Command/Parameter	Description	Range	Default
<code>dynamic-multicast-optimization</code>	Allows the IAP to convert multicast streams into unicast streams over the wireless link. Enabling Dynamic Multicast Optimization (DMO) enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients.  <b>NOTE:</b> When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN.	–	Disabled
<code>enable</code>	Re-enables the deactivated SSIDs.	–	Enabled
<code>enforce-dhcp</code>	Enforces dynamic VLAN assignment for clients from the DHCP server.	–	Disabled
<code>ssid &lt;SSID-Name&gt;</code>	Defines a name that uniquely identifies a wireless network.	–	–
<code>external-server</code>	Configures an external RADIUS server for authentication.	–	–
<code>g-min-tx-rate &lt;transmission-rate&gt;</code>	Configures the specify the minimum transmission rate for the 2.4 GHz band.	1-54 Mbps	1 Mbps
<code>g-max-tx-rate &lt;transmission-rate&gt;</code>	Configures the specify the maximum transmission rate for the 2.4 GHz band.	1-54 Mbps	54 Mbps
<code>hide-ssid</code>	Hides the SSID. When enabled, the SSID will not be visible for the users.	–	Disabled
<code>hotspot-profile &lt;profile-name&gt;</code>	Associates a hotspot profile with the WLAN SSID profile.	–	–



Command/Parameter	Description	Range	Default
<code>inactivity-timeout &lt;seconds&gt;</code>	<p>Configures a timeout value for the inactive user sessions.</p> <p>When a client session is inactive for the specified duration, the session expires and the users are required to log in again.</p>	60-1000 seconds	1000
<code>index</code>	Assigns an index value for the SSID.	–	–
<code>l2-auth-failthrough</code>	Allows the clients to use 802.1X authentication when MAC authentication fails.	–	Disabled
<code>leap-use-session-key</code>	<p>Allows the users to derive session keys for Lightweight Extensible Authentication Protocol (LEAP) authentication.</p> <p>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.</p>	–	Disabled
<code>local-probe-req-thresh &lt;threshold&gt;</code>	<p>Configures a Received signal strength indication (RSSI) threshold value to limit the number of incoming probe requests.</p> <p>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,</p>	0-100 dB	–
<code>mac-authentication</code>	Enables MAC authentication for clients that use this SSID profile.	–	Disabled

Command/Parameter	Description	Range	Default
<code>mac-authentication-delimiter &lt;delimiter&gt;</code>	<p>Allows you to set a delimiter that can be used in the MAC address string for MAC authentication.</p> <p>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.</p>	colon or dash	–
<code>mac-authentication-upper-case</code>	Enables the IAP to use uppercase letters in MAC address string for MAC authentication.	–	–
<code>max-authentication-failures &lt;limit&gt;</code>	<p>Configures the maximum number of authentication failures to dynamically blacklist the users.</p> <p>The users who exceed the number of authentication failures configured through this command are dynamically blacklisted.</p>	–	–
<code>max-clients-threshold &lt;threshold&gt;</code>	Configures the maximum number of clients for a BSSID on a WLAN.	0-255	64
<code>multicast-rate-optimization</code>	<p>Allows the IAP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients.</p> <p>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 5.0 GHz is 6 Mbps.</p>	–	Disabled

Command/Parameter	Description	Range	Default
okc-disable	<p>Disables opportunistic key caching (OKC).</p> <p>In the OKC based roaming, the AP stores one pairwise master key (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 IAP to allow faster roaming of clients.</p> <p><b>NOTE:</b> If the wireless client (the 802.1X supplicant) does not support this feature, a complete 802.1X authentication is required whenever it roams to a new IAP. OKC is supported on WPA2-AES Enterprise network only.</p>	–	–
opmode {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}	<p>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:</p> <ul style="list-style-type: none"> <li>• opensystem – No authentication and encryption.</li> <li>• wpa2-aes –WPA2 with AES encryption and dynamic keys using 802.1x.</li> <li>• wpa2-psk-aes – WPA2 with AES encryption using a preshared key.</li> <li>• wpa-tkip – WPA with TKIP encryption and dynamic keys using 802.1x.</li> <li>• wpa-psk-tkip – WPA with TKIP encryption using a pre-shared key.</li> <li>• wpa-tkip, wpa2-aes – WPA with TKIP</li> </ul>	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	opensystem

Command/Parameter	Description	Range	Default
	<p>and WPA2 with AES encryption.</p> <ul style="list-style-type: none"> <li>• wpa-psk-tkip,wpa2-psk-aes - WPS with TKIP and WPA2 with AES encryption using a pre-shared key.</li> <li>• static-wep – WEP with static keys.</li> <li>• dynamic-wep – WEP with dynamic keys.</li> </ul>		
per-user-bandwidth-limit <limit>	<p>Configures a bandwidth limit in Kbps for the SSID users.</p> <p><b>NOTE:</b> The bandwidth contracts can also be applied per SSID user.</p>	1–65535 Kbps	–
radius-accounting	<p>Enables accounting for the RADIUS server authentication.</p> <p>When enabled, the IAPs post accounting information to the Radius server at the specified accounting interval.</p>	–	Disabled
radius-accounting-mode {user-authentication  user-association}	<p>Configures an accounting mode for the Captive portal users.</p> <p>You can configure any of the following modes for accounting:</p> <ul style="list-style-type: none"> <li>• <b>user-authentication</b> – when configured, the accounting starts only after client authentication is successful and stops when the client logs out of the network.</li> <li>• <b>user-association</b> – When configured, the accounting starts when the client associates to the network successfully and stops when the client is disconnected.</li> </ul>	–	user-authentication

Command/Parameter	Description	Range	Default
radius-interim-accounting-interval <minutes>	Configures an interval for posting accounting information as RADIUS INTERIM accounting records to the RADIUS server.  When configured, the IAP sends interim-update messages with current user statistics to the RADIUS server at regular intervals.	Any integer value in minutes	–
radius-reauth-interval <minutes>	Configures an interval at which IAPs can periodically reauthenticate all associated and authenticated clients.	Any integer value in minutes	–
rf-band {2.4 5  all}	Configures the radio frequency band on which this SSID will be broadcast. You can select either 2.4GHz, 5 GHz, or all to specify both bands.	2.4 GHz, 5 GHz, all	all
server-load-balancing	Enables load balancing across two RADIUS servers if two authentication servers are configured for the SSID.	–	Enabled
set-role <attribute> {equals  not-equal starts-with ends-with contains matches-regular-expression} <operator> <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: <ul style="list-style-type: none"> <li>contains – The rule is applied only if the attribute value contains the specified string.</li> <li>ends-with – The rule is applied only if the attribute value ends with the specified string.</li> <li>equals – The rule is applied only if the attribute value is equal to the</li> </ul>	–	–

Command/Parameter	Description	Range	Default
	<p>specified string.</p> <ul style="list-style-type: none"> <li>not-equals – The rule is applied only if the attribute value is not equal to the specified string.</li> <li>starts-with – The rule is applied only if the attribute value begins with the specified string.</li> <li>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 IAP.</li> <li>matches-regular-expression – The rule is applied only if the attribute value matches the regular expression pattern specified in <i>Operand</i>. This operator is available only if the <b>mac-address-and-dhcp-options</b> attribute is selected in the <b>Attribute</b> drop-down.</li> </ul>		
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-authentication-only> <user-authentication-only>	<p>Configures a machine authentication rule.</p> <p>You can assign different rights to clients based on whether their hardware device supports machine authentication.</p> <p>Machine authentication is only supported on Windows devices, so this can be used to</p>	–	–

Command/Parameter	Description	Range	Default
	distinguish between Windows devices and other devices such as iPads.		
set-role-pre-auth <pre-authentication-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 matches-regular-expression}<operator> <VLAN-ID> value-of}	<p>Assigns a VLAN to the clients. The first rule that matches the configured condition is applied.</p> <p>You can specify any of the following conditions:</p> <ul style="list-style-type: none"> <li>contains – The rule is applied only if the attribute value contains the specified string.</li> <li>ends-with – The rule is applied only if the attribute value ends with the specified string.</li> <li>equals – The rule is applied only if the attribute value is equal to the specified string.</li> <li>not-equals – The rule is applied only if the attribute value is not equal to the specified string.</li> <li>starts-with – The rule is applied only if the attribute value begins with the specified string.</li> <li>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 IAP.</li> <li>matches-regular-expression – The</li> </ul>	–	–

Command/Parameter	Description	Range	Default
	rule is applied only if the attribute value matches the regular expression pattern specified in <i>Operand</i> . This operator is available only if the <b>mac-address-and-dhcp-options</b> attribute is selected in the <b>Attribute</b> drop-down.		
termination	<p>Configures the EAP portion of 802.1X authentication on the IAP instead of the RADIUS server.</p> <p>When enabled, this command reduces network traffic to the external RADIUS server by terminating the authorization protocol on the IAP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the IAP acts as a relay for this exchange. The 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.</p>	–	Disabled
type {employee  voice   guest}	Configures the type of network such as employee, voice, or guest network for a WLAN SSID	–	–
vlan <VLAN-id>	Allows the administrators to assign a VLAN to the SSID users.	1...4095	–
wep-key <WEP-key>	Static WEP key associated with the key index. The WEP key	–	–



Command/Parameter	Description	Range	Default
	values can be 10 or 26 hexadecimal characters in length.		
wispr	Enables WISPr authentication for the SSID profile.	–	–
wmm-background-share <Percentage-of-traffic-share>	Allocates bandwidth for background traffic such as file downloads or print jobs.	–	–
wmm-best-effort-share <Percentage-of-traffic-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-video-share <Percentage-of-traffic-share>	Allocates bandwidth for video traffic generated from video streaming.	–	–
wmm-voice-share <Percentage-of-traffic-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	–	–
wpa-passphrase <passphrase>	Defines a WPA passphrase with which you can generate a pre-shared key (PSK).	–	–

## Usage Guidelines

Use this command to configure a WLAN SSID profile to set up an employee, voice, or guest network.

## Example

The following example configures an employee WLAN SSID profile:

```
(Instant Access Point) (config)# wlan ssid-profile employee1
(Instant Access Point) (SSID Profile "employee1")# enable
(Instant Access Point) (SSID Profile "employee1")# index 0
(Instant Access Point) (SSID Profile "employee1")# type employee
(Instant Access Point) (SSID Profile "employee1")# essid employee1
(Instant Access Point) (SSID Profile "employee1")# wpa-passphrase user@123
(Instant Access Point) (SSID Profile "employee1")# opmode wpa2-psk-aes
(Instant Access Point) (SSID Profile "employee1")# max-authentication-failures 0
(Instant Access Point) (SSID Profile "employee1")# vlan 1
(Instant Access Point) (SSID Profile "employee1")# mac-authentication
```

```

(Instant Access Point) (SSID Profile "employee1") # l2-auth-failthrough
(Instant Access Point) (SSID Profile "employee1") # termination
(Instant Access Point) (SSID Profile "employee1") # blacklist
(Instant Access Point) (SSID Profile "employee1") # mac-authentication
(Instant Access Point) (SSID Profile "employee1") # auth-server InternalServer
(Instant Access Point) (SSID Profile "employee1") # rf-band all
(Instant Access Point) (SSID Profile "employee1") # captive-portal disable
(Instant Access Point) (SSID Profile "employee1") # dtim-period 1
(Instant Access Point) (SSID Profile "employee1") # inactivity-timeout 1000
(Instant Access Point) (SSID Profile "employee1") # broadcast-filter none
(Instant Access Point) (SSID Profile "employee1") # dmo-channel-utilization-threshold 90
(Instant Access Point) (SSID Profile "employee1") # local-probe-req-thresh 0
(Instant Access Point) (SSID Profile "employee1") # max-clients-threshold 64
(Instant Access Point) (SSID Profile "employee1") # set-role Group-Name contains wireless employ
ee
(Instant Access Point) (SSID Profile "employee1") # set-vlan mac-address-and-dhcp-options matche
s-regular-expression ..link 200
(Instant Access Point) (SSID Profile "employee1") # end
(Instant Access Point) # commit apply

```

The following example configures a guest WLAN SSID profile:

```

(Instant Access Point) (config) # wlan ssid-profile guestNetwork
(Instant Access Point) (SSID Profile "guestNetwork") # enable
(Instant Access Point) (SSID Profile "guestNetwork") # index 0
(Instant Access Point) (SSID Profile "guestNetwork") # type guest
(Instant Access Point) (SSID Profile "guestNetwork") # essid guestNetwork
(Instant Access Point) (SSID Profile "guestNetwork") # opmode opensystem
(Instant Access Point) (SSID Profile "guestNetwork") # rf-band all
(Instant Access Point) (SSID Profile "guestNetwork") # dtim-period 1
(Instant Access Point) (SSID Profile "guestNetwork") # g-min-tx-rate 1
(Instant Access Point) (SSID Profile "guestNetwork") # g-max-tx-rate 54
(Instant Access Point) (SSID Profile "guestNetwork") # a-min-tx-rate 6
(Instant Access Point) (SSID Profile "guestNetwork") # a-max-tx-rate 54
(Instant Access Point) (SSID Profile "guestNetwork") # inactivity-timeout 1000
(Instant Access Point) (SSID Profile "guestNetwork") # vlan 1
(Instant Access Point) (SSID Profile "guestNetwork") # dmo-channel-utilization-threshold 90
(Instant Access Point) (SSID Profile "guestNetwork") # max-clients-threshold 64
(Instant Access Point) (SSID Profile "guestNetwork") # local-probe-req-thresh 0
(Instant Access Point) (SSID Profile "guestNetwork") # blacklist
(Instant Access Point) (SSID Profile "guestNetwork") # max-authentication-failures 3
(Instant Access Point) (SSID Profile "guestNetwork") # radius-interim-accounting-interval 10
(Instant Access Point) (SSID Profile "guestNetwork") # radius-reauth-interval 30
(Instant Access Point) (SSID Profile "guestNetwork") # captive-portal external
(Instant Access Point) (SSID Profile "guestNetwork") # mac-authentication
(Instant Access Point) (SSID Profile "guestNetwork") # auth-server server1
(Instant Access Point) (SSID Profile "guestNetwork") # set-role-by-ssid
(Instant Access Point) (SSID Profile "guestNetwork") # set-role-pre-auth test1
(Instant Access Point) (SSID Profile "guestNetwork") # end
(Instant Access Point) # commit apply

```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.4	This command is modified.
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and WLAN SSID profile configuration sub-mode.

## wlan sta-profile

```
wlan sta-profile
  essid <ESSID>
  cipher-suite <cipher-suite-string>
  wpa-passphrase <WPA-key>
  uplink-band <band>
  no...
```

### Description

This command enables Wi-Fi uplink on an IAP.

### Syntax

Command/Parameter	Description	Range	Default
wlan sta-profile	Configures a Wi-Fi uplink profile for an 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}	Configures encryption settings. You can specify the following types of encryption: <ul style="list-style-type: none"><li>• clear –To clear a cipher suite</li><li>• wpa-tkip-psk –To use WPA with TKIP encryption along with Pre-shared key (PSK).</li><li>• wpa2-ccmp-psk – To use WPA2 with Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption mode with strong security.</li></ul>	–	–
wpa-passphrase <WPA-key>	Defines a WPA passphrase with which a pre-shared key (PSK) can be generated.  The passphrase must be between 8 and 64 characters.	–	–
uplink-band <band>	Configures the band for uplink connection. The valid options are dot11a and dot11g.	–	–
no...	Removes the configuration	–	–

### Usage Guidelines

Use this command to configure Wi-Fi uplink for a client station connected to an IAP.

### Example

The following commands configure the Wi-Fi uplink profile:

```
(Instant Access Point) (config) # wlan sta-profile
(Instant Access Point) (sta uplink) # uplink-band dot11a
(Instant Access Point) (sta uplink) # uplink-band dot11a
(Instant Access Point) (sta uplink) # cipher-suite wpa-tkip-psk
(Instant Access Point) (sta uplink) # wpa-passphrase user@123
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

IAP Platform	Command Mode
All platforms	Configuration mode and Wi-Fi uplink (sta) sub-mode.

## wlan walled-garden

```
wlan walled-garden
  white-list <domain>
  black-list <domain>
  no...
```

### Description

This command configures a walled garden to control user access to the web content and services. The walled garden access is required when an external captive portal is used.

### Syntax

Command/Parameter	Description	Range	Default
wlan walled-garden	Creates a Walled Garden profile for the 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, <a href="#">yahoo.com/*</a> to provide access to various domains such as <a href="#">news.yahoo.com</a> , <a href="#">travel.yahoo.com</a> and <a href="#">finance.yahoo.com</a> . Similarly, the <a href="#">www.apple.com/library/test</a> is only allow a subset of <a href="#">www.apple.com</a> site corresponding to path <a href="#">/library/test/*</a> .	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, IAP sends an HTTP 403 response to the client with a simple error message.	URLs	–
no...	Removes the configuration.	–	–

### Usage Guidelines

Use this command to configure a walled garden profile. 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.

## Example

The following example configures a walled garden profile:

```
(Instant Access Point) (config) # wlan walled-garden
(Instant Access Point) (Walled Garden) # white-list <domain>
(Instant Access Point) (Walled Garden) # black-list <domain>
(Instant Access Point) (Walled Garden) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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...
```

### Description

This command configures a Wireless Internet Service Provider roaming (WISPr) authentication profile for an IAP. WISPr authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an Internet Service Provider (ISP) with whom the client may not have an account.

### Syntax

Command/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 configuration

### Usage Guidelines

Use this command to configure a WISPr authentication profile for the Captive portal users. Instant supports the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) redirect, authentication, and logoff messages within HTML messages that are sent to the 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](http://www.iso.org) and <http://www.itu.int>).



## Example

The following commands configure a WISPr authentication profile:

```
(Instant Access Point) (config) # wlan wispr-profile
(Instant Access Point) (WISPr) # wispr-location-id-ac 408
(Instant Access Point) (WISPr) # wispr-location-id-cc 1
(Instant Access Point) (WISPr) # wispr-location-id-isocc US
(Instant Access Point) (WISPr) # wispr-location-id-network wispr
(Instant Access Point) (WISPr) # wispr-location-name-location airport
(Instant Access Point) (WISPr) # wispr-location-name-operator-name KNP
(Instant Access Point) (WISPr) # end
(Instant Access Point) # commit apply
```

## Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

## Command Information

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

### Syntax

Parameter	Description
erase <all> <reboot>	Erases the running system configuration file. Rebooting the IAP resets it to the factory default configuration. If you specify all, the configuration and all data in the IAP databases are erased.
memory	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.

### Usage Guidelines

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 IAP:

The IAP returns the following messages:

```
Do you really want to reset the system(y/n): y
System will now restart!
...
Restarting system.
```

### Example

The following command saves your changes so they are retained after a reboot:

```
write memory
```

### Command History

Version	Description
Aruba Instant 6.2.1.0-3.3	This command is introduced.

### Command Information

IAP Platform	Command Mode
All platforms	Privileged EXEC mode



## Acronyms and Abbreviations

The following table lists the abbreviations used in this user guide.

**Table 12:** *List of abbreviations*

Abbreviation	Expansion
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IAP	IAP
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
Instant UI	Instant User Interface
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol

**Table 12:** *List of abbreviations*

Abbreviation	Expansion
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network

## Glossary

The following table lists the terms and their definitions used in this guide.

**Table 13:** *List of Terms*

Term	Definition
802.11	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 CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz 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.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and 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 speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with 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. 802.11n operates in the 2.4 and 5.0 bands.

**Table 13: List of Terms**

Term	Definition
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep a track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.
DNS Server	A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server 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.
DST	Daylight saving time (DST), also known as summer time, is 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.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (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.

**Table 13: List of Terms**

Term	Definition
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.
hotspot	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 hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
IEEE 802.11 standards	The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.
POE	Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways: <ul style="list-style-type: none"> <li>● Endspan– The switch that an AP is connected for power supply.</li> <li>● Midspan– A device can sit between the switch and APs</li> </ul> The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
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.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (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 than commonly offered in today's market.

**Table 13: List of Terms**

Term	Definition
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) 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.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a local area network (LAN) that the users access through a wireless connection.



